Recriar a imagem de um FireSIGHT Management Center e de um dispositivo FirePOWER

Contents

Introduction

Este documento descreve os processos com exemplos para o procedimento de recriação de um Cisco FireSIGHT Management Center (FMC) e dispositivos FirePOWER.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Dispositivo gerenciado	FireSIGHT Management Center	Versões de software disponíveis para recriação
Cisco Firepower 7000 Series Cisco Firepower 7100 Series Cisco Firepower 8100 Series Cisco Firepower 8200	FS 750 FS 1500 FS 3500	5.2 ou posterior

Series		
Firepower série 8300 Cisco AMP 7150 Cisco AMP 8150		5.3 ou posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Processo de recriação de imagem

> **Cuidado**: não insira um dispositivo de armazenamento USB nem conecte um switch de teclado, vídeo e mouse (KVM) ao atualizar ou recriar um FireSIGHT Management Center ou um dispositivo FirePOWER.

Antes de Começar

1. Se você planeja recriar um Management Center ou um dispositivo Firepower independente, é recomendável fazer backup do dispositivo antes de continuar.

2. Identifique o modelo do seu sensor e use a lista de modelos na seção Componentes usados para verificar se este guia é apropriado.

3. Baixe o guia de instalação e a imagem de disco apropriados para a versão de software desejada no site de suporte da Cisco.

   > **Observação**: não renomeie um arquivo .iso

   Servir a imagem: O arquivo .iso deve ser copiado para um host que execute um servidor SSH acessível a partir da rede de gerenciamento do equipamento para ser recriado.

   > **Observação**: se nenhum outro servidor SSH estiver disponível, um FMC poderá ser usado para esse processo.

   Verifique a integridade do iso: a soma md5dos arquivos é fornecida no lado direito da página para verificação com um utilitário md5sum.

4. Os guias de instalação contêm instruções passo a passo sobre a recriação e também descrevem vários métodos para o processo de recriação. As imagens fornecidas neste documento podem ser usadas como referência.

Visão geral do processo de recriação

Observação: a versão 5.3 foi usada para capturar as imagens mostradas neste artigo. O processo de recriação é idêntico para outras versões 5.x, exceto para os números de versão que aparecem nas imagens mostradas.

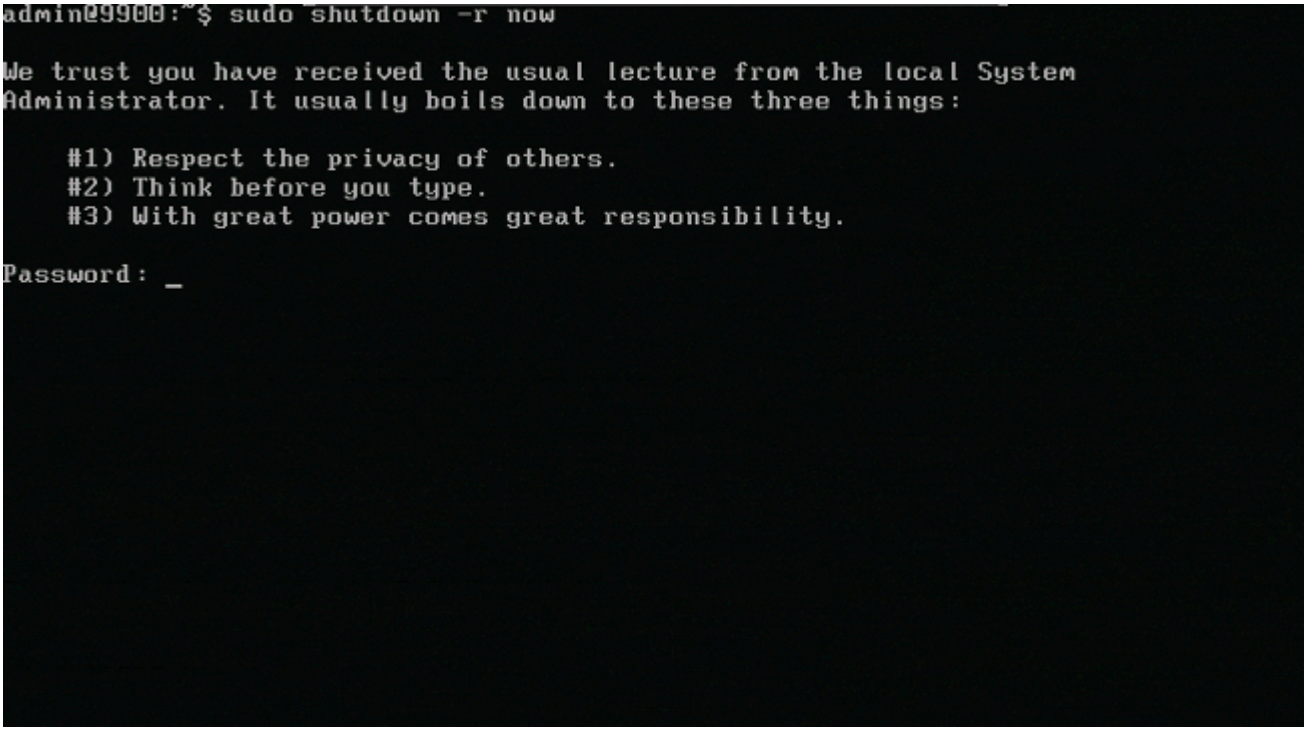


Figure 1

Figura 2 - Quando o sistema for reinicializado, pressione uma tecla de seta no teclado para interromper a contagem regressiva e escolher a opção **System_Restore** para a tela mostrada a seguir.

Observação: se o prompt **System_Restore** não for exibido, você deverá alterar a ordem de inicialização para inicializar diretamente na partição de restauração (DOM). Para obter mais informações, consulte System_Restore LILO opção de menu está faltando.

Figure 3

Figura 4 - Escolha a opção **0** se você usa um teclado e um monitor.

Observação: às vezes, foi visto que o menu da opção Restore (Restaurar) só é mostrado quando apenas o Console está conectado (com o teclado desconectado). Assim que a opção Recuperação for selecionada, o teclado poderá ser conectado novamente

---

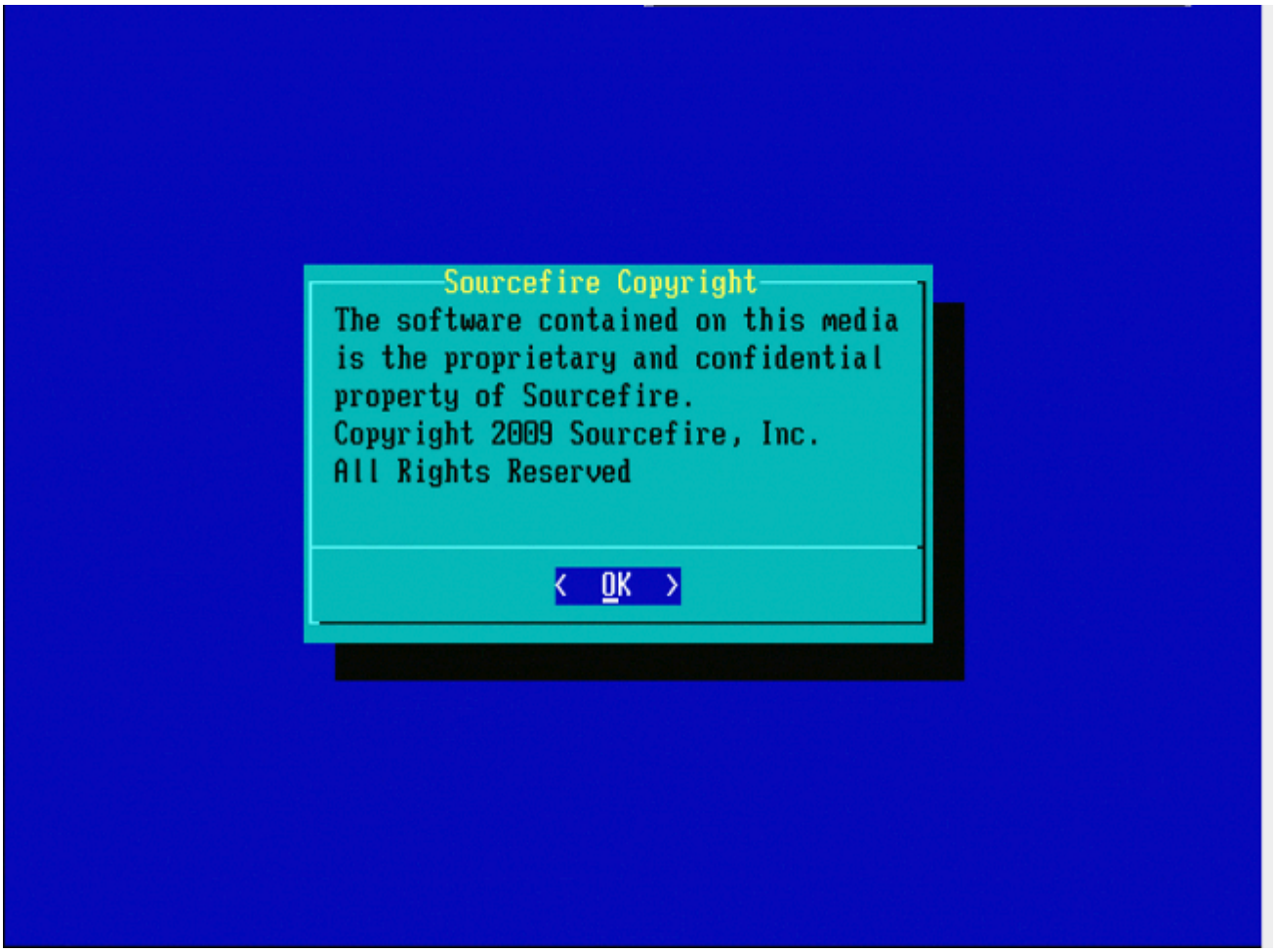


Figure 5

Figura 6

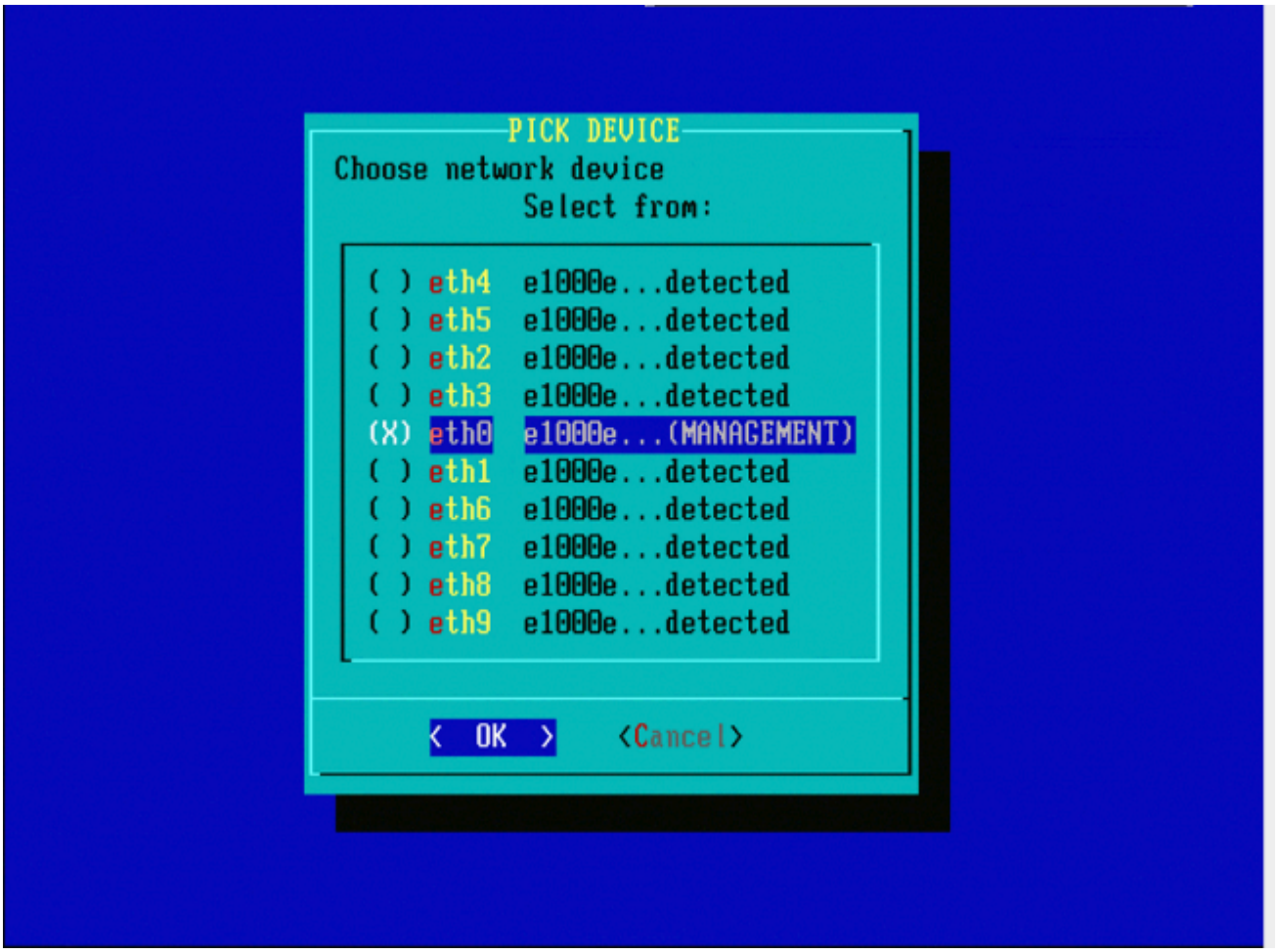


Figura 7 - Para selecionar o dispositivo de rede, pressione a barra de espaço.

