Problemen oplossen FTD IP-adreswijziging mislukt vanwege ongeldige en niet-ondersteunde regels in iptables-bestand

Inhoud

uitgifte

Het nieuwe IP-adres voor het beheer van Secure Firewall Threat Defense (FTD) dat is geconfigureerd met de opdracht configure network ipv4 manual <address> <netmask> <gateway> is niet van toepassing.

Het bericht "IPv4-netwerkconfiguratie instellen" wordt weergegeven en de prompt wordt geretourneerd.

Niettemin weerspiegelt de opdracht Show Network het oude IP-adres:

```
<#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
```

milieu

- Firepower 2110 met Secure Firewall Threat Defense. Ook andere hardwareplatforms kunnen worden getroffen.
- FTD versie 7.4.4. Ook andere softwareversies kunnen worden beïnvloed.
- /NGFW/ETC/SYSconfig/IPTABLES-bestanden bevatten ongeldige/niet-ondersteunde regels.
- De beheerder probeert het IP-adres van het FTD-beheer te wijzigen met de opdracht Network ipv4 manual <address> <netmask> <gateway> configureren.

resolutie

analyse

1. Het bericht "Gewijzigde netwerkinstellingen" ontbreekt in de uitvoer van de handleiding voor het configureren van netwerk ipv4 <adres> <netmask> <gateway> opdracht:

<#root>

>

configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254

Setting IPv4 network configuration...

2. Het bericht "Gewijzigde netwerkinstellingen" ontbreekt, geeft aan dat de bewerking onvolledig is.

De verwachte output:

<#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. Er zijn relevante logs in het /ngfw/var/log/messages-bestand zonder de oorzaak aan te wijzen:

```
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
...
```

Andere bestanden zoals process_stderr.log of process_stdout.log in /ngfw/var/log/ bevatten geen relevante logbestanden.

4. Bij gebrek aan logboeken is de volgende stap het uitvoeren van het strace-hulpprogramma en het onderzoeken van de systeemaanroepen. De CLISH-opdracht Network IPv4 configureren voert een actie uit in de modus Expert. Dit is een Perl script:

<#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

…

De opdracht complete strace:

<#root>

```
firewall #
```

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

Uitleg van argumenten:

· -t - Prefix elke getraceerde systeemaanroep met de huidige tijd van de dag (uren: minuten: seconden).

· -y - Toon bestandsdescriptorpaden. Wanneer een syscall een bestandsdescriptor gebruikt, drukt strace de bijbehorende padnaam af (indien bekend), waardoor het gemakkelijker wordt om te identificeren welke bestanden, sockets of pijpen worden geopend.

· -f - Traceer onderliggende processen. Als het getraceerde programma nieuwe processen creëert, blijft strace die kinderen ook volgen.

· -s 1024 - Verhoog de maximale grootte van gedrukte string argumenten tot 1024 bytes. Standaard worden met strace lange tekenreeksen afgekapt (meestal met 32 bytes). Dit is handig voor het zien van volledige opdrachtregelargumenten, buffers of bestandsnamen.

· -o /ngfw/var/common/strace.out - Schrijf alle trace-uitvoer naar het opgegeven bestand in plaats van de standaardfout.

5. Inspectie van de afsluitcode van verschillende processen toont aan dat het proces / usr/sbin/iptables-restore met PID 7793 afliep met foutcode 2, in tegenstelling tot andere met afsluitcode 0 of 1.

Het spoor toont ook een regel "Slecht argument `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. Dit proces parseert en past de Linux iptables-regels van het /ngfw/etc/sysconfig/iptables-bestand opnieuw toe. In dit geval bevat het bestand om onbekende redenen ongeldige/niet-ondersteunde regels:

<#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
```

Daarnaast kan het bestand /ngfw/var/log/initialize.log regels bevatten die wijzen op de iptables herstart mislukt als gevolg van een slecht argument in het bestand:

<#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.)
```

Tijdelijke oplossing

1. Toegang tot de firewallconsole en de switch tot de expertmodus:

<#root>

```
>

expert


firewall:~$

sudo su
```

2. Maak een back-up van de bestaande iptables-bestanden:

<#root>

```
firewall#
```

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

3. Verwijder alle niet-ondersteunde en onjuiste regels. Houd er rekening mee dat, afhankelijk van de hardware, softwareversies en configuratie, de inhoud van iptables kan verschillen. De basislijnconfiguratie kan worden verkregen via de laboratoriuminstelling met dezelfde hardware- en softwareversies.

4. Start de iptables opnieuw op:

<#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. Configureer het IP-adres van het beheer op FTD CLISH.

Oorzaak

Ongeldige/niet-ondersteunde vermeldingen in het bestand /ngfw/etc/sysconfig/iptables leiden tot een voortijdige onderbreking van de wijziging van het IP-adres. Dit wordt bijgehouden in Cisco bug ID CSCwv52279.

Gerelateerde inhoud

- Cisco bug ID CSCwv52279.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.