# Resolución de problemas de error de cambio de dirección IP de FTD debido a líneas no válidas y no admitidas en el archivo iptables

## Contenido

## Problema

No se aplica la nueva dirección IP de administración de Secure Firewall Threat Defence (FTD) configurada mediante el comando configure network ipv4 manual <address> <netmask> <gateway>.

Se muestra el mensaje "Setting IPv4 network configuration" y se devuelve el mensaje.

Sin embargo, el comando show network refleja la dirección IP antigua:

<#root>

>

**configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254**

Setting IPv4 network configuration...
>
>

**show network**

```
===============[ System Information ]===============
Hostname                : firewall
Domains                 :
DNS Servers             : 192.0.2.253
DNS from router         : disabled
Management port         : 8305
IPv4 Default route
  Gateway               : 192.0.2.254

=====================[ eth0 ]=====================
Admin State             : Enabled
Admin Speed             : 10gbps
```

```
Operation Speed           : 10gbps
Duplex                    : Full-duplex
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:50:56:8D:9C:1F
----------------------[ IPv4 ]----------------------
Configuration             : Manual

Address                   : 192.0.2.10

<- old IP address
Netmask                   : 255.255.255.0
Gateway                   : 192.0.2.254
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled
```

# Entorno

- Firepower 2110 con Secure Firewall Threat Defence. Otras plataformas de hardware también pueden verse afectadas.
- FTD versión 7.4.4. Otras versiones de software también pueden verse afectadas.
- /ngfw/etc/sysconfig/iptables contiene líneas no válidas/no admitidas.
- El administrador intenta cambiar la IP de administración de FTD mediante el comando configure network ipv4 manual <address> <netmask> <gateway>.

# Resolución

## Análisis

1. Falta el mensaje "Network settings changed" en la salida del comando configure network ipv4 manual <address> <netmask> <gateway>:

<#root>

>

**configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254**

Setting IPv4 network configuration...

2. Si falta el mensaje "Network settings changed" (Parámetros de red cambiados), indica que la operación está incompleta.

El resultado esperado:

<#root>

>

**configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254**

Setting IPv4 network configuration...
Network settings changed.

3. Hay registros relevantes en el archivo /ngfw/var/log/messages sin señalar la causa raíz:

```
Jul  9 08:22:28 FIREWALL sudo:    admin : TTY=ttyS0 ; PWD=/ ; USER=root ; COMMAND=/usr/local/sf/bin/sfc
Jul  9 08:22:30 FIREWALL SF-IMS[58786]: [58786] sfifd:sfifd [INFO] Stopping '/ngfw/usr/local/sf/bin/sfi
Jul  9 08:22:30 FIREWALL SF-IMS[10865]: [10865] sfifd:monitor [WARN] sfifd is not running. starting it.
Jul  9 08:22:30 FIREWALL SF-IMS[10870]: [10870] sfifd:sfifd [INFO] Starting '/ngfw/usr/local/sf/bin/sfi
Jul  9 08:22:30 FIREWALL SF-IMS[10871]: [10871] sfifd:config [INFO] Found interface index 9 for managem
Jul  9 08:22:30 FIREWALL SF-IMS[10871]: [10871] sfifd:config [INFO] Added interface 'management0'.
Jul  9 08:22:30 FIREWALL SF-IMS[10871]: [10871] sfifd:config [INFO] Reading config for interface 'manag
Jul  9 08:22:31 FIREWALL SF-IMS[10724]: Net:Speed [INFO] Interface eth0 is ready :1000
Jul  9 08:22:31 FIREWALL SF-IMS[10724]: Net:Speed [INFO] Interface eth1 is ready :10000
Jul  9 08:22:31 FIREWALL SF-IMS[10724]: Net:Speed [INFO] Interface management0 is ready :10000
Jul  9 08:22:35 FIREWALL sensord: Chip: coretemp-isa-0000
Jul  9 08:22:35 FIREWALL sensord: Adapter: ISA adapter
Jul  9 08:22:35 FIREWALL sensord:   Package id 0: 58.0 C
Jul  9 08:22:35 FIREWALL sensord:   Core 0: 58.0 C
Jul  9 08:22:35 FIREWALL sensord:   Core 1: 58.0 C
Jul  9 08:22:35 FIREWALL sensord:   Core 2: 58.0 C
Jul  9 08:22:35 FIREWALL sensord:   Core 3: 58.0 C
...
```

Otros archivos como process_stderr.log o process_stdout.log en /ngfw/var/log/ no contienen

registros relevantes.

