تكوين تسجيل جهاز FirePOWER والتحقق منه واستكشاف أخطائه وإصلاحها

المحتويات

المقدمة

يصف هذا المستند إجراءات أستكشاف أخطاء الاتصال وإصلاحها بين FirePOWER Threat Defense (FTD) ومركز إدارة FirePOWER (FMC).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج FTD الإصدار 6.5.x و 6.6.x
- برنامج FMC، الإصدار 6.6.x

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

يصف هذا المستند إجراءات العملية والتحقق واستكشاف أخطاء الاتصال (SFTUNNEL) وإصلاحها بين FTD المدار و FMC المدار.

تستند المعلومات والأمثلة إلى FTD، ولكن معظم المفاهيم تنطبق أيضا بشكل كامل على أجهزة NGIPS (أجهزة سلسلة 7000/8000) أو وحدة FirePOWER على ASA55xx.

يدعم برنامج الإرسال فائق السرعة (FTD) وضعي إدارة رئيسيين:

- ميزة إيقاف التشغيل عبر وحدة التحكم في إدارة اللوحة الأساسية (FMC) - المعروفة أيضا باسم الإدارة عن بعد
- جهاز في المربع عبر FirePOWER Device Manager (FDM) و/أو Cisco Defense Orchestrator (CDO) - المعروف أيضا باسم الإدارة المحلية

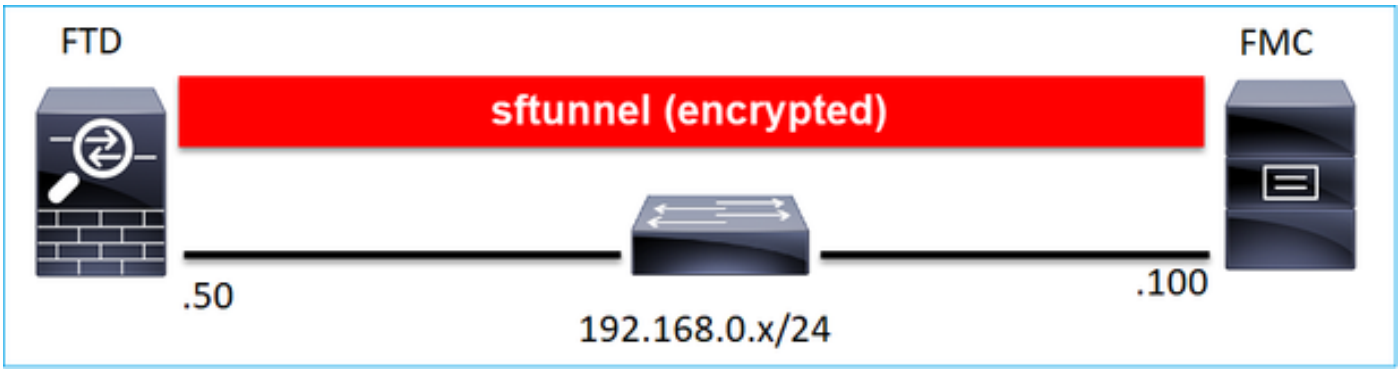
في حالة الإدارة عن بعد، يحتاج برنامج الإرسال فائق السرعة (FTD) أولا للتسجيل في وحدة التحكم في إدارة الأجهزة (FMC) التي تستخدم عملية تعرف باسم تسجيل الأجهزة.

عند إتمام التسجيل، يقوم FTD و FMC بإنشاء نفق آمن يسمى sftunnel (الاسم مشتق من نفق Sourcefire).

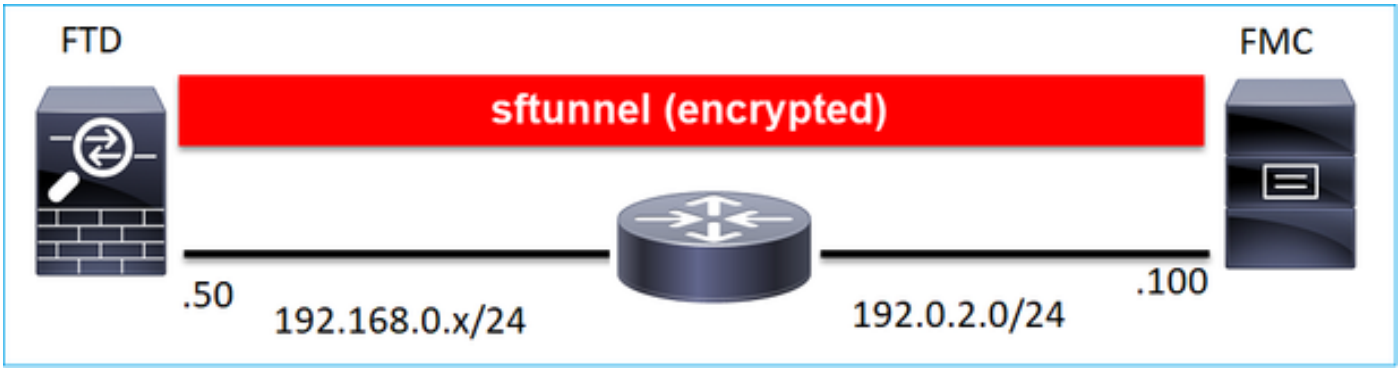
خيارات التصميم

من وجهة نظر تصميمية، يمكن أن يكون FTD - FMC في نفس الشبكة الفرعية من

المستوى الثالث:

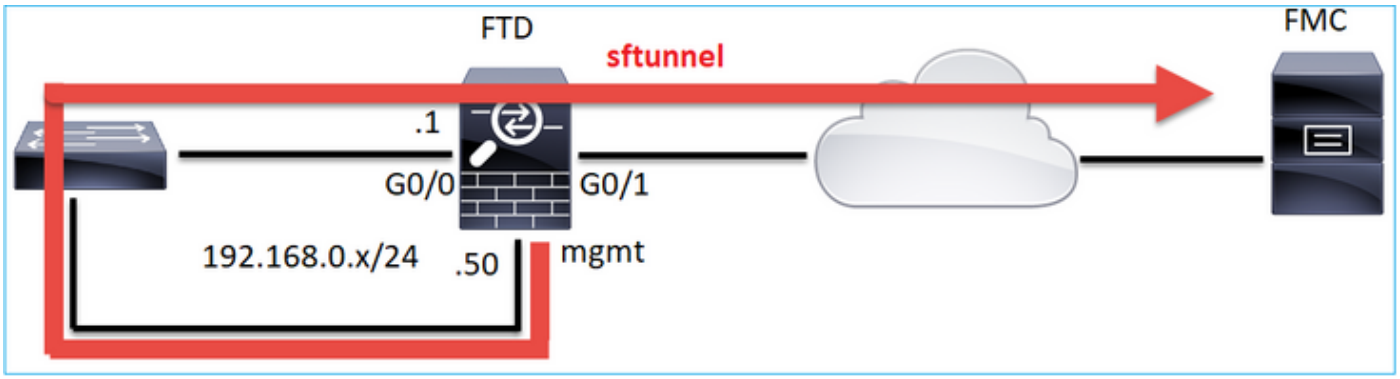


أو أن تكون منفصلة بشبكات مختلفة:



192.0.2.0

ملاحظة: يمكن أيضا ل SFTD نفسه أن يمر. ال ينصح بهذا التصميم. السبب هو أن مشكلة مستوى بيانات FTD يمكن أن تعطل الاتصال بين FTD و FMC.



أية معلومات يجري تبادلها عبر النفق؟

تحتوي هذه القائمة على معظم المعلومات التي يتم نقلها عبر النفق النصفي:

- نبضات قلب الجهاز (رسائل تنشيط الاتصال)

- مزامنة الوقت (NTP)
- الأحداث (الاتصال، التطفل/بروتوكول IPS، الملف، SSL وما إلى ذلك)
- عمليات البحث عن البرامج الضارة
- أحداث/تنبيهات الحماية
- معلومات المستخدم والمجموعة (نهج الهوية)
- معلومات حالة FTD HA
- معلومات حالة نظام مجموعة FTD
- معلومات/أحداث تقنية Security Intelligent (SI)
- معلومات/أحداث مدير إستخبارات التهديدات (TID)
- ملفات ملتقطة
- أحداث اكتشاف الشبكة
- حزمة النهج (نشر النهج)
- مجموعات ترقية البرامج
- حزم برامج التصحيح
- VDBs
- SRUs

ما البروتوكول/المنفذ الذي يتم إستخدامه من قبل Sftunnel؟

يستعمل ال sftunnel TCP ميناء 8305. في الخلفية يوجد نفق TLS:

No.	Source	Destination	Protocol	Length	TCP Segment	Info
57	10.62.148.75	10.62.148.42	TCP	74	0	47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1176730050 TSecr=0 WS=128
58	10.62.148.42	10.62.148.75	TCP	74	0	8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=558472
59	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=29312 Len=0 TSval=1176730050 TSecr=55847291
60	10.62.148.75	10.62.148.42	TLSv1.2	229	163	Client Hello
61	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=30080 Len=0 TSval=55847291 TSecr=1176730051
62	10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Server Hello
63	10.62.148.42	10.62.148.75	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=32128 Len=0 TSval=1176730053 TSecr=55847292
64	10.62.148.42	10.62.148.75	TLSv1.2	803	737	Certificate, Certificate Request, Server Hello Done
65	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=35072 Len=0 TSval=1176730053 TSecr=55847292
66	10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec Encrypted Handshake Message
67	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=35072 Len=0 TSval=55847292 TSecr=1176730056
68	10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
69	10.62.148.75	10.62.148.42	TLSv1.2	364	298	Application Data
70	10.62.148.42	10.62.148.75	TLSv1.2	364	298	Application Data
71	10.62.148.42	10.62.148.75	TLSv1.2	103	37	Application Data
72	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860696607 Ack=279539116 Win=40832 Len=0 TSval=1176730059 TSecr=55847292
73	10.62.148.42	10.62.148.75	TLSv1.2	367	301	Application Data
74	10.62.148.75	10.62.148.42	TLSv1.2	103	37	Application Data
75	10.62.148.75	10.62.148.42	TLSv1.2	367	301	Application Data

كيف أن يغير ال SFTUNNEL TCP ميناء على FTD؟

<#root>

>

configure network management-port 8306

Management port changed to 8306.

