

FTD ري دم ىل لوصول تانايب هجاو ري غت

تايوت حمل

[قمدق مل](#)

[قيساس ال تابل طت مل](#)

[تابل طت مل](#)

[قمدخت سمل تانوك مل](#)

[قيلوالا قئيه تل](#)

[نئوكتل تاوطخ](#)

[اهجال صاو قرا دل لاصتا عا طخ افاشكت س](#)

[عجل مل](#)

قمدق مل

ديدهت نع عافدل ري دمل لوصول تانايب هجاو ري غت مل زلال تاوطخل دنت سمل اذه فصلي (FTD) نمل آلا قئيه حمل راج.

قيساس ال تابل طت مل

تابل طت مل

- جنت نمل اب قيساس ال قفر عمل
- تانايب ال تاهجاو ربع اه ترا دلو (FTD) قعرسل قئاف لاسر ال جمان رب "قرا دل ع فرعتل

قمدخت سمل تانوك مل

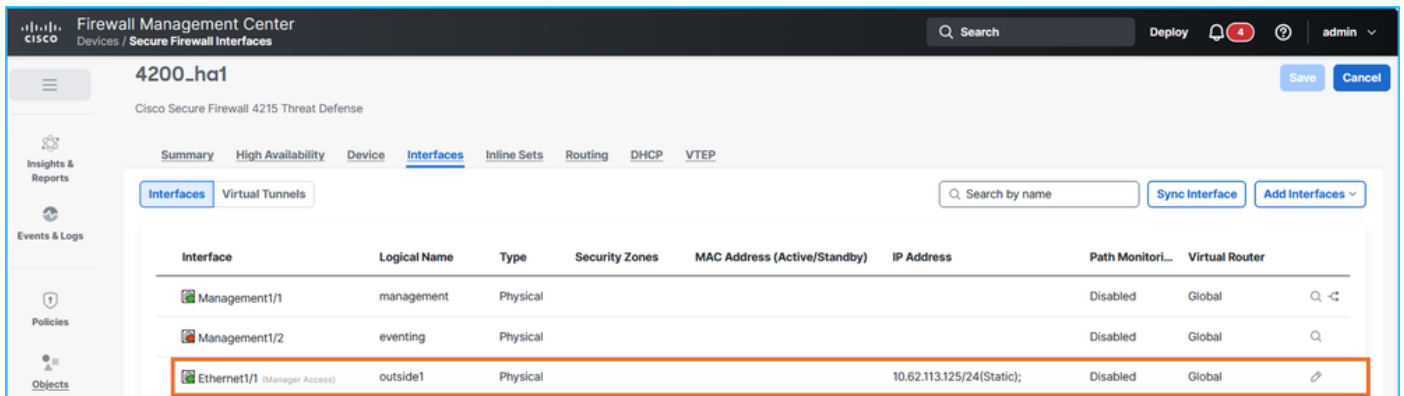
قصاخ قئيه عمل قئيه ب ي قدوجومل قزه ال نمل دنت سمل اذه ي قدراول تامول عمل عاشن مت تانك اذ. (قضارت فا) حوسم نئوكتل دنت سمل اذه ي قمدخت سمل قزه ال عي مج تادب رمل آل لمحت حمل ري ثاتلل كمهف نمل دكأتف، لي غشتل دي قكتك بش

قئيلال قئيه دامل تانوك مل او جمار بل تارادصل ل دنت سمل اذه ي قدراول تامول عمل دنت ست

- Secure Firewall 4200
- 7.6.4 رادصإلإ 10.0.x (FTD) نمآلآ ةيماحل رادج ديدت دض عافدل اجم انرب
- 10.0.x (FMC) نمآلآ ةيماحل رادج ةرادا زكرم

ةيلوألآ ةئي هتلا

- 1، جراخ م سالا عم Ethernet1/1 تانا يبالآ ةهجاو رب ع (HA) لاء رفوت ةلاحي في FMC FTD ريدي 1،
يلاوتلا ىلع 10.62.113.125 و 10.62.113.125 ةيطايتحال او ةطشننلا IP يناونع مادختساب



FTD CLISH: ةحص نم ققحتلا

<#root>

>

show network management-data-interface

Physical Interface Name of the Interface

Ethernet1/1 outside1

>

show network

```
===== [ System Information ] =====
Hostname                               : CSF4215-3
..
DNS from router                        : enabled
Management port                       : 8305
```

```

Gateway                                     IPv4 Default route
                                           : data-interfaces
...
===== [ System Information - Data Interfaces ] =====
DNS Servers                               : 192.0.2.100

Interfaces                                : Ethernet1/1

===== [

Ethernet1/1

] =====

State                                     : Enabled
Link                                       : Up

Name                                       : outside1

MTU                                         : 1500
MAC Address                               : 40:F4:9F:3D:5A:0E

----- [ IPv4 ] -----

Configuration                             : Manual

Address                                   : 10.62.113.125

Netmask                                   : 255.255.255.0

Gateway                                   : 10.62.113.1

...

