# Recreación de imágenes de FireSIGHT Management Center y FirePOWER Appliance

## Contenido



## Introducción

Este documento describe los procesos con ejemplos para el procedimiento de recreación de imágenes de un Cisco FireSIGHT Management Center (FMC) y appliances FirePOWER.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

| Dispositivo administrado | Centro de administración de FireSIGHT | Versiones de software disponibles para recreación de imágenes |
|---|---|---|

| | | |
|---|---|---|
| Cisco Firepower de la serie 7000<br><br>Cisco Firepower de la serie 7100<br><br>Cisco Firepower de la serie 8100<br>Cisco Firepower de la serie 8200 | FS 750<br>FS 1500<br>FS 3500 | 5.2 o posterior |
| Firepower serie 8300<br><br>Cisco AMP 7150<br>Cisco AMP 8150 | | 5.3 o posterior |

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Proceso de recrear imágenes

⚠ Precaución: no inserte un dispositivo de almacenamiento USB ni enchufe un conmutador de teclado, vídeo y ratón (KVM) al actualizar o recrear imágenes de FireSIGHT Management Center o un equipo FirePOWER.

## Antes de comenzar

1. Si tiene pensado recrear imágenes de un Management Center o un dispositivo Firepower independiente, se recomienda realizar una copia de seguridad del dispositivo antes de continuar.
2. Identifique el modelo de su sensor y utilice la lista de modelos en la sección Componentes Utilizados para verificar que esta guía es apropiada.
3. Descargue la guía de instalación y la imagen de disco adecuadas para la versión de software deseada desde el sitio de soporte de Cisco.

   ✎ Nota: No cambie el nombre de un fichero .iso

   Servir la imagen: el archivo .iso debe copiarse en un host que ejecute un servidor SSH accesible desde la red de administración del dispositivo para que se vuelva a crear la imagen.

Nota: Si no hay otro servidor SSH disponible, se puede utilizar un FMC para este proceso.

Verificar la integridad del iso: La suma md5sum de los archivos se proporciona en el lado derecho de la página para la verificación con una utilidad md5sum.

4. Las guías de instalación contienen instrucciones paso a paso para la recreación de imágenes y también describen varios métodos para el proceso de recreación de imágenes. Las imágenes proporcionadas en este documento se pueden utilizar como referencia.

## Descripción general del proceso de recreación de imágenes

Nota: La versión 5.3 fue utilizada para capturar las imágenes mostradas en este artículo. El proceso de recreación de imágenes es idéntico para otras versiones 5.x, excepto para los números de versión que aparecen en las imágenes mostradas.

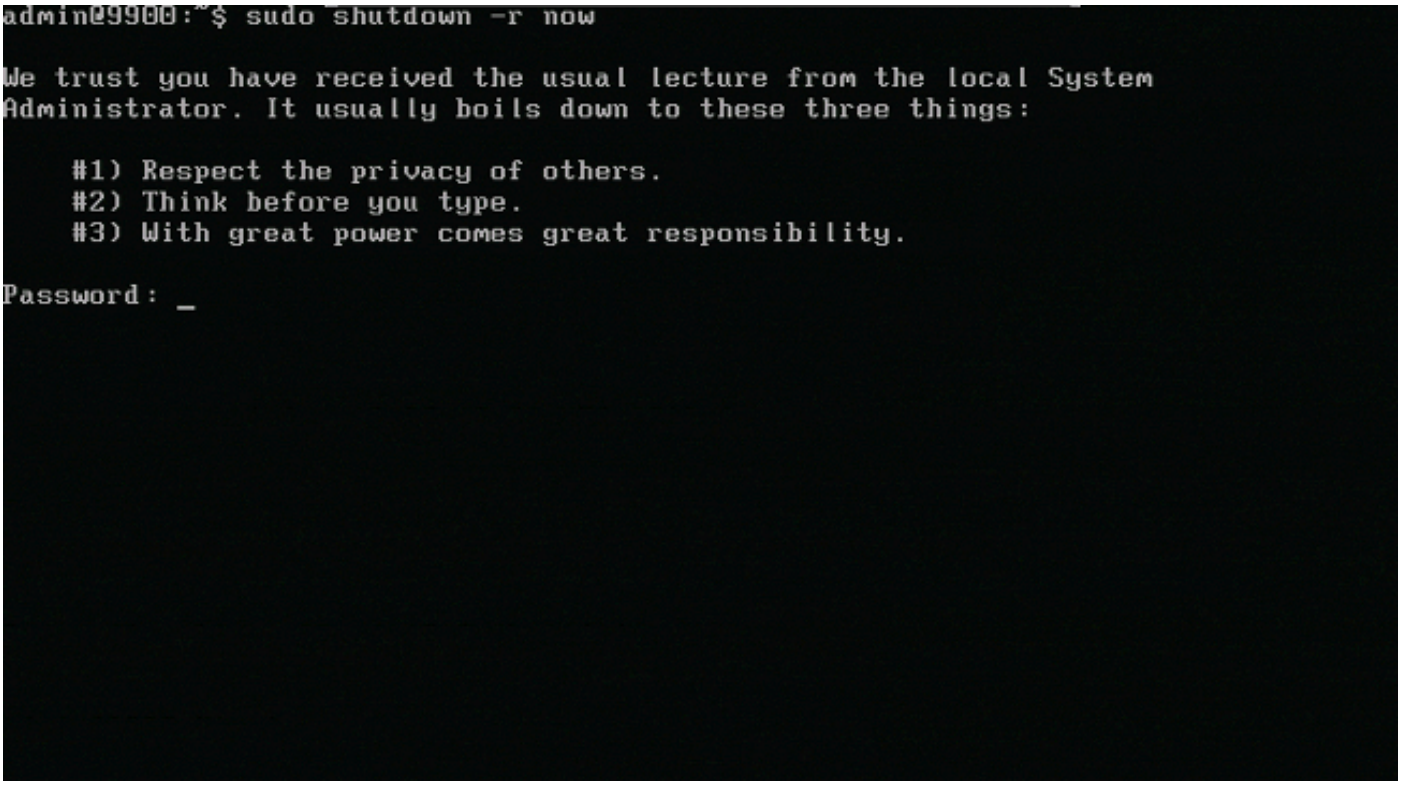



Figure 1


Figura 2: Cuando el sistema se reinicie, presione una tecla de flecha en el teclado para detener la cuenta atrás y elegir la opción System_Restore para la pantalla que se muestra a continuación.

---

Nota: Si el mensaje System_Restore no se muestra, debe cambiar el orden de arranque para arrancar directamente en la partición Restore (DOM). Para obtener más información, vea Falta la opción de menú System_Restore LILO.

---


Figure 3


Figura 4: Elija la opción 0 si utiliza un teclado y un monitor.

Nota: A veces se ha visto que el menú de la opción Restore (Restaurar) solo se muestra cuando solo la consola está conectada (con el teclado desconectado). Tan pronto como se selecciona la opción de recuperación, el teclado se puede conectar de nuevo

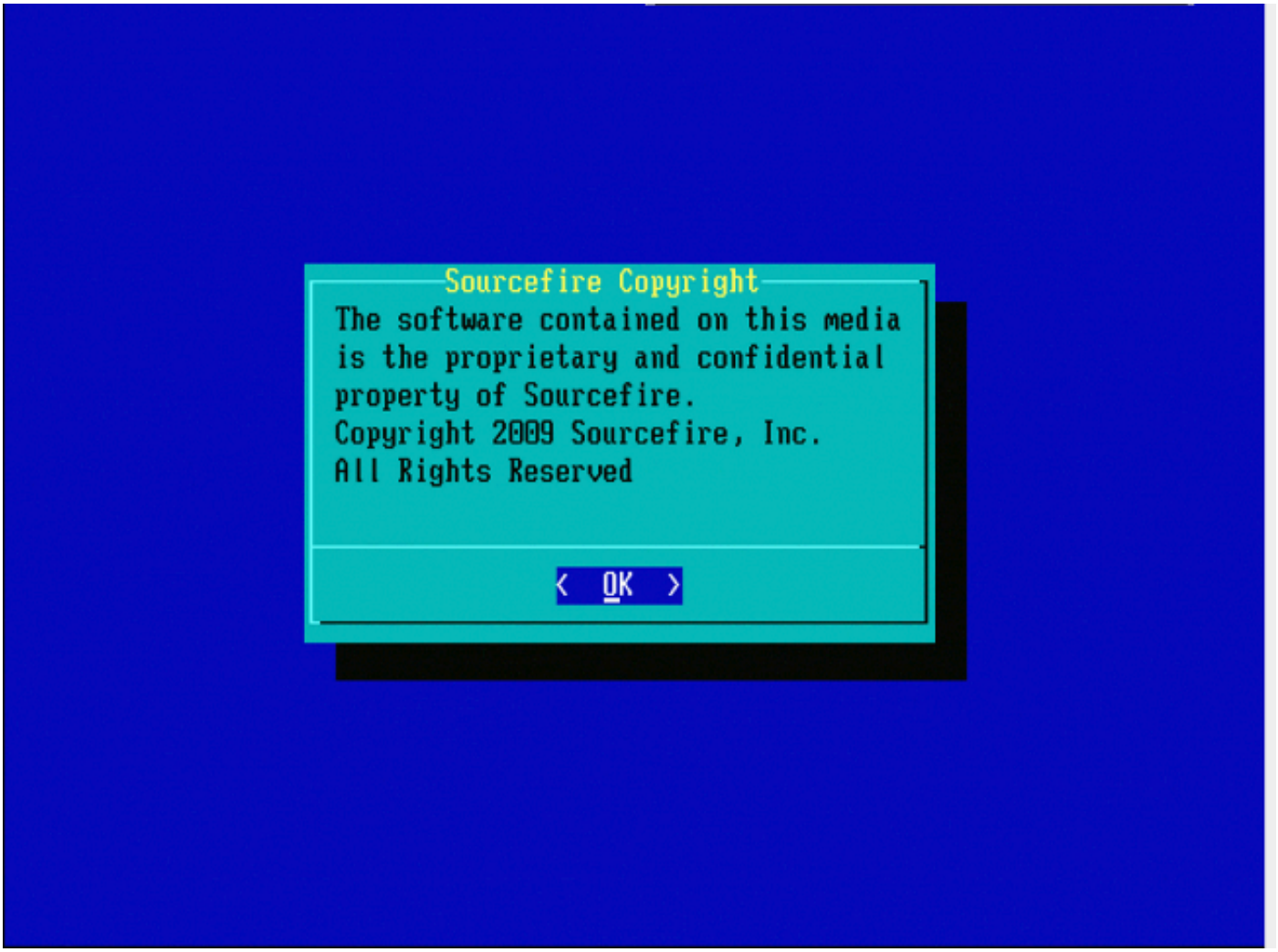



Figure 5


Sourcefire 3D Appliance 5.3.0-52 Configuration Menu
Choose one of the following or press <Cancel> to exit
1 IP Configuration
2 Choose the transport protocol
3 Select Patches/Rule Updates
4 Download and Mount ISO
5 Run the Install
6 Save Configuration
7 Load Configuration
8 Wipe Contents of Disk
< OK >
<Cancel>

‘Figura 6’

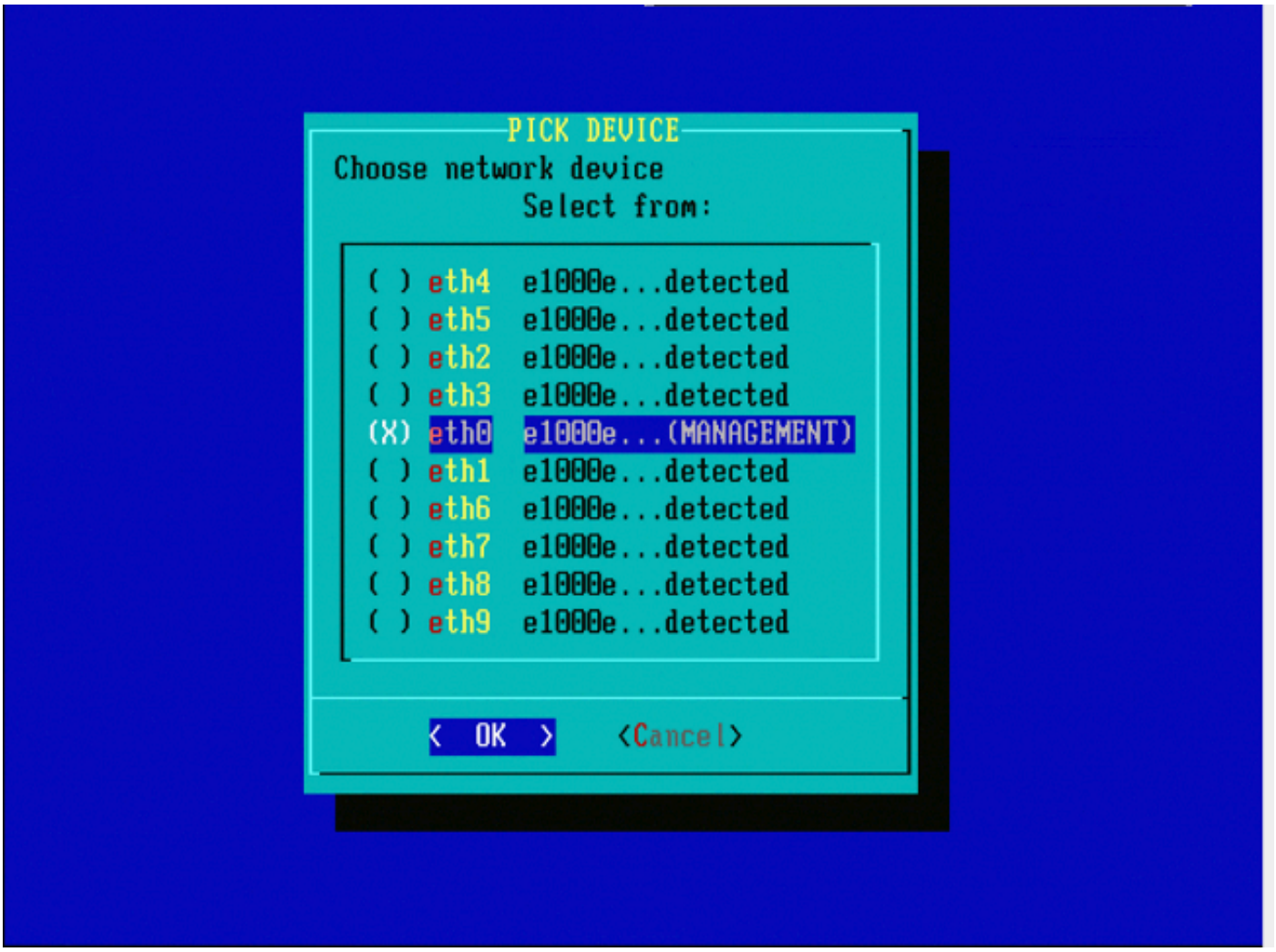



Figura 7: Para seleccionar el dispositivo de red, presione la barra espaciadora.

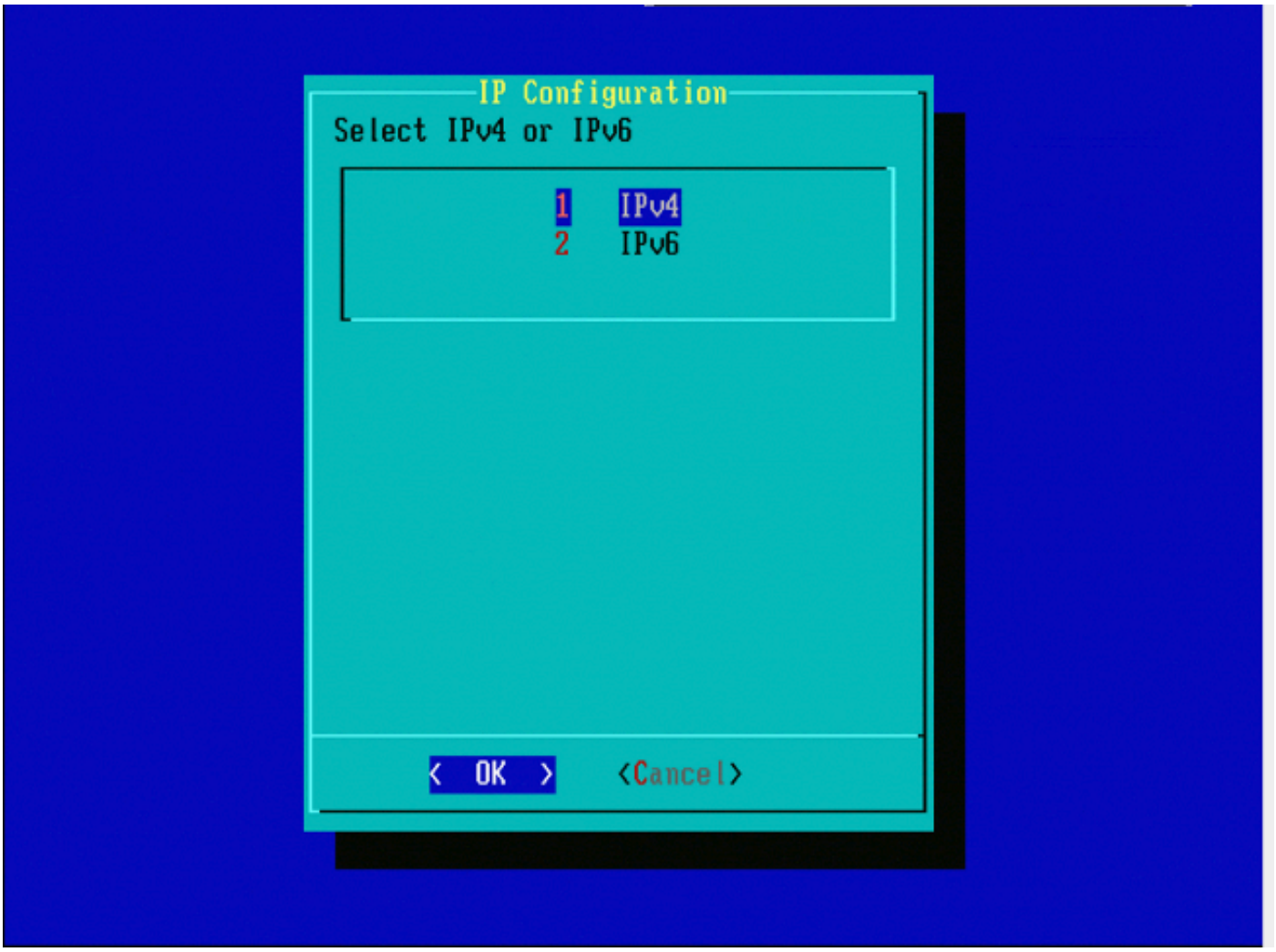



Figura 8

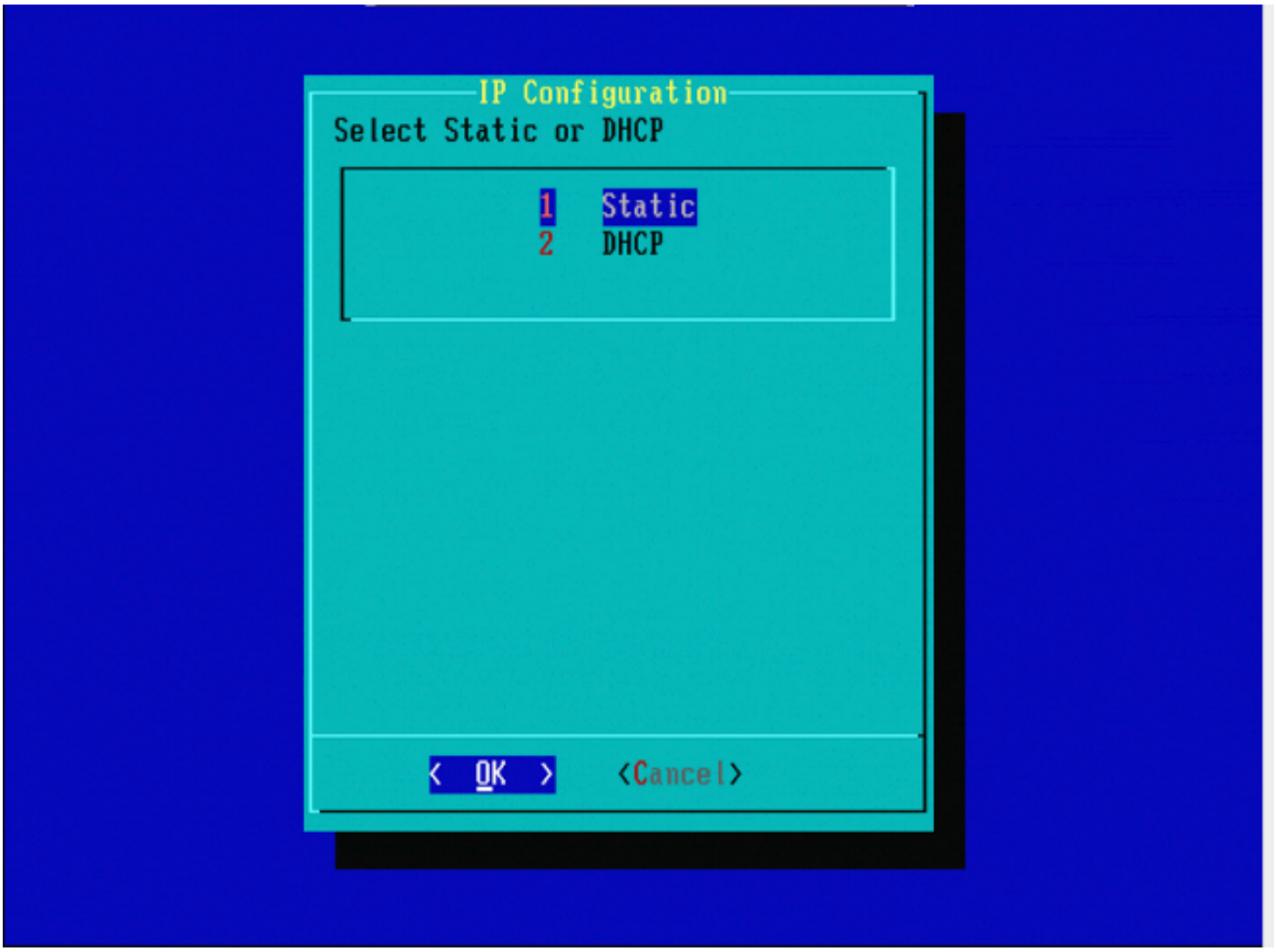

IP Configuration
Select Static or DHCP
1 Static
2 DHCP
< OK >
<Cancel>

Figura 9


IP Address
Enter an IP address for this system:
10.5.30.23
< OK >
<Cancel>

Figura 10


Figura 11


Figura 12


Verify IP Configuration
IP: 10.5.30.23
Netmask: 255.255.0.0
Gateway: 10.5.1.1
< OK >

Figura 13


Sourcefire 3D Appliance 5.3.0-52 Configuration Menu
Choose one of the following or press <Cancel> to exit
1 IP Configuration
2 Choose the transport protocol
3 Select Patches/Rule Updates
4 Download and Mount ISO
5 Run the Install
6 Save Configuration
7 Load Configuration
8 Wipe Contents of Disk
< OK >
<Cancel>

Figura 14


Figura 15: Cisco Support recomienda utilizar el protocolo Secure Copy (SCP).

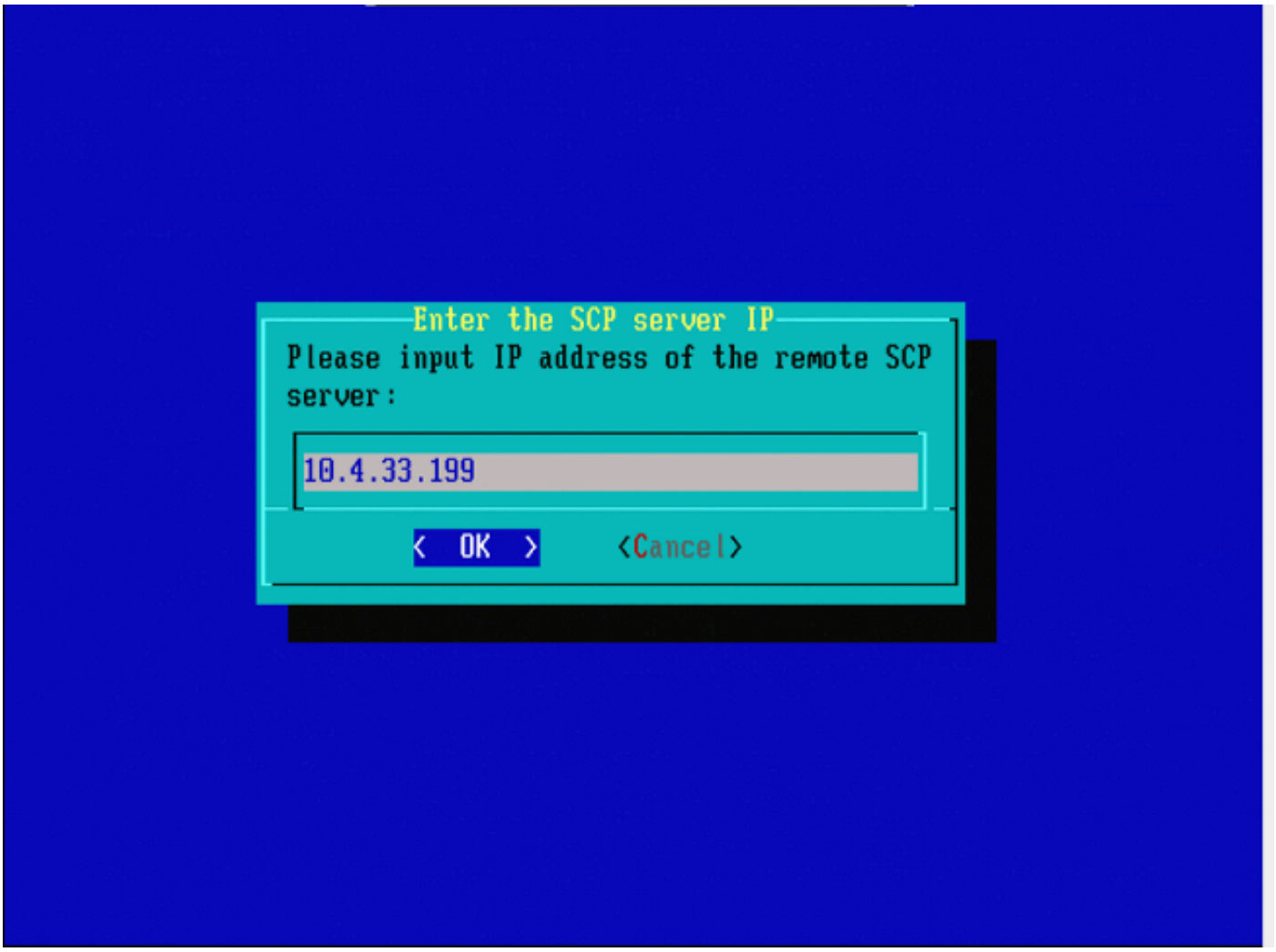



Figura 16: Es posible utilizar FireSIGHT Management Center como servidor SCP para este paso. Continúe con este procedimiento y utilice la dirección IP y las credenciales para Management Center para rellenar los campos del menú Restaurar sistema. Más información en

Se utiliza un servidor de copia segura (SCP) para transferir archivos de forma segura. Si En caso necesario, se puede utilizar un centro de defensa de Sourcefire (DC) como servidor SCP para transferir archivos a otro dispositivo de Sourcefire. Esto puede ser útil cuando una imagen ISO necesita ser transferida a un dispositivo Sourcefire para fines de recreación de imágenes, pero el servidor SCP normal es inalcanzable o no está disponible.

Paso 1. Descargue un archivo .iso adecuado en su escritorio desde el portal de soporte de Sourcefire.
Paso 2. Utilice un cliente SCP y copie el archivo desde el escritorio al centro de defensa.

---

Sugerencia: Un cliente SCP suele estar disponible en un sistema operativo Linux o Mac. Sin embargo, en el sistema operativo Windows, puede tener que instalar un software cliente SCP de terceros. Sourcefire no proporciona recomendaciones ni asistencia para instalar ningún software de cliente SCP específico.

---

El siguiente ejemplo muestra cómo copiar un archivo de imagen .iso de Sourcefire desde el directorio Downloads de un sistema Linux al directorio /var/tmpdel Centro de defensa de

Sourcefire:

<#root>

```
LinuxSystem:~$ cd Downloads
LinuxSystem:~/Downloads$ scp Sourcefire_3D_Sensor_S3-4.10.2-Restore.iso
```

**user_name**

@

**IP_Address_of_Defense_Center**

:/var/tmp

---

⚠ Precaución: no cambie el nombre del archivo .iso. Puede crear un problema con la detección del archivo durante una recreación de imágenes.

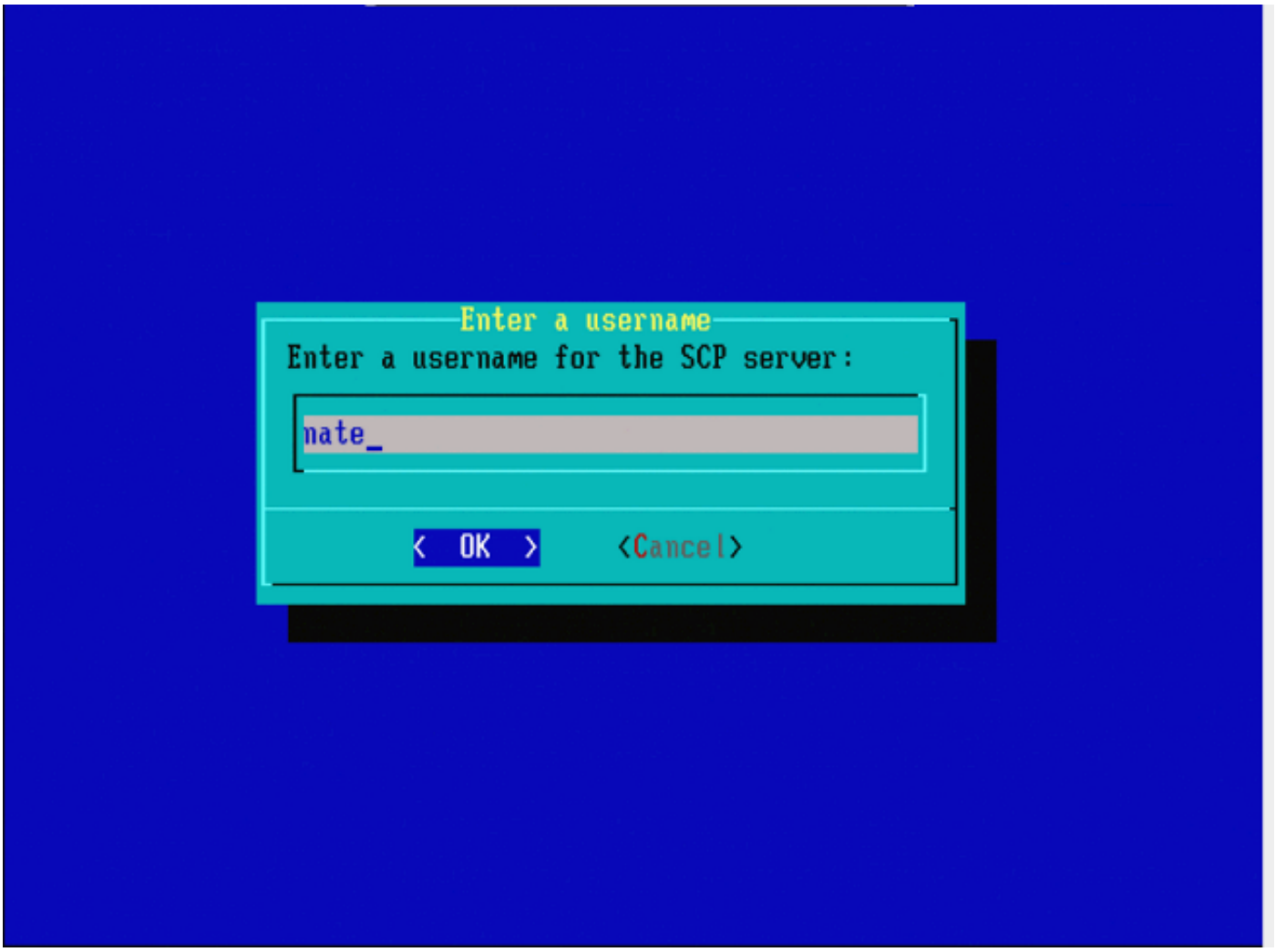
---

Ahora el archivo se copia en el Centro de Defensa. Puede continuar con el proceso de recreación de imágenes de los dispositivos Sourcefire. En la recreación de imágenes, cuando sea necesario, puede proporcionar la dirección IP y el nombre de usuario del DC y la ruta donde copió el archivo de imagen con las instrucciones anteriores.

---

 Advertencia: Una vez finalizada la recreación de imágenes, debe eliminar el archivo .iso del directorio /var/tmp del centro de defensa para reducir el uso del espacio en disco.

---


Enter a username
Enter a username for the SCP server:
nate_
< OK >
<Cancel>

‘Figura 17’

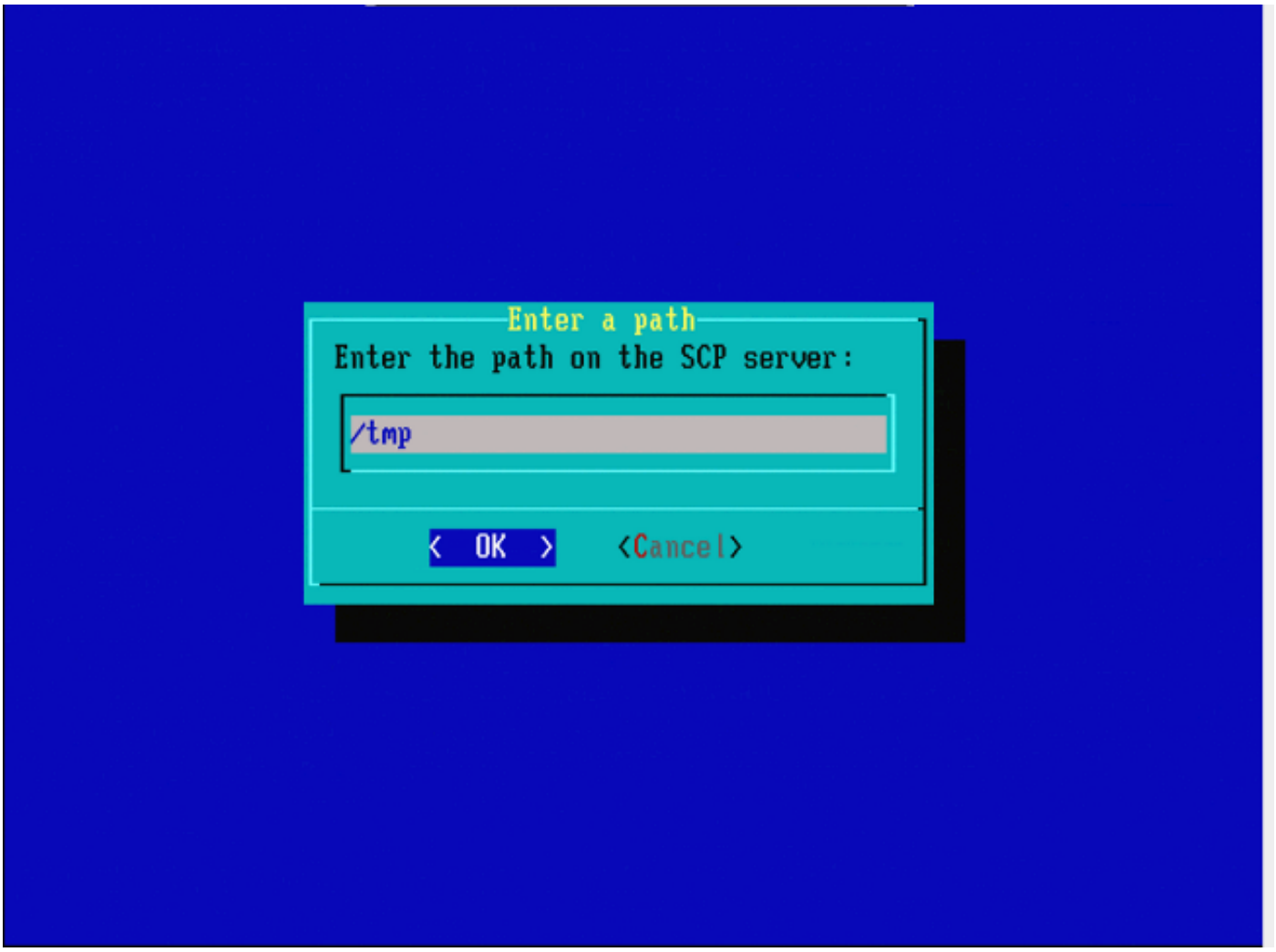



Figura 18

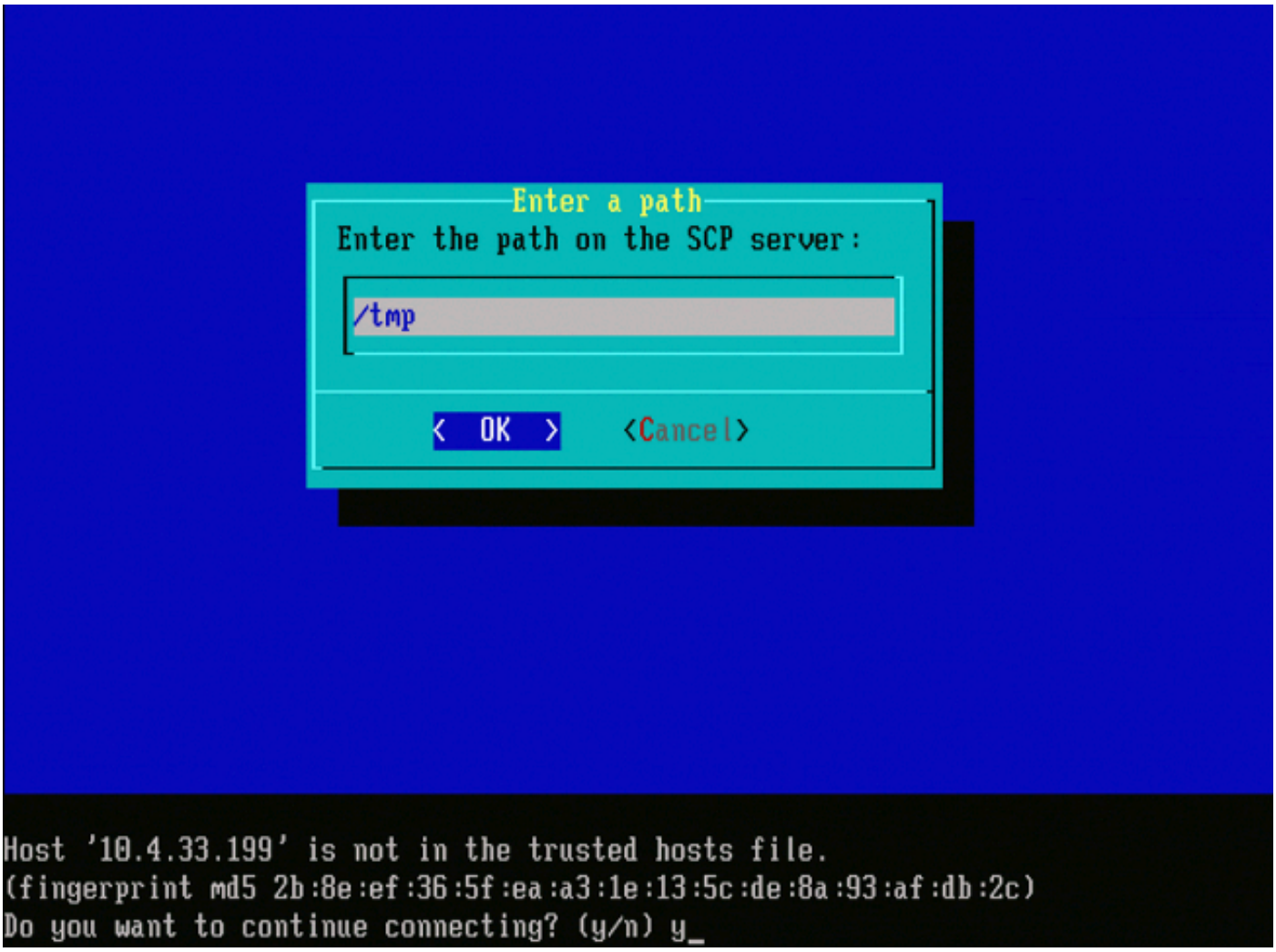



Figura 19

Nota: Si recibe un error de conectividad en este punto en lugar del mensaje esperado, verifique su conexión al servidor SSH.

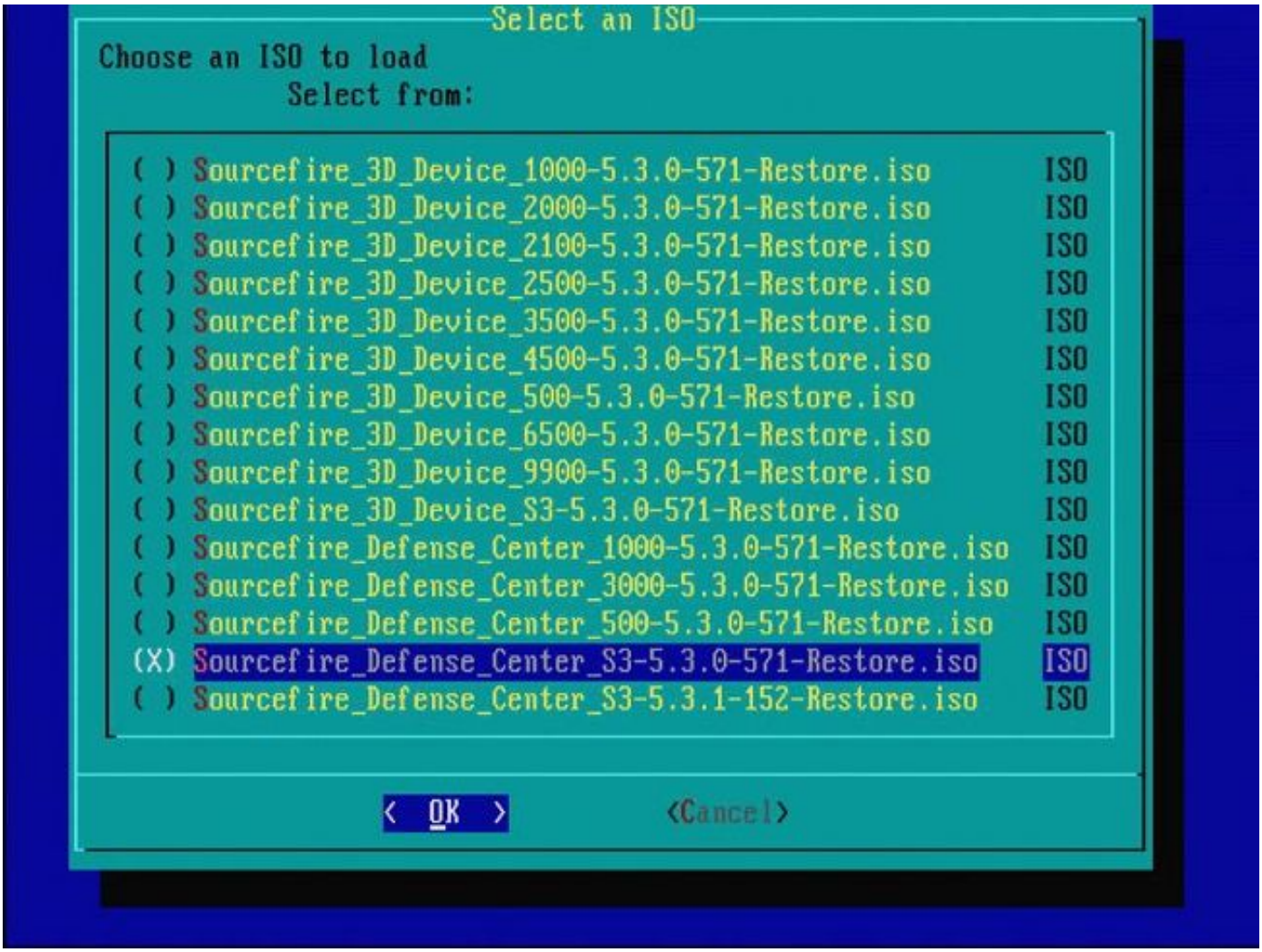



Figura 20 - Para seleccionar la imagen .iso, presione la barra espaciadora.

Nota: Es necesario utilizar los nombres de archivo predeterminados para los archivos .iso o es posible que los archivos no se detecten en este paso.
Error: No se ha encontrado ninguna imagen ISO
En la versión 6.3, la convención de nombres ISO ha cambiado de Sourcefire_3D_Device_S3-<ver>-<build>-Restore.iso a Cisco_Firepower_NGIPS_Appliance-<ver>-<build>-Restore.iso. Si encuentra "No se encontraron imágenes ISO", cambie el nombre del archivo ISO por el nombre de archivo heredado. Esto sucede normalmente cuando una re-imagen de la versión 6.2.x o anterior a la versión 6.3.0 o posterior.

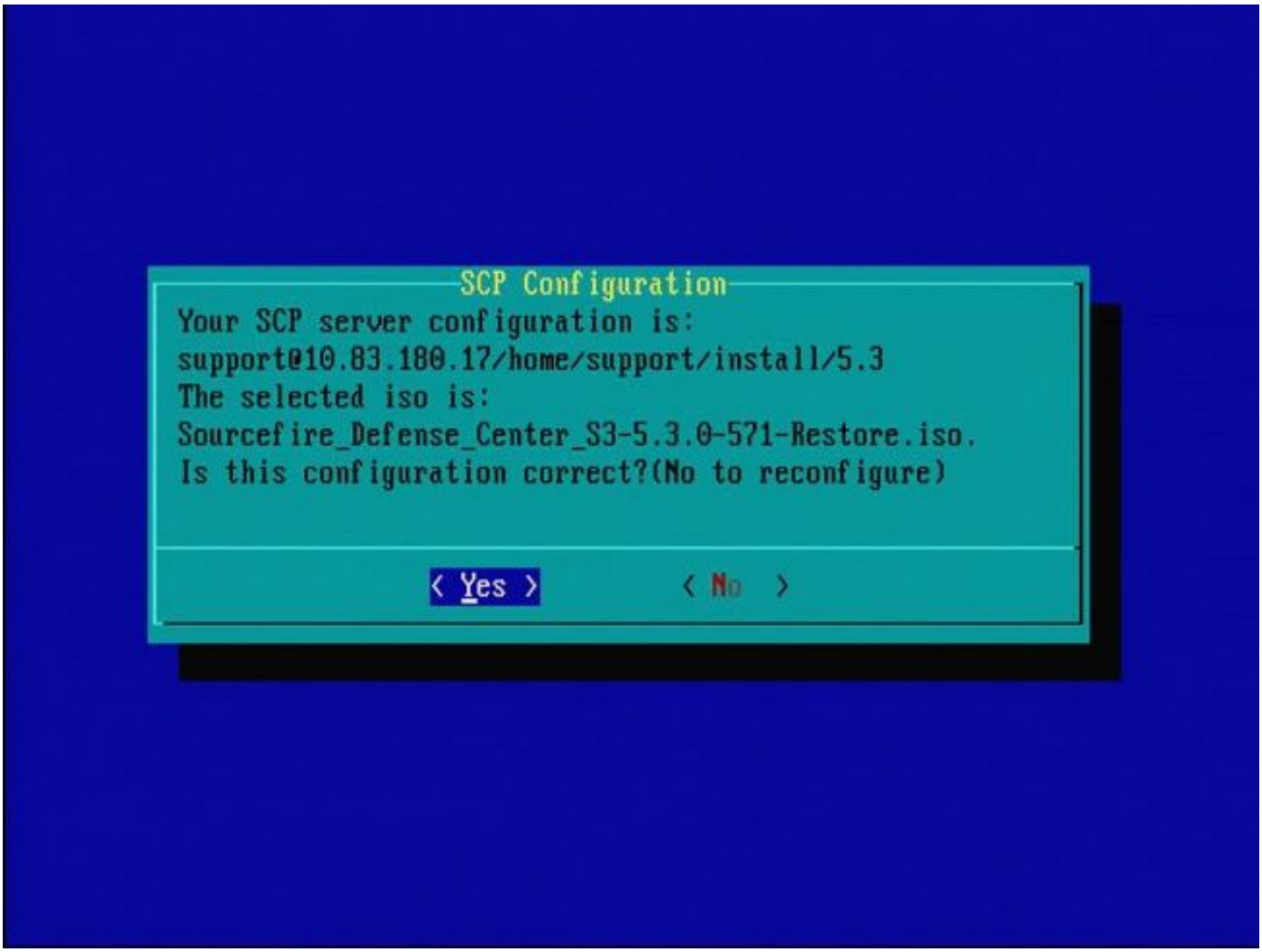

SCP Configuration
Your SCP server configuration is:
support@10.83.180.17/home/support/install/5.3
The selected iso is:
Sourcefire_Defense_Center_S3-5.3.0-571-Restore.iso.
Is this configuration correct?(No to reconfigure)
< Yes >
< No >

Figura 21


Figura 22 - El Soporte de Cisco recomienda saltarse el paso 3 en este proceso. Los parches y las actualizaciones de reglas de snort (SRU) se pueden instalar una vez finalizada la recreación de imágenes.

