

يـفـ صـيـخـشـتـلـاوـ ةـرـادـإـلـاـ ةـهـجـاوـ جـمـدـ نـيـوـكـتـ

تـايـوـتـحـمـلـاـ

[قـمـدقـمـلـاـ](#)

[قـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ](#)

[قـيـسـاسـأـ تـامـوـلـعـمـ](#)

[قـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـاـ](#)

[نـيـوـكـتـلـاـ](#)

[قـيـلـخـادـلـاـ FTDـ قـيـنـبـلـيـ طـخـتـلـاـ مـسـرـلـاـ](#)

[بـرـاقـتـلـاـ عـارـجـاـ](#)

[قـحـصـلـلـاـ بـنـمـ قـقـحـتـلـاـ](#)

[قـسـارـدـلـاـ قـلـاحـ -ـ اـهـحـالـصـ اوـ اـعـاطـخـأـلـاـ فـاشـكـتـسـأـ](#)

[بـرـاقـتـنـيـوـكـتـلـبـقـ](#)

[بـرـاقـتـنـيـوـكـتـدـعـبـ](#)

ةـمـدقـمـلـاـ

يـتلـاـ ـقـيـمـلـاـ ،ـصـيـخـشـتـلـاوـ ةـرـادـإـلـاـ تـاهـجـاوـ جـمـدـ نـيـوـكـتـلـاـ دـنـتـسـمـلـاـ اـذـهـ فـصـيـ

ـرـادـصـاـ يـفـ اـهـتـفـاصـاـ تـمـتـ

FTD 7.4.0.

ةـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ

ـقـيـلـاتـلـاـ عـيـضـاـوـمـلـاـبـ ـقـفـرـعـمـ كـيـدـلـ نـوـكـتـ نـأـبـ Ciscoـ يـصـوـتـ

- ـنـمـ Ciscoـ نـمـ (FTD)ـ ةـيـاـمـحـلـاـ رـادـجـ دـيـدـهـتـ نـعـ نـمـآـلـاـ عـافـدـلـاـ
- ـنـمـ Ciscoـ نـمـ (FMC)ـ ةـيـاـمـحـلـاـ رـادـجـ رـيـدـمـ زـكـرـمـ

ةـيـسـاسـأـ تـامـوـلـعـمـ

ـةـهـجـاـوـلـاـ نـيـبـ ةـيـدـامـلـاـ ةـرـادـإـلـاـ ةـهـجـاوـ ةـكـراـشـمـ مـتـتـ ،ـقـقـبـاـسـلـاـ تـارـادـصـإـلـاـوـ 7.3ـ رـادـصـإـلـاـ يـفـ

ـةـرـادـإـلـلـ ةـيـقـطـنـمـلـاـ ةـهـجـاـوـلـاـوـ (Linux)ـ صـيـخـشـتـلـلـ ةـيـقـطـنـمـلـاـ.

ـةـبـرـجـتـ طـيـسـبـتـلـ ةـرـادـإـلـاـ عـمـ صـيـخـشـتـلـاـ ةـهـجـاوـ جـمـدـ مـتـيـ ،ـثـدـحـأـلـاـ تـارـادـصـإـلـاـوـ 7.4ـ رـادـصـإـلـاـ يـفـ

ـمـدـخـتـسـمـلـاـ.

ـمـاـدـخـتـسـاـ لـكـنـكـمـيـ الـ ،ـثـدـحـأـلـاـ تـارـادـصـإـلـاـوـ 7.4ـ رـادـصـإـلـاـ مـدـخـتـسـتـ يـتـلـاـ ةـدـيـدـجـلـاـ ةـزـهـجـأـلـلـ ةـبـسـنـلـاـبـ

ـطـقـفـ ةـجـمـدـمـلـاـ ةـرـادـإـلـاـ ةـهـجـاوـ رـفـوـتـ .ـقـمـيـدـقـلـاـ صـيـخـشـتـلـاـ ةـهـجـاوـ

ةـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـاـ

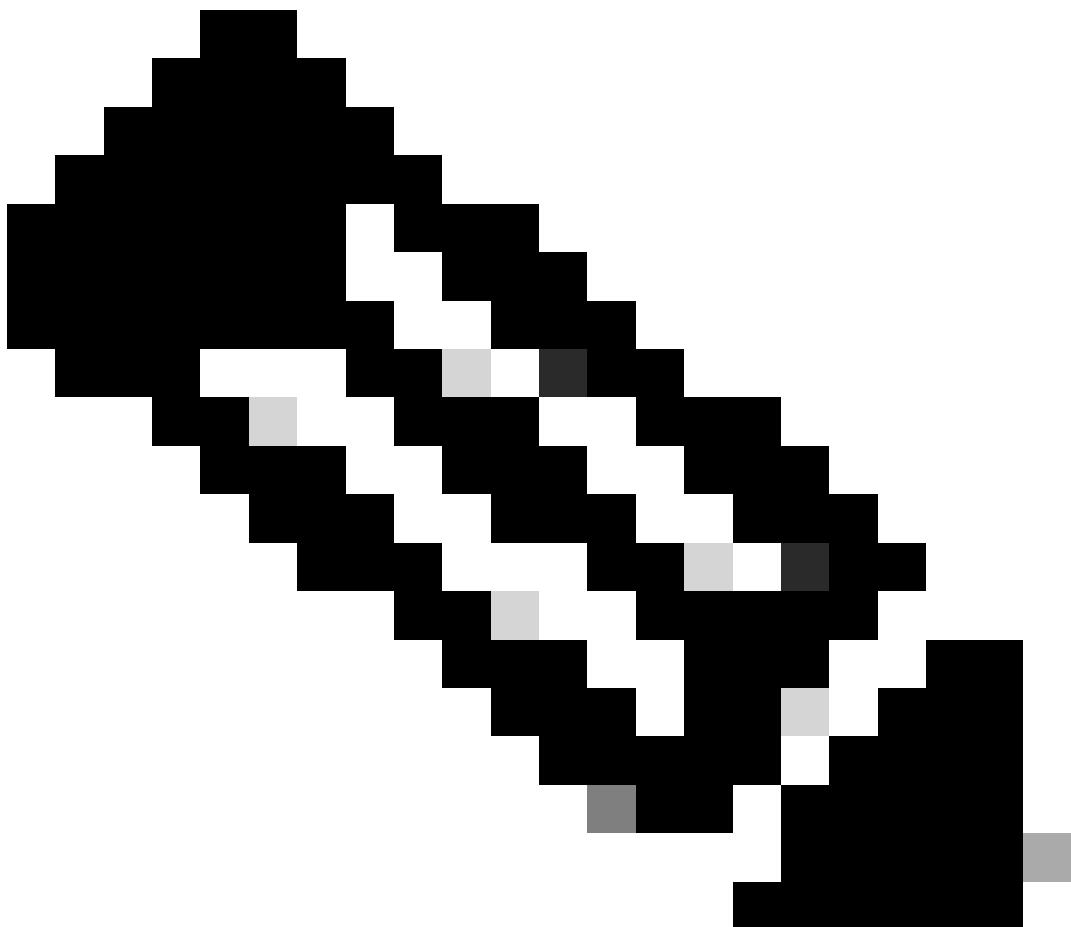
ـقـيـلـاتـلـاـ ةـيـدـامـلـاـ تـانـوـكـمـلـاـوـ جـمـارـبـلـاـ تـارـادـصـإـلـاـ يـلـاـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ دـنـتـسـتـ

