# Clarifier l'objectif de l'adresse IP 203.0.113.x pour l'interface de gestion FTD

## Table des matières


Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Trafic de gestion dans les déploiements d'interface de gestion convergée

Vérification

Conclusion

Références


## Introduction

Ce document décrit l'adresse IP 203.0 .113.x indiquée dans le résultat de quelques commandes dans le Secure Firewall Threat Defense (FTD).

## Conditions préalables

### Exigences

Connaissances de base sur les produits.

### Composants utilisés

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.

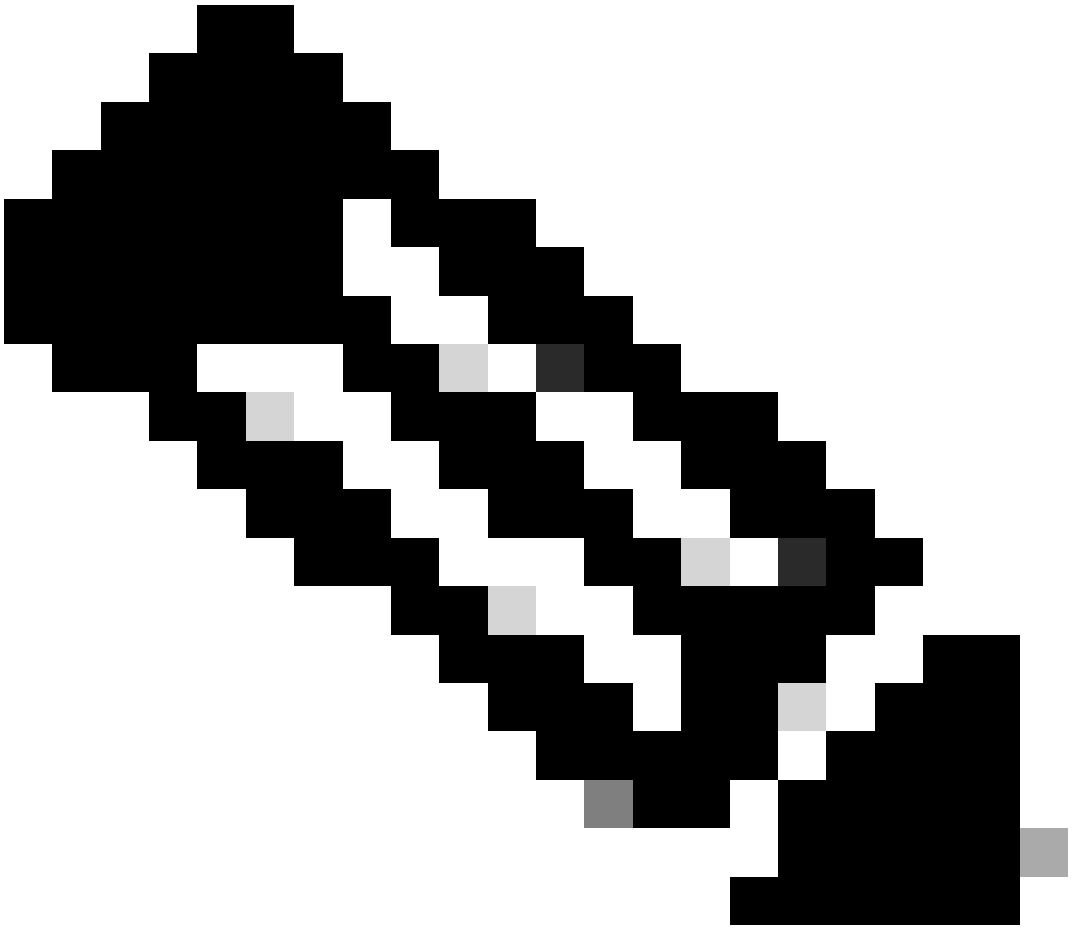
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Défense de thread de pare-feu sécurisée (FTD) 7.4.x, 7.6.x. géré par le Gestionnaire de périphériques de pare-feu sécurisé (FDM) ou le Centre de gestion de pare-feu sécurisé (FMC).

## Informations générales

Après la mise à niveau logicielle vers les versions 7.4.x ou 7.6.x, vous pouvez remarquer des changements liés à l'adresse IP de l'interface de gestion :

---



Remarque : Les résultats de cet article concernent les FTD gérés par FMC lorsque l'interface d'accès du gestionnaire n'est pas une interface de données et les FTD gérés par FDM lorsque l'option « Utiliser des passerelles uniques pour l'interface de gestion » n'est pas configurée.
Dans les cas où une interface de données est utilisée pour l'accès du gestionnaire,

---

certains détails tels que le chemin du trafic de gestion ou le résultat de la commande show network diffèrent.

Reportez-vous à la section « Modifier l'interface d'accès du manager de la gestion aux données » du chapitre : Paramètres du périphérique dans le Guide de configuration du périphérique Cisco Secure Firewall Management Center, 7.6 et la section « Configurer l’interface de gestion » du chapitre : Interfaces du Guide de configuration de Cisco Secure Firewall Device Manager, version 7.6.

---

1. L'adresse IP est 203.0.113.x, bien qu'elle n'ait pas été configurée manuellement. Voici un exemple de sortie de FTD exécuté sur toutes les plates-formes à l'exception de Firepower 4100/9300 :

```
<#root>

>

show nameif

Interface                Name                    Security
Management1/1            management                0



>

show interface ip brief

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



>

show interface Management


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


  Hardware is en_vtun rev00, DLY 1000 usec
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0053.500.2222, MTU 1500

        IP address 203.0.113.130, subnet mask 255.255.255.248


…

>
```

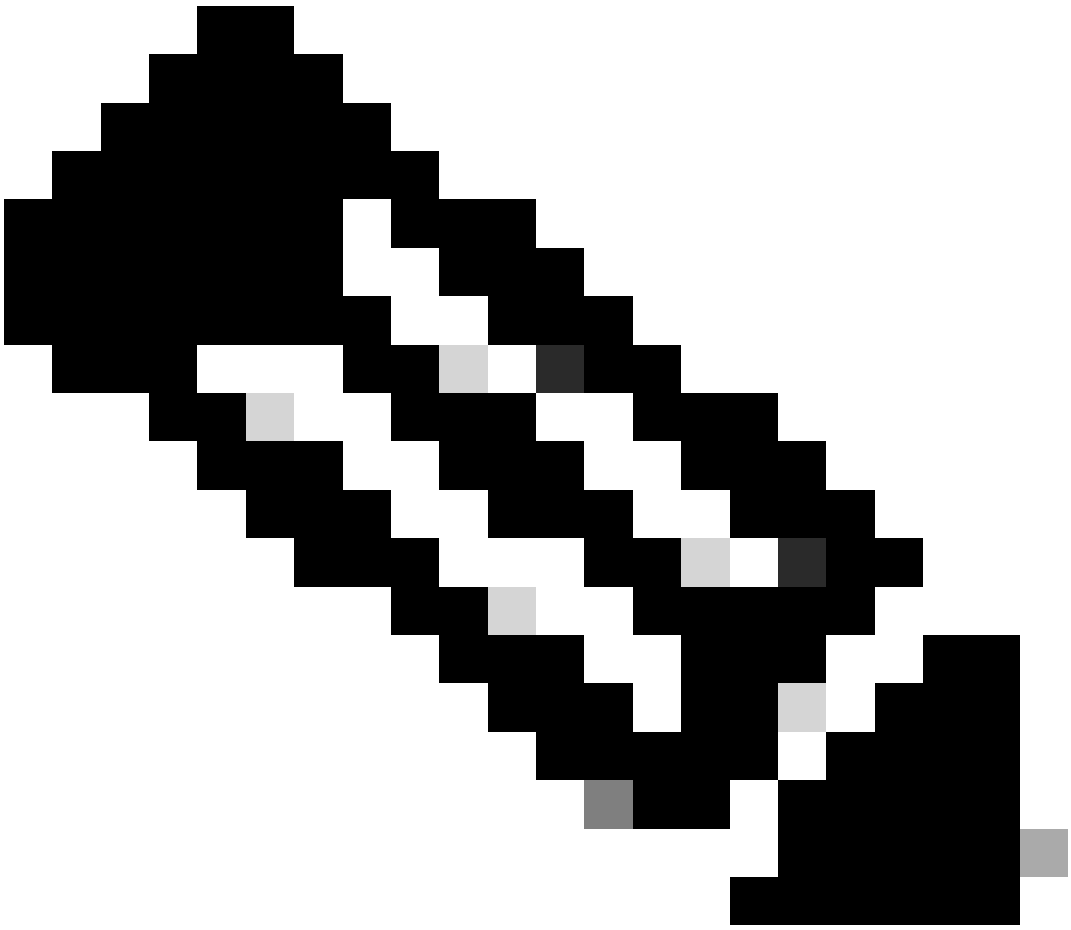
```
show running-config interface Management 1/1

!
interface Management1/1

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

Interface de gestion du FTD exécuté sur Firepower 4100/9300 :

```
<#root>
>
show nameif

Interface                Name                    Security
…
Ethernet1/1              management                0



>
show interface ip brief

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



>
show interface management


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


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


…
```

```
>

show running-config interface Ethernet 1/1


interface Ethernet1/1


 management-only

 nameif management


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

---



Remarque : Sur Firepower 4100/9300, vous pouvez créer une interface Ethernetx/y dédiée en tant qu'interface de gestion personnalisée pour les applications. Par

---

conséquent, le nom de l'interface physique est Ethernetx/y, et non Managementx/y.

2. Cette adresse IP est différente de l'adresse IP affichée dans le résultat de la commande show network :

```
<#root>

>

show network


===============[ System Information ]===============
Hostname                  : firewall
Domains                   : www.example.org
DNS Servers               : 198.51.100.100
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : 192.0.2.1


==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : sfpDetect
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:53:00:00:00:01

---------------------[ IPv4 ]----------------------
Configuration             : Manual

Address                   : 192.0.2.100


Netmask                   : 255.255.255.0
Gateway                   : 192.0.2.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

L'adresse IP 203.0.113.x est attribuée à l'interface de gestion dans le cadre de la fonctionnalité d'interface de gestion convergente (CMI) introduite dans la version 7.4.0. Plus précisément, après la mise à niveau logicielle vers la version 7.4.x ou ultérieure, le logiciel propose de fusionner les interfaces de gestion et de diagnostic comme indiqué dans la section Fusionner les interfaces de gestion et de diagnostic. Si la fusion réussit, le nom de l'interface de gestion if devient management et se voit automatiquement attribuer l'adresse IP interne 203.0.113.x.

## Trafic de gestion dans les déploiements d'interface de gestion

# convergée

L'adresse IP 203.0.113.x est utilisée pour fournir une connectivité de gestion à partir du moteur Lina et vers les réseaux de gestion externes via l'interface management0 du châssis, comme suit. Cette connectivité est essentielle dans les cas où vous configurez des services Lina comme syslog, la résolution de noms de domaine (DNS), l'accès aux serveurs d'authentification, d'autorisation et de comptabilité (AAA) et ainsi de suite.

Ce diagramme présente une vue d'ensemble de haut niveau du chemin du trafic de gestion du moteur Lina au réseau de gestion externe :


Principaux points :

1. L'adresse IP 203.0.113.x avec le masque de réseau /29 est configurée sous l'interface avec le nom if management. Mais cette configuration n'est pas visible dans le résultat de la commande show run interface :

<#root>

>

**show interface Management**

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

        IP address 203.0.113.130, subnet mask 255.255.255.248

…
```

>

**show running-config interface Management 1/1**

```
!
interface Management1/1
 management-only
 nameif management
 cts manual
```

```
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
```

La passerelle par défaut 203.0.113.129 network est configurée dans la table de routage de gestion. Cette route par défaut n'est pas visible dans le résultat de la commande show route management-only sans arguments. Vous pouvez vérifier la route en spécifiant l'adresse 0.0.0.0 :

```
<#root>

>

show route management-only



Routing Table: mgmt-only
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set


>

show route management-only 0.0.0.0


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

203.0.113.129, via management


      Route metric is 0, traffic share count is 1


>

show asp table routing management-only


route table timestamp: 51
in   203.0.113.128   255.255.255.248 management

in   0.0.0.0         0.0.0.0         via 203.0.113.129, management


out  255.255.255.255 255.255.255.255 management
```

```
out  203.0.113.130   255.255.255.255 management
out  203.0.113.128   255.255.255.248 management
out  224.0.0.0       240.0.0.0       management
out  0.0.0.0         0.0.0.0         via 203.0.113.129, management

out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
```

2. L’adresse IP 203.0.113.129 est configurée côté Linux et visible en mode expert et attribuée à une interface interne, par exemple, tap_M0:

```
<#root>

admin@KSEC-FPR3100-2:~$

 ip route show 203.0.113.129/29

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

3. Sous Linux, l’adresse IP de gestion du châssis est attribuée à l’interface management0. Voici l'adresse IP visible dans le résultat de la commande show network :

```
<#root>

>

show network

===============[ System Information ]===============
Hostname                  : firewall
Domains                   : www.example.org
DNS Servers               : 198.51.100.100
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : 192.0.2.1

==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : sfpDetect
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:53:00:00:00:01
```

```
---------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.0.2.100


Netmask                   : 255.255.255.0
Gateway                   : 192.0.2.1
---------------------[ IPv6 ]----------------------
Configuration             : Disabled


>
expert


admin@KSEC-FPR3100-2:~$
ip addr show management0


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


default via 192.0.2.1 dev management0
```

4. Il existe une traduction d'adresse de port dynamique (PAT) sur l'interface management0 qui traduit l'adresse IP source en adresse IP de l'interface management0. La PAT dynamique est obtenue en configurant une règle iptables avec l'action MASQUERADE sur l'interface management0 :

<#root>

```
admin@KSEC-FPR3100-2:~$
sudo iptables -t nat -L -v -n


Password:
…
Chain POSTROUTING (policy ACCEPT 49947 packets, 2347K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
6219  407K MASQUERADE  all  --  *      management0+  0.0.0.0/0            0.0.0.0/0
```

# Vérification

Dans cet exemple, CMI est activé et dans les paramètres de la plate-forme, la résolution DNS via l'interface de gestion est configurée :

```
<#root>

>

show management-interface convergence


management-interface convergence



>

show running-config dns


dns domain-lookup management

DNS server-group DefaultDNS
DNS server-group ciscodns

name-server 198.51.100.100 management

dns-group ciscodns
```

Les captures de paquets sont configurées sur les interfaces de gestion Lina, Linux tap_M0 et management0 :

```
<#root>

>

show capture


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


  match udp any any eq domain
```

```
>
expert

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

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

>
expert

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

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

Une requête d'écho ICMP vers un exemple de nom de domaine complet (FQDN) génère une requête DNS à partir du moteur Lina. La capture de paquets dans le moteur Lina et l'interface Linux tap_M0 affiche l'adresse IP de l'initiateur 203.0.113.130, qui est l'adresse IP CMI de l'interface de gestion :

```
<#root>
>
ping interface management www.example.org

Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 198.51.100.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/122/130 ms

>
show capture dns

2 packets captured
   1: 23:14:22.562303
203.0.113.130
```

```
.45158 > 198.51.100.100.53:  udp 29
   2: 23:14:22.595351       198.51.100.100.53 >
```

**203.0.113.130**

```
.45158:  udp 45
2 packets shown


admin@firewall
```

**:~$ sudo tcpdump -n -i tap_M0 udp and port 53**

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

23:14:22.570892 IP
```

**203.0.113.130**

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

**203.0.113.130**

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

Les captures de paquets sur l'interface management0 affichent l'adresse IP de l'interface management0 comme adresse IP de l'initiateur. Cela est dû à la PAT dynamique mentionnée dans la section « Chemin de trafic de gestion dans les déploiements d'interface de gestion convergente » :

<#root>

```
admin@firewall:~$
```

**sudo tcpdump -n -i management0 udp and port 53**

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

23:14:22.570927 IP
```

**192.0.2.100**

```
.45158 > 198.51.100.100.53: 38323+ A? www.example.org. (29)
23:14:22.603877 IP 198.51.100.100.53 >
```

**192.0.2.100**

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

## Conclusion

Si CMI est activé, l'adresse IP 203.0.113.x est automatiquement attribuée et utilisée en interne par le logiciel pour fournir la connectivité entre le moteur Lina et le réseau de gestion externe. Vous pouvez ignorer cette adresse IP.
L'adresse IP affichée dans le résultat de la commande show network reste inchangée et est la seule adresse IP valide que vous devez appeler l'adresse IP de gestion FTD.

## Références

- Fusionner les interfaces de gestion et de diagnostic
- Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.6
- Guide de configuration de Cisco Secure Firewall Device Manager, version 7.6

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.