

ىلإ ةرادإل نم FTD ىلع ريذملا لوصو نيوكت تانايبل ةهجاو

تايوتحملا

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ةهجاو لىحرت ةعباتم](#)

[يساسأل ماظنلا تادادعلا ىلع SSH نيكمت](#)

[ةحصلا نم ققحتلا](#)

[FMC ب ةصاخلا \(GUI\) ةيموسرلا مدختسملا ةهجاو نم ققحتلا](#)

[FTD ل \(CLI\) رماوأل رطس ةهجاو لىلخ نم ققحتلا](#)

[اهجالص او عاخالأل فاشكسلا](#)

[ةرادال لىصتا ةلاخ](#)

[لمعلا ويرانىس](#)

[لمعلا مدع ويرانىس](#)

[ةكبشلا تامولعم ةحص نم ققحتلا](#)

[ةرادال ةلاخ ةحص نم ققحتلا](#)

[ةكبشلا لىصتا نم ققحتلا](#)

[ةرادال زكرم لىصتا لىلخ](#)

[مزجالا ددعو تايءاصحال او ةهجاو ةلاخ نم ققحتلا](#)

[FMC لىل لوصولل FTD ىلع راسملا ةحص نم ققحتلا](#)

[لىصتال او SFTUNNEL تايءاصحال نم ققحتلا](#)

[ةلص تاذ تامولعم](#)

ةمدقملا

FirePOWER (FTD) ديدهت نع عافدلا" ىلع ريذملا لوصو ليذعت ةي لمع دنتسملا اذه فصى
تانايبل ةهجاو ىلإ ةرادإ نم.

ةيساسأل تابلطتملا

تابلطتملا

ةي لىل عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت:

- Firepower Threat Defense
- Firepower ةرادإ زكرم

ةمدختسملا تانوكملا

- Firepower Management Center Virtual 7.4.1
- Firepower Threat Defense Virtual 7.2.5

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل اشنإ م ت ت ناك اذا .(يضا رتفا) حوسمم نيوك ت ب دنتسمل اذه ي ف ةمدختسمل ةزهجال عي مج ت ادب رما يال لمحتمل ري ثاتلل كم هف نم دكات ف ، ليغشتلا دي ق كتك ب ش

ةيساسا تامولعمل

لكش ب كنكمي . FMC م كحتلا ةدحوب لاصتال ةدحاو ةصصخم ةرادا ةهجاو يلع زا هج لك يوتحي نوكيو ، ةصصخملا ةرادال ةهجاو نم ال دب ةرادال تانايب ةهجاو مادختسال زا هجال نيوك ت يراي تخا ن ع "Firepower" ديهت ن ع اف دلا" ةرادا ديرت ت نك اذا ادي فم تانايبلا ةهجاو يلع FMC لوصو ريغيغتل اذه اارجا ب جي . ةلصفنم ةرادا ةكبش كي دل نكي مل اذا وا ، ةيجراخل ةهجاو نم دب FMC ةطساوب هترادا متت يذلا FTD ل FirePOWER (FMC) ةرادا زكرم يلع

دويقل نم ةلقل تانايبلا ةهجاو نم FMC لوصو عرضخي

- ال عيطتسي تنأ . ةدحاو ةي دام تانايب ةهجاو يلع ري دمل لوصو ني كمت طقف كنكمي EtherChannel و ا يعرف نراق لمعتسي .
- ةهجوم ةهجاو مادختساب ، طقف هجوملا ةيامحل رادج عرضو .
- PPPoE لوكوتورب بلطتي كي دل (ISP) تنرتنالا ةمدخ دوزم ناك اذا . موعدم ريغ PPPoE ، FirePOWER Threat Defense ني ب PPPoE لوكوتورب معدب دوزم هجوم عرضو كي لعل ب جي ف WAN م دومو .
- طقف ةلصفنملا ثادجال او ةرادال تاهجاو مادختسا كنكمي ال .

