FTD管理インターフェイスのIPアドレス203.0.113.xの目的の明確化

内容

はじめに

このドキュメントでは、Secure Firewall Threat Defense(FTD)のいくつかのコマンドの出力に表示されるIPアドレス203.0 .113.xについて説明します。

前提条件

要件

製品の基礎知識

使用するコンポーネント

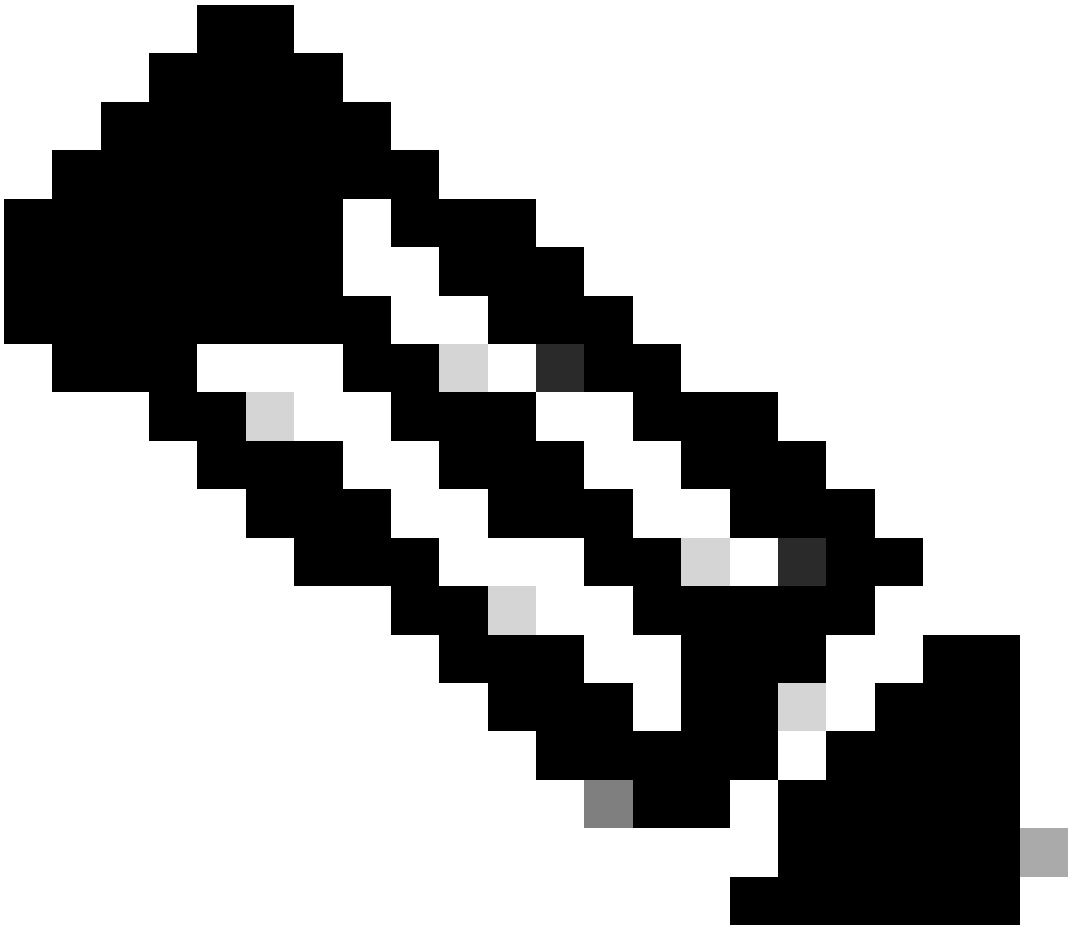
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Firewall Thread Defense(FTD)7.4.x、7.6.x。Secure Firewall Device Manager(FDM)またはSecure Firewall Management Center(FMC)で管理されます。

背景説明

バージョン7.4.xまたは7.6.xにソフトウェアをアップグレードした後で、管理インターフェイスのIPアドレスに関連する変更に気付く場合があります。



注意：この記事の出力は、マネージャ・アクセス・インタフェースがデータ・インタフェースでない場合はFMCで管理されるFTDに関連し、「管理インタフェースに一意のゲートウェイを使用」オプションが構成されていない場合はFDMで管理されるFTDに関連します。
マネージャアクセスにデータインターフェイスが使用されている場合、管理トラフィックパスやshow networkコマンドの出力などの詳細情報が異なります。