```

FMC: دحوو FTD HA دحوو ني ب ق فنل تالاصت اءاشن ا متي 2.

<#root>

>

sftunnel-status-brief

PEER:fmc.example.org

SFTunnel Status:-

Channel A: Connected

Channel B: Connected

Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' via
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '198.51.100.23' via
Registration: Completed.
IPv4 Connection to peer 'fmc.example.org' Start Time: Fri Jul 17 08:22:31 2026 UTC
Heartbeat Send Time: Fri Jul 17 08:52:42 2026 UTC
Heartbeat Received Time: Fri Jul 17 08:53:03 2026 UTC
Last disconnect time : Fri Jul 17 08:22:16 2026 UTC
Last disconnect reason : Process shutdown due to stop request from PM

3. لاصت الال (DNS) تالاجم الءامسأ ماطن لءى لء (FTD) ةعرسلال قئاف لالسلال ءمانرب ءمء عى.
مسا لىل اءانءسا نىوكءالاب رىءم ال موقى (FMC) ةىلارءىفال ءوللل ةراءل لى ف مكءءال ءءوب
(FQDN): لملكالب لهؤم ال لاءم ال

<#root>

>

show managers

Type	: Manager
Host	: fmc.example.org
Display name	: fmc.example.org
Version	: 10.0.1 (Build 1)
Identifier	: 6d86efc4-c095-11f0-9244-48f1a7894b18

```
Registration : Completed
Management type : Configuration and analytics
```

>

show network

```
===== [ System Information ] =====
Hostname : KSEC-FPR-4215-3
```

```
Domains : example.org
```

```
DNS Servers : 192.0.2.100
```

```
DNS from router : enabled
Management port : 8305
IPv4 Default route
Gateway : data-interfaces
...
```

1. ڌيڄ راڻال ءهه اوال ربع DNS مءاوخ ىل لوصولا نكمي

4. Lina كرحم ربع SFtunnel تالاصت اءاشن مءي

<#root>

>

show conn all port 8305

```
26 in use, 32 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

```
TCP nlp_int_tap 10.62.113.125(169.254.1.3):8305 outside1 198.51.100.23:45647, idle 0:00:03, bytes 2129
```