نيوكتلا

ةهجاو لا ليحرت ةعباتم

لبق FMC و FTD نم لكل يطايحتا خسن ةي لمع رخآ ءارجإب ةدشب ى صوي: ةظحالم
تاريغت ةيأ ةعباتم.

1. تاريغت ال ءارجإب موقت يذلا زاهجل ريرحت ىلع رقنا ، ءزهجالا ةرادإ > ءزهجالا ىلإ لقتنا .
هيلع .

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	Group	
<input type="checkbox"/>	▼ FMT Test (1)								
<input type="checkbox"/>	FTD-Test Short 3 192.168.1.8 - Routed	FTDv for VMware	7.2.5	N/A	Essentials	Base-ACP	↺		Edit →

2. ريدم لل لوصول ءهجاوب صاخلا طابترالا قوف رقنا مٲ ، ءرادإلا > زاهجالا ىلإ لقتنا .

Management	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	✔
Manager Access Interface:	→ Management Interface

عون ديدحتل طابترالال قوف رقنا .ةدوجوملا ةرادإلا ةهجاو ري دملل لوصوللا ةهجاو لقح ضرعي قوف رقنا مٲ زاهجلا ةرادإ ةلدسنملا ةمئاقلا يف تانايبلا ةهجاو رايلال وهو ،ديدل ةهجاو لظفح .

Manager Access Interface ?

i This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by

Management Interface

Management Interface

Data Interface

Close
Save

3. لىل حفصتلاو ،تانايبلا ةهجاو لىل ةرادإلا لىل لوصوللا ني كمتل ةعباتملا نألا كيلىل ع بچي .
ري دمل لوصول ةي دامل ةهجاو ل ريحت > تاهجاو ل > ةزهجال ةرادإ > ةزهجال

Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

Enable management access

Available Networks



Search

10.201.204.129

192.168.1.0_24

any-ipv4

any-ipv6

CSM

Data_Store

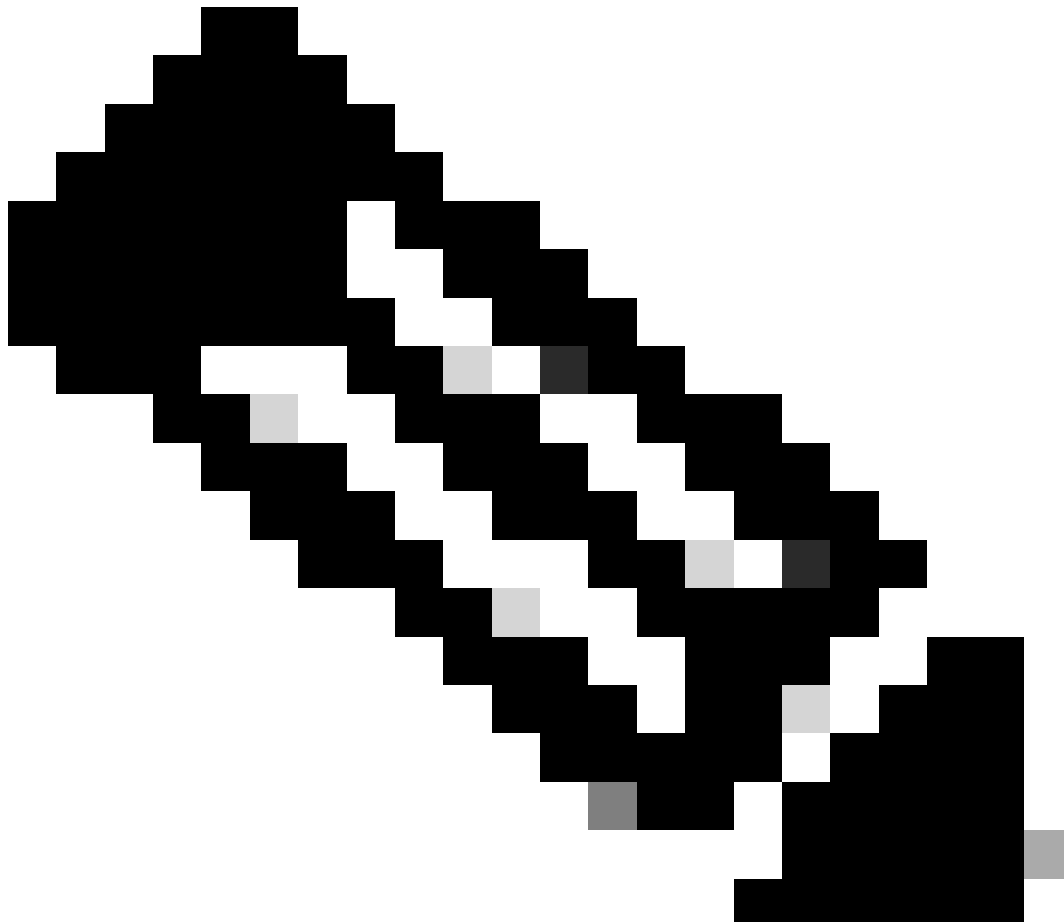
Add

Allowed Management Networks

any

Cancel

OK



لوصول نيكم تب مقف، رارك تلل ةيوناث ةهجاو مدختست تنك اذا (يراي تخا): ةظحال م رارك تلل ضرغل ةمدختست م ل ةهجاو لىل ع ةرادال لىل

ببول عونل DDNS ةقيرط نيكم تب مق، ةهجاو ل DHCP مدختست تنك اذا (يراي تخا) راوخل ع برم DHCP > DDNS > ةزهجال ةرادا > ةزهجال لىل

اذه لىل ع هقبطو، ساسال ماطنل تاداعا ساسا س ي ف DNS نيوك تب مق (يراي تخا) DNS > ساسال ماطنل تاداعا > ةزهجال لىل ف زاوجل

4. فضا؛ تانايبل ةهجاو لال خ نم ةرادال زكرم لىل هجوي نا نكم ي ديدهتل نع عافدل نا نم دكأت. تباثل راسم لاهيجوتل > ةزهجال ةرادا > ةزهجال لىل ع رمال مزل اذا تباثل راسم

1. هتفاضاب موقت يذلا تباثل راسم لىل ادانسا IPv6 و IPv4 قوف رونا.

2. قبطي كي تاتاسا نكاس رمم اذه ي لىل نراقل ترتخا.

3. ةهجال ةكبشلا رتخا، ةحاتملا ةكبشلا ةمئاق ي ف.

4. اذهل ةيلال ةوطخل وه يذلا و هراتخا و ةرابعل هجوم لخدأ، IPv6 ةرابع و ةباوبل ل قح ي ف راسم ل.

ةمدخل لىل ةيقافتا ةبقارم نئاك مسا رتخا و لخدأ، راسم ل رفوت ةبقارم ل (يراي تخا) راسم ل بقعت ل قح ي ف، ةبقارم ل ساسا س ددحي يذلا (SLA)

Add Static Route Configuration



Type: IPv4 IPv6

Interface*



(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Add

Selected Network



10.201.204.129

192.168.1.0_24

any-ipv4

CSM

Data_Store

FDM

Gateway*

+



Metric:

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

+

Cancel

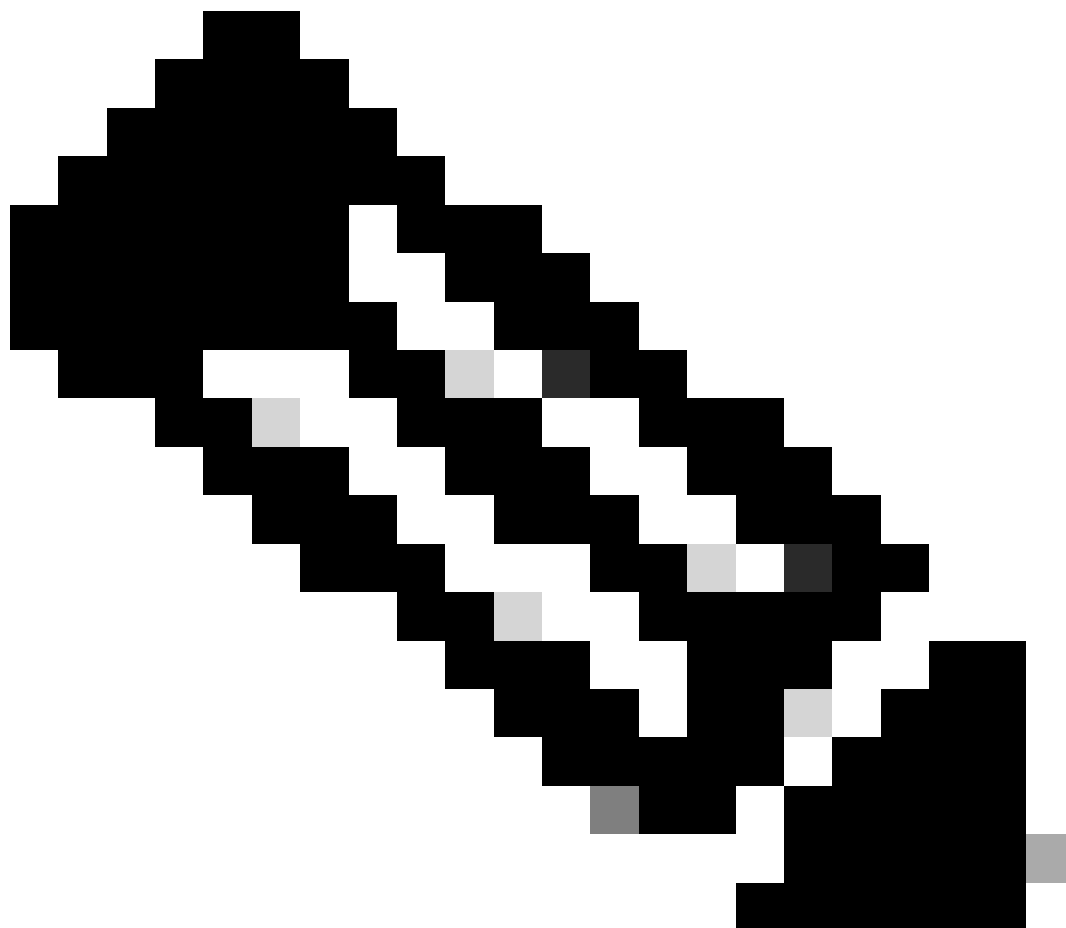
OK

5. ٲىللحلال ةرادلل ةهءاو ربع نىوكتلل ءارىىغء رشن نأل مءى. نىوكتلل ءارىىغء رشن

6. ناونع مادءءءسال ةرادلل ةهءاونىىىعءءب مق، FTD ب ءصااءل (CLI) رماوالل رطس ةهءاو ىف. ءاناىب ءاهءاونوكءل ءباوبلل او ءبء

