

Configuration de la fusion de l'interface de gestion et de diagnostic dans FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Informations générales](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme d'architecture interne FTD](#)

[Procédure De Convergence](#)

[Vérifier](#)

[Dépannage - Étude de cas](#)

[Avant la configuration de convergence](#)

[Configuration après convergence](#)

Introduction

Ce document décrit les étapes pour configurer la fusion des interfaces de gestion et de diagnostic, fonctionnalité ajoutée dans la version FTD 7.4.0.

Conditions préalables

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Cisco Secure Firewall Threat Defense (FTD)
- Centre Cisco Secure Firewall Manager (FMC)

Informations générales

Dans les versions 7.3 et antérieures, l'interface de gestion physique est partagée entre l'interface logique de diagnostic (Lina) et l'interface logique de gestion (Linux).

Dans les versions 7.4 et ultérieures, l'interface Diagnostic est fusionnée avec Management pour une expérience utilisateur simplifiée.

Pour les nouveaux périphériques utilisant 7.4 et versions ultérieures, vous ne pouvez pas utiliser l'interface de diagnostic héritée. Seule l'interface de gestion fusionnée est disponible.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Threat Defense (FTD) virtuel, version 7.4.2
- Cisco Secure Firewall Manager Center (FMC) virtuel, version 7.4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Si vous avez effectué une mise à niveau vers la version 7.4 ou ultérieure et que vous disposez d'une configuration pour l'interface de diagnostic, vous pouvez fusionner les interfaces manuellement ou continuer à utiliser l'interface de diagnostic distincte.

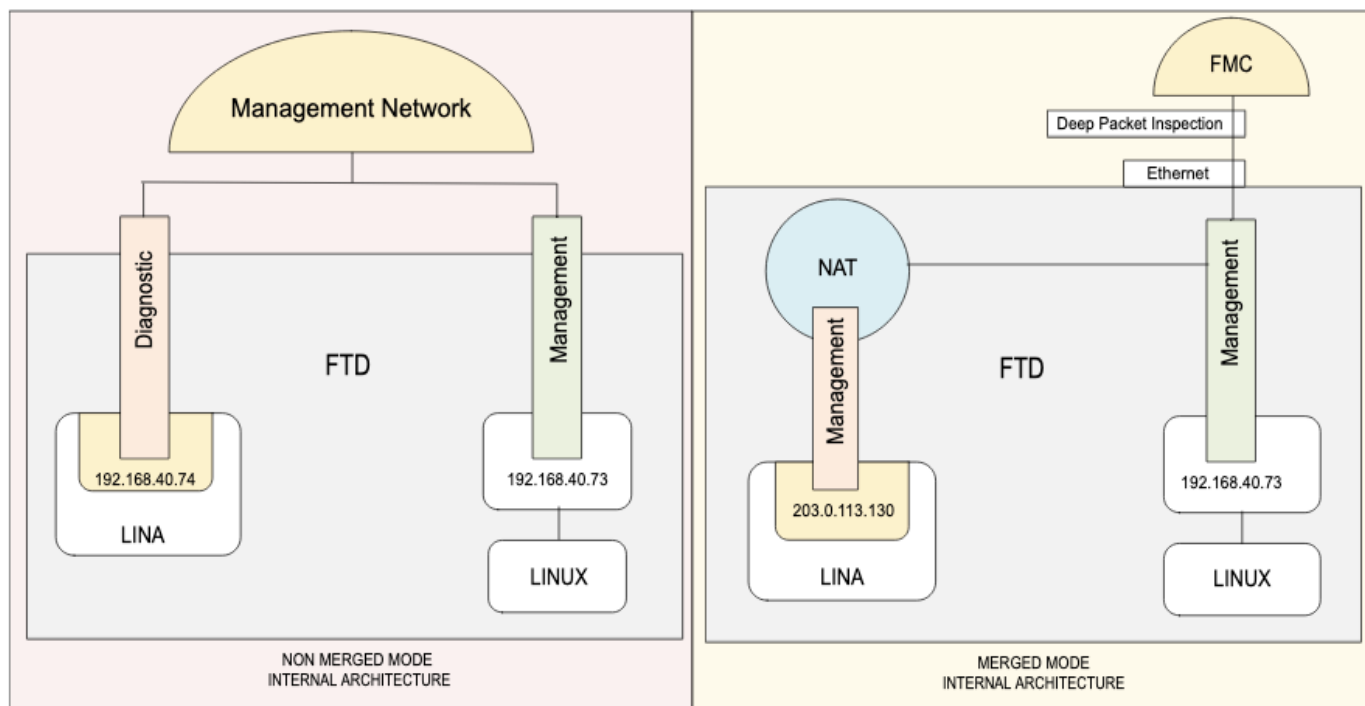
Si vous n'avez pas configuré l'interface de diagnostic, la fusion des interfaces est automatique.



Remarque : La prise en charge de l'interface de diagnostic doit être supprimée dans une version ultérieure. Par conséquent, prévoyez de fusionner les interfaces dès que possible.

Diagramme d'architecture interne FTD

Présentation de l'interface de gestion convergente



Présentation de l'architecture interne avant et après l'interface de gestion de la convergence

À gauche, l'architecture interne de l'interface logique de diagnostic (Lina) et de l'interface logique de gestion (Linux). Versions 7.3 et antérieures.

À droite, l'architecture interne d'une interface de gestion unique. L'accès de ligne au réseau de gestion utilise le service NAT.

Procédure De Convergence

Dans le cas où la configuration existe dans l'interface de diagnostic, les interfaces ne sont pas fusionnées automatiquement après une mise à niveau et vous devez effectuer la procédure de convergence.

Cette procédure vous oblige à accuser réception des modifications de configuration et, dans certains cas, à corriger manuellement la configuration.

Pour afficher le mode actuel du périphérique, entrez la commande `show management-interface converge` dans le champ FTD CLI Clish

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

Ce résultat montre que les interfaces de gestion ne sont pas fusionnées.

Étape 1.

Dans l'interface utilisateur de FMC, accédez à `Devices > Device Management`, et sélectionnez le FTD à modifier. Il s'ouvre directement sur l'onglet Interfaces.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 10 ⚙️ ? admin ✓ **SECURE**

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		✎

Action nécessaire pour fusionner l'interface de diagnostic et de gestion après la mise à niveau du périphérique vers la version 7.4.2 du logiciel

Étape 2.

Supprimez toute la configuration sur l’interface de diagnostic. Il est obligatoire que l'interface de diagnostic ne dispose d'aucune configuration pour poursuivre la fusion.

Par exemple, dans cette interface de diagnostic, il y a : Adresse IP et route statique.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 10 ⚙️ ? admin ✓ **SECURE**

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

Supprimer l'adresse IP de l'interface de diagnostic

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 Save Cancel

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							

Route statique configurée sur l'interface de diagnostic

Étape 3.

Cliquez sur la zone Management Interface Merge action required ou sur l'icône Merge en regard de l'icône Edit (crayon) sur l'interface Diagnostic.

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

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 ▾

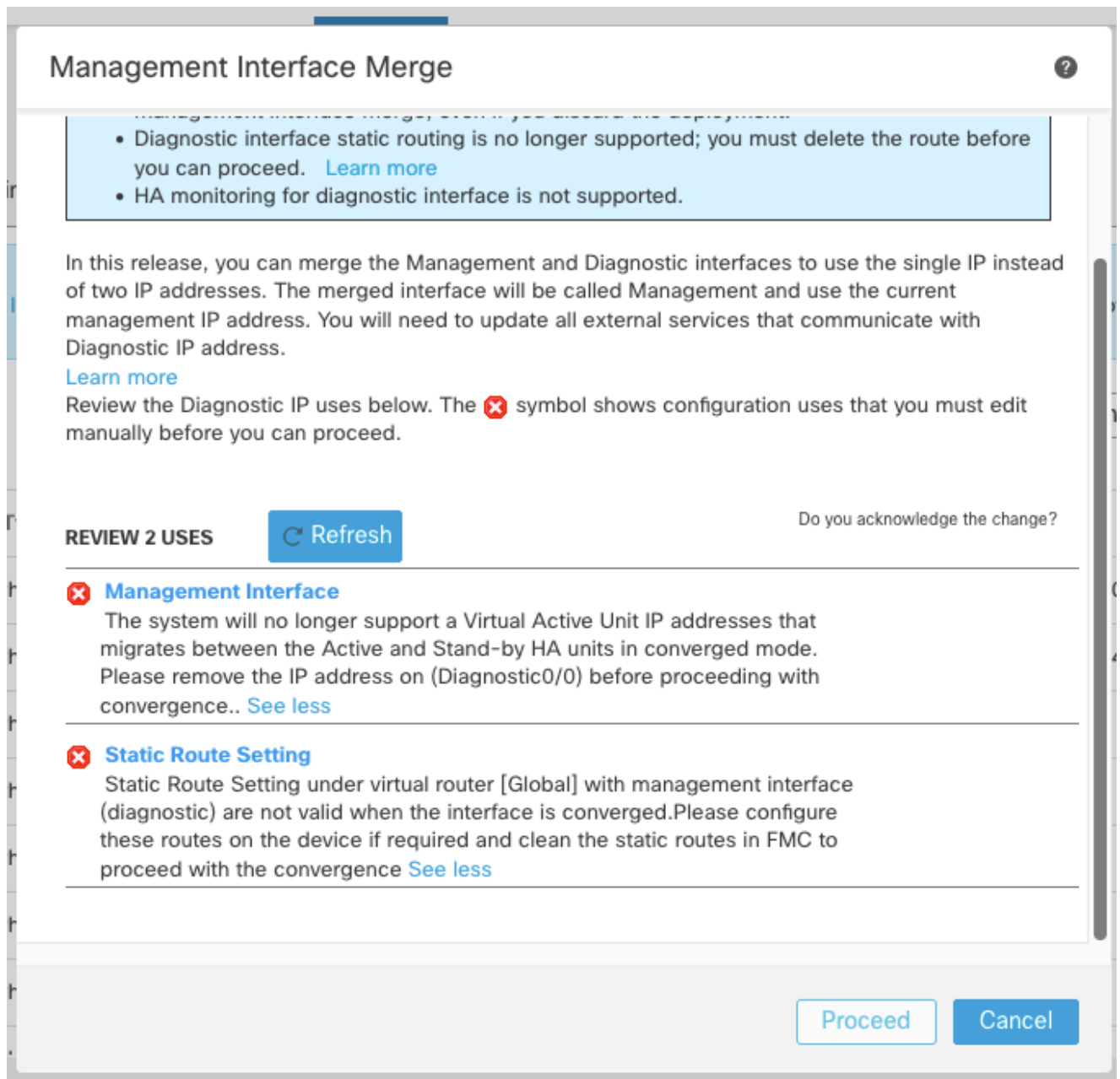
Path Monitoring	Virtual Router	
Disabled	Global	 
Disabled		
Disabled		
Disabled		

Informations de fusion de l'interface de gestion avant de continuer



Remarque : Pour les paires et les clusters à haute disponibilité, effectuez cette tâche sur l'unité active/de contrôle. La configuration fusionnée est répliquée automatiquement sur les unités de secours/données.

-
- Une icône d'avertissement peut s'afficher pour toute occurrence nécessitant une modification ou une suppression manuelle.



Exemple d'avertissement sur les configurations à supprimer avant la fusion

Si tel est le cas : annulez la boîte de dialogue, procédez à la suppression de la configuration ou de la reconfiguration, puis rouvrez la boîte de dialogue Fusion de l'interface de gestion.

- Les paramètres de la plate-forme qui vont fonctionner sur le périphérique sont signalés par une icône d'avertissement et nécessitent un accusé de réception.

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

Exemple d'avertissement de configurations de paramètres de plateforme qui doivent être modifiées

- Cliquez sur la case dans Accusez-vous réception de la modification ? , puis cliquez sur Continuer.

Étape 4.

Une fois la configuration fusionnée, une bannière de réussite s'affiche :

"La fusion de l'interface de gestion a été enregistrée et est prête à être déployée.

Notez que vous ne pouvez pas annuler les modifications de configuration liées à la fusion ; vous devez reconfigurer manuellement l'interface de diagnostic et la configuration associée."

Déployez la nouvelle configuration fusionnée.

La fusion de l'interface de gestion est enregistrée et prête à être déployée

L'interface de gestion est affichée sur la page Interfaces, bien qu'elle soit en lecture seule.

Une fois le déploiement terminé, la procédure de convergence sur l'interface de gestion est terminée.

Étape 5. Facultatif

Si vous aviez des services externes qui communiquaient avec l'interface de diagnostic, vous devez modifier leur configuration pour utiliser l'adresse IP de l'interface de gestion, car la reprise de la route de gestion a été supprimée en mode convergé.

Exemple :

- Client SNMP
- serveur RADIUS
- Pour que le serveur DNS soit accessible via le réseau de gestion, l'utilisateur doit explicitement sélectionner « Enable DNS Lookup via diagnostic/Management Interface also. » dans Platform Settings > DNS configuration, une exception est définie pour les recherches DNS et ICMP (ping et traceroute) : dans ce cas, la protection contre les menaces utilise les données, puis la gestion est automatiquement rétablie si aucune route n'est trouvée.

L'utilisation de routes statiques pour l'interface de gestion ne peut être configurée que par l'intermédiaire de la CLI Clish FTD (Linux)

La route par défaut du port de gestion Lina envoie toutes les trames au module 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
```

Sur l'interface utilisateur FMC, l'interface de gestion est grisée pour la sélection.

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 >

L'interface de gestion n'est pas disponible pour la sélection sur les routes statiques une fois la fusion terminée.

Vérifier

Modifications attendues après la fusion sur l'interface de gestion

- Vérifier le mode de convergence sur FTD CLI Clish en exécutant la commande

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

- Sur l'interface utilisateur FMC, le nom de l'interface devient Management0/0 , le nom logique devient management.

Firewall Management Center
Devices / Secure Firewall Interfaces

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

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		✎

Confirmation de fusion sur le nom de l'interface de gestion et le nom logique

- Sur FTD CLI Clish, les nouvelles adresses IP sont automatiquement configurées sur l'interface Lina for Management.
La NAT est utilisée comme implémentation interne : Les adresses IPv4 privées internes 203.0.113.130 et l'adresse IPv6 fd00:0:1:1::2 sont celles qui sont attribuées (toutes deux sujettes à modification).
Ces adresses IP sont envoyées par NAT aux adresses IPv4 et IPv6 FTD du noyau Linux public. Par conséquent, il n'est plus nécessaire d'utiliser des adresses IP publiques sur Lina.

En mode expert, « ifconfig » affiche l'adresse IPv4 interne (203.0.113.129) et l'adresse IPv6 (fd00:0:1:1::1) pour 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:febf:6d16 prefixlen 64 scopeid 0x20

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

Dépannage - Étude de cas

Dans ce cas d'étude, l'interface de diagnostic sur un FTD virtuel a configuré une adresse IP distincte pour la connectivité aux services externes de la recherche DNS, avant la mise à niveau vers la version 7.4.2.

Après la mise à niveau vers la version 7.4.2, la convergence est nécessaire. C'est ainsi que se présente la configuration dans l'interface utilisateur FMC, la ligne de commande FTD et Linux, avant et après la fusion.

Il existe également des captures de trafic sur FTD CLI Lina et Linux pour afficher le trafic à l'aide du déplacement de l'interface de diagnostic logique pour utiliser l'interface de gestion.

Avant la configuration de convergence

L'interface de diagnostic a une adresse IP séparée et une route statique pour la recherche DNS, de cette façon, elle fonctionne en utilisant les deux interfaces logiques de Lina à Linux dans le FTD.

Configuration de l'interface FMC

Firewall Management Center
Devices / Secure Firewall Interfaces

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 ⓘ ⚙️ ⓘ admin 🔽 Cisco **SECURE**

Tac_test

Cisco Firepower Threat Defense for VMware

DeviceInterfacesInline SetsRoutingDHCPVTEP

SaveCancel

All InterfacesVirtual Tunnels

🔍 Search by nameSync DeviceAdd 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		✎

Configuration de l'interface de diagnostic avant fusion

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

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

Route statique configurée sur l'interface de diagnostic

Configuration DNS sur

Périphériques > Paramètres de plate-forme, sélectionnez la stratégie, puis l'onglet 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

Configuration DNS dans les paramètres de plateforme

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.

Case à cocher également sélectionnée pour Activer la recherche DNS via l'interface de diagnostic/gestion

Configuration de l'interface de diagnostic sur 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
```

Configuration DNS sur la ligne de commande FTD

```
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
```

Capture sur l'interface de diagnostic du trafic DNS allant au serveur DNS 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#
```

Capture en mode expert Linux, pour confirmer le flux correct du trafic de recherche DNS sur l'interface de gestion à partir de l'interface de diagnostic

```
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)

```

Configuration après convergence

Comme mentionné dans la procédure de convergence, pour effectuer la fusion, toutes les configurations sur l'interface de diagnostic doivent être supprimées.

Voici les informations sur l'interface de ligne de commande FMC et FTD une fois la fusion terminée.

Configuration de l'interface de gestion sur FMC UI

Périphériques > Gestion des périphériques, sélectionnez le FTD. Il s'ouvre directement sur l'onglet Interfaces.

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 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		✎

Interface de gestion après la fusion

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							

Aucune route statique vers le serveur DNS n'est ajoutée

La configuration DNS doit rester identique dans les paramètres de la plate-forme.

Périphériques > Paramètres de plate-forme, sélectionnez la stratégie, puis l'onglet DNS.

Pour que la recherche DNS continue à être envoyée à l'interface de gestion sans qu'il soit nécessaire d'ajouter une route statique, la commande « Enable DNS Lookup via diagnostic/Management interface also » (Activer la recherche DNS via l'interface de diagnostic/gestion). doit rester sélectionné.



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

Configuration DNS sur les paramètres de plateforme

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.

L'option d'activation de la recherche DNS via l'interface de diagnostic/gestion doit également rester la même

Configuration sur l'interface CLI FTD

```
> 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

Configuration DNS sur l'interface de ligne de commande FTD côté LINA

```
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
```

Effectuez une capture en mode expert Linux pour confirmer le flux correct du trafic de recherche DNS sur l'interface de gestion.

```
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)
```

Avec cette preuve, il peut être confirmé que la recherche DNS continue à fonctionner même si aucune route statique n'est ajoutée sur l'interface de gestion via Linux.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.