FTD 관리 인터페이스에 대한 IP 주소 203.0.113.x의 용도 이해

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[배경 정보](#)

[통합 관리 인터페이스 구축의 관리 트래픽 경로](#)

[확인](#)

[결론](#)

[참조](#)

소개

이 문서에서는 FTD(Secure Firewall Threat Defense)의 몇 가지 명령 출력에 표시된 IP 주소 203.0.113.x에 대해 설명합니다.

사전 요구 사항

요구 사항

기본 제품 지식

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

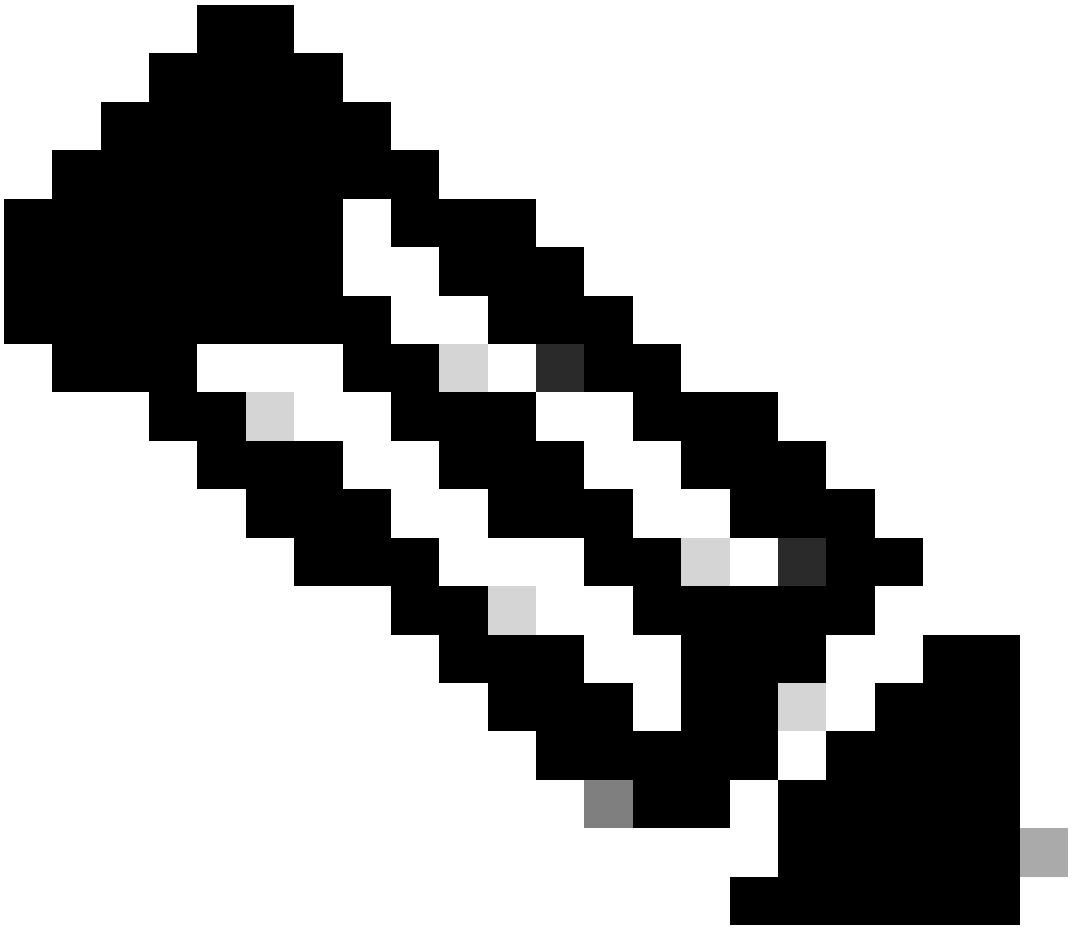
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD(Secure Firewall Thread Defense) 7.4.x, 7.6.x FDM(Secure Firewall Device Manager) 또

는 FMC(Secure Firewall Management Center)에서 관리됩니다.

배경 정보

버전 7.4.x 또는 7.6.x로 소프트웨어를 업그레이드한 후 관리 인터페이스 IP 주소와 관련된 변경 사항을 확인할 수 있습니다.