- `configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces`

```
>
>
> configure network ipv4 manual IP_ADDRESS192.168.1.8 NETMASK255.255.255.0 GATEWAYdata-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```




لېبس ىلع .تبات IP ناووع نېيىعت كېلىع بچې هئأ ال، ةرادال ةهجاو مادختس ال ططخت ال كنأ نم مغرلا ىلع :عظالم
ةكره هيجوت ةداعال ةرادال هذو مادختسإ متي .تانايبلا تاهجاو ىلإ ةباوبال نېيىعت كنكمي ىتح صاخ ناووع ،لاتملا
TAP_NLP. ةهجاو مادختساب تانايبلا ةهجاو ىلإ ةرادال رورم


لإصتال نيكمتب مقو، قرادال مسق > زاهجلا > زاهجلا قرادا > زهجالا يف ديهتلا نع عافدلل يوناتلا

Management

Remote Host Address: 192.168.1.8

Secondary Address:

Status: 

Manager Access Interface:  [Data Interface](#)

Manager Access Details: [Configuration](#)

يساسألا ماظنلا تاداعل SSH نيكمت

ماظنلا تاداعل > زهجالا دنع زاهجلا اذه لعل هتقبطو، يساسألا ماظنلا تاداعل ةسايس يف تانايبللا ههجالا SSH نيكمتب مق . قفاضل رقن SSH لوصلو > يساسألا

- SSH تالاصتلا عارجاب اهل حمست يتلا تاكبشلا وأ ةفيملا تائيبلا
- يف تسيل يتلا تاهجالا ةبسنلاب . اه SSH تالاصتال حمست يتلا تاهجالا لعل يوتحت يتلا قطانملا فضا . قفاضل قوف رقن اولقحلا يف ةدحمل تاهجالا قيطانملا ةمئاق يف ههجالا مساباتك كنكمي ، ام ةقطنم تاريغتلارشن . OK قوف رقن او

Add Secure Shell Configuration



IP Address* +



Available Zones/Interfaces C

- DMZ
- Inside
- outside

Add

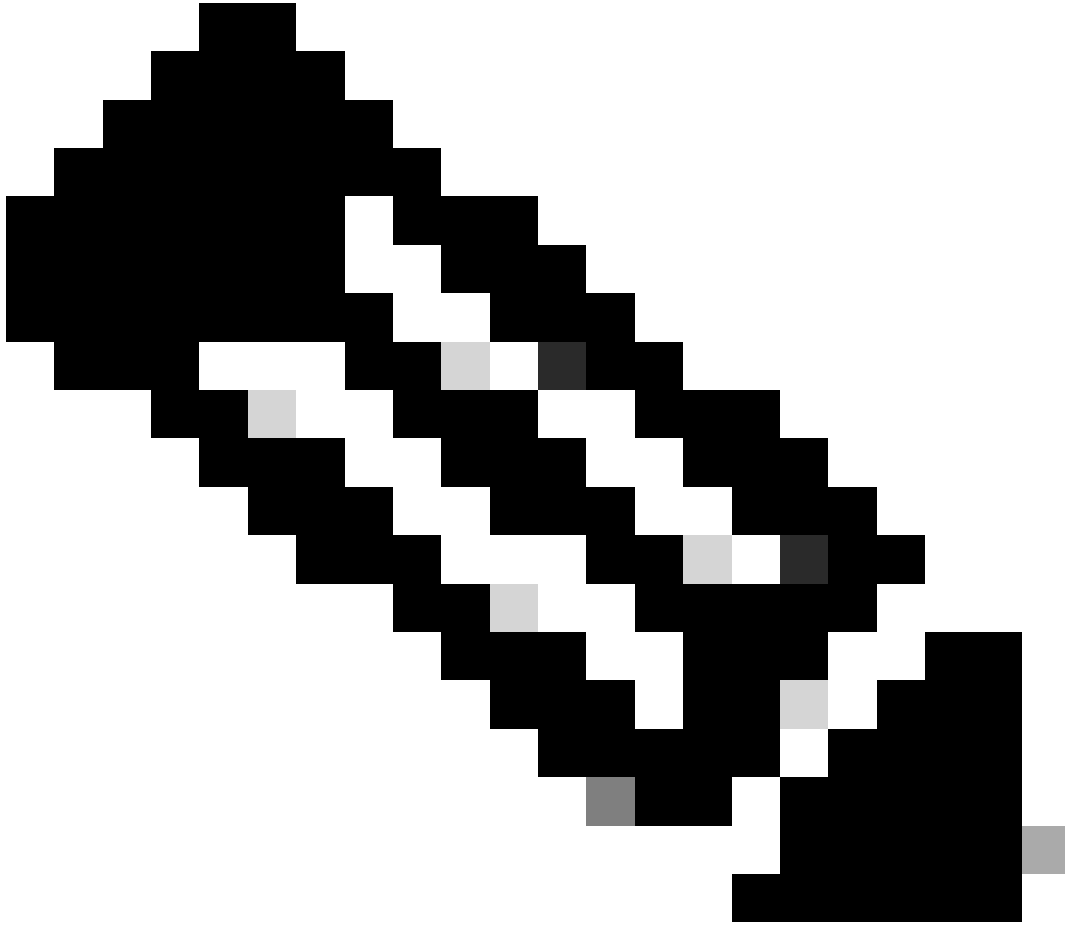


Selected Zones/Interfaces

Add

Cancel

OK






عافدلا قرادإ يف بـغرت تنك اذإ كلذل، تانايبلا تاهجاو ىلع يضارتفا لكشب SSH لوكوتورب نيكمتم متي ال: **تظحالم**
جـيرص لكشب هب جامسلا ىلإ ةجاحب تنأف، SSH مادختساب ديدتهتلا نع

ةحصلا نم ققحتلا

تانايبلا ةهجاو ربع قرادإلا لاصتا عاشن| نم دكأت

FMC ب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو نم ققحتلا

ةحفص<نيولكتلا ليصافت - لوصولا قرادإ > قرادإلا > زاهجلا > ةزهجالا قرادإ > ةزهجالا ليصوت ةلاح نم ققحت، ةرادإلا زكرم يف
لاصتالا ةلاح

Management 	
Remote Host Address:	192.168.1.30
Secondary Address:	
Status:	Connected  
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

FTD ل (CLI) رماوأل رطس ةهجاو لالغ نم ققحتلا

ةرادإلا لاصتا ةلاح ضرعل **fTunnel-status-brief** رمالا لخدأ، ديدتهتلاب ةصاخلا (CLI) رماوأل رطس ةهجاو يف

