Het doel van IP-adres 203.0.13.x voor de FTD-beheerinterface verduidelijken

Inhoud

Inleiding

Dit document beschrijft het IP-adres 203.0 .113.x dat wordt weergegeven in de uitvoer van een aantal opdrachten in de Secure Firewall Threat Defence (FTD).

Voorwaarden

Vereisten

Basisproductkennis.

Gebruikte componenten

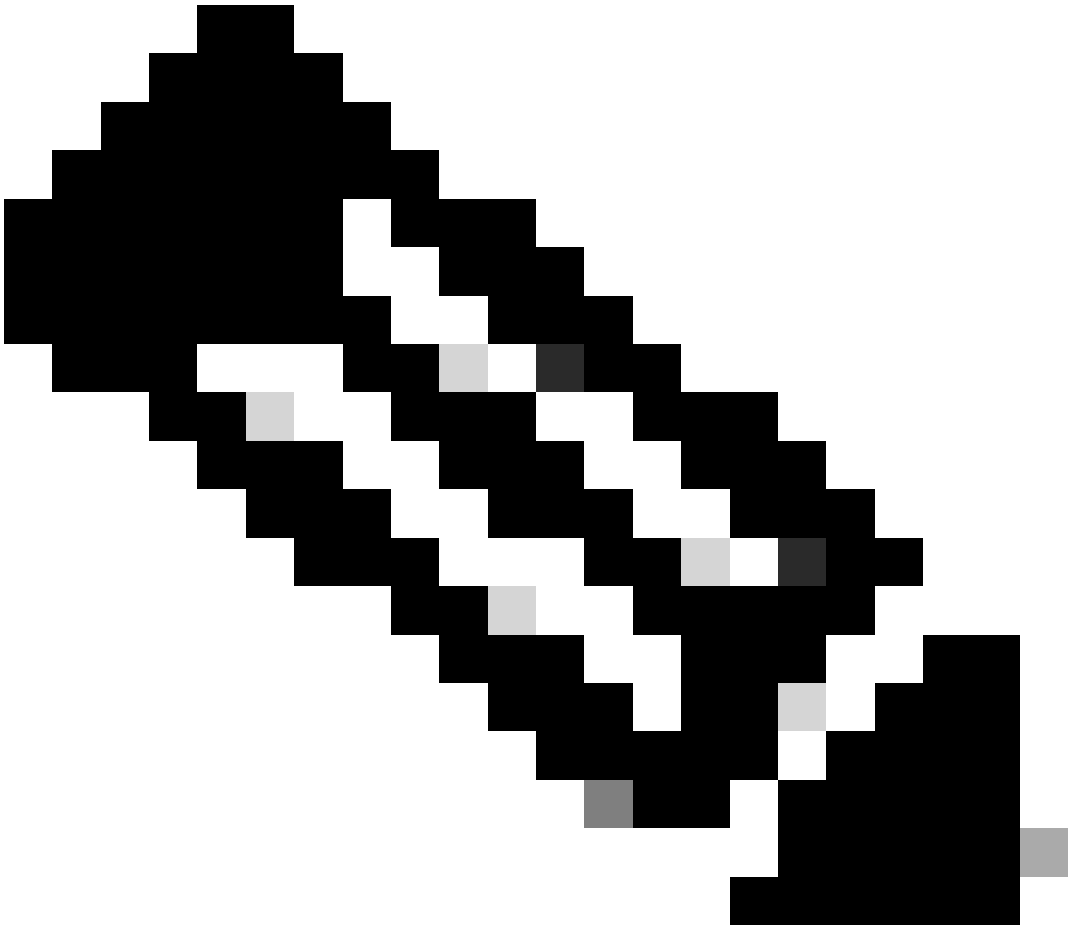
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall Thread Defence (FTD) 7.4.x, 7.6.x. beheerd door Secure Firewall Device Manager (FDM) of Secure Firewall Management Center (FMC).

Achtergrondinformatie

Na software upgrade naar versies 7.4.x of 7.6.x kunt u wijzigingen met betrekking tot de beheerinterface IP-adres:



Opmerking: De outputs in dit artikel zijn relevant voor FTD's die door het FMC worden beheerd wanneer de toegangsinterface van de beheerder geen gegeveninterface is en FDM-beheerde FTD's wanneer de optie "Gebruik unieke gateways voor de beheerinterface" niet geconfigureerd is.
In gevallen waarin een gegevensinterface wordt gebruikt voor de beheerderstoegang, verschillen sommige details zoals het pad van het beheerverkeer of de opdrachtoutput

---

van het shownetwerk.

Raadpleeg het gedeelte "De Manager Access Interface van beheer naar gegevens wijzigen" in het hoofdstuk: Apparaatinstellingen in Cisco Secure Firewall Management Center Configuratiehandleiding voor apparaten, 7.6 en de sectie "De beheerinterface configureren" in het hoofdstuk: Interfaces in de configuratiehandleiding voor Cisco Secure Firewall Device Manager, versie 7.6.

---

1. Het IP-adres is 203.0.113.x, hoewel het niet handmatig is ingesteld. Dit is een voorbeelduitvoer van FTD die op alle platforms behalve Firepower 4100/9300 loopt:

```
<#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
```

De beheerinterface van FTD met 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


…


>
```

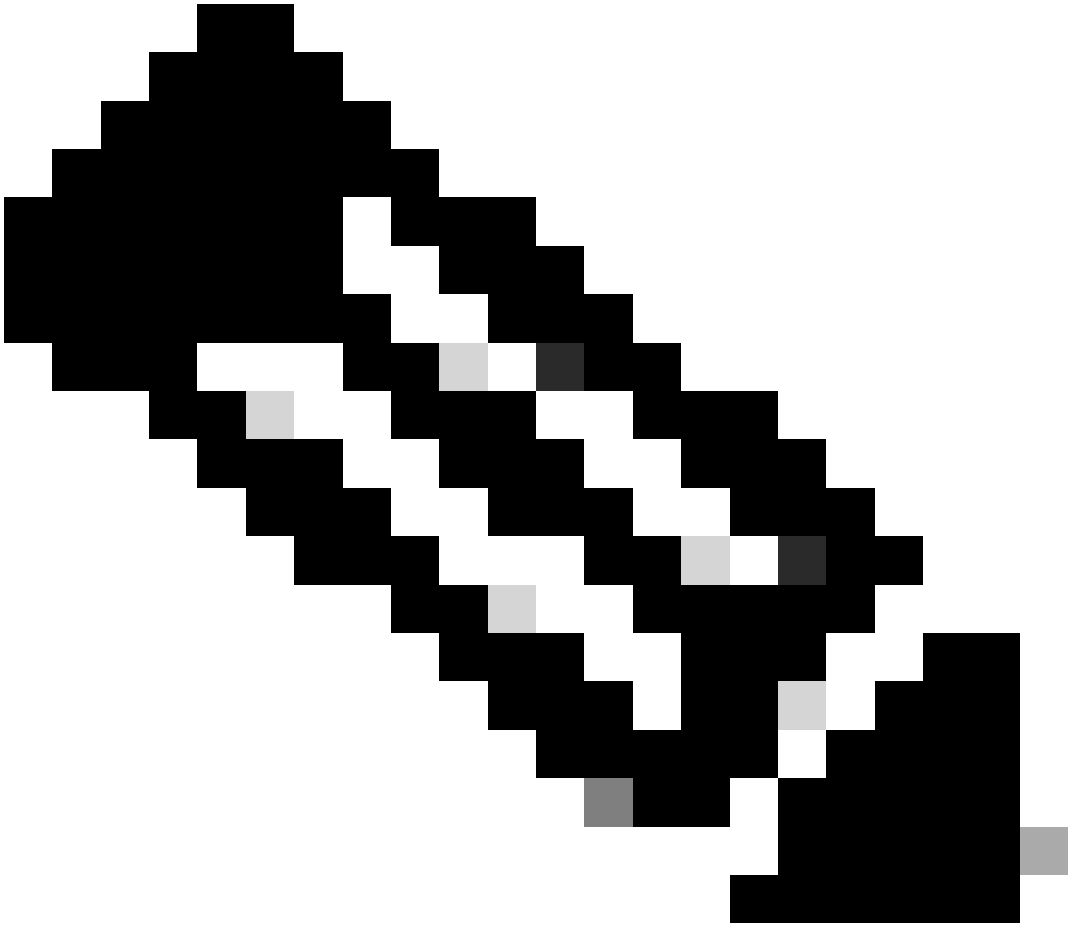
```
show running-config interface Ethernet 1/1


interface Ethernet1/1


 management-only

 nameif management


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



Opmerking: Op Firepower 4100/9300 kunt u een speciale Ethernet/y aanmaken als een aangepaste beheerinterface voor toepassingen. De fysieke interfacenaam is daarom Ethernet/y, niet ManagementX/y.