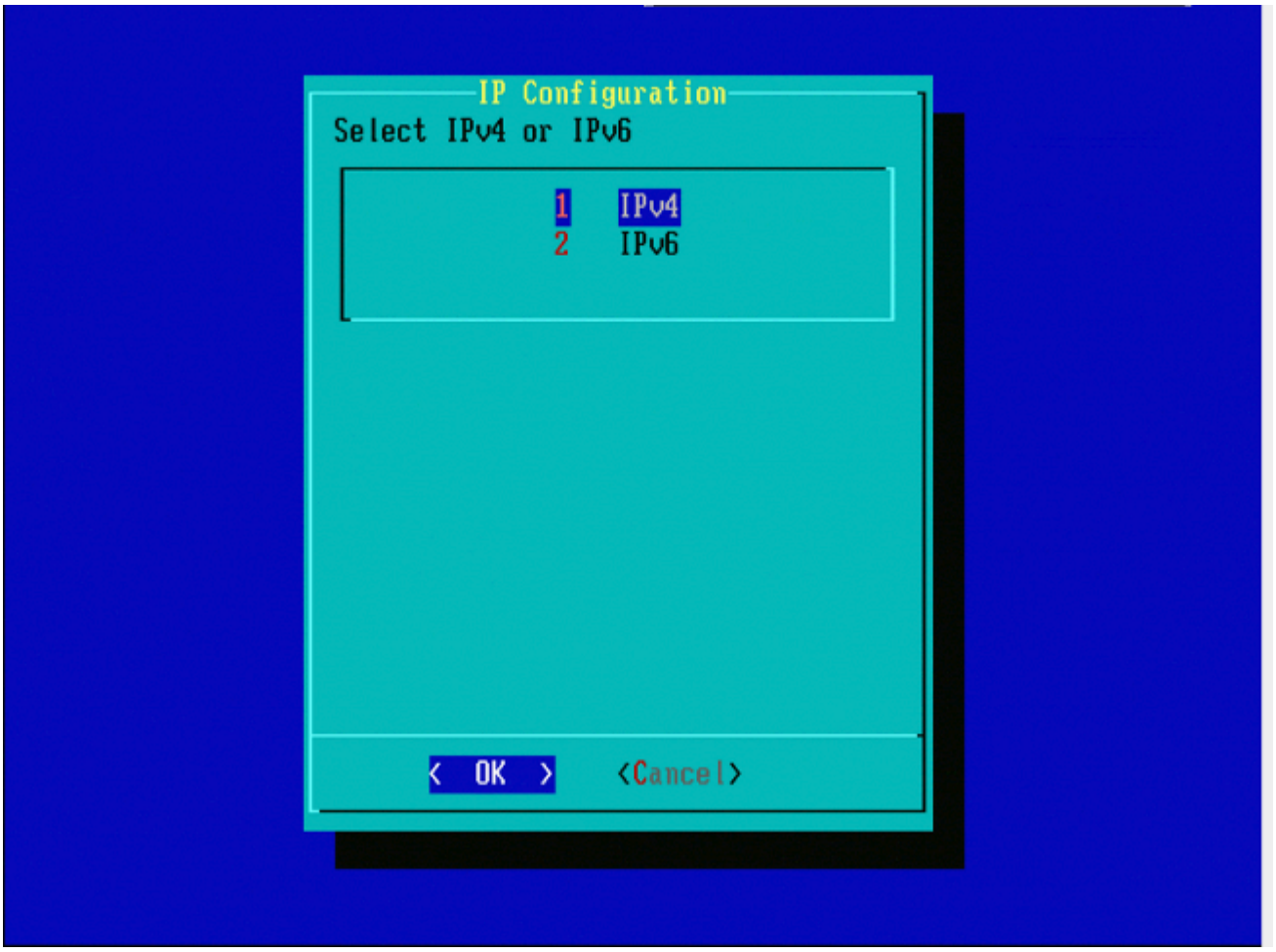
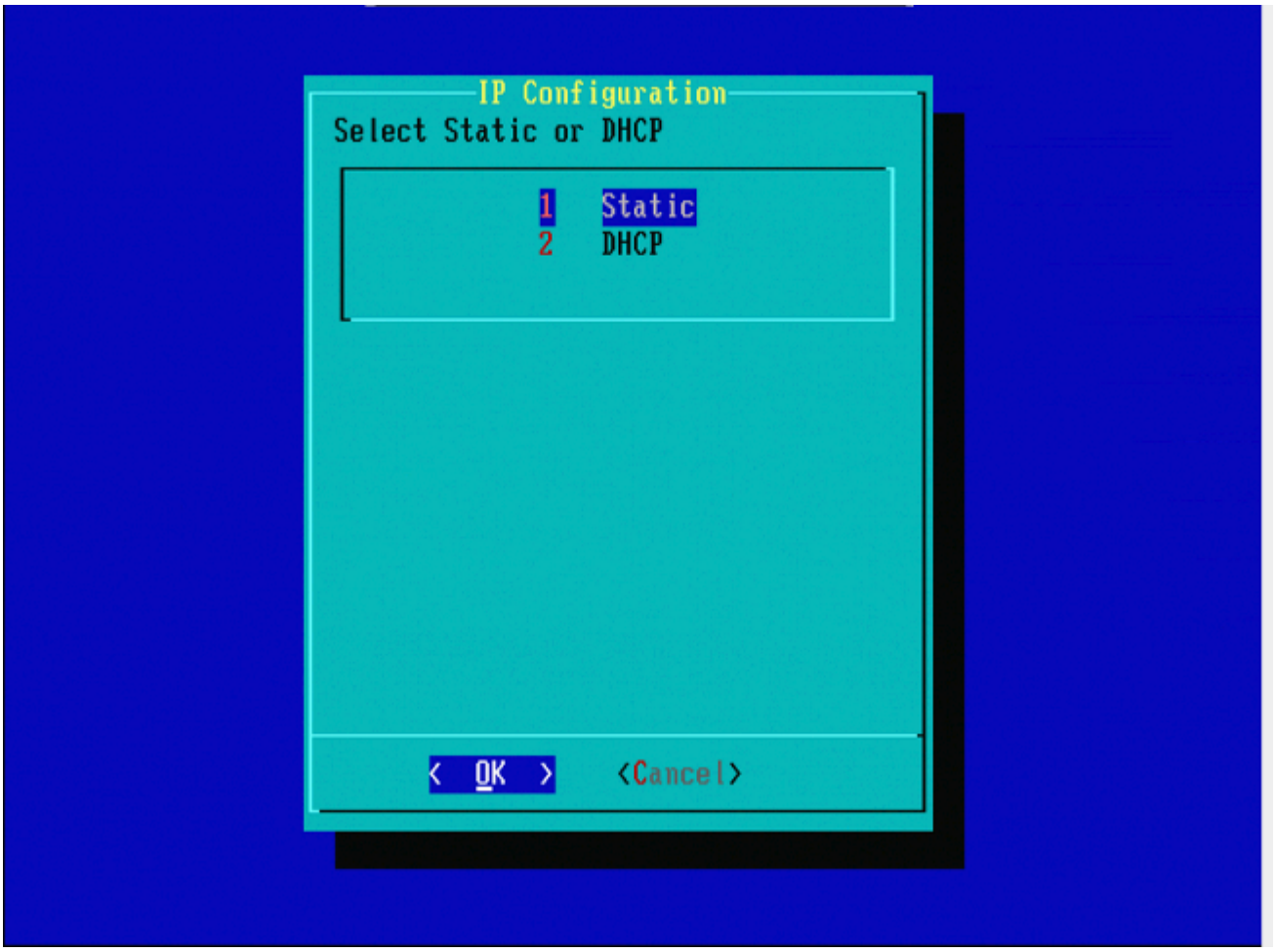


Figura 8


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 - O Suporte da Cisco recomenda que você use o protocolo SCP (Secure Copy, cópia segura).

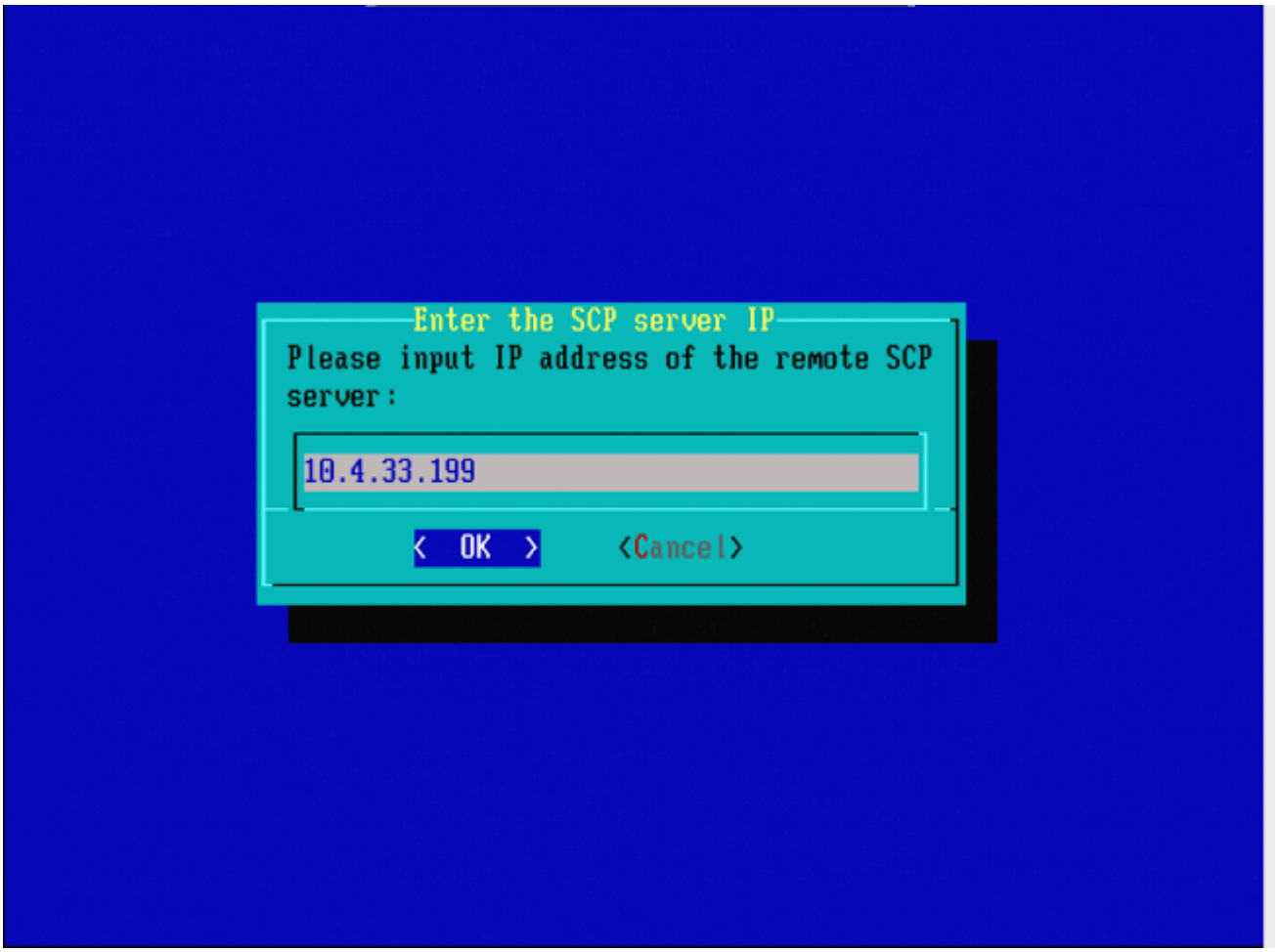


Figura 16 - É possível usar um FireSIGHT Management Center como o servidor SCP para essa etapa. Continue com esse procedimento e use o endereço IP e as credenciais do Centro de gerenciamento para preencher os campos no menu **Restauração do sistema**. Mais detalhes em

Um servidor SCP (Secure Copy) é usado para transferir arquivos com segurança. Se Se necessário, um Sourcefire Defense Center (DC) pode ser usado como um servidor SCP para transferir arquivos para outro dispositivo Sourcefire. Isso pode ser útil quando uma imagem iso precisa ser transferida para um dispositivo da Sourcefire para fins de recriação, mas o servidor SCP regular está inacessível ou indisponível.

Etapa 1. Faça o download de um arquivo .iso apropriado para seu desktop no Sourcefire Support Portal.
Etapa 2. Use um cliente SCP, copie o arquivo da área de trabalho para o Defense Center.

> **Dica**: Um cliente SCP geralmente está disponível em um sistema operacional Linux ou Mac. No entanto, no sistema operacional Windows, você pode precisar instalar um software cliente SCP de terceiros. A Sourcefire não oferece recomendações ou suporte para instalar nenhum software cliente SCP específico.

O próximo exemplo demonstra como copiar um arquivo de imagem .iso da Sourcefire do diretório Downloads de um sistema Linux para o diretório **/var/tmpdo Sourcefire Defense Center**:

<#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
```

> **Cuidado**: não altere o nome do arquivo .iso. Ele pode criar um problema com a detecção do arquivo durante uma nova imagem.

Agora o arquivo é copiado para o Centro de Defesa. Você pode prosseguir com o processo de recriação dos dispositivos da Sourcefire. Na recriação, quando necessário, você pode fornecer o endereço IP e o nome de usuário do DC e o caminho onde você copiou o arquivo de imagem com as instruções anteriores.

> **Aviso**: após concluir a recriação, você deve remover o arquivo .iso do diretório /var/tmp do Defense Center para reduzir a utilização do espaço em disco.

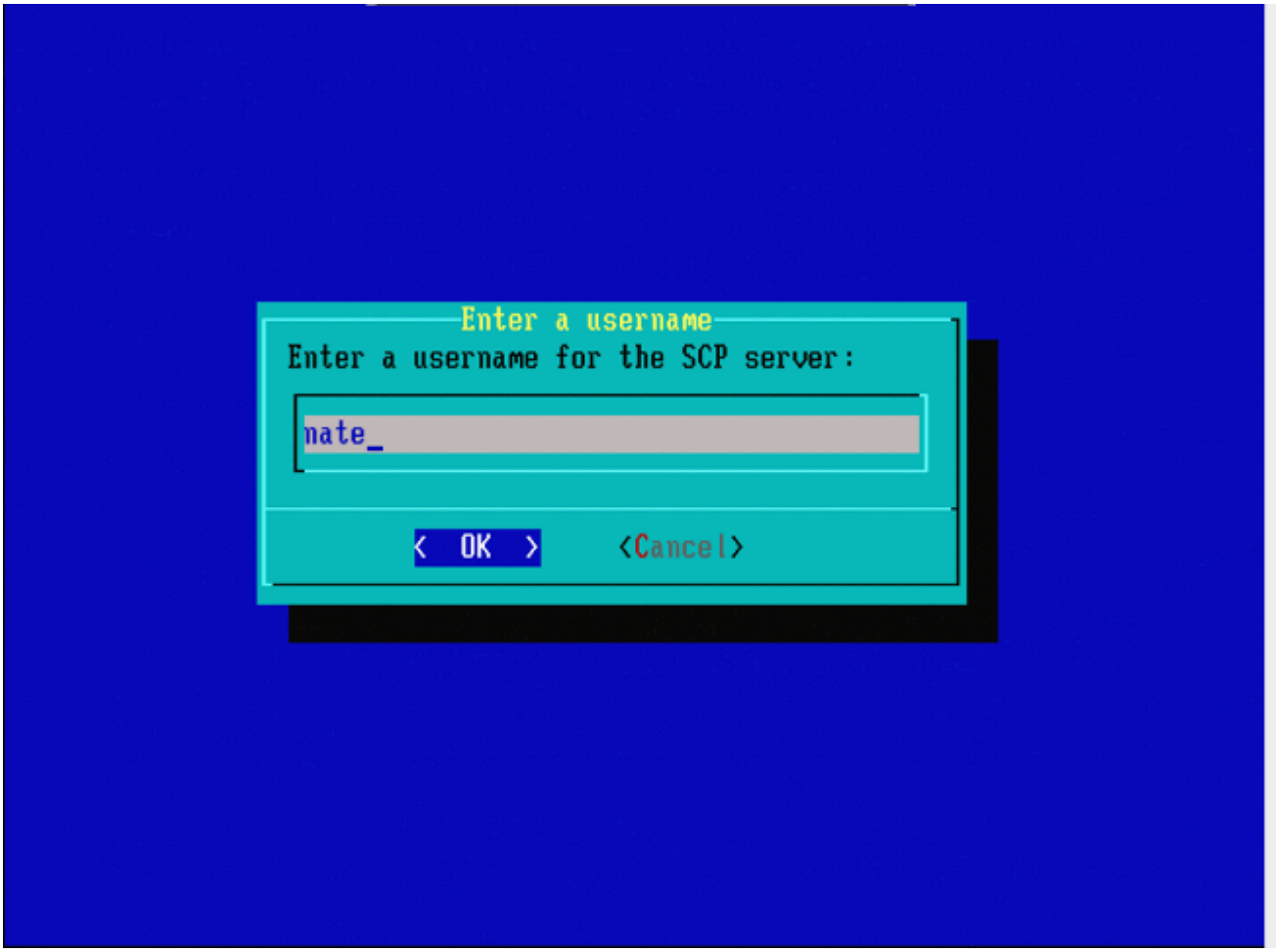


Figura 17

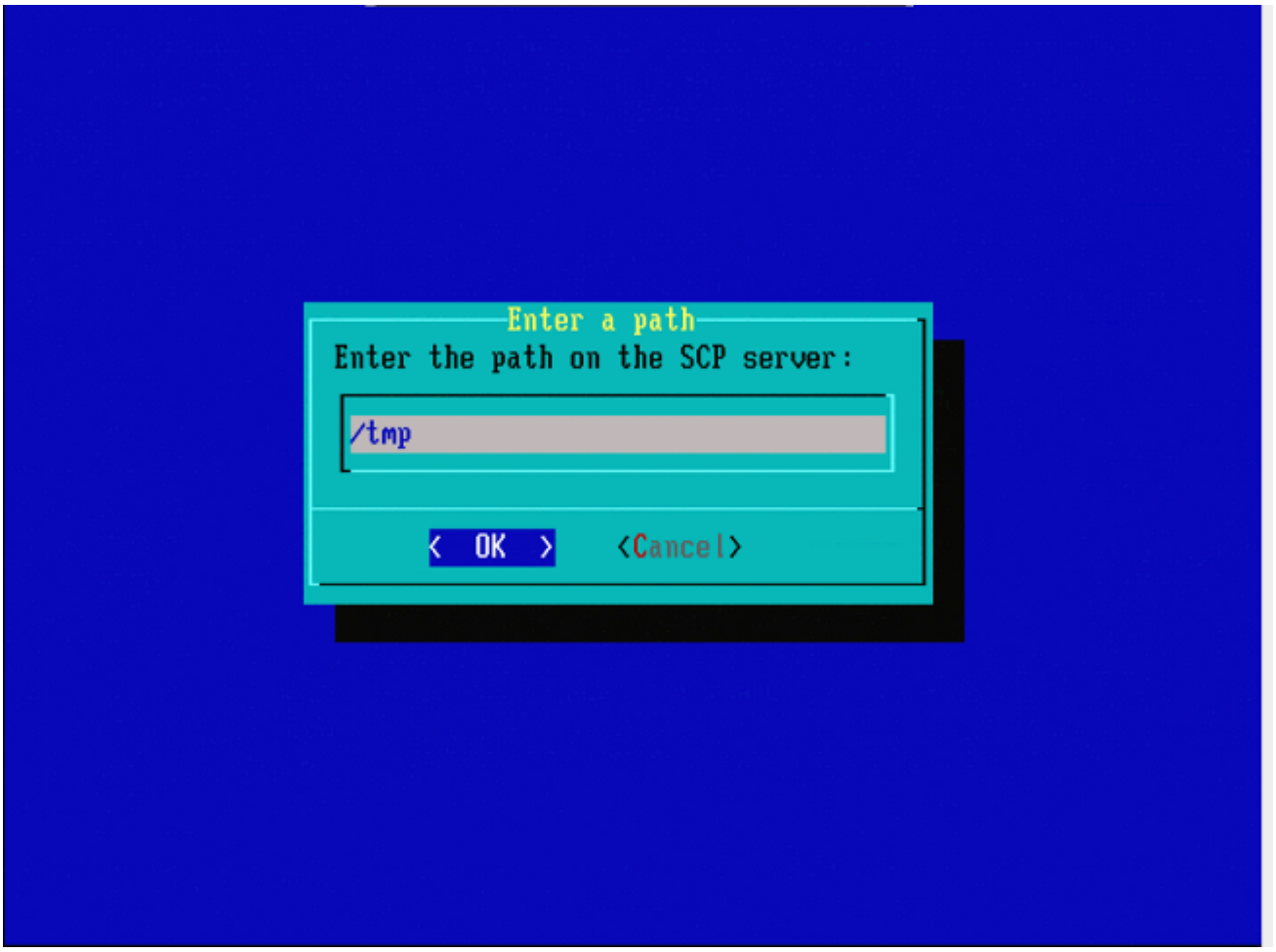


Figura 18

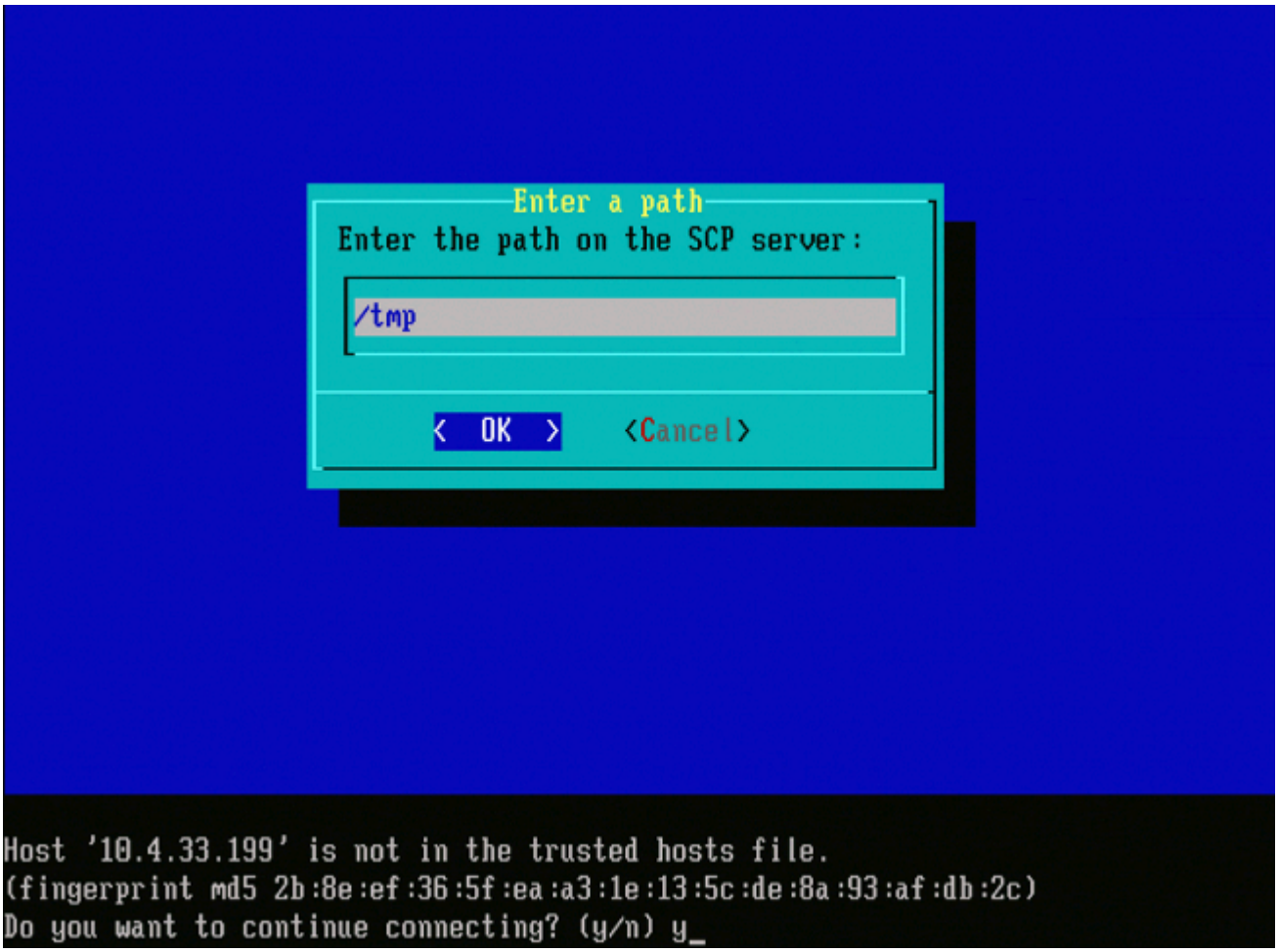


Figura 19

Observação: se você receber um erro de conectividade neste ponto em vez da mensagem esperada, verifique sua conexão com o servidor SSH.

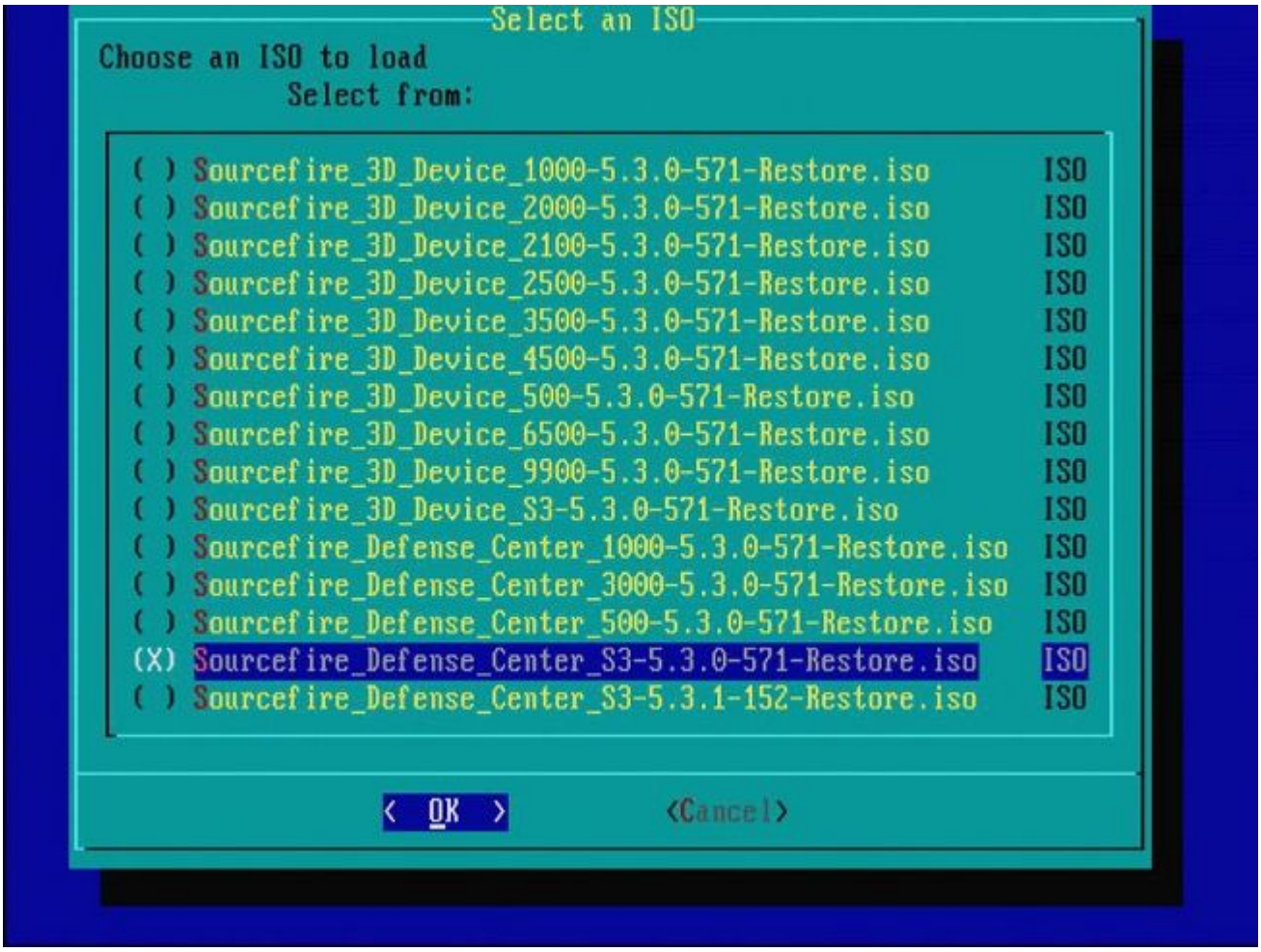


Figura 20 - Para selecionar a imagem .iso, pressione a barra de espaço.

Observação: é necessário usar os nomes de arquivo padrão para os arquivos .iso ou os arquivos possivelmente não serão detectados nesta etapa.
Erro: Nenhuma Imagem ISO Encontrada
Na versão 6.3, a convenção do nome ISO mudou de Sourcefire_3D_Device_S3-<ver>-<build>-Restore.iso para Cisco_Firepower_NGIPS_Appliance-<ver>-<build>-Restore.iso. Se você encontrar **"Nenhuma imagem ISO encontrada",** renomeie o arquivo ISO para o nome de arquivo herdado. Isso normalmente acontece quando uma nova imagem do 6.2.x ou de uma versão mais antiga para o 6.3.0 ou uma versão mais recente.