```
TCP nlp_int_tap 10.62.113.125(169.254.1.3):37141 outside1 198.51.100.23:8305, idle 0:00:04, bytes 1485
```

نيوكتلا تاو طخ

IP اناونع نوکي 2. ههجاو لا جراخ فدهلا ىللا ىللا 1 جراخ لا نم ري دمل لوصو لقن وه فدهلا ىللا ىللا 10.62.114.52/24 و 10.62.114.51/24 وه IP 2 جراخ دادعت سالاو طشنلا

معدت ثدحالا تارادصالا واً (FTD) ةعرسلال قئاف لاسرالا جم انرب" نم 7.7.0 تارادصالا نا طحال ري دمل لوصو ههجاو نم رثكاً نيوكت حيتت ىتلاو، ري دمل ىللا ةرركت ممل لوصولا تانايب تاهجاو 7.7.0 نم مدقالا تارادصالا يف ةم وعدم ريغ ةزيملا هذه. اهرشنو

ةفل تخم تاءارجا ىللا ىوتحت واً ةني عم تاو طخ ىطخت متي، ةقي قحلا هذهل ارظنو



ةو طخ ىا يف FMC نم FTD تافلم فذح/لجست ءاغل اب مقت ال :ري دخت

1.FTDs ىللا مكحتلا ةدحو ىللا لوصو كيدل نوکي نا نسحت سمل نم

- م ث نمو، SSH مادختساب لك يهلا اب لاصتالا كنكمي، Firepower 4100/9300 ةلاح يف لاصتالا ةدحو رمأ مادختساب ةي لصلالا (FTD) لاسرالا يف مكحتلا ةدحو اب لاصتالا slot/نامالا ةدحو فرع م x لثم ي شيح، مكحتلا ةدحو ل x ةي طمنلا
- كنكمي، تال ي ثمل ددعت م (MI) عضو يف FTD 4100/9300 Firepower ل ي غشت ةلاح يف FTD يف ةي لصلالا مكحتلا ةدحو اب لاصتالا م ث، SSH مادختساب لك يهلا اب لاصتالا مق م ث. ذفنم ل/نامالا ةدحو فرع م x لثم ي شيح، connect module x telnet رمأالا مادختساب <ftd_id> connect ftd رمأالا مادختساب FTD ل ي ثم اب لاصتالا اب
- لك يهلا اب لاصتالا كنكمي، MI عضو يف 3100/4200 نم آالا ةي امحلا رادج ةلاح يف connect ftd رمأالا مادختساب FTD يف مكحتلا ةدحو اب لاصتالا م ث SSH مادختساب <identifier> .

2.ةق ل عمل جهنلا رشن

3.FTD ةلاح يف FMC و FTD نم لك ىللا ىطاي تحالا خسنلا تاي لمع ءارجا ب ةدشب ىصوي ني دحو لا لك ل ي طاي تحالا خسنلا ءارجا ب مق HA،

4.ةط ب ترم ىرخأ تادادع و نامالا ةقطنمو IP اناونعو فدهلا ههجاو لا مسا نيوكت ب مق

انكم كلذ ناك اذ،ةهاولاب

5.فدهال ةهاولل يطايتحال IP ناوع نيوكتب مق

6.ةهاولا يلع ريذمال لوصو نيكمتب مقف ،ثدحأ رادصا و FTD 7.7.0 چمانرب رادصا ناك اذ
ةحال بسح ةرادال لوصولا تاكباش طبضو فدهال

The screenshot shows the Cisco Firepower Management Center (FMC) interface for device configuration. The main window displays the 'Interfaces' tab for device '4200_ha1'. A table lists various interfaces, with 'Ethernet1/2' highlighted in orange. A modal window titled 'Edit Physical Interface' is open, showing the 'Manager Access' tab. The 'Enable management access' checkbox is checked. The 'Available Networks' list contains several IP addresses, and the 'Allowed Management Networks' field is set to 'any'. The 'Add' button is visible next to the network list.

تانايب تاهچاو معدت ال 7.7.0 نم مدقأال (FTD) ةعرسال قئاف لاسرال چمانرب تارادصا نأ طحال
أطخال ةلاسر ةيناثال ريذمال لوصو ةهچاو نيوكتب ةلواح نم چتنې .ريذمال ةرركتمال لوصولا
هذه:

Error - Device Configuration

⚠ High availability device cannot have more than 1 interface enabled for FMC access

OK

7.7.0. رادصلإل لب ق FTD تارادصلإل 8 و 7 تاوطخلإل يطخت نم دكأت

لثالم اذه يف FTD CLISH. لعل ةدوجوملإل تادادعلإل نم ققحتلإل واسايسلإل رشن ب مق 7. لعل 10.62.114.52 و 10.62.114.51 IP يناونع لعل 2 جراخ مصلإل تاذ Ethernet1/2 ةهجالو يوتحت يلال:

<#root>

>

show ip

		System IP Addresses:			
Interface	Name	IP address	Subnet mask	Method	
Ethernet1/1	outside1	10.62.113.125	255.255.255.0	manual	<- source interface
Ethernet1/2	outside2	10.62.114.51	255.255.255.0	manual	
Ethernet1/4	fover	10.9.0.21	255.255.255.0	unset	<- target interface

sftunnel: نيوكت لىل 2جراخ ةهجالو افاضلإل متت

<#root>

>

show running-config sftunnel

sftunnel interface outside2

<- target interface

sftunnel interface outside1

<- source interface

sftunnel port 8305

sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346

عم دعاوقل نأ الل (NAT)، ةكبشل ناونع ةمجرت لودج يف ةيفاضلإل دعاوق تيبتت نم مغلل لعل مادختصلإل ديق 1 ةجراخل ةهجالو

<#root>

>

show nat detail

Manual NAT Policies Implicit (Section 0)

1 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_0.0.0.0_intf5 interface destination s
translate_hits = 1448, untranslate_hits = 1448
Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
Service - Protocol: tcp Real: 8305 Mapped: 8305

2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface destination st

translate_hits = 0, untranslate_hits = 0
Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
Service - Protocol: tcp Real: 8305 Mapped: 8305

