Troubleshooting de Falha de Alteração de Endereço IP FTD Devido a Linhas Inválidas e Sem Suporte no Arquivo iptables

Contents

Problema

O novo endereço IP de gerenciamento do Secure Firewall Threat Defense (FTD) configurado usando o comando configure network ipv4 manual <endereço> <máscara de rede> <gateway> não é aplicado.

A mensagem "Definindo a configuração de rede IPv4" é mostrada e o prompt é retornado.

No entanto, o comando show network reflete o endereço IP antigo:

<#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 executando Secure Firewall Threat Defense. Outras plataformas de hardware também podem ser afetadas.
- FTD versão 7.4.4. Outras versões de software também podem ser afetadas.
- /ngfw/etc/sysconfig/iptables contém linhas inválidas/sem suporte.
- O administrador tenta alterar o IP de gerenciamento do FTD usando o comando configure network ipv4 manual <endereço> <máscara de rede> <gateway>.

Resolução

Análise

1. A mensagem "Network settings changed" está faltando na saída do comando configure network ipv4 manual <endereço> <máscara de rede> <gateway>:

<#root>

>

configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254

Setting IPv4 network configuration...

2. A mensagem "Configurações de rede alteradas" ausente indica que a operação está incompleta.

A saída esperada:

<#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. Há logs relevantes no arquivo /ngfw/var/log/messages sem apontar a causa raiz:

```
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
...
```

Outros arquivos como process_stderr.log ou process_stdout.log em /ngfw/var/log/ não contêm

logs relevantes.

4. Devido à falta de registros, a próxima etapa é executar o utilitário strace e investigar as chamadas do sistema. O comando CLISH configure network ipv4 manual executa uma ação no modo especialista. Este é um 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

…

O comando completo strace:

<#root>

```
firewall #

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

Expansão de argumentos:

· -t - Prefixe cada chamada rastreada do sistema com a hora atual do dia (horas:minutos:segundos).

· -y - Mostrar caminhos do descritor de arquivos. Quando um syscall usa um descritor de arquivo, o strace imprime o nome do caminho associado (se conhecido), facilitando a identificação de quais arquivos, soquetes ou pipes estão sendo acessados.

· -f - Rastrear processos filho. Se o programa rastreado criar novos processos, o strace continuará rastreando esses filhos também.

· -s 1024 - Aumenta o tamanho máximo dos argumentos de string impressos para 1024 bytes. Por padrão, o strace trunca longas cadeias de caracteres (geralmente em 32 bytes). Isso é útil para ver argumentos completos da linha de comando, buffers ou nomes de arquivos.

· -o /ngfw/var/common/strace.out - Grava todas as saídas de rastreamento no arquivo especificado, em vez do erro padrão.

5. A inspeção do código de saída de diferentes processos revela que o processo /usr/sbin/iptables-restore com PID 7793 saiu com o código de erro 2, ao contrário de outros com o código de saída 0 ou 1.

O trace também mostra uma linha "Bad arguments `vi' :

<#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. Este processo analisa e reaplica as regras iptables Linux a partir do arquivo /ngfw/etc/sysconfig/iptables. Nesse caso, o arquivo contém linhas inválidas/sem suporte por motivos desconhecidos:

<#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
```

Além disso, o arquivo /ngfw/var/log/initialize.log pode conter linhas que apontam para a falha de reinicialização de iptables devido a argumentos incorretos no arquivo:

<#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.)
```

Solução

1. Acesse o console do firewall e mude para o modo especialista:

<#root>

```
>

expert


firewall:~$

sudo su
```

2. Faça o backup dos arquivos iptables existentes:

<#root>

```
firewall#

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

3. Remova todas as linhas incorretas e sem suporte. Observe que, dependendo do hardware, das versões de software e da configuração, o conteúdo dos iptables pode ser diferente. A configuração de linha de base pode ser obtida na configuração do laboratório com as mesmas versões de hardware e software.

4. Reinicie o 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. Reconfigure o endereço IP de gerenciamento no FTD CLISH.

Causa

Entradas inválidas/sem suporte no arquivo /ngfw/etc/sysconfig/iptables resultam na interrupção prematura da alteração do endereço IP. Isso é rastreado no bug da Cisco ID CSCwv52279.

Conteúdo relacionado

- ID de bug Cisco CSCwv52279.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.