

ةجـهـاـلـاـ حـيـصـوتـ نـمـ ضـرـغـلـاـ IP 203.0.113.x نـاـونـعـ نـمـ

ةـرـادـاـ FTD

تـايـوـتـحـمـلـاـ

[ةـمـدـقـمـلـاـ](#)

[ةـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ](#)

[تـابـلـطـتـمـلـاـ](#)

[ةـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـاـ](#)

[ةـيـسـاسـأـتـامـوـلـعـمـ](#)

[ةـعـمـجـمـلـاـ قـرـادـالـاـ ةـهـجـاـوـرـشـنـ تـايـلـمـعـ يـفـ قـيـرـادـالـاـ تـانـاـيـبـلـاـ رـورـمـ قـكـرـحـ رـاسـمـ](#)

[قـقـحـتـلـاـ](#)

[نـلـقـلـاـ](#)

[عـجـارـمـلـاـ](#)

ةـمـدـقـمـلـاـ

دـضـ عـافـدـلـاـ "ـيـفـ رـمـاـوـأـلـاـ ضـعـبـ جـارـخـاـ يـفـ حـضـوـمـلـاـ 203.0.113.xـ نـاـونـعـ دـنـتـسـمـلـاـ اـذـهـ فـصـيـ".ـ نـمـآـلـاـ ةـيـاـمـحـلـاـ رـادـجـ دـيـدـهـتـ".ـ

ةـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ

تابـلـطـتـمـلـاـ

جـتـنـمـلـابـ ةـيـسـاسـأـلـاـ ةـفـرـعـمـلـاـ.

ةـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـاـ

ةـصـاخـ ةـيـلـمـعـ ةـئـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ ءـاعـشـنـاـ مـتـ تـنـاـكـ اـذـاـ.ـ (ـيـصـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ،ـ لـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

ةـيـلـاتـلـاـ ةـيـدـامـلـاـ تـانـوـكـمـلـاـوـ جـمـارـبـلـاـ تـارـاـدـصـاـ ئـلـاـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ دـنـتـسـتـ

