

De samenvoeging van beheer- en diagnostische interface in VCC configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Achtergrondinformatie](#)

[Gebruikte componenten](#)

[Configureren](#)

[FTD - Intern architectuurdiagram](#)

[Convergentieprocedure](#)

[Verifiëren](#)

[Probleemoplossing - Study Case](#)

[Vóór convergentieconfiguratie](#)

[Na convergentieconfiguratie](#)

Inleiding

Dit document beschrijft de stappen voor het configureren van het samenvoegen van de beheer- en diagnostische interfaces, onderdeel toegevoegd in FTD 7.4.0 versie release.

Voorwaarden

Cisco raadt u aan kennis te hebben over deze onderwerpen:

- Cisco Secure Firewall Threat Defence (FTD)
- Cisco Secure Firewall Manager Center (FMC)

Achtergrondinformatie

In versie 7.3 en eerder wordt de fysieke beheerinterface gedeeld tussen de diagnostische logische interface (Lina) en de beheerlogische interface (Linux).

In versie 7.4 en hoger wordt de diagnostische interface samengevoegd met Management voor een vereenvoudigde gebruikerservaring.

Voor nieuwe apparaten die 7.4 en hoger gebruiken, kunt u de oude diagnostische interface niet gebruiken. Alleen de samengevoegde beheerinterface is beschikbaar.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Virtual Cisco Secure Firewall Threat Defence (FTD), versie 7.4.2
- Virtual Cisco Secure Firewall Manager Center (FMC), versie 7.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Als u een upgrade hebt uitgevoerd naar 7.4 of hoger, en u hebt configuratie voor de diagnostische interface, dan hebt u de keuze om de interfaces handmatig samen te voegen, of u kunt doorgaan met het gebruik van de afzonderlijke diagnostische interface.

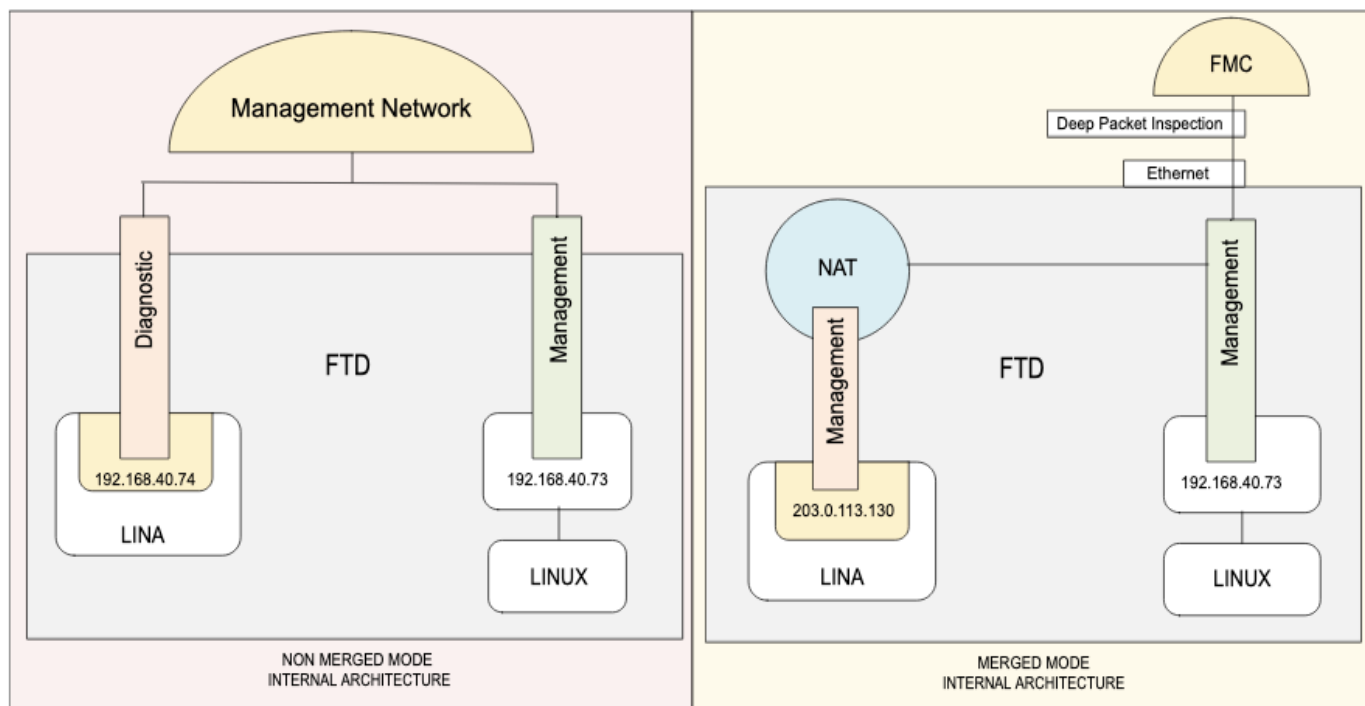
Mocht u geen configuratie hebben voor de diagnostische interface, dan worden de interfaces automatisch samengevoegd.



Opmerking: Ondersteuning voor de diagnostische interface moet worden verwijderd in een latere release, daarom, plan om de interfaces zo snel mogelijk samen te voegen.

FTD - Intern architectuurdiagram

Converged Management Interface - Overzicht



Overzicht van de interne architectuur voor en na de convergentiebeheerinterface

Links de interne architectuur voor de diagnostische logische interface (Lina) en de beheerlogische interface (Linux). Versie 7.3 en hoger.

Rechts de interne architectuur voor één beheerinterface. Lina-toegang tot het beheernetwerk maakt gebruik van de NAT-service.

Convergentieprocedure

In het geval waar de configuratie in de Kenmerkende interface bestaat, worden de interfaces niet automatisch samengevoegd na een verbetering, en u moet de convergentieprocedure uitvoeren.

Deze procedure vereist dat u wijzigingen in de configuratie bevestigt en in sommige gevallen de configuratie handmatig repareert.

Om de huidige modus van het apparaat te bekijken, voert u de opdracht `show management-interface converge` in bij de FTD CLI Clish

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

Dat resultaat laat zien dat de Management interfaces niet worden samengevoegd.

Stap 1.

Ga in de FMC UI naar Apparaten > Apparaatbeheer en selecteer de FTD die moet worden bewerkt. Het wordt rechtstreeks geopend in het tabblad Interfaces.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 10 ⚙️ ? admin ✓

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		✎

Noodzakelijke actie om de interface voor diagnostiek en beheer samen te voegen na het upgraden van het apparaat naar softwareversie 7.4.2

Stap 2.

Verwijder alle configuratie op de diagnostische interface. Het is verplicht dat de Diagnostische interface geen configuratie heeft om door te gaan met de samenvoeging.

In deze diagnostische interface is er bijvoorbeeld: IP-adres en statische route.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 10 ⚙️ ? admin ✓

Tac_test

Cisco Firepower Threat Defense for VM

Device Interfaces **Inline Sets** Routing DHCP VTEP

Management Interface action

Merge the Management and Diagnostic

Merging the interface will cause some d

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		✎

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

IP-adres van diagnostische interface verwijderen

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin ▾

Tac_test Save Cancel

Cisco Firepower Threat Defense for VMware

Device Interfaces **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

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

+ Add Route

Statische routeconfiguratie op diagnostische interface

Stap 3.

Klik op de actie samenvoegen van de beheerinterface nodig gebied of het pictogram samenvoegen naast het pictogram Bewerken (potlood) op de diagnostische interface.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin ▾

Tac_test Save Cancel

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 ▾

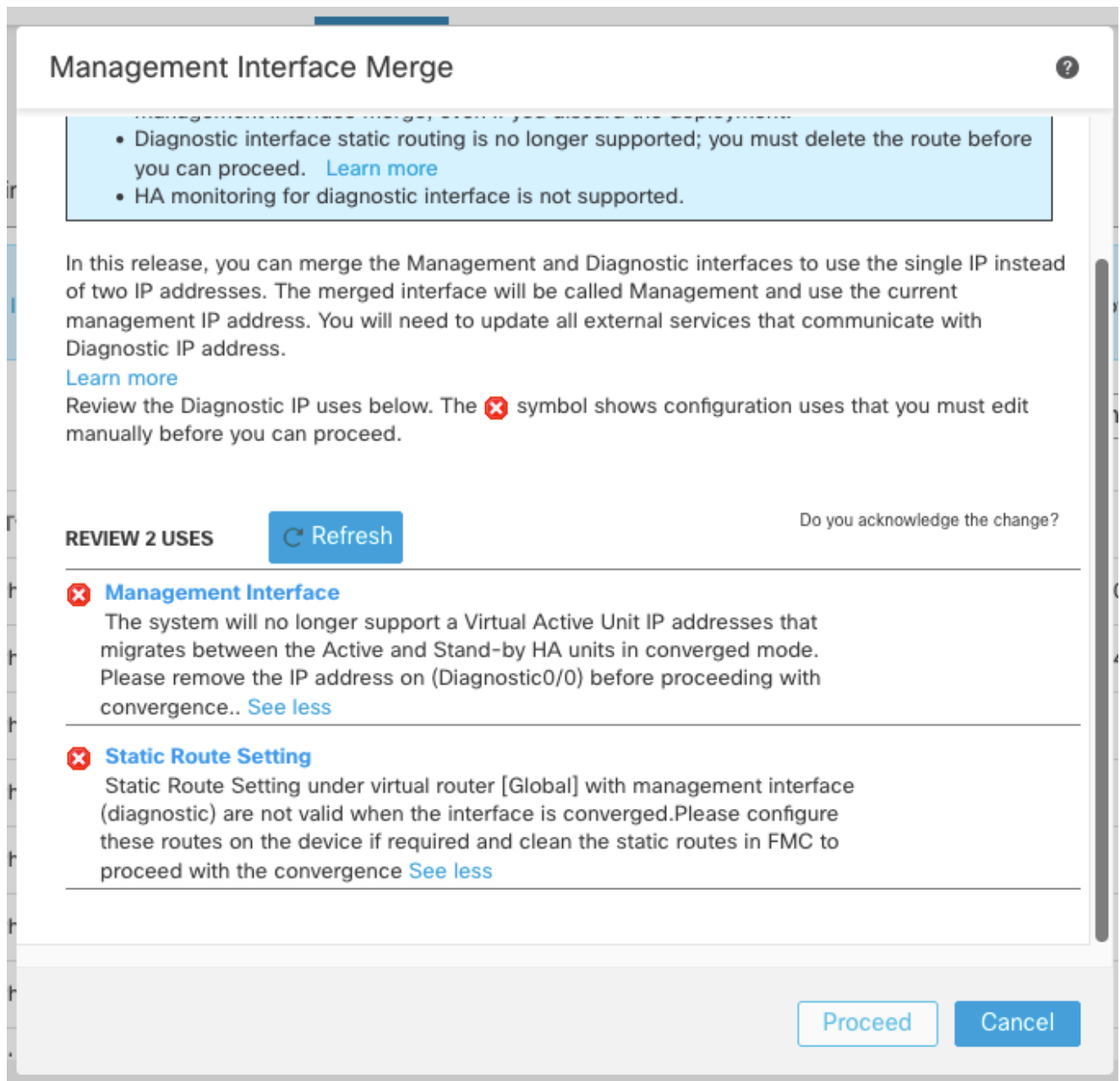
Path Monitoring	Virtual Router	
Disabled	Global	
Disabled		
Disabled		
Disabled		

Informatie over samenvoegen van beheerinterface voordat u verdergaat



Opmerking: Voor paren en clusters met hoge beschikbaarheid voert u deze taak uit op de active/control-unit. De samengevoegde configuratie wordt automatisch gerepliceerd naar de stand-by/data-eenheden.

-
- Voor elk exemplaar dat handmatig moet worden gewijzigd of verwijderd, kan een waarschuwpictogram worden weergegeven.



Voorbeeld van waarschuwing over configuraties moesten worden verwijderd vóór samenvoeging

Indien dit het geval is: Annuleert het dialoogvenster, gaat u verder met het verwijderen van de configuratie of herconfiguratie en opent u vervolgens het dialoogvenster Samenvoegen van beheerinterface.

- Platform-instellingen die op het apparaat gaan werken worden gemarkeerd met een waarschuwingspictogram en vereisen een bevestiging.

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

Voorbeeld van waarschuwing van platforminstellingen die moeten worden bewerkt

- Klik op het vak in Bevestig je de wijziging? kolom, en klik vervolgens op Doorgaan.

Stap 4.

Nadat de configuratie is samengevoegd, wordt een succesbanner weergegeven:

"De samenvoeging van de beheerinterface is opgeslagen en is klaar om te worden geïmplementeerd."

Merk op dat u de configuratieveranderingen met betrekking tot fusie niet kunt ongedaan maken; u moet de diagnostische interface en de bijbehorende configuratie handmatig opnieuw configureren."

Stel de nieuwe samengevoegde configuratie op.

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

Save Cancel

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 ▼

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	

De samenvoeging van de beheerinterface wordt opgeslagen en kan worden geïmplementeerd

De beheerinterface wordt op de pagina Interfaces weergegeven, hoewel deze alleen-lezen is.

Na de implementatie is de convergentieprocedure voor de Management-interface voltooid.

Stap 5. Optioneel

Als u externe services had die communiceerden met de diagnostische interface, moet u hun configuratie wijzigen om het IP-adres van de beheerinterface te gebruiken, aangezien de Management Route fallback is verwijderd in de geconvergeerde modus.

Voorbeeld:

- SNMP-client
- RADIUS-server
- DNS-server bereikbaar te zijn via het beheernetwerk, moet de gebruiker expliciet "DNS-raadpleging via diagnostische/beheerinterface inschakelen" selecteren. Op Platform Instellingen > DNS configuratie als uitzondering is ingesteld voor DNS lookups en ICMP (ping en traceroute): in deze gevallen gebruikt de bedreigingsverdediging gegevens en valt dan automatisch terug naar het beheer als een route niet wordt gevonden.

Het gebruik van statische routes voor beheerinterface kan alleen worden geconfigureerd via de FTD CLI Clish (Linux)

Lina management poort standaard route stuurt alle frames naar de Linux module.

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

Op de FMC UI wordt de beheerinterface grijs weergegeven voor selectie.

Add Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*

Null0 (indicates it is available for route leak)

management

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

Selected Network

Metric

Viewing 1-100 of 3660

De beheerinterface is niet beschikbaar voor selectie op statische routes nadat de fusie volledig is.

Verifiëren

Verwachte wijzigingen na samenvoeging op de beheerinterface

- Controleer de convergentiemodus op FTD CLI Clish door de opdracht uit te voeren

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

- Op FMC UI wordt de interfacenaam gewijzigd in Management0/0 , Logische naam voor beheer.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin ▾ **SECURE**

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		✎

Bevestiging samenvoegen op naam van beheerinterface en logische naam

- Op FTD CLI Clish, worden de nieuwe IP adressen automatisch gevormd op Lina voor de interface van het Beheer.
NAT wordt gebruikt als interne implementatie: Het interne privé IPv4-adres 203.0.113.130 en IPv6-adres fd00:0:1:1:2 zijn de toegewezen adressen (beide kunnen worden gewijzigd).
Deze IP's zijn NATed naar de openbare Linux Kernel FTD IPv4- en IPv6-adressen, daarom is er geen behoefte meer aan openbare IP's op Lina.

In de expertmodus geeft "ifconfig" het interne IPv4 (203.0.113.129) en IPv6 (fd00:0:1:1:1) adres voor Linux weer.

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:fefb:6d16 prefixlen 64 scopeid 0x20

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

Probleemoplossing - Study Case

In dit studiegeval heeft de diagnostische interface op een virtuele FTD een afzonderlijk IP-adres geconfigureerd voor connectiviteit met externe services van DNS Lookup, vóór de upgrade naar 7.4.2.

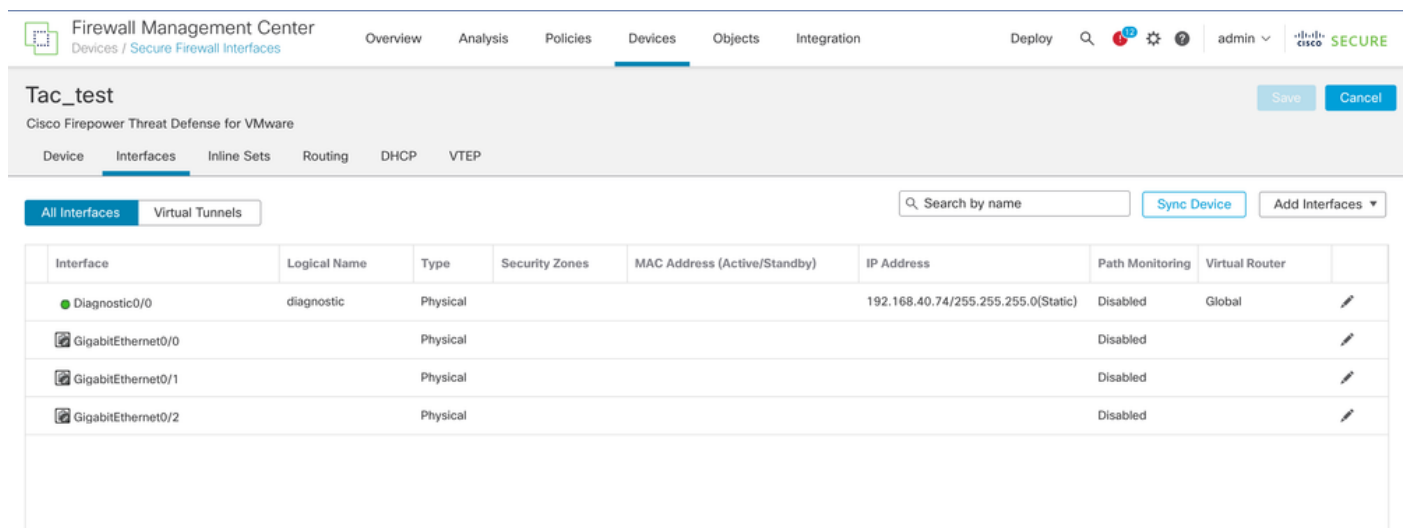
Na de upgrade naar 7.4.2 is convergentie nodig, zo is de configuratie in de FMC UI, FTD CLI Lina en Linux, voor en na de fusie.

Er zijn ook traffic captures op FTD CLI Lina en Linux om het verkeer te tonen met behulp van de logische diagnostische interfacebeweging om de Management interface te gebruiken.

Vóór convergentieconfiguratie

De diagnostische interface heeft een aparte IP en een statische route voor de DNS Lookup, op deze manier werkt het met behulp van beide logische interfaces van Lina naar Linux in de FTD.

Configuratie FMC UI



Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 12 ⚙️ ⓘ admin ▾ CISCO SECURE

Tac_test Save Cancel

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	
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		✎

Diagnostische interfaceconfiguratie vóór samenvoegen

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ **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							

Statische route geconfigureerd op diagnostische interface

DNS-configuratie via IP

Apparaten > Platform-instellingen, selecteer het beleid en vervolgens het tabblad DNS.

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 Add

DNS_Server_lab (Default)

any

Expiry Entry Timer:

Range: 1-65535 minutes

Poll Timer:

Range: 1-65535 minutes

DNS-configuratie in platforminstellingen

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.

Selectievakje voor Schakel DNS-raadpleging ook in via interface voor diagnose/beheer

Configuratie voor diagnostische interface via 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
```

DNS-configuratie op FTD CLI Lina

```
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
```

Leg op de diagnostische interface vast voor DNS-verkeer naar de DNS-server 10.10.10.10

```
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#
```

Leg vast in de Linux expert-modus om de juiste stroom van het DNS Lookup-verkeer op de Management-interface vanuit de diagnostische interface te bevestigen

```
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)
```

Na convergentieconfiguratie

Zoals gezegd over de convergentieprocedure, om de samenvoeging te doen, moeten alle configuraties op de diagnostische interface worden verwijderd.

Dit is de informatie over FMC en FTD CLI zodra de samenvoeging is voltooid.

Beheer van interfaceconfiguratie via FMC UI

Apparaten > Apparaatbeheer, selecteer de FTD. Het wordt rechtstreeks geopend in het tabblad Interfaces.

Firewall Management Center
Devices / Secure Firewall Interfaces

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 12 ⚙️ ⓘ admin ▾ CISCO SECURE

Tac_test

SaveCancel

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	
● Management0/0	management	Physical				Disabled	Global	🔍 ↺
🔌 GigabitEthernet0/0		Physical				Disabled		✎
🔌 GigabitEthernet0/1		Physical				Disabled		✎
🔌 GigabitEthernet0/2		Physical				Disabled		✎

Beheerinterface na de fusie

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 12 ⚙️ ⓘ 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							

Er worden geen statische routes naar de DNS-server toegevoegd

DNS-configuratie moet hetzelfde blijven op Platform-instellingen.

Apparaten > Platform-instellingen, selecteer het beleid en vervolgens het tabblad DNS.

Opdat de DNS Lookup verder naar de Management Interface wordt verzonden zonder de noodzaak om een statische route toe te voegen, "laat DNS Lookup via diagnostische/Management interface ook toe." moet geselecteerd blijven.



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

DNS-configuratie op platform-instellingen

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.

Optie voor het inschakelen van DNS-raadpleging via diagnostische/beheerinterface moet ook hetzelfde blijven

Configuratie op de FTD CLI

```
> 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

DNS-configuratie op FTD CLI aan LINA-zijde

```
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
```

Leg vast in de Linux expert-modus om de juiste stroom van het DNS Lookup-verkeer op de Management-interface te bevestigen.

```
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)
```

Met dit bewijs kan worden bevestigd dat de DNS Lookup blijft werken zelfs als er geen statische route is toegevoegd aan de Management-interface via Linux.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.