- Cisco Virtual Secure Firewall Threat Defense (FTD)، رادص إلـا 7.4.2
- Cisco، رادص إلـا 7.4.2 (FMC) نـم يـرـهـاـظـلـا ئـيـامـحـلـا رـادـجـ زـكـرـم

ةـصـاخـ ئـيـلـمـعـمـ ئـيـبـ يـفـ ئـدـوـجـوـمـلـا ئـزـهـجـأـلـا نـمـ دـنـتـسـمـلـا اـذـهـ يـفـ ئـدـرـاـوـلـا تـامـوـلـعـمـلـا عـاـشـنـا مـتـ
تـنـاـكـ اـذـاـ. (يـضـارـتـفـاـ) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـهـ يـفـ ئـمـدـخـتـسـمـلـا ئـزـهـجـأـلـا عـيـمـجـ تـأـدـبـ
رـمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ، لـيـغـشـتـلـا دـيـقـ كـتـكـبـشـ.

نـيـوـكـتـلـا

كـيـدـلـفـ، صـيـخـشـتـلـا ئـهـجـاـوـلـا نـيـوـكـتـ كـيـدـلـ نـاـكـوـ، ثـدـحـأـ رـادـصـاـ وـأـ 7.4ـىـلـا ئـيـقـرـتـلـابـ تـمـقـ اـذـاـ
ةـلـصـفـنـمـلـا صـيـخـشـتـلـا ئـهـجـاـوـمـاـدـخـتـسـاـ يـفـ رـاـرـمـتـسـاـلـا كـنـكـمـيـ وـأـ، اـيـوـدـيـ تـاهـجـاـوـلـا جـمـدـلـ رـايـخـلـاـ.
اـيـئـاقـلـتـ تـاهـجـاـوـلـا جـمـدـمـتـيـ، صـيـخـشـتـلـا ئـهـجـاـوـلـا نـيـوـكـتـ يـأـ دـوـجـوـمـدـعـ ئـلـاحـ يـفـ.

