Fehlerbehebung bei FTD-IP-Adressänderungsfehlern aufgrund ungültiger und nicht unterstützter Zeilen in der IP-Datei

Inhalt

Problem

Die neue, mit dem manuellen Befehl configure network ipv4 <address> <netmask> <gateway> konfigurierte Management-IP-Adresse von Secure Firewall Threat Defense (FTD) wird nicht angewendet.

Die Meldung "Setting IPv4 network configuration" wird angezeigt, und die Eingabeaufforderung wird zurückgegeben.

Der Befehl show network gibt jedoch die alte IP-Adresse wieder:

<#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
```

Umwelt

- Firepower 2110 mit Secure Firewall Threat Defense Auch andere Hardwareplattformen können betroffen sein.
- FTD Version 7.4.4. Andere Softwareversionen können ebenfalls betroffen sein.
- /ngfw/etc/sysconfig/iptables-Dateien enthalten ungültige/nicht unterstützte Zeilen.
- Der Administrator versucht, die FTD-Management-IP mithilfe des Befehls configure network ipv4 manual <Adresse> <Netzmaske> <Gateway> zu ändern.

Auflösung

Analyse

1. In der Ausgabe des Befehls configure network ipv4 manual <Adresse> <Netzmaske> <Gateway> (Netzwerk-IPv4-Konfiguration konfigurieren) fehlt die Meldung "Network settings changes" (Netzwerkeinstellungen geändert):

```
<#root>

>

configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254


Setting IPv4 network configuration...
```

2. Die Meldung "Netzwerkeinstellungen geändert" fehlt und zeigt an, dass der Vorgang unvollständig ist.

Erwartete Leistung:

```
<#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. Es gibt relevante Logs in /ngfw/var/log/messages Datei ohne Angabe der Ursache:

```
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
...
```

Andere Dateien wie process_stderr.log oder process_stdout.log in /ngfw/var/log/ enthalten keine relevanten Protokolle.

4. Aufgrund fehlender Protokolle besteht der nächste Schritt darin, das strace-Dienstprogramm auszuführen und die Systemaufrufe zu untersuchen. Der CLISH-Befehl configure network ipv4 führt eine Aktion im Expertenmodus aus. Dies ist ein Perl-Skript:

<#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

…

Der vollständige Befehl strace:

<#root>

```
firewall #
```

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

Erweiterung der Argumente:

- -t - Stellen Sie jedem verfolgten Systemaufruf die aktuelle Tageszeit (Stunden:Minuten:Sekunden) voran.

- -y - Dateideskriptorpfade anzeigen. Wenn ein syscall einen Dateideskriptor verwendet, druckt strace den zugehörigen Pfadnamen (sofern bekannt), um leichter festzustellen, auf welche Dateien, Sockets oder Pipes zugegriffen wird.

- -f - Nachverfolgen von Kindprozessen Wenn das verfolgte Programm neue Prozesse erzeugt, verfolgt strace auch diese Kinder weiter.

- -s 1024 - Erhöhen Sie die maximale Größe der gedruckten Zeichenfolgenargumente auf 1024 Byte. Standardmäßig kürzt strace lange Zeichenfolgen (in der Regel mit 32 Byte). Dies ist nützlich, um vollständige Befehlszeilenargumente, Puffer oder Dateinamen anzuzeigen.

- -o /ngfw/var/common/strace.out - Schreiben Sie die gesamte Ablaufverfolgungsausgabe in die angegebene Datei, anstatt auf einen Standardfehler.

5. Untersuchung von Exit-Code aus verschiedenen Prozessen zeigt, dass der Prozess /usr/sbin/iptables-restore mit PID 7793 mit Fehlercode 2 beendet, im Gegensatz zu anderen mit Exit-Code 0 oder 1.

Die Ablaufverfolgung zeigt auch eine "Bad argument `vi'"-Zeile:

<#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. Dieser Prozess parst und wendet die Linux-iptables-Regeln aus der Datei /ngfw/etc/sysconfig/iptables erneut an. In diesem Fall enthält die Datei aus unbekannten Gründen ungültige/nicht unterstützte Zeilen:

<#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
```

Darüber hinaus kann die Datei /ngfw/var/log/initialize.log Zeilen enthalten, die auf den Fehler beim Neustart von iptables aufgrund eines fehlerhaften Arguments in der Datei verweisen:

<#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.)
```

Problemumgehung

1. Rufen Sie die Firewall-Konsole auf, und wechseln Sie in den Expertenmodus:

<#root>

```
>

expert


firewall:~$

sudo su
```

2. Sichern Sie die vorhandenen iptables-Dateien:

<#root>

```
firewall#
```

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

3. Entfernen Sie alle nicht unterstützten und falschen Posten. Beachten Sie, dass je nach Hardware, Softwareversionen und Konfiguration der Inhalt von iptables unterschiedlich sein kann. Die Basiskonfiguration kann mit derselben Hardware- und Softwareversion aus der Übung bezogen werden.

4. iptables neu starten:

<#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. Konfigurieren Sie die Verwaltungs-IP-Adresse auf FTD CLISH neu.

Ursache

Ungültige/nicht unterstützte Einträge in der Datei /ngfw/etc/sysconfig/iptables führen zu einer vorzeitigen Unterbrechung der IP-Adressänderung. Dies wird in der Cisco Bug-ID CSCwv52279 nachverfolgt.

Verwandte Inhalte

- Cisco Bug-ID CSCwv52279.

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.