阐明FTD管理接口的IP地址203.0.113.x的用途

目录

简介

本文档介绍在安全防火墙威胁防御(FTD)中的几个命令输出中显示的IP地址203.0 .113.x。

先决条件

要求

基本的产品知识。

使用的组件

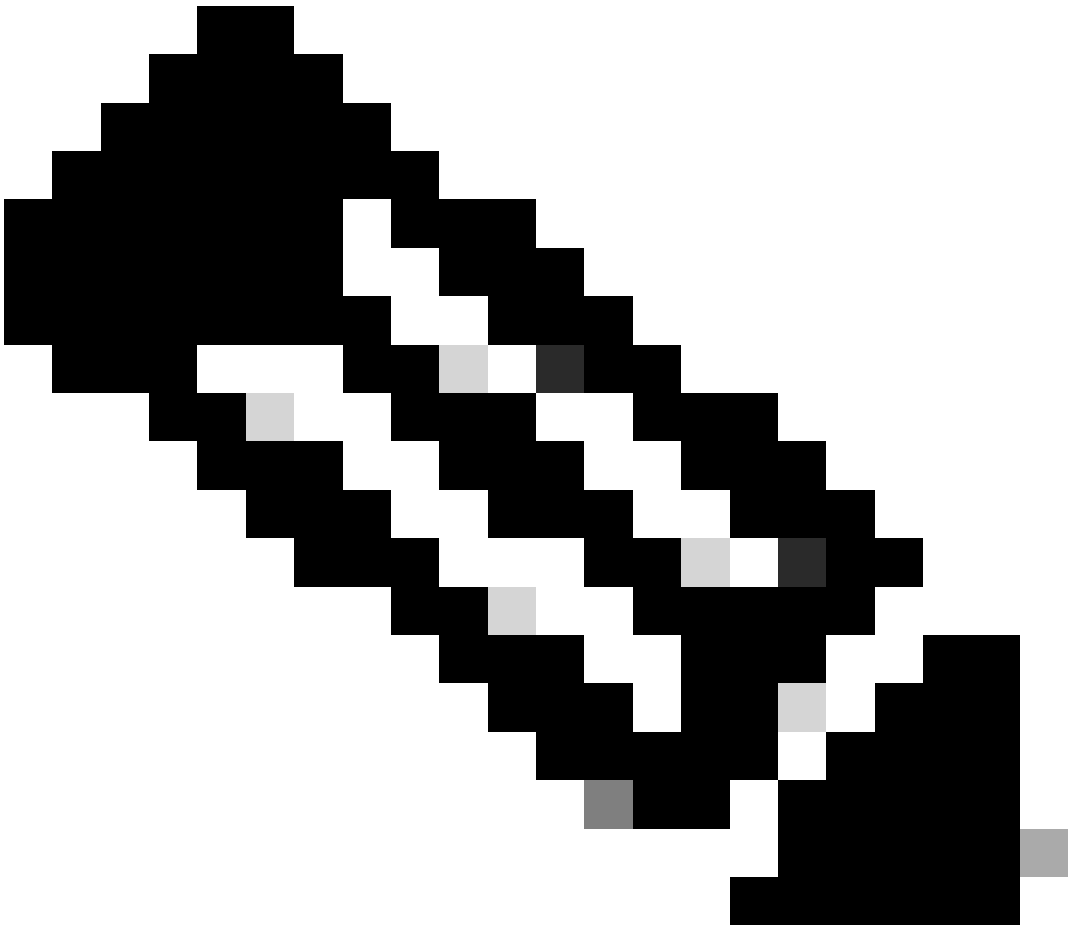
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙线程防御(FTD)7.4.x、7.6.x。由安全防火墙设备管理器(FDM)或安全防火墙管理中心(FMC)管理。

背景信息

软件升级到版本7.4.x或7.6.x后，您可以注意到与管理接口IP地址相关的更改：



注意：当管理器访问接口不是数据接口时，本文中的输出与FMC管理的FTD相关；当未配置“将唯一网关用于管理接口”选项时，与FDM管理的FTD相关。
当数据接口用于管理器访问时，一些详细信息(例如管理流量路径或show network命令输出)会有所不同。

请参阅本章中的“将Manager访问接口从管理更改为数据”部分：Cisco Secure Firewall Management Center Device Configuration Guide， 7.6 and the section "Configure the Management Interface"中的Device Settings:Cisco安全防火墙设备管理器配置指南7.6版中的接口。

1. IP地址为203.0.113.x，但并未手动配置。以下是在除Firepower 4100/9300之外的所有平台上

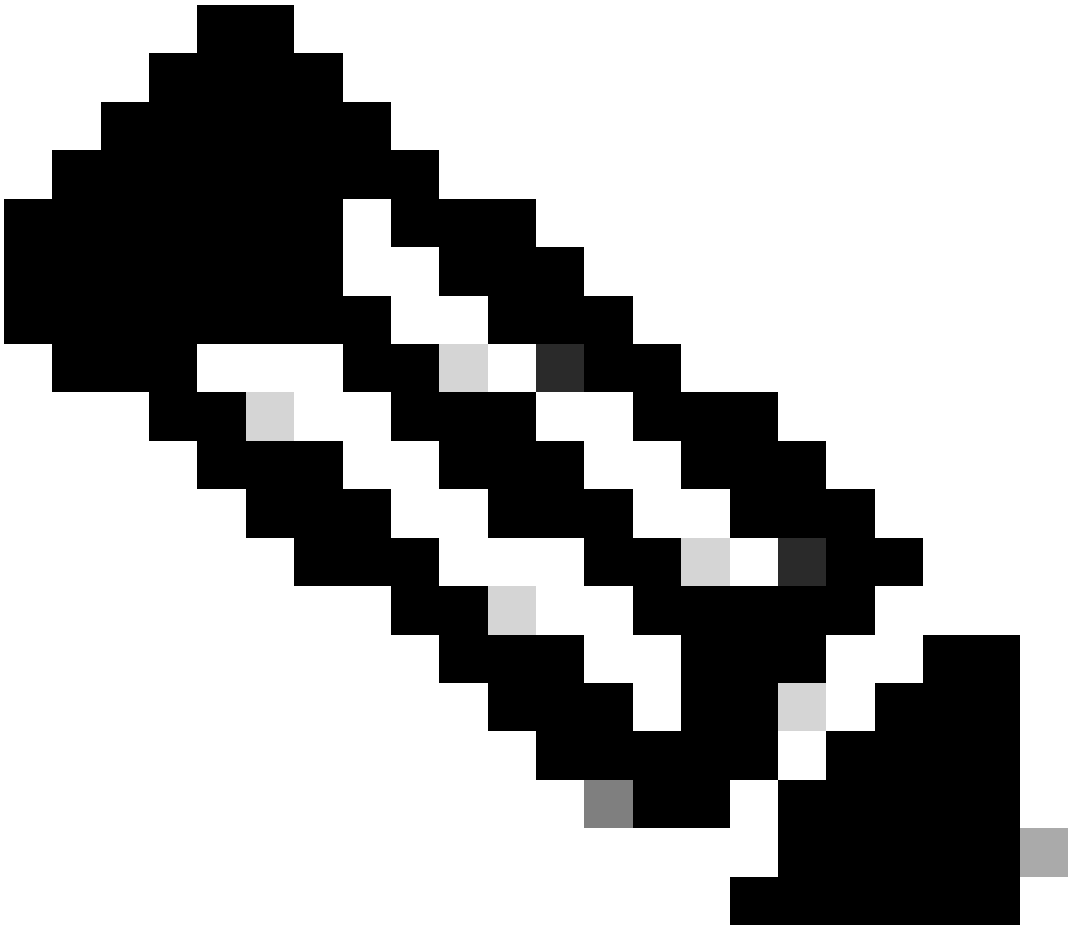
运行的FTD的示例输出：

```
<#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
```

在Firepower 4100/9300上运行的FTD的管理接口：

```
<#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
```



注意：在Firepower 4100/9300上，您可以创建专用Ethernetx/y作为应用的自定义管理接口，因此物理接口名称为Ethernetx/y，而不是Managementx/y。

---

2. 此IP地址与show network命令输出中显示的IP地址不同：

<#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
```

IP地址203.0.113.x作为版本7.4.0中引入的融合管理接口功能(CMI)的一部分分配给管理接口。具体而言，在软件升级到版本7.4.x或更高版本后，软件建议合并管理和诊断接口，如合并管理和诊断接口部分所示。如果合并成功，管理接口名称if将变为management并自动分配内部IP地址203.0.113.x。

融合管理接口部署中的管理流量路径

IP地址203.0.113.x用于提供从Lina引擎以及通过机箱管理0接口到外部管理网络的管理连接，如下所示。当您配置Lina服务(如系统日志、域名解析(DNS)解析、身份验证、授权和记帐服务器(AAA)访问等)时，此连接至关重要。

下图显示了从Lina引擎到外部管理网络的管理流量路径的概要信息：

关键点

1. 使用/29网络掩码的IP地址203.0.113.x在带有nameif management的接口下配置。但是，此配

置在show run interface 命令输出中不可见：

```
<#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
```

默认网关203.0.113.129网络在管理路由表中进行配置。不带参数的show route management-only命令的输出中看不到此默认路由。您可以通过指定地址0.0.0.0来验证路由：

```
<#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. IP地址203.0.113.129配置在Linux端，在专家模式下可见，并分配给内部接口，例如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.在Linux中，机箱管理IP地址被分配给management0接口。这是show network命令输出中可见的IP地址：

<#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. management0接口上有动态端口地址转换(PAT)，可将源IP地址转换为management0接口IP地址。通过在管理接口0上使用MASQUERADE操作配置iptables规则来实现动态PAT:

```
<#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
```

确认

在本示例中，CMI已启用，并且在平台设置中通过管理接口配置DNS解析：

```
<#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
```

数据包捕获在Lina管理、Linux tap_M0和management0接口上配置：

```
<#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
```

对示例完全限定域名(FQDN)的ICMP回应请求会从Lina引擎生成DNS请求。Lina引擎和Linux tap_M0接口中的数据包捕获显示启动器IP地址203.0.113.130，该地址是管理接口CMI IP地址：

```
<#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)
```

management0接口上的数据包捕获将management0接口的IP地址显示为发起方IP地址。这是因为“融合管理接口部署中的管理流量路径”一节中提到的动态PAT:

```
<#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)
```

结论

如果启用CMI，软件会自动分配IP地址203.0.113.x并在内部使用该地址，以提供Lina引擎和外部管理网络之间的连接。您可以忽略此IP地址。
show network命令输出中显示的IP地址保持不变，并且是唯一有效的IP地址，您必须将其称为FTD管理IP地址。

参考

- 合并管理和诊断接口
- 思科安全防火墙管理中心设备配置指南，7.6
- 思科安全防火墙设备管理器配置指南，版本7.6

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。