Esclareça a Finalidade do Endereço IP 203.0.113.x para a Interface de Gerenciamento de FTD

Contents

Introdução

Este documento descreve o endereço IP 203.0 .113.x mostrado na saída de alguns comandos no Secure Firewall Threat Defense (FTD).

Pré-requisitos

Requisitos

Conhecimento básico do produto.

Componentes Utilizados

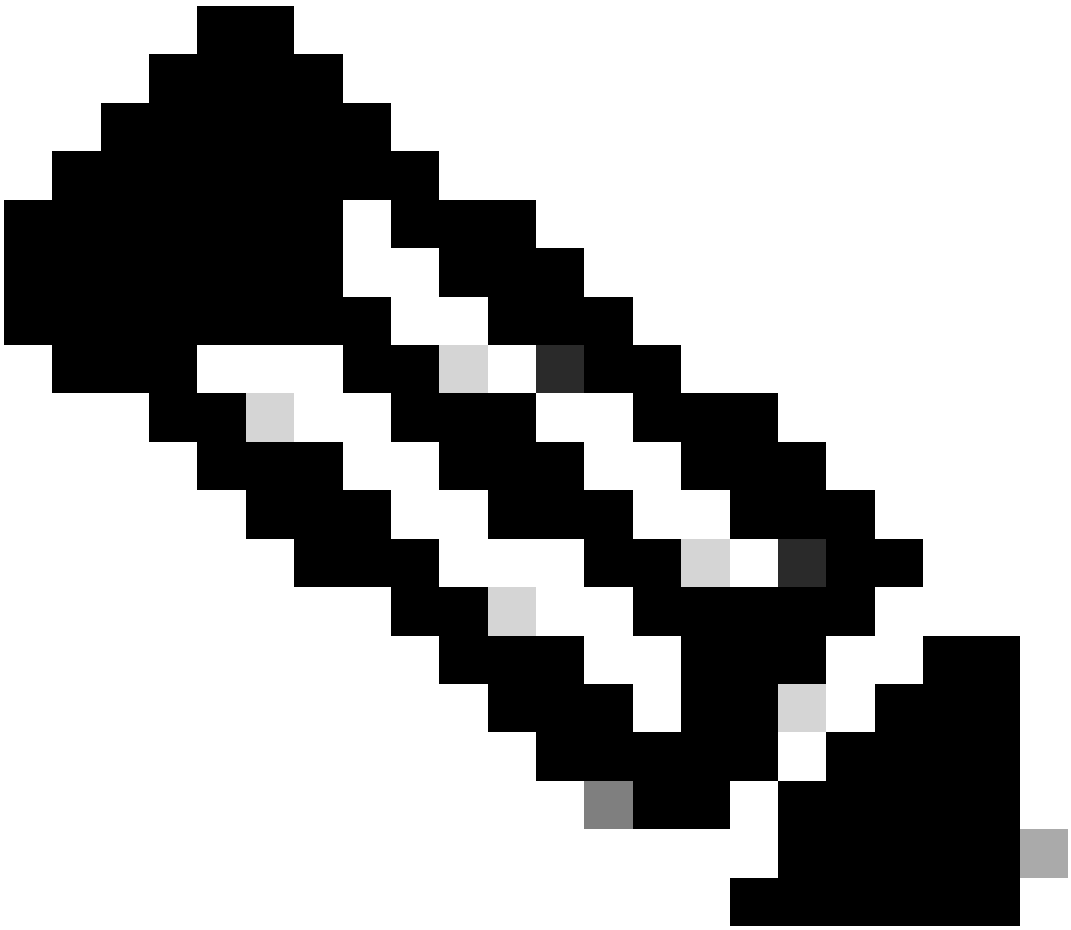
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

As informações neste documento são baseadas nestas versões de software e hardware:

- Defesa Segura de Segmento de Firewall (FTD) 7.4.x, 7.6.x. gerenciado pelo FDM (Secure Firewall Device Manager) ou pelo FMC (Secure Firewall Management Center).

Informações de Apoio

Após o upgrade do software para as versões 7.4.x ou 7.6.x, você poderá observar as alterações relacionadas ao endereço IP da interface de gerenciamento:



Note: As saídas neste artigo são relevantes para FTDs gerenciados pelo FMC quando a interface de acesso do gerente não é uma interface de dados e FTDs gerenciados pelo FDM quando a opção "Usar Gateways Exclusivos para a Interface de Gerenciamento" não está configurada.