3 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel::_intf5 interface ipv6 destination s
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:
Destination - Origin: ::/0, Translated: ::/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
4

(nlp_int_tap) to (outside2) source static nlp_server__sftunnel::_intf6 interface ipv6 destination stat

translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:
Destination - Origin: ::/0, Translated: ::/0
Service - Protocol: tcp Real: 8305 Mapped: 8305

5 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_intf5 interface
translate_hits = 653, untranslate_hits = 0
Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
6

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface

translate_hits = 0, untranslate_hits = 0
Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
7 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_ipv6_intf5 interface ipv6
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:
8

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6

translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:

ههجاو الو بقرمو و يلاعال رفوتلا ةلح نم ققحتلا 8.

<#root>

>

show monitor-interface

This host: Primary - Active

Interface management (203.0.113.130): Normal (Monitored)
Interface outside1 (10.62.113.125): Normal (Monitored)
Interface outside2 (10.62.114.51): Normal (Monitored)

Other host: Secondary - Standby Ready

Interface management (203.0.113.131): Normal (Monitored)
Interface outside1 (10.62.113.126): Normal (Monitored)
Interface outside2 (10.62.114.52): Normal (Monitored)

مسق ىل لوصولاب حامسلال نم دكأتف ،2ةيجراخلا ههجاو الو ربع FTDs ةرادال ططخت تنك اذإ 9.
يساسأل ماظنل تادادعإ نم SSH لوصولو

عامسأ مداوخب فدهل ههجاو الو ربع لاصلتالاب حامسلال ةمزالل تاريغتلا ءارجإب مق 10.
FMC و (DNS) تالاجمل

- FTDs نأ نم دكأتف ، FTDs و FMC نيپ لاصلتال ةبولطم (DNS) لاجمل مسا ةقد ناك اذإ ىل لوصول ةمدختسمل ةيلائل ةوطخل ىل فدهل ههجاو الو ربع لوصول ةيناكمإ اهل لقنل راسم في DNS لحب حامسلال بجي امك . DNS مداوخ
- نوكي نأ لجنج يلائل ىل نراق فدهل ربع reachability ىلقلتي FTDs نأ تنمض FMC غلب في نأ تلمعتسا
- في TCP 8305 ذفنم ربع FTDs و FMC نيپ هاجتإل يئانث لاصلتالاب حامسلال نم دكأت نيهاجتالالك في لاصلتالاب حامسلال بجي . فدهل ههجاو الو ربع لقنل راسم

نكمي . فدهل ههجاو الو ربع ةيضارتفا ةباوبك 10.62.114.1 IP مادختسا مزلي ،ةلحال هذه في
تنرتنإل في مكحتل لئاسر لوكتورب مادختساب ةيلائل ةوطخلل IP ناونع ىل لوصول
(ICMP):

<#root>

>

ping 10.62.114.1

Please use 'CTRL+C' to cancel/abort...

Sending 5, 100-byte ICMP Echos to 10.62.114.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

في مكححتل ناو نع نأ نم دكأت ف ،ةيالاتل ةوطخل وأ لقنل راسم في اي راد ICMP رطح مت اذا
حل اصلو show arp رمأل جارخا في فيئرم ةيالاتل ةوطخل اب صاخلا (MAC) طئاسولا إلى لوصول

<#root>

>

show arp

fover 10.9.0.22 4c01.f7e9.e111 13275
outside1 10.62.113.1 c02c.1782.2cbf 1
outside1 10.62.113.126 4c01.f7e9.e10e 5453

outside2 10.62.114.1 c02c.1782.2cbf 0

outside2 10.62.114.52 4c01.f7e9.e10f 5453

FTD رادصل اق فو تاوطخل هذه عارج اب مق 11:

- ردصل مال ةهجاو ربع ري دم لوصول لي طعتب مق FMC، ثدح رادصل وأ 7.7.0 رادصل إلى DNS مادختسا مت اذا DNS مداوخ إلى هي جوتل كلذ في امب ،هي جوتل طبضب مق و (1جارخ) ني وكتب مق ،لا ثمل لېبس لىل (2جارخ) فدهل ةهجاو ربع فMC و (FMC إلى لوصولل فدهل ةهجاو ربع ةيضا رتفال ةباو بل ني وكت وأ ةني عم ةتباث تاراسم
- ردصل مال ةهجاو ربع ري دم لىل لوصولل لي طعتب مق FMC، في 7.7.0 نم مدقأل رادصل إلى في امب ،هي جوتل طبضو ، (2جارخ) فدهل ةهجاو ربع ري دم لىل لوصولل ني كمتو ، (1جارخ)

ههجاوول ربه فمف و فمف الى لوصولل DNS مادلللسا م اذل DNS مداول الى هلچولل كلذل
نلوكل وائلنعم قلبالل لاراسم نلوكل ب مقل، لاللم للللس للل. (2لراخ) فدهل
فدهل ههجاوول ربه قللضارللالالابولل

12. لاساللل رشن

13. فم فمف فمف:

<#root>

>

show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

* 10.62.114.1, via outside2

<- default route over outside2
Route metric is 0, traffic share count is 1

>

show running-config sftunnel

sftunnel interface outside2

<- sftunnel is enabled only over outside2
sftunnel port 8305

>

show nat detail

Manual NAT Policies Implicit (Section 0)

1 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface destination st

translate_hits = 3, untranslate_hits = 3