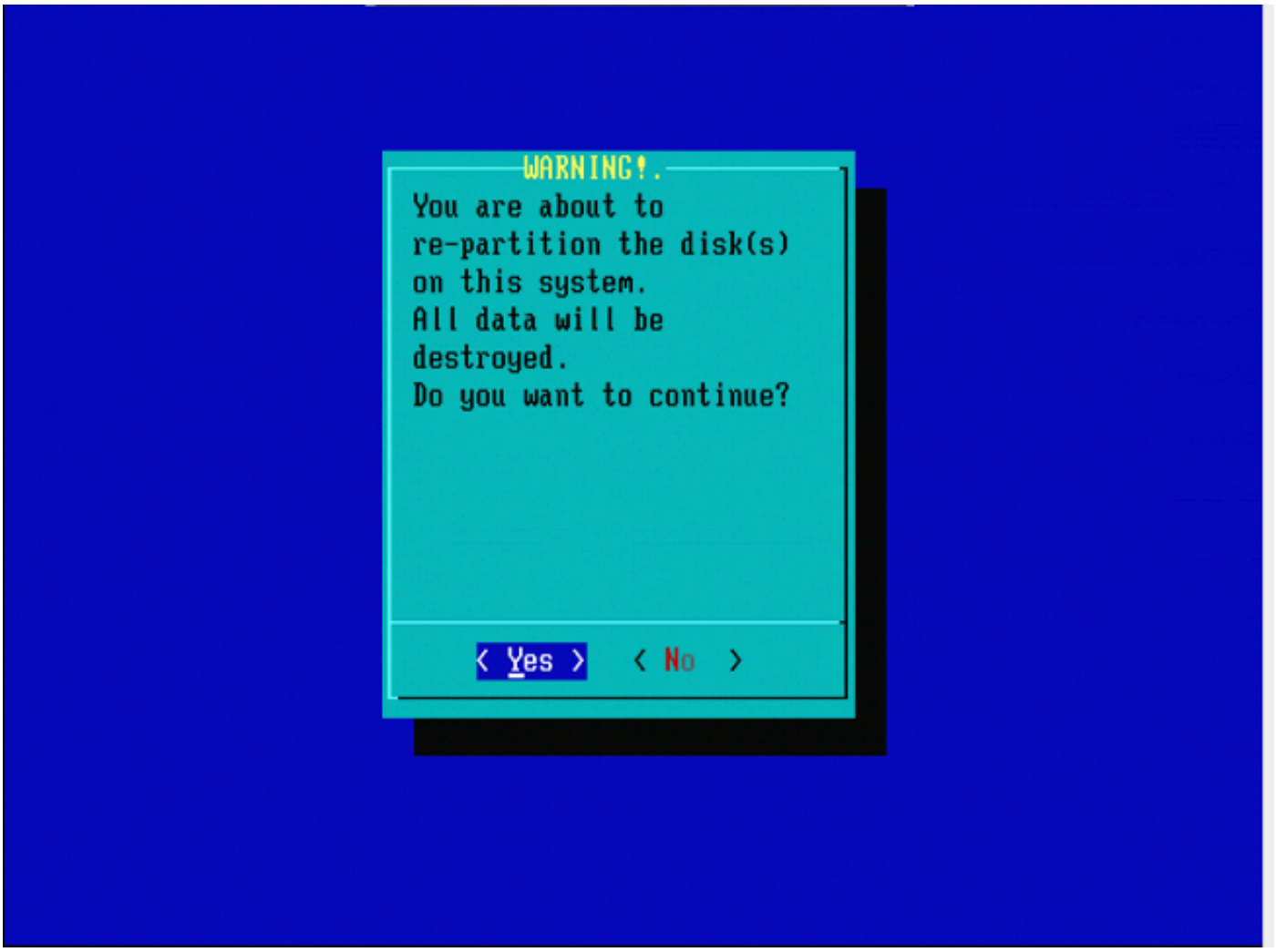
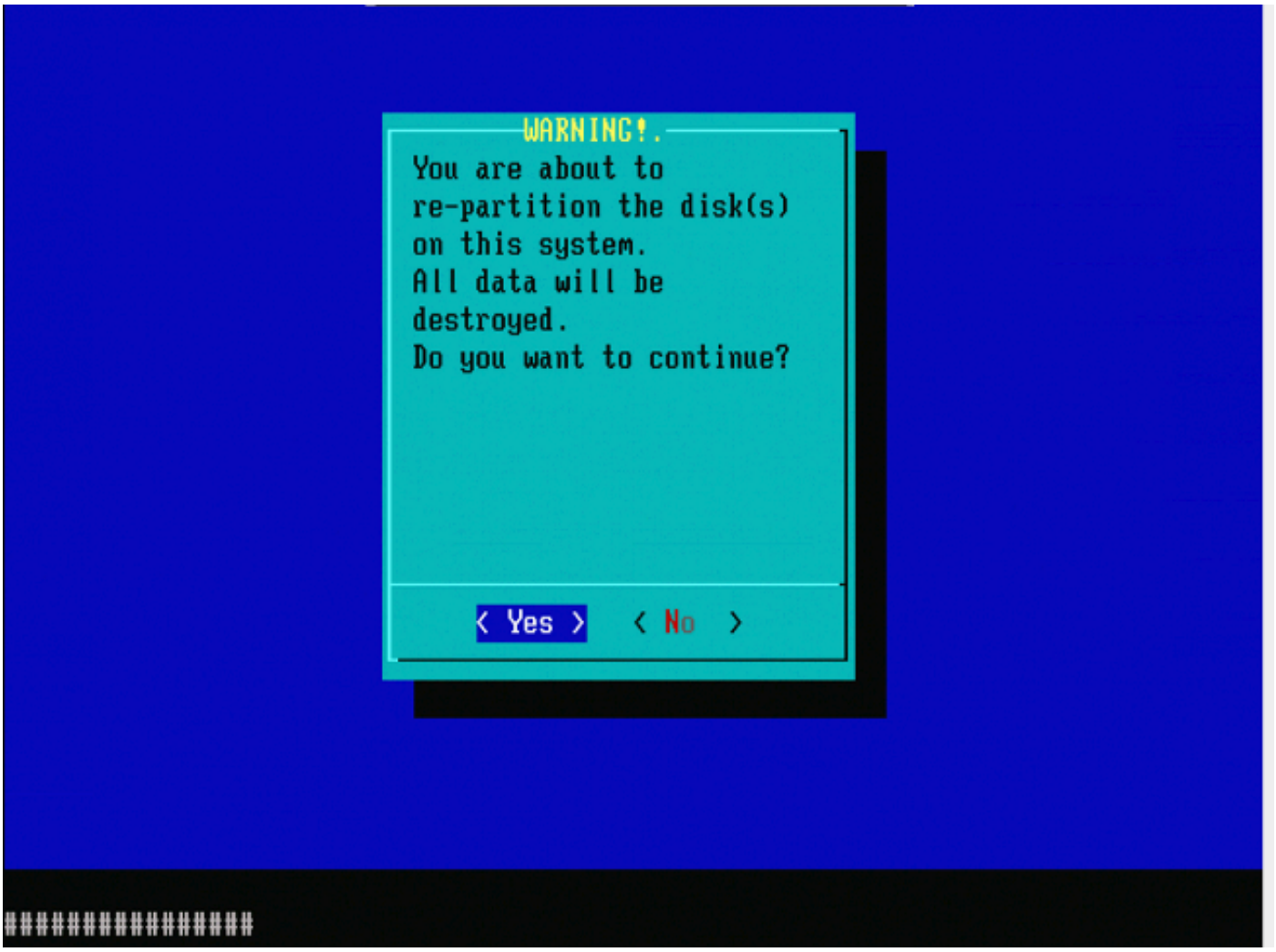

WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >

Figura 23


WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >
##################

‘Figura 24’

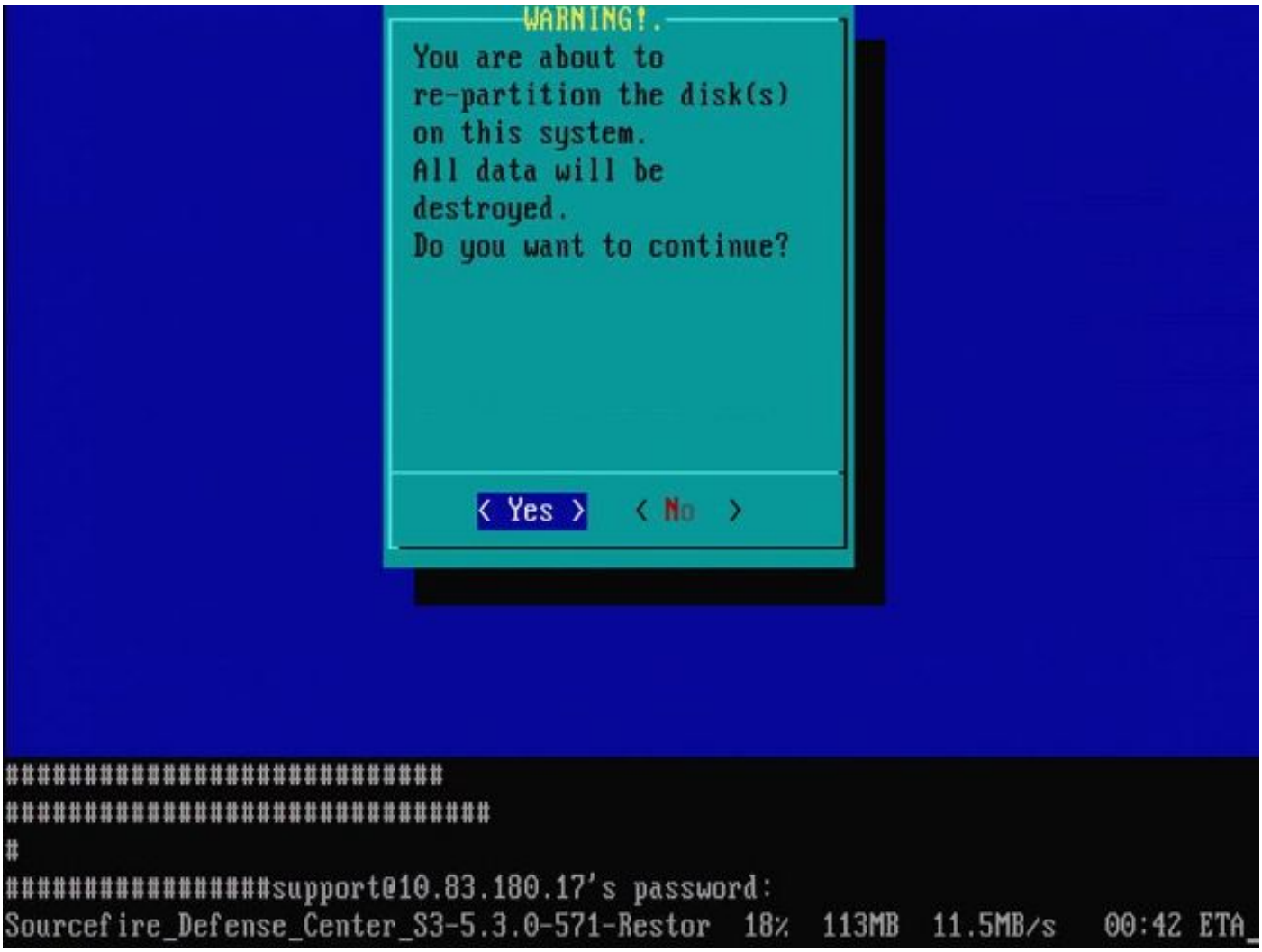

WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >
##############################
##################################
#
##################support@10.83.180.17's password:
Sourcefire_Defense_Center_S3-5.3.0-571-Restor 18% 113MB 11.5MB/s 00:42 ETA

Figura 25


Figura 26

Nota importante con respecto a la recreación de imágenes de una versión de software principal diferente: Si intenta crear una nueva imagen de un dispositivo que previamente ejecutó una versión de software principal diferente, como si vuelve a crear imágenes de 5.1 > 5.2, 5.2 > 5.3, 5.3 > 5.2, etc., debe completar los pasos que se muestran en las Figuras 1 - 26 dos veces.

1. Después de elegir OK en el mensaje como se muestra en la imagen 26, la partición Restaurar sistema se parpadea a la nueva versión y el dispositivo se reinicia.
2. Después del reinicio, debe comenzar de nuevo el proceso de recreación de imágenes desde el principio y continuar con el proceso representado en las Figuras 27b a 31.

Si esta es la primera recreación de imágenes de una versión de software principal diferente, verá la pantalla como se muestra en la imagen 27a y, a continuación, las Figuras 31 y 32.

---

⚠ Precaución: si ve esta pantalla, existe un posible retraso sin salida visible después de "Comprobar hardware" y antes de "El dispositivo USB...". No presione ninguna tecla en este momento, o el dispositivo se reinicia en un estado inutilizable y necesita ser recreado una vez más.

---

Si no es así, puede ver las pantallas de la Figura 27b a la Figura 32.