```
>
> sftunnel-status-brief
PEER:192.168.1.2
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC
Heartbeat Send Time: Tue Jul 16 22:39:52 2024 UTC
Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC
Last disconnect time : Tue Jul 16 22:17:42 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

ةيلخادلا TAP_NLP ةهجاو رهظتو، تانايب ةهجاو ل اجان لاصتا ةلاحلا ضرعت

اهجالصاو ءاطخال فاشكتسا

ةحفص<نيوكتلا ليصافت - لوصولا قرادا> > قرادإلا > زاهجال > ةزهجالا قرادا > ةزهجالا لىل ع قرادال لىصوت ةلاح نم ققحت، ةرادال زكرم يف لاصتالا ةلاح

مادختسا اضيأ كنكمي. ةرادإلا لاصتا ةلاح ضرعل **fTunnel-status-brief** رمالا لخدأ، ديدتهتلاب ةصاخلا (CLI) رماوأل رطس ةهجاو يف ةلامكلا تامولعمل نم ديزم ضرعل قفنلا ةلاح

ةرادإلا لاصتا ةلاح

لمعلا ويراني

> sftunnel-status-brief

PEER:192.168.1.2

Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC
Heartbeat Send Time: Wed Jul 17 17:15:20 2024 UTC
Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC
Last disconnect time : Wed Jul 17 06:21:12 2024 UTC
Last disconnect reason : Process shutdown due to stop request from PM

لمعال مدع ويراني س

> sftunnel-status-brief

PEER:192.168.1.2

Registration: Completed.
Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC
Last disconnect time : Wed Jul 17 17:20:26 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down

ةكبشال تامولعم ةحص نم ققحتلا

ريدملاو ةرادال لوصول تانايب ةهجاو ةكبش تادادع| ضرع، ديدتلاب ةصاخلا (CLI) رماوأل رطس ةهجاو دنع