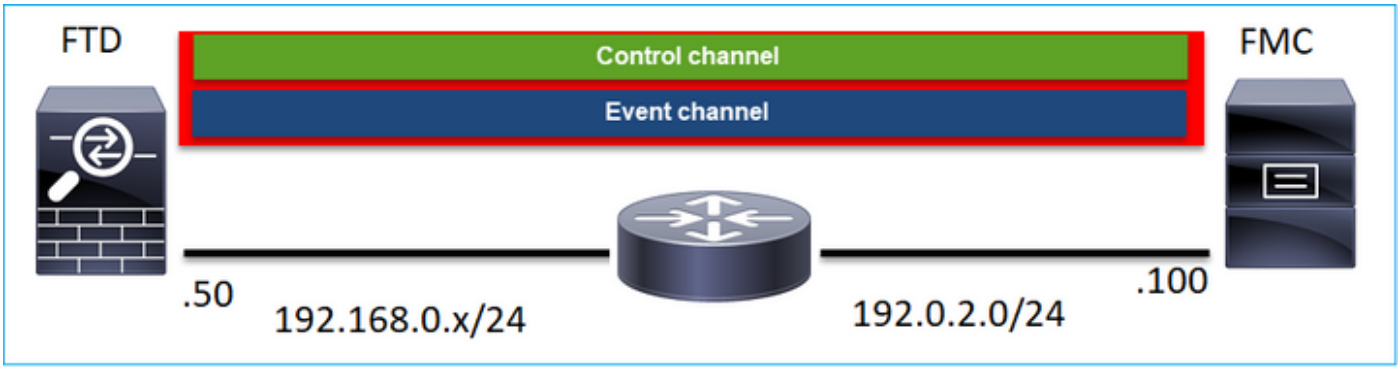
ملاحظة: في هذه الحالة، يجب عليك أيضا تغيير المنفذ على FMC (التكوين > واجهات

الإدارة > الإعدادات المشتركة). ويؤثر ذلك على جميع الأجهزة الأخرى المسجلة بالفعل في وحدة التحكم في الوصول عن بعد (FMC) نفسها. cisco يوصي بشدة أن يحتفظ أنت التقصير عملية إعداد لمنفذ الإدارة عن بعد، غير أن إن الإدارة ميناء يتعارض مع آخر اتصال على شبكتك، أنت يستطيع أخترت ميناء مختلف. إذا قمت بتغيير منفذ الإدارة، فيجب عليك تغييره لجميع الأجهزة الموجودة في عملية النشر التي تحتاج إلى الاتصال معا.

كم عدد الاتصالات التي تم إنشاؤها بواسطة SFTUNNEL؟

يحدد SFTUNNEL إتصالين (قنوات):

- قناة التحكم
- قناة الحدث



ما هو الجهاز الذي يقوم بتهيئة كل قناة؟

ذلك يعتمد على السيناريو. تحقق من السيناريوهات التي يتم وصفها في باقي المستند.

التكوين

أساسيات التسجيل

واجهة سطر الأوامر في FTD

في FTD، تكون الصياغة الأساسية لتسجيل الجهاز:

> تكوين إضافة مدير <FMC Host> <مفتاح التسجيل> <nat ID>

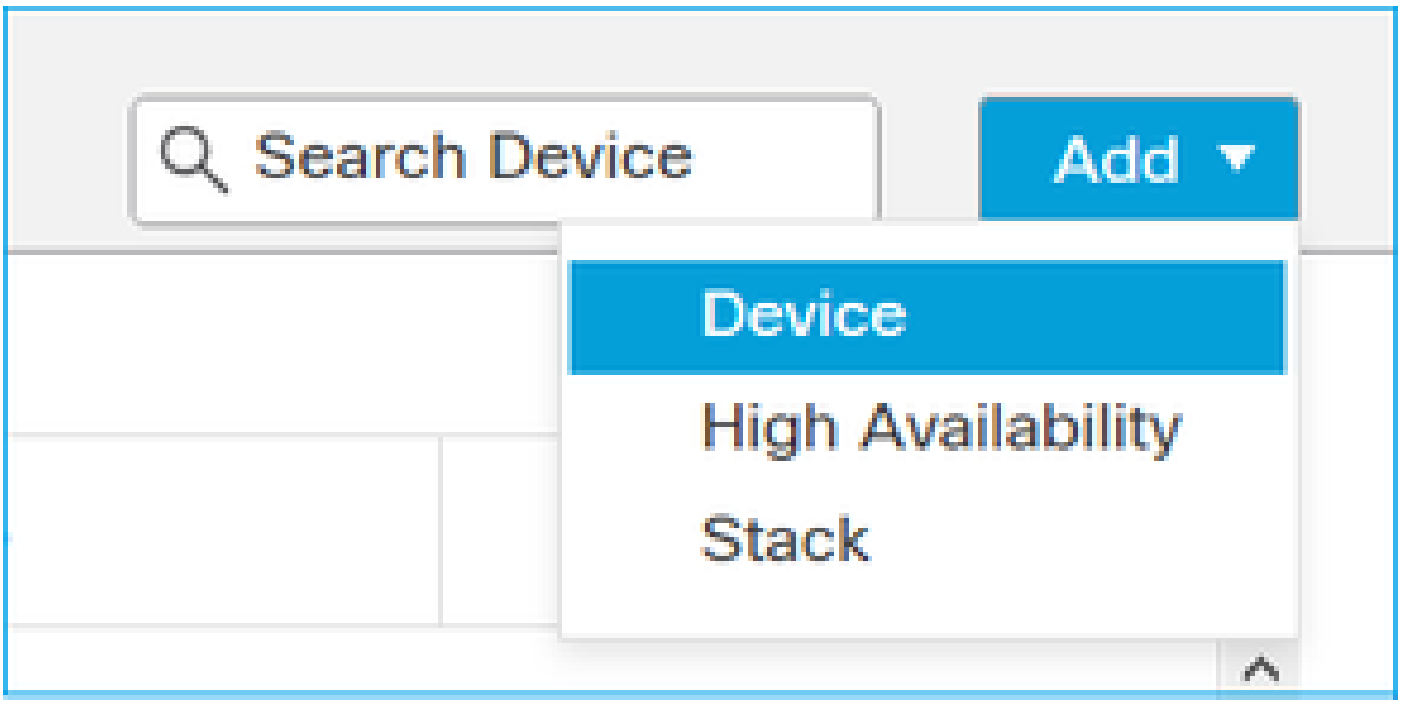
القيمة	الوصف

مضيف FMC	يمكن أن يكون هذا إما: • اسم المضيف • عنوان IPv4 • عنوان IPv6 • Dontresolve
مفتاح التسجيل	هذه عبارة عن سلسلة أبجدية رقمية سرية مشتركة (بين 2 و 36 حرفا) تستخدم لتسجيل الجهاز. يسمح فقط بالأبجدية والرقم الرقمي والواصلة (-) وعلامة التسطير السفلي (_) والنقطة (.).
معرف NAT	خيط أبجدي رقمي يستخدم أثناء عملية التسجيل بين وحدة التحكم في إدارة اللوحة (FMC) والجهاز عندما لا يحدد جانب عنوان IP. حدد نفس معرف NAT على FMC.

للحصول على تفاصيل إضافية، تحقق من مرجع أمر الدفاع عن تهديد الحماية من Cisco Firepower

واجهة مستخدم FMC

على FMC، انتقل إلى الأجهزة > إدارة الأجهزة. حدد إضافة > جهاز



Add Device

Host:*

Display Name:

Registration Key:*

Domain:

Select Domain

Group:

None

Access Control Policy:*

Smart Licensing

- [ ] Malware
- [ ] Threat
- [ ] URL Filtering

Advanced

Unique NAT ID:*

- [x] Transfer Packets

واجهة سطر الأوامر في FTD

> تكوين مدير إضافة <FMC ساكن إستاتيكي IP> <مفتاح التسجيل>

على سبيل المثال:

<#root>

```
>
configure manager add 10.62.148.75 Cisco-123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

معلومات أساسية

ما إن يدخل أنت ال FTD أمر ال FTD يحاول أن يربط إلى ال FMC كل 20 ثانية، غير أن بما أن ال FMC ال يشكل بعد هو يرد مع TCP RST:

<#root>

```
>
capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection?
0

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
-n host 10.62.148.75
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:53:33.365513 IP 10.62.148.42.46946 > 10.62.148.75.8305: Flags
[S]
, seq 2274592861, win 29200, options [mss 1460,sackOK,TS val 55808298 ecr 0,nop,wscale 7], length 0
18:53:33.365698 IP 10.62.148.75.8305 > 10.62.148.42.46946: Flags
[R.]
```

```
, seq 0, ack 2274592862, win 0, length 0
18:53:53.365973 IP 10.62.148.42.57607 > 10.62.148.75.8305: Flags

[S]

, seq 1267517632, win 29200, options [mss 1460,sackOK,TS val 55810298 ecr 0,nop,wscale 7], length 0
18:53:53.366193 IP 10.62.148.75.8305 > 10.62.148.42.57607: Flags

[R.]

, seq 0, ack 1267517633, win 0, length 0
18:54:13.366383 IP 10.62.148.42.55484 > 10.62.148.75.8305: Flags

[S]

, seq 4285875151, win 29200, options [mss 1460,sackOK,TS val 55812298 ecr 0,nop,wscale 7], length 0
18:54:13.368805 IP 10.62.148.75.8305 > 10.62.148.42.55484: Flags

[R.]

