闡明FTD管理介面IP位址203.0.113.x的用途

目錄

簡介

必要條件

需求

採用元件

背景資訊

融合管理介面部署中的管理流量路徑

驗證

結論

參考資料

簡介

本檔案介紹IP位址203.0 .113.x，顯示在安全防火牆威脅防禦(FTD)中幾個指令的輸出中。

必要條件

需求

基本產品知識。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆執行緒防禦(FTD)7.4.x、7.6.x。由安全防火牆裝置管理器(FDM)或安全防火牆管理中心(FMC)管理。

背景資訊

軟體升級到7.4.x或7.6.x版後，您可以注意到與管理介面IP地址相關的更改：

附註：當管理器訪問介面不是資料介面時，本文中的輸出與FMC管理的FTD相關；當未配置「將唯一網關用於管理介面」選項時，此輸出與FDM管理的FTD相關。
在資料介面用於管理器訪問時，某些詳細資訊(如管理流量路徑或show network命令輸出)會有所不同。

請參閱一章中的「將Manager訪問介面從管理更改為資料」部分：Cisco Secure Firewall Management Center Device Configuration Guide， 7.6 and the Section "Configure the Management Interface" in Cisco Secure Firewall Management Center Device Configuration Guide， 7.6 and the Chapter:思科安全防火牆裝置管理器配置指南7.6版中的介面。

1. IP地址是203.0.113.x，但並未手動配置。以下是在除Firepower 4100/9300以外的所有平台上運行的FTD的範例輸出：

<#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上運行的FTD管理介面：

<#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
```

附註：在Firepower 4100/9300上，您可以建立一個專用的Ethernetx/y作為應用程式的自定義管理介面，因此物理介面名稱為Ethernetx/y，而不是Managementx/y。

2. 此IP位址與show network命令輸出中所示的IP位址不同：

<#root>

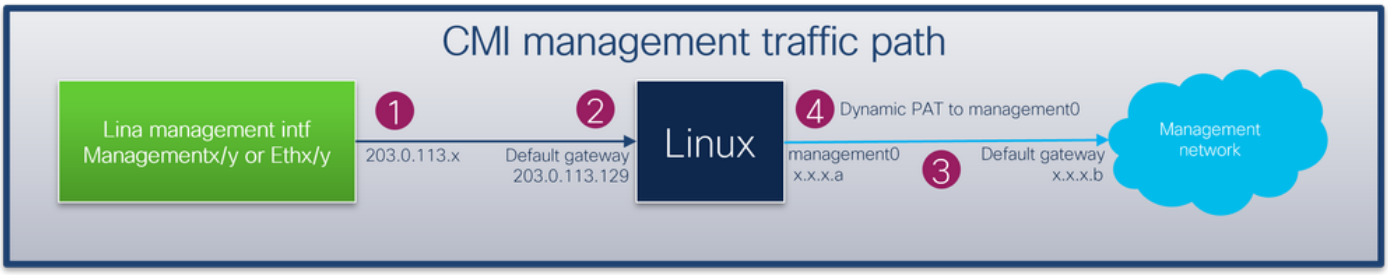
```
>

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作為7.4.0版中引入的聚合管理介面功能(CMI)的一部分分配給管理介面。具體來說，在軟體升級到版本7.4.x或更高版本後，軟體建議合併管理和診斷介面，如合併管理和診斷介面部分所示。如果合併成功，管理介面nameif將變成management，並自動分配內部IP地址203.0.113.x。

融合管理介面部署中的管理流量路徑

IP地址203.0.113.x用於通過chassis management0介面提供從Lina引擎到外部管理網路的管理連線，如下所示。當您設定Lina服務(例如系統日誌、網域名稱解析(DNS)解析、存取驗證、授權及計費伺服器(AAA)等時，這種連線是必不可少的。

此圖顯示從Lina引擎到外部管理網路的管理流量路徑的簡要概觀：



重點：

1. 使用/29網路掩碼的IP地址203.0.113.x在介面下配置nameif management。但是此組態無法在

show run interface 指令輸出中看到：

<#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
```

預設網關203.0.113.129網路在管理路由表中配置。不帶引數的show route management-only命令的輸出中看不到此預設路由。您可以通過指定地址0.0.0.0來驗證路由：

<#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，在專家模式下可見，並分配給內部介面，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，機箱管理IP地址被分配給management0接口。這是show network命令輸出中可見的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介面上有動態埠地址轉換(PAT)，可將源IP地址轉換為管理介面0的IP地址。動態PAT是通過在management0介面上使用MASQUERADE操作配置iptables規則實現的：

<#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
```

驗證

在此示例中，啟用CMI，並在平台設定中配置通過管理介面的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
```

封包擷取是在Lina管理、Linux tap_M0和management0介面上設定的：

<#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
```

對樣本完全限定域名(FQDN)的ICMP回應請求會從Lina引擎生成DNS請求。Lina引擎和Linux tap_M0介面中的資料包捕獲顯示啟動器IP地址203.0.113.130，這是管理介面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介面上的資料包捕獲將management0介面的IP地址顯示為啟動器IP地址。這是因為在「融合管理介面部署中的管理流量路徑」一節中提到的動態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)
```

結論

如果啟用CMI，則軟體會自動分配IP地址203.0.113.x，並在內部使用，以提供Lina引擎和外部管理網路之間的連線。您可以忽略此IP地址。
show network命令輸出中顯示的IP位址會保持不變，而且是您必須稱為FTD管理IP位址的唯一有效IP位址。

參考資料

- 合併管理和診斷介面
- 思科安全防火牆管理中心裝置配置指南7.6
- 思科安全防火牆裝置管理器配置指南7.6版

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。