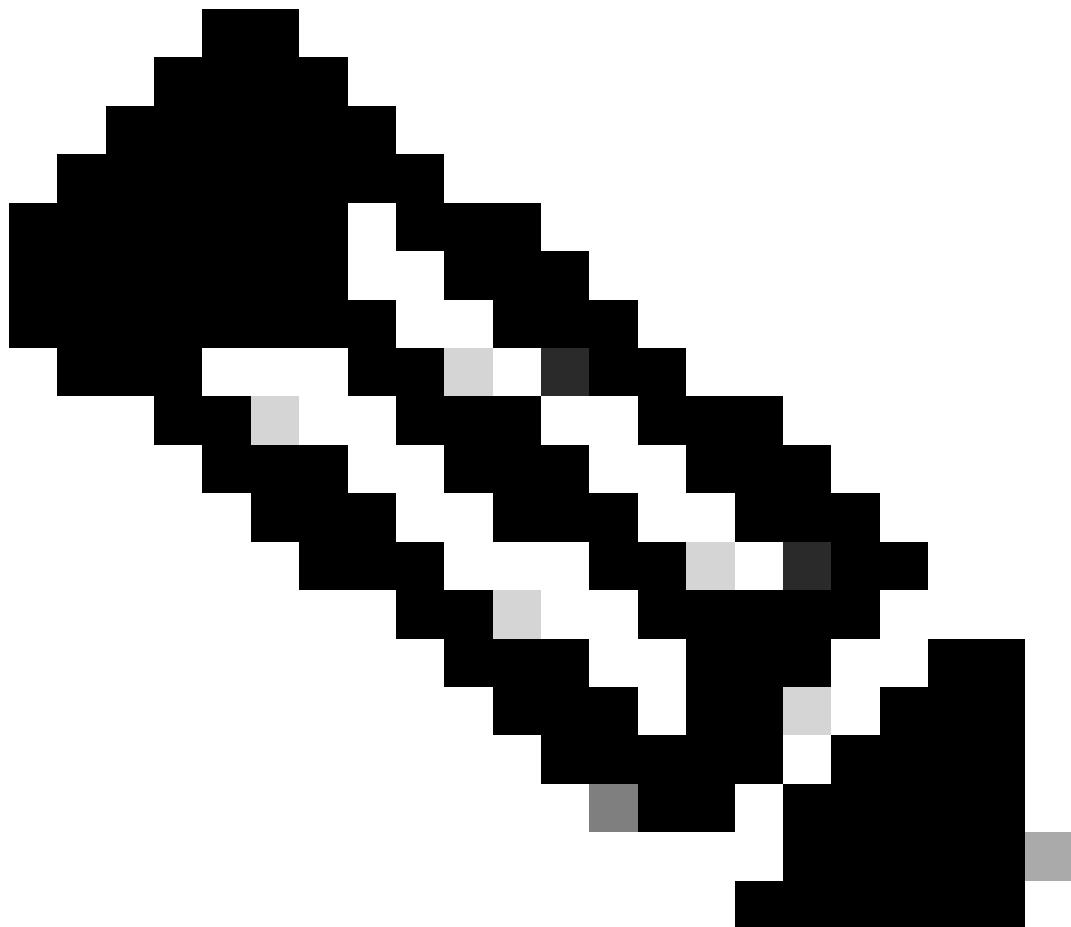
رـيـدـمـ ةـطـسـاوـبـ اـهـتـرـادـاـ مـتـ.ـ xـ 7.4.xـ،ـ 7.6.xـ FTDـ (ـةـيـاـمـحـلـاـ رـادـجـ طـبـارـتـ رـشـفـمـ نـعـ نـمـآـلـاـ عـافـدـلـاـ

-

(FMC) نمآلا ڦيامحل رادج ڦرادا زکرم وا (FDM) نمآلا ڦيامحل رادج ڦهنجا.

ةيسياساً تام ولع

نأونع ب ظل عتملا تارييغتل ظحالم كنكمي x 7.6.7 وأ x 7.4.7 رادص إلأ جمانربلا ئيقرت دعب ئارادإلا ئهجاول IP



تادادع| لصفلا يف "تانايبلا يل ٽرادالا يل ٽوصولا ٽهجاورىيغت" مسقلا يل عجرا

7.6 رادص إلـا Cisco نـم نـم آلـا ئـيـامـحـلـا رـادـج ئـرـادـإ زـكـرـم زـاهـج نـيـوـكـت لـيـلـد ئـف زـاهـجـلـا
رـادـج رـيـدـم نـيـوـكـت لـيـلـد ئـف تـاهـجـأـوـلـا: لـصـفـلـا ئـف "ئـرـادـإـلـا ئـهـجـأـوـنـيـوـكـت" مـسـقـلـاوـ
رـادـصـإـلـا Cisco نـم نـم آلـا ئـيـامـحـلـا 7.6.

يـتلـا FTD تـاجـخـمـلـلـاـثـمـ اـذـهـ ايـوـديـ هـنـيـوـكـتـ مـتـيـ مـلـهـنـأـ مـغـرـ،ـ IPـ 203.0.113.xـ وـهـ نـاـونـعـ.
ءـانـثـتـسـابـ ئـيـسـاسـأـلـاـ ئـمـظـنـأـلـاـ عـيـمـجـىـلـعـ لـمـعـتـ

```
<#root>

>

show nameif

Interface          Name           Security
Management1/1      management      0

>
show interface ip brief

Interface          IP-Address     OK?    Method Status   Protocol
...
Management1/1      203.0.113.130  YES    unset   up        up

>
show interface Management

Interface Management1/1 "management", is up, line protocol is up

Hardware is en_vtun rev00, DLY 1000 usec
Input flow control is unsupported, output flow control is unsupported
MAC address 0053.500.2222, MTU 1500
IP address 203.0.113.130, subnet mask 255.255.255.248

...
>
show running-config interface Management 1/1

!
interface Management1/1
```

```
management-only
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
```