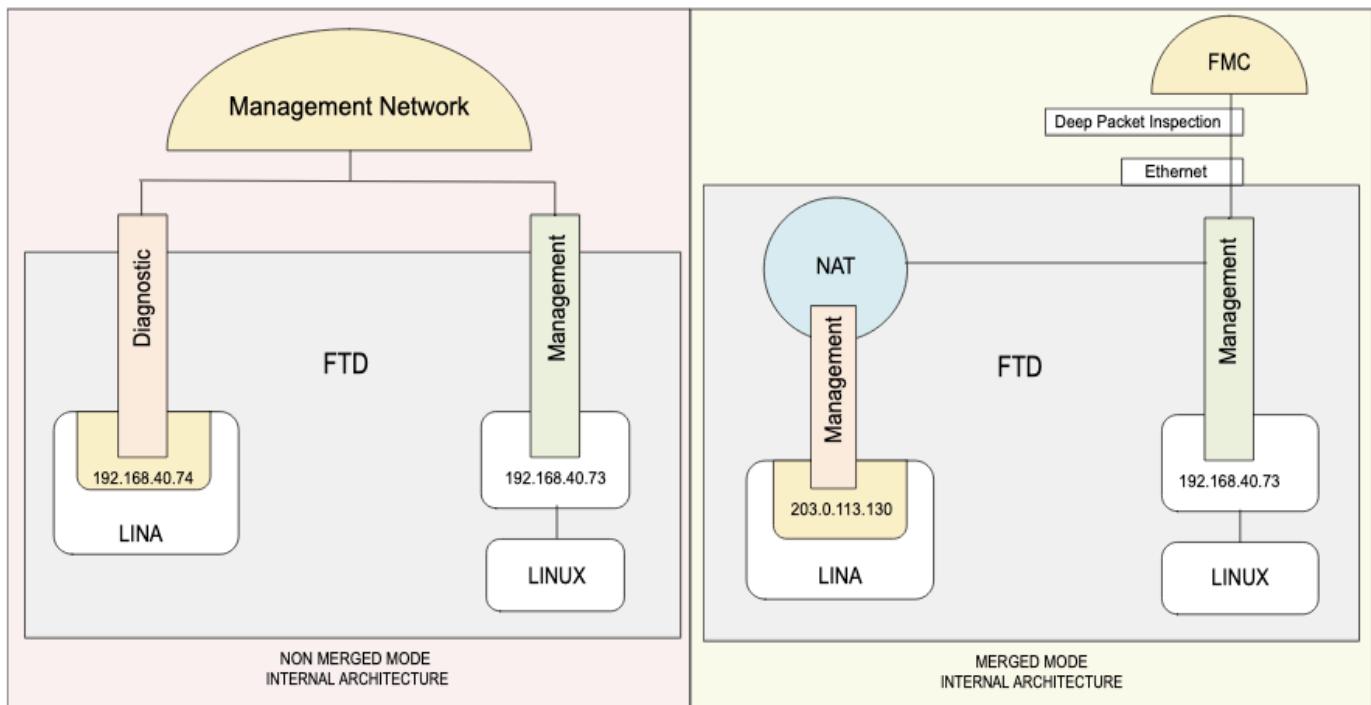


طـيـطـخـتـلـابـ مـقـ، كـلـذـلـ، قـحـالـ رـادـصـاـ يـفـ صـيـخـشـتـلـا ئـهـجـاـوـمـعـدـ ئـلـاـزاـ مـتـتـسـ: ئـظـحـاـلـمـ

نكمم تقو برقاً يف تاهج اولا جمدل.

ةيلخادلـا FTD ةينبلـي طيـطختـلا مـسـرـلـا

ةـعمـجمـلـا ةـرـادـلـا ةـهـجـاوـلـع ةـمـاع ةـرـظـنـ



اهـدـعـبـوـبـرـاقـتـلـا ةـرـادـا ةـهـجـاوـلـع ةـيـلـخـادـلـا ةـيـنـبـلـا ئـلـع ةـمـاع ةـرـظـنـ

ةـيـقـطـنـمـلـا ةـهـجـاوـلـاـو (Lina) ةـيـصـيـخـشـتـلـا ةـيـقـطـنـمـلـا ةـهـجـاوـلـل ةـيـلـخـادـلـا ةـيـنـبـلـا ، رـاسـيـلـا ئـلـعـ
ةـقـبـاـسـلـا تـارـادـصـإـلـاـو 3 . 7 رـادـصـإـلـا ةـرـادـلـلـاـو (Linux).

ةـمـدـخ ةـرـادـلـا ةـكـبـشـىـلـا Lina لـوـصـوـمـدـخـتـسـيـ. ةـدـحـاـو ةـرـادـا ةـهـجـاوـلـا ةـيـلـخـادـلـا ةـيـنـبـلـا ، نـيـمـيـلـا ئـلـعـ
NAT.

براقتـلـا ءـارـجـاـ

ايـئـاقـلتـتـ تـاهـجـاوـلـا جـمـدـمـتـيـ الـ ، صـيـخـشـتـلـا ةـهـجـاوـيـفـ نـيـوـكـتـلـاـ ايـفـ دـجـوـيـ يـتـلـا ةـلـاحـلـاـ يـفـ
براقتـلـا ءـارـجـاـ ذـيـفـنـتـ كـيـلـعـ بـجـيـوـ، ةـيـقـرـتـلـا دـعـبـ.

نـيـوـكـتـلـا حـالـصـاـ ، تـالـاحـلـا ضـعـبـ يـفـوـ، نـيـوـكـتـلـا تـارـيـيـغـتـبـ رـارـقـإـلـاـ كـنـمـ ءـارـجـإـلـاـ اـذـهـ بـلـطـتـيـ
ايـوـديـ.

رـطـسـ ةـهـجـاوـيـفـ show management-interface converge رـمـأـلـا لـخـأـ ، زـاهـجـلـلـ يـلـاحـلـا عـضـولـا ضـرعـلـ
لـ (رمـأـلـاـ رـطـسـ ةـهـجـاوـ) CLI رـمـأـلـاـ FTD

```
> show management-interface convergence  
no management-interface convergence
```

ةجمدم ريع ةرادلأا تاهجاونأ ةجيتنلا هذه حضوت.

1. وةوطخلأا.

متى .٥. ريرحت دارملأا FTD ددحو، ةزهجألا ةرادا > ةزهجألا ةرادا لقتنا، FMC مدخلتسم ةهجاو لعل تاهجاولا بيوبتللا ةمالمع ليل ةرشابم ٥ حتف.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices (which is selected), Objects, and Integration. On the right, there are Deploy, Search, Settings, and User admin options. The main content area is titled 'Tac_test' and describes 'Cisco Firepower Threat Defense for VMware'. Below this, there are tabs for Device, Interfaces (selected), Inline Sets, Routing, DHCP, and VTEP. A message box at the top left says 'Management Interface action needed.' It provides instructions to merge management and diagnostic interfaces or merge them later via a dialog box. It also notes that merging will cause some downtime and provides a link to learn more. The main table lists interfaces: Diagnostic0/0 (selected, highlighted in green), GigabitEthernet0/0, GigabitEthernet0/1, and GigabitEthernet0/2. Columns include Interface, Logical Name, Type, Security Zones, MAC Address (Active/Standby), IP Address, Path Monitoring, Virtual Router, and a edit icon. The IP address for Diagnostic0/0 is 192.168.40.74/255.255.255.0.

7.4.2 جمانربلا رادصا ليل زاهجلا ةيقرت دعب ةرادلأا صيخشتلا ةهجاو جمدل بولطمملأا عارجلإا

2. وةوطخلأا.

صيخشتلا ةهجاو يوتحت الـأ يرورضلأا نم .صيخشتلا ةهجاو لعل نـيـوكـتـلـا عـيـمـجـ ةـلـازـابـ مـقـ جـمـدـلـا عـبـاتـمـلـ نـيـوكـتـ يـأـ لـعـ.

تباثلأا هجوملأاو IP ناونع :كانه ،هذه صيخشتلا ةهجاويـفـ ،ـلـاثـمـلـاـ لـيـبـسـ لـعـ.

