由于iptables文件中无效和不支持的行，对FTD IP地址更改失败进行故障排除

目录

问题

未应用使用configure network ipv4 manual <address> <netmask> <gateway>命令配置的新安全防火墙威胁防御(FTD)管理IP地址。

系统将显示消息Setting IPv4 network configuration（设置IPv4网络配置），并返回提示。

但是，show network命令反映的是旧的IP地址：

<#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
```

环境

- 运行安全防火墙威胁防御的Firepower 2110。其他硬件平台也可能受到影响。
- FTD版本7.4.4。其它软件版本也可能会受到影响。
- /ngfw/etc/sysconfig/iptables文件包含无效/不受支持的行。
- 管理员尝试使用configure network ipv4 manual <address> <netmask> <gateway> 命令更改FTD管理IP。

分辨率

分析

1. configure network ipv4 manual <address> <netmask> <gateway>命令的输出中缺少“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“网络设置已更改”消息表明操作不完整。

预期输出：

```
<#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文件中存在相关日志，但没有指出根本原因：

```
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/ 中的其他文件（如process_stderr.log 或process_stdout.log）不包含相关日志。

4.由于缺乏日志，下一步是运行strace实用程序并调查系统调用。CLISH命令configure network ipv4 manual 在专家模式下运行操作。这是一个Perl脚本：

```
<#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-

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

…

完整的strace命令：

<#root>

firewall #

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

参数的扩展：

· -t — 为每个跟踪的系统呼叫设置当前时间（小时：分钟：秒）的前缀。

· -y — 显示文件描述符路径。当syscall使用文件描述符时，strace会打印关联的路径名（如果已知），从而更容易识别正在访问的文件、套接字或管道。

·-f — 跟踪子进程。如果跟踪的程序创建了新进程，strace也会继续跟踪这些子进程。

· -s 1024 -将打印字符串参数的最大大小增加到1024字节。默认情况下，字符串截断长字符串（通常为32字节）。 这对于查看完整的命令行参数、缓冲区或文件名非常有用。

· -o /ngfw/var/common/strace.out — 将所有跟踪输出写入指定文件，而不是写入标准错误。

5.检查不同进程的退出代码后发现，使用PID 7793的进程/usr/sbin/iptables-restore退出时带有错误代码2，而其它进程则带有退出代码0或1。

跟踪还显示“错误参数‘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.此过程解析并重新应用来自/ngfw/etc/sysconfig/iptables文件的Linux iptables规则。在这种情况下，文件包含由于未知原因而无效/不受支持的行：

<#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，文件/ngfw/var/log/initialize.log可能包含由于文件中的错误参数而指向iptables restart failure的行：

```
<#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.)
```

解决方法

1.访问防火墙控制台并切换到专家模式：

```
<#root>

>

expert


firewall:~$

sudo su
```

2.备份现有的iptables文件：

<#root>

```
firewall#
```

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

3.删除所有不支持和不正确的行。请注意，根据硬件、软件版本和配置，iptables的内容可能会有所不同。基线配置可通过实验室设置获得，硬件版本和软件版本相同。

4.重新启动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文件中的无效/不受支持的条目导致IP地址更改过早中断。思科漏洞ID CSCwv52279中会对此进行跟踪。

相关内容

- 思科漏洞ID CSCwv52279。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。