Erläutern des Zwecks der IP-Adresse 203.0.113.x für die FTD-Verwaltungsschnittstelle

Inhalt

Einleitung

In diesem Dokument wird die IP-Adresse 203.0 .113.x beschrieben, die in der Ausgabe einiger Befehle in Secure Firewall Threat Defense (FTD) angezeigt wird.

Voraussetzungen

Anforderungen

Grundlegendes Produktwissen.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

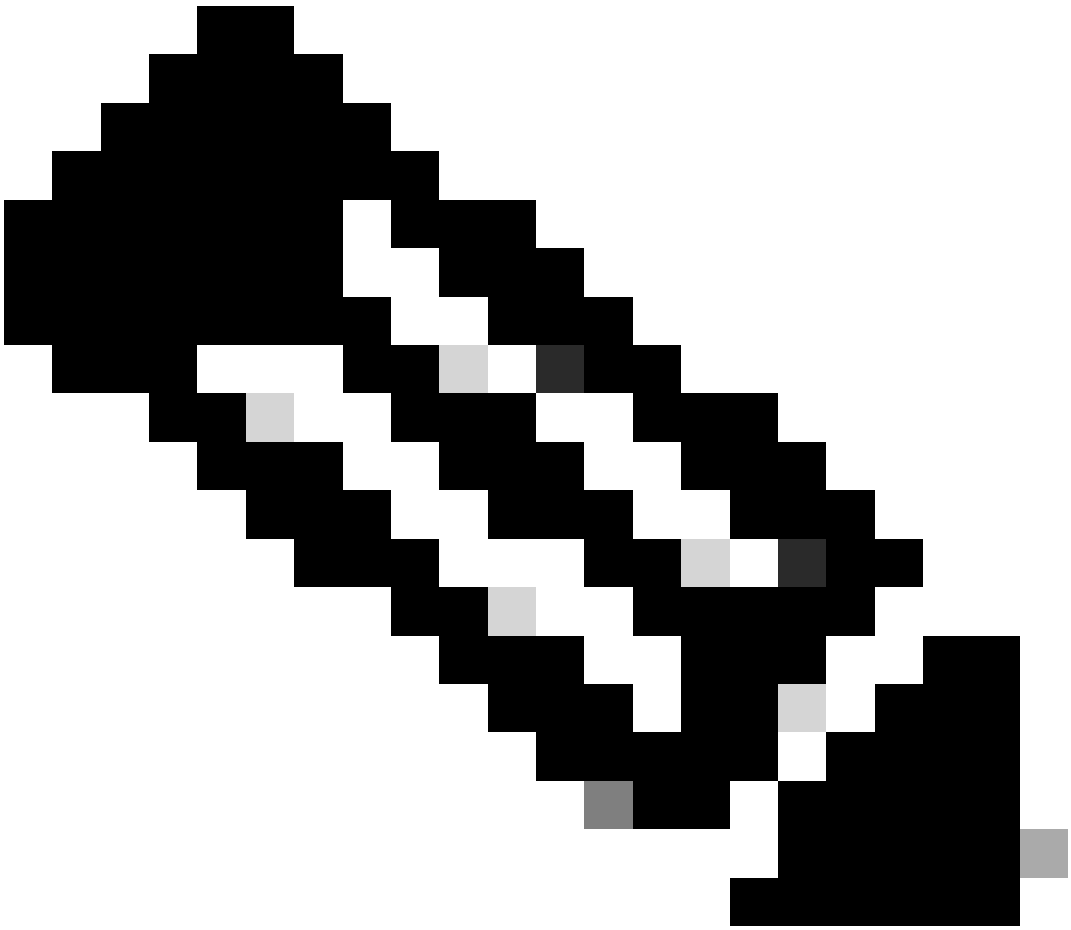
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Sicherer Firewall-Thread-Schutz (FTD) 7.4.x, 7.6.x verwaltet vom Secure Firewall Device Manager (FDM) oder Secure Firewall Management Center (FMC).

Hintergrundinformationen

Nach dem Software-Upgrade auf Version 7.4.x oder 7.6.x können Sie Änderungen in Bezug auf die IP-Adresse der Verwaltungsschnittstelle feststellen:



Anmerkung: Die Ausgaben in diesem Artikel sind für von FMC verwaltete FTDs relevant, wenn die Manager-Zugriffsschnittstelle keine Datenschnittstelle ist, und für von FDM verwaltete FTDs, wenn die Option "Use Unique Gateways for the Management Interface" (Eindeutige Gateways für die Verwaltungsschnittstelle verwenden) nicht konfiguriert ist.

Wenn eine Datenschnittstelle für den Manager-Zugriff verwendet wird, unterscheiden sich einige Details, wie der Verwaltungs-Datenverkehrspfad oder die Ausgabe des Befehls show network (Netzwerk anzeigen).

Weitere Informationen finden Sie im Abschnitt "Ändern der Manager-Zugriffsschnittstelle von "Management in Daten" im Kapitel: Geräteeinstellungen im Cisco Secure Firewall Management Center Device Configuration Guide, 7.6, und im Abschnitt "Configure the Management Interface" (Konfigurieren der Verwaltungsschnittstelle) im Kapitel: Schnittstellen im Konfigurationsleitfaden für den Cisco Secure Firewall Device Manager, Version 7.6

1. Die IP-Adresse lautet 203.0.113.x, wurde jedoch nicht manuell konfiguriert. Dies ist ein Beispiel für FTD, das auf allen Plattformen außer Firepower 4100/9300 ausgeführt wird:

```
<#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
```

Die Verwaltungsschnittstelle von FTD, die auf Firepower 4100/9300 ausgeführt wird:

```
<#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
```

…

>

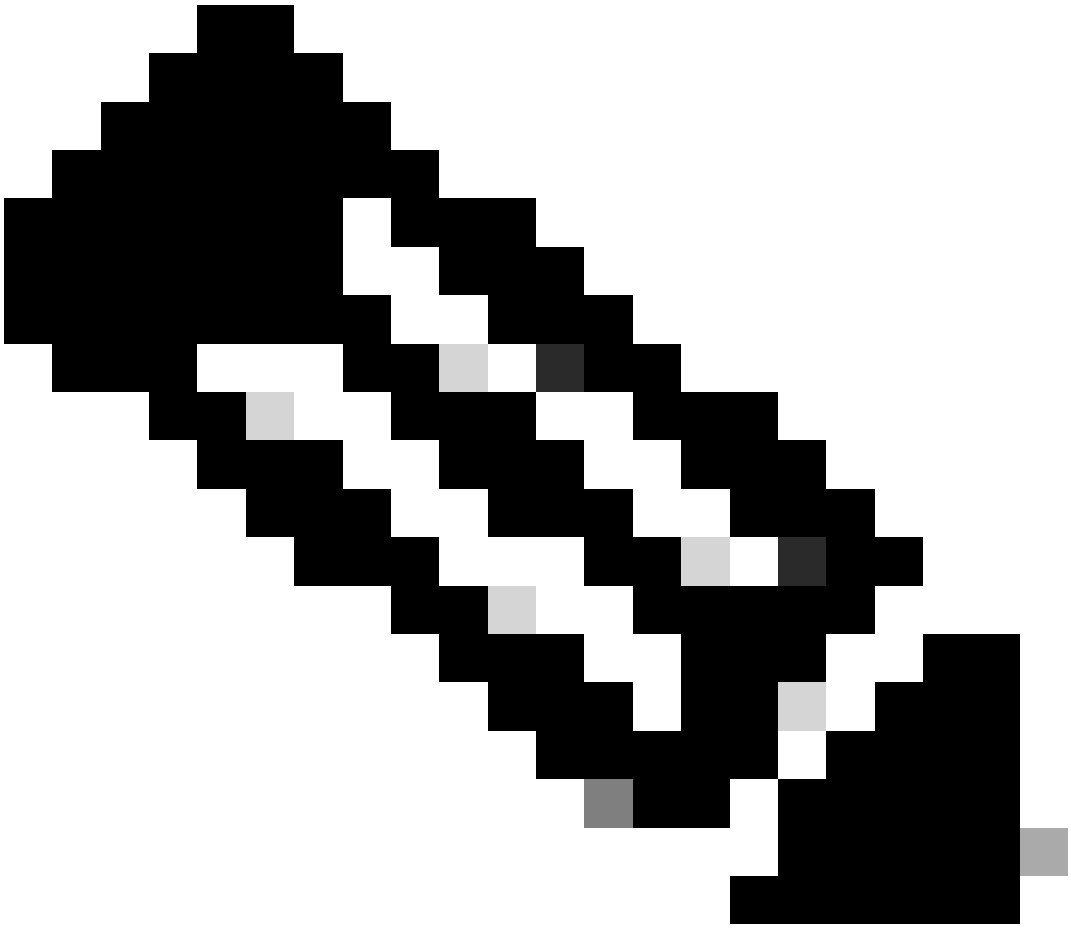
show running-config interface Ethernet 1/1

interface Ethernet1/1

 management-only

 nameif management

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



Anmerkung: Auf Firepower 4100/9300 können Sie ein dediziertes Ethernet x/y als benutzerdefinierte Management-Schnittstelle für Anwendungen erstellen. Daher lautet der Name der physischen Schnittstelle Ethernet x/y, nicht Managementx/y.