4. Debido a la falta de registros, el siguiente paso es ejecutar la utilidad strace e investigar las llamadas del sistema. El comando CLISH configure network ipv4 manual ejecuta una acción en modo experto. Este es un script Perl:

<#root>

>

**expert**

firewall:~$

**sudo su**

firewall#

**cd /etc/clish**

firewall:/etc/clish#

**grep "configure network ipv4" /etc/clish/* -A 10**

…
/etc/clish/configure.xml-    <COMMAND access="ldapgroup"
/etc/clish/configure.xml-             escape_chars=";`|$<>&()#\'*!"
/etc/clish/configure.xml-             help="Configure IPv4 manually"
/etc/clish/configure.xml:

**name="configure network ipv4 manual">**

/etc/clish/configure.xml-

**<ACTION>sudo /usr/local/sf/bin/sfcli.pl configure_ipv4 network man ${ipaddr} ${netmask} ${gw} ${interfac**

…

El comando complete strace:

<#root>

```
firewall #

strace -t -y -f -s 1024 -o /ngfw/var/common/strace.out /usr/local/sf/bin/sfcli.pl configure_ipv4 network
```

Expansión de argumentos:

· -t: anteponga a cada llamada del sistema rastreada la hora actual del día (horas:minutos:segundos).

· -y: muestra las rutas del descriptor de archivo. Cuando una llamada del sistema utiliza un descriptor de archivo, strace imprime el nombre de ruta asociado (si se conoce), lo que facilita la identificación de los archivos, sockets o canalizaciones a los que se accede.

· -f - Seguimiento de procesos secundarios. Si el programa rastreado crea nuevos procesos, strace también sigue rastreando esos elementos secundarios.

· -s 1024 - Aumenta el tamaño máximo de los argumentos de cadena impresos a 1024 bytes. De forma predeterminada, strace trunca las cadenas largas (normalmente en 32 bytes). Esto resulta útil para ver argumentos, búferes o nombres de archivo completos de la línea de comandos.

· -o /ngfw/var/common/strace.out: escribe todos los resultados de seguimiento en el archivo especificado en lugar del error estándar.

5. La inspección del código de salida de diferentes procesos revela que el proceso /usr/sbin/iptables-restore con PID 7793 salió con el código de error 2, a diferencia de otros con el código de salida 0 o 1.

El seguimiento también muestra una línea "Bad argument `vi':

<#root>

```
7793  08:02:09

execve("/usr/sbin/iptables-restore", ["/usr/sbin/iptables-restore", "-cv"], 0x56139209fb60 /* 11 vars */

…
7793  08:02:09 close(6</etc/passwd>)    = 0

7793  08:02:09 write(2<pipe:[230296101]>, "Bad argument `vi'\n", 18 <unfinished ...>  <-- Bad argument

7011  08:02:09 <... pselect6 resumed>)  = 1 (in [12], left {tv_sec=4, tv_nsec=964587331})
```

```
7793  08:02:09 <... write resumed>)     = 18
7011  08:02:09 read(12<pipe:[230296101]>,  <unfinished ...>
7793  08:02:09 write(2<pipe:[230296101]>, "Error occurred at line: 51\n", 27 <unfinished ...>
7011  08:02:09 <... read resumed>"Bad argument `vi'\n", 8192) = 18
7793  08:02:09 <... write resumed>)     = 27
7011  08:02:09 pselect6(16, [10<pipe:[230296100]> 12<pipe:[230296101]>], NULL, NULL, {tv_sec=5, tv_nsec=
7793  08:02:09 write(2<pipe:[230296101]>, "Try `iptables-restore -h' or 'iptables-restore --help' for m
7011  08:02:09 <... pselect6 resumed>)  = 1 (in [12], left {tv_sec=4, tv_nsec=999997162})
7793  08:02:09 <... write resumed>)     = 77
7011  08:02:09 read(12<pipe:[230296101]>,  <unfinished ...>
7793  08:02:09 lseek(0<pipe:[230296367]>, -429, SEEK_CUR <unfinished ...>
7011  08:02:09 <... read resumed>"Error occurred at line: 51\nTry `iptables-restore -h' or 'iptables-re
7793  08:02:09 <... lseek resumed>)     = -1 ESPIPE (Illegal seek)
7011  08:02:09 pselect6(16, [10<pipe:[230296100]> 12<pipe:[230296101]>], NULL, NULL, {tv_sec=5, tv_nsec=
7793  08:02:09 exit_group(2)            = ?

7793  08:02:09 +++ exited with 2 +++
```