, seq 0, ack 4285875152, win 0, length 0
```

حالة تسجيل الجهاز:

```
<#root>

>

show managers

Host                    : 10.62.148.75
Registration Key        : ****
Registration            : pending
RPC Status              :
Type                    : Manager
Host                    : 10.62.148.75
Registration            : Pending
```

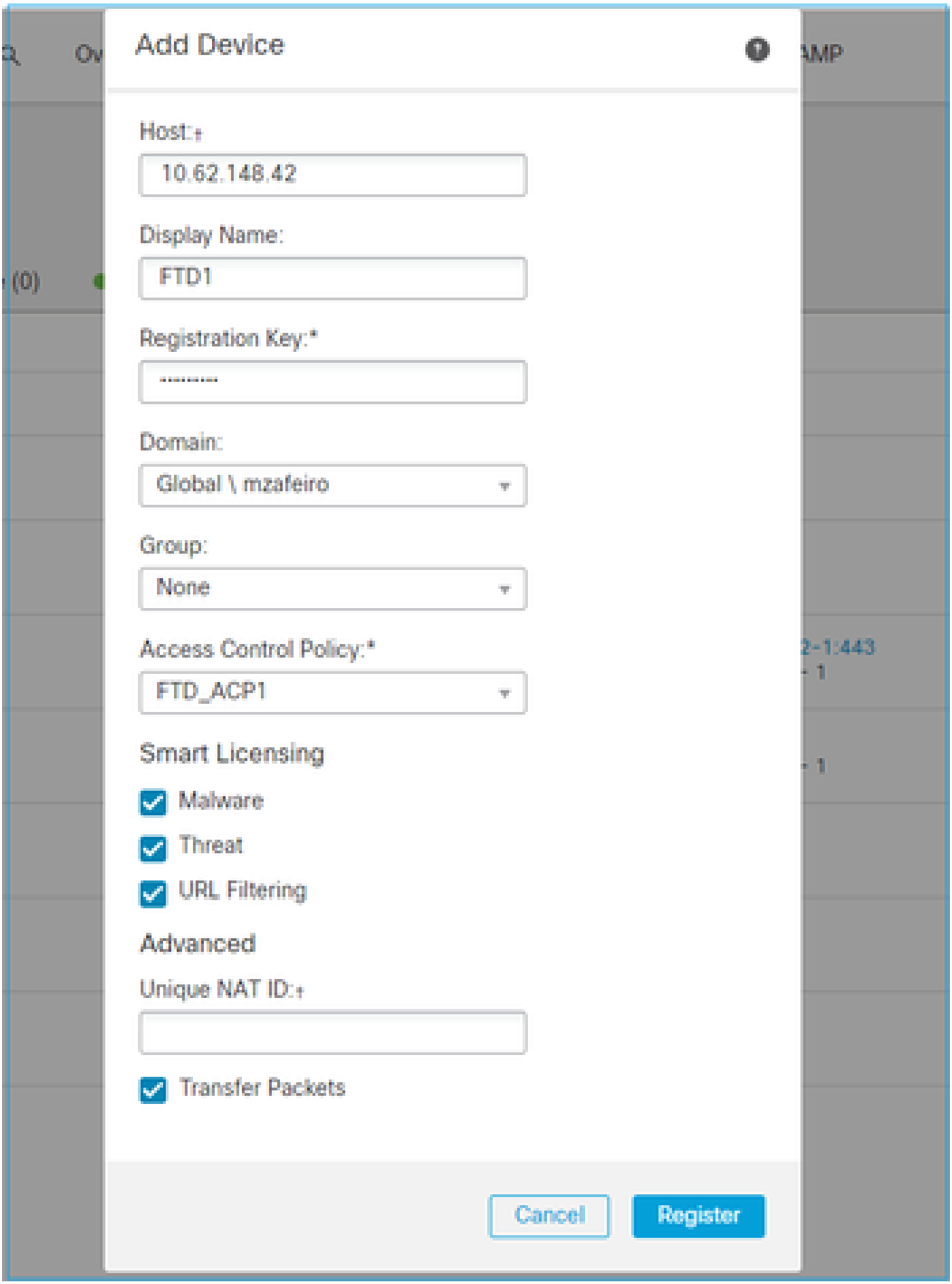
يستمع FTD على منفذ TCP 8305:

```
<#root>

admin@vFTD66:~$

netstat -na | grep 8305

tcp        0      0 10.62.148.42:

8305

       0.0.0.0:*

LISTEN
```

واجهة مستخدم FMC

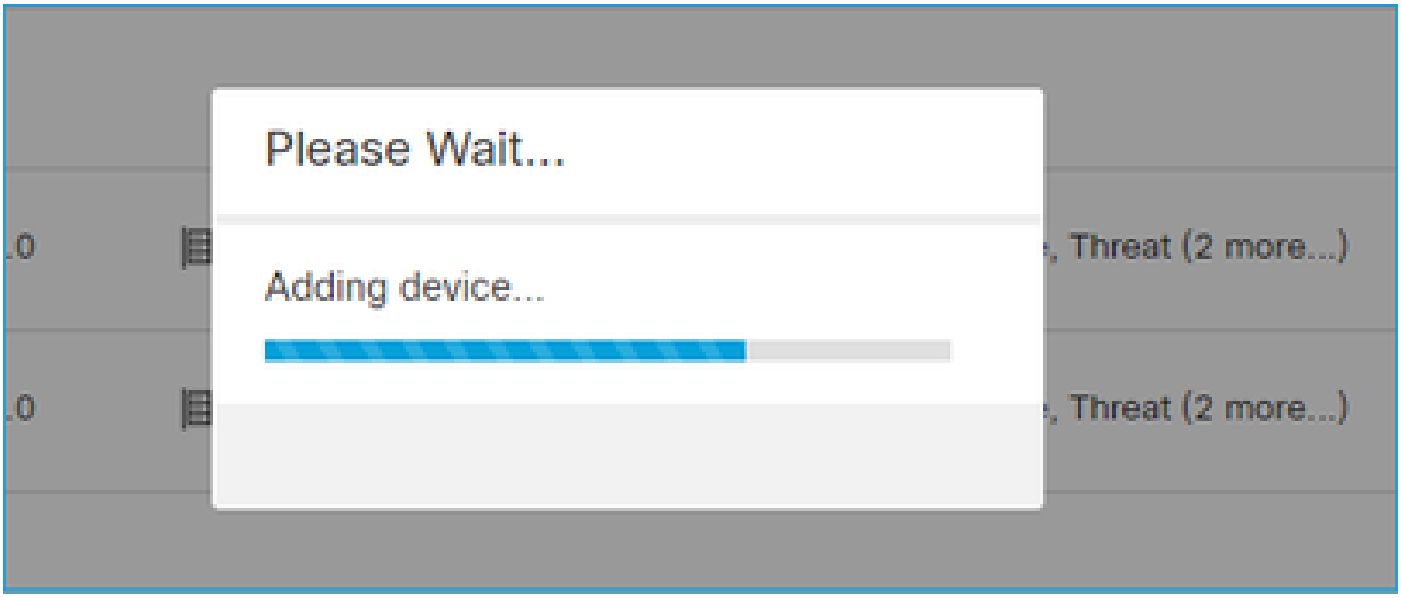
في هذه الحالة، قم بتعيين:

- المضيف (عنوان IP الخاص ب FTD)
- اسم العرض
- مفتاح التسجيل (يجب أن يطابق هذا المفتاح المفتاح الذي تم تكوينه على FTD)
- سياسة التحكم في الوصول
- مجال
- معلومات الترخيص الذكي


Add Device
Host:*
10.62.148.42
Display Name:
FTD1
Registration Key:*
Domain:
Global \ mzafeiro
Group:
None
Access Control Policy:*
FTD_ACP1
Smart Licensing
Malware
Threat
URL Filtering
Advanced
Unique NAT ID:*
Transfer Packets
Cancel
Register

تحديد التسجيل

تبدأ عملية التسجيل:



تبدأ FMC في الإنصات على منفذ TCP 8305:

<#root>

admin@FMC2000-2:~$

netstat -na | grep 8305

tcp 0 0 10.62.148.75:

8305

0.0.0.0:*

LISTEN

في الخلفية يقوم FMC بدء اتصال TCP:

<#root>

```
20:15:55.437434 IP 10.62.148.42.49396 > 10.62.148.75.8305: Flags [S], seq 655146775, win 29200, options
20:15:55.437685 IP 10.62.148.75.8305 > 10.62.148.42.49396: Flags [R.], seq 0, ack 655146776, win 0, len
20:16:00.463637 ARP, Request who-has 10.62.148.42 tell 10.62.148.75, length 46
20:16:00.463655 ARP, Reply 10.62.148.42 is-at 00:50:56:85:7b:1f, length 28
20:16:08.342057 IP
```

10.62.148.75

.50693 > 10.62.148.42.8305: Flags

[S]

```
, seq 2704366385, win 29200, options [mss 1460,sackOK,TS val 1181294721 ecr 0,nop,wscale 7], length 0
20:16:08.342144 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags
```

[S.]

```
, seq 1829769842,
```

ack

```
 2704366386, win 28960, options [mss 1460,sackOK,TS val 56303795 ecr 1181294721,nop,wscale 7], length 0
20:16:08.342322 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [.],
```

ack

```
 1, win 229, options [nop,nop,TS val 1181294722 ecr 56303795], length 0
20:16:08.342919 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win 229, optio
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.], ack 164, win 235, options [nop,no
```

يتم إنشاء قناة التحكم في SFTUNNEL:

<#root>

```
admin@FMC2000-2:~$
```

netstat -na | grep 8305

```
tcp        0      0 10.62.148.75:8305       0.0.0.0:*               LISTEN
tcp        0      0
```

10.62.148.75:50693 10.62.148.42:8305

ESTABLISHED

<#root>

```
>
```

sftunnel-status

```
SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020

        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 4
        Reserved SSL connections: 0
        Management Interfaces: 1
        eth0 (control events) 10.62.148.42,

**********************

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
```

ChannelA Connected: Yes, Interface eth0

```
ChannelB Connected: No

        Registration: Completed.
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020


PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
        eth0 (control events) 10.62.148.75,

Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to '10.62.148.75' via '10.62.14


Peer channel Channel-B is not valid
```

بعد دقائق قليلة، يتم تأسيس قناة الحدث. يمكن أن يكون بادئ قناة الحدث إما جانب. في هذا المثال، كان FMC:

```
<#root>

20:21:15.347587 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags

[S]

, seq 3414498581, win 29200, options [mss 1460,sackOK,TS val 1181601702 ecr 0,nop,wscale 7], length 0
20:21:15.347660 IP 10.62.148.42.8305 > 10.62.148.75.43957: Flags

[S.]

