

FMC في صيخشتلاو ةرادال ةهجاو جم د نيوكت

تايوت حمل

[ةمدقم](#)

[ةيساس الابل طتم](#)

[ةيساس ا تامول عم](#)

[ةمدختسم ل تانوكم](#)

[نيوكت](#)

[فيلخادل FTD في نبل طي طيخت ل م س ر](#)

[ب ر ا ق ت ل ا ع ا ر ج](#)

[ق ح ص ل ا ن م ق ق ح ت ل ا](#)

[ق س ا ر د ل ا ق ل ا ح - ا ه ا ل ص ا و ا ط ا ل ا ف ا ش ك ت س ا](#)

[ب ر ا ق ت ن ي و ك ت ل ب ق](#)

[ب ر ا ق ت ن ي و ك ت د ع ب](#)

ةمدقم

يتل ةزيم ل ، صيخشتلاو ةرادال تاهجاو جم د نيوكت ل ةمزالا تاوطخل دنتسم ل اذه فصي FTD 7.4.0 رادصل ي ف اهتفاضل تمت

ةيساس الابل طتم

ةيلاتل عيضاوم ل ا ب ةفرعم كيدل نوكت ن ا ب Cisco ي صوت

- Cisco ن م (FTD) ةيامحل راج ديهت ن م آل عافدل
- Cisco ن م (FMC) ن م آل ةيامحل راج ريدم زكرم

ةيساس ا تامول عم

ةهجاو ل ني ب ةيدام ل ةرادال ةهجاو ةكراشم مت ، ةقباس ل تارادصل او 7.3 رادصل ي ف (Linux) ةرادال ةي قطنم ل ةهجاو ل او (LINA) صيخشتل ةي قطنم ل

ةبرجت طي سبتل ةرادال عم صيخشتلا ةهجاو جم د متي ، ثدحل تارادصل او 7.4 رادصل ي ف م دختسم ل

م ادختس ل كنكمي ال ، ثدحل تارادصل او 7.4 رادصل م دختست يتل ةديجل ةزهجل ةبسن ل ا ب . طقف ةجمدم ل ةرادال ةهجاو رفوت . ةميدق ل صيخشتلا ةهجاو

ةمدختسم ل تانوكم

ةيلاتل ةيدام ل تانوكم ل ا و جم اربل تارادصل ل دنتسم ل اذه ي ف ةدراول تامول عم ل دنتست

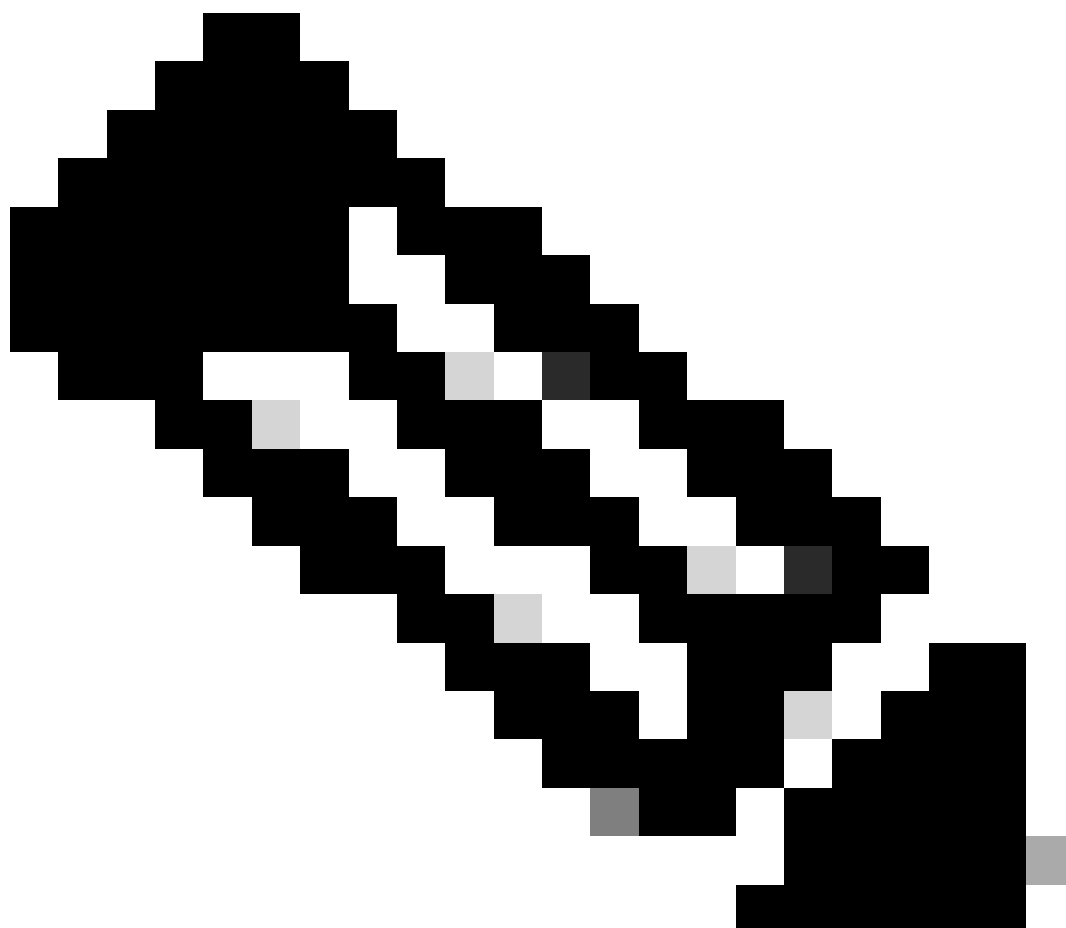
- Cisco Virtual Secure Firewall Threat Defense (FTD)، رادصلال 7.4.2
- Cisco، رادصلال 7.4.2 نم يره اظلال (FMC) نم آلال ةي امحل رادج ريدم زكرم

