iptables 파일에서 유효하지 않거나 지원되지 않는 라인으로 인한 FTD IP 주소 변경 실패 트러블슈팅

목차

문제

configure network ipv4 manual <address> <netmask> <gateway> 명령을 사용하여 구성된 새로운 FTD(Secure Firewall Threat Defense) 관리 IP 주소가 적용되지 않았습니다.

"IPv4 네트워크 컨피그레이션 설정" 메시지가 표시되고 프롬프트가 반환됩니다.

그럼에도 불구하고 show network 명령은 기존 IP 주소를 반영합니다.

<#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
```

환경

- Firepower 2110 보안 방화벽 위협 방어. 다른 하드웨어 플랫폼도 영향을 받을 수 있습니다.
- FTD 버전 7.4.4. 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- /ngfw/etc/sysconfig/iptables 파일에 유효하지 않거나 지원되지 않는 행이 있습니다.
- 관리자는 configure network ipv4 manual <address> <netmask> <gateway> 명령을 사용하여 FTD 관리 IP 변경을 시도합니다.

해결

분석

1. configure network ipv4 manual <address> <netmask> <gateway> 명령 출력에 "Network settings changed"라는 메시지가 없습니다.

<#root>

>

configure network ipv4 manual 192.0.2.100 255.255.255.0 192.0.2.254

```
Setting IPv4 network configuration...
```

2. "Network settings changed(네트워크 설정 변경됨)" 메시지가 없으면 작업이 완료되지 않았음을 나타냅니다.

예상 출력:

<#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. 근본 원인을 정확히 파악하지 않고 /ngfw/var/log/messages 파일에 관련 로그가 있습니다.

```
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/의 process_stderr.log 또는 process_stdout.log와 같은 다른 파일에는 관련 로그가 포함되어 있지 않습니다.

4. 로그가 부족하여 다음 단계는 strace 유틸리티를 실행하고 시스템 호출을 조사하는 것입니다. CLISH 명령 configure network ipv4 manual은 expert 모드에서 작업을 실행합니다. 다음은 Perl 스크립트입니다.

<#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}

…

complete strace 명령은 다음과 같습니다.

<#root>

```
firewall #

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

인수 확장:

· -t - 추적된 각 시스템 통화에 현재 시간(시:분:초)을 접두사로 붙입니다.

· -y - 파일 설명자 경로를 표시합니다. 시스템이 파일 설명자를 사용하는 경우, strace는 연결된 경로 이름(알려진 경우)을 인쇄하므로, 액세스하는 파일, 소켓 또는 파이프를 쉽게 식별할 수 있습니다.

· -f - 하위 프로세스 추적 추적한 프로그램이 새로운 과정을 만들면 스트레스는 그 아이들도 계속 추적한다.

· -s 1024 - 인쇄된 문자열 인수의 최대 크기를 1024바이트로 늘립니다. 기본적으로 문자열은 긴 문자열(일반적으로 32바이트)을 자릅니다. 이 기능은 전체 명령줄 인수, 버퍼 또는 파일 이름을 확인하는 데 유용합니다.

· -o /ngfw/var/common/strace.out - 모든 추적 출력을 표준 오류 대신 지정된 파일에 기록합니다.

5. 여러 프로세스에서 종료 코드를 검사한 결과, 종료 코드 0 또는 1의 프로세스/usr/sbin/iptables-restore와 달리 PID 7793이 오류 코드 2로 종료되었습니다.

추적에는 "잘못된 인수 `vi'" 줄도 표시됩니다.

<#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. 이 프로세스는 /ngfw/etc/sysconfig/iptables 파일에서 Linux iptables 규칙을 구문 분석하고 다시 적용합니다. 이 경우 파일에 알 수 없는 이유로 유효하지 않거나 지원되지 않는 행이 포함되어 있습니다.

<#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
```

또한 /ngfw/var/log/initialize.log 파일에는 파일의 잘못된 인수로 인한 iptables 재시작 실패를 가리키는 행이 포함될 수 있습니다.

```
<#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.)
```

해결 방법

1. 방화벽 콘솔에 액세스하고 expert 모드로 전환합니다.

```
<#root>

>

expert
```

```
firewall:~$
```

sudo su

2. 기존 iptables 파일을 백업합니다.

<#root>

```
firewall#
```

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

3. 지원되지 않거나 잘못된 행을 모두 제거합니다. 하드웨어, 소프트웨어 버전 및 컨피그레이션에 따라 iptable의 내용이 다를 수 있습니다. 기본 구성은 동일한 하드웨어 및 소프트웨어 버전을 사용하여 랩 설정에서 가져올 수 있습니다.

4. iptables를 다시 시작합니다.

<#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 CLISH에서 관리 IP 주소를 다시 구성합니다.

원인

/ngfw/etc/sysconfig/iptables 파일에서 유효하지 않거나 지원되지 않는 항목으로 인해 IP 주소 변경이 중간에 중단됩니다. 이는 Cisco 버그 ID CSCwv52279에서 추적됩니다.

관련 콘텐츠

- Cisco 버그 ID CSCwv52279.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.