و جا دا ة رادا لمعت یتل ا FTD ىلع Firepower 4100/9300:

```
<#root>

>

show nameif

Interface          Name           Security
...
Ethernet1/1        management      0

>

show interface ip brief

Interface          IP-Address     OK?    Method Status   Protocol
...
Ethernet1/1        203.0.113.130  YES   unset   up        up

>

show interface management

Interface Ethernet1/1 "management", is up, line protocol is up

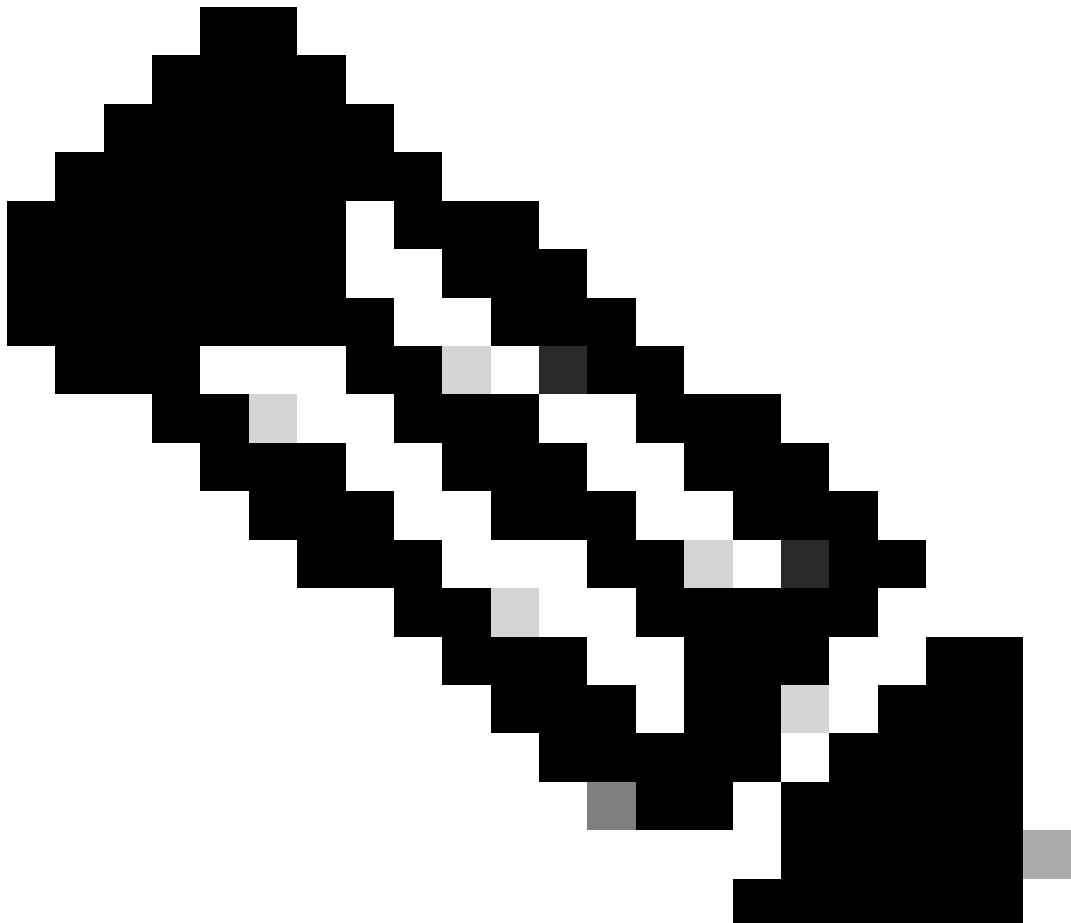
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
MAC address 0053.500.1111, MTU 1500
IP address 203.0.113.130, subnet mask 255.255.255.248

...
>

show running-config interface Ethernet 1/1

interface Ethernet1/1
```

```
management-only  
nameif management  
  
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0
```



ةرادإ ڈھاچاک سیل وہ Firepower 4100/9300 EtherNetX/y کنکمی، اسونا کنکمی، ڈھاچاک سیل وہ EtherNetX/y، ڈھاچاک مس ا ناف یل اتابو، تاقیب طتلل ڈھاچاک ManagementNetX/y.

2. show network: اونع نع اذه IP ناوونع جارخا یف نیبملا رمألا

<#root>

>

show network

===== [System Information] =====

| | | |
|--------------------|---|-----------------|
| Hostname | : | firewall |
| Domains | : | www.example.org |
| DNS Servers | : | 198.51.100.100 |
| DNS from router | : | enabled |
| Management port | : | 8305 |
| IPv4 Default route | | |
| Gateway | : | 192.0.2.1 |

===== [management0] =====

| | | |
|-----------------|---|---------------------|
| Admin State | : | enabled |
| Admin Speed | : | sfpDetect |
| Operation Speed | : | 1gbps |
| Link | : | up |
| Channels | : | Management & Events |
| Mode | : | Non-Autonegotiation |
| MDI/MDIX | : | Auto/MDIX |
| MTU | : | 1500 |
| MAC Address | : | 00:53:00:00:00:01 |

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

Configuration : Manual

Address : 192.0.2.100

Netmask : 255.255.255.0
Gateway : 192.0.2.1

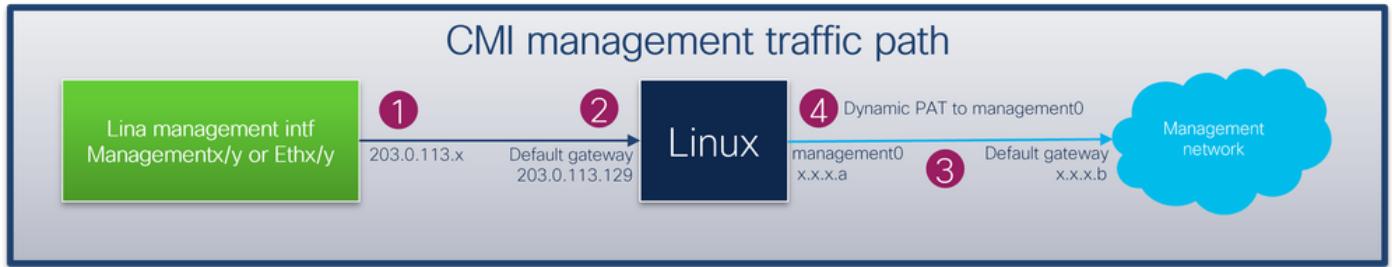
-----[IPv6]-----
Configuration : Disabled

(CMI) ةعجمجلـا ةرادـلاا ةـهـجـاـوـىـلـا IP 203.0.113.x نـاـونـعـنـيـيـعـتـ مـتـيـ وأـx 7.4.x رـادـصـإـلـاـىـلـاـ جـمـانـرـبـلـاـ ةـيـقـرـتـ دـعـبـ ،ـصـاـخـ لـكـشـبـ وـ 7.4.0 رـادـصـإـلـاـ يـفـ اـهـلـاخـدـاـ مـتـ يـتـلـاـ تـاهـجـاـوـجـمـدـ مـسـقـ يـفـ حـضـوـمـ وـهـ اـمـكـ صـيـخـشـتـلـاـوـ ةـرـادـلـاـ تـاهـجـاـوـجـمـدـ جـمـانـرـبـلـاـ حـرـتـقـيـ ،ـثـدـحـأـ رـادـصـإـ اـيـئـاقـلـتـ هـنـيـيـعـتـ مـتـيـ وـ ةـرـادـلـاـ وـهـ ةـرـادـلـاـ ةـهـجـاـوـىـلـاـ حـبـصـيـ ،ـجـمـدـلـاـ حـجـنـ اـذـاـ .ـصـيـخـشـتـلـاـوـ ةـرـادـلـاـ 203.0.113.x يـلـخـاـدـلـاـ IPـ نـاـونـعـلـ