Nos casos em que uma interface de dados é usada para o acesso do gerenciador, alguns detalhes como o caminho do tráfego de gerenciamento ou a saída do comando show network diferem.

Consulte a seção "Alterar a Interface de Acesso do Gerente de Gerenciamento para Dados" no Capítulo: Configurações do dispositivo no Guia de configuração do dispositivo do Cisco Secure Firewall Management Center, 7.6 e na seção "Configurar a interface de gerenciamento" no capítulo: Interfaces no Guia de configuração do gerenciador de dispositivos do Cisco Secure Firewall, versão 7.6.

1. O endereço IP é 203.0.113.x, embora não tenha sido configurado manualmente. Este é um exemplo de saída do FTD executado em todas as plataformas, exceto no Firepower 4100/9300:

```
<#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
```

A interface de gerenciamento do FTD executado no 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
```

…

>

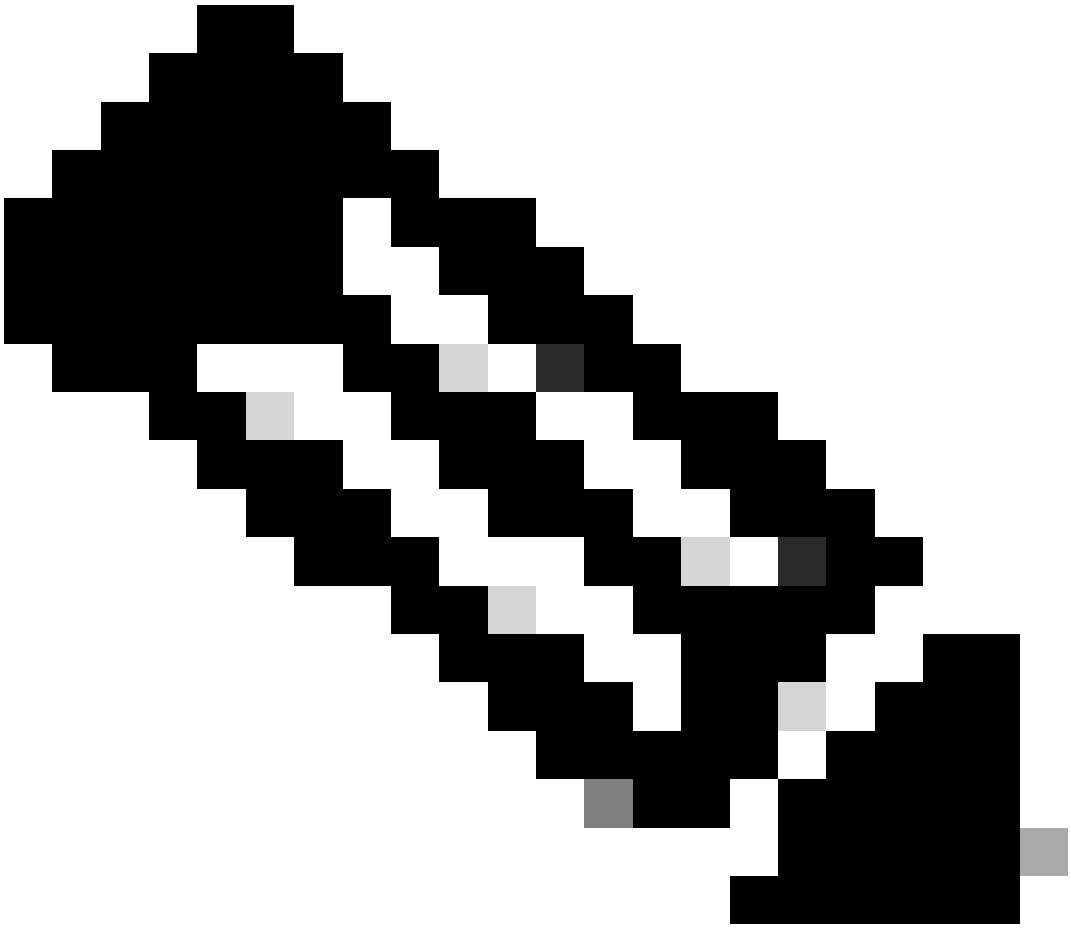
show running-config interface Ethernet 1/1

interface Ethernet1/1

 management-only

 nameif management

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



Note: No Firepower 4100/9300, você pode criar um Ethernetx/y dedicado como uma interface de gerenciamento personalizada para aplicativos, portanto, o nome da interface física é Ethernetx/y, não Managementx/y.

2. Esse endereço IP é diferente do endereço IP mostrado na saída do comando show network:

```
<#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
```

O endereço IP 203.0.113.x é atribuído à interface de gerenciamento como parte do recurso de interface de gerenciamento convergente (CMI) introduzido na versão 7.4.0. Especificamente, após o upgrade do software para a versão 7.4.x ou posterior, o software propõe a fusão das interfaces de gerenciamento e diagnóstico como mostrado na seção Mesclar as interfaces de gerenciamento e diagnóstico. Se a mesclagem for bem-sucedida, o nome da interface de gerenciamento se tornará management e receberá automaticamente o endereço IP interno 203.0.113.x.

Caminho do tráfego de gerenciamento em implantações de interface de gerenciamento convergente

O endereço IP 203.0.113.x é usado para fornecer conectividade de gerenciamento a partir do mecanismo Lina e para redes de gerenciamento externas através da interface de gerenciamento0 do chassi da seguinte maneira. Essa conectividade é essencial nos casos em que você configura serviços Lina, como syslog, resolução de nomes de domínio (DNS), acesso aos servidores de autenticação, autorização e contabilidade (AAA) e assim por diante.

Este diagrama mostra uma visão geral de alto nível do caminho do tráfego de gerenciamento do mecanismo Lina para a rede de gerenciamento externa:

Pontos principais:

1. O endereço IP 203.0.113.x com a máscara de rede /29 é configurado na interface com o nome management. Mas essa configuração não é visível na saída do comando 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
```

O gateway padrão da rede 203.0.113.129 é configurado na tabela de roteamento de gerenciamento. Essa rota padrão não é visível na saída do comando show route management-only sem argumentos. Você pode verificar a rota especificando o endereço 0.0.0.0:

```
<#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. O endereço IP 203.0.113.129 está configurado no lado do Linux e é visível no modo especialista e atribuído a uma interface interna, por exemplo, 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. No Linux, o endereço IP de gerenciamento do chassi é atribuído à interface management0. Este é o endereço IP visível na saída do comando show network:

<#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. Existe uma PAT (conversão dinâmica de endereço de porta) na interface management0 que converte o endereço IP de origem para o endereço IP da interface management0. O PAT dinâmico é obtido pela configuração de uma regra iptables com a ação MASQUERADE na interface management0:

<#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
```

Verificação

Neste exemplo, a CMI está ativada e, nas configurações da plataforma, a resolução DNS através da interface de gerenciamento está configurada:

```
<#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
```

As capturas de pacotes são configuradas nas interfaces de gerenciamento Lina, Linux tap_M0 e 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
```

Uma solicitação de eco ICMP para um FQDN (nome de domínio totalmente qualificado) de exemplo gera uma solicitação DNS do mecanismo Lina. A captura de pacotes no mecanismo Lina e na interface tap_M0 do Linux mostra o endereço IP do iniciador 203.0.113.130, que é o endereço IP CMI da interface de gerenciamento:

```
<#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)
```

As capturas de pacote na interface management0 mostram o endereço IP da interface management0 como o endereço IP do iniciador. Isso se deve ao PAT dinâmico mencionado na seção "Caminho de tráfego de gerenciamento em implantações de interface de gerenciamento convergente":

```
<#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)
```

Conclusão

Se a CMI estiver habilitada, o endereço IP 203.0.113.x será automaticamente atribuído e internamente usado pelo software para fornecer conectividade entre o mecanismo Lina e a rede de gerenciamento externa. Você pode ignorar esse endereço IP.
O endereço IP mostrado na saída do comando show network permanece inalterado e é o único endereço IP válido que você deve chamar de endereço IP de gerenciamento do FTD.

Referências

- Mesclar as Interfaces de Gerenciamento e Diagnóstico
- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.6
- Guia de configuração do gerenciador de dispositivos do Cisco Secure Firewall, versão 7.6

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.