Cisco Secure Firewall Management Center Device Configuration Guide, 7.6の章「Device Settings」の「Change the Manager Access Interface from Management to Data」の項、およびCisco Secure Firewall Device Manager Configuration Guide, Version 7.6の章「Interfaces」の「Configure the Management Interface」の項を参照してください。

1. IPアドレスは203.0.113.xですが、手動で設定されていません。次に、Firepower 4100/9300以外のすべてのプラットフォームで実行されているFTDからの出力例を示します。

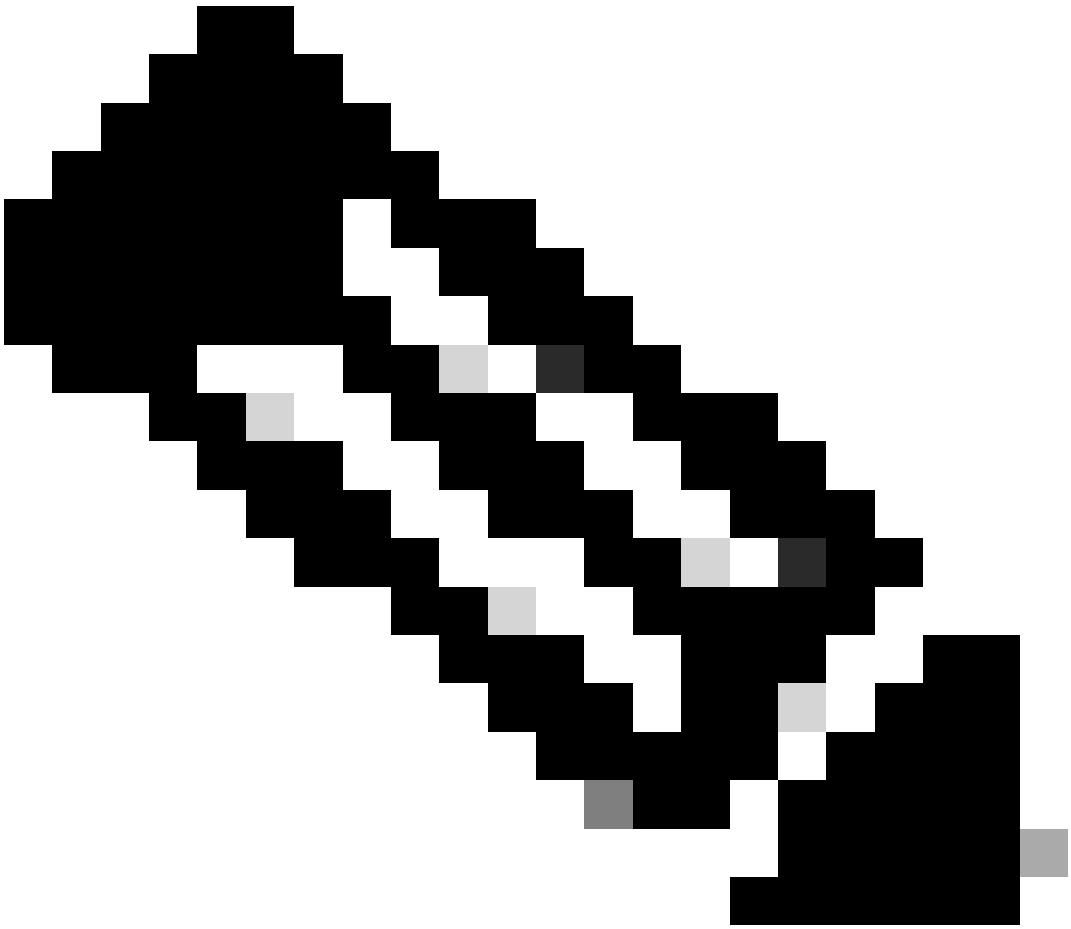
```
<#root>

>

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
```

Firepower 4100/9300で動作するFTDの管理インターフェイスは次のとおりです。

```
<#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:Firepower 4100/9300では、専用のEthernetx/yをアプリケーション用のカスタム管理インターフェイスとして作成できます。したがって、物理インターフェイスの名前はEthernetx/yであり、Managementx/yではありません。

---

2. このIPアドレスは、show networkコマンドの出力に表示されるIPアドレスとは異なります。

```
<#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アドレス203.0.113.xは、バージョン7.4.0で導入された統合管理インターフェイス(CMI)機能の一部として管理インターフェイスに割り当てられます。特に、バージョン7.4.x以降へのソフトウェアアップグレード後は、「管理および診断インターフェイスのマージ」セクションに示されているように、ソフトウェアによって管理および診断インターフェイスのマージが提案されます。マージが成功すると、「管理インターフェイス」nameifは管理になり、自動的に内部IPアドレス203.0.113.xが割り当てられます。

統合管理インターフェイス展開での管理トラフィックパス

IPアドレス203.0.113.xは、次のように、Linaエンジンから外部管理ネットワークへの、シャーシ管理0インターフェイスを介した管理接続を提供するために使用されます。この接続は、syslog、ドメイン名解決(DNS)解決、認証、許可、およびアカウンティング(AAA)サーバへのアクセスなどのLinaサービスを設定する場合に不可欠です。

次の図は、Linaエンジンから外部管理ネットワークへの管理トラフィックパスの概要を示しています。

キー ポイント：

1. IPアドレス203.0.113.x(/29ネットマスク付き)は、nameif managementを使用してインターフェイスで設定されます。ただし、この設定は、show run interface コマンドの出力には表示されません。

```
<#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
```

デフォルトゲートウェイの203.0.113.129ネットワークは、管理ルーティングテーブルの下で設定されます。このデフォルトルートは、引数を指定しない場合、show route management-onlyコマ

ンドの出力では表示されません。アドレス0.0.0.0を指定して、ルートを確認できます。

```
<#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アドレス203.0.113.129がLinux側で設定され、expertモードで表示され、内部インターフェイス(tap_M0:など)に割り当てられます。

<#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. Linuxでは、シャーシ管理IPアドレスはmanagement0インターフェイスに割り当てられます。これは、show networkコマンドの出力に表示されるIPアドレスです。

<#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. 送信元IPアドレスを管理0インターフェイスのIPアドレスに変換する、管理0インターフェイス上のダイナミックポートアドレス変換(PAT)が存在する。ダイナミックPATを実現するには、management0インターフェイスでMASQUERADEアクションを使用してiptablesルールを設定します。

```
<#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
```

検証

この例では、CMIが有効になっており、プラットフォーム設定で管理インターフェイスを介したDNS解決が設定されています。

<#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

パケットキャプチャは、Lina管理、Linux tap_M0、およびmanagement0インターフェイスで設定されます。

<#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
```

サンプルの完全修飾ドメイン名(FQDN)へのICMPエコー要求は、Linaエンジンから DNS要求を生成します。LinaエンジンおよびLinux tap_M0インターフェイスのパケットキャプチャは、管理インターフェイスCMI IPアドレスであるイニシエータIPアドレス203.0.113.130を示しています。

<#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インターフェイス上のパケットキャプチャは、management0インターフェイスのIPアドレスをイニシエータIPアドレスとして示します。これは、「統合管理インターフェイスの導入における管理トラフィックパス」の項で説明したダイナミックPATが原因です。

```
<#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

CMIがイネーブルの場合、IPアドレス203.0.113.xが自動的に割り当てられ、ソフトウェアによって内部的に使用されて、Linaエンジンと外部管理ネットワーク間の接続が提供されます。このIPアドレスは無視してかまいません。
show networkコマンドの出力に示されるIPアドレスは変更されず、FTD管理IPアドレスとして参

照する必要がある唯一の有効なIPアドレスになります。

参考資料

- 管理インターフェイスと診断インターフェイスのマージ
- Cisco Secure Firewall Management Centerデバイス設定ガイド、7.6
- Cisco Secure Firewall Device Managerコンフィギュレーションガイド、バージョン7.6

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。