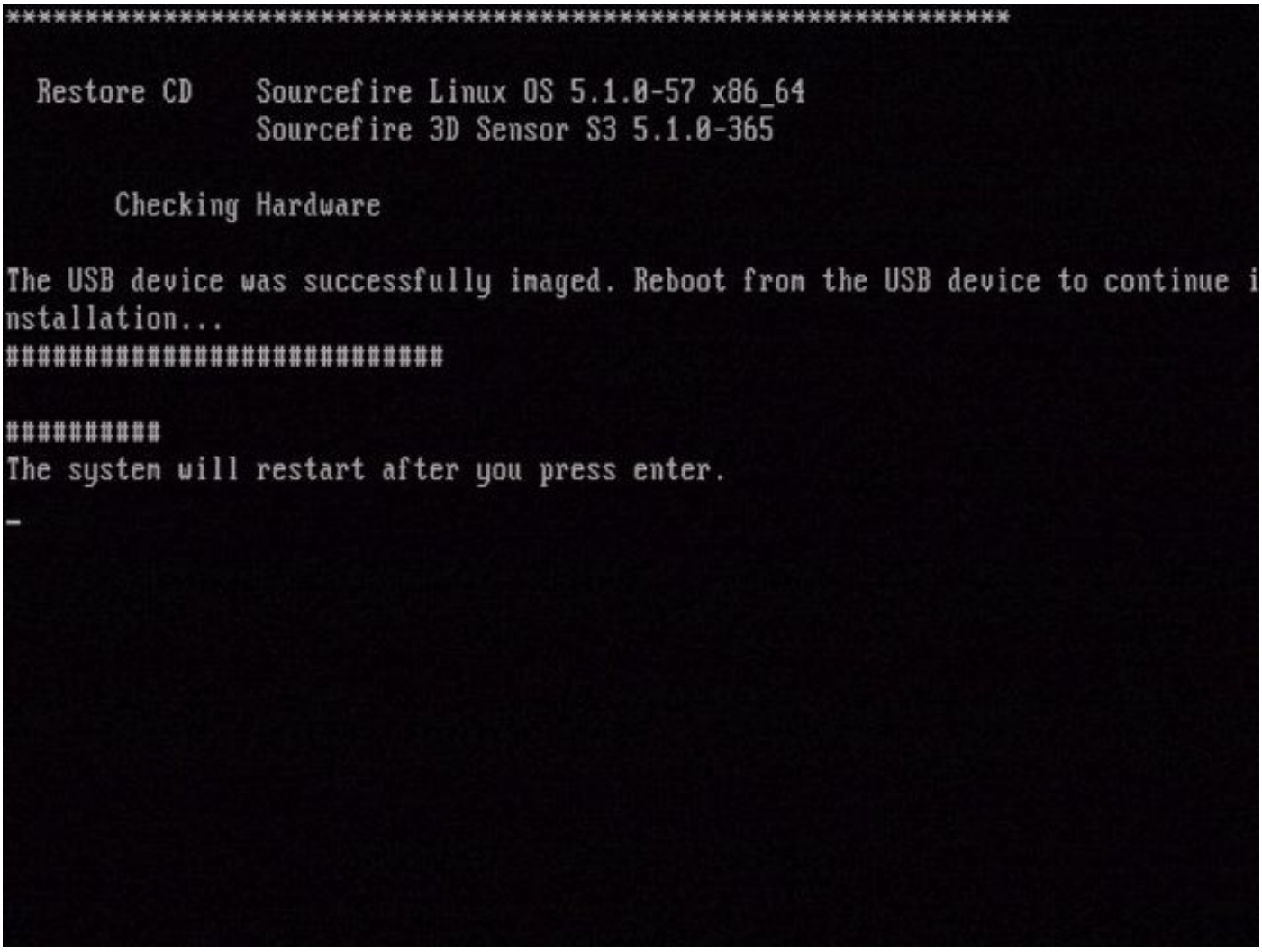



Figura 27a

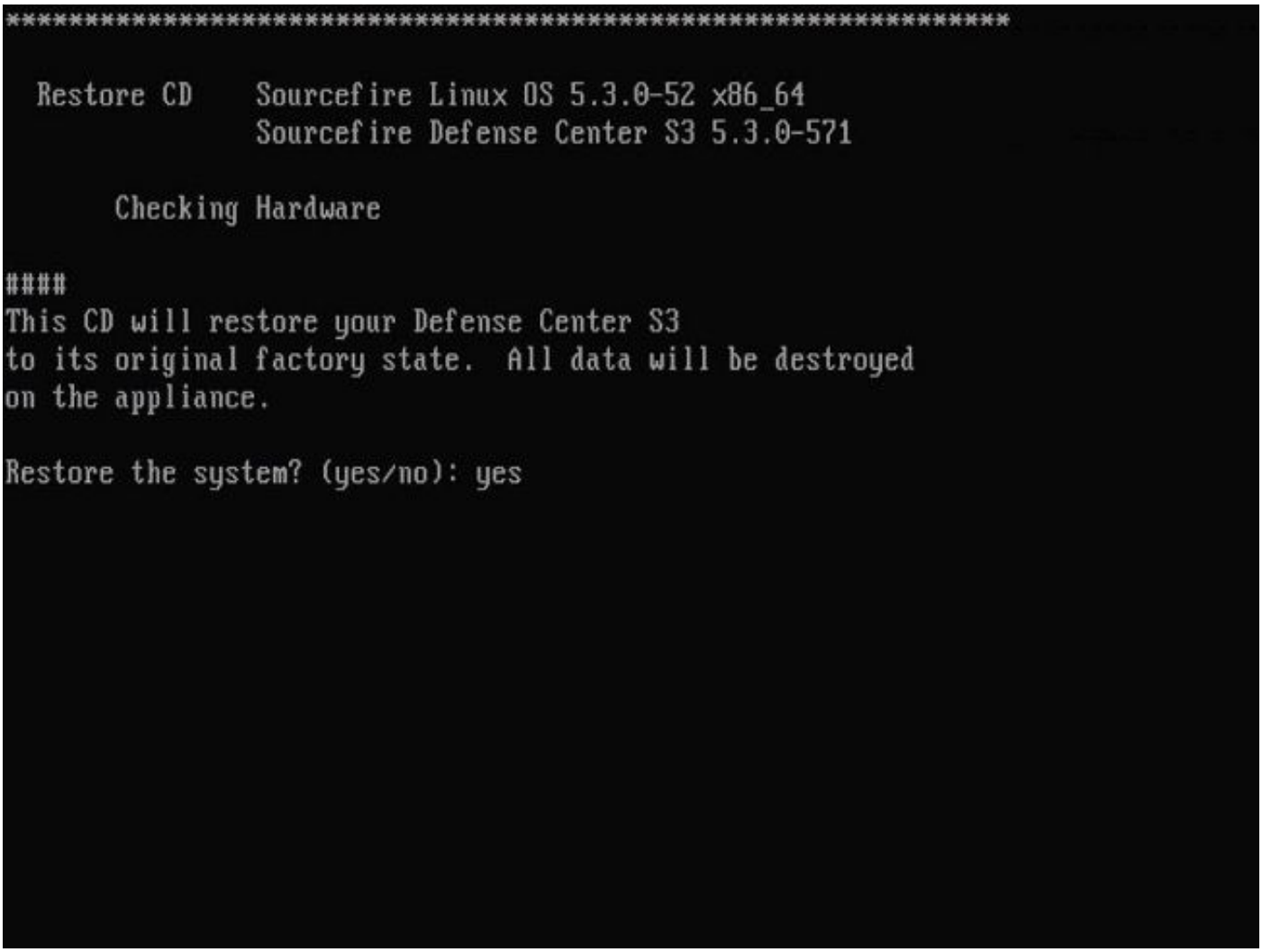

**********
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes

Figura 27b

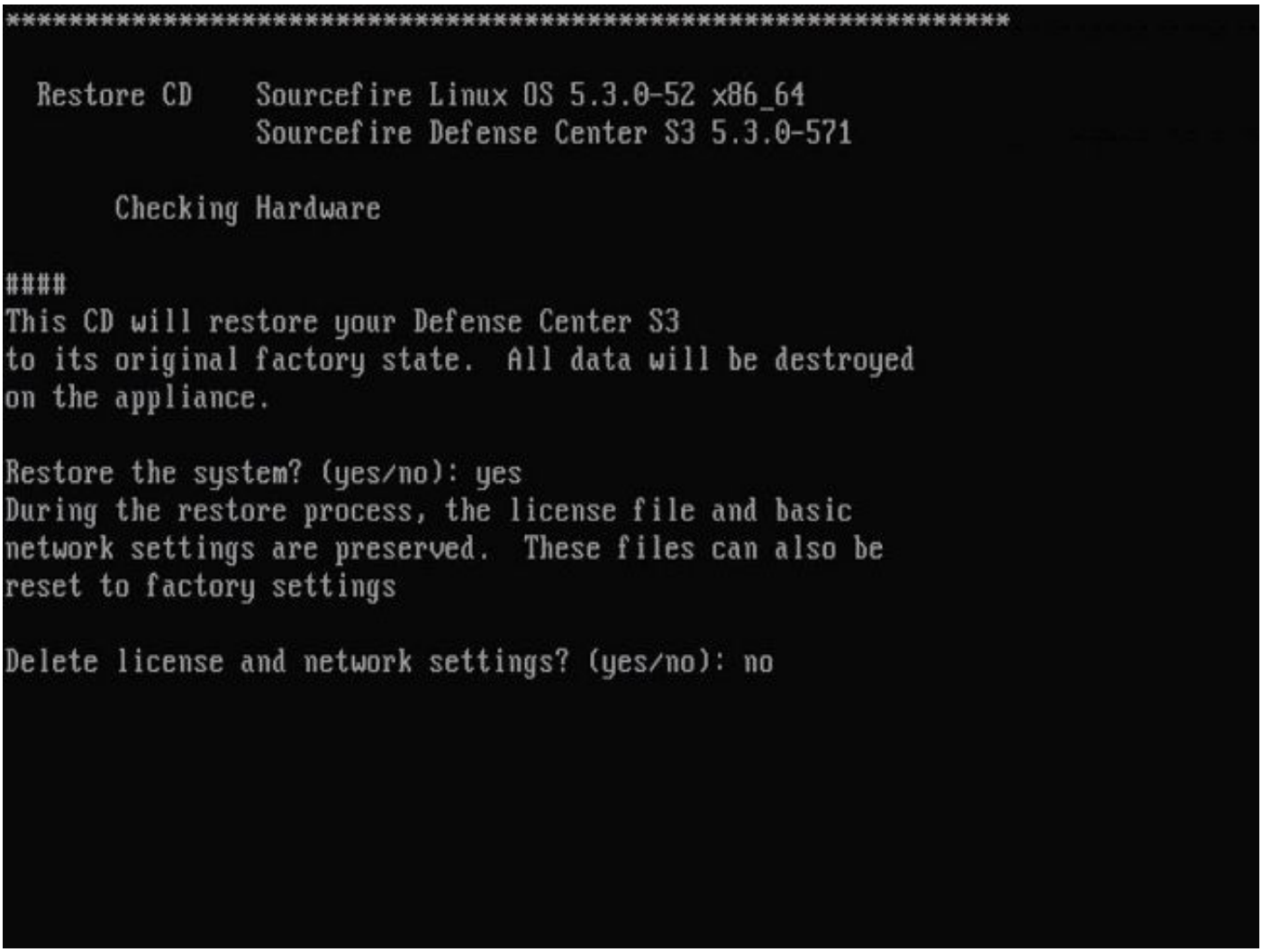
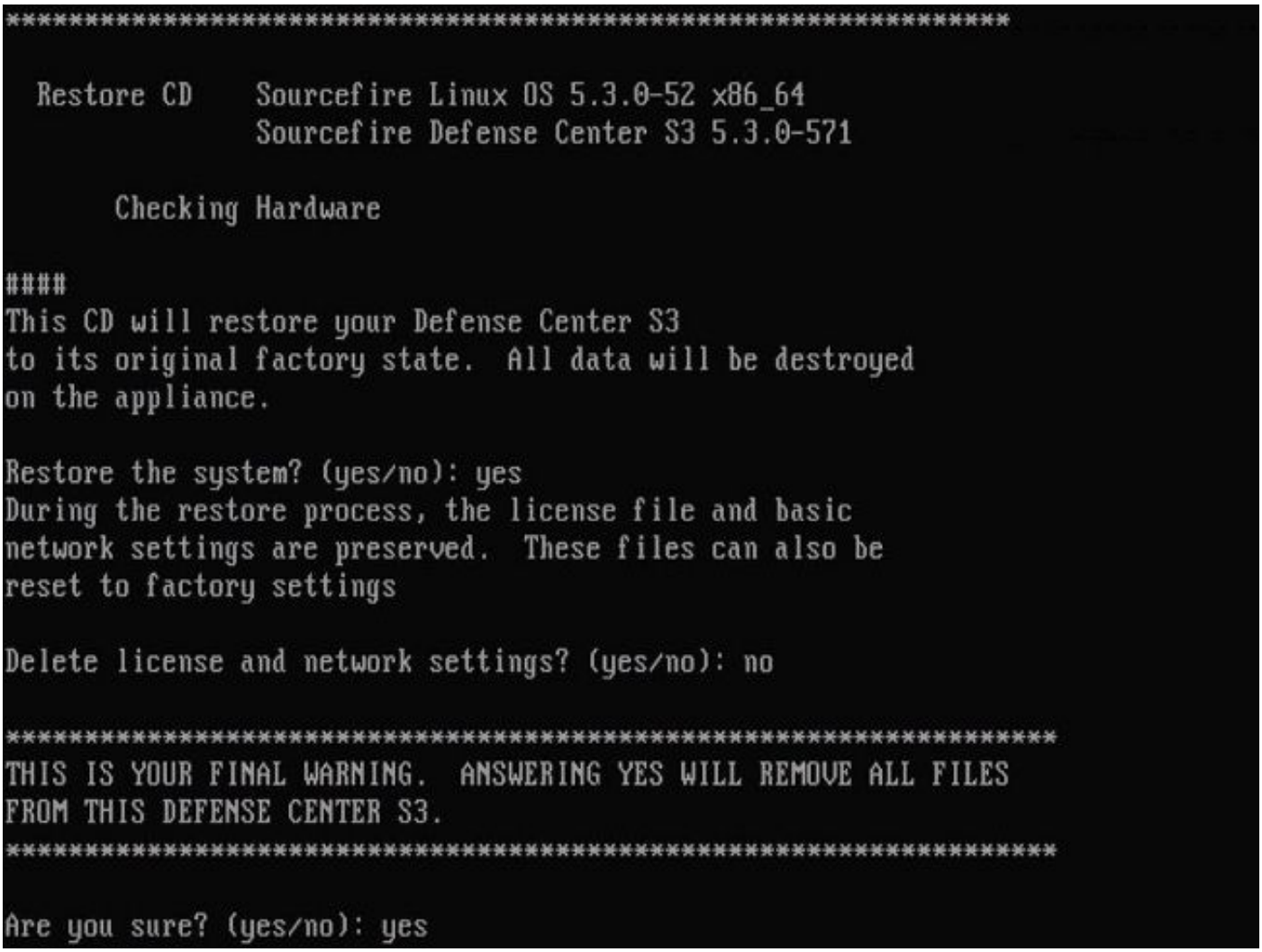

**********
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes
During the restore process, the license file and basic
network settings are preserved. These files can also be
reset to factory settings
Delete license and network settings? (yes/no): no

Figura 28


**********
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes
During the restore process, the license file and basic
network settings are preserved. These files can also be
reset to factory settings
Delete license and network settings? (yes/no): no
**********
THIS IS YOUR FINAL WARNING. ANSWERING YES WILL REMOVE ALL FILES
FROM THIS DEFENSE CENTER S3.
**********
Are you sure? (yes/no): yes
Figura 29

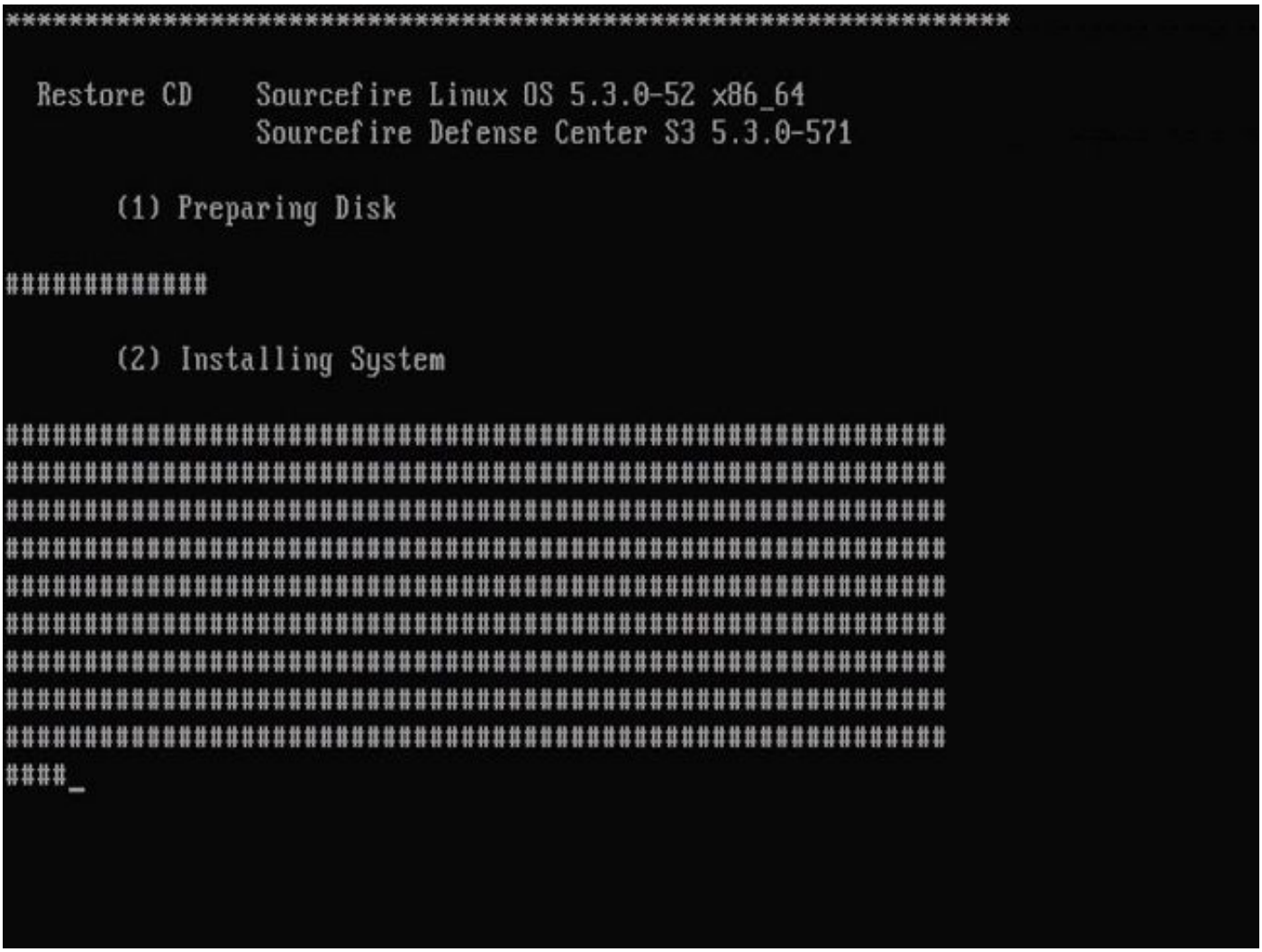

Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
(1) Preparing Disk
(2) Installing System