참고: 이 문서의 출력은 관리자 액세스 인터페이스가 데이터 인터페이스가 아닌 경우의 FMC 관리 FTD와 "관리 인터페이스에 고유 게이트웨이 사용" 옵션이 구성되지 않은 경우의 FDM 관리 FTD와 관련됩니다.
데이터 인터페이스가 관리자 액세스에 사용되는 경우 관리 트래픽 경로 또는 show network 명령 출력과 같은 일부 세부 정보가 다릅니다.

다음 장의 "관리자 액세스 인터페이스를 관리에서 데이터로 변경" 섹션을 참조하십시오.

Cisco Secure Firewall Management Center Device Configuration Guide, 7.6의 Device Settings 및 다음 장의 "Configure the Management Interface" 절: Cisco Secure Firewall Device Manager 컨피그레이션 가이드, 버전 7.6의 인터페이스.

1. IP 주소는 수동으로 구성되지 않았지만 203.0.113.x입니다. firepower 4100/9300을 제외한 모든 플랫폼에서 실행되는 FTD의 출력 예입니다.

```
<#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 4100/9300에서 실행되는 FTD의 관리 인터페이스:

<#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

…

>

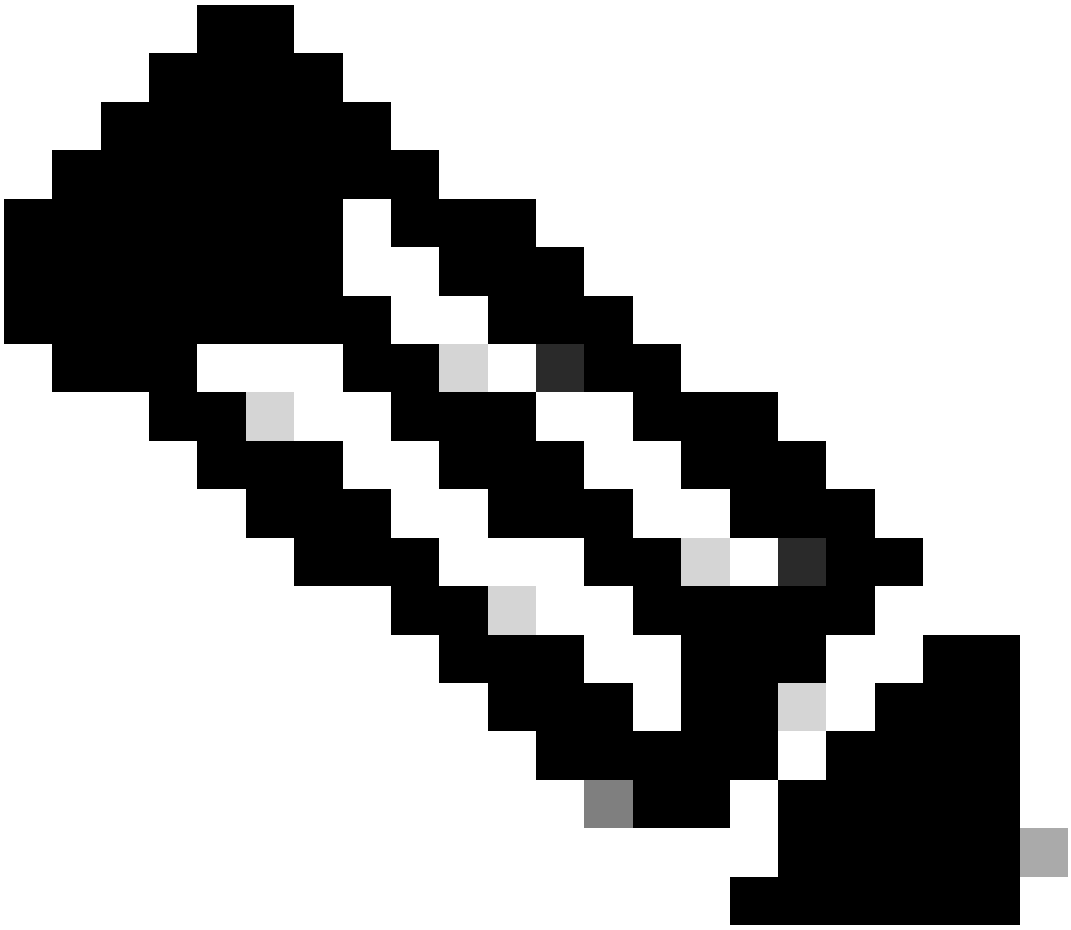
show running-config interface Ethernet 1/1

interface Ethernet1/1

```
management-only

nameif management


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



참고: Firepower 4100/9300에서 전용 Ethernetx/y를 애플리케이션의 사용자 지정 관리 인터페이스로 생성할 수 있으므로 물리적 인터페이스 이름은 Managementx/y가 아니라 Ethernetx/y입니다.