The screenshot shows the Firewall Management Center interface with the Devices tab selected for 'Tac_test'. A modal dialog box is open over the interface list, titled 'Edit Physical Interface'. The 'IPv4' tab is active. Inside the dialog, the 'IP Type:' dropdown is set to 'Use Static IP', and the 'IP Address:' field contains '192.168.40.74/255.255.255.0'. Below the address is an example: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'. At the bottom of the dialog are 'Cancel' and 'OK' buttons. The background shows the list of interfaces: Diagnostic0/0 (selected), GigabitEthernet0/0, GigabitEthernet0/1, and GigabitEthernet0/2. The 'All Interfaces' tab is selected. The right side of the screen shows the same interface configuration table as the previous screenshot.

ةـصـيـخـشـتـلـاـ ةـهـجـاوـلـلـ IPـ نـاـونـعـ

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Tac_test
Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing

BGP

IPv4
IPv6

Static Route

Multicast Routing

+ Add Route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
DNS	diagnostic	Global	192.168.40.254	false	1	
IPv6 Routes						

صيختلا ٰههوجاوىل عتابلا راسملانىوكت

3. ٰهوطخل.

ريحتلا ٰنوقىأ ٰرواجملاجمدلا ٰنوقىأ ٰهبولطملا ٰرادلا ٰههوجمدا ٰققطنم قوف رقنا صيختلا ٰههوجاوىل (صاصللا ملقلا).

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Tac_test
Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP

Management Interface Merge

Management Interface action needed.
Merge the Management and Diagnostic interfaces on the Management interface will cause some downtime. [Learn more](#)

All Interfaces Virtual Tunnels

Interface	Logical Name
Diagnostic0/0	diagnostic
GigabitEthernet0/0	
GigabitEthernet0/1	
GigabitEthernet0/2	

The management interface merge will be synced to the standby/data unit. The IP addresses shown in the "Review Uses" section shows the active unit's active address.

- After you click Proceed, IP address changes will be saved, and you cannot revert the management interface merge, even if you discard the deployment.
- Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed. [Learn more](#)
- HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address. [Learn more](#)

Sync Device Add Interfaces

Path Monitoring	Virtual Router
Disabled	Global
Disabled	
Disabled	
Disabled	

Proceed Cancel

تعاباتملال بق ٰرادلا ٰههوجمدا ٰهبولطم



ىلע ۋەمەلە ھەذە ذىفەن تې مۇق ، رفوو تلا ۋەيلاع تاوعومەجەل او جاۋازلەل ۋە بىسەنلىپ : ۋە ظەحالىم
ايئاقلەت ئىثامتم اخسن جەمدەلە نېۋەكتەلە خسن مەتى . مەكھەتلە ۋە دەحۋە / ۋە طشەنلە ۋە دەحۋە ئەلە
تانايىبىلە / دادعەتسالا تادحۋە ئەلە.

-
- رېذھەت ۋەن وقىي أ رەھەت نأ نەكمىي ، ۋەيودى ۋە لازا وأ رېييغەت نوکىي نأ بىلەتتى راركەت يىأل .

Management Interface Merge

- Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed. [Learn more](#)
 - HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address.

[Learn more](#)

Review the Diagnostic IP uses below. The symbol shows configuration uses that you must edit manually before you can proceed.

REVIEW 2 USES

C Refresh

Do you acknowledge the change?

Management Interface

The system will no longer support a Virtual Active Unit IP addresses that migrates between the Active and Stand-by HA units in converged mode. Please remove the IP address on (Diagnostic0/0) before proceeding with convergence.. [See less](#)

Static Route Setting

Static Route Setting under virtual router [Global] with management interface (diagnostic) are not valid when the interface is converged. Please configure these routes on the device if required and clean the static routes in FMC to proceed with the convergence [See less](#)

Proceed

Cancel

جمدلا لباق هتلانا بولطملا تانيوكتلا لوح ريدجتلا لاثم

دعأ مث ،نيوكتلا ڦداعاً وأ نيوكتلا ڦلما عبات مث ،راوحلا عبرم ۽اغلاب مق :لاحلا وه اذه ناك اذا ڦرادلاا ڦهجاو جمد" راوحلا عبرم حتف".

- ري ذخت زمرب زاهجل اىلع لممعت يتلا يس اسألا ماظنلا تادادع اىلع ٩م الاع عض و متى اراغش بـ لـ طـ تـ تو.

Management Interface Merge

? ×

- The management interface merge will be synced to the standby unit. The IP addresses shown in the "Review Uses" section shows the active unit's active address.
- After you click Proceed, IP address changes will be saved, and you cannot revert the management interface merge, even if you discard the deployment.
- Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed. [Learn more](#)
- HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address.

[Learn more](#)

Review the Diagnostic IP uses below. The  symbol shows configuration uses that you must edit manually before you can proceed.

REVIEW 2 USES

 Refresh

Do you acknowledge the change?

▲ **HTTP Access**

Management interface (management) is used in (HTTP Access) of PF... [See more](#)



▲ **ICMP Access**

Management interface (management) is used in (ICMP Access) of PF... [See more](#)



 Cancel

 Proceed

اوريحـت بـجـي يـتلـا يـسـاسـالـا مـاظـنـلـا تـادـاعـا تـانـيـوـكـتـنـم رـيـذـحـتـلـا يـلـعـلـا لـاثـمـ

• ةـعـبـاتـمـ قـوـفـ رـقـنـاـ مـثـ ، دـوـمـعـ ؟ رـيـيـغـتـلـاـ فـرـتـعـتـ لـهـ يـفـ عـبـرـمـلـاـ رـقـنـاـ.