, seq 2735864611,

ack

 3414498582, win 28960, options [mss 1460,sackOK,TS val 56334496 ecr 1181601702,nop,wscale 7], length 0
20:21:15.347825 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [.],

ack

 1, win 229, options [nop,nop,TS val 1181601703 ecr 56334496], length 0
20:21:15.348415 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win 229, optio
```

يشير منفذ المصدر العشوائي إلى بادئ الاتصال:

```
<#root>

admin@FMC2000-2:~$

netstat -na | grep 10.62.148.42

tcp        0      0 10.62.148.75:

50693

      10.62.148.42:8305       ESTABLISHED
```

```
tcp        0      0 10.62.148.75:
43957
      10.62.148.42:8305       ESTABLISHED
```

في حال تم بدء قناة الحدث من قبل FTD، يكون الإخراج:

```
<#root>
admin@FMC2000-2:~$
netstat -na | grep 10.62.148.42
tcp        0      0 10.62.148.75:
58409
      10.62.148.42:8305       ESTABLISHED
tcp        0      0 10.62.148.75:8305       10.62.148.42:
46167
      ESTABLISHED
```

من جانب FTD:

```
<#root>
>
sftunnel-status

SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020

        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 6
        Reserved SSL connections: 0
        Management Interfaces: 1
        eth0 (control events) 10.62.148.42,

**********************

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)

ChannelA Connected: Yes,

Interface eth0
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)

 ChannelB Connected: Yes,

Interface eth0
        Registration: Completed.
```

```
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020

PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
        eth0 (control events) 10.62.148.75,

 Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to '10.62.148.75' via '10.62.1
        Peer channel Channel-B is valid  type (EVENT), using 'eth0', connected to '10.62.148.75' via '10
```

<#root>

>

show managers

Type : Manager
Host : 10.62.148.75

Registration : Completed

>

السيناريو 2. FTD DHCP عنوان - FMC ساكن إستاتيكي عنوان

في هذا السيناريو، حصلت واجهة إدارة FTD على عنوان IP الخاص به من خادم DHCP:

واجهة سطر الأوامر في FTD

أنت ينبغي عينت ال nat id:

> تكوين مدير إضافة <FMC ثابت IP> <مفتاح التسجيل> <nat ID>

على سبيل المثال:

```
<#root>

>

configure manager add 10.62.148.75 Cisco-123 nat123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

حالة تسجيل FTD:

```
<#root>

>

show managers

Host                    : 10.62.148.75
Registration Key        : ****

Registration            : pending

RPC Status              :
Type                    : Manager
Host                    : 10.62.148.75
Registration            : Pending
```

واجهة مستخدم FMC

في هذه الحالة، قم بتعيين:

- اسم العرض
- مفتاح التسجيل (يجب أن يطابق هذا المفتاح المفتاح الذي تم تكوينه على FTD)
- سياسة التحكم في الوصول
- مجال
- معلومات الترخيص الذكي
- معرف NAT (يكون هذا مطلوبا عند عدم تحديد المضيف. يجب أن تتطابق مع تلك التي تم تكوينها على FTD)

Add Device

Host:*

empty

Display Name:

FTD1

Registration Key:*

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

- [x] Malware
- [x] Threat
- [x] URL Filtering

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

من الذي يبدأ SFTUNNEL في هذه الحالة؟

يقوم FTD بتهيئة كل من إتصالات القناة:

<#root>

```
ftd1:/home/admin#
```

netstat -an | grep 148.75

```
tcp        0      0 10.62.148.45:
```

40273

```
      10.62.148.75:8305       ESTABLISHED
tcp        0      0 10.62.148.45:
```

39673

```
      10.62.148.75:8305       ESTABLISHED
```

السيناريو 3. عنوان IP الثابت ل FTD - عنوان IP ل FMC DHCP

<#root>

```
>
```

configure manager add DONTRESOLVE Cisco-123 nat123

```
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

ملاحظة: يتطلب الأمر إستخدام NAT ID.

واجهة مستخدم FMC

في هذه الحالة قم بتحديد:

- عنوان IP ل FTD
- اسم العرض
- مفتاح التسجيل (يجب أن يطابق هذا المفتاح المفتاح الذي تم تكوينه على FTD)
- سياسة التحكم في الوصول
- مجال
- معلومات الترخيص الذكي
- معرف NAT (يجب أن يطابق المعرف الذي تم تكوينه على FTD)

Add Device

Host:*

10.62.148.42

Display Name:

FTD1

Registration Key:*

.....

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

- [x] Malware
- [x] Threat
- [x] URL Filtering

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

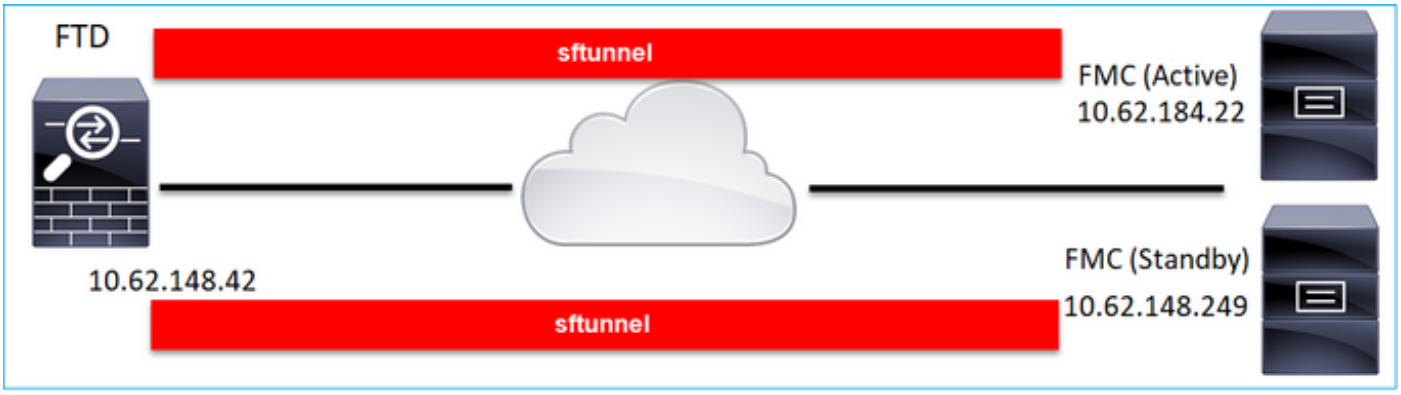
- تقوم FMC بتهيئة قناة التحكم.
- يمكن بدء قناة الحدث من قبل أي من الجانبين.

```
<#root>

root@FMC2000-2:/Volume/home/admin#

netstat -an | grep 148.42

tcp        0      0 10.62.148.75:

50465

      10.62.148.42:8305       ESTABLISHED
tcp        0      0 10.62.148.75:

48445

      10.62.148.42:8305       ESTABLISHED
```

السيناريو 4. التسجيل في برنامج الإرسال فائق السرعة (FTD) إلى FMC HA

في FTD قم بتكوين FMC النشط فقط:

```
<#root>

>

configure manager add 10.62.184.22 cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

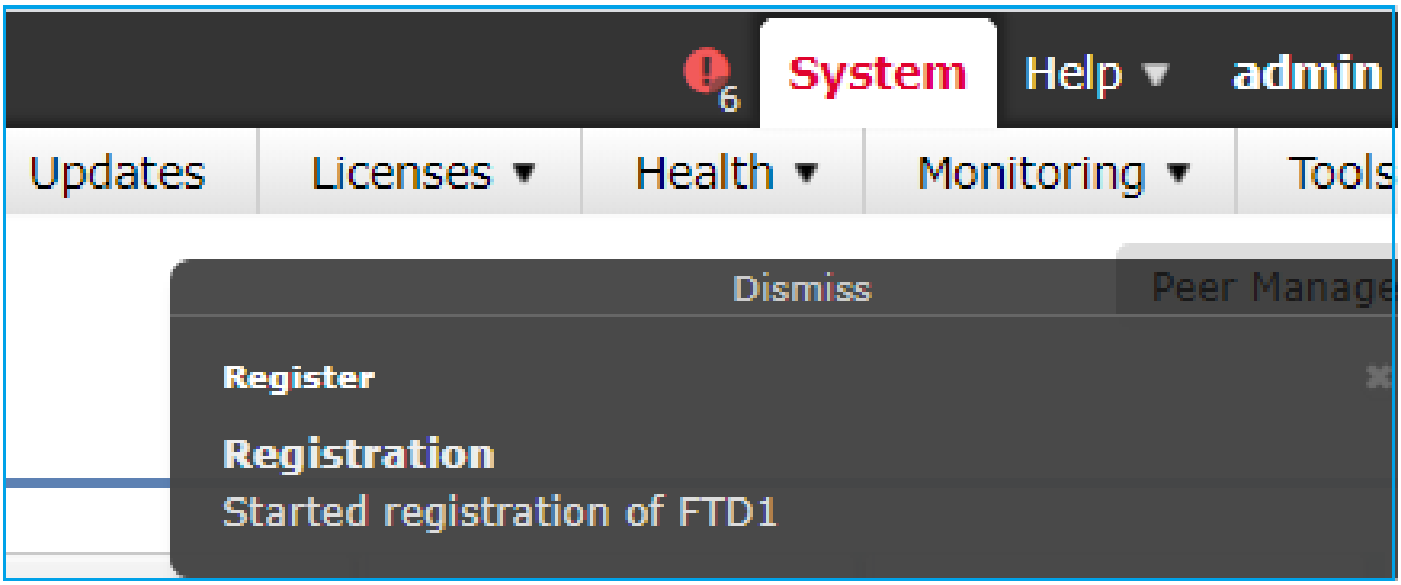


ملاحظة: تأكد من السماح بحركة مرور منفذ TCP 8305 من FTD إلى كل من FMCs.

أولا، تم إنشاء FMC Tunnel to Active:

```
<#root>

>

show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed
```

بعد بضع دقائق يبدأ FTD التسجيل إلى FMC في وضع الاستعداد:




```
<#root>

>

show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed


Type                    : Manager
```

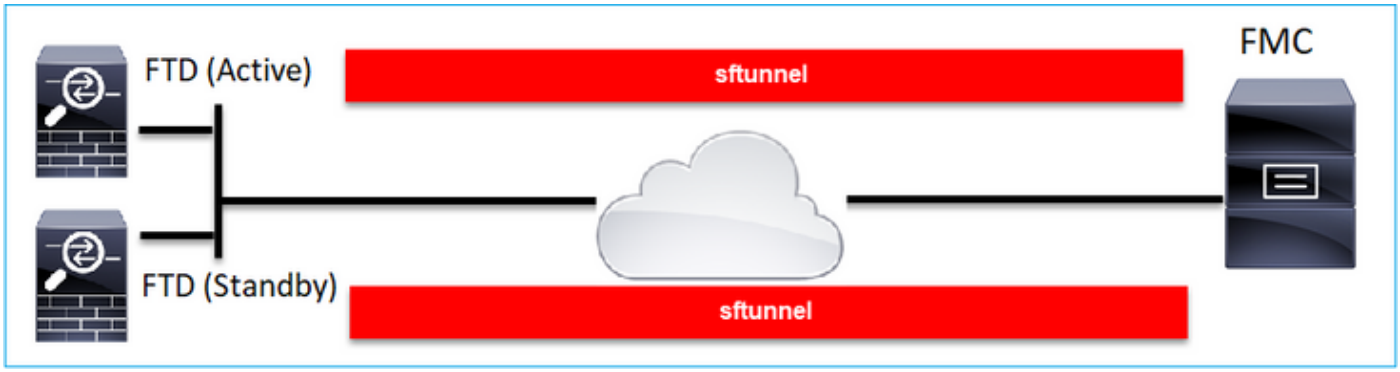
```
Host                          :

10.62.148.249

Registration                  : Completed
```