> show network

```
> show network
===== [ System Information ] =====
Hostname                : ftdcdo.breakstuff.com
Domains                 : breakstuff.com
DNS Servers             : 192.168.1.103
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ eth0 ] =====
State                   : Enabled
Link                   : Up
Channels               : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 1500
MAC Address            : 00:0C:29:54:D4:47
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 192.168.1.8
Netmask                : 255.255.255.0
Gateway                : 192.168.1.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication         : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers            :
Interfaces             : GigabitEthernet0/0

===== [ GigabitEthernet0/0 ] =====
State                   : Enabled
Link                   : Up
Name                   : Outside
MTU                    : 1500
MAC Address            : 00:0C:29:54:D4:5B
```

قردادال لاصتال ةللخال ةلال رمال اذو ضرعو ال :نظالم

ةكبشلا لاصتا نم ققحتلا

قردال زكرمب لاصتال رابتخا

:تانايبل تاهواو نم تانايبل قردا زكرمب لاصتال رمال مدختسا ،ديدهتلاب ةصاخلا (CLI) رماوالا رطس ةهواو دنو

> FMC_IP لاصتال رابتخا

```
> ping 192.168.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

هوجوتلاب موقت يتلا ،قردال ةهواو نم قردال زكرمب لاصتال رمال مدختسا ،ديدهتلاب ةصاخلا (CLI) رماوالا رطس ةهواو دنو
:تانايبل تاهواو لىل ةفللخال ةحوللا ربع

> FMC_IP لاصتال رابتخا ماضن

```
> ping system 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.282 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 132ms
rtt min/avg/max/mdev = 0.282/0.311/0.340/0.030 ms
```

مزلل ددو تانايصاصل او ةهواو ةلال نم ققحتلا

ةفللخال ةحوللا ةهواو لوح تامولعم عجار ،ديدهتلاب ةصاخلا (CLI) رماوالا رطس ةهواو يف nlp_int_tap:

> ةهواو لىل صافت راظن

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
311553 packets input, 41414494 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
232599 packets output, 165049822 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "nlp_int_tap":
  311553 packets input, 37052752 bytes
  232599 packets output, 161793436 bytes
  167463 packets dropped
  1 minute input rate 0 pkts/sec, 3 bytes/sec
  1 minute output rate 0 pkts/sec, 0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec, 3 bytes/sec
  5 minute output rate 0 pkts/sec, 0 bytes/sec
  5 minute drop rate, 0 pkts/sec
Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active
```

FMC إلى لوصول FTD إلى راسملا ةحص نم ققحتالا

(NLP_INT_TAP) ةرادالا ةهجاول ةيلخادلا NAT دعاوق دوجو نمو (S*) يضارتفالا راسملا ةفاضلا نم دكأت، Challenge CLI في

راسملا راهظا >

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

```
C      192.168.1.0 255.255.255.0 is directly connected, Outside
L      192.168.1.30 255.255.255.255 is directly connected, Outside
```

> **رابطه nat**

```
> show nat
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface destination static 0_0.0.0.0_5 0_0.0.0.0_5 service tcp 8305 8305
  translate_hits = 5, untranslate_hits = 6
2 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel::_intf3 interface ipv6 destination static 0::_6 0::_6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
3 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 10, untranslate_hits = 0
4 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0
```

لأصتال او SFTUNNEL نتاي اصح | نم ققحتلا

> show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface Outside
sftunnel port 8305
```



FMC نم FTD فذح ضرر/لڃس تءاغل ا و FTD ىل ع رڃدم ل فذح ن ع ن ن ت م ا ، رڃدم ل لوص و رڃي غ ت ة ڃلم ع ل اوط : رڃي ذح

ةلص تاذ تام ول عم

- [ڃس اس ا ل ا م اظ ن ل ا ت اذ اذ ع ل رڃ ع DNS نڃ وكت](#)
- [رڃ ع FMC \(SSH و HTTPS\) ىل ا ةر اذ ل لوص و نڃ وكت](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعل وه
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل