Risoluzione dei problemi relativi alla modifica dell'indirizzo IP FTD non riuscita a causa di righe non valide e non supportate nel file iptables

Sommario

Problema

Il nuovo indirizzo IP di gestione Secure Firewall Threat Defense (FTD) configurato utilizzando il comando configure network ipv4 manual <indirizzo> <netmask> <gateway> non è applicato.

Viene visualizzato il messaggio "Setting IPv4 network configuration" e viene restituito il prompt.

Tuttavia, il comando show network riflette il vecchio indirizzo IP:

<#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
```

Ambiente

- Firepower 2110 con Secure Firewall Threat Defense. Il problema potrebbe riguardare anche altre piattaforme hardware.
- FTD versione 7.4.4. Possono essere interessate anche altre versioni software.
- /ngfw/etc/sysconfig/iptables contiene righe non valide/non supportate.
- L'amministratore cerca di modificare l'IP di gestione FTD usando il comando configure network ipv4 manual <indirizzo> <netmask> <gateway>.

Risoluzione

Analisi

1. Messaggio "Impostazioni di rete modificate" mancante nell'output del comando configure network ipv4 manual <indirizzo> <netmask> <gateway>:

<#root>

>

configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254

Setting IPv4 network configuration...

2. Il messaggio "Impostazioni di rete modificate" mancante indica che l'operazione è incompleta.

L'output previsto:

<#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. Il file /ngfw/var/log/messages contiene log pertinenti senza individuare la causa principale:

```
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
...
```

Altri file come process_stderr.log o process_stdout.log in /ngfw/var/log/ non contengono registri rilevanti.

4. A causa della mancanza di log, il passo successivo consiste nell'eseguire l'utility strace e nell'esaminare le chiamate di sistema. Il comando CLISH configure network ipv4 manual esegue un'azione in modalità Expert. Questo è uno script Perl:

<#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

…

Il comando di traccia completa:

<#root>

firewall #

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

Espansione degli argomenti:

· -t - Anteporre a ciascuna chiamata di sistema tracciata l'ora corrente (ore:minuti:secondi).

· -y - Mostra i percorsi dei descrittori dei file. Quando un syscall utilizza un descrittore di file, strace stampa il percorso associato (se noto), facilitando l'identificazione dei file, dei socket o delle pipe a cui si accede.

· -f - Traccia dei processi figlio. Se il programma tracciato crea nuovi processi, strace continua a tracciare anche quei figli.

· -s 1024 - Aumenta le dimensioni massime degli argomenti della stringa stampata a 1024 byte. Per impostazione predefinita, la stringa troncata le stringhe lunghe (in genere a 32 byte). Ciò è utile per visualizzare argomenti, buffer o nomi di file completi della riga di comando.

· -o /ngfw/var/common/strace.out - Scrive tutto l'output di analisi nel file specificato anziché l'errore standard.

5. L'ispezione del codice di uscita da diversi processi rivela che il processo /usr/sbin/iptables-restore con PID 7793 è uscito con codice di errore 2, a differenza di altri con codice di uscita 0 o 1.

La traccia mostra anche una riga "Argomento 'vi' errato":

<#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. Questo processo analizza e riapplica le regole iptables di Linux dal file /ngfw/etc/sysconfig/iptables. In questo caso, il file contiene righe non valide/non supportate per motivi sconosciuti:

<#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
```

Inoltre, il file /ngfw/var/log/initialize.log può contenere righe che puntano all'errore di riavvio iptables causato da un argomento errato nel 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.)
```

Soluzione alternativa

1. Accedere alla console del firewall e passare alla modalità Expert:

<#root>

```
>

expert


firewall:~$

sudo su
```

2. Eseguire il backup dei file iptables esistenti:

<#root>

```
firewall#

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

3. Rimuovere tutte le righe non supportate e non corrette. Si noti che, a seconda dell'hardware,

delle versioni software e della configurazione, il contenuto delle iptable può variare. La configurazione di base può essere ottenuta dalla configurazione lab con le stesse versioni hardware e software.

4. Riavviare 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. Riconfigurare l'indirizzo IP di gestione su FTD CLISH.

Causa

Le voci non valide/non supportate nel file /ngfw/etc/sysconfig/iptables determinano un'interruzione prematura della modifica dell'indirizzo IP. Questa condizione viene rilevata nel bug Cisco con ID CSCwv52279.

Contenuto correlato

- ID bug Cisco CSCwv52279.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).