Chiarire lo scopo dell'indirizzo IP 203.0.113.x per l'interfaccia di gestione FTD

Sommario

Introduzione

Questo documento descrive l'indirizzo IP 203.0 .113.x mostrato nell'output di alcuni comandi di Secure Firewall Threat Defense (FTD).

Prerequisiti

Requisiti

Conoscenze base dei prodotti.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

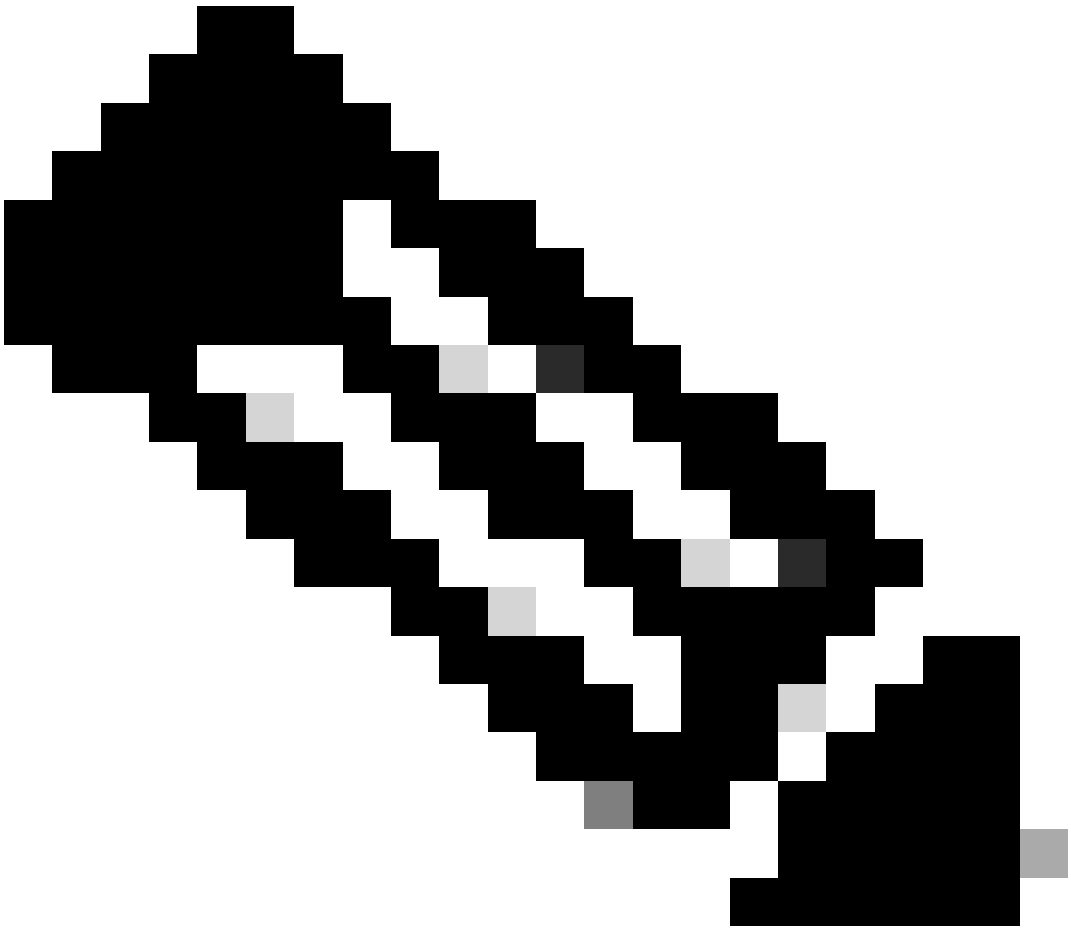
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Secure Firewall Thread Defense (FTD) 7.4.x, 7.6.x gestito da Gestione periferiche firewall protette (FDM) o Centro gestione firewall protette (FMC).

Premesse

Dopo l'aggiornamento del software alle versioni 7.4.x o 7.6.x è possibile notare le modifiche relative all'indirizzo IP dell'interfaccia di gestione:



Nota: Gli output di questo articolo sono rilevanti per i FTD gestiti da FMC quando l'interfaccia di accesso del manager non è un'interfaccia dati e i FTD gestiti da FDM quando l'opzione "Usa gateway univoci per l'interfaccia di gestione" non è configurata. Nei casi in cui viene utilizzata un'interfaccia dati per l'accesso del manager, alcuni dettagli,

come il percorso del traffico di gestione o l'output del comando show network, differiscono.

Fare riferimento alla sezione "Modifica dell'interfaccia di accesso di Manager da Gestione a Dati" nel capitolo: Device Settings (Impostazioni dispositivo) in Cisco Secure Firewall Management Center Device Configuration Guide (Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center), 7.6 e la sezione "Configure the Management Interface" (Configura interfaccia di gestione) nel capitolo: Interfacce nella Guida alla configurazione di Cisco Secure Firewall Device Manager, versione 7.6.

1. L'indirizzo IP è 203.0.113.x, anche se non è stato configurato manualmente. Questo è un esempio di output del comando FTD in esecuzione su tutte le piattaforme ad eccezione di 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
```

L'interfaccia di gestione di FTD su 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
```

…

>

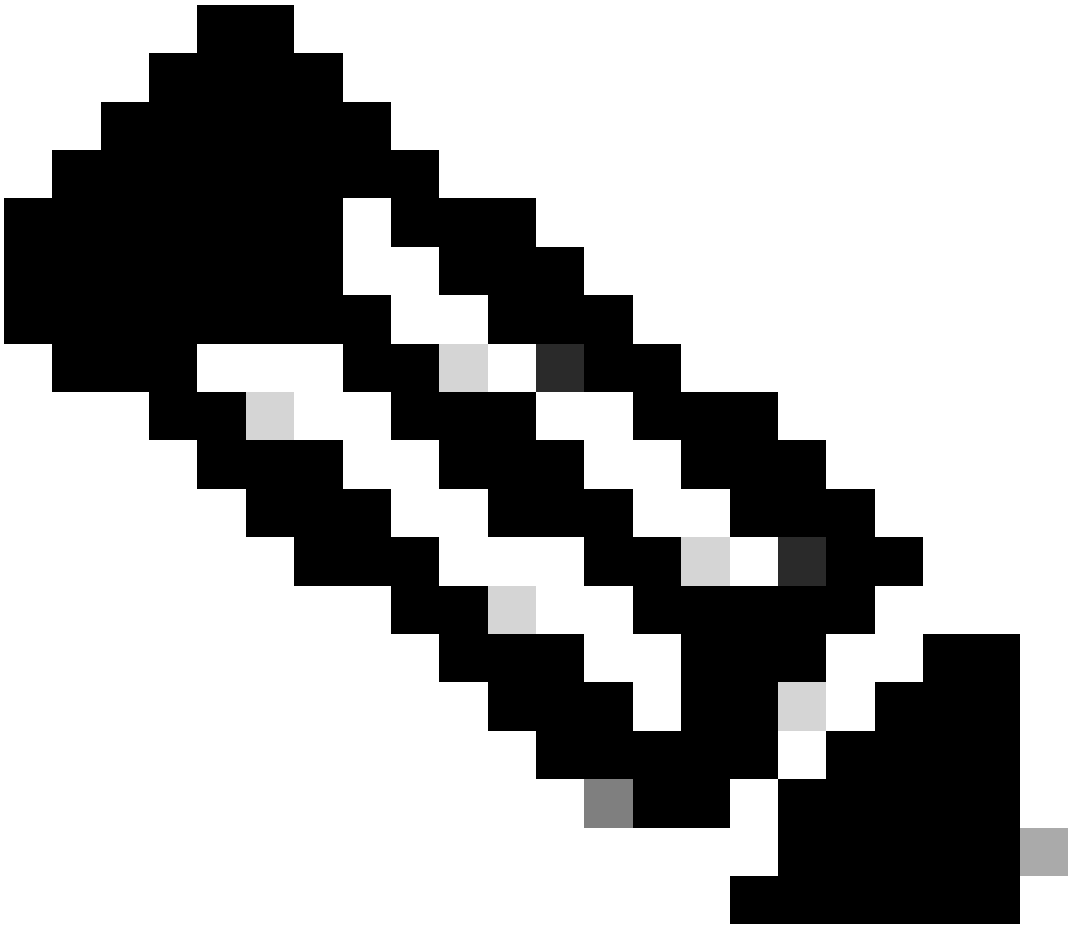
show running-config interface Ethernet 1/1

interface Ethernet1/1

 management-only

 nameif management

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



Nota: Su Firepower 4100/9300, è possibile creare un'interfaccia Ethernet dedicata/y come interfaccia di gestione personalizzata per le applicazioni, pertanto il nome dell'interfaccia fisica è Ethernet/y, non Managementx/y.

2. Questo indirizzo IP è diverso da quello mostrato nell'output 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
```

L'indirizzo IP 203.0.113.x viene assegnato all'interfaccia di gestione come parte della funzionalità CMI (Converged Management Interface) introdotta nella versione 7.4.0. In particolare, dopo l'aggiornamento del software alla versione 7.4.x o successive, il software propone di unire le interfacce di gestione e diagnostica come mostrato nella sezione Unisci interfacce di gestione e diagnostica. Se l'unione viene completata correttamente, il nome dell'interfaccia di gestione diventa management e viene automaticamente assegnato all'indirizzo IP interno 203.0.113.x.

Percorso del traffico di gestione nelle implementazioni dell'interfaccia di gestione convergente

L'indirizzo IP 203.0.113.x viene utilizzato per fornire connettività di gestione dal motore Lina e a reti di gestione esterne tramite l'interfaccia chassis management0 come indicato di seguito. Questa connettività è essenziale nei casi in cui si configurano servizi Lina quali syslog, risoluzione DNS (Domain Name Resolution), accesso ai server di autenticazione, autorizzazione e accounting (AAA) e così via.

Il diagramma mostra una panoramica di alto livello del percorso del traffico di gestione dal motore Lina alla rete di gestione esterna:

Considerazioni principali:

1. L'indirizzo IP 203.0.113.x con netmask /29 è configurato nell'interfaccia con il nome management if. Tuttavia, questa configurazione non è visibile nell'output 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 rete del gateway predefinito 203.0.113.129 è configurata nella tabella di routing di gestione. Questa route predefinita non è visibile nell'output del comando show route management-only senza argomenti. È possibile verificare la route specificando l'indirizzo 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'indirizzo IP 203.0.113.129 è configurato sul lato Linux e visibile in modalità Expert e assegnato a un'interfaccia interna, ad esempio 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. In Linux, l'indirizzo IP di gestione dello chassis viene assegnato all'interfaccia management0. Questo è l'indirizzo IP visibile nell'output 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. Nell'interfaccia management0 è presente una conversione dinamica dell'indirizzo di porta (PAT) che converte l'indirizzo IP di origine nell'indirizzo IP dell'interfaccia management0. Il percorso dinamico si ottiene configurando una regola iptables con l'azione MASQUERADE sull'interfaccia 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
```

Verifica

In questo esempio, CMI è abilitato e nelle impostazioni della piattaforma la risoluzione DNS tramite l'interfaccia di gestione è configurata:

```
<#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
```

Le acquisizioni dei pacchetti sono configurate sulle interfacce Lina management, Linux tap_M0 e 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 richiesta echo ICMP a un nome di dominio completo (FQDN) di esempio genera una richiesta DNS dal motore Lina. L'acquisizione del pacchetto nel motore Lina e nell'interfaccia Linux tap_M0 mostra l'indirizzo IP dell'iniziatore 203.0.113.130, ossia l'indirizzo IP dell'interfaccia di gestione CMI:

```
<#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)
```

Il pacchetto acquisito sull'interfaccia management0 mostra l'indirizzo IP dell'interfaccia management0 come indirizzo IP dell'iniziatore. Ciò è dovuto al percorso dinamico indicato nella sezione "Percorso del traffico di gestione nelle implementazioni dell'interfaccia di gestione 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)
```

Conclusioni

Se CMI è abilitato, l'indirizzo IP 203.0.113.x viene assegnato automaticamente e utilizzato internamente dal software per fornire la connettività tra il motore Lina e la rete di gestione esterna. Puoi ignorare questo indirizzo IP.
L'indirizzo IP mostrato nell'output del comando show network rimane invariato ed è l'unico indirizzo IP valido a cui si deve fare riferimento come indirizzo IP di gestione FTD.

Riferimenti

- Unire le interfacce di gestione e diagnostica
- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.6
- Guida alla configurazione di Cisco Secure Firewall Device Manager, versione 7.6

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).