```

Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel::_intf6 interface ipv6 destination s
    translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:
Destination - Origin: ::/0, Translated: ::/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
    translate_hits = 407, untranslate_hits = 0
Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
4 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6
    translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:

```

>

show conn all port 8305

```

31 in use, 42 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

```

```
TCP nlp_int_tap 10.62.114.51(169.254.1.3):56853 outside2 198.51.100.23:8305, idle 0:00:06, bytes 33008
```

<- connectivity over outside2

```
TCP nlp_int_tap 10.62.114.51(169.254.1.3):32905 outside2 198.51.100.23:8305, idle 0:00:00, bytes 15959
```

<- connectivity over outside2

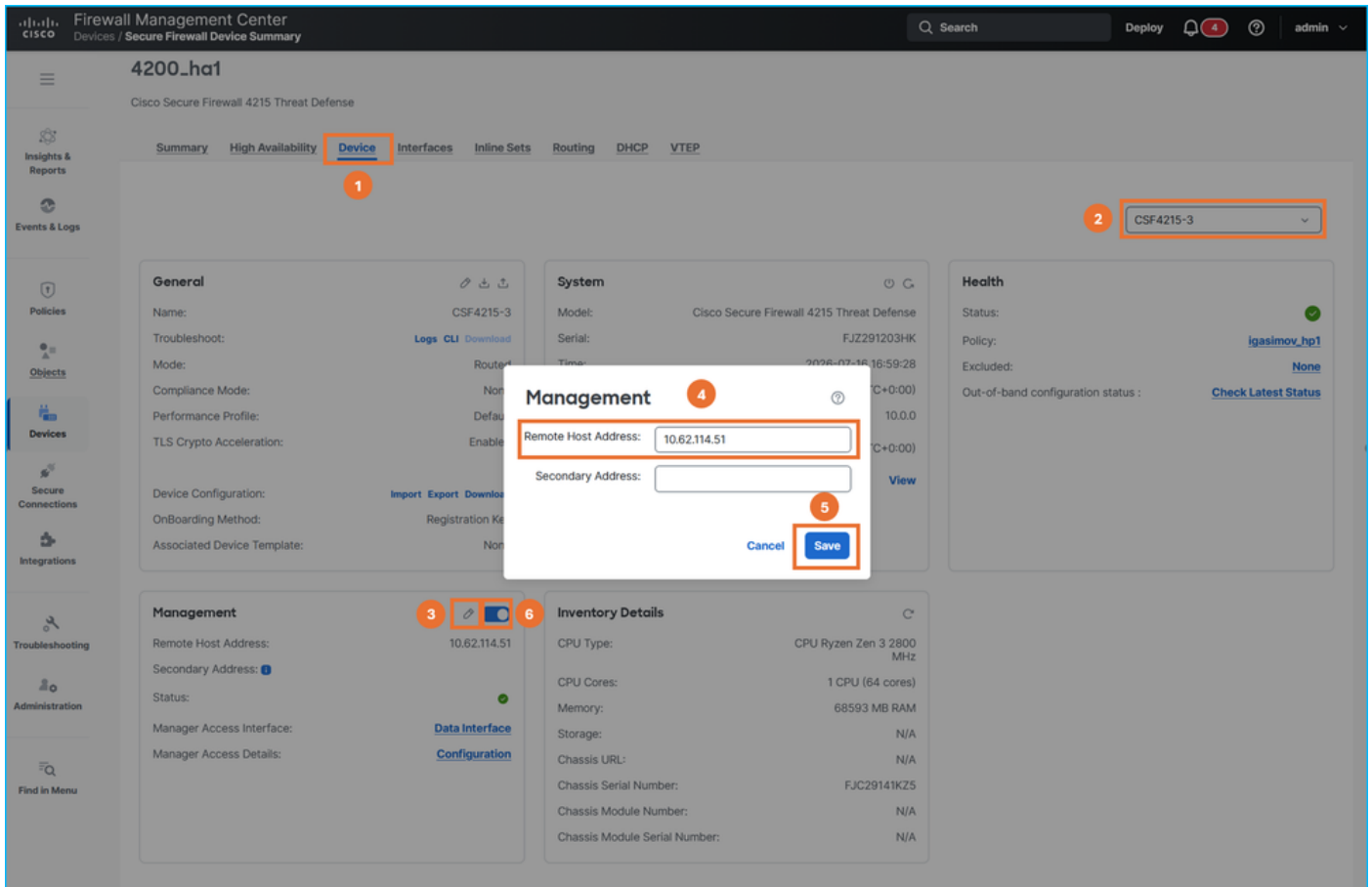
مقف، ريغتل الى ةجأب CLISH "show network" رمأل جأرأ يف DNS مءاوخ تنأك اءا 14.
ةءءءال DNS مءاوخ نءوكءب

<#root>

>

configure network dns servers 192.0.2.184

لءءعءب مق مء 2، ءءأرأل IP ناوع الى FTD ةرءءب صأرأل IP ناوع رءءءب مق، FMC يف 15.
HA يف نءءءءال الكل ةوءأل هءه ررك. قلزنمءل مءءءسأب هءءمء ةءاعءو لءصءال



16. FTDs عي مج ىل ع SFTDs لاصتا نم ققحت لا .

<#root>

>

sftunnel-status-brief

PEER:198.51.100.23
SFTunnel Status:-

Channel A: Connected

Channel B: Connected

Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