---

2. 이 IP 주소는 show network 명령 출력에 표시된 IP 주소와 다릅니다.

<#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 주소 203.0.113.x는 버전 7.4.0에 도입된 통합 관리 인터페이스 기능(CMI)의 일부로 관리 인터페이스에 할당됩니다. 특히, 소프트웨어를 버전 7.4.x 이상으로 업그레이드한 후 소프트웨어는 관리 및 진단 인터페이스 병합 섹션에 표시된 대로 관리 및 진단 인터페이스 병합을 제안합니다. 병합에 성공하면 관리 인터페이스 nameif가 관리가 되고 내부 IP 주소 203.0.113.x가 자동으로 할당됩니다.

통합 관리 인터페이스 구축의 관리 트래픽 경로

IP 주소 203.0.113.x는 다음과 같이 섀시 management0 인터페이스를 통해 Lina 엔진과 외부 관리 네트워크에 대한 관리 연결을 제공하는 데 사용됩니다. 이 연결은 syslog, DNS(Domain Name Resolution) 확인, AAA(Authentication, Authorization, Accounting Server) 액세스 등과 같은 Lina 서비스를 구성할 때 필수적입니다.

이 다이어그램은 Lina 엔진에서 외부 관리 네트워크로의 관리 트래픽 경로에 대한 개괄적인 개요를 보여줍니다.

요점:

1. /29 넷마스크를 사용하는 IP 주소 203.0.113.x는 nameif management를 사용하는 인터페이스 아래에 구성됩니다. 그러나 이 컨피그레이션은 show run interface 명령 출력에 표시되지 않습니다.

<#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
```

기본 게이트웨이 203.0.113.129 네트워크는 관리 라우팅 테이블에서 구성됩니다. 이 기본 경로는 show route management-only 명령 출력에 인수 없이 표시되지 않습니다. 주소 0.0.0.0을 지정하여 경로를 확인할 수 있습니다.

<#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 주소 203.0.113.129는 Linux 측에서 구성되며 전문가 모드에서 표시되며 내부 인터페이스(예: tap_M0)에 할당됩니다.

```
<#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. Linux에서는 섀시 관리 IP 주소가 management0 인터페이스에 할당됩니다. 다음은 show network 명령의 출력에 표시되는 IP 주소입니다.

```
<#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. 소스 IP 주소를 management0 인터페이스 IP 주소로 변환하는 동적 PAT(Port Address Translation)가 management0 인터페이스에 있습니다. 동적 PAT는 management0 인터페이스에서 MASQUERADE 작업을 사용하여 iptables 규칙을 구성하여 구현됩니다.

<#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

확인

이 예에서는 CMI가 활성화되며 플랫폼 설정에서 관리 인터페이스를 통한 DNS 확인이 구성됩니다.

<#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
```

패킷 캡처는 Lina management, Linux tap_M0 및 management0 인터페이스에 구성됩니다.

```
<#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
```

샘플 FQDN(정규화된 도메인 이름)에 대한 ICMP 에코 요청은 Lina 엔진에서 DNS 요청을 생성합니다. Lina 엔진 및 Linux tap_M0 인터페이스의 패킷 캡처는 개시자 IP 주소 203.0.113.130을 보여주며, 이는 관리 인터페이스 CMI IP 주소입니다.

```
<#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 인터페이스에서 캡처되는 패킷은 management0 인터페이스의 IP 주소를 개시자 IP 주소로 표시합니다. 이는 "Management Traffic Path in Converged Management Interface Deployments" 섹션에 언급된 동적 PAT 때문입니다.

<#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)
```

결론

CMI가 활성화된 경우 IP 주소 203.0.113.x가 자동으로 할당되고 소프트웨어에서 내부적으로 사용되어 Lina 엔진과 외부 관리 네트워크 간의 연결을 제공합니다. 이 IP 주소를 무시할 수 있습니다. show network 명령의 출력에 표시된 IP 주소는 변경되지 않으며 FTD 관리 IP 주소라고 참조해야 하는 유일한 유효한 IP 주소입니다.

참조

- 관리 및 진단 인터페이스 병합
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.6
- Cisco Secure Firewall Device Manager 컨피그레이션 가이드, 버전 7.6

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.