أستكشاف أخطاء تغيير عنوان IP ل FTD وإصلاحها بسبب وجود خطوط غير صحيحة وغير مدعومة في ملف IPTABLES

المحتويات

مسألة

يتم تطبيق الأمر configure network ipV4 manual <address> <netmask> <gateway>IP الخاصة بإدارة تحديد جدار الحماية الآمن (FTD) الجديد باستخدام الأمر <netmask> <gateway>IP الخاصة بإدارة تحديد جدار الحماية الآمن (FTD) الجديد باستخدام الأمر configure network ipV4 manual <address> <netmask>.

يتم عرض الرسالة "إعداد تكوين شبكة IPv4" وإرجاع المطالبة.

ومع ذلك، يعكس الأمر show network عنوان IP القديم:

```
<#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
```

البيئة

- Firepower 2110 الذي يشغل حماية الحماية ضد التهديد باستخدام جدار الحماية الآمن. يمكن أن تتأثر أيضا منصات الأجهزة الأخرى.
- الإصدار 7.4.4 من FTD. يمكن أن تتأثر أيضا إصدارات البرامج الأخرى.
- تحتوي ملفات /ngfw/etc/sysconfig/iptables على أسطر غير صحيحة/غير مدعومة.
- يحاول المسؤول تغيير IP الخاص بإدارة FTD باستخدام الأمر configure ipV4 manual <address> <netmask> <gateway>.

قرار

تحليل

1. الرسالة "تم تغيير إعدادات الشبكة" مفقودة في إخراج الأمر configure 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. تشير الرسالة "تم تغيير إعدادات الشبكة" المفقودة إلى أن العملية غير مكتملة.

الناتج المتوقع:

```
<#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. هناك سجلات ذات صلة في الملف /ngfw/var/log/messages دون الإشارة إلى السبب الجذري:

```
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
                                                                                          ...
```

لا تحتوي الملفات الأخرى مثل process_stdout.log in /ngfw/var/log/ وأ process_stderr.log على السجلات ذات الصلة.

4. نظر لنقص السجلات، تتمثل الخطوة التالية في تشغيل الأداة المساعدة Strace لتشغيل أمر CLISH configure network ipV4 manual والتحقيق في مكالمات النظام. يقوم بذلك نص برمجي. هذا نص برمجي في وضع الخبير إجراء:

```
<#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="`|$&lt;&gt;&amp;()#\'*!"
/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}

…
```

أمر السلسلة الكاملة:

<#root>

firewall #

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

توسيع نطاق الحجج:

· -t - قم ببادئة إستدعاء كل نظام تم تتبعه مع الوقت الحالي من اليوم (الساعات:الدقائق:ثوان).

· -y - إظهار مسارات واصف الملف. عندما يستخدم syscall واصف ملف، يقوم السلسلة بطباعة اسم المسار المقترن (إذا كان ذلك معروفا)، مما يسهل التعرف على أي الملفات، المقابس، أو المواسير التي يتم الوصول إليها.

· -f - تتبع العمليات التابعة. إذا قام البرنامج المتتبع بإنشاء عمليات جديدة، تستمر Strace في تتبع هؤلاء الأطفال أيضا.

· -s 1024 - قم بزيادة الحد الأقصى لحجم وسيطات السلسلة المطبوعة إلى 1024 بايت. بشكل افتراضي، تقوم السلسلة باقتطاع سالسل طويلة (بشكل خاص عند 32 بايت). يفيد ذلك في رؤية وسيطات سطر الأوامر الكامل، المخازن المؤقتة، أو أسماء الملفات.

· -o /ngfw/var/common/strace.out - اكتب جميع مخرجات التتبع إلى الملف المحدد بدلا من الخطأ القياسي.

5. يكشف فحص رمز الخروج من عمليات مختلفة أن العملية /USR/sbin/iptables-restore مع PID 7793 تم إنهاؤه مع رمز الخطأ 2، بخلاف الآخرين مع رمز الخروج 0 أو 1.

ظهر التتبع أيضا سطر "حجة سيئة '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

, "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. تقوم هذه العملية بتحليل وإعادة تطبيق قواعد Linux IPTABLES من ملف /ngfw/etc/sysconfig/iptables. في هذه الحالة، يحتوي الملف على خطوط غير صحيحة/غير معتمدة/غير معروفة لأسباب:

```
<#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
```

بالإضافة إلى ذلك، يمكن أن يحتوي الملف /ngfw/var/log/initialize.log على أسطر تشير إلى فشل إعادة تشغيل IPTABLES ظرا لوجود وسيطة غير صحيحة في الملف:

```
<#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.)
```

الحل

1. الوصول إلى وحدة تحكم جدار الحماية والتبديل إلى وضع الخبراء:

```
<#root>

>
```

```
expert
```

```
firewall:~$
```

```
sudo su
```

2. قم بإجراء النسخ الاحتياطي لملفات جداول البيانات الموجودة:

<#root>

```
firewall#
```

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

3. قم بإزالة كافة الخطوط غير المدعومة وغير الصحيحة. لاحظ أنه، وفقا للأجهزة وإصدارات الطراز والتهيئة، يمكن أن يختلف محتوى جداول البيانات. يمكن الحصول على تكوين الخط الأساسي من إعداد المختبر باستخدام نفس إصدارات الأجهزة والبرامج.

4. قم بإعادة تشغيل ملفات الإنترنت:

<#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. إعادة تكوين عنوان IP الخاص بالإدارة على FTD CLISH.

السبب

مقاطعة سابقة /ngfw/etc/sysconfig/iptables في المدعومة/غير الصالحة/غير الإدخالات ينتج عن. يتم تعقب هذا في معرف تصحيح الأخطاء من Cisco CSCwv52279 لأوانها لتغيير عنوان IP.

المحتوى ذي الصلة

- معرف تصحيح الأخطاء من Cisco CSCwv52279.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).