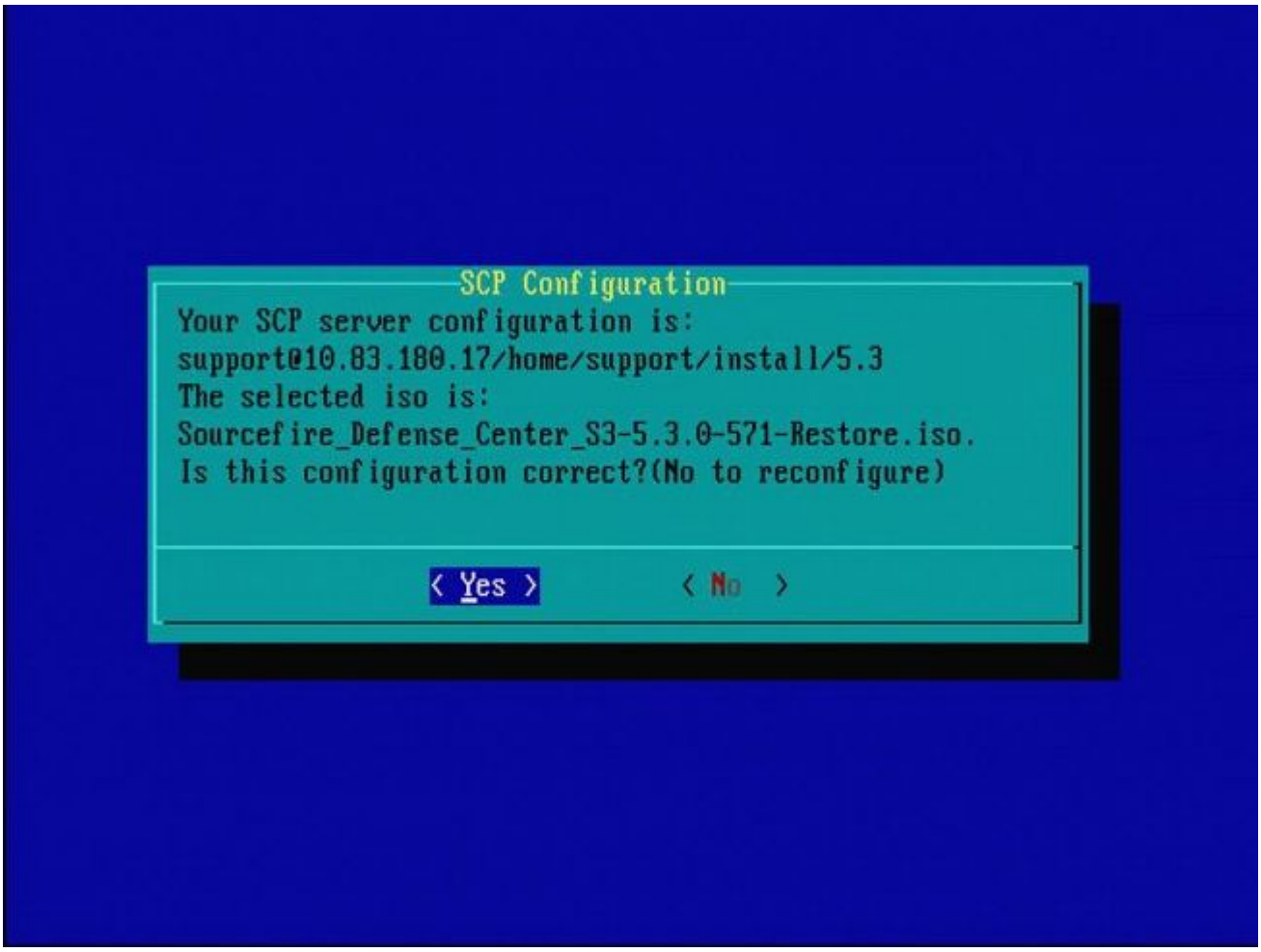
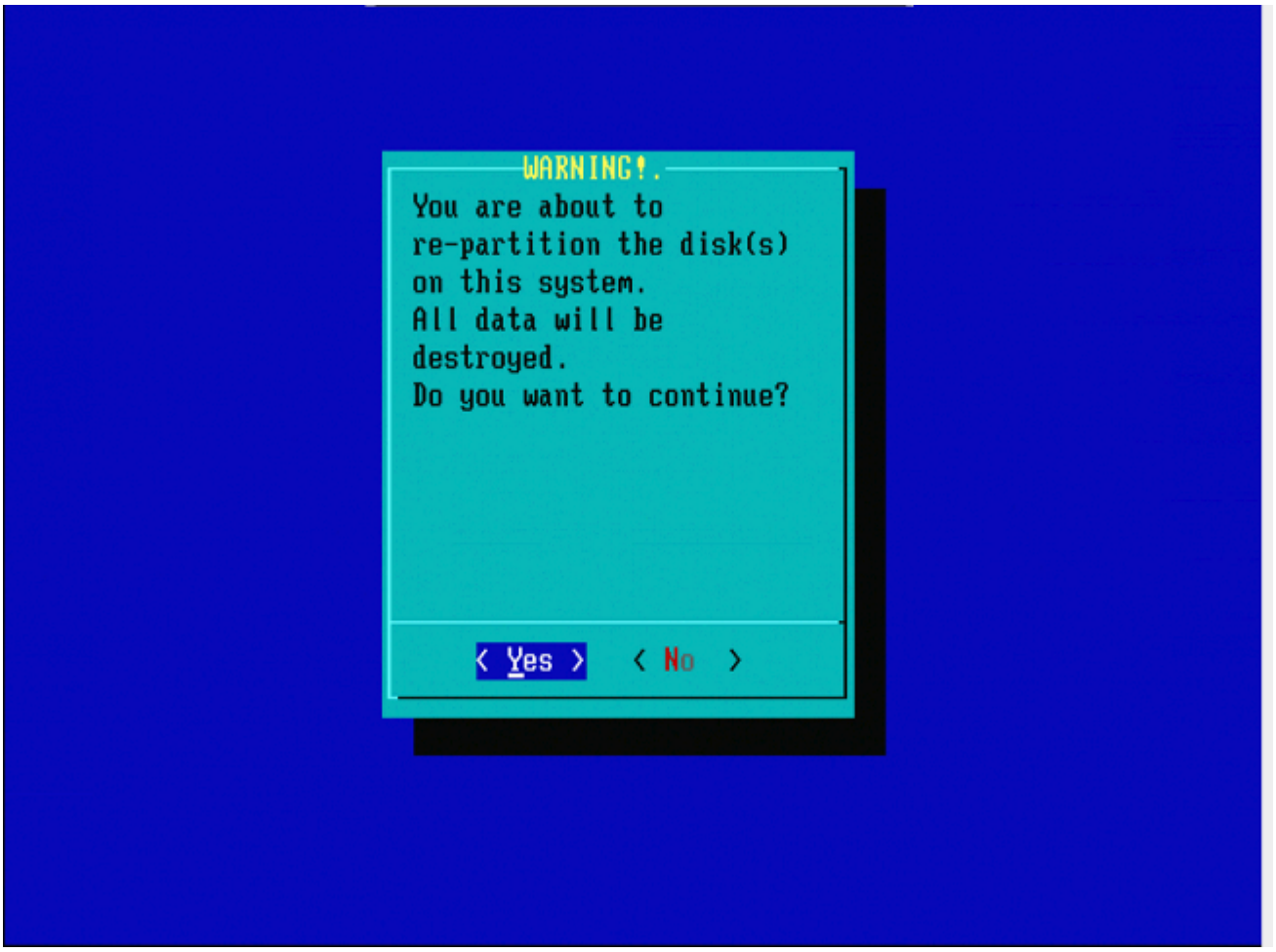
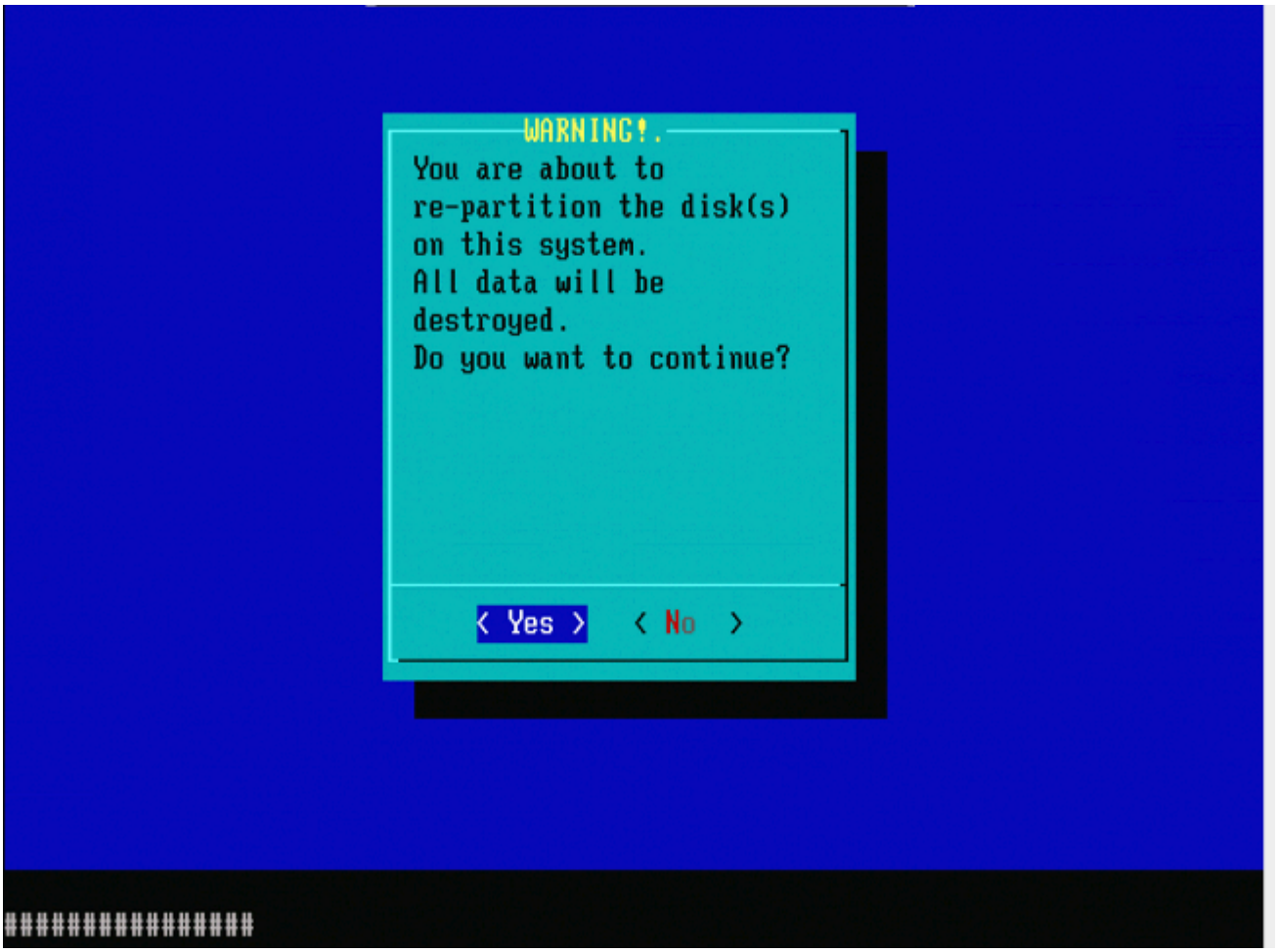

SCP Configuration
Your SCP server configuration is:
support@10.83.180.17/home/support/install/5.3
The selected iso is:
Sourcefire_Defense_Center_S3-5.3.0-571-Restore.iso.
Is this configuration correct?(No to reconfigure)
< Yes >
< No >
Figura 21

Figura 22 - O Suporte da Cisco recomenda ignorar a etapa 3 neste processo. Patches e atualizações de regras de Snort (SRUs) podem ser instalados após a conclusão da recriação.


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

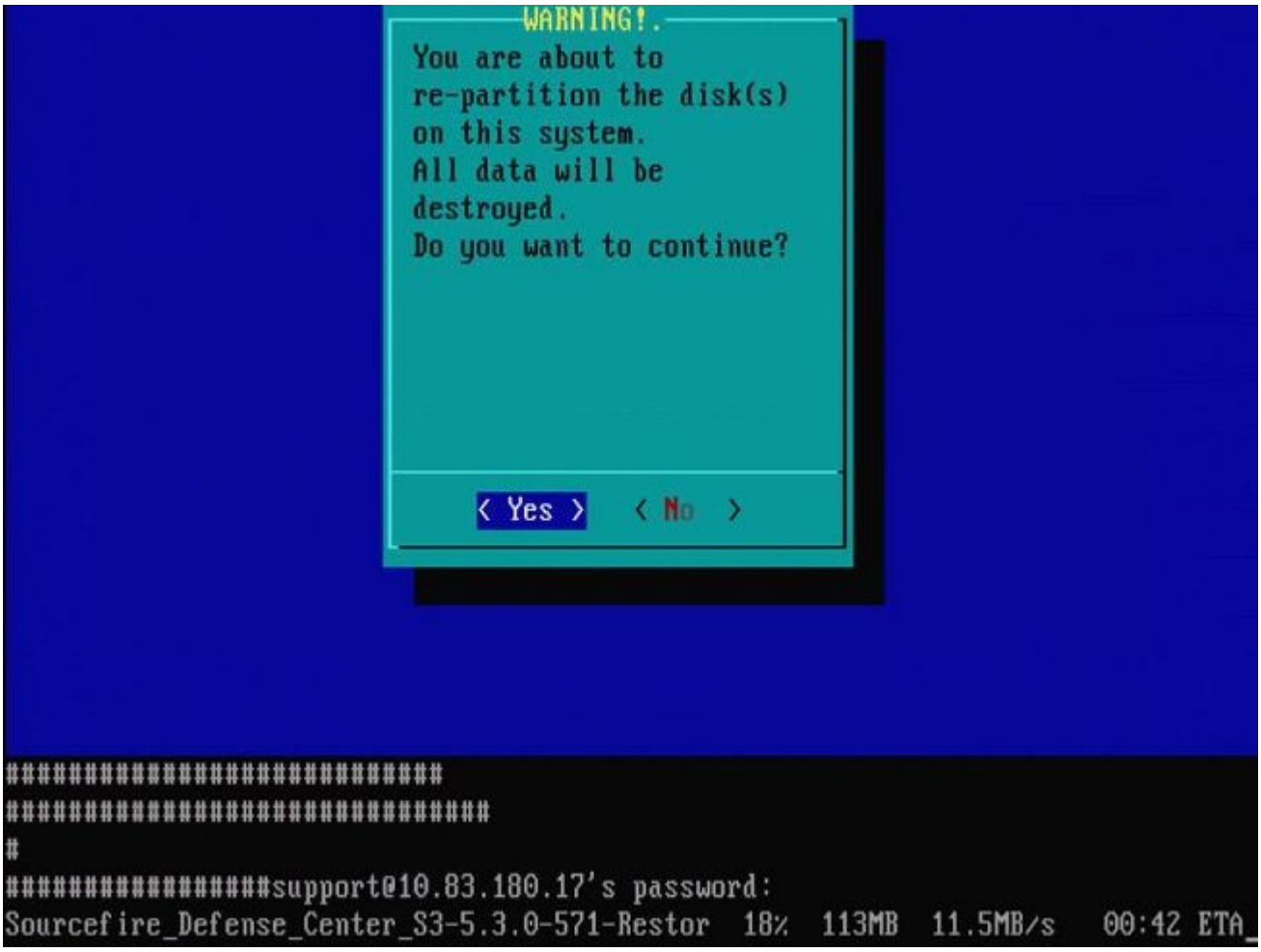

WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >
##############################
##################################
#
##################support@10.83.180.17's password:
Sourcefire_Defense_Center_S3-5.3.0-571-Restor 18% 113MB 11.5MB/s 00:42 ETA
Figura 25

Figura 26

Observação importante com relação a uma nova imagem de uma versão de software principal diferente: Se você tentar fazer uma nova imagem de um dispositivo que executava anteriormente uma versão de software principal diferente, como se você fizesse uma nova imagem de 5.1 > 5.2, 5.2 > 5.3, 5.3 > 5.2 e assim por diante, você deverá concluir as etapas descritas nas Figuras 1 - 26 **duas vezes**.

1. Depois que você escolhe **OK** no prompt, como mostrado na imagem 26, a partição Restauração do sistema é atualizada para a nova versão e o equipamento é reinicializado.
2. Após a reinicialização, você deve iniciar o processo de recriação novamente desde o início e continuar pelo processo descrito nas Figuras 27b a 31.

Se esta for a primeira recriação de uma versão de software principal diferente, você verá a tela como mostrado na imagem 27a e, em seguida, nas Figuras 31 e 32.

> **Cuidado**: se você vir essa tela, há um possível atraso sem saída visível após "Verificar o hardware" e antes de "O dispositivo USB...". **Não** pressione nenhuma tecla neste momento, ou o dispositivo reinicializa em um estado inutilizável e precisa ser recriado novamente.

Se esse não for o caso, você pode ver as telas nas Figuras 27b a 32.

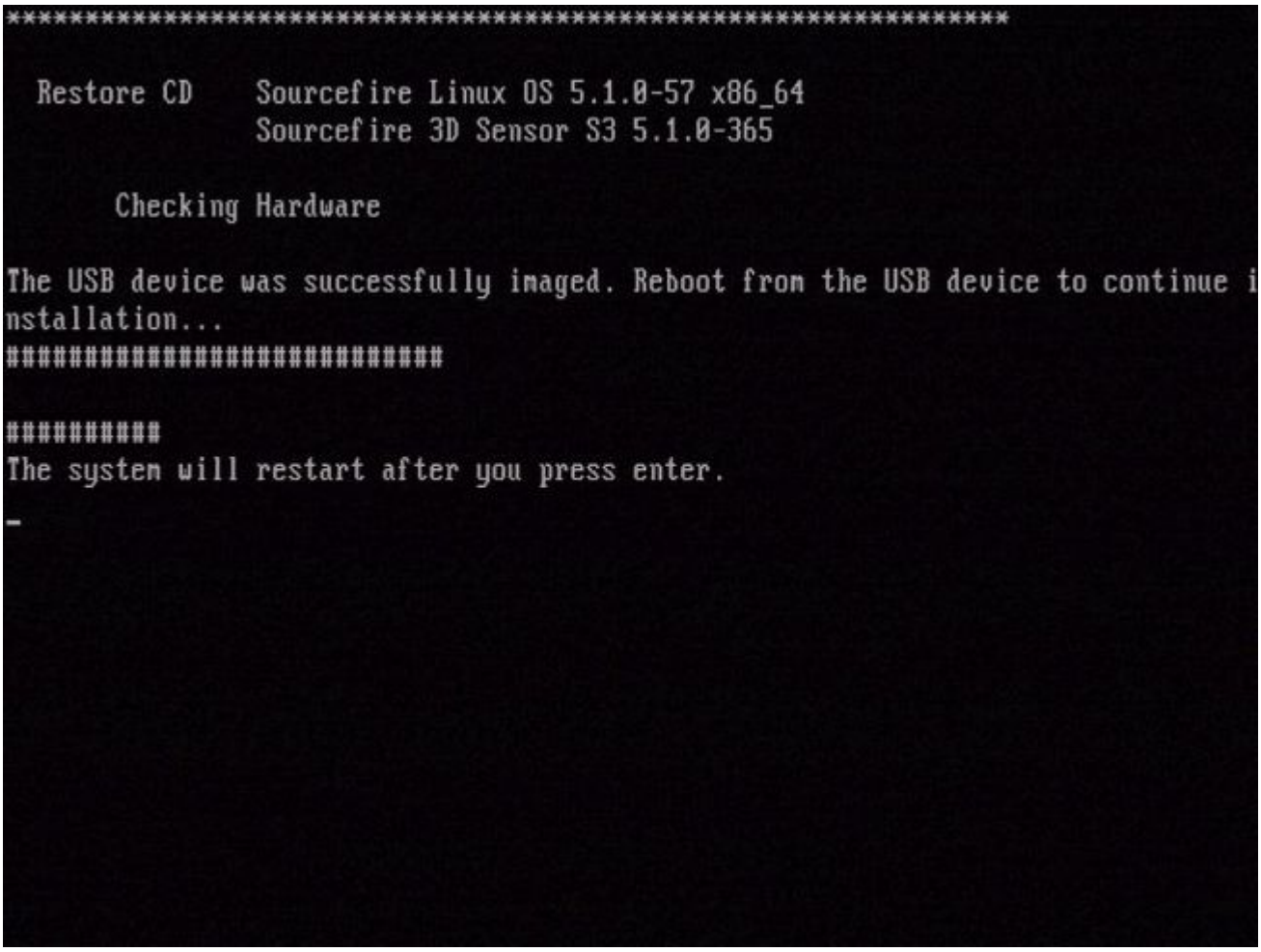
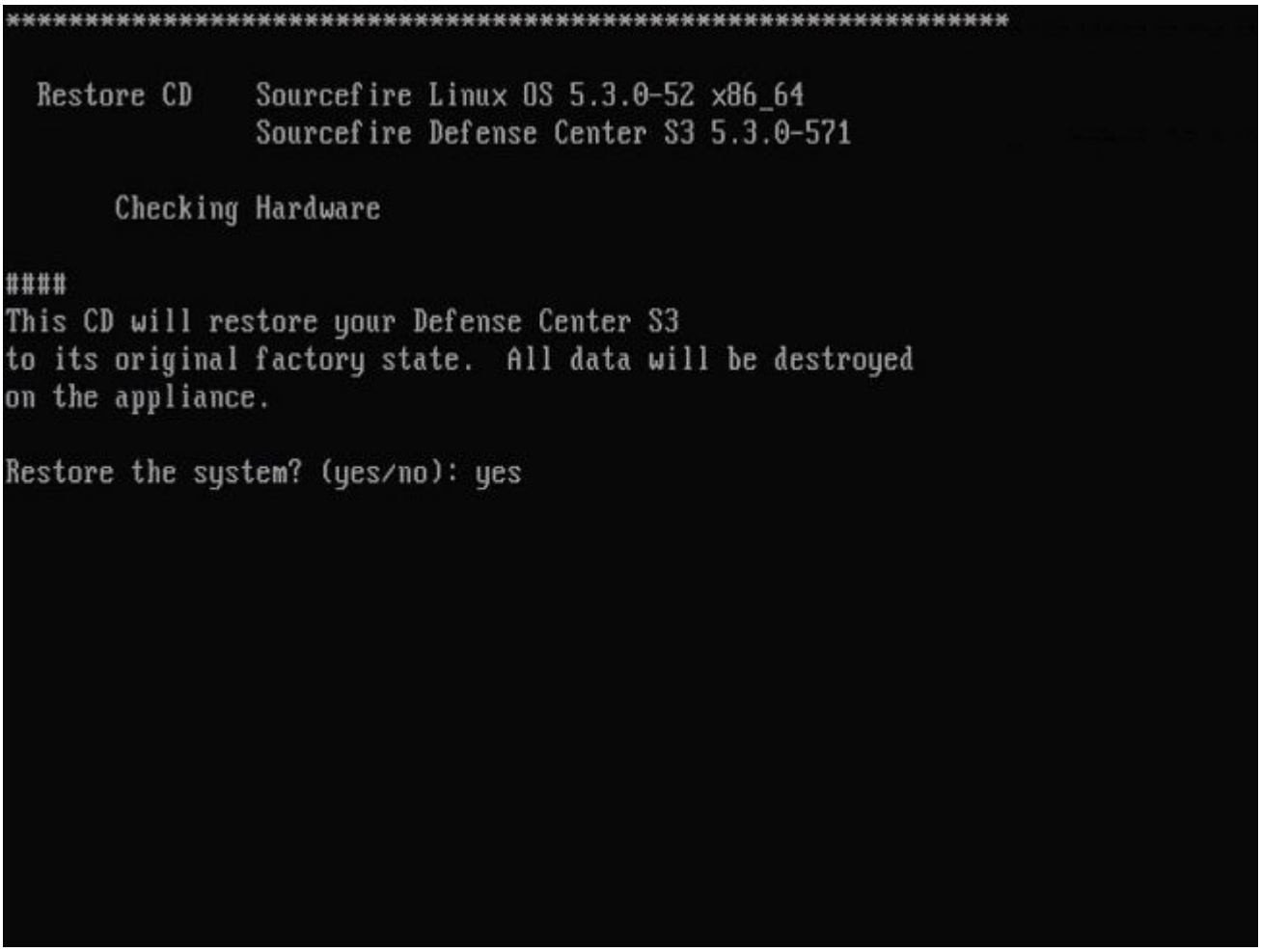
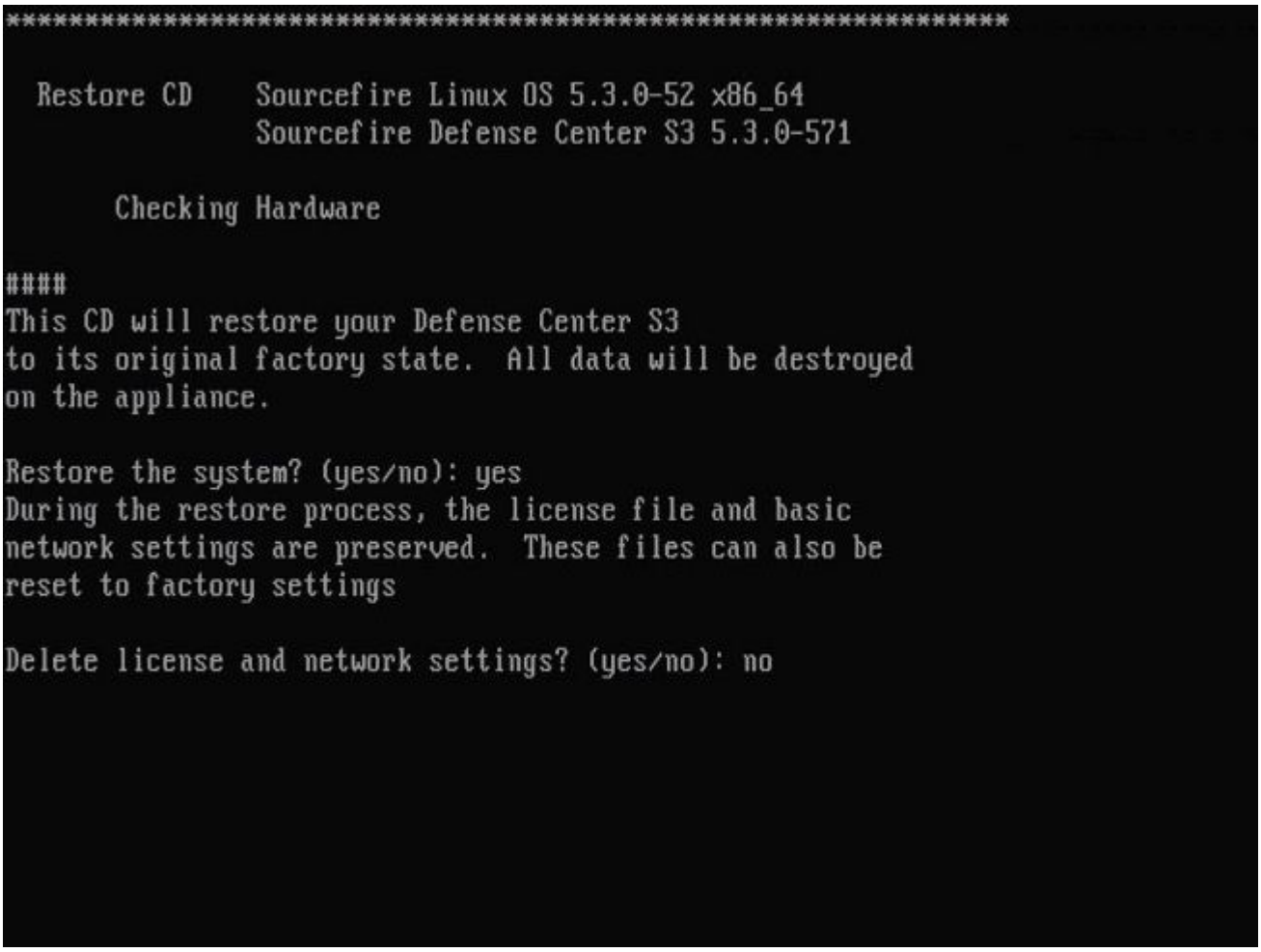
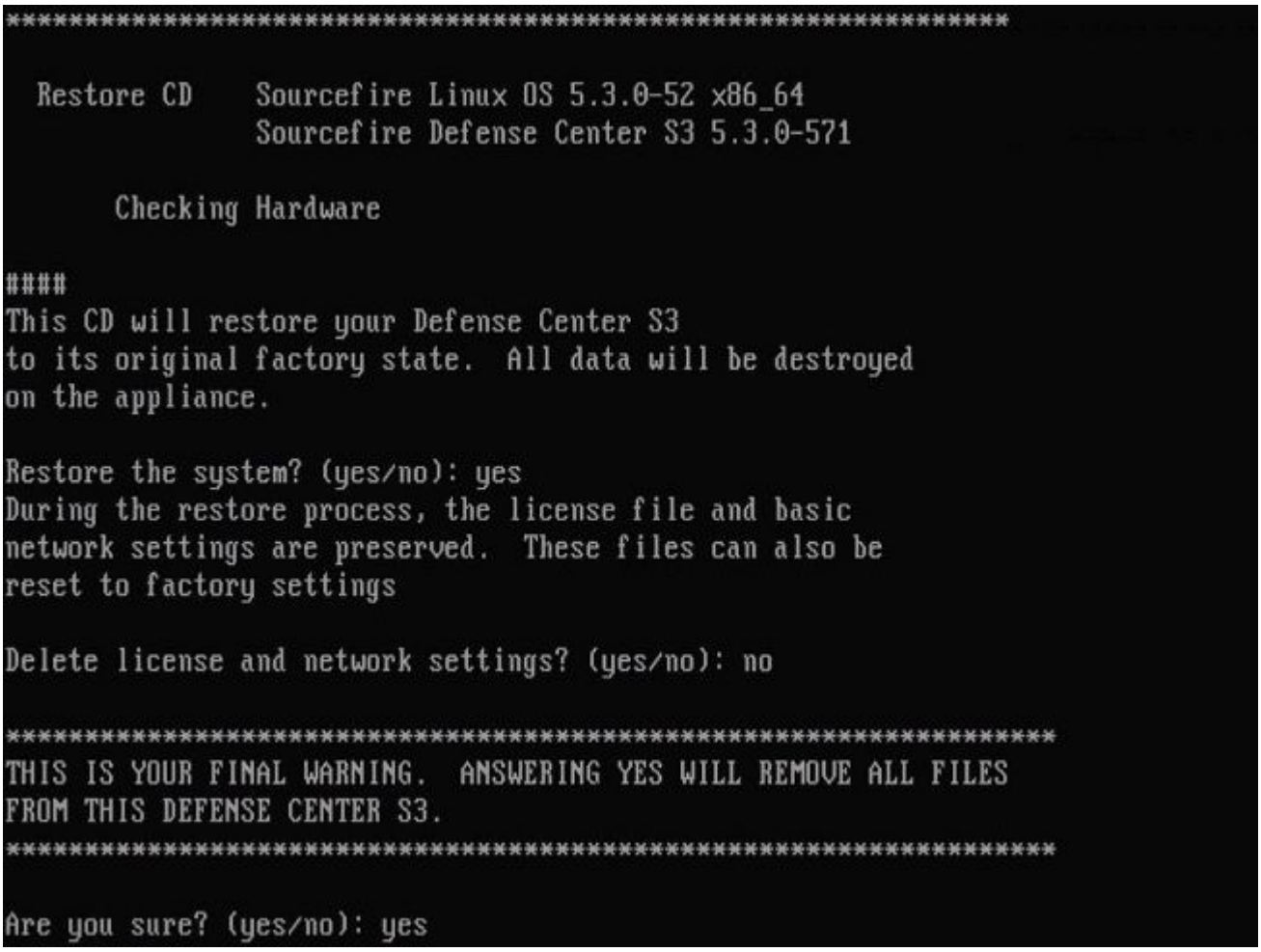
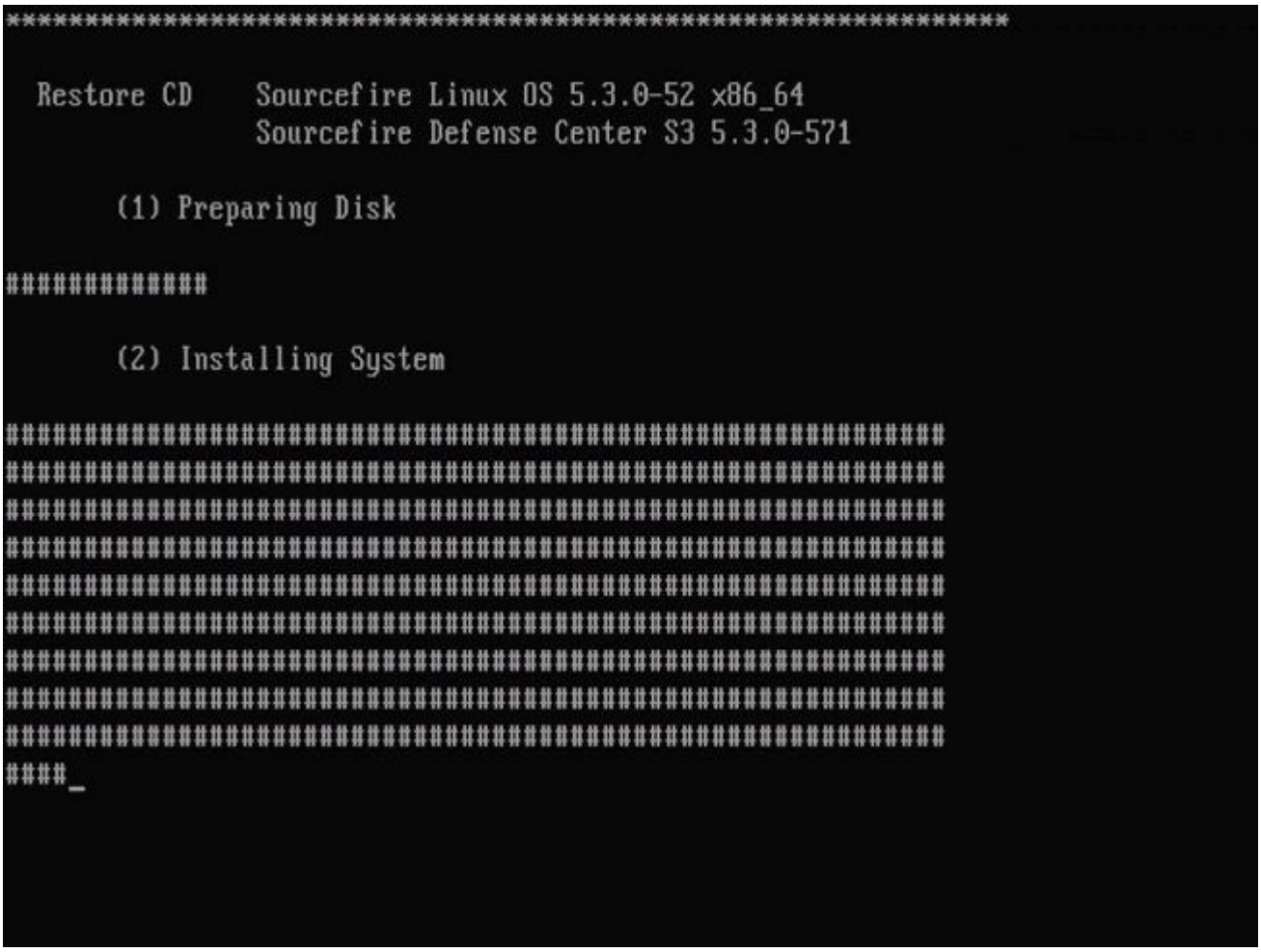

****
Restore CD Sourcefire Linux OS 5.1.0-57 x86_64
Sourcefire 3D Sensor S3 5.1.0-365
Checking Hardware
The USB device was successfully imaged. Reboot from the USB device to continue i
nstallation...
##########
##########
The system will restart after you press enter.

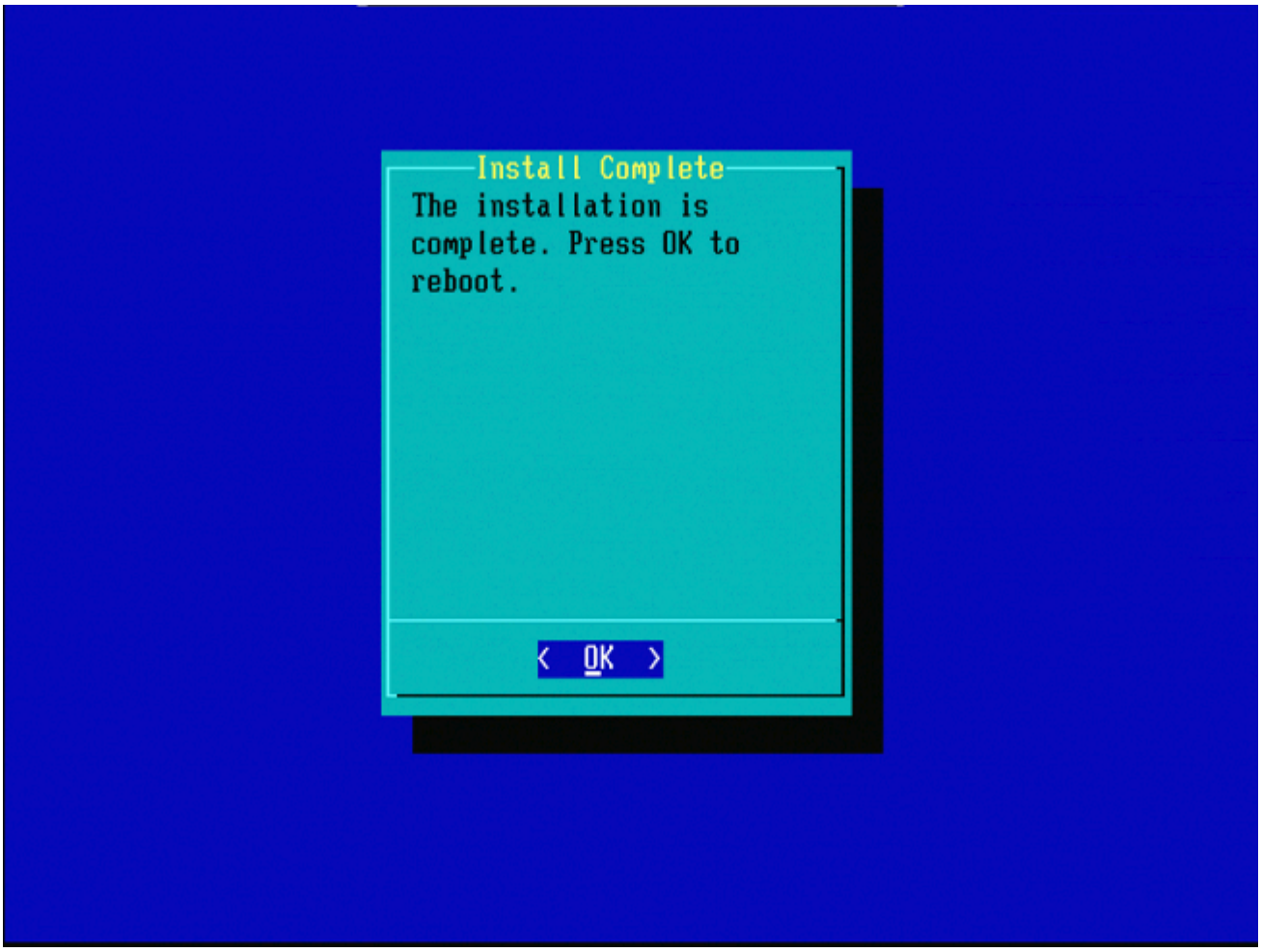
Figura 27a


****
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

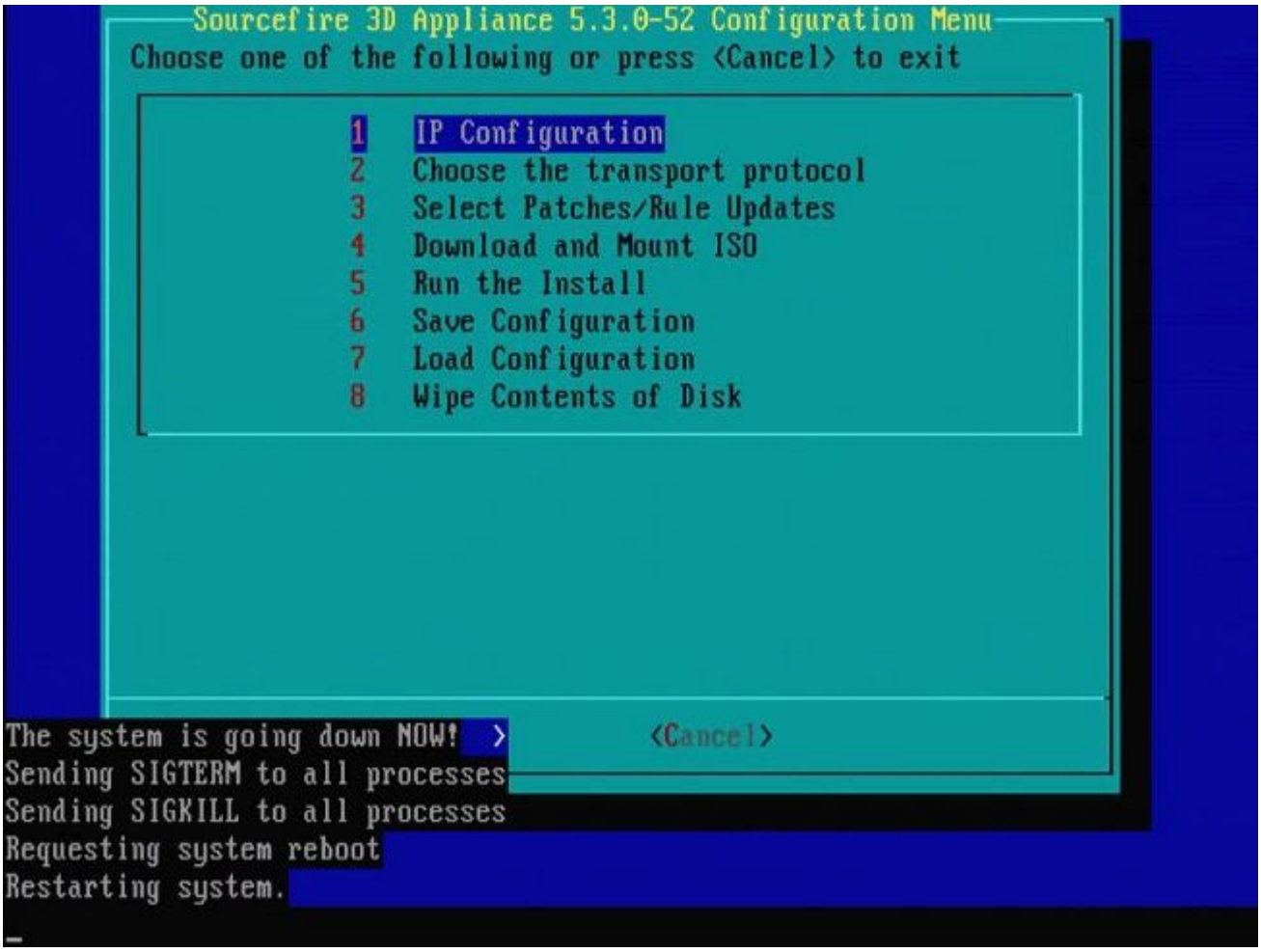


Figura 32

Cisco Firepower Management Center 1000, 2500 e 4500

No FMC 1000, 2500 e 4500, as opções são diferentes. Use um switch KVM ou o CIMC e, enquanto o dispositivo é iniciado, você verá estas opções:

1 - Modo VGA do Cisco Firepower Management Console

2 - Cisco Firepower Management Console Serial

3 - Modo de restauração do sistema do Cisco Firepower Management Console

4 - Modo de restauração de senha do Cisco Firepower Management Console

Se quiser entrar no Modo de restauração com a interface do usuário, selecione a opção 'Modo de restauração do sistema do Cisco Firepower Management Console' (opção **3**) e, em seguida, 'Modo de restauração VGA do sistema do Cisco Firepower Management Console' (opção **1**

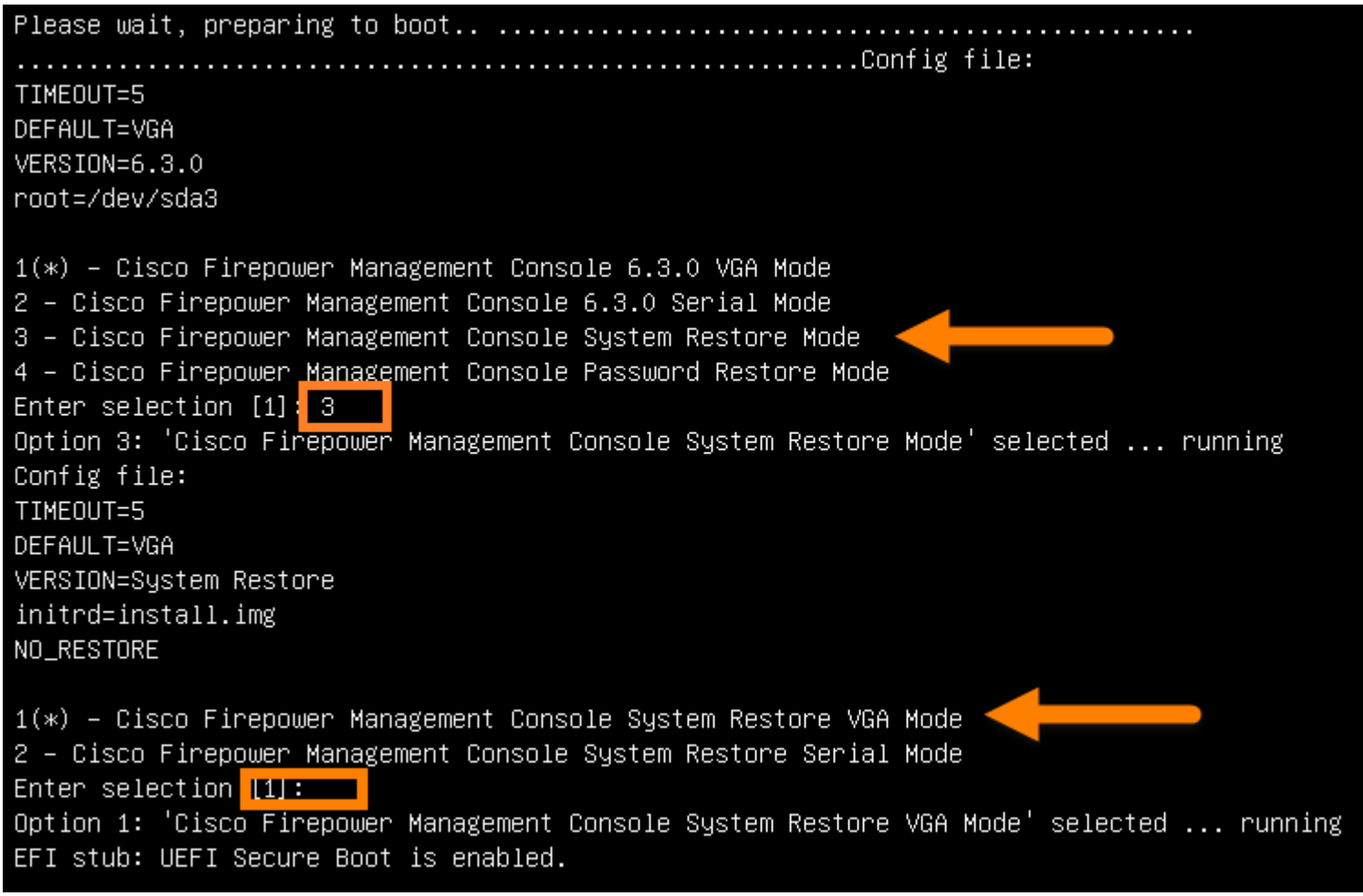


Figura 33

O resto do processo é o mesmo que em outros dispositivos FMC.

Troubleshoot

A opção de menu System_Restore LILO não está listada

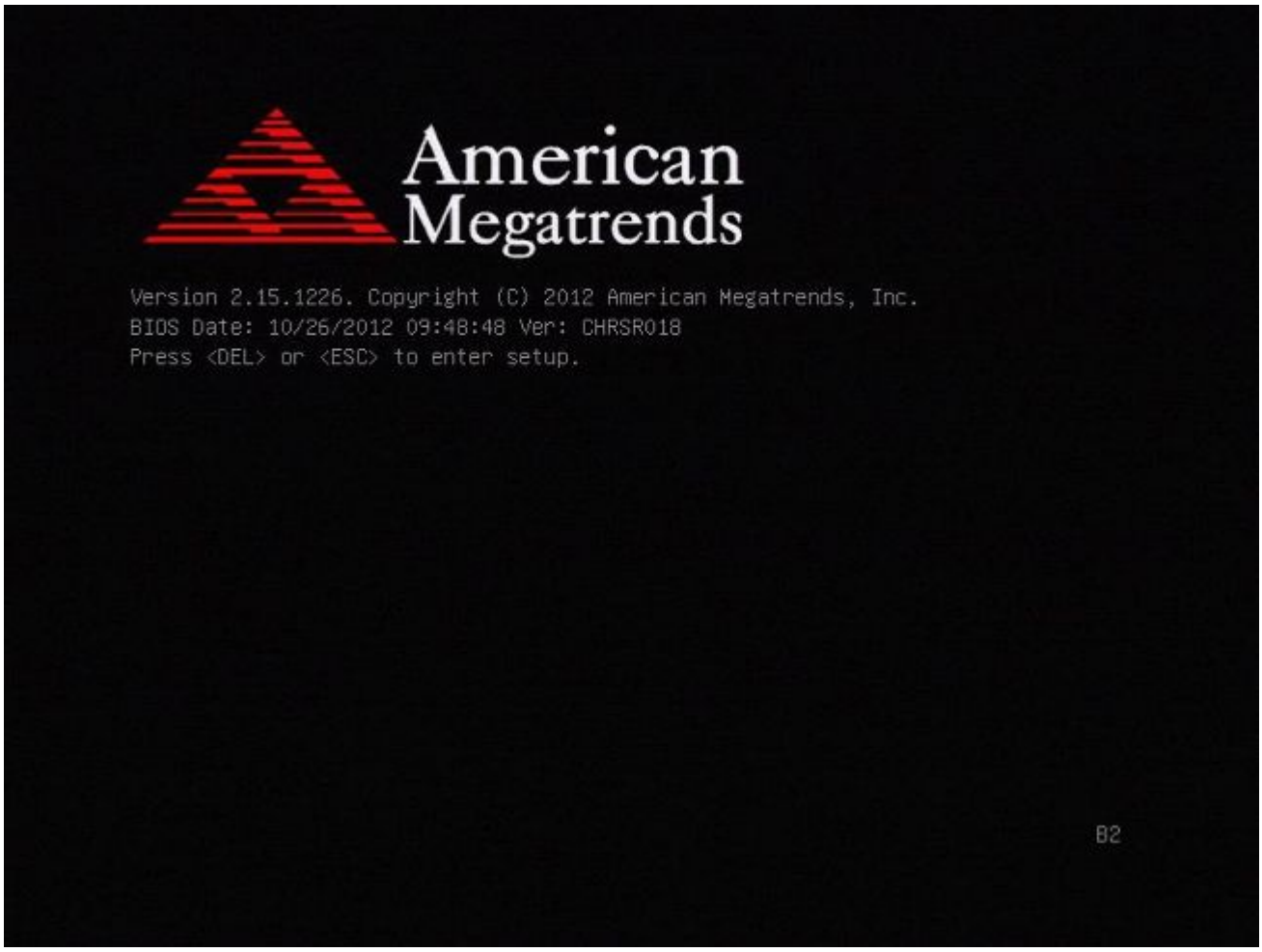
O FireSIGHT Management Center e os dispositivos FirePOWER 7000 e 8000 Series têm uma unidade flash integrada que contém o sistema de recriação de imagem. Se a opção "**System_Restore**" não estiver listada no menu de inicialização do LILO (Linux Loader), ainda será possível acessar essa unidade para concluir a recriação.

Dispositivos 7010, 7020 e 7030

Se você usa um dispositivo da série 70XX, siga estas etapas para selecionar o dispositivo de inicialização:

1. Desligue o dispositivo normalmente.

2. Ligue o equipamento e pressione a tecla **Delete** várias vezes enquanto o equipamento é inicializado para acessar a tela de seleção do dispositivo de inicialização. Veja a imagem aqui:


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

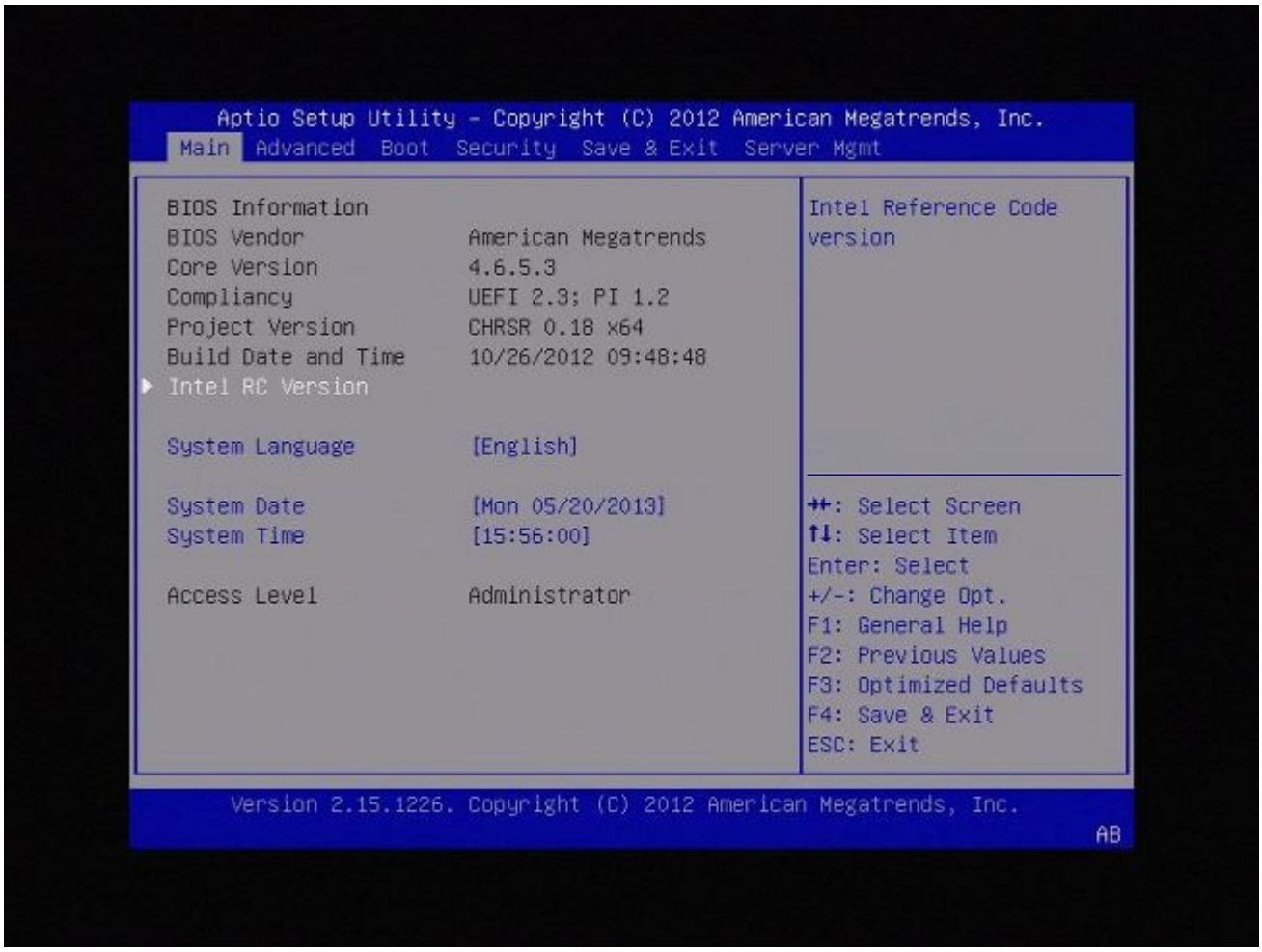


Figura A2

3. Use a tecla de seta para a direita para selecionar a guia **Save & Exit**. Nesta guia, use a tecla de seta para baixo para selecionar **SATA SM: InnoDisk. - InnoLite** e pressione a tecla **Enter**.

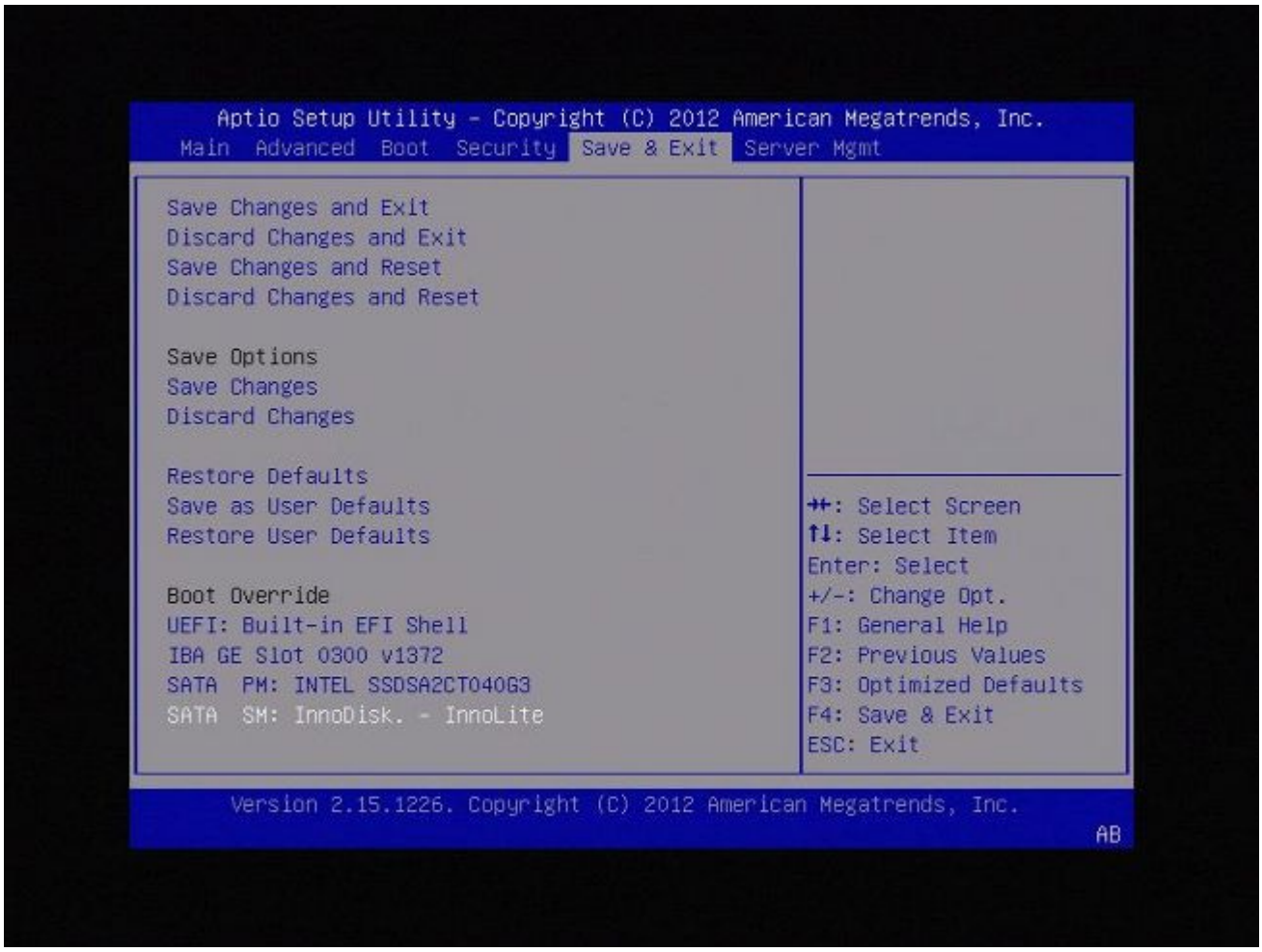


Figura A3

4. Escolha a opção **0** se você usa um teclado e um monitor.

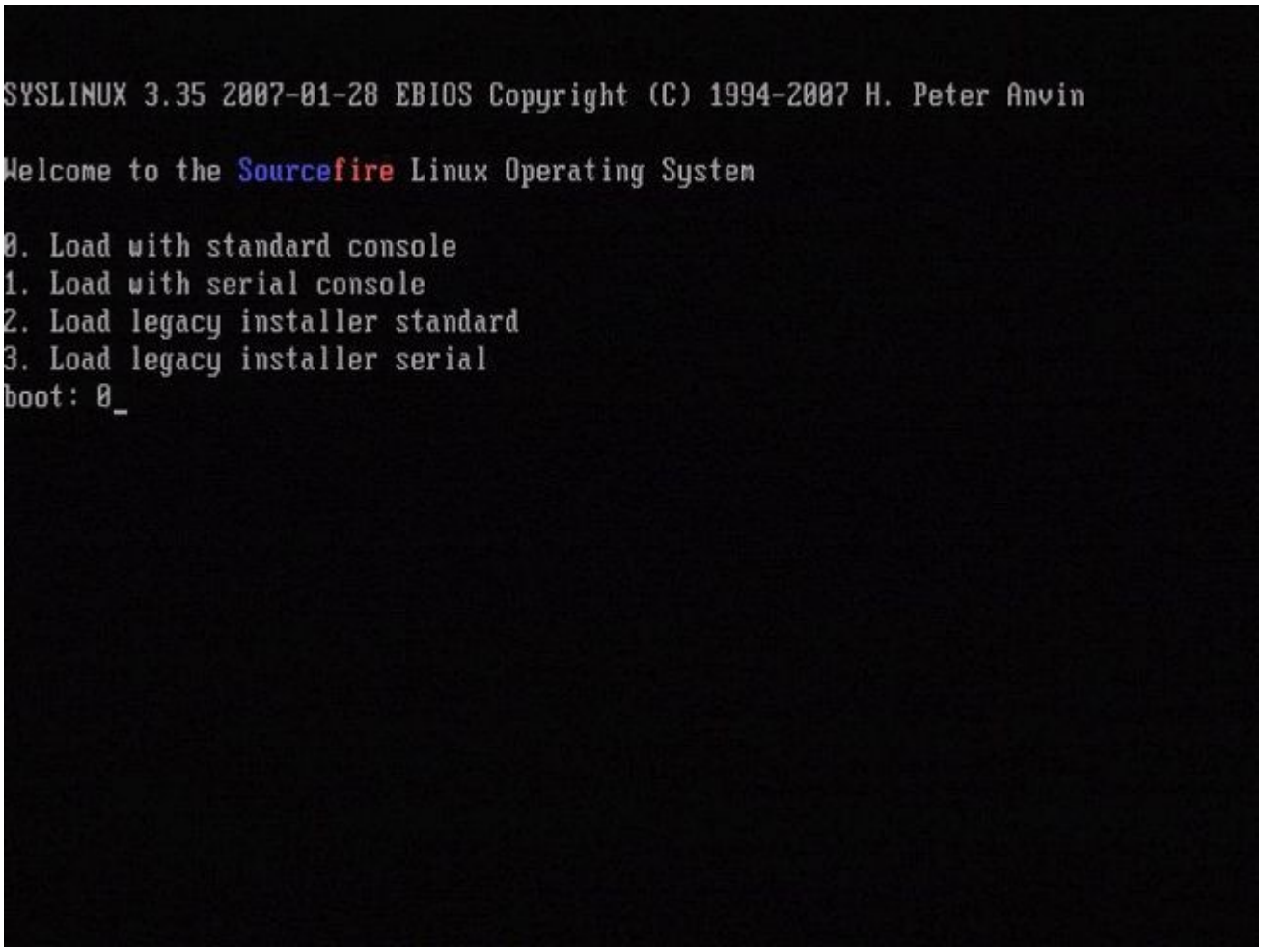

SYSLINUX 3.35 2007-01-28 EBIOS Copyright (C) 1994-2007 H. Peter Anvin
Welcome to the Sourcefire Linux Operating System
0. Load with standard console
1. Load with serial console
2. Load legacy installer standard
3. Load legacy installer serial
boot: 0_
Figura A4

Figura A5

Dispositivos 7110 e 7120

Se você usa um dispositivo da série 71XX, siga estas etapas para selecionar o dispositivo de inicialização:

1. Desligue o dispositivo normalmente.

2. Ligue o equipamento e pressione a tecla **F11** várias vezes enquanto ele é inicializado para acessar a tela de seleção do dispositivo de inicialização. Veja a imagem mostrada aqui:

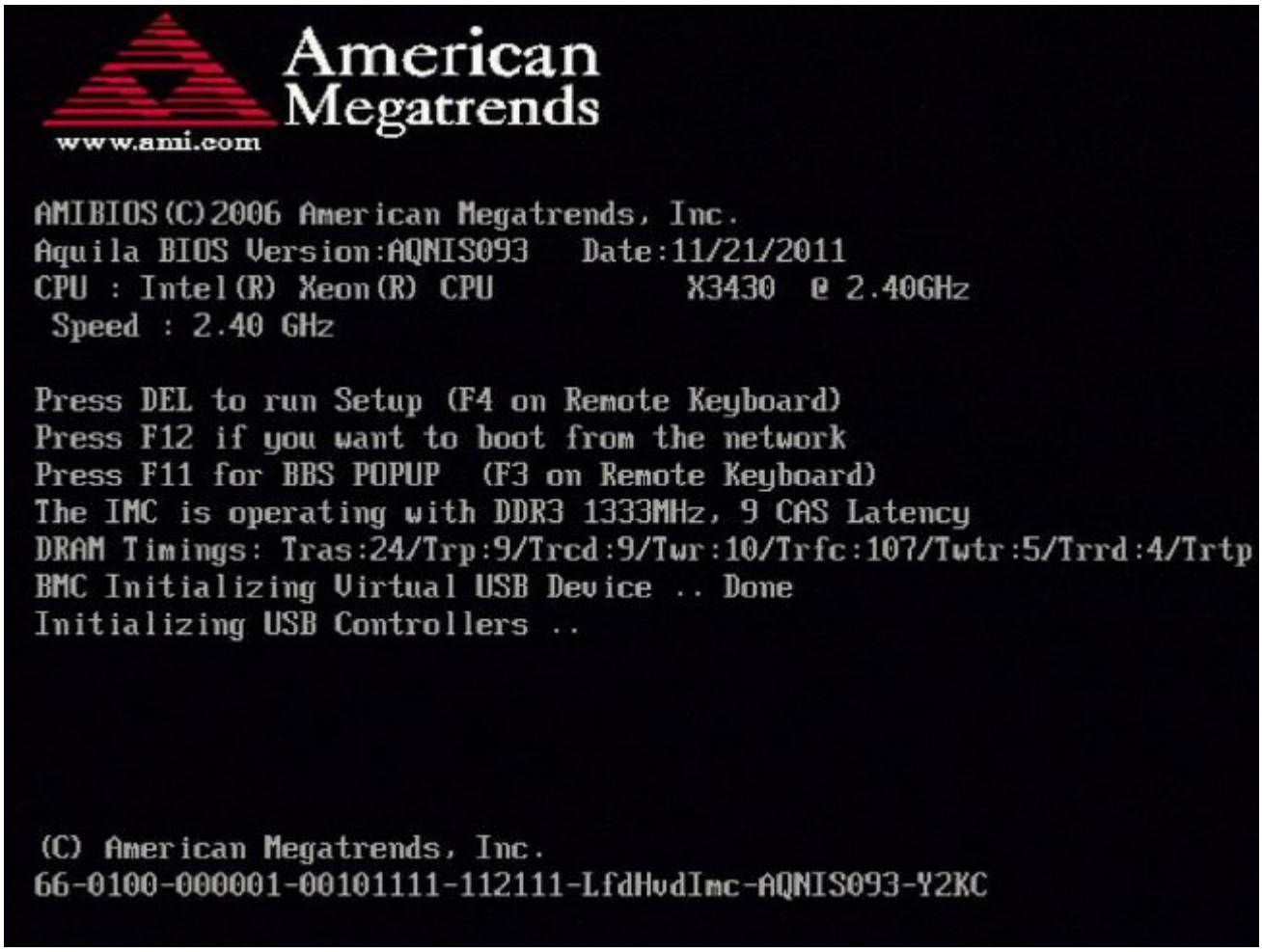


Figura B1

3. Selecione a opção **HDD:P1-SATADOM** e pressione **Enter** para inicializar na partição **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

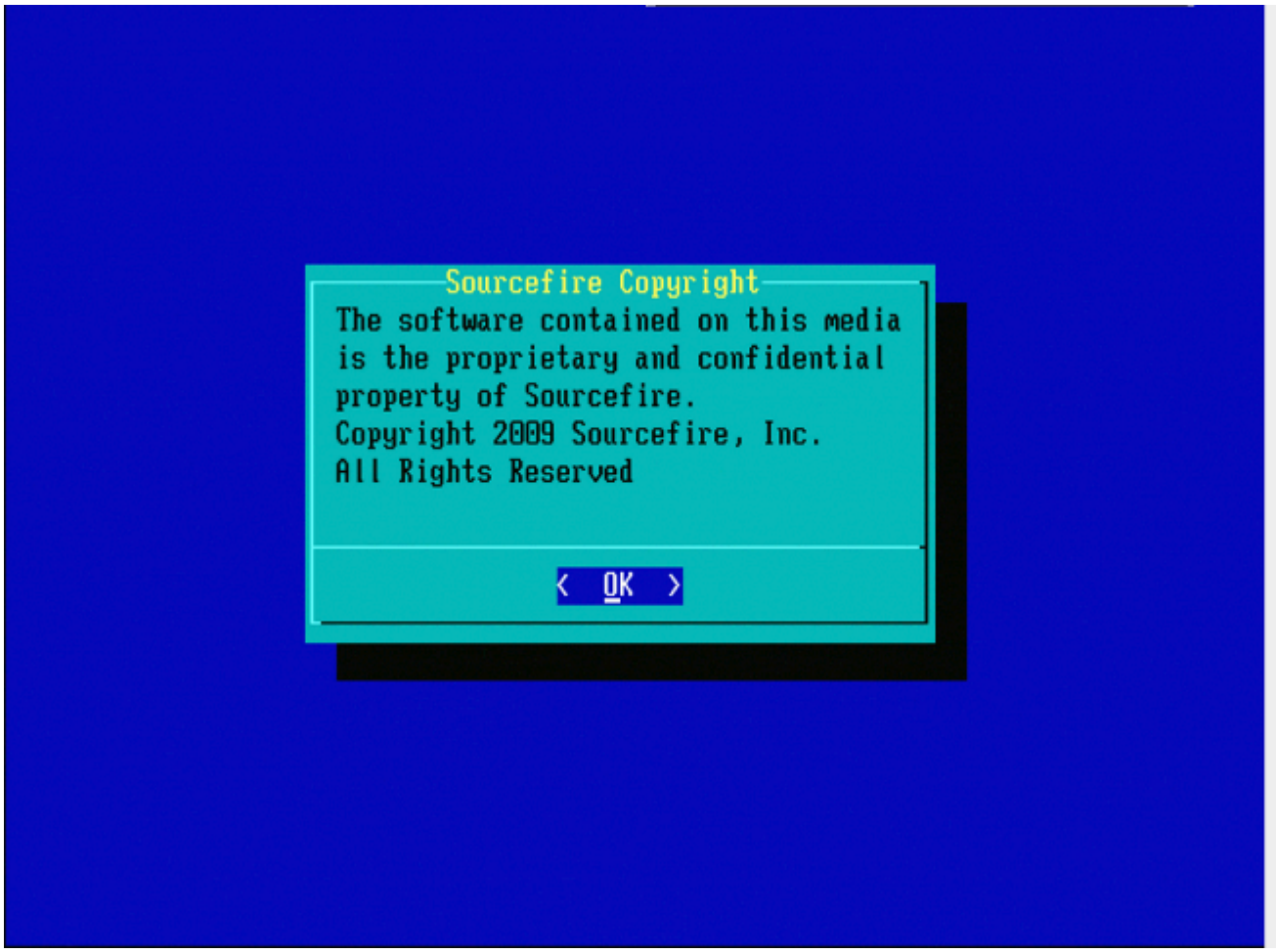


Figura B3

Dispositivos 8000 Series ou modelos Management Center FS750, FS1500 ou FS3500

Se você usa um dispositivo 8000 Series ou um Management Center modelo FS750, FS1500 ou FS3500, conclua estas etapas para selecionar o dispositivo de inicialização:

1. Desligue o dispositivo normalmente.