---

2. Dit IP-adres is anders dan het IP-adres dat in de uitvoer van de opdracht netwerk tonen wordt weergegeven:

<#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
```

Het IP-adres 203.0.113.x wordt aan de beheerinterface toegewezen als onderdeel van de geconvergeerde beheerinterface (CMI), die in versie 7.4.0 is geïntroduceerd. Meer bepaald stelt de software na een upgrade van de software naar versie 7.4.x of hoger voor om de beheers- en diagnostische interfaces samen te voegen, zoals in de sectie Beheer en diagnostische interfaces samenvoegen. Als de fusie succesvol is, wordt de naam van de beheerinterface beheer en wordt automatisch toegewezen intern IP-adres 203.0.113.x.

Beheer van verkeerspad in geconvergeerde beheerinterfaceprestaties

Het IP-adres 203.0.113.x wordt als volgt gebruikt om beheerconnectiviteit van de Lina-motor en externe beheernetwerken via de chassis management0-interface te bieden. Deze connectiviteit is essentieel wanneer u Lina-services configureert zoals syslog, Domain Name Resolution (DNS), toegang tot de verificatie-, autorisatie- en accounting servers (AAA) enzovoort.

Dit diagram toont een overzicht op hoog niveau van het pad voor beheerverkeer van de Lina-motor naar het externe beheernetwerk:

Belangrijkste punten:

1. Het IP-adres 203.0.113.x met het /29-netmasker is geconfigureerd onder de interface met het nameif-beheer. Maar deze configuratie is niet zichtbaar in de opdrachtoutput van de show run interface:

```
<#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
```

Het standaardgateway 203.0.113.129-netwerk is in het kader van de beheerrouteringstabel geconfigureerd. Deze standaardroute is niet zichtbaar in de output van het bevel van de showroute beheer-slechts zonder argumenten. U kunt de route verifiëren door het adres 0.0.0.0 te specificeren:

```
<#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. Het IP-adres 203.0.113.129 wordt aan de Linux-kant geconfigureerd, zichtbaar in de expert-modus en toegewezen aan een interne interface, bijvoorbeeld 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 wordt het IP-adres voor chassisbeheer toegewezen aan de management0-interface. Dit is het IP-adres dat zichtbaar is in de uitvoer van de opdracht netwerk tonen:

<#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. Er is dynamische poortadresomzetting (PAT) op de management0-interface die het IP-bronadres vertaalt naar het IP-adres van de management0-interface. Dynamisch PAT wordt bereikt door een IPtables-regel te configureren met de actie MASQUERADE op de 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
```

Verificatie

In dit voorbeeld is CMI ingeschakeld en in de platforminstellingen wordt DNS-resolutie via de beheerinterface geconfigureerd:

```
<#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
```

De pakketopnamen worden geconfigureerd op de Lina-beheerinterfaces, Linux tap_M0 en management0:

```
<#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
```

Een ICMP-echoverzoek naar een voorbeeld van een volledig gekwalificeerde domeinnaam (FQDN) genereert een DNS-verzoek van de Lina-engine. De pakketopname in de Lina engine en de Linux tap_M0 interface toont initiator IP adres 203.0.113.130, dat is de beheerinterface CMI IP adres:

```
<#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)
```

Het pakket vangt op de management0 interface toont het IP adres van de management0 interface als initiator IP adres. Dit komt door dynamisch PAT zoals vermeld in de sectie "Management Traffic Path in Converged Management Interface implementaties":

```
<#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)
```

Conclusie

Als CMI is ingeschakeld, wordt het IP-adres 203.0.113.x automatisch toegewezen en intern door de software gebruikt om de verbinding tussen de Lina-engine en het externe beheernetwerk te verzorgen. U kunt dit IP-adres negeren.
Het IP-adres dat wordt weergegeven in de uitvoer van de opdracht netwerk tonen blijft ongewijzigd en is het enige geldige IP-adres dat u als het FTD-IP-adres voor beheer moet aanduiden.

Referenties

- De beheer- en diagnostische interfaces samenvoegen
- Handleiding voor configuratie van apparaat in Cisco Secure Firewall Management Center, 7.6
- Configuratiehandleiding voor Cisco Secure Firewall Device Manager, versie 7.6

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.