٥٥ جاوشن تايىلمع يف ئيرادىلا تانايىبلا رورم ئىرخ راسىم
ئىعمجملا ئيرادىلا

ةرادإلا تاكبش ىل او Lina كرحم نم ةرادإلا لاصتا ريفوتل IP 203.0.113.x ناونع مادختس ا متى اي ف موقدت يتلا تالاحلا يف يرورض لاصتا الا اذه .يلي امك 0لكيهل ٠ةرادإ ٠ةهج او رباع ٠ةيجراخلا ٠ةقداص ملا مدافخ ىل ا لوصول او ، (DNS) لاجمل ا مسا لحو ، syslog لثم Lina تامدخ نيوكتب كل ذ ىل ا امو (AAA) ةبساحمل او ليوختل او

ىلى Lina كرحم نم ۋاردىلا رورم ۋەكىر راسىم ىلۇغىنى سەملا ۋە يىلاع ۋە مامۇ ئەرظان طاطخىملا اذە حضۇرى
ئەجىرالىخ لە ئەردا ئەنلىك ئەتكەن ئەجىرالىخ لە ئەردا ئەتكەن:



ةيسيئرلا طاقنلا:

مسا مادختساب ٰهـجـاـولـا لـفـسـأـ 29 / ةـكـبـشـلـا عـانـقـعـمـ IP 203.0.113.x نـاـونـعـ نـيـوـكـتـ مـتـيـ . 1. رـمـأـلـا جـارـخـا يـفـ يـئـرـمـ رـيـغـ نـيـوـكـتـلـا اـذـهـ نـكـلـوـ IF ٰهـرـادـاـ show run interface:

```
<#root>
>
show interface Management
```

```
Interface Management1/1 "management", is up, line protocol is up
Hardware is en_vtun rev00, DLY 1000 usec
Input flow control is unsupported, output flow control is unsupported
MAC address bce7.1234.ab82, MTU 1500

IP address 203.0.113.130, subnet mask 255.255.255.248
```

```
...
>
show running-config interface Management 1/1

!
interface Management1/1
management-only
nameif management
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
```

راسملـا اـذـهـ . ٰهـرـادـا هـيـجـوـتـ لـوـدـجـ نـمـضـ 203.0.113.129 ةـيـضـاـرـتـفـالـا ةـبـاوـبـلـا ةـكـبـشـ نـيـوـكـتـ مـتـيـ كـنـكـمـيـ . تـاطـيـسـ وـنـوـدـبـ show route management-only رـمـأـلـا جـارـخـا يـفـ يـئـرـمـ رـيـغـ يـضـاـرـتـفـالـا نـاـونـعـلـا دـيـدـحـتـ لـالـخـ نـمـ رـاسـمـلـا نـمـ قـقـحـتـلـا 0.0.0.0:

```
<#root>
```

```

>

show route management-only

Routing Table: mgmt-only
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

>

show route management-only 0.0.0.0

Routing Table: mgmt-only
Routing entry for 0.0.0.0 0.0.0.0, supernet
  Known via "static", distance 128, metric 0, candidate default path
  Routing Descriptor Blocks:
    *

203.0.113.129, via management

  Route metric is 0, traffic share count is 1

>

show asp table routing management-only

route table timestamp: 51
in  203.0.113.128  255.255.255.248 management
in  0.0.0.0          0.0.0.0          via 203.0.113.129, management

out 255.255.255.255 255.255.255.255 management
out 203.0.113.130  255.255.255.255 management
out 203.0.113.128  255.255.255.248 management
out 224.0.0.0        240.0.0.0        management

out 0.0.0.0          0.0.0.0          via 203.0.113.129, management

out 0.0.0.0          0.0.0.0          via 0.0.0.0, identity

```

متي وءاربخلا عضويف هتى فرنكمي و Linux IP 203.0.113.129 بناجىل عن نيونوكت متي.

