Dépannage de l'échec de modification d'adresse IP FTD en raison de lignes non valides et non prises en charge dans le fichier iptables

Table des matières

Problème

La nouvelle adresse IP de gestion Secure Firewall Threat Defense (FTD) configurée à l'aide de la commande configure network ipv4 manual <address> <netmask> <gateway> n'est pas appliquée.

Le message « Setting IPv4 network configuration » s'affiche et l'invite est renvoyée.

Néanmoins, la commande show network reflète l'ancienne adresse 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
```

Environnement

- Firepower 2110 exécute Secure Firewall Threat Defense. D'autres plates-formes matérielles peuvent également être affectées.
- FTD version 7.4.4. D’autres versions logicielles peuvent également être affectées.
- /ngfw/etc/sysconfig/iptables contient des lignes non valides/non prises en charge.
- L'administrateur tente de modifier l'adresse IP de gestion FTD à l'aide de la commande configure network ipv4 manual <address> <netmask> <gateway>.

Résolution

Analyse

1. Le message « Network settings changed » est manquant dans le résultat de la commande configure network ipv4 manual <address> <netmask> <gateway :

<#root>

>

configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254

Setting IPv4 network configuration...

2. Un message « Network settings changed » manquant indique que l'opération est incomplète.

Le résultat attendu :

<#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 existe des journaux pertinents dans le fichier /ngfw/var/log/messages sans indiquer la cause racine :

```
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
...
```

Les autres fichiers tels que process_stderr.log ou process_stdout.log dans /ngfw/var/log/ ne contiennent pas de journaux pertinents.

4. En raison de l'absence de journaux, l'étape suivante consiste à exécuter l'utilitaire de trace et à examiner les appels système. La commande CLISH configure network ipv4 manual exécute une action en mode expert. C'est un 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

…

La commande complète strace :

<#root>

firewall #

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

Explication des arguments :

· -t - Préfixe chaque appel système suivi avec l'heure actuelle (heures:minutes:secondes).

· -y - Affiche les chemins des descripteurs de fichiers. Lorsqu'un appel système utilise un descripteur de fichier, strace imprime le chemin d'accès associé (s'il est connu), ce qui facilite l'identification des fichiers, des sockets ou des canaux auxquels on accède.

· -f - Traçage des processus enfants. Si le programme suivi crée de nouveaux processus, trace continue également à suivre ces enfants.

· -s 1024 - Augmentez la taille maximale des arguments de chaîne imprimés à 1024 octets. Par défaut, strace tronque les chaînes longues (généralement à 32 octets). Cela est utile pour afficher les arguments de ligne de commande complets, les tampons ou les noms de fichiers.

· -o /ngfw/var/common/strace.out - Écrire toutes les sorties de trace dans le fichier spécifié au lieu de l'erreur standard.

5. L’inspection du code de sortie de différents processus révèle que le processus /usr/sbin/iptables-restore avec le PID 7793 est sorti avec le code d’erreur 2, contrairement à d’autres avec le code de sortie 0 ou 1.

La commande trace affiche également une ligne "Bad 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. Ce processus analyse et réapplique les règles iptables Linux à partir du fichier /ngfw/etc/sysconfig/iptables. Dans ce cas, le fichier contient des lignes non valides/non prises en charge pour des raisons inconnues :

<#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
```

En outre, le fichier /ngfw/var/log/initialize.log peut contenir des lignes qui pointent vers l'échec de redémarrage iptables en raison d'un argument incorrect dans le fichier :

<#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.)
```

Solution de contournement

1. Accédez à la console du pare-feu et passez en mode expert :

<#root>

```
>

expert


firewall:~$

sudo su
```

2. Effectuez la sauvegarde des fichiers iptables existants :

<#root>

```
firewall#

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

3. Supprimez toutes les lignes non prises en charge et incorrectes. Notez que, selon le matériel,

les versions logicielles et la configuration, le contenu des iptables peut varier. La configuration de référence peut être obtenue à partir de la configuration des travaux pratiques avec les mêmes versions matérielles et logicielles.

4. Redémarrez 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. Reconfigurez l'adresse IP de gestion sur FTD CLISH.

Motif

Les entrées non valides/non prises en charge dans le fichier /ngfw/etc/sysconfig/iptables entraînent une interruption prématurée de la modification de l'adresse IP. Ceci est suivi dans l'ID de bogue Cisco CSCwv52279.

Autres informations utiles

- ID de bogue Cisco CSCwv52279.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.