4. ةـوطـخـلـاـ

ـحـاجـنـ رـاعـشـ ضـرـعـ مـتـيـ ، نـيـوـكـتـلـاـ جـمـدـ دـعـبـ

ـرـشـنـلـلـ زـهـاجـ وـهـوـ ةـرـادـإـلـاـ ةـهـجـاـوـجـمـدـ ظـفـحـ مـتـ

ـةـهـجـاـوـ نـيـوـكـتـ ةـدـاعـاـ بـجـيـ ؛ جـمـدـلـاـ بـقـلـعـتـمـلـاـ نـيـوـكـتـلـاـ تـارـيـيـغـتـ نـعـ عـجـارـتـلـاـ كـنـكـمـيـ الـ هـنـأـ ظـحـاـلـ

ايوه ئەلصلانى يۈچۈن كەلەپىلىم

دي دجله جمدمل نويوك تلا رشنب مق.

Tac_test

Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP VTEP

The Management interface merge was saved and is ready to be deployed.
Note that you cannot undo the configuration changes related to merge; you must manually reconfigure the Diagnostic interface and related configuration.

All Interfaces	Virtual Tunnels	Search by name	Sync Device	Add Interfaces
Management0/0	management	Physical	Disabled	Global
GigabitEthernet0/0		Physical	Disabled	
GigabitEthernet0/1		Physical	Disabled	
GigabitEthernet0/2		Physical	Disabled	

رشنلل ازهاج حبص أو ۀرادإلا ۀهج او جمد ظفح مت

طقف ةءارقلل اهنأ نم مغزلاب ،تاهج اولا ٔحفص ىلع ٔرادإا ٔهنج او رهظت

لمنتکا دق ۋەردىلا ٩٥جى او ىلىع بىراققىتلا ئارجا نوڭى، رشنلدا دىپ

۵. ۋە طاخلا ئرایت خا.

نیوکتلا رییغت یل اقاحب تنافس، صیخشتلا ۆهجاوب تلصتا ۆیجراخ تامدخ یا کیدل ناک اذإ یلع یطایتحالا راسملە ۆرادا ۆلازا تمت ثیح، ۆرادەلا ۆهجاول IP ناونع مادختسال اھب صاخلا عمجملە عضولا.

لایبس ملائم:

- میں SNMPL میں
 - میں RADIUS میں داخل

دي دحت مدخلت سملأا ىلع بجي ، ئرادإلا ئكبس رباع ھيلإ لوصولنا نكمي يذلا DNS مداخل ماظنلا تادادعإ يف ."اضيأ ئرادإلا/اصي خشتلا ۋەھج او رباع حىررص لكشب DNS ثحب نيكىمت DNS و ICMP يف ثحبلا تايىلماعل ھنېيىعت متي ئانىتتساك DNS نىوكت < يساسألا تانايىبلالا ديدەتلار نع عافدىلا مدخلتىسى ، تالاحلا ھذه يفو: traceroute (ولاصتالا رابتخا) راسم ىلع روڭعالا مدع ۋەلاح يف يئاقلىت لكشب ئرادإلا ىلا دوعىي مىث

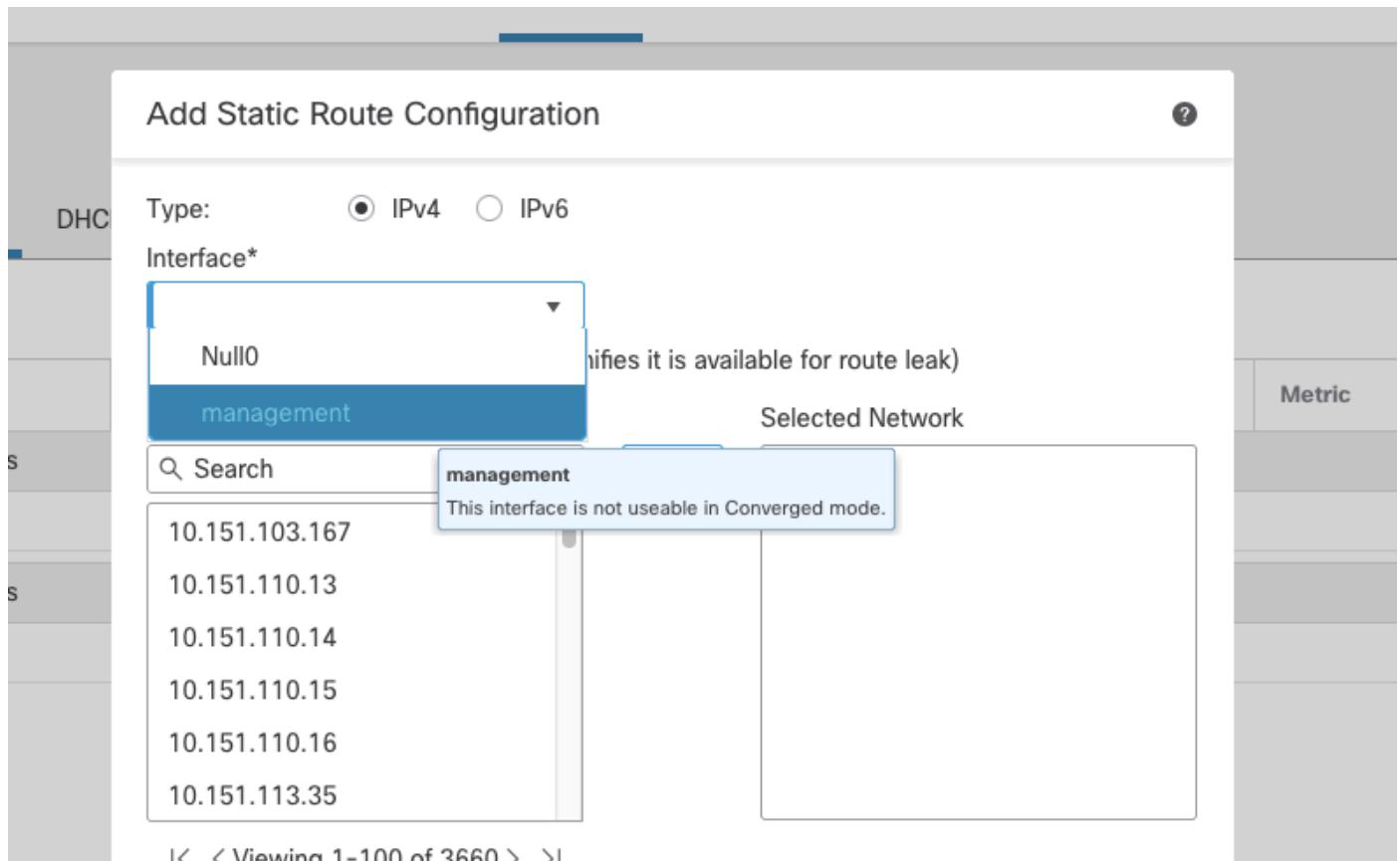
(CLI) رم اوأ رطس ڦهجاو لالخ نم طقف ڦرادإلا ڻهنجاول ٿتباثلا تاراس ملا مادختس! نيوكت نکمي ل FTD (Linux)