في خلفية FTD، يتم إنشاء قناتي تحكم (واحدة لكل وحدة تحكم في الإدارة الفيدرالية (FMC)) وقناتي أحداث (واحدة لكل وحدة تحكم في الإدارة الفيدرالية (FMC)):

```
<#root>

ftd1:/home/admin#

netstat -an | grep 8305

tcp        0      0 10.62.148.42:8305       10.62.184.22:36975      ESTABLISHED
tcp        0      0 10.62.148.42:42197      10.62.184.22:8305       ESTABLISHED
tcp        0      0 10.62.148.42:8305       10.62.148.249:45373     ESTABLISHED
tcp        0      0 10.62.148.42:8305       10.62.148.249:51893     ESTABLISHED
```

السيناريو 5. إف تي دي اه

في حالة نظام الإرسال فائق السرعة (FTD)، تحتوي كل وحدة على نفق منفصل إلى FMC:

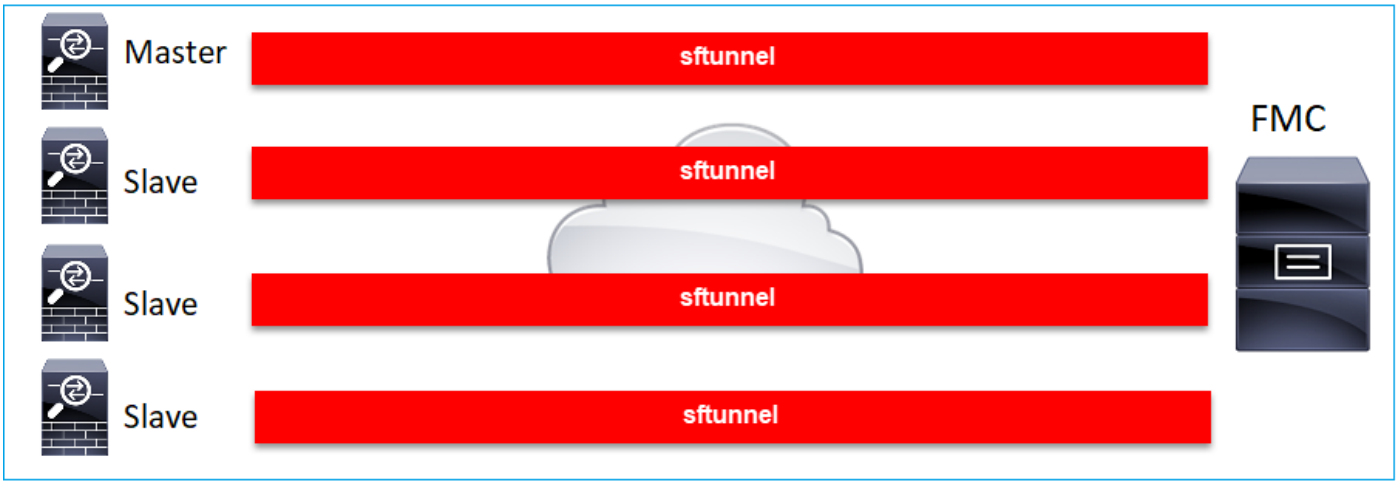


تقوم بتسجيل كل من FTD بشكل مستقل ثم من FMC تقوم بتكوين FTD HA. لمزيد من التفاصيل، راجع:

- تكوين برنامج FTD عالي التوافر على أجهزة Firepower
- إمكانية توفر عالية للدفاع عن تهديد الطاقة النارية

السيناريو 6. مجموعة برنامج الإرسال فائق السرعة (FTD)

في حالة "نظام مجموعة الإرسال فائق السرعة (FTD)"، تحتوي كل وحدة على نفق منفصل إلى وحدة التحكم في إدارة الوحة الأساسية (FMC). اعتبارا من إصدار وحدة التحكم في برنامج الإرسال فائق السرعة (FMC) إصدار 6.3، لا تحتاج سوى إلى تسجيل وحدة التحكم في برنامج الإرسال فائق السرعة (FMC) إلى وحدة التحكم في برنامج الإرسال فائق السرعة (FTD). ثم تتولى وحدة إدارة الاتصالات الفيدرالية رعاية بقية الوحدات ويتم الاكتشاف التلقائي + تسجيلها.

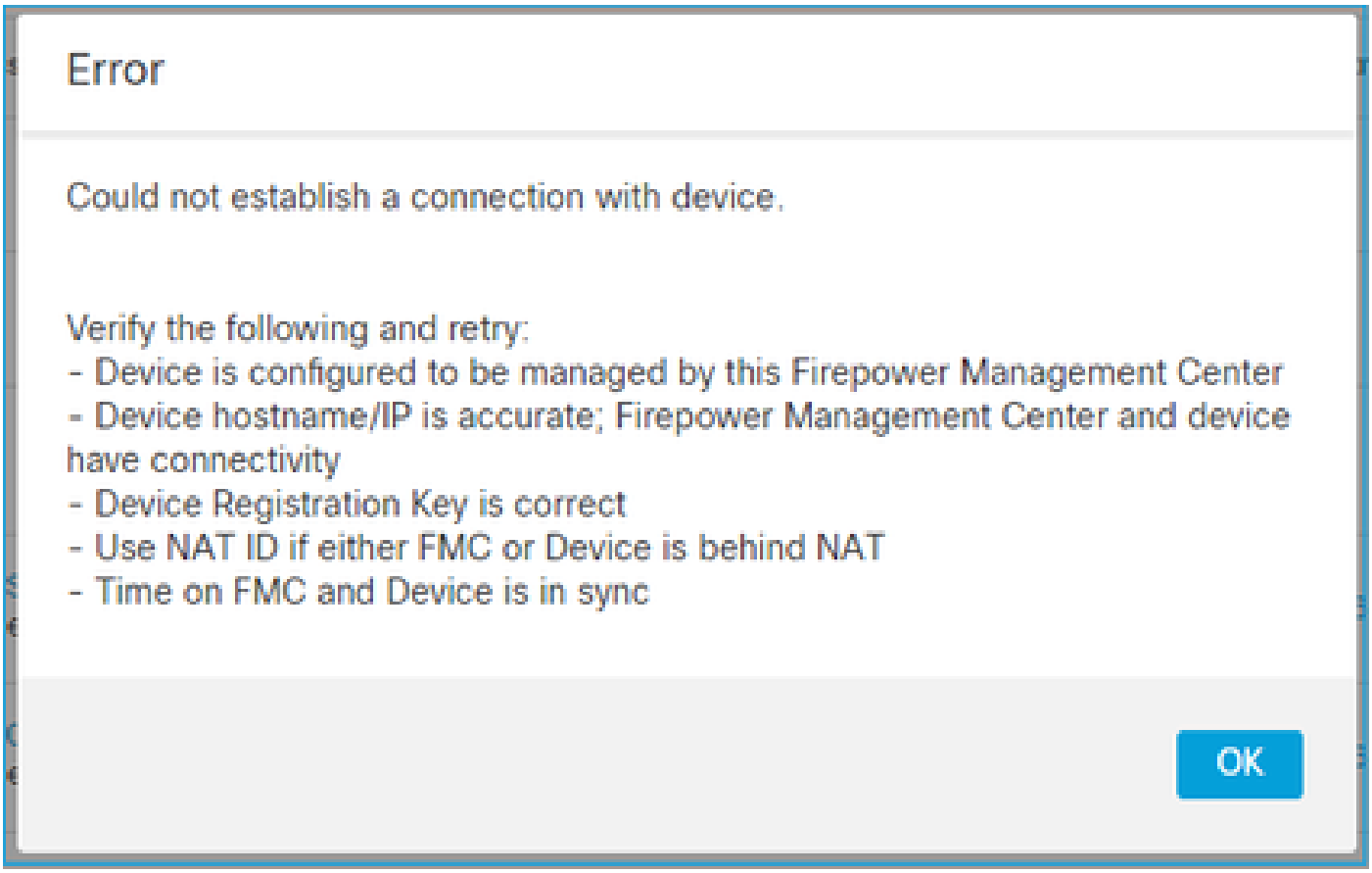


ملاحظة: نوصي بإضافة وحدة التحكم للحصول على أفضل أداء، ولكن يمكنك إضافة أي وحدة من نظام المجموعة. لمزيد من التفاصيل، تحقق من إنشاء مجموعة دفاع ضد تهديدات الطاقة النارية

أستكشاف المشكلات الشائعة وإصلاحها

1. بناء جملة غير صالح على واجهة سطر الأوامر (CLI) ل FTD

في حالة وجود بناء جملة غير صالح على FTD ومحاولة تسجيل فاشلة، تظهر واجهة مستخدم FMC رسالة خطأ عامة تمامًا:



في هذا الأمر، يكون الكلمة الأساسية مفتاح التسجيل بينما يكون Cisco123 هو معرف nat. من الشائع جدا إضافة مفتاح الكلمة الأساسية بينما لا يوجد من الناحية الفنية كلمة أساسية من هذا القبيل:

```
<#root>

>

configure manager add 10.62.148.75 key cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

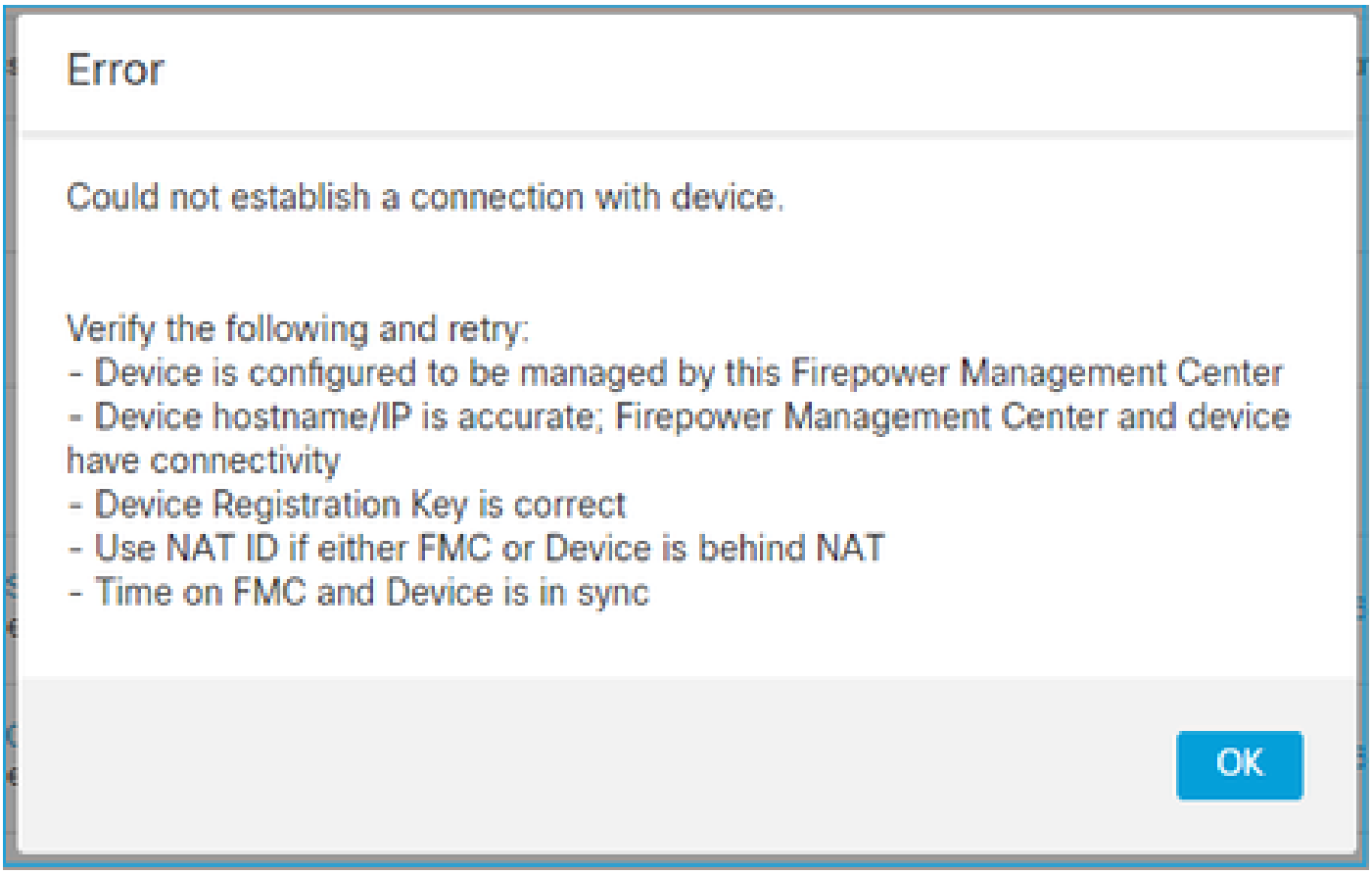
الإجراء الموصى به

أستخدم الصياغة المناسبة ولا تستخدم الكلمات الأساسية غير الموجودة.