2. Ligue o dispositivo e pressione a tecla **F6** repetidamente enquanto o dispositivo é inicializado para acessar a tela de seleção do dispositivo de inicialização. Veja a imagem mostrada aqui:

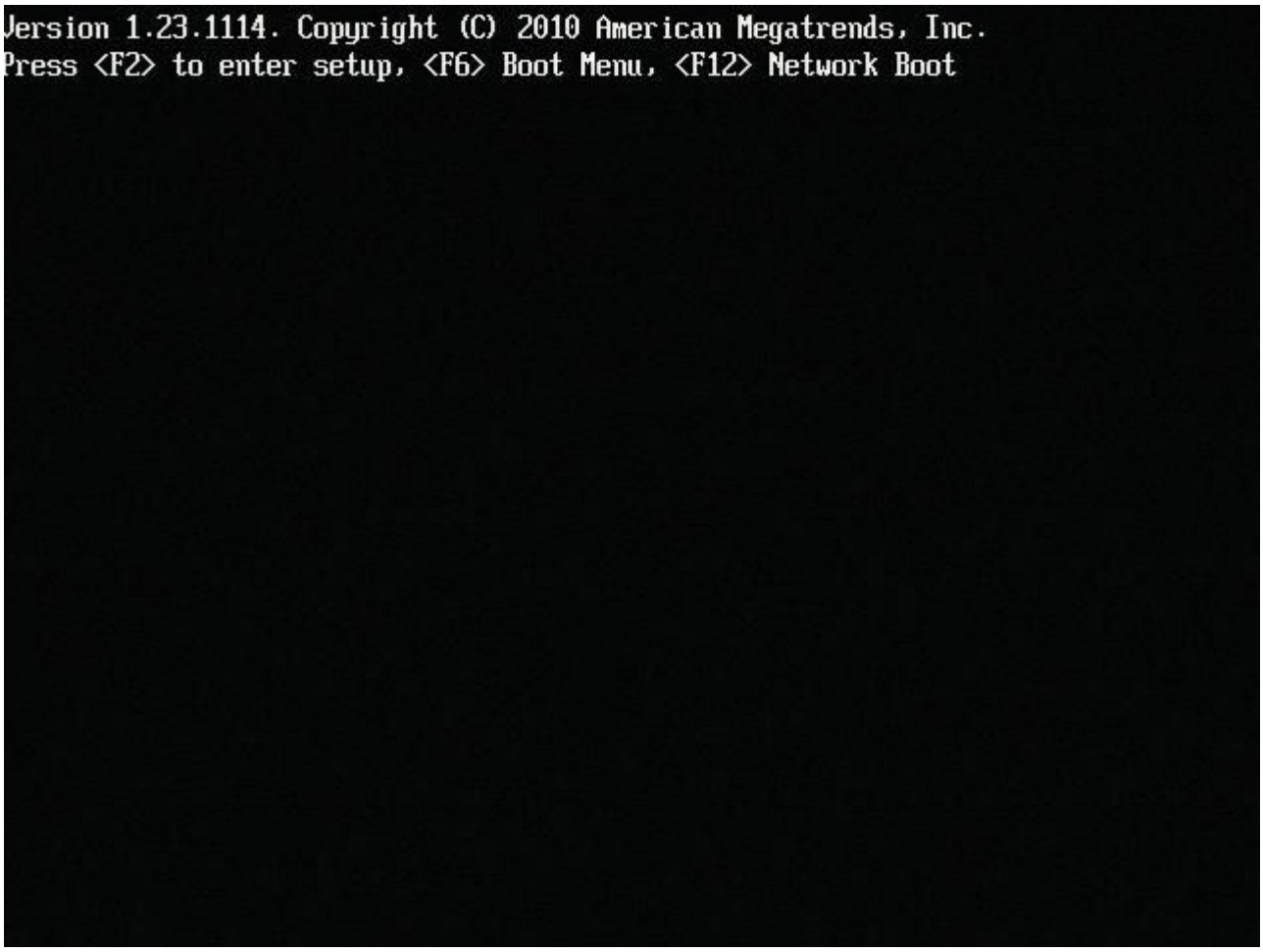


Figura C1

3. Selecione a opção USB.

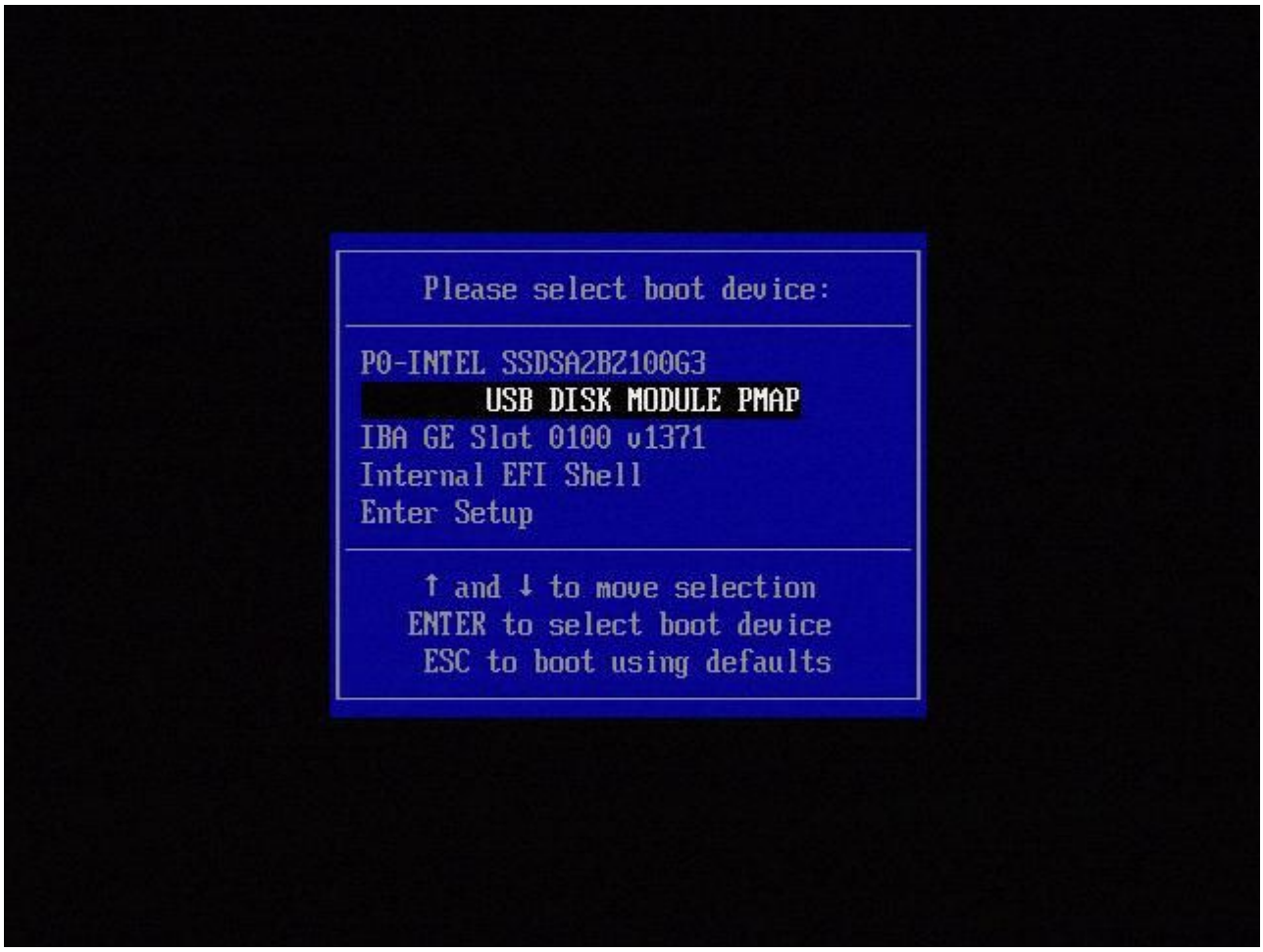


Figura C2

4. O equipamento é inicializado a partir da partição System_Restore e exibe o menu **System_Restore**.

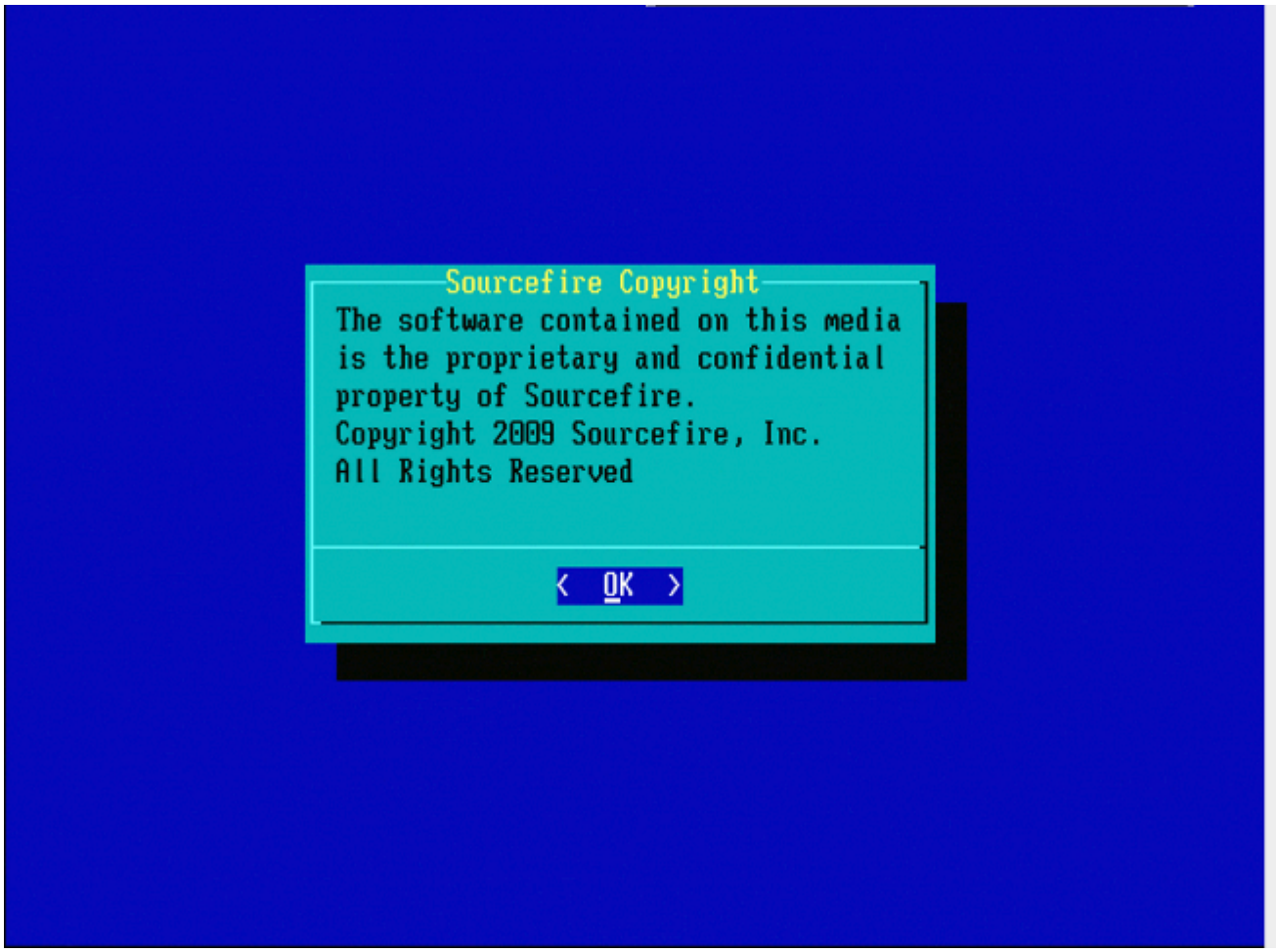


Figura C3

Restauração do sistema para modelos FMC1000, FMC2500, FMC4500 (FMCs baseados em M4)

> **Observação**: para o FMC4500, este modelo tem um menu de inicialização diferente, mais detalhes estão no próximo link

---

O prompt para selecionar a restauração do sistema é exibido de forma diferente nos seguintes modelos: FMC1000, FMC2500, FMC4500

1. Durante a inicialização, você pode ver esta tela por 5 segundos:

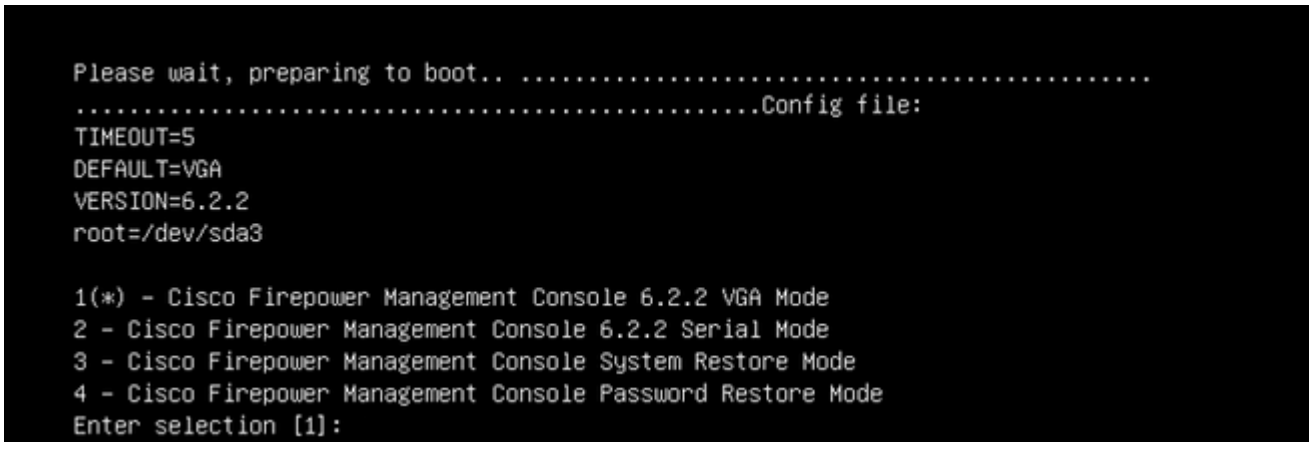


Figura D1

2. Selecione a opção Restauração do sistema (#3 nesse caso).

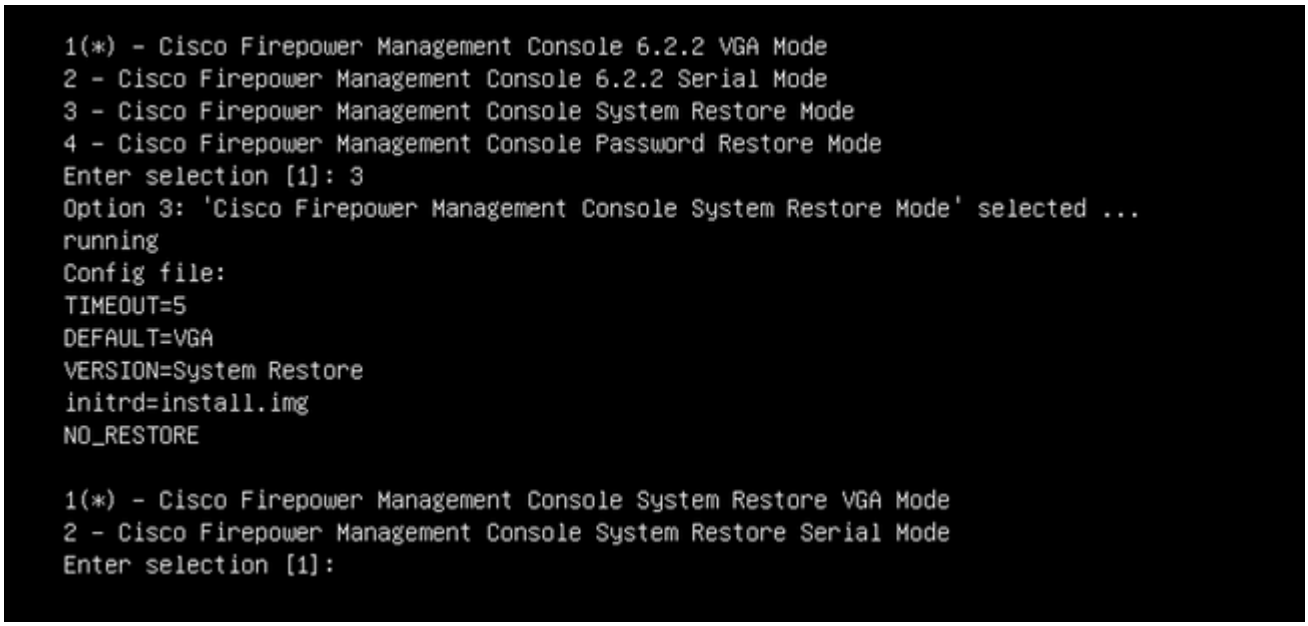


Figura D2

3. Selecione o método de exibição para a restauração do sistema (#1 para VGA, neste caso)

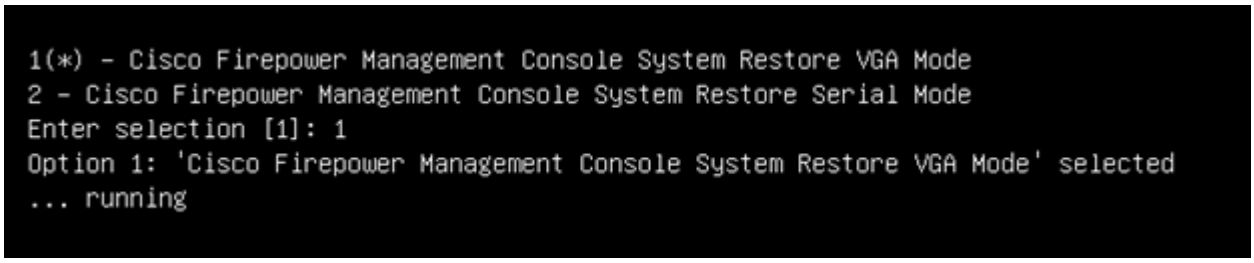


Figura D3

4. Em seguida, você chega ao prompt visto na figura 5 e o processo continua normalmente.

Opção de inicialização não listada

É possível que a opção de inicializar na partição de recriação não esteja listada no BIOS ou no menu de inicialização. Se esse for o caso, a unidade que contém o sistema de recriação possivelmente está ausente ou danificada. Uma RMA é provavelmente necessária.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.