ڏڌو ۾ لى تاراطا إلٽا عي مج Lina ۽ رادا ڏف نمل يض ارت فا لاس ملا لسري Linux.

```
> configure network static-routes ipv4 add management ?
```

IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 destination address

دیدحتل لردادلا ڈھج او فینصت متی، مدخلت سم ڈھج او لع.



جمدل لامتكا دعب ةتباثلا تاراسملاء لع ديدحتل لردادلا ڈھج او رفوتت ال.

ڇھصلانم ڦققحتلا

ردادلا ڈھج او لع جمدلا دعب ڇعقولتملا تارييغتلما

- رمألا ذيفنت لالخ نم FTD ل (CLI) رمأولا رطس ڈھج او لع براقتلا عضونم ڦققحتلا

```
> show management-interface convergence  
management-interface convergence
```

- مسالا ، ڈھج اولا مسا رئييغت متی، مدخلت سم ڈھج او لع ردادلا ڈھج اولا يقطنم ملما.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	

يقطنملا مسالا او ٓرادلا ٗهجاو مسا ىلع جمدلا ديڪات

- ايئاقلت ٗديجل IP نيوانع نيوكت متي، لـ FTD (CLI) رم اوأ رطس ٗهجاو رطس ٗهجاو ىلع ٓرادلا ٗهجاول Lina ىلع ناونع و 203.0.113.130 يلخادلا صاخلا IPv4 ناونع نا: يلخاد ذيفنتك NAT مادختسا متي IPv6 fd00:0:1:1::2 (رييغتلل عضخي ام هالکو) ٗنيعملا كلت يه IPv4 و IPv6 نيowanع ىلى NATed يه هذه IPs نيowanع نا، ٗماماعلا سکونيل ٗاونب ٗصاخلا ٗجاح لـ Lina ىلع ٗماماعلا IP نيowanع ىلى ٗجاح كانه دعت مل كلذل.

IPv6 ناونع و (203.0.113.129) يلخاد IPv4 ناونع "ifconfig" ضرع ي، عاربخلا عضويف (fd00:0:1:1::1) ليغشتلا Linux.

FTD CLI Clish:

```
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
    Input flow control is unsupported, output flow control is unsupported
    MAC address 0050.56b3.f75d, MTU 1500
    IP address 203.0.113.130, subnet mask 255.255.255.248
```

Expert mode on Linux:

```
root@ftd01:/home/admin# ifconfig
...
tap5: flags=4419

      mtu 1500
      inet 203.0.113.129 netmask 255.255.255.248 broadcast 203.0.113.135
      inet6 fe80::8403:9ff:fe:6d16 prefixlen 64 scopeid 0x20

      inet6 fd00:0:1:1::1 prefixlen 123 scopeid 0x0
```

ةساردلا ةللاح - اححالص او عاطخألا فاشكتسأ

لصفنم IP نیوانع نیوکتب یرهاظ FTD یلع صیخشتلا ۰۵۰ج او تماق، ۰۵۰س اردا ۰للاح یف ۷.۴.۲. DNS نع ۰ثحب لاب ۰صاخلا ۰یجراخلا تامدخلاب لاصتالل ۰لیا ۰یقرتلابق.

يـفـ نـيـوـكـتـلـاـ اـهـ مـتـيـ يـتـلـاـ ةـقـيـرـطـلـاـ يـهـ ـهـذـهـ وـ،ـ بـرـاقـتـلـاـ رـفـوتـ مـزـلـيـ،ـ 7.4.2ـ يـلـاـ ةـيـقـرـتـلـاـ دـعـبـ دـعـبـ وـجـمـدـلـاـ لـبـقـ FMCـ وـ FTD~CLI~Lina~Linuxـ وـ

ةكرح مادختس اب رورملـا ةكرح ضرعـل FTD CLI Lina و Linux ىـلـع رورـم ةـكرـح طـاقـتـلـا اـضـيـأـ كـانـهـ.
ةـرـادـإـلـا ةـهـجـاـوـ مـادـخـتـسـ اـلـ ـةـقـطـنـمـلـا صـيـخـشـتـلـا ةـهـجـاـوـ.

براقت نیوکت لبوق

FMC مدختس، م ٥٥ جاونیوکت

Tac_test

Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP VTEP

All Interfaces Virtual Tunnels Sync Device Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical			192.168.40.74/255.255.255.0(Static)	Disabled	Global	
GigabitEthernet0/0		Physical				Disabled		
GigabitEthernet0/1		Physical				Disabled		
GigabitEthernet0/2		Physical				Disabled		

جـمـدـلـا لـبـقـ ةـيـصـيـخـشـتـلـا ةـهـجـاـولـا نـيـوـكـ

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices (which is highlighted with a blue underline), Objects, and Integration. To the right of the tabs are buttons for Deploy, Search, and Settings, along with the user name admin and the Cisco logo.

The main content area has a title **Tac_test** and a subtitle **Cisco Firepower Threat Defense for VMware**. Below the title are tabs for Device, Interfaces, Inline Sets, Routing (which is selected and highlighted in blue), DHCP, and VTEP.