```
<#root>

>

configure manager add 10.62.148.75 cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

2. عدم تطابق مفتاح التسجيل بين FTD - FMC

ظهر واجهة مستخدم FMC:



الإجراء الموصى به

في FTD تحقق من ملف /ngfw/var/log/messages لمشاكل المصادقة.

الطريقة 1 - تحقق من السجلات السابقة

```
<#root>

>

system support view-files

Type a sub-dir name to list its contents:

s


Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
>
```

```
messages
Apr

 19 04:02:05 vFTD66 syslog-ng[1440]: Configuration reload request received, reloading configuration;
Apr 19 04:02:07 vFTD66 SF-IMS[3116]: [3116] pm:control [INFO] ControlHandler auditing message->type 0x9
w/usr/bin/perl /ngfw/usr/local/sf/bin/run_hm.pl --persistent', pid 19455 (uid 0, gid 0)

/authenticate


Apr 19 20:17:14 vFTD66 SF-IMS[18974]: [19131] sftunneld:sf_ssl [WARN] Accept:

Failed to authenticate peer '10.62.148.75' <- The problem
```

الطريقة 2 - تحقق من السجلات المباشرة

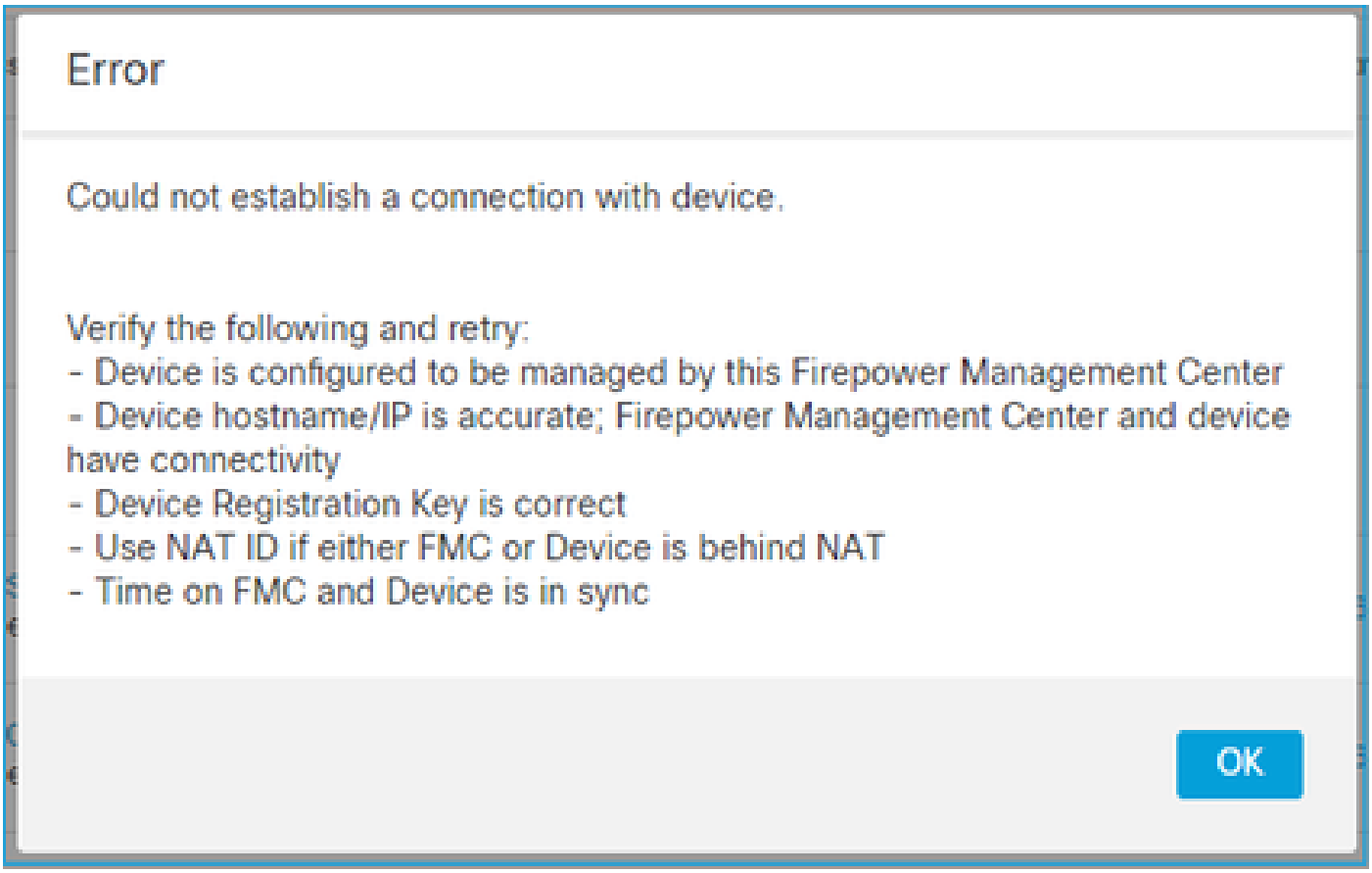
```
<#root>

>

expert
ftd1:~$


sudo su

Password:
ftd1::/home/admin#

tail -f /ngfw/var/log/messages
```

على FTD تحقق من محتويات ملف /etc/sf/sftunnel.conf للتأكد من صحة مفتاح التسجيل:

```
<#root>

ftd1:~$

cat /etc/sf/sftunnel.conf | grep reg_key

        reg_key

cisco-123

;
```

3. مشكلات الاتصال بين FTD - FMC

تظهر واجهة مستخدم FMC:



الإجراءات الموصى بها

- تأكد من عدم وجود جهاز في المسار (على سبيل المثال، جدار حماية) يمنع حركة مرور البيانات (TCP 8305). في حالة FMC HA، تأكد من السماح بحركة المرور إلى منفذ TCP 8305 من وإلى كل FMCs.
- قم بالتقاط الصور للتحقق من الاتصال ثنائي الإتجاه. في FTD أستخدم الأمر capture-traffic. تأكد من وجود مصافحة TCP ثلاثية الإتجاه وعدم وجود حزم TCP FIN أو RST.

```
<#root>

>

capture-traffic


Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection?

0


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n host 10.62.148.75
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:56:09.393655 IP 10.62.148.42.53198 > 10.62.148.75.8305: Flags
```

[S]

```
, seq 3349394953, win 29200, options [mss 1460,sackOK,TS val 1033596 ecr 0,nop,wscale 7], length 0
20:56:09.393877 IP 10.62.148.75.8305 > 10.62.148.42.53198: Flags
```

[R.]

```
, seq 0, ack 3349394954, win 0, length 0
20:56:14.397412 ARP, Request who-has 10.62.148.75 tell 10.62.148.42, length 28
20:56:14.397602 ARP, Reply 10.62.148.75 is-at a4:6c:2a:9e:ea:10, length 46
```

وبالمثل، قم بالتقاط وحدة التحكم في إدارة الاتصالات الفيدرالية (FMC) لضمان الاتصال ثنائي الإتجاه:

<#root>

```
root@FMC2000-2:/var/common#
```

tcpdump -i eth0 host 10.62.148.42 -n -w sftunnel.pcap

يوصى أيضا بتصدير الالتقاط بتنسيق PCAP والتحقق من محتويات الحزمة:

<#root>

```
ftd1:/home/admin#
```

tcpdump -i eth0 host 10.62.148.75 -n -w tunnel.pcap

```
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

الأسباب المحتملة:

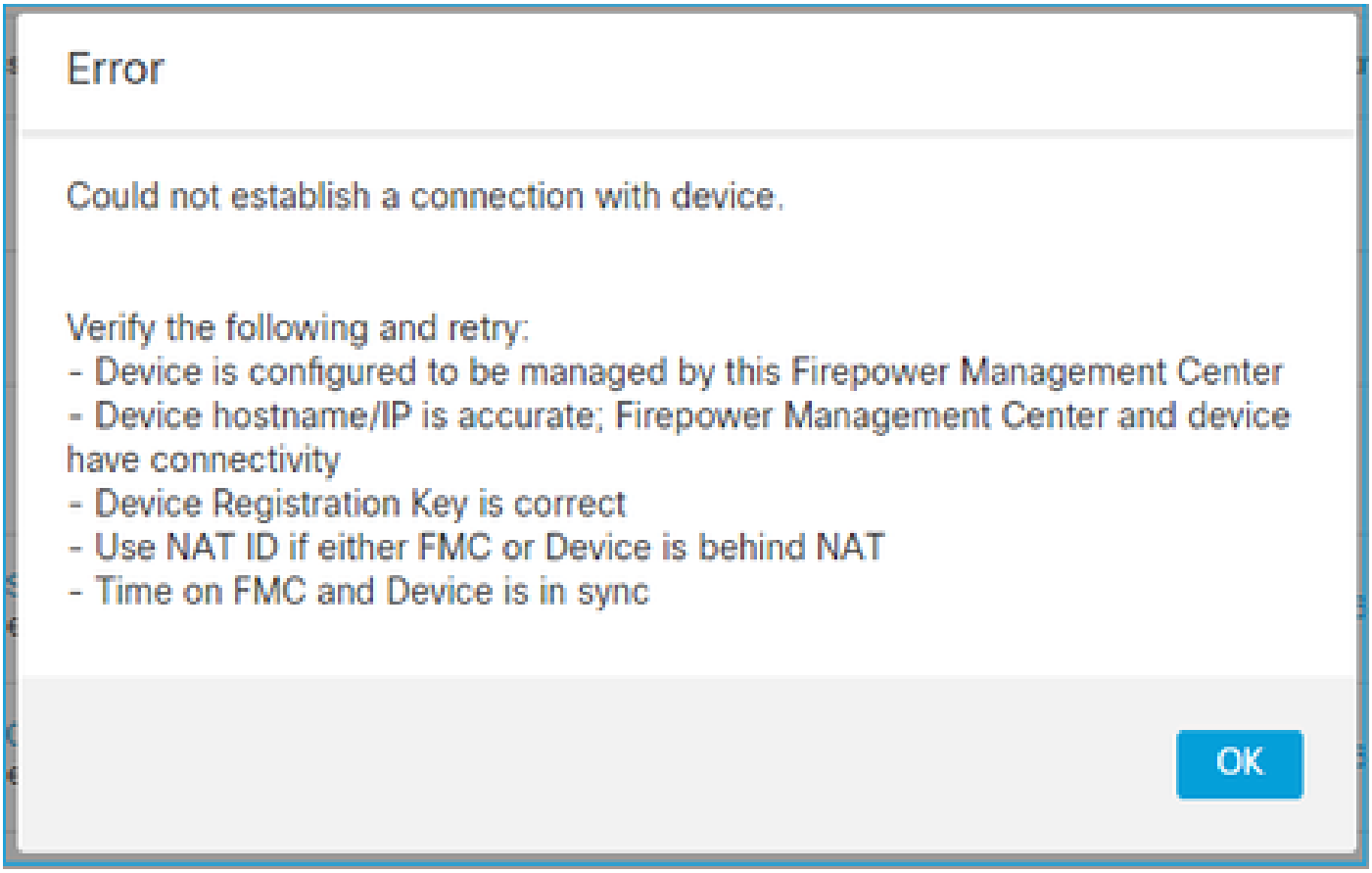
- ال تتوفر في وحدة التحكم في إدارة للوحة الأساسية (FTD) جهاز تمت إضافته.
- يقوم جهاز في المسار (على سبيل المثال، جدار الحماية) بحظر حركة المرور أو تعديلها.
- ال يتم توجيه الحزم بشكل صحيح في المسار.
- عملية SFTUNNEL على FTD أو FMC معطلة (تحقق من السيناريو 6)
- هناك مشكلة MTU في المسار (تدقيق سيناريو).

لتحليل الالتقاط تحقق من هذا المستند:

تحليل لقطات Firepower Firewall (جدار حماية Firepower) الاستكشاف مشكلات الشبكة وإصلاحها بشكل أعمق

4. البرامج غير المتوافقة بين FTD - FMC

ظهر واجهة مستخدم FMC:



الإجراء الموصى به

تحقق من ملف FTD /ngfw/var/log/messages:

<#root>

```
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] Need to send SW
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState do_d
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_heartbeat [INFO] Saved SW VERSION f
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:ssl_mac [WARN]

FMC(manager) 10.62.148.247 send unsupported version 10.10.0.4

Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] <<<<<<<<<<<<<<<<<
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:stream_file [INFO] Stream CTX destroye
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState Shut
```

تحقق من مصفوفة توافق Firepower:

دليل توافق Cisco Firepower

5. فرق الوقت بين FTD و FMC

يعد اتصال FTD-FMC حساسا لفروق الوقت بين الجهازين. 2. من متطلبات التصميم أن
تتم مزامنة FTD و FMC مع نفس خادم NTP.

وعلى وجه الخصوص، عند تثبيت برنامج FTD على نظام أساسي مثل 41xx أو 93xx، فإنه يأخذ
إعدادات وقته من الهيكل الأصلي (FXOS).

الإجراء الموصى به

تأكد من إستخدام مدير الهيكل (FCM) ووحدة التحكم في إدارة الهيكل (FMC) لمصدر الوقت
نفسه (خادم NTP)

6. إيقاف عملية SFtunnel أو تعطيلها

في FTD، تتعامل عملية sftunnel مع عملية التسجيل. هذه هي حالة العملية قبل تكوين
المدير:

<#root>

>

pmtool status

…

sftunnel

(system) -

Waiting

Command:

/ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 06:12:06 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh

حالة التسجيل:

```
<#root>

>

show managers

No managers configured.
```

قم بتكوين المدير:

```
<#root>

>

configure manager add 10.62.148.75 cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

والآن انتهت العملية:

```
<#root>

>

pmtool status
…
sftunnel

 (system) -

Running

 24386
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:12:35 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh(enrolled)
```

في بعض الحالات النادرة، يمكن أن تكون العملية معطلة أو معطلة:

<#root>

>

pmtool status
…
sftunnel

 (system) -

User Disabled

Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:09:46 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh

تبدو حالة المدير عادية:

<#root>

>

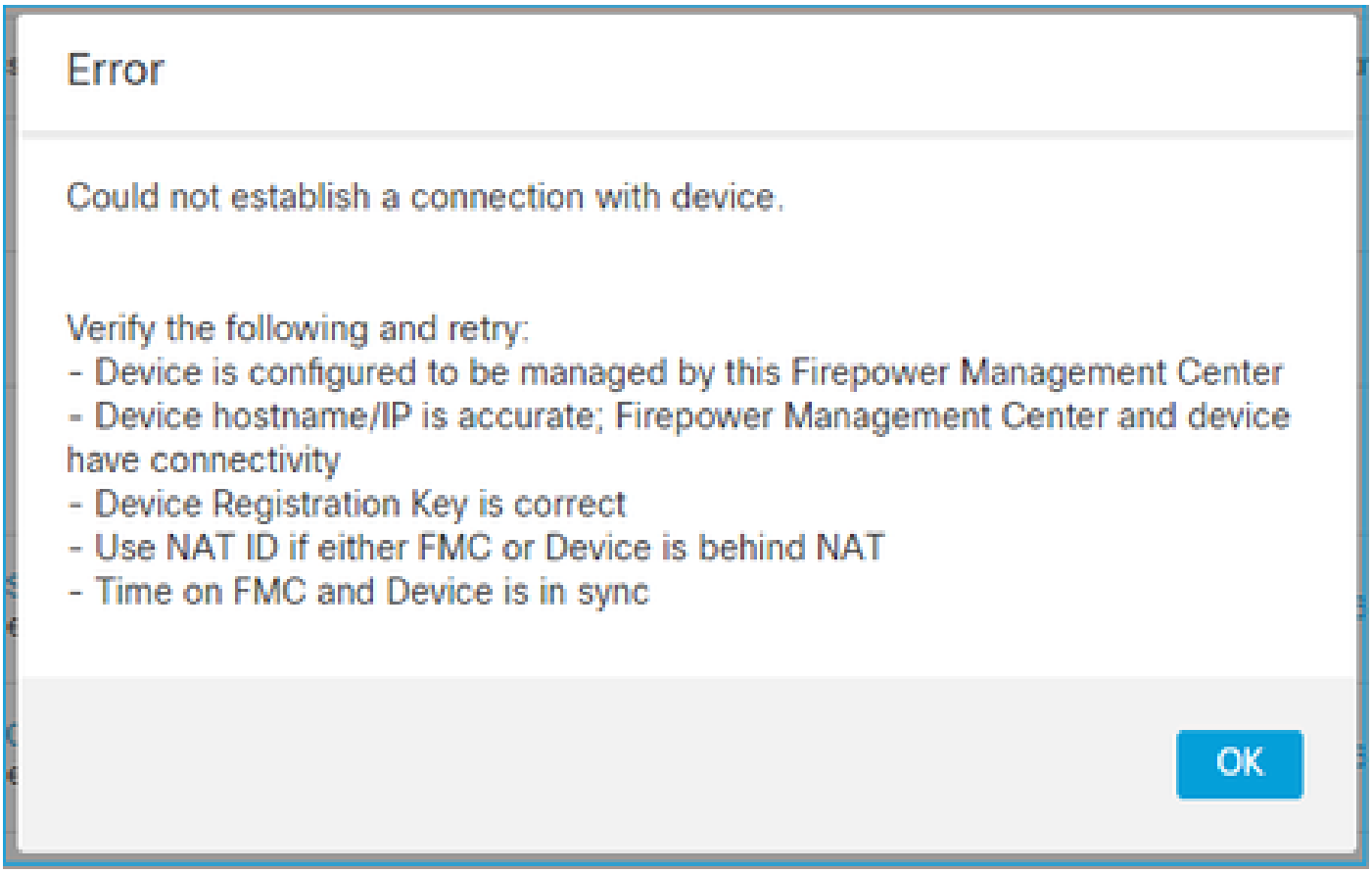
show managers

Host   : 10.62.148.75
Registration Key   : ****

Registration   : pending

RPC Status   :

من ناحية أخرى، يفشل تسجيل الجهاز:



في FTD ال توجد رسائل ذات صلة ظاهرة في /ngfw/var/log/messages

الإجراء الموصى به

جمع ملف أستكشاف أخطاء FTD وإصلاحها والاتصال ب cisco TAC

7. تعليق FTD على FMC الثانوي

هناك سيناريوهات ال يتم فيها إضافة جهاز FTD إلى FMC HA Setup إلى FTD الثانوي بعد التسجيل الأولي ل FTD.

الإجراء الموصى به

أستخدم الإجراء الموضح في هذا المستند:

[استخدام واجهة سطر الأوامر (CLI) لحل مشكلة تسجيل الأجهزة في مركز إدارة FirePOWER على التوفر]

تحذير: هذا الإجراء اقتحامي لأنه يحتوي على إلغاء تسجيل الجهاز. يؤثر ذلك على تكوين جهاز FTD (يتم حذفه). يوصى باستخدام هذا الإجراء فقط أثناء التسجيل الأولي ل FTD والإعداد. في حالة مختلفة، قم بجمع ملفات أستكشاف أخطاء FTD و FMC وإصلاحها والاتصال ب cisco TAC.

