Troubleshoot FTD IP Address Change Failure Due To Invalid and Unsupported Lines in iptables File

Contents

Issue

The new Secure Firewall Threat Defense (FTD) management IP address configured using the **configure network ipv4 manual <address> <netmask> <gateway>** commandis not applied.

The message **"**Setting IPv4 network configuration" is shown and the prompt is returned.

Nevertheless, the **show network** command reflects the old IP address:

<#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
```

Environment

- Firepower 2110 running Secure Firewall Threat Defense. Other hardware platforms can also be affected.
- FTD version 7.4.4. Other software versions can also be affected.
- **/ngfw/etc/sysconfig/iptables** files contains invalid/unsupported lines.
- The administrator attempts to change the FTD management IP using the **configure network ipv4 manual <address> <netmask> <gateway>** command.

Resolution

Analysis

1. The “Network settings changed” message is missing in the output of the **configure network ipv4 manual <address> <netmask> <gateway>** command:

<#root>

>

```
configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254


Setting IPv4 network configuration...
```

2. Missing “Network settings changed” message indicates that the operation is incomplete.

The expected output:

```
<#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. There are relevant logs in **/ngfw/var/log/messages** file without pinpointing to the root cause:

```
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
...
```

Other files such as **process_stderr.log** or **process_stdout.log** in **/ngfw/var/log/** do not contain relevant logs.

4. Due to lack of logs, the next step is to run the **strace** utility and investigate the system calls. The CLISH command **configure network ipv4 manual** runs an action in expert mode. This is a Perl script:

```
<#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=";`|$&lt;&gt;&amp;()#\'*!"
/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



…
```

The complete strace command:

<#root>

```
firewall #

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

Expanation of arguments:

· **-t** - Prefix each traced system call with the current time of day (hours:minutes:seconds).

· **-y** - Show file descriptor paths. When a syscall uses a file descriptor, strace prints the associated pathname (if known), making it easier to identify which files, sockets, or pipes are being accessed.

· **-f** - Trace child processes. If the traced program creates new processes, strace continues tracing those children as well.

· **-s 1024** - Increase the maximum size of printed string arguments to 1024 bytes. By default, strace truncates long strings (typically at 32 bytes). This is useful for seeing full command-line arguments, buffers, or filenames.

· **-o /ngfw/var/common/strace.out** - Write all trace output to the specified file instead of standard error.

5. Inspection of exit code from different processes reveals that the process **/usr/sbin/iptables-restore** with PID **7793** exited with error code **2,** unlike others with exit code 0 or 1.

The trace also shows a **"Bad argument `vi'"** line:

<#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. This process parses and reapplies Linux iptables rules from the **/ngfw/etc/sysconfig/iptables** file. In this case, the file contains invalid/unsupported lines for unknown reasons:

<#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
```

Additionally, the file **/ngfw/var/log/initialize.log** can contain lines that point to the iptables restart failure due to bad argument in the file:

<#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.)
```

Workaround

1. Access the firewall console and switch to the expert mode:

```
<#root>

>

expert


firewall:~$

sudo su
```

2. Take the backup of the existing iptables files:

```
<#root>

firewall#

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

3. Remove all unsupported and incorrect lines. Note that, depending on hardware, software versions and configuration, the content of iptables can differ. The baseline config can be obtained from the lab setup with the same hardware and software versions.

4. Restart 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. Reconfigure the management IP address on FTD CLISH.

Cause

Invalid/unsupported entries in **/ngfw/etc/sysconfig/iptables** file result in premature interruption of the IP address change. This is tracked in Cisco bug ID CSCwv52279.

Related Content

- Cisco bug ID CSCwv52279.