6. Este proceso analiza y vuelve a aplicar las reglas iptables de Linux desde el archivo /ngfw/etc/sysconfig/iptables. En este caso, el archivo contiene líneas no válidas/no admitidas por razones desconocidas:

<#root>

```
device#

cat /ngfw/etc/sysconfig/iptables



...
-A OUTPUT -o lo -p tcp --dport 5000:9000 -m owner ! --uid-owner root -j DROP
-A OUTPUT -o lo -j ACCEPT
-A DUMP -j DROP

vi /etc/sysconfig/iptables <------------- BAD LINE



#start MANAGEMENT PORT STATEFUL BLOCK
-A STATEFUL -i management0 -m state --state NEW -j DROP
#stop MANAGEMENT PORT STATEFUL BLOCK


-A STATEFUL -j DUMP

COMMIT

t <-------------- ANOTHER BAD LINE + FEW NEW LINES.
```

```
# Completed on Tue Sep 15 15:06:41 2015
```

Además, el archivo /ngfw/var/log/initialize.log puede contener líneas que apuntan a la falla de reinicio de iptables debido a un argumento incorrecto en el archivo:

<#root>

```
device#

cat /ngfw/var/log/initialize.log


Re-Initialize MGMT Configuration if missing or updated... at .../SF/Sensor.pm line 5390.
Caught Exception!
  System (/ngfw/usr/local/sf/bin/service_control.sh iptables restart) Failed -- (Bad argument `vi'
Error occurred at line: 51
Try `iptables-restore -h' or 'iptables-restore --help' for more information.)
```

## Solución Aternativa

1. Acceda a la consola del firewall y cambie al modo experto:

<#root>

```
>

expert


firewall:~$

sudo su
```

2. Tome la copia de seguridad de los archivos iptables existentes:

<#root>

```
firewall#

cp /ngfw/etc/sysconfig/iptables /ngfw/var/common/
```

3. Elimine todas las líneas no admitidas e incorrectas. Tenga en cuenta que, dependiendo del hardware, las versiones de software y la configuración, el contenido de iptables puede diferir. La configuración básica se puede obtener de la configuración del laboratorio con las mismas versiones de hardware y software.

4. Reinicie iptables:

<#root>

```
firewall #

/ngfw/etc/rc.d/init.d/iptables restart


Flushing all current IPv4 rules and user defined chains: ...success
Clearing all current IPv4 rules and user defined chains: ...success
Applying iptables firewall rules:
Flushing chain `PREROUTING'
Flushing chain `INPUT'
Flushing chain `OUTPUT'
Flushing chain `POSTROUTING'
Flushing chain `PREROUTING'
Flushing chain `OUTPUT'
Flushing chain `PREROUTING'
Flushing chain `INPUT'
Flushing chain `FORWARD'
Flushing chain `OUTPUT'
Flushing chain `POSTROUTING'
Flushing chain `INPUT'
Flushing chain `FORWARD'
Flushing chain `OUTPUT'

Applying rules successed <-------- Expected line
```

5. Vuelva a configurar la dirección IP de administración en FTD CLISH.

# Causa

Las entradas no válidas/no admitidas en el archivo /ngfw/etc/sysconfig/iptables provocan la interrupción prematura del cambio de dirección IP. Se realiza un seguimiento de esto en el Id. de bug Cisco CSCwv5279.

## Contenido relacionado

- Id. de error de Cisco CSCwv5279.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).