Figura 30

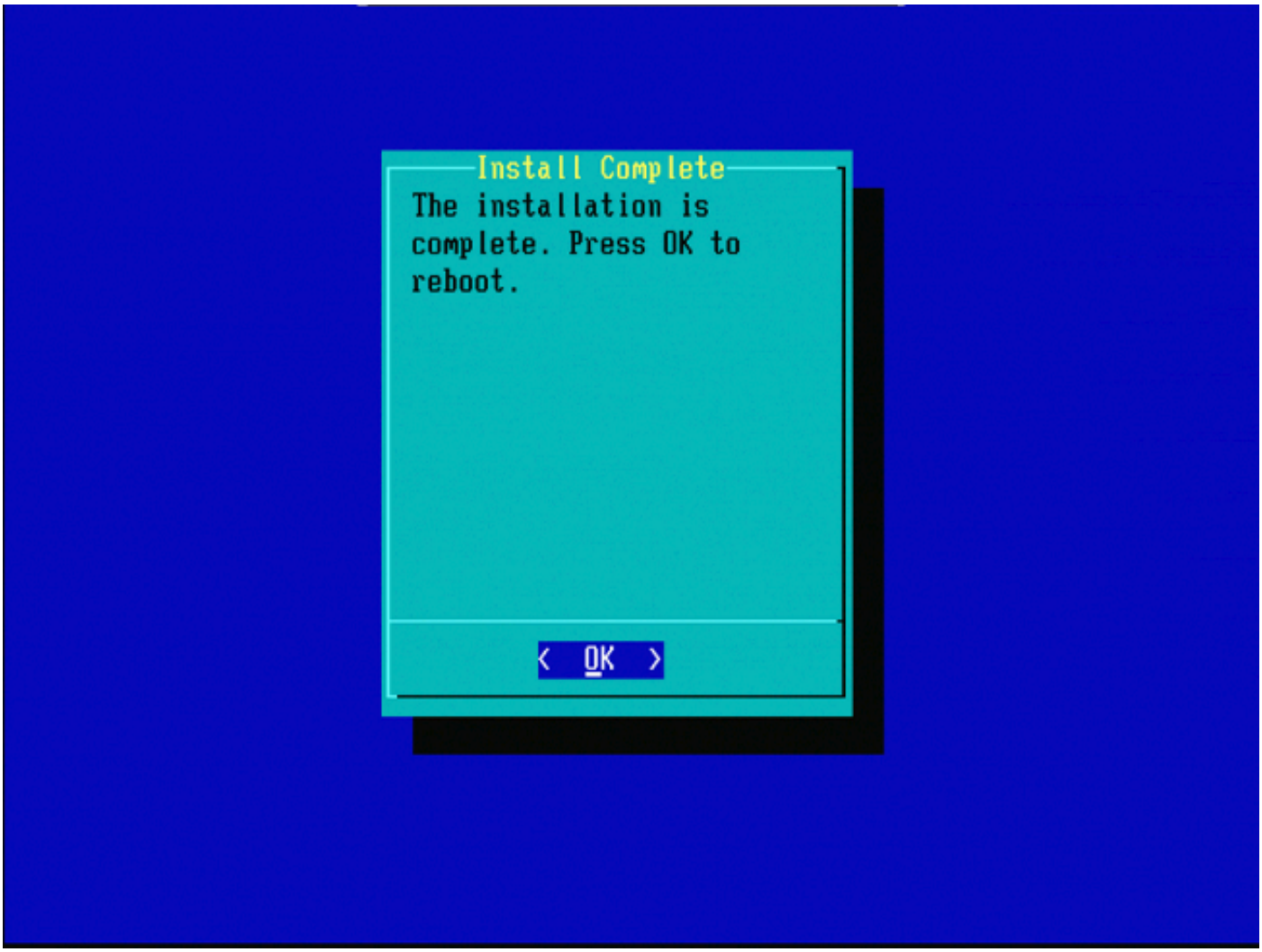

Install Complete
The installation is complete. Press OK to reboot.
< OK >

Figure 31

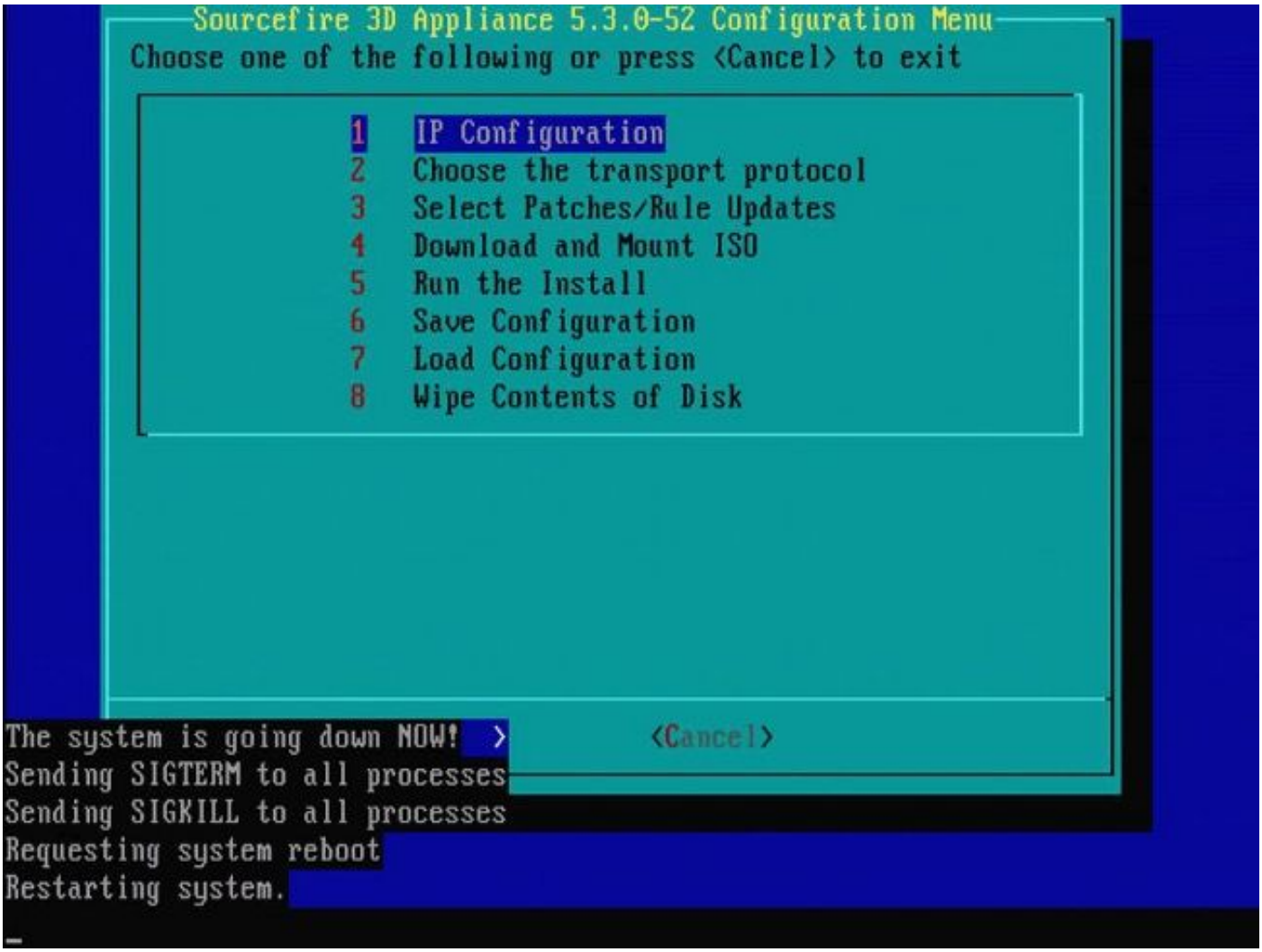



Figura 32

## Cisco Firepower Management Center 1000, 2500 y 4500

En FMC 1000, 2500 y 4500, las opciones son diferentes. Utilice un conmutador KVM o el CIMC y, mientras se inicia el dispositivo, se le mostrarán estas opciones:

1 - Modo VGA de la consola de administración de Cisco Firepower

2 - Consola de administración de Cisco Firepower serie

3 - Modo de restauración del sistema de la consola de administración de Cisco Firepower

4 - Modo De Restauración De Contraseña De La Consola De Administración De Cisco Firepower

Si desea acceder al modo de restauración con interfaz de usuario, seleccione la opción "Modo de restauración del sistema de la consola de Cisco Firepower Management" (opción 3) y, a continuación, "Modo VGA de restauración del sistema de la consola de Cisco Firepower Management" (opción 1)

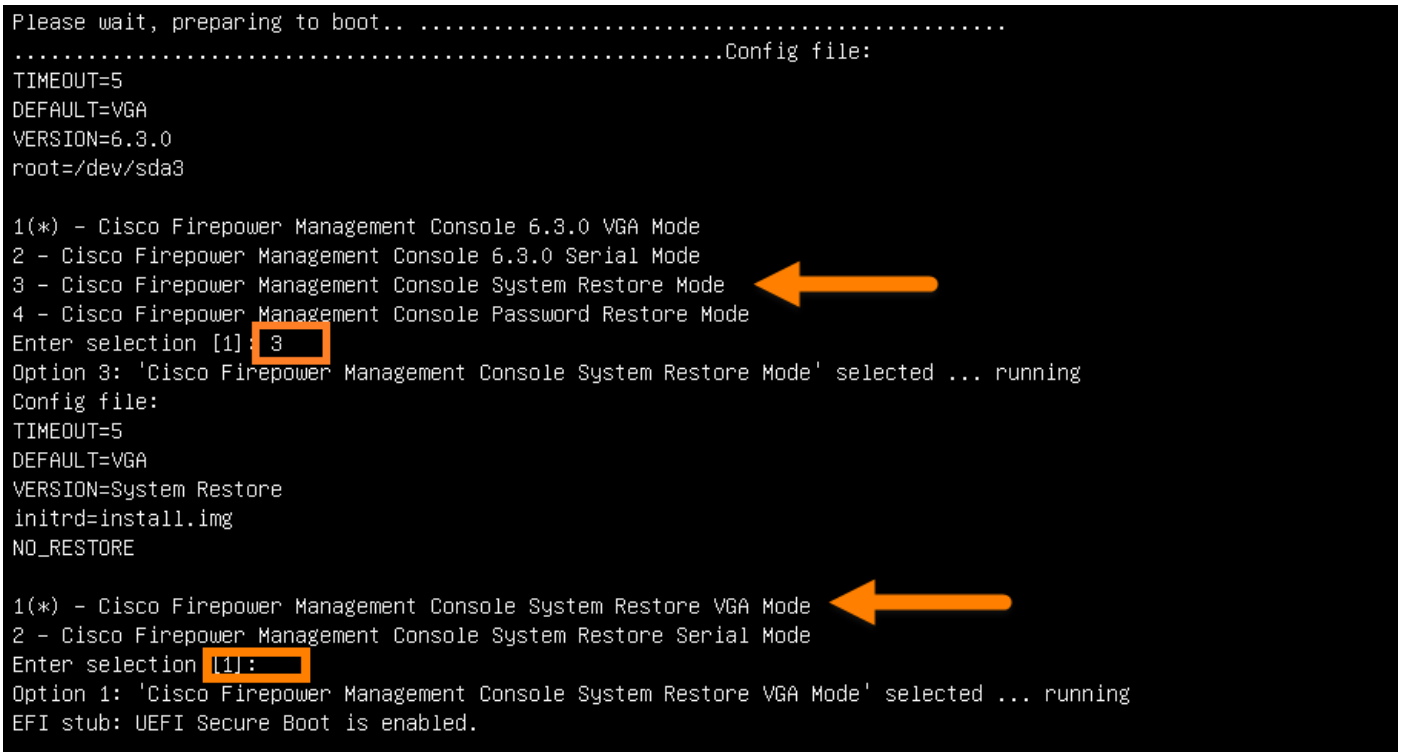



Figura 33

El resto del proceso es el mismo que en otros equipos FMC.

# Troubleshoot

## No se muestra la opción de menú Restaurar sistema LILO

FireSIGHT Management Center y los appliances FirePOWER series 7000 y 8000 cuentan con una unidad flash integrada que contiene el sistema de recreación de imágenes. Si la opción "System_Restore" no aparece en el menú de arranque LILO (Linux Loader), todavía es posible acceder a esta unidad para completar la recreación de imágenes.

Dispositivos 7010, 7020 y 7030

Si utiliza un dispositivo de la serie 70XX, complete estos pasos para seleccionar el dispositivo de arranque:

1. Apague el dispositivo correctamente.

2. Encienda el dispositivo y presione la tecla Delete repetidamente mientras el dispositivo arranca para acceder a la pantalla de selección del dispositivo de arranque. Vea la imagen aquí:

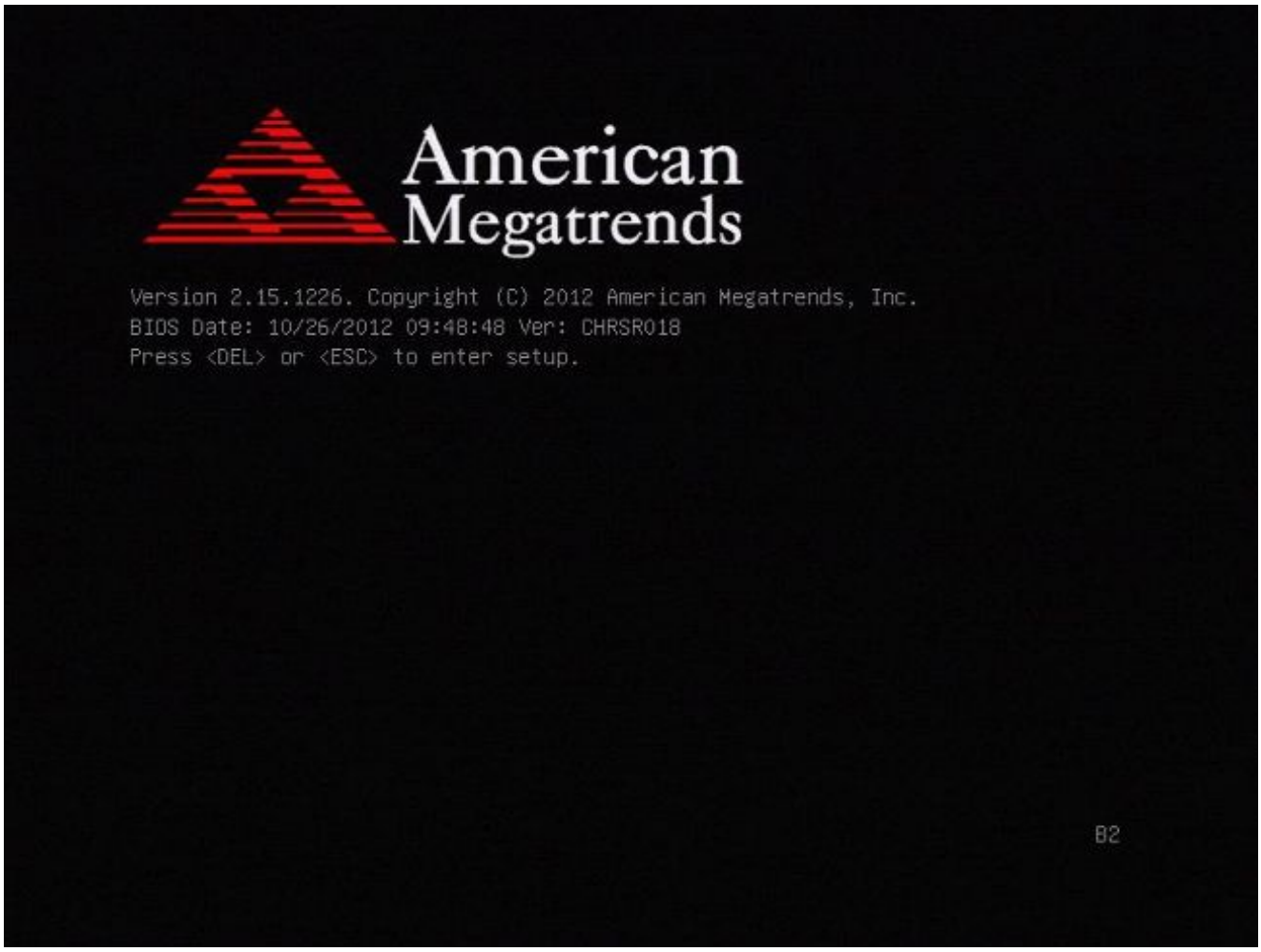

American
Megatrends
Version 2.15.1226. Copyright (C) 2012 American Megatrends, Inc.
BIOS Date: 10/26/2012 09:48:48 Ver: CHRSR018
Press <DEL> or <ESC> to enter setup.
B2

Figura A1

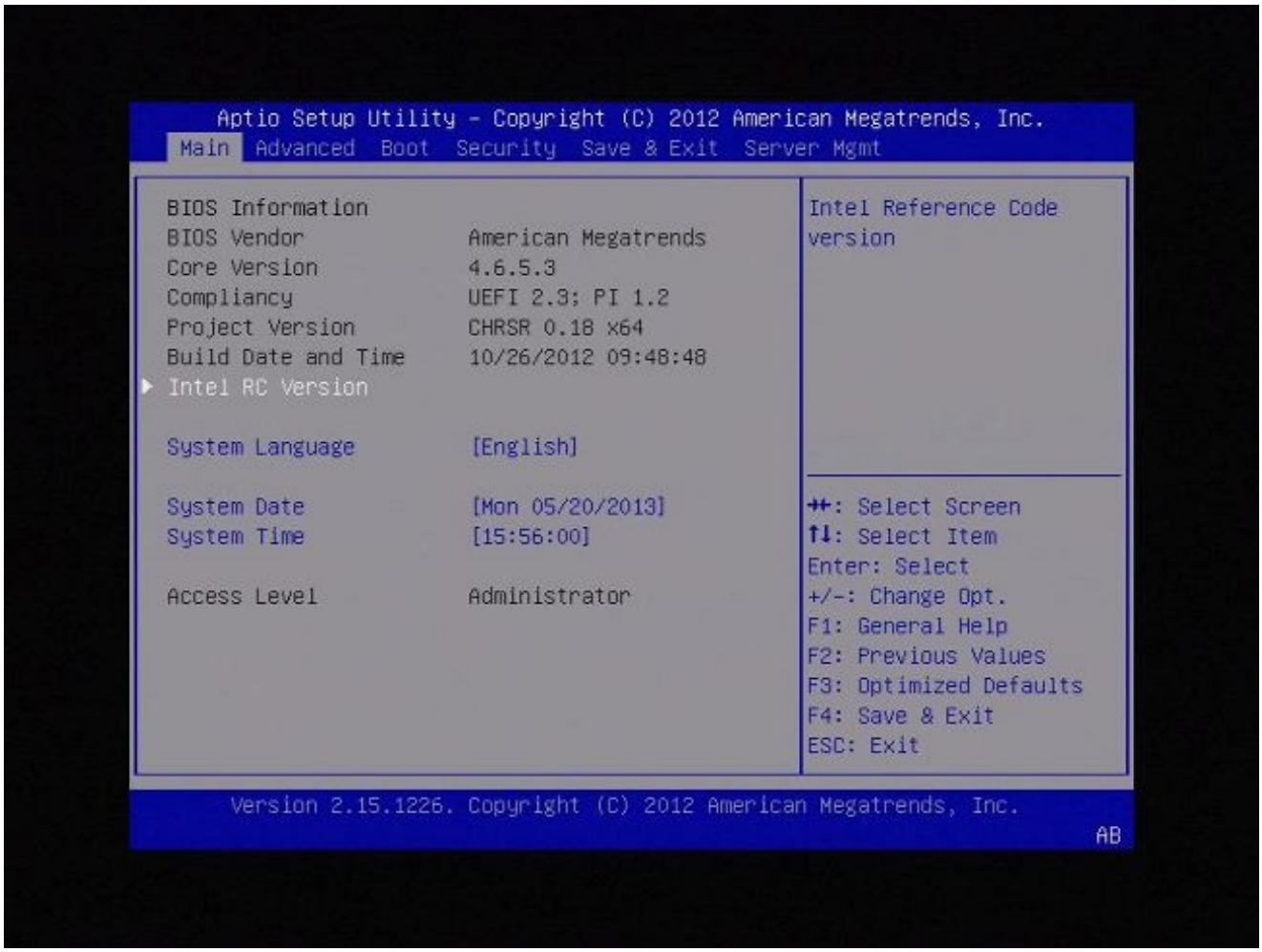



Figura A2

3. Utilice la tecla de flecha derecha para seleccionar la pestaña Save & Exit. En esta ficha, utilice la tecla de flecha abajo para seleccionar SATA SM: InnoDisk. - InnoLite y pulse la tecla Intro.

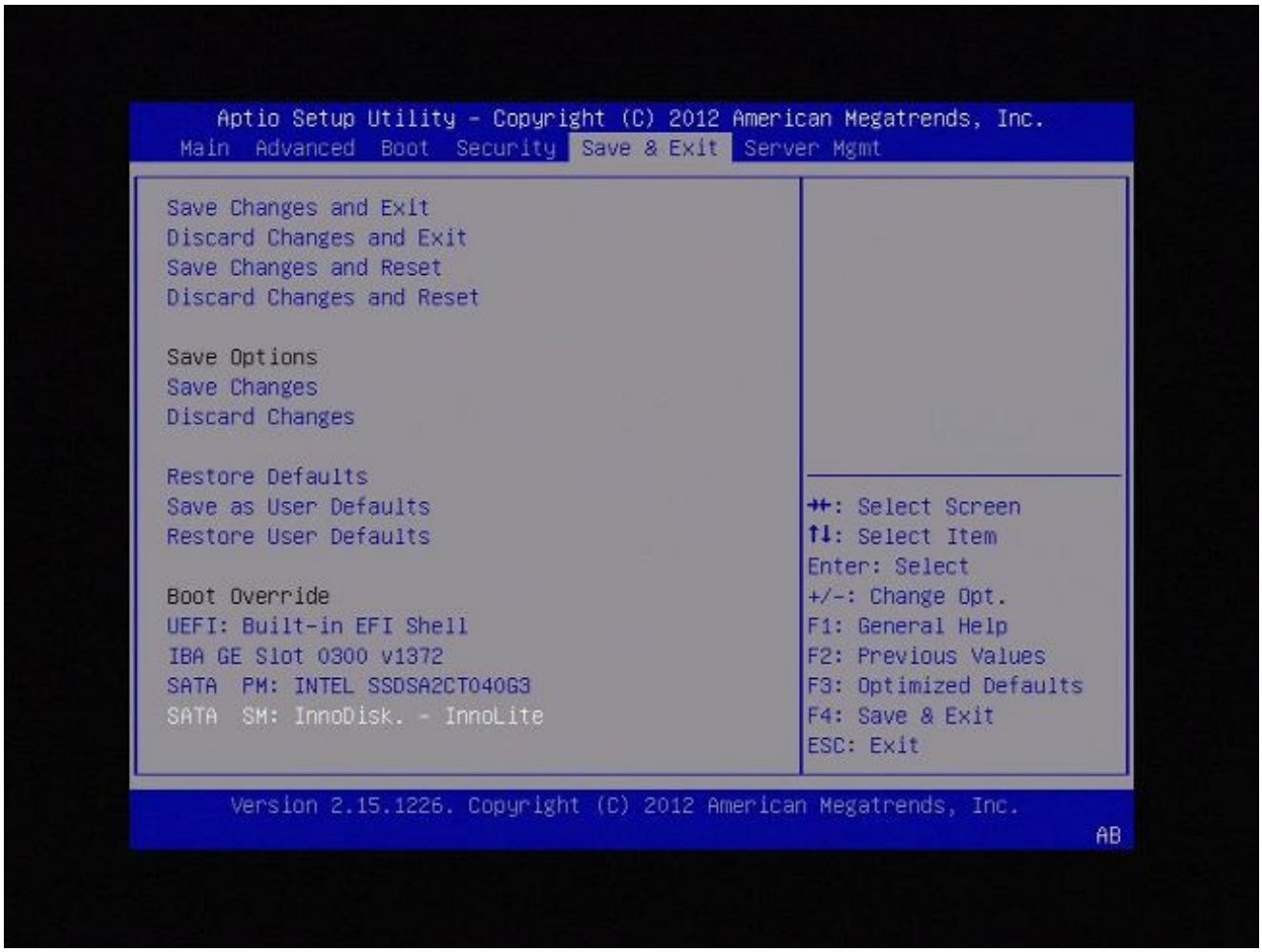



Figura A3

4. Elija la opción 0 si utiliza un teclado y un monitor.

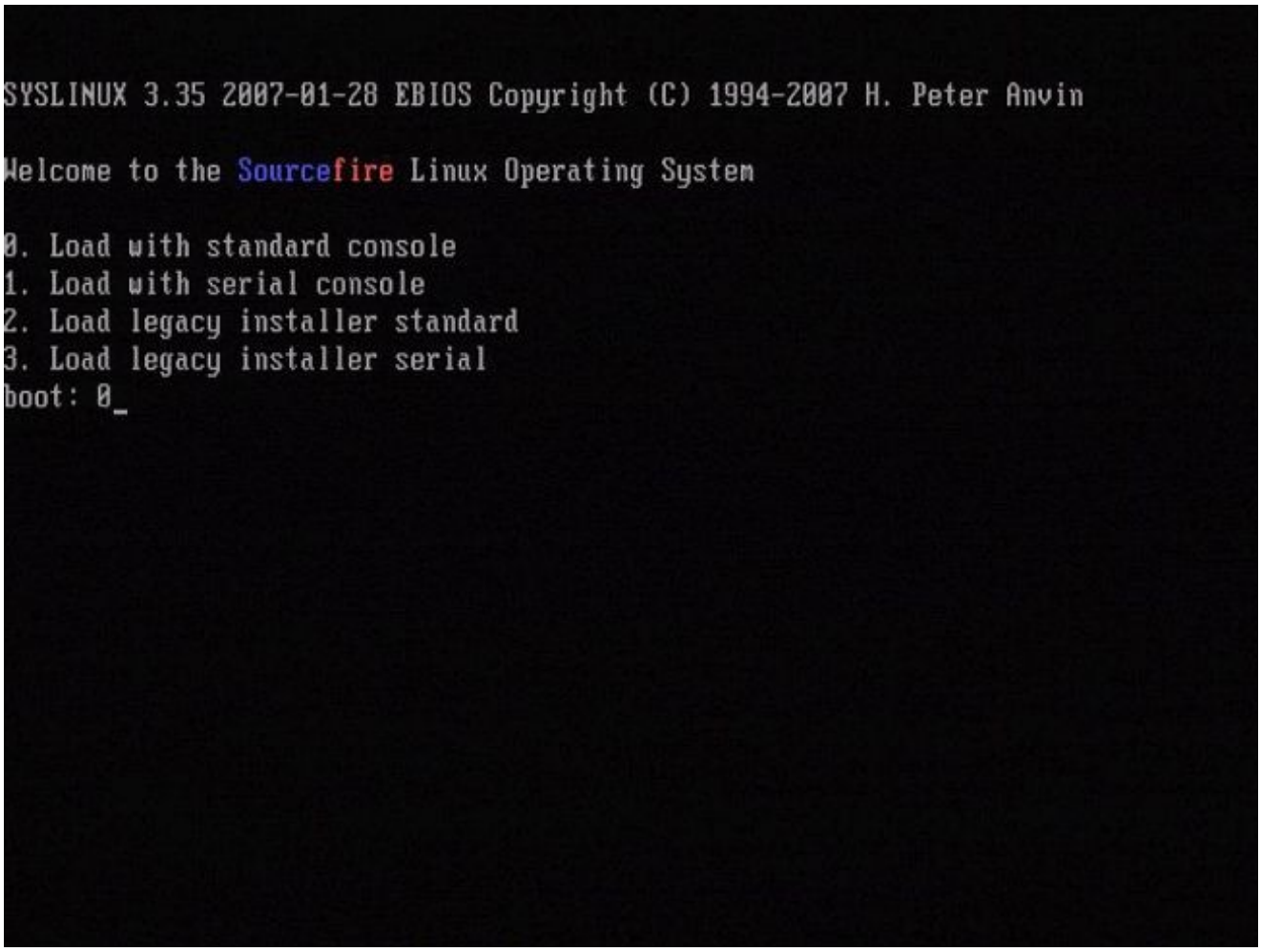

SYSLINUX 3.35 2007-01-28 EBIOS Copyright (C) 1994-2007 H. Peter Anvin
Welcome to the Sourcefire Linux Operating System
0. Load with standard console
1. Load with serial console
2. Load legacy installer standard
3. Load legacy installer serial
boot: 0_
Figura A4


Figura A5

Dispositivos 7110 y 7120

Si utiliza un dispositivo de la serie 71XX, complete estos pasos para seleccionar el dispositivo de inicio:

1. Apague el dispositivo correctamente.

2. Encienda el dispositivo y presione la tecla F11 repetidamente mientras el dispositivo arranca para acceder a la pantalla de selección del dispositivo de arranque. Vea la imagen que se muestra aquí:

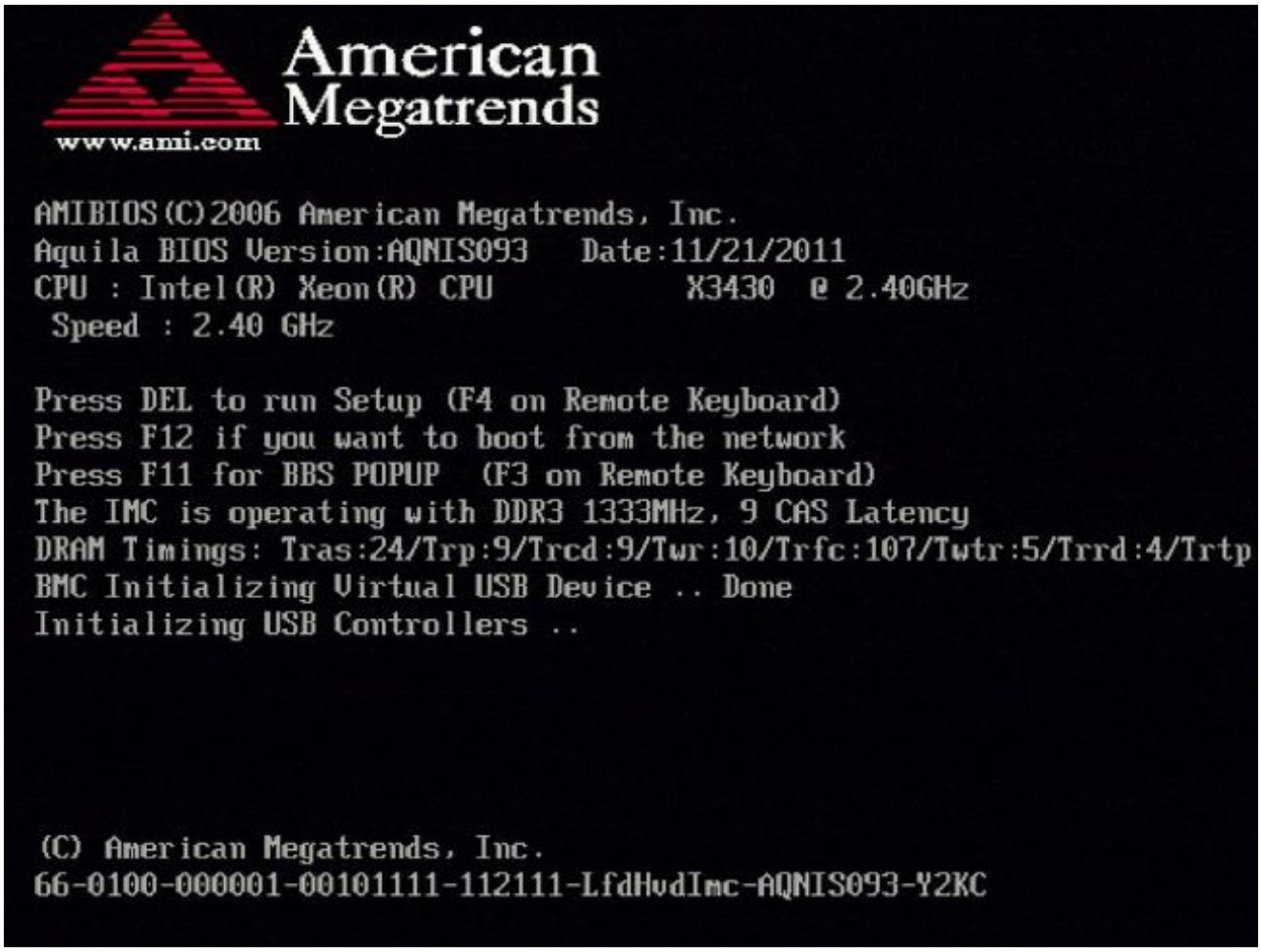



Figura B1

3. Seleccione la opción HDD:P1-SATADOM y presione Enter para iniciar la partición System_Restore.


Please select boot device:
HDD:P0-INTEL SSDSA2CT040G3
HDD:P1-SATADOM
Network:IBA GE Slot 0300 v1336
↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

Figura B2

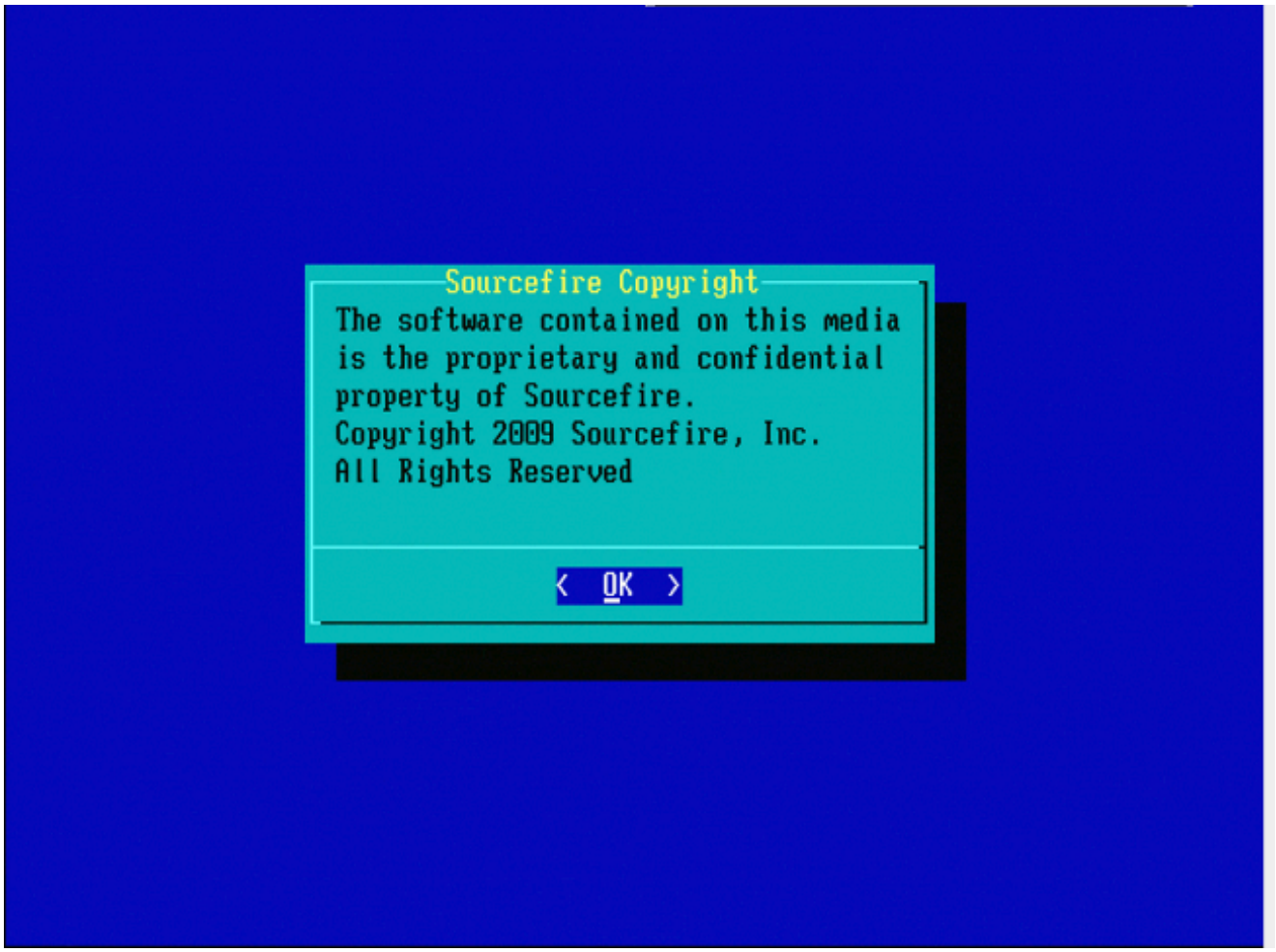



Figura B3

Dispositivos serie 8000 o modelos de Management Center FS750, FS1500 o FS3500

Si utiliza un dispositivo de la serie 8000 o un modelo de Management Center FS750, FS1500 o FS3500, complete estos pasos para seleccionar el dispositivo de inicio:

1. Apague el dispositivo correctamente.

2. Encienda el dispositivo y presione la tecla F6 repetidamente mientras el dispositivo arranca para acceder a la pantalla de selección del dispositivo de arranque. Vea la imagen que se muestra aquí:

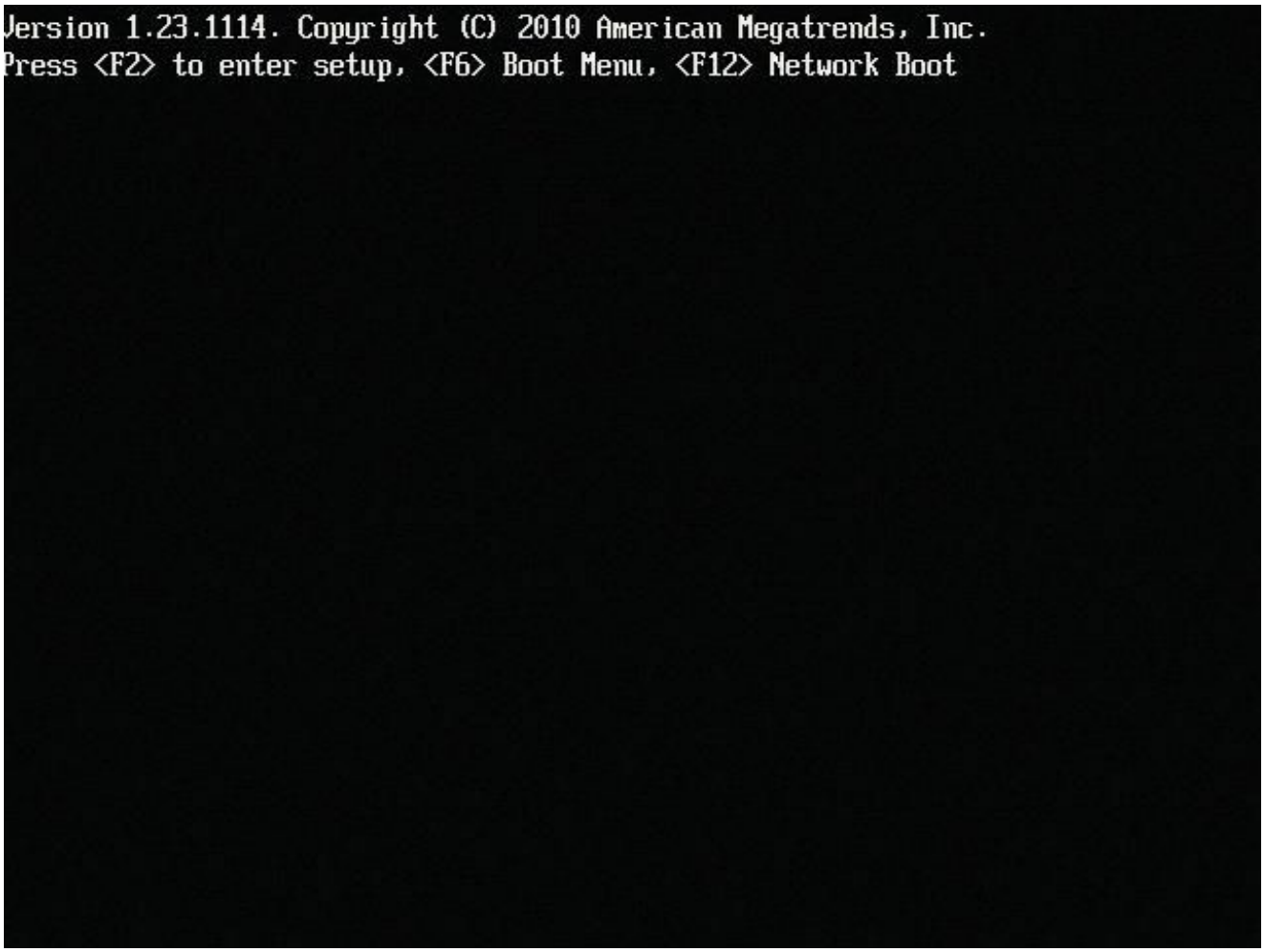



Figura C1

3. Seleccione la opción USB.

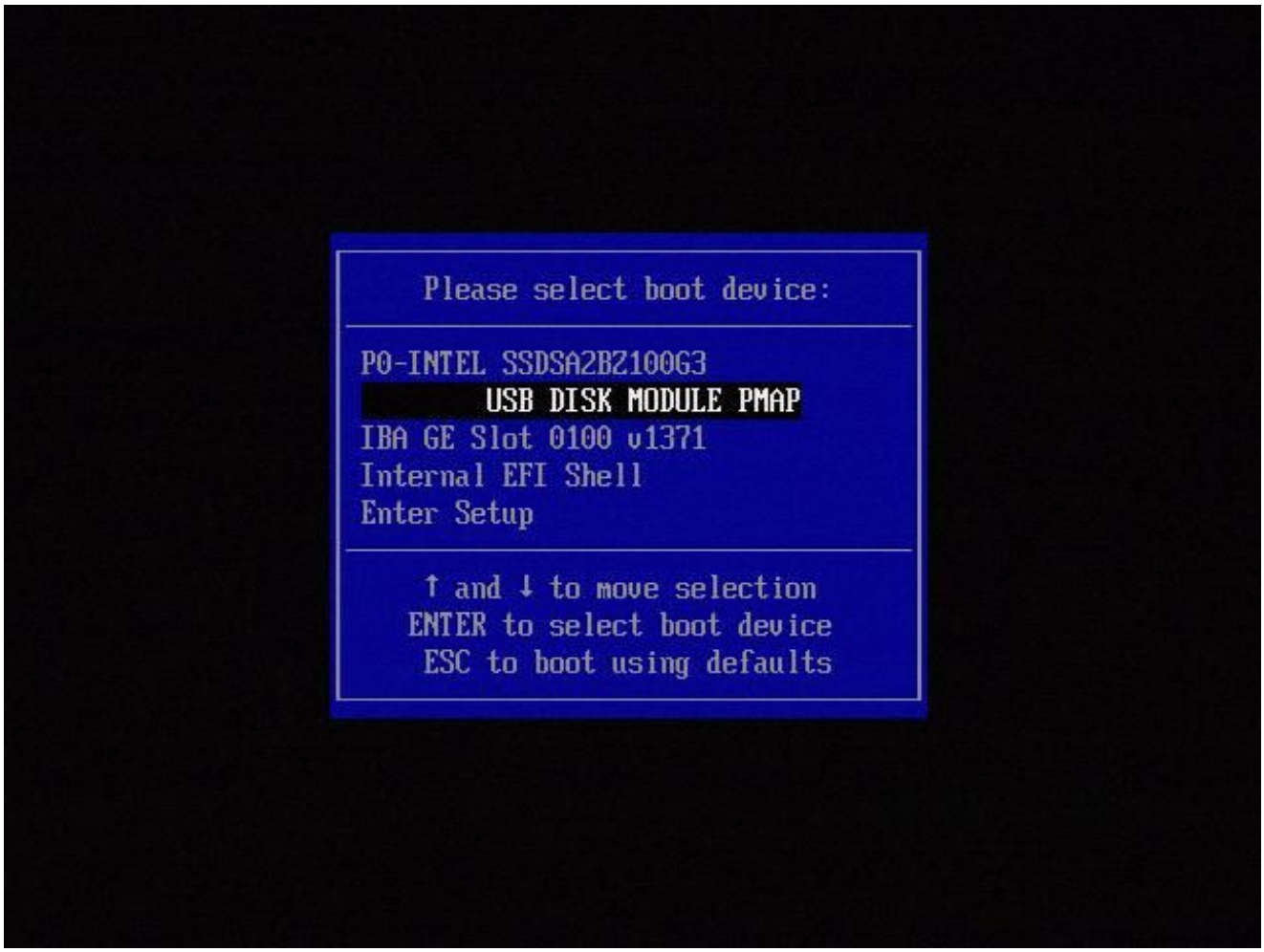



Figura C2

4. El dispositivo arranca desde la partición System_Restore y muestra el menú System_Restore.

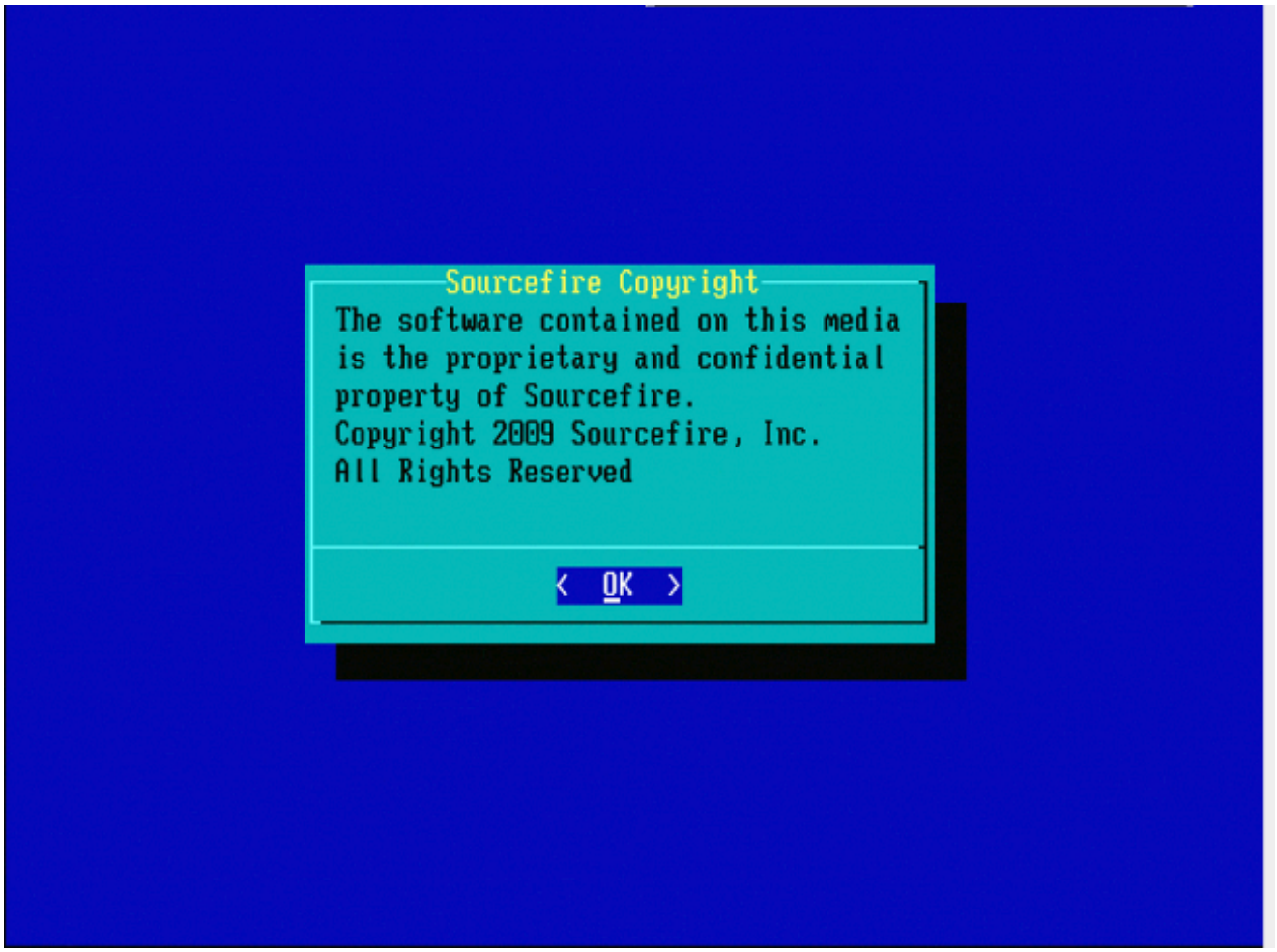



Figura C3

## Restauración del sistema para los modelos FMC1000, FMC2500, FMC4500 (FMC basados en M4)

Nota: Para FMC4500, este modelo tiene un menú de arranque diferente. Encontrará más información en el siguiente enlace

La indicación para seleccionar la restauración del sistema aparece de forma diferente para estos modelos: FMC1000, FMC2500, FMC4500

1. Durante el arranque, puede ver esta pantalla durante 5 segundos:

```
Please wait, preparing to boot.. ..........................................
.............................................Config file:
TIMEOUT=5
DEFAULT=VGA
VERSION=6.2.2
root=/dev/sda3

1(*) - Cisco Firepower Management Console 6.2.2 VGA Mode
2 - Cisco Firepower Management Console 6.2.2 Serial Mode
3 - Cisco Firepower Management Console System Restore Mode
4 - Cisco Firepower Management Console Password Restore Mode
Enter selection [1]:
```

Figura D1

2. Seleccione la opción Restaurar sistema (#3 en este caso).

```
1(*) - Cisco Firepower Management Console 6.2.2 VGA Mode
2 - Cisco Firepower Management Console 6.2.2 Serial Mode
3 - Cisco Firepower Management Console System Restore Mode
4 - Cisco Firepower Management Console Password Restore Mode
Enter selection [1]: 3
Option 3: 'Cisco Firepower Management Console System Restore Mode' selected ...
running
Config file:
TIMEOUT=5
DEFAULT=VGA
VERSION=System Restore
initrd=install.img
NO_RESTORE

1(*) - Cisco Firepower Management Console System Restore VGA Mode
2 - Cisco Firepower Management Console System Restore Serial Mode
Enter selection [1]:
```

Figura D2

3. Seleccione el método de visualización para la restauración del sistema (#1 para VGA en este caso)

```
1(*) - Cisco Firepower Management Console System Restore VGA Mode
2 - Cisco Firepower Management Console System Restore Serial Mode
Enter selection [1]: 1
Option 1: 'Cisco Firepower Management Console System Restore VGA Mode' selected
... running
```

Figura D3

4. A continuación, se llega al mensaje que aparece en la figura 5 y el proceso continúa normalmente.

## Opción de arranque no enumerada

Es posible que la opción para arrancar en la partición de recreación de imágenes no aparezca en la BIOS o en el menú de arranque. Si este es el caso, es posible que la unidad que contiene el sistema de recreación de imágenes no exista o esté dañada. Probablemente sea necesario un RMA.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).