A sidebar on the left is titled "Manage Virtual Routers". It contains a dropdown menu set to "Global" and a list of routing protocols: Virtual Router Properties, ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP (with sub-options for IPv4 and IPv6), and Static Route (which is currently selected).

The main pane displays a table titled "Manage Virtual Routers" with a "Add Route" button. The table columns are: Network, Interface, Leaked from Virtual Router, Gateway, Tunneled, Metric, and Tracked. There are two entries in the table:

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes	DNS	diagnostic	Global	192.168.40.254	false	1
▼ IPv6 Routes						

ةيصيخشتلا ٰهنجاولى ىلع هنـيوكـت مـت يـذـلـا تـبـاثـلـا رـاسـمـلـا

نيوكـت زـواـجـت DNS

بيـوـبـت ةـمـالـع مـث ،ـسـاسـأـلـا دـح ،ـسـاسـأـلـا مـاظـنـلـا تـادـادـعـا > ةـزـهـجـأ

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Firewall Management Center', 'Devices / Platform Settings Editor', 'Overview', 'Analysis', 'Policies', 'Devices' (which is underlined in blue), 'Objects', and 'Integration'. The main title is 'FQDN_Test_PlatformSettings' with a placeholder 'Enter Description'. On the left, a sidebar lists various settings: ARP Inspection, Banner, **DNS** (selected), External Authentication, Fragment Settings, HTTP Access, ICMP Access, NetFlow, SSH Access, SMTP Server, SNMP, SSL, Syslog, Timeouts, Time Synchronization, Time Zone, UCAPL/CC Compliance, and Performance Profile. The right panel is titled 'DNS Settings' and contains tabs for 'DNS Settings' (selected) and 'Trusted DNS Servers'. It includes a section for 'DNS Resolution Settings' with a note about specifying DNS servers and device interfaces. A toggle switch is set to 'Enable DNS name resolution by device'. Below this is a 'DNS Server Groups' section with an 'Add' button. A group named 'DNS_Server_Lab (Default)' is listed with the entry 'any'. There are edit and delete icons next to the group name. At the bottom, there are fields for 'Expiry Entry Timer' (set to 1) with a range of 1-65535 minutes, and 'Poll Timer' (set to 240) with a range of 1-65535 minutes.

يـسـاسـأـلـا مـاظـنـلـا تـادـادـعـا يـف نـيـوكـت

FQDN_Test_PlatformSettings

Enter Description

The screenshot shows the 'DNS' tab selected in a sidebar. On the right, there are two input fields: 'Poll Timer:' set to 240 with a range of 1-65535 minutes, and 'Interface Objects' which includes a search bar and two lists: 'Available Interface Objects' and 'Selected Interface Objects'. A checkbox at the bottom enables DNS lookup via the diagnostic/management interface.

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access
ICMP Access
NetFlow
SSH Access
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
Time Zone
UCAPL/CC Compliance
Performance Profile

Poll Timer: 240 Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects Selected Interface Objects

Search

Add

Enable DNS Lookup via diagnostic/Management interface also.

اضيأ ڦراداڻا/صيخشتل ڦهنج او ربع DNS ٺچب نيكمٿل رايٽخالا ۽ ناخ ديدھت مٿ

ربع ڦيسيخشتل ڦهنج اولانويڪت FTD LINA

```
interface Management0/0
management-only
nameif diagnostic
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.40.74 255.255.255.0
```

```
ftd01# sh ip
System IP Addresses:
Interface          Name          IP address      Subnet mask    Method
Management0/0       diagnostic   192.168.40.74 255.255.255.0  manual
Current IP Addresses:
Interface          Name          IP address      Subnet mask    Method
Management0/0       diagnostic   192.168.40.74 255.255.255.0  manual
```

```
ftd01# sh 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

```
S      10.10.10.10 255.255.255.255 [1/0] via 192.168.40.254, diagnostic  
C      192.168.40.0 255.255.255.0 is directly connected, diagnostic  
L      192.168.40.74 255.255.255.255 is directly connected, diagnostic
```

لینا FTD CLI DNS نیوکت

```
ftd01# sh run dns
dns domain-lookup diagnostic
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 diagnostic
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

مدخـلـةـةـهـجـتـمـلـاـ DNSـ 10.10.10.10ـ رـوـرـمـ ةـكـرـحـلـ ةـيـصـيـخـشـتـلـاـ ةـهـجـاـولـاـ ئـلـعـ طـاقـتـلـاـ

```
ftd01# sh cap
capture diag type raw-data trace detail interface diagnostic [Capturing - 340 bytes]
  match udp any host 10.10.10.10 eq domain
```

ftd01# sh cap diag

5 packets captured

```
1: 00:15:39.660442      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
2: 00:15:54.661953      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
3: 00:16:09.661739      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
4: 00:16:24.667674      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
5: 00:16:39.684946      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
```

5 packets shown

ftd01#

ةهجاو لىع DNS ثحب رورم ةكرحل حيحصل اقفلتلا ديكأتل، Linux، ريبخ عضو لىع طاقتلا اـ ئيسيخشتلا ئهنجاولن نم ئرادلا

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
```

HS_PACKET_BUFFER_SIZE is set to 4.

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
04:58:14.648941 IP 192.168.40.74.49171 > 10.10.10.10.domain: 5655+ AAAA? cisco.com. (27)
04:58:29.656317 IP 192.168.40.74.11606 > 10.10.10.10.domain: 26905+ A? cisco.com. (27)
04:58:44.686568 IP 192.168.40.74.11606 > 10.10.10.10.domain: 24324+ A? cisco.com. (27)
04:58:59.704586 IP 192.168.40.74.11606 > 10.10.10.10.domain: 35592+ A? cisco.com. (27)
04:59:14.742685 IP 192.168.40.74.11606 > 10.10.10.10.domain: 40993+ A? cisco.com. (27)
04:59:29.763690 IP 192.168.40.74.11606 > 10.10.10.10.domain: 62225+ A? cisco.com. (27)
04:59:44.796484 IP 192.168.40.74.11606 > 10.10.10.10.domain: 25350+ A? cisco.com. (27)
```

براقت نیوکت دعب

ةدوچوملا تانیوکتلار عیمج ۋەل ازا بجى، جمدىلا ئارجا لجأ نمف، براقتلار ئارجا ئەپەنەن، حضۇم وە امكىنلىكىنىڭ ئەچىشلى ئەجاؤلىع.