Registration: Completed.

IPv4 Connection to peer '198.51.100.23' Start Time: Thu Jul 16 16:37:14 2026 UTC
Heartbeat Send Time: Thu Jul 16 16:38:13 2026 UTC
Heartbeat Received Time: Thu Jul 16 16:39:13 2026 UTC
Last disconnect time : Thu Jul 16 16:37:11 2026 UTC
Last disconnect reason : Both control and event channel connections with peer went down

>

show conn all port 8305

32 in use, 42 most used

Inspect Snort:

preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:36383, idle 0:00:00, bytes 23575

<- new connection over different source port

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:50963, idle 0:00:01, bytes 12319

<- new connection over different source port

ءارجا كئيل عف ،ةيساسألا ةمظنألا تادادعإ ي ف DNS مداوخ ربيغت ىلإ ةجاح كانه تناك اذا - 17
تاسايسلا رشنو نيوكتلا ي ف ةبسانم تاريغت

اهحالصإو ةرادإلا لاصتا ءاطخأ فاشكتسأ

ققحتلل رماوأل هذه مدختسأ

1. ةرادإلا ةهجاو نيوكت ضرعي - show network
2. sftunnel لاصتا ةلاح ضرعي - sftunnel-status-brief
3. (Lina) ةيhamحلا راج كرحم ي ف sftunnel نيوكت ضرعي - show run sftunnel
4. Lina كرحم ربع قفن تالاصتا ضرعي - show conn all port 8305

[ةرادإلا لاصتا ءاطخأ فاشكتسأ](#) مسق ىلإ عجرا ،اهحالصإو ةرادإلا تالاصتا ءاطخأ فاشكتسال
ي.مسرلا ليلدلا ي ف [اهحالصإو](#)

عجارملا

1. [10.x Cisco، نم نم آلا ةيامحل رادج قرادازك نرم زاهج نيوكت ليلد](#)
2. [ريدملل لوصول ةهجاورييغت](#)
3. [اهجالص او قرادل لاصتا عاطا فاشكتسا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا