Aclare el propósito de la dirección IP 203.0.113.x para la interfaz de administración de FTD

Contenido

Introducción

Este documento describe la dirección IP 203.0.113.x que se muestra en la salida de algunos comandos de la defensa contra amenazas de firewall seguro (FTD).

Prerequisites

Requirements

Conocimiento básico del producto.

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

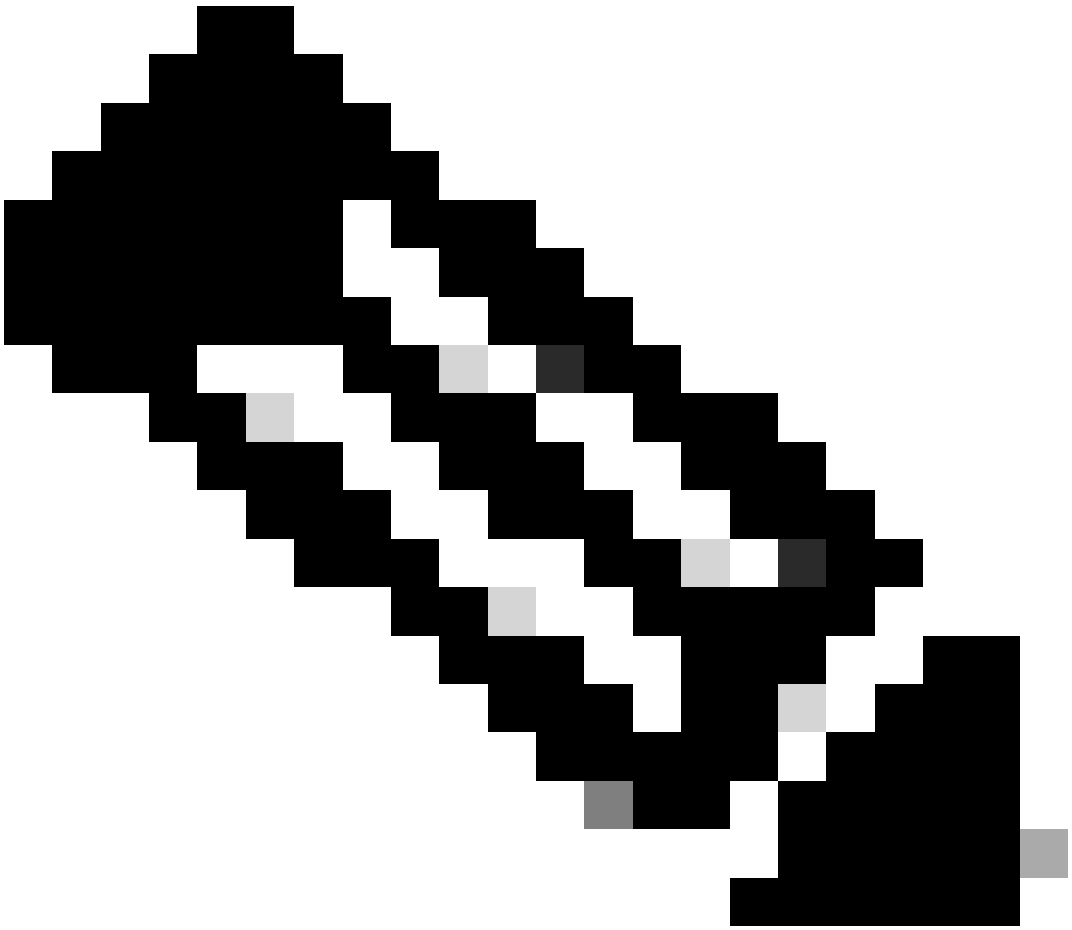
La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Secure Firewall Thread Defense (FTD) 7.4.x, 7.6.x. gestionado por el administrador de dispositivos de firewall seguro (FDM) o el centro de gestión de firewall seguro (FMC).

Antecedentes

Después de actualizar el software a las versiones 7.4.x o 7.6.x, puede observar cambios relacionados con la dirección IP de la interfaz de administración:



Nota: Los resultados de este artículo son relevantes para los FTD gestionados por FMC cuando la interfaz de acceso del administrador no es una interfaz de datos y los FTD gestionados por FDM cuando la opción "Utilizar gateways únicos para la interfaz de gestión" no está configurada.

En los casos en que se utiliza una interfaz de datos para el acceso del administrador, algunos detalles como la trayectoria del tráfico de administración o el resultado del comando show network difieren.

Consulte la sección "Cambio de la interfaz de acceso del jefe de la gestión a los datos" en el capítulo: Configuración de dispositivos en la Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.6 y en la sección "Configuración de la interfaz de gestión" del capítulo: Interfaces de la Guía de configuración de Cisco Secure Firewall Device Manager, versión 7.6.

1. La dirección IP es 203.0.113.x, aunque no se configuró manualmente. Este es un ejemplo de salida de FTD que se ejecuta en todas las plataformas excepto Firepower 4100/9300:

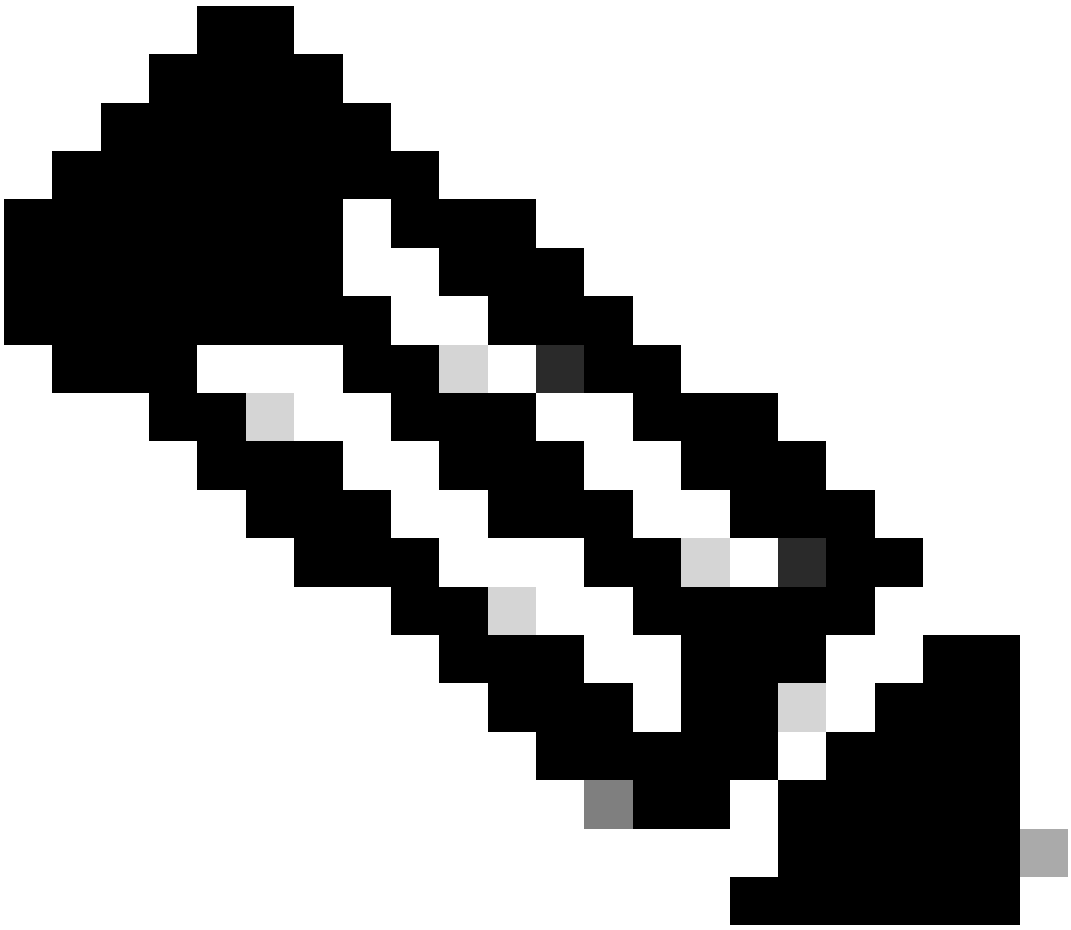
```
<#root>

>

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
```

La interfaz de administración de FTD que se ejecuta en 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
```



Nota: En Firepower 4100/9300, puede crear un Ethernet/y dedicado como interfaz de administración personalizada para aplicaciones, por lo tanto, el nombre de la interfaz

---

física es Ethernet/y, no ManagementX/y.

2. Esta dirección IP es diferente de la dirección IP que se muestra en la salida del comando 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
```

La dirección IP 203.0.113.x se asigna a la interfaz de administración como parte de la función de interfaz de administración convergente (CMI) introducida en la versión 7.4.0. Específicamente, después de la actualización del software a la versión 7.4.x o posterior, el software propone combinar las interfaces de administración y diagnóstico como se muestra en la sección Fusionar las interfaces de administración y diagnóstico. Si la fusión es exitosa, el nombre de la interfaz de administración if se convierte en administración y se le asigna automáticamente la dirección IP interna 203.0.113.x.

Ruta de tráfico de administración en implementaciones de interfaz de administración convergente

La dirección IP 203.0.113.x se utiliza para proporcionar conectividad de administración desde el motor Line y a las redes de administración externas a través de la interfaz management0 del chasis de la siguiente manera. Esta conectividad es esencial en los casos en los que se configuran servicios de línea como syslog, resolución de nombres de dominio (DNS), acceso a los servidores de autenticación, autorización y contabilidad (AAA), etc.

Este diagrama muestra una descripción general de alto nivel de la trayectoria del tráfico de administración desde el motor Lina a la red de administración externa:

Puntos clave:

1. La dirección IP 203.0.113.x con la máscara de red /29 se configura en la interfaz con la administración nameif. Pero esta configuración no es visible en el resultado del comando 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 gateway predeterminada 203.0.113.129 network se configura en en la tabla de ruteo de administración. Esta ruta predeterminada no está visible en la salida del comando show route management-only sin argumentos. Puede verificar la ruta especificando la dirección 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. La dirección IP 203.0.113.129 se configura en el lado de Linux y es visible en el modo experto y se asigna a una interfaz interna, por ejemplo, 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. En Linux, la dirección IP de administración del chasis se asigna a la interfaz management0. Ésta es la dirección IP visible en el resultado del comando 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. Hay traducción dinámica de direcciones de puerto (PAT) en la interfaz management0 que traduce la dirección IP de origen a la dirección IP de la interfaz management0. La PAT dinámica se logra configurando una regla iptables con la acción MASQUERADE en la interfaz 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
```

Verificación

En este ejemplo, CMI está habilitado y en la configuración de la plataforma se configura la resolución DNS a través de la interfaz de administración:

```
<#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
```

Las capturas de paquetes se configuran en las interfaces Lina management, Linux tap_M0 y 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
```

Una solicitud de eco ICMP a un nombre de dominio completo (FQDN) de muestra genera una solicitud DNS desde el motor de línea. La captura de paquetes en el motor Lina y la interfaz tap_M0 de Linux muestra la dirección IP del iniciador 203.0.113.130, que es la dirección IP CMI de la interfaz de administración:

<#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)
```

Las capturas de paquetes en la interfaz management0 muestran la dirección IP de la interfaz management0 como dirección IP de iniciador. Esto se debe a la PAT dinámica mencionada en la sección "Ruta de tráfico de administración en implementaciones de interfaz de administración 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)
```

Conclusión

Si CMI está habilitado, la dirección IP 203.0.113.x es asignada automáticamente y utilizada internamente por el software para proporcionar conectividad entre el motor de línea y la red de administración externa. Puede ignorar esta dirección IP.
La dirección IP que se muestra en la salida del comando show network no se modifica y es la única dirección IP válida a la que debe referirse como dirección IP de administración de FTD.

Referencias

- Combinación de las interfaces de gestión y de diagnóstico
- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.6
- Guía de configuración de Cisco Secure Firewall Device Manager, versión 7.6

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).