ةصاخ ةي لمعم ةئي ب ي ف ةدوچومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل ءاشنإ م ت ت ناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال ةي مچ ت ادب رملأ يال لمحتحمل ري ثاتلل كمهف نم دكأتف ،ليغشتل دي ق ك تكبش

نيوكتل

كيدلف ،صيخشتل ةهجال نيوكت كيدل ناك و ،ثدحأ رادصلأ وأ 7.4 ىلا ةي قرتلاب تمق اذا .ةلصفنمل صيخشتل ةهجاو مادختسإ ي ف رارمتسالال كنكمي وأ ،ايودي تاهجال جمدل رايلال

ايئاقلت تاهجال جمد م تي ،صيخشتل ةهجال نيوكت يأ دوچو مدع ةلاح ي ف

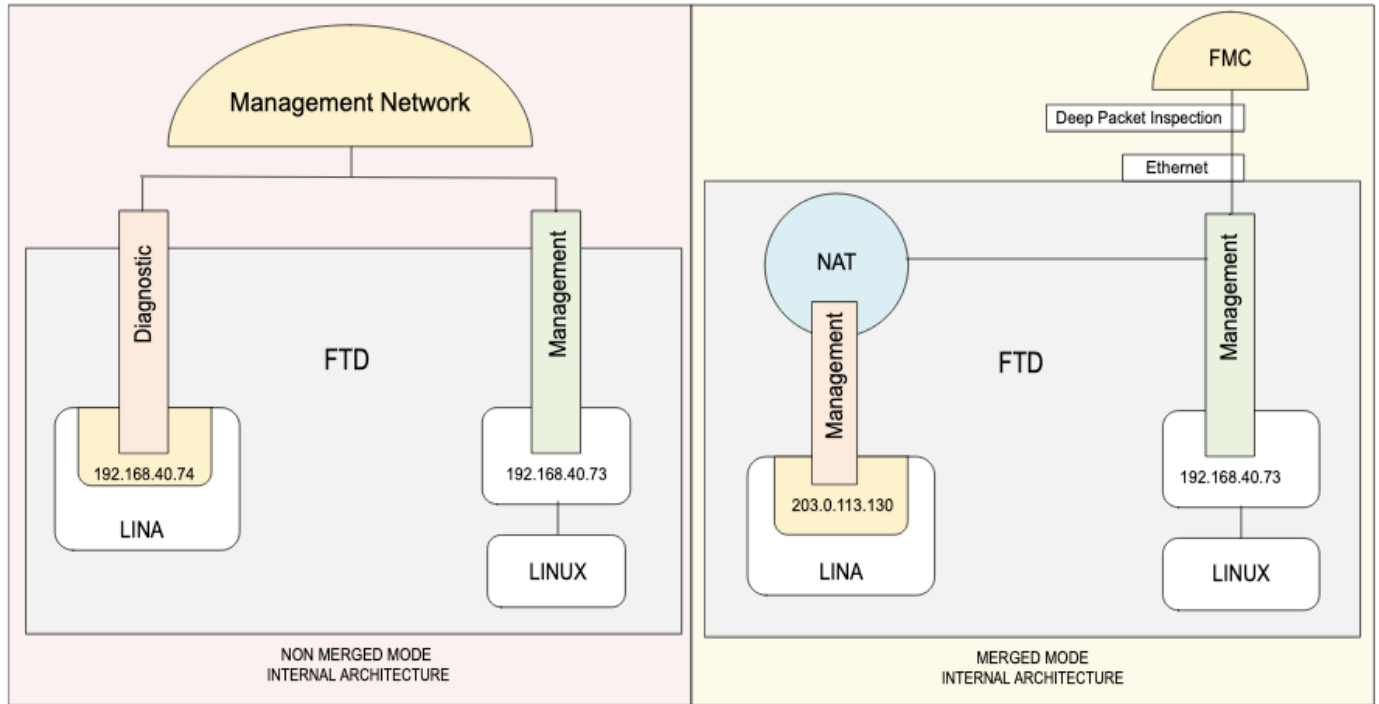


طي طختلاب مق ،كلذل ،قحال رادصلأ ي ف صيخشتل ةهجاو معد ةلازا م متتس :ةطحال م

نكمم تقو برقأ يف تاهجاولا جمدل

ةيلخادلا FTD ةينبل يطيختالتا مسرلا

ةعجملا ةرادإلا ةهجاو ىلع ةماع ةرطن



اهدعبو براقالتا ةرادإ ةهجاو لبق ةيلخادلا ةينبل ىلع ةماع ةرطن

ةيقتنملا ةهجاو (Lina) ةيصيخشالتا ةيقتنملا ةهجاو ةيلخادلا ةينبل، راسيلا ىلع ةقباستلا تارادصلا او 7. 3 رادصلا (Linux). ةرادإلا

ةمدخ ةرادإلا ةكبش ىلإ Lina لوصو مدختسي. ةدحاو ةرادإ ةهجاو ةيلخادلا ةينبل، نيميلا ىلع NAT.

براقالتا ءارجإ

ايقئقلت تاهجاو جمد متي ال، صيخشالتا ةهجاو يف نيوكتلا اهي ف دجوي يتلا ةلاحلا يف براقالتا ءارجإ ذيفنت كيلىل بجيو، ةيقرتلا دعب

نيوكتلا حالصا، تالاحلا ضعب يفو، نيوكتلا تاريغيغت ب رارقإلا كنم ءارجإلا اذه بلطتي ايودي.

رطس ةهجاو يف show management-interface converge رمالا لخدأ، زاهجلل يلاحلا عضولا ضرعل FTD ل (رماوأل رطس ةهجاو) CLI رماوأل

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

ةجدم ريغ ةرادإلا تاهجاو نأ ةجيتنللا هذه حضوت

1. ةوطخل

م تي .هريحت دارمل FTD دحو ،ةزهجالا ةرادإ > ةزهجالا ىلإ لقتنا ،FMC مدختسم ةهجاو ىل ع .تاهجاوالبىوبتللةمالع ىلإ ةرشابم هحتف

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration Deploy

Tac_test
Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP VTEP

Management interface action needed.
Merge the Management and Diagnostic interfaces on the Management Interface Merge dialog box, or merge them later by clicking the >+ icon for Diagnostic interface in the table below.
Merging the interface will cause some downtime. [Learn more](#)

All Interfaces Virtual Tunnels

Search by name 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(Stat...	Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	

7.4.2 جمانربل رادصا ىلإ زاهجال ةيقرت دعب ةرادإلاو صيخشتللةهجاو جمدل بولطملا ءارجالا

2. ةوطخل

صيخشتللةهجاو يوتحت الأ يروضال نم .صيخشتللةهجاو ىل ع نيوكتلل عي مج ةلازاب مق .جمدللةعباتمل نيوكتللأ ىل ع

.تباثللهجوملاو IP ناو نع :كانه ،هذه صيخشتللةهجاو في ،لاثللليبس ىل ع

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration Deploy

Tac_test
Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP VTEP

Management interface action needed.
Merge the Management and Diagnostic interfaces on the Management Interface Merge dialog box, or merge them later by clicking the >+ icon for Diagnostic interface in the table below.
Merging the interface will cause some downtime. [Learn more](#)

All Interfaces Virtual Tunnels

Search by name Sync Device Add Interfaces

Interface

Diagnostic0/0

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/2

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
192.168.40.74/255.255.255.0
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Cancel OK

ةيصوصيخشتللةهجاو لل IP ناو نع ةلازنا

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							
DNS	diagnostic	Global	192.168.40.254	false	1		✎ 🗑
▼ IPv6 Routes							

صيخشتلا ةهجاو ىلع تباثلا راسملا نيوكت

3. ةوطخل

ريحتلا ةنوقيأل ةرواجملا جمدلا ةنوقيأ وأ ةبولطملا ةرادإلا ةهجاو جمد ءارجإ ةقطنم قوف رقنا صيخشتلا ةهجاو ىلع (صاصرلا 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 action needed.
Merge the Management and Diagnostic interfaces on the Management Interface. Merging the interface will cause some downtime. [Learn more](#)

All Interfaces Virtual Tunnels

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

Management Interface Merge ⓘ

- 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.

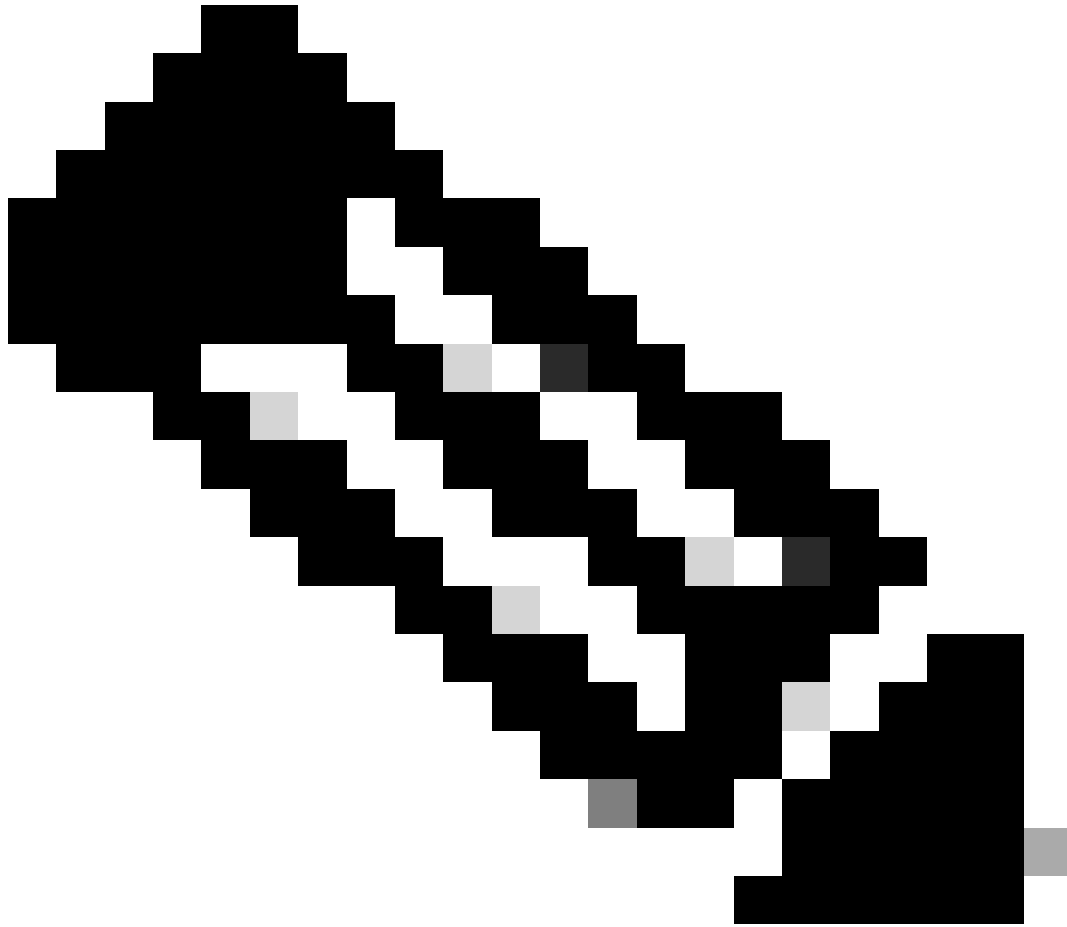
In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address.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

Proceed Cancel

Sync Device Add Interfaces ▾

Path Monitoring	Virtual Router	
Disabled	Global	✎ ➡
Disabled		✎
Disabled		✎
Disabled		✎

ةعباتملا لبق ةرادإلا ةهجاو جمد تامولعم



ىلع ةمهمل هذه ذيفنتب مق ،رفوتلا ةيلع تاعومجمل او جاوزألل ةبسنلاب :ةطحال م
ايئاقلت الاثامتم اخسن جمدمل نيوكتلا خسن متي .مكحتلا ةدحو/ةطشنلا ةدحول
ت.انايبل/دادعتسال تادحو ىلإ

-
- ريذحت ةنوقي رهظت نا نكمي ،ةيودي ةلازا وأ رييغت نوئي نا بلطتي راركتي أل

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

 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

جمدال لب ق هتلازا بولطم التانيوكتال لوح ريذحتال لاثم

دعأ م ث ، نيوكتال ةداعإ وأ نيوكتال ةلازا عبات م ث ، راوخال ع برم ءاغلب مق :لاخال وه اذه ناك اذا
"ةرادإلا ةهجاوخم د" راوخال ع برم حتف

- ريذحت زمرب زاخال ىلع لمعت يتل يساسألماظنل تادادعإ ىلع ةمالع عضو متي
اراعشإ بلطتو

Management Interface Merge

? x

- 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

اهري رحت بجي يتل يساس ال ماظننل تادادع| تانيوكت نم ريذحتل يل لاثم

• ةعباتم قوف رقنا م ث ،دومع ؟رييغتلاب فترعت له في عب رمل رقنا

4. ةوطخل

حاجن راعش ضرع متي ،نيوكتل جمد دب
رشنلل زهاج وهو ةرادال ةهجاو جمد ظفح مت

ةهجاو نيوكت ةداع| بجي ؛جمدلاب ةقلعتمل نيوكتل تاريغت نع عجارتل كنكمي ال هنا طحال

ايودي ةلصلال يذ نيوكتلالو صيخشتلال.

ديدلال جمدملال نيوكتلال رشنل مق.

رشنلل ازهاج حبصأو ةرادلال ةهجاو جمد ظفح مت

طقف ةعارقلل اهنأ نم مغرلاب ،تاهجاوالا ةحفص ىل ةرادلال ةهجاو رهظت

ل.مكتك دق ةرادلال ةهجاو ىل ع براقتلال عارج نوكتي ،رشنلل دعب

يرايتخا 5. ةوطخلال

نيوكتلال ريغت ىل ةجاحب تنأف ،صيخشتلال ةهجاوب تلصتا ةيجراخ تامدخ يأ كي دل ناك اذا ىل ع يطايتحالال راسملا ةرادلا ةلازا تمت شيح ،ةرادلال ةهجاوول IP ناونع مادختسال اهب صاخلا ع.مجمملال عضولال

لالاملل لىبس ىل ع:

- SNMP لىمع
- RADIUS مداخ
- ديدحت مدختسملا ىل ع بجي ،ةرادلال ةكبش ربع هيلل لوصولو نكمي يذل DNS مداخ ماطنللا تاداعل ي ف "اضيا ةرادلال/صيخشتلال ةهجاو ربع حيرص لكشب DNS ثحب نيكتمت ICMP و DNS ي ف ثحبلا تايلمعل هنييعت متي ءانثتساك DNS نيوكت > يساسألانايبلل ديدعتلل نع عافدل مدختسي ،تالاحال هذه ي فو (tracert و لاصلتال رابتخا) راسم ىل ع روثعلال مدع ةلاح ي ف يئاقلت لكشب ةرادلال ىل ع دوعي م

(CLI) رماوأ رطس ةهجاو لال خ نم طقف ةرادلال ةهجاوول ةتباثلل تاراسملا مادختسال نيوكت نكمي ل FTD (Linux)

Linux. ةدحو ىل ةاراطلال عي مج Lina ةرادلا ذفنمل يضا رتفالال راسملا لسري

```
> configure network static-routes ipv4 add management ?
IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 destination address
```

دي دحتلل ةرادال ةهجاو في نصت متي، FMC مدختسم ةهجاو ىلع

Add Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*

Null0 (indicates it is available for route leak)

management

Selected Network

Metric

Search

management
This interface is not useable in Converged mode.

10.151.103.167

10.151.110.13

10.151.110.14

10.151.110.15

10.151.110.16

10.151.113.35

< Viewing 1-100 of 3660 >

جمدل لامتك دعب ةتباتل تاراسملا ىلع دي دحتلل ةرادال ةهجاو رفوتت ال

ةحصل نم ققحتلا

ةرادال ةهجاو ىلع جمدل دعب ةعقوتملا تاريغيغتلا

- رمال ذيفنت لالخ نم FTD ل (CLI) رماوالا رطس ةهجاو ىلع براققتلا عضو نم ققحتلا

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

- مسالا، Management0/0 ىل ةهجاوالمسا ريغيغت متي، FMC مدختسم ةهجاو ىلع ةرادال ىل يقطنملا

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin ▾

Tac_test Cisco Firepower Threat Defense for VMware

Device Interfaces **Inline Sets** Routing DHCP VTEP

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces ▼

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		✎

يقتطعن المراسل او قرا دل ا ه ا و م س ا ل ع ج م د ل ا ك ا ت

- ايقا ل ت ا د ل ا ل IP ن و ا ن ع ن و ك ت م ت ي ، FTD ل (CLI) ر م ا و ا ر ط س ا ه ا و م س ا ل ع ل ع ا ه ا و ل Lina ل ع ا و ن ع و 203.0.113.130 ل ا ل ا ص ا خ ا ل IPv4 ا و ن ع ن ا : ل ا ل ا د ذ ي ف ن ت ك NAT م ا د خ ت س ا م ت ي (ر ي غ ت ل ل ع ض خ ي ا م ه ا ل ك و) ا ن ع م ل ا ك ل ت ي ه fd00:0:1:1::2 IPv6 ا م ا ل س ك و ن ي ل ا و ا ن ب ا ص ا خ ا ل IPv6 و IPv4 ن و ا ن ع ل ا NATed ي ه ه ذ ه IPs ن و ا ن ع ن ا ، Lina ل ع ا م ا ل IP ن و ا ن ع ل ا ا ج ا ح ك ا ن ه د ع ت م ل ك ل ذ ل

IPv6 ا و ن ع و (203.0.113.129) ل ا ل ا د IPv4 ا و ن ع "ifconfig" ض ر ع ي ، ا ر ب خ ا ل ع ض و ي ف Linux ل ي غ ش ت ل م ا ط ن ل (fd00:0:1:1::1)

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:febf:6d16 prefixlen 64 scopeid 0x20

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

تساردل ةلاح - اهحالصاوا عا طخال افاشكتسا

ةلصفنم IP ننيوانع نيوكتب يرهاظ FTD ىلع صيخشتل ةهجاو تماق ،هذه ةساردل ةلاح ي 7.4.2 ىل ةيقرتل لباق ،DNS نع ثحبلاب ةصاخلا ةيجراخلا تامدخال لاصتال

ي ف نيوكتل اهب متي يتل ةقيرطال يه هذو ،بقاتل رفوت مزلي ،7.4.2 ىل ةيقرتل دعب هذو بوجمدل لباق Linux و FTD CLI Lina و FMC مدختسم ةهجاو

ةكرح مادختساب رورملا ةكرح ضرعل Linux و FTD CLI Lina ىلع رورم ةكرح طاقتل اضيأ كانه ةرادلا ةهجاو مادختسال ةيقتنملا صيخشتل ةهجاو

بقات نيوكتل لباق

لمعت ةقيرطال هذو ،DNS نع ثحبلل تباث راسمولصفنم IP ىلع صيخشتل ةهجاو يوتحت ف FTD ىل Linux و Lina نم ةيقتنملا تاهجاوالا لك مادختساب

FMC مدختسم ةهجاو نيوكتل

Firewall Management Center
Devices / Secure Firewall Interfaces

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 10 ⚙️ ⓘ admin ▾ Cisco **SECURE**

Tac_test

Cisco Firepower Threat Defense for VMware

DeviceInterfacesInline SetsRoutingDHCPVTEP

All InterfacesVirtual Tunnels

🔍 Search by name 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		✎

جمدل لباق ةيصوصخشتل ةهجاوالا نيوكتل

Firewall Management Center
Devices / Secure Firewall Routing

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 10 ⚙️ ⓘ admin ▾ Cisco **SECURE**

Tac_test

Cisco Firepower Threat Defense for VMware

DeviceInterfacesInline SetsRoutingDHCPVTEP

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							
DNS	diagnostic	Global	192.168.40.254	false	1		✎ 🗑
IPv6 Routes							

ةيصيخششتلا ةهجاولا ىلع هنيوكت مت يذلا تباثلا راسملا

DNS نيوكت زواجت

DNS بيوبت ةمالع م ث ،ةسايسلا دح ،يساسألا ماظنلا تادادع| > ةزهجأ

Firewall Management Center

Devices / Platform Settings Editor

Overview

Analysis

Policies

Devices

Objects

Integration

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

DNS_Server_lab (Default)

any

Expiry Entry Timer:

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

يساسألا ماظنلا تادادع| ي DNS نيوكت

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

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

Interface Objects

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

Available Interface Objects

Q Search

Selected Interface Objects

Add



Enable DNS Lookup via diagnostic/Management interface also.

اضيف ايراد ال/صيغش التلة هج او ربع DNS شح ب نيكم تل رايتخاله اناخ دي دحت مت

FTD LINA ربع فيصيغش التلة هج اول نيوكت

```
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
```

FTD CLI Lina ىلع DNS نيوكت

```
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
```

DNS 10.10.10.10 مداخل ىلإ ةهجتالم DNS رورم ةكرحل ةيصيخششتلا ةهجاو لا ىلع طاقوتلا

```
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 ىلع DNS شحب رورم ةكرحل حيحصلا قفدتلا ديكأتل Linux، ريبخ عضو ىلع طاقوتلالا ةيصيخششتلا ةهجاو لا نم ةراداللا

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

```
04:59:44.796484 IP 192.168.40.74.11606 > 10.10.10.10.domain: 25350+ A? cisco.com. (27)
```

جمدلا دعب قرادال ا هجاو

Firewall Management Center

Devices / Secure Firewall Routing

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Tac_test

Save

Cancel

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						

DNS مداخل ىل ىتبات تاراسم ىأ ةفاضل مت مل

ىساسأل ماظنل تادادل ىل وه امك DNS نىوكت ىقبى نأ بجى

DNS بىوبت ةمالع م ث ، ةساىسل دح ، ىساسأل ماظنل تادادل > ةزءأ

شحب نىكمت " ، تبات راسم ةفاضل ىل ةءال نود ةرادل ةءاو ىل DNS شحب لاسرا ةعبات مل ادح ىقبى نأ بجى " .اضىأ ةرادل/صىخشتل ةءاو ربع 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

يُستَخدَم DNS لـ تَدارُجِ المَظانِلِ

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

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

Interface Objects

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

Available Interface Objects

Search

Selected Interface Objects

Add



Enable DNS Lookup via diagnostic/Management interface also.

هسفن وه ةرادال/صخششلتل ةهجاو ربع DNS ثحب نينمكمت رايخ لظي نأ بجي امك

FTD ل (CLI) رماوالا رطس ةهجاو ىلع نيوكتلا

```
> 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

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

LINA بىناچىلىق FTD لى CLI لى DNS نىيوكىت

```
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
```

ههجاو ىلع DNS شحب رورم ةكرحل حيحصلا قفدتلا ديكأتلا ،Linux ريبخ عضو ىلع طقتلا ةرادإلا.

```

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)

```

راسم ةفاضل مت مل اذا ىتح لمعلل في رمتسي DNS ثحب أن نم دكأتل نكمي ،ليلدل اذه عم Linux ربة ةرادال ةهجاو ىلع تباث

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 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