由於iptables檔案中無效和不支援的行，對FTD IP地址更改失敗進行故障排除

目錄

問題

未應用使用configure network ipv4 manual <address> <netmask> <gateway>命令配置的新的安全防火牆威脅防禦(FTD)管理IP地址。

系統會顯示訊息「Setting IPv4 network configuration」，並返回提示。

但是，show network命令會反映舊的IP位址：

<#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
```

環境

- 運行安全防火牆威脅防禦的Firepower 2110。其他硬體平台也可能受到影響。
- FTD版本7.4.4。其他軟體版本也可能受影響。
- /ngfw/etc/sysconfig/iptables檔案包含無效/不受支援的行。
- 管理員嘗試使用configure network ipv4 manual <address> <netmask> <gateway> 命令更改FTD管理IP。

解析

分析

1. configure network ipv4 manual <address> <netmask> <gateway> 命令的輸出中缺少「Network settings changed」消息：

<#root>

>

```
configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254

Setting IPv4 network configuration...
```

2.缺少「網路設定已更改」消息表明操作未完成。

預期輸出：

```
<#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. /ngfw/var/log/messages 檔案中存在相關日誌，但沒有指出根本原因：

```
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
...
```

/ngfw/var/log/ 中的其他檔案(如process_stderr.log或process_stdout.log)不包含相關日誌。

4.由於缺少日誌，下一步是運行strace實用程式並調查系統呼叫。CLISH命令configure network ipv4 manual 在專家模式下運行操作。這是Perl指令碼：

```
<#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-
```

sudo /usr/local/sf/bin/sfcli.pl configure_ipv4 network man ${ipaddr} ${netmask} ${gw} ${interface}

…

完整的字串命令：

<#root>

```
firewall #
```

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

引數的擴展：

· -t — 為每個跟蹤的系統呼叫設定當前時間（小時：分鐘：秒）的字首。

· -y — 顯示檔案描述符路徑。當syscall使用檔案描述符時，strace將列印關聯的路徑名（如果已知），從而更容易識別正在訪問的檔案、套接字或管道。

· -f — 跟蹤子進程。如果跟蹤的程式建立了新的進程，則字串也會繼續跟蹤這些兒童。

· -s 1024 -將列印字串引數的最大大小增加到1024位元組。預設情況下，字串截斷長字串（通常為32位元組）。 這對於檢視完整的命令列引數、緩衝區或檔名非常有用。

· -o /ngfw/var/common/strace.out — 將所有跟蹤輸出寫入指定檔案，而不是標準錯誤。

5.檢查不同進程的退出代碼後發現，PID 7793的/usr/sbin/iptables-restore進程退出時帶有錯誤代碼2，而其它進程退出代碼為0或1。

跟蹤還會顯示「Bad argument 'vi'」行：

<#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

     , "Bad argument `vi'\n", 18

        <-- 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.此過程從/ngfw/etc/sysconfig/iptables檔案中解析並重新應用Linux iptables規則。在這種情況下，由於未知原因，檔案包含無效/不支援的行：

<#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
```

此外，檔案/ngfw/var/log/initialize.log還可以包含一些行，這些行指向由於檔案中有錯誤引數而導致iptables重新啟動失敗：

<#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.)
```

因應措施

1.訪問防火牆控制檯並切換至專家模式：

<#root>

```
>

expert


firewall:~$

sudo su
```

2.備份現有的iptables檔案：

<#root>

```
firewall#
```

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

3.刪除所有不支援的和不正確的行。請注意，根據硬體、軟體版本和配置，iptables的內容可能不同。使用相同的硬體和軟體版本，可以從實驗室設定獲取基線配置。

4.重新啟動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.重新配置FTD CLISH上的管理IP地址。

原因

/ngfw/etc/sysconfig/iptables 檔案中的無效/不受支援的條目導致IP地址更改過早中斷。思科錯誤ID CSCwv5279會追蹤此錯誤。

相關內容

- 思科錯誤ID CSCwv52279。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。