جمدىلا لامتكا درجمب FMC و FTD CLI بە صاخلا تامولۇملا يە هەذە.

مەختىسىم ئەجاؤر بىرەن ئەجاؤر ئەجاؤر ئەجاؤر FMC

تاهاجاولا بىيوبتلار ئەم الى ئەرشابىم ھەتھى مەتى FTD. دەخ، ئەزەجألا ئەرادا > ئەزەجألا.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	

جمدىلا دعب ئەرادالا ئەجاؤر

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Tac_test
Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

 IPv4

 IPv6

Static Route

✗ Multicast Routing

+ Add Route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
IPv6 Routes						

Save Cancel

م داخىل ا ئتاباڭ تاراسىم يأ فاصل مەتت مل DNS

يىسالا ماظنلا تادادعىلىع وە امك DNS نىوكتىقىبى نأ بجى.

بىوبت ئامالع مىث، ئاسىسلا ددح، يىسالا ماظنلا تادادعى > ئزەجأ

ئىكەن ئەتكەن، تباڭ راسىم ئافاصلانىلى ئەجاحلا نۇد ئەردىلا ئەجەۋىلى DNS ئىچب لاسرا ئەپباتىمىل
اددەم ئىقىبى نأ بجى." اضىيأ ئەردىلا/صىخشتىلا ئەجەۋىلى رېبىع DNS.



FQDN_Test_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

DNS Settings

Trusted DNS Servers

DNS Resolution Settings

Specify DNS servers group and device interfaces to reach them.

 Enable DNS name resolution by device

DNS Server Groups

Add

DNS_Server_lab (Default)

any



Expiry Entry Timer:

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

نیوکت DNS نیوکت ایل جعل ایڈادع ماظنل ایلا اس اس

FQDN_Test_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPI/CC Compliance

Performance Profile

Range: 1-65535 minutes

Poll Timer:

 Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Add

Selected Interface Objects

Enable DNS Lookup via diagnostic/Management interface also.

FTD J (CLI) رم اوّلا رطس ۃج او لع نیوک تلا

```
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
    Input flow control is unsupported, output flow control is unsupported
    MAC address 0050.56b3.f75d, MTU 1500
    IP address 203.0.113.130, subnet mask 255.255.255.248

> show interface ip brief
+-----+-----+-----+-----+-----+
| Interface | IP-Address | OK? | Method | Status | Protocol |
+-----+-----+-----+-----+-----+
| GigabitEthernet0/0 | unassigned | YES | unset | administratively down | up |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | up |
| GigabitEthernet0/2 | unassigned | YES | unset | administratively down | up |
| Internal-Control0/0 | 127.0.1.1 | YES | unset | up | up |
| Internal-Control0/1 | unassigned | YES | unset | up | up |
| Internal-Data0/0 | unassigned | YES | unset | down | up |
| Internal-Data0/0 | unassigned | YES | unset | up | up |
| Internal-Data0/1 | 169.254.1.1 | YES | unset | up | up |
| Internal-Data0/2 | unassigned | YES | unset | up | up |
| Management0/0 | 203.0.113.130 | YES | unset | up | up |
```

```
ftd01# sh 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
```

بناج ىلع DNS لـ FTD بـ نـيـوكـتـ

```
ftd01# sh run dns  
dns domain-lookup management  
DNS server-group DNS_Server_lab  
  retries 5  
  timeout 15  
  name-server 10.10.10.10 management  
  domain-name test.lab  
DNS server-group DefaultDNS  
dns-group DNS_Server_lab
```

ةـجـاـوـىـلـعـ رـوـرـمـ ةـكـرـحـلـ حـيـحـصـلـاـ قـفـدـلـاـ دـيـكـأـتـلـ رـيـبـخـ عـضـوـىـلـعـ طـقـتـلـاـ ةـرـادـإـلـاـ.

```
root@ftd01:/home/admin# tcpdump -i br1 port 53  
HS_PACKET_BUFFER_SIZE is set to 4.  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes  
20:20:33.623146 IP ftd01.60310 > 10.10.10.10.domain: 61954+ A? cisco.com. (27)  
20:20:33.623533 IP ftd01.33417 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)  
20:20:48.660172 IP ftd01.60310 > 10.10.10.10.domain: 41252+ A? cisco.com. (27)  
20:20:52.638426 IP ftd01.39304 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)  
20:21:09.669133 IP ftd01.47150 > umbrella.domain: 39343+ AAAA? ftd01. (23)  
20:21:09.669305 IP ftd01.50173 > umbrella.domain: 57694+ AAAA? ftd01. (23)  
20:21:11.659352 IP ftd01.48092 > umbrella.domain: 46478+ PTR? opendns.in-addr.arpa. (45)  
20:21:14.673992 IP ftd01.58547 > umbrella.domain: 57694+ AAAA? ftd01. (23)  
20:21:18.673371 IP ftd01.47607 > umbrella.domain: 39343+ AAAA? ftd01. (23)  
20:21:18.695507 IP ftd01.60310 > 10.10.10.10.domain: 29973+ A? cisco.com. (27)
```

راسـمـ ةـفـاضـاـ مـتـتـ مـلـ اـذـاـ يـفـ رـمـتـسـيـ شـحـبـ نـأـ نـمـ دـكـأـتـلـاـ نـكـمـيـ ،ـلـيـلـدـلـاـ اـذـهـ عـمـ رـبـعـ ةـرـادـإـلـاـ ةـجـاـوـىـلـعـ تـبـاـثـ

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).