<#root>

```
admin@KSEC-FPR3100-2:~$
```

```
ip route show 203.0.113.129/29
```

```
203.0.113.128/29 dev tap_M0 proto kernel scope link src 203.0.113.129
```

اذه .0.ةرادلـا ةـهـجـاـولـ لـكـيـهـلـا ةـرـادـابـ صـاـخـلـا IPـ نـاـونـعـ صـيـصـخـتـ مـتـيـ،ـ لـيـغـشـتـلـاـ مـاطـنـ يـفـ 3.

ـرـمـأـلـاـ تـاجـخـمـ يـفـ يـئـرـمـلـاـ IPـ نـاـونـعـ وـهـ show network:

```
<#root>
```

```
>
```

```
show network
```

```
===== [ System Information ] =====
```

```
Hostname : firewall  
Domains : www.example.org  
DNS Servers : 198.51.100.100  
DNS from router : enabled  
Management port : 8305  
IPv4 Default route  
    Gateway : 192.0.2.1
```

```
===== [ management0 ] =====
```

```
Admin State : enabled  
Admin Speed : sfpDetect  
Operation Speed : 1gbps  
Link : up  
Channels : Management & Events  
Mode : Non-Autonegotiation  
MDI/MDIX : Auto/MDIX  
MTU : 1500  
MAC Address : 00:53:00:00:00:01
```

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

```
Configuration : Manual  
Address : 192.0.2.100
```

```
Netmask : 255.255.255.0  
Gateway : 192.0.2.1
```

```
----- [ IPv6 ] -----
```

```
Configuration : Disabled
```

```
>
```

```
expert
```

```
admin@KSEC-FPR3100-2:~$
```

```
ip addr show management0
```

```

15: management0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 00:53:00:00:00:01 brd ff:ff:ff:ff:ff:ff
    inet
        192.0.2.100
        /
        24
        brd 192.0.2.255 scope global management0
            valid_lft forever preferred_lft forever
...
admin@KSEC-FPR3100-2:~$ ip route show default

```

default via 192.0.2.1 dev management0

ىلإ ناونع ردصملا مجرتي نأ نراق 0ةرالا ىلع (برض) يكرح رسياً ناونع 0ةمجرت كانه. مادختساب لواج 0دعاق نيوكت لالخ نم يكيمانيد برض قيقحت متى .ناونع نراق 0ةرالا MASQUERADE 0هجاو ىلع management0:

```

<#root>
admin@KSEC-FPR3100-2:~$ sudo iptables -t nat -L -v -n
Password:
...
Chain POSTROUTING (policy ACCEPT 49947 packets, 2347K bytes)
 pkts bytes target     prot opt in     out     source          destination
 6219  407K MASQUERADE  all  --  *      management0+  0.0.0.0/0           0.0.0.0/0

```

ققحتلا

نراق 0ةرالا قيرط نع لح DNS تلکش يسأسألا ماظنلا يفو تنكم CMI ،لاثم اذه يف:

```

<#root>
>
show management-interface convergence
management-interface convergence

```

```
>

show running-config dns

dns domain-lookup management

DNS server-group DefaultDNS
DNS server-group ciscodns

name-server 198.51.100.100 management

dns-group ciscodns
```