8. فشل التسجيل بسبب MTU للمسار

هناك سيناريو يرى في cisco TAC حيث يجب على حركة مرور sftunnel أن تجتاز إرتباط به MTU صغير. تحتوي حزم SFtunnel على مجموعة بت عدم تجزئة وبالتالي ال يتم السماح بالتجزئة:

	Source	Destination	Protocol	Length	TCP Segment	Don't fragment	Info
57	10.62.148.75	10.62.148.42	TCP	74	0	Set	47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MS
58	10.62.148.42	10.62.148.75	TCP	74	0	Set	8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631
59	10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=
60	10.62.148.75	10.62.148.42	TLSv1.2	229	163	Set	Client Hello
61	10.62.148.42	10.62.148.75	TCP	66	0	Set	8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=
62	10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Set	Server Hello
63	10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=
64	10.62.148.42	10.62.148.75	TLSv1.2	803	737	Set	Certificate, Certificate Request, Server Hello Done
65	10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=
66	10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Set	Certificate, Client Key Exchange, Certificate Verify
67	10.62.148.42	10.62.148.75	TCP	66	0	Set	8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=
68	10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	Set	New Session Ticket, Change Cipher Spec, Encrypted Ha
69	10.62.148.75	10.62.148.42	TLSv1.2	364	298	Set	Application Data
70	10.62.148.42	10.62.148.75	TLSv1.2	364	298	Set	Application Data

بالإضافة إلى ذلك، في ملفات /ngfw/var/log/messages، يمكنك مشاهدة رسالة مثل هذه:

MSGS: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunneld:sf_ssl [أطخ] فشل تأكيد اتصال:SSL

الإجراء الموصى به

للتحقق مما إذا كان هناك فقد حزم بسبب التجزئة، التقاط على FTD، FMC، وبشكل مثالي على الأجهزة في المسار. تحقق مما إذا كنت ترى الحزم التي تصل إلى كل النهايتين.

في FTD، اخفض وحدة الحد الأقصى للنقل (MTU) على واجهة إدارة FTD. القيمة الافتراضية هي 1500 بايت. الحد الأقصى هو 1500 لواجهة الإدارة و 9000 لواجهة الاختبار. تمت إضافة الأمر في إصدار FTD 6.6.

مرجع أمر الدفاع عن تهديد الحماية من Cisco Firepower

مثال

```
<#root>

>

configure network mtu 1300

MTU set successfully to 1300 from 1500 for eth0
Refreshing Network Config...
Interface eth0 speed is set to '10000baseT/Full'
```

التحقق

<#root>

>

show network

```
===============[ System Information ]===============
Hostname                  : ksec-sfvm-kali-3.cisco.com
DNS Servers               : 192.168.200.100
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.62.148.1
  Netmask                 : 0.0.0.0


======================[ eth0 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
```

MTU   : 1300

```
MAC Address               : 00:50:56:85:7B:1F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.62.148.42
Netmask                   : 255.255.255.128
Gateway                   : 10.62.148.1
----------------------[ IPv6 ]----------------------
```

للتحقق من مسار MTU من FTD يمكنك إستخدام هذا الأمر:

<#root>

root@firepower:/home/admin#

ping -M do -s 1472 10.62.148.75

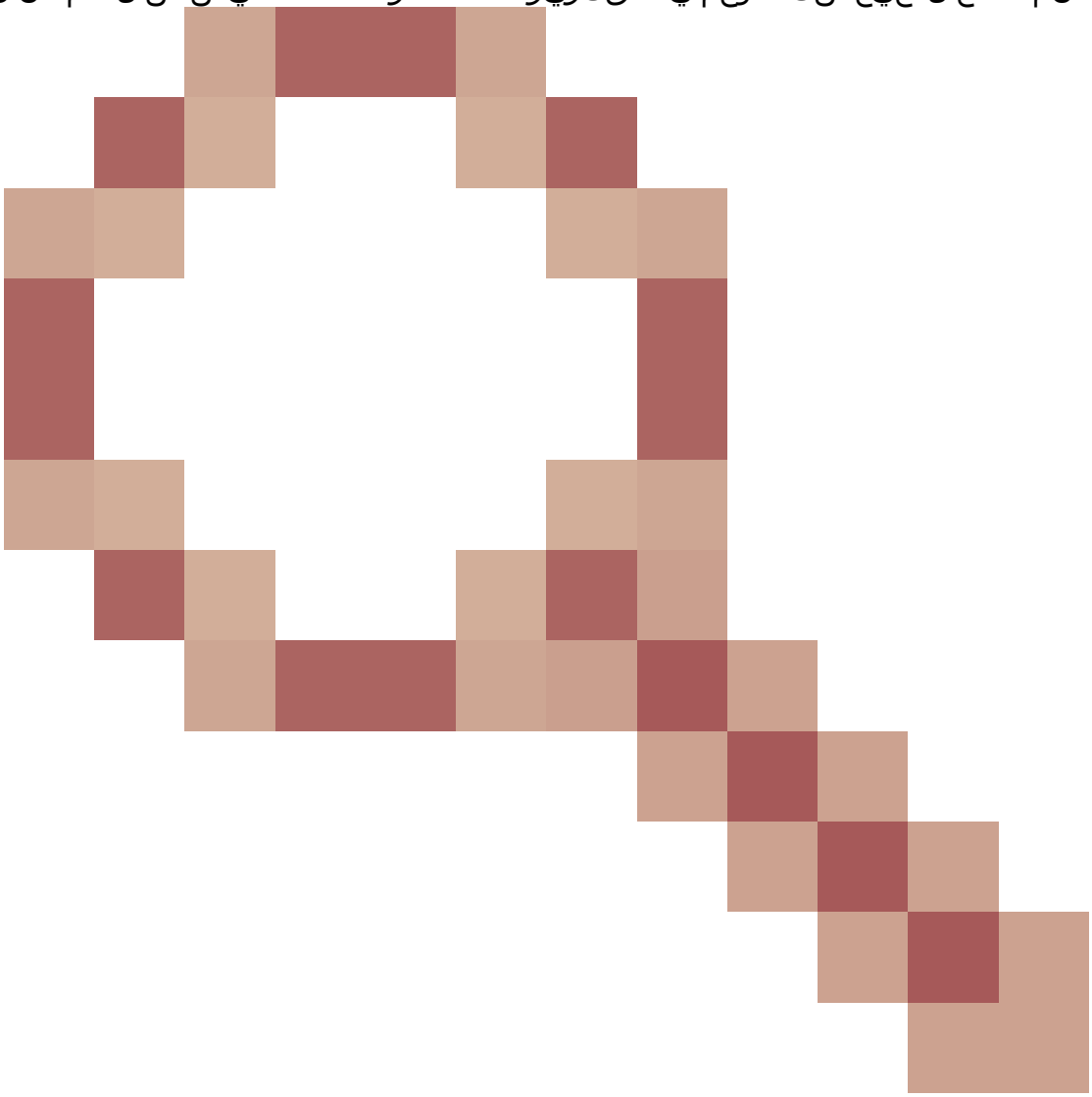
يعمل الخيار do على تعيين عدم تجزئة بت في حزم ICMP. بالإضافة إلى ذلك، عند تحديد 1472، يرسل الجهاز 1500 بايت: (رأس IP = 20 بايت) + (رأس ICMP = 8 بايت) + (بيانات ICMP 1472 بايت)

في FMC، اخفض قيمة وحدة الحد الأقصى للنقل (MTU) على واجهة إدارة FMC كما هو موضح في هذا المستند:

تكوين واجهات إدارة مركز إدارة Firepower

9. يتم إلغاء تسجيل FTD بعد تغيير Bootstrp من واجهة مستخدم "مدير الهيكل"

وهذا ينطبق على الأنظمة الأساسية FP41xx و FP93xx وي وثق في معرف تصحيح الأخطاء من



Cisco CSCvn45138

.

بشكل عام، يجب عليك عدم إجراء تغييرات بروتوكول نظام تمهيد تشغيل الكمبيوتر (FCM) من مدير الهيكل (FCM) ما لم تقم باستعادة البيانات بعد الكوارث.

الإجراء الموصى به

في حالة إجراء تغيير في bootstrap ومطابقتك للشرط (يتم قطع اتصال FTD-FMC أثناء ظهور FTD بعد تغيير BOOTSTRAP) يجب حذف FTD والتسجيل مرة أخرى إلى FMC.

10. يفقد برنامج الإرسال فائق السرعة (FTD) إمكانية الوصول إلى وحدة

التحكم في إدارة الحلول الأساسية (FMC) بسبب رسائل إعادة توجيه ICMP

قد تؤثر هذه المشكلة على عملية التسجيل أو تعطل اتصال FTD-FMC بعد التسجيل.

المشكلة في هذه الحالة هي جهاز شبكة يرسل رسائل إعادة توجيه ICMP إلى واجهة إدارة FTD واتصال FTD-FMC بفتحات سوداء.

كيفية تحديد هذه المشكلة

في هذه الحالة، الـ 10.100.1.1 هو عنوان IP لـ FMC. على FTD، يوجد مسار مخزن مؤقتات بسبب رسالة إعادة توجيه ICMP التي تم تلقيها بواسطة FTD على واجهة الإدارة:

```
<#root>

ftd1:/ngfw/var/common#

ip route get 10.100.1.1

10.100.1.1 via 10.10.1.1 dev br1  src 10.10.1.23

cache
```

الإجراء الموصى به

الخطوة 1

قم بتعطيل إعادة توجيه ICMP على الجهاز الذي يرسلها (على سبيل المثال، محول L3 من الخادم، والموجه، وما إلى ذلك).

الخطوة 2

مسح ذاكرة التخزين المؤقت للمسار الخاص بـ FTD من واجهة سطر الأوامر (CLI) الخاصة بـ FTD:

```
<#root>

ftd1:/ngfw/var/common#

ip route flush 10.100.1.1
```

عندما ال يتم إعادة توجيهها فإنها تبدو كما يلي:

<#root>

```
ftd1:/ngfw/var/common#
```

ip route get 10.100.1.1

```
10.100.1.1 via 10.62.148.1 dev eth0  src 10.10.1.23
    cache  mtu 1500 advmss 1460 hoplimit 64
```

المراجع

- فهم رسائل إعادة توجيه ICMP
- معرف تصحيح الأخطاء من Cisco CSCvm53282 FTD: تصبح جداول التوجيه التي تمت إضافتها بواسطة عمليات إعادة توجيه ICMP عالقة في ذاكرة التخزين المؤقت لجدول التوجيه إلى الأبد

معلومات ذات صلة

- أدلة تكوين NGFW

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).