---

2. Diese IP-Adresse unterscheidet sich von der IP-Adresse, die in der Ausgabe des Befehls show network angezeigt wird:

```
<#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
```

Die IP-Adresse 203.0.113.x wird der Verwaltungsschnittstelle als Teil der in Version 7.4.0 eingeführten Funktion für konvergente Verwaltungsschnittstellen (CMI) zugewiesen. Insbesondere schlägt die Software nach dem Software-Upgrade auf Version 7.4.x oder höher das Zusammenführen der Verwaltungs- und Diagnoseschnittstellen vor, wie im Abschnitt Management- und Diagnoseschnittstellen zusammenführen dargestellt. Wenn die Zusammenführung erfolgreich ist, wird der Name der Verwaltungsschnittstelle management und die interne IP-Adresse 203.0.113.x automatisch zugewiesen.

Management-Datenverkehrspfad in konvergenten Management-Schnittstellenbereitstellungen

Die IP-Adresse 203.0.113.x wird wie folgt verwendet, um Managementverbindungen von der Lina-Engine und zu externen Managementnetzwerken über die Chassis-Management-Schnittstelle0 bereitzustellen. Diese Konnektivität ist in Fällen, in denen Sie Lina-Dienste wie Syslog, DNS-Auflösung (Domain Name Resolution), Zugriff auf die Authentifizierungs-, Autorisierungs- und Abrechnungsserver (AAA) usw. konfigurieren, unerlässlich.

Dieses Diagramm zeigt eine grobe Übersicht des Management-Datenverkehrspfads von der Lina Engine zum externen Management-Netzwerk:

Wichtigste Punkte:

1. Die IP-Adresse 203.0.113.x mit der /29-Netzmaske wird unter der Schnittstelle mit der nameif-Verwaltung konfiguriert. In der Befehlsausgabe der show run-Schnittstelle ist diese Konfiguration jedoch nicht sichtbar:

<#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
```

Das Standard-Gateway 203.0.113.129-Netzwerk wird in der Management-Routing-Tabelle unter konfiguriert. Diese Standardroute ist in der Ausgabe des Befehls show route management-only ohne Argumente nicht sichtbar. Sie können die Route überprüfen, indem Sie die Adresse 0.0.0.0 angeben:

```
<#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. Die IP-Adresse 203.0.113.129 ist Linux-seitig konfiguriert und im Expertenmodus sichtbar und einer internen Schnittstelle zugeordnet, z.B. 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. Unter Linux wird die IP-Adresse für das Chassis-Management der management0-Schnittstelle zugewiesen. Dies ist die IP-Adresse, die in der Ausgabe des Befehls show network (Netzwerk anzeigen) angezeigt wird:

<#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. Es gibt eine dynamische Portadressenumwandlung (PAT) an der management0-Schnittstelle, die die Quell-IP-Adresse in die IP-Adresse der management0-Schnittstelle übersetzt. Die dynamische PAT wird durch die Konfiguration einer iptables-Regel mit der Aktion MASQUERADE auf der management0-Schnittstelle erreicht:

<#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
```

Verifizierung

In diesem Beispiel ist CMI aktiviert, und in den Plattformeinstellungen ist die DNS-Auflösung über die Verwaltungsschnittstelle konfiguriert:

```
<#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
```

Die Paketerfassungen werden an den Schnittstellen Lina management, Linux tap_M0 und management0 konfiguriert:

```
<#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
```

Eine ICMP-Echoanfrage an einen voll qualifizierten Beispieldomänennamen (FQDN) generiert eine DNS-Anfrage von der Lina-Engine. Die Paketerfassung in der Lina-Engine und der Linux tap_M0-Schnittstelle zeigt die Initiator-IP-Adresse 203.0.113.130 an, die die CMI-IP-Adresse der Verwaltungsschnittstelle ist:

<#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)
```

Die auf der management0-Schnittstelle erfassten Pakete zeigen die IP-Adresse der management0-Schnittstelle als Initiator-IP-Adresse an. Dies ist auf die dynamische PAT zurückzuführen, die im Abschnitt "Management Traffic Path in Converged Management Interface Deployments" beschrieben wird:

```
<#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)
```

Schlussfolgerung

Wenn CMI aktiviert ist, wird die IP-Adresse 203.0.113.x automatisch zugewiesen und intern von der Software verwendet, um die Verbindung zwischen der Lina-Engine und dem externen Managementnetzwerk herzustellen. Sie können diese IP-Adresse ignorieren.
Die IP-Adresse, die in der Ausgabe des Befehls show network (Netzwerk anzeigen) angezeigt wird, bleibt unverändert und ist die einzige gültige IP-Adresse, die Sie als FTD-Management-IP-Adresse bezeichnen müssen.

Referenzen

- Zusammenführen der Management- und Diagnoseschnittstellen
- Konfigurationsleitfaden für Cisco Secure Firewall Management Center-Geräte, 7.6
- Konfigurationsleitfaden für Cisco Secure Firewall Device Manager, Version 7.6

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.