iptablesファイルの無効およびサポート対象外の行が原因で発生するFTD IPアドレス変更エラーのトラブルシューティング

内容

問題

configure network ipv4 manual <address> <netmask> <gateway>コマンドを使用して設定された新しいセキュアファイアウォール脅威対策(FTD)管理IPアドレスは適用されません。

「Setting IPv4 network configuration」というメッセージが表示され、プロンプトが返されます。

それでも、show networkコマンドには古いIPアドレスが反映されます。

<#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

- セキュアファイアウォール脅威対策を実行するFirepower 2110。他のハードウェアプラットフォームも影響を受ける可能性があります。
- FTDバージョン7.4.4他のソフトウェアバージョンも影響を受ける可能性があります。
- /ngfw/etc/sysconfig/iptables ファイルに無効またはサポートされていない行が含まれています。
- 管理者は、configure network ipv4 manual <address> <netmask> <gateway> コマンドを使用してFTDの管理IPを変更しようとします。

解決方法

分析

1.「Network settings changed」メッセージがconfigure network ipv4 manual <address> <netmask> <gateway> コマンドの出力に表示されない：

<#root>

>

configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254

Setting IPv4 network configuration...

2.「ネットワーク設定が変更されました」というメッセージが表示されない場合は、操作が不完全です。

予想される出力は次のようになります。

<#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. 根本原因を特定せずに、/ngfw/var/log/messages ファイルに関連ログがある場合。

```
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/にあるprocess_stderr.log やprocess_stdout.log などの他のファイルには、関連する

ログは含まれていません。

4. ログがないため、次のステップはstraceユーティリティを実行し、システムコールを調査することです。CLISHコマンドconfigure network ipv4 manualは、エキスパートモードでアクションを実行します。これはPerlスクリプトです。

<#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}

…

完全なstraceコマンド：

<#root>

```
firewall #
```

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

引数の展開：

・ -t：トレースされた各システムコールの前に、現在の時刻（時：分：秒）を付けます。

・ -y：ファイル記述子のパスを表示します。syscallがファイル記述子を使用する場合、straceは関連するパス名（既知の場合）を出力します。これにより、どのファイル、ソケット、またはパイプにアクセスしているかを識別しやすくなります。

・ -f：子プロセスをトレースします。トレースされたプログラムが新しいプロセスを作成した場合、トレースはこれらの子プロセスのトレースも継続します。

・ -s 1024 – 出力される文字列引数の最大サイズを1024バイトに増やします。デフォルトでは、文字列は長い文字列（通常は32バイト）を切り捨てます。 これは、完全なコマンドライン引数、バッファ、またはファイル名を表示する場合に便利です。

・ -o /ngfw/var/common/strace.out – すべてのトレース出力を、標準エラーではなく指定したファイルに書き込みます。

5. 異なるプロセスからの終了コードの検査は、終了コード0または1の他のプロセスとは異なり、PID 7793のプロセス/usr/sbin/iptables-restore がエラーコード2で終了したことを明らかにします。

トレースには「Bad argument 'vi'」の行も表示されます。

<#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. このプロセスは、/ngfw/etc/sysconfig/iptablesファイルからLinux iptablesルールを解析し、再適用します。この場合、不明な理由により、ファイルに無効な行またはサポートされていない行が含まれています。

<#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
```

また、ファイル/ngfw/var/log/initialize.logには、ファイル内の不正な引数が原因で発生したiptables再起動エラーを指す行が含まれている場合があります。

<#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.)
```

回避策

1. ファイアウォールコンソールにアクセスし、expertモードに切り替えます。

<#root>

>

expert

firewall:~$

sudo su

2. 既存のiptablesファイルのバックアップを作成します。

<#root>

firewall#

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

3. サポートされていない行と正しくない行をすべて削除します。ハードウェア、ソフトウェアバージョン、および設定によっては、iptablesの内容が異なる場合があることに注意してください。ベースライン設定は、同じバージョンのハードウェアとソフトウェアを使用してラボのセットアップから取得できます。

4. iptablesを再起動します。

<#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. FTD CLISHの管理IPアドレスを再設定します。

原因

/ngfw/etc/sysconfig/iptables ファイル内の無効またはサポートされていないエントリにより、IPアドレスの変更が早期に中断されます。この問題は、Cisco Bug ID CSCwv52279で追跡されています。

関連コンテンツ

- Cisco Bug ID CSCwv52279。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。