تاهج او لع مزح لـ Linux tap_m0 و Management0: نـيـوكـتـ مـتـيـ

```
<#root>

>

show capture

capture dns type raw-data interface management [Capturing - 0 bytes]

match udp any any eq domain

>

expert

admin@firewall1:~$ sudo tcpdump -n -i tap_M0 udp and port 53

Password:
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tap_M0, link-type EN10MB (Ethernet), capture size 262144 bytes

>

expert

admin@firewall1:~$ sudo tcpdump -n -i management0 udp and port 53
```

```
Password:  
HS_PACKET_BUFFER_SIZE is set to 4.  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on management0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

كرحم نم DNS بـلـط عـاـشـنـابـ (FQDN) لمـاـكـلـابـ لـهـفـمـ لـاجـمـ مـسـاـ ةـنـيـعـلـ ICMP ئـدـاـبـلـلـ IP نـاـونـعـ Linux tap_m0 203.0.113.130،
Lina. يـفـ ةـمـزـحـلـاـ طـاقـتـلـاـ رـهـظـيـ لـيـفـ كـرـحـمـ اـوـجـاـوـ وـهـوـ:ـ نـاـونـعـ CMI ةـرـادـإـلـاـ ةـهـجـاـوـ وـهـوـ:

```
<#root>  
>  
ping interface management www.example.org  
  
Please use 'CTRL+C' to cancel/abort...  
Sending 5, 100-byte ICMP Echos to 198.51.100.254, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/122/130 ms
```

```
>  
show capture dns  
  
2 packets captured  
 1: 23:14:22.562303  
  
203.0.113.130  
  
.45158 > 198.51.100.100.53: udp 29  
 2: 23:14:22.595351      198.51.100.100.53 >  
  
203.0.113.130  
  
.45158: udp 45  
2 packets shown
```

```
admin@firewall  
:~$ sudo tcpdump -n -i tap_M0 udp and port 53  
  
Password:  
HS_PACKET_BUFFER_SIZE is set to 4.  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on tap_M0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
23:14:22.570892 IP  
203.0.113.130  
.45158 > 198.51.100.100.53: 38323+ A? www.example.org. (29)  
23:14:22.603902 IP 198.51.100.100.53 >  
203.0.113.130
```

PAT ىلا عجري اذهو .نانونع ئدابلاك نراق 0 ئراديلا نم نانونعلانراق 0 ئراديلا ىلع طبرلا رهظت ۋەج او رشن تايلىمع يف ئراديلا تانايىب رورم ئىچ راسىم "مسقىلا يف روکذىملائىكمانىدىلا ئېلاقىتملا ئراديلا":

<#root>

admin@firewall:~\$

sudo tcpdump -n -i management0 udp and port 53

Password:

HS_PACKET_BUFFER_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on management0, link-type EN10MB (Ethernet), capture size 262144 bytes

23:14:22.570927 IP

192.0.2.100

.45158 > 198.51.100.100.53: 38323+ A? www.example.org. (29)

23:14:22.603877 IP 198.51.100.100.53 >

192.0.2.100

.45158: 38323 1/0/0 A 198.51.100.254 (45)

رارقلا

ايلىخاد ھمادختسى مىتىو ايئاقلت IP 203.0.113.x ناونع نىيىعت مىتى ، CMI نىكىمت مىت اذى لەجەت كنكمىي .ئېجراخلا ئراديلا ئېكېش و Lina كرحم نىپ لاصتالا رىفوتل جمانربلا ئەتساوب IP ناونع.

ديحوللا حىحىسىلا IP ناونع وھو رىيغەت نود show network رمألا جارخا يف رەاظىلا IP ناونع لە ئەتساوب FTD.

عجارملا

• [صىخشتلىك ئەراديلا تاھجاوجىد](#)

• [7.6 Cisco، ئەراديلا نم نمآلما ئىامحللارادىز كرم زاھج نىيوكتلىيىلد](#)

• [7.6 Cisco، ئەراديلا نم نمآلما ئىامحللارادىز كرم زاھج رىدم نىيوكتلىيىلد](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).