Clarify the Purpose of IP Address 203.0.113.x for the FTD Management Interface

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Management Traffic Path in Converged Management Interface Deployments

Verification

Conclusion

References

Introduction

This document describes the IP address 203.0 .113.x shown in the output of a few commands in the Secure Firewall Threat Defense (FTD).

Prerequisites

Requirements

Basic product knowledge.

Components Used

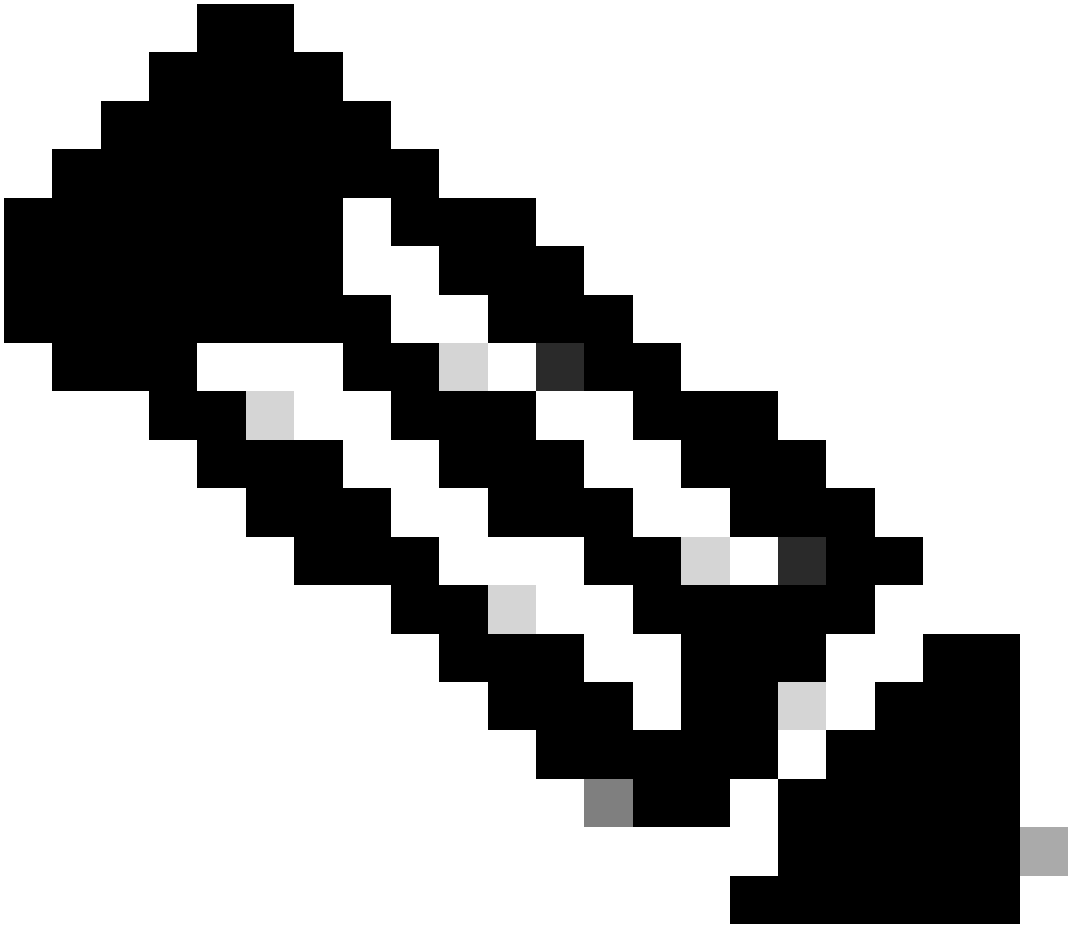
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

- Secure Firewall Thread Defense (FTD) 7.4.x, 7.6.x. managed by the Secure Firewall Device Manager (FDM) or Secure Firewall Management Center (FMC).

Background Information

After software upgrade to versions 7.4.x or 7.6.x you can notice changes related to the management interface IP address:



Note: The outputs in this article are relevant to FMC-managed FTDs when the manager access interface is **not** a data interface and FDM-managed FTDs when the "Use Unique Gateways for the Management Interface" option is **not** configured.
In cases when a data interface is used for the manager access, some details such as the management traffic path or the **show network** command output differ.

Refer to the section "Change the Manager Access Interface from Management to Data" in the Chapter: Device Settings in Cisco Secure Firewall Management Center Device Configuration Guide, 7.6 and the section "Configure the Management Interface" in the Chapter: Interfaces in Cisco Secure Firewall Device Manager Configuration Guide, Version 7.6.

---

1. The IP address is **203.0.113.x**, although it was not manually configured. This is an example output

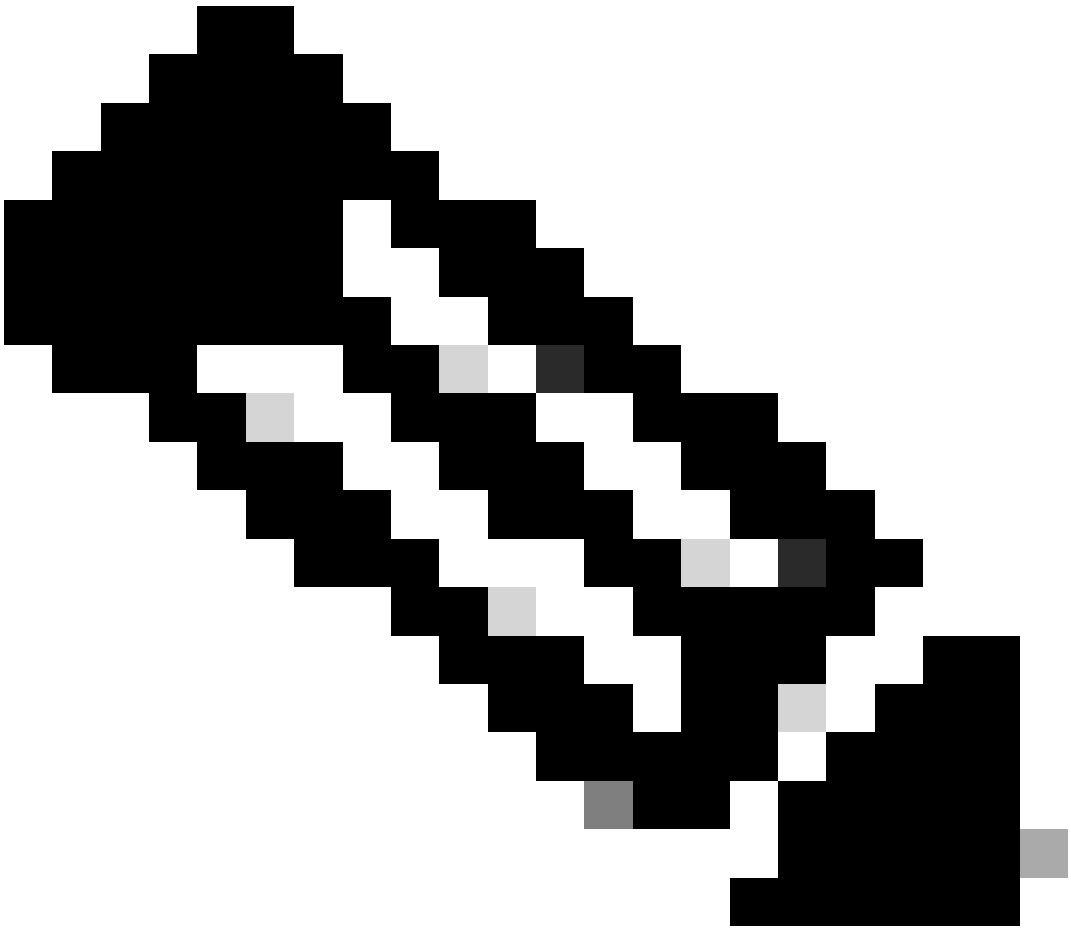
from FTD running on all platforms except Firepower 4100/9300:

```
<#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
```

The management interface of FTD running on 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
```



Note: On Firepower 4100/9300, you can create a dedicated Ethernetx/y as a custom management interface for applications, therefore the physical interface name is **Ethernetx/y**, not **Managementx/y**.

---

2. This IP address is different than the IP address shown in the output of the **show network** command:

<#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
```

The IP address **203.0.113.x** is assigned to the management interface as part of the converged management interface feature (CMI) introduced in the version 7.4.0. Specifically, after software upgrade to version 7.4.x or later, the software proposes merging the management and diagnostic interfaces as shown in the Merge the Management and Diagnostic Interfaces section. If the merge is successful, the management interface nameif becomes **management** and is **automatically** assigned **internal** IP address **203.0.113.x.**

Management Traffic Path in Converged Management Interface Deployments

The IP address **203.0.113.x** is used to provide management connectivity from the Lina engine and to external management networks via the chassis management0 interface as follows. This connectivity is essential in cases when you configure Lina services like syslog, Domain Name Resolution (DNS) resolution, access to the authentication, authorization and accounting servers (AAA) and so on.

This diagram shows high-level overview of the management traffic path from the Lina engine to the external management network:

Key points:

1. The IP address **203.0.113.x** with the **/29** netmask is configured under the interface with the nameif **management**. But this configuration is not visible in the **show run interface** command output:

```
<#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
```

The default gateway **203.0.113.129** network is configured under in the management routing table. This default route is not visible in the output of the **show route management-only** command without arguments. You can verify the route by specifying the address 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. The IP address 203.0.113.129 is configured on the Linux side and visible in the expert mode and assigned to an internal interface, for example, **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, the chassis management IP address is assigned to the **management0** interface. This is the IP address visible in the output of the **show network** command:

<#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. There is dynamic port address translation (PAT) on the management0 interface that translates the source IP address to the management0 interface IP address. Dynamic PAT is achieved by configuring an iptables rule with the **MASQUERADE** action on the management0 interface:

```
<#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
```

Verification

In this example, CMI is enabled and in the platform settings DNS resolution via the management interface is configured:

```
<#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
```

The packet captures are configured on the Lina management, Linux tap_M0 and management0 interfaces:

```
<#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
```

An ICMP echo request to a sample fully qualified domain name (FQDN) generates a DNS request from the Lina engine. The packet capture in the Lina engine and the Linux tap_M0 interface shows initiator IP address **203.0.113.130**, which is the management interface CMI IP address:

```
<#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)
```

The packet captures on the management0 interface show the IP address of the management0 interface as the initiator IP address. This is due to dynamic PAT mentioned in the section "**Management Traffic Path in Converged Management Interface Deployments":**

<#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

If CMI is enabled, the IP address **203.0.113.x** is **automatically** assigned and **internally** used by the software to provide connectivity between the Lina engine and the external management network. You can ignore this IP address.
The IP address shown in the output of the **show network** command remains unchanged and is the only valid IP address that you must refer to as the FTD management IP address.

References

- Merge the Management and Diagnostic Interfaces
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.6
- Cisco Secure Firewall Device Manager Configuration Guide, Version 7.6