FireSIGHT Management Center 및 Firepower 어플라이언스 재이미지화

목차

소개

이 문서에서는 Cisco FMC(FireSIGHT Management Center) 및 Firepower 어플라이언스의 리이미지 처리 절차에 대한 예제와 함께 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

관리되는 디바이스	FireSIGHT Management Center	이미지로 다시 설치할 수 있는 소프트웨어 버전
Cisco Firepower 7000 Series	FS 750 1500	5.2 이상

Cisco Firepower 7100 Series Cisco Firepower 8100 Series Cisco Firepower 8200 Series	FS 3500	
Firepower 8300 시리즈 Cisco AMP 7150 Cisco AMP 8150		5.3 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

이미지로 다시 설치 프로세스

⚠ 주의: FireSIGHT Management Center 또는 Firepower 어플라이언스를 업그레이드하거나 이미지로 다시 설치할 때 USB 스토리지 디바이스를 삽입하거나 KVM(키보드, 비디오 및 마우스) 스위치를 연결하지 마십시오.

시작하기 전에

1. Management Center 또는 독립형 Firepower 디바이스를 재이미지화하려는 경우 계속하기 전에 어플라이언스를 백업하는 것이 좋습니다.
2. 센서의 모델을 식별하고 사용된 컴포넌트(Components Used) 섹션의 모델 목록을 사용하여 이 가이드가 적절한지 확인합니다.
3. Cisco 지원 사이트에서 원하는 소프트웨어 버전에 맞는 설치 가이드 및 디스크 이미지를 다운로드하십시오.

   참고: .iso 파일의 이름을 바꾸지 마십시오

   이미지 제공: .iso 파일은 이미지로 다시 설치할 어플라이언스의 관리 네트워크에서 연결할 수 있는 SSH 서버를 실행하는 호스트에 복사해야 합니다.

   참고: 다른 SSH 서버를 사용할 수 없는 경우 이 프로세스에 FMC를 사용할 수 있습니다.

iso의 무결성 확인: md5sum 유틸리티를 사용하여 확인할 수 있도록 파일의 md5sum이 페이지의 오른쪽에 제공됩니다.

4. 설치 설명서에는 단계별 리이미지 지침이 포함되어 있으며 리이미지 프로세스를 위한 몇 가지 방법에 대한 개요도 나와 있습니다. 이 문서에 제공된 이미지는 참조용으로 사용할 수 있습니다.

이미지로 다시 설치 프로세스 개요

참고: 5.3 버전은 이 기사에 표시된 이미지를 캡처하는 데 사용되었습니다. 재이미지화 프로세스는 표시된 이미지에 나타나는 버전 번호를 제외하고 다른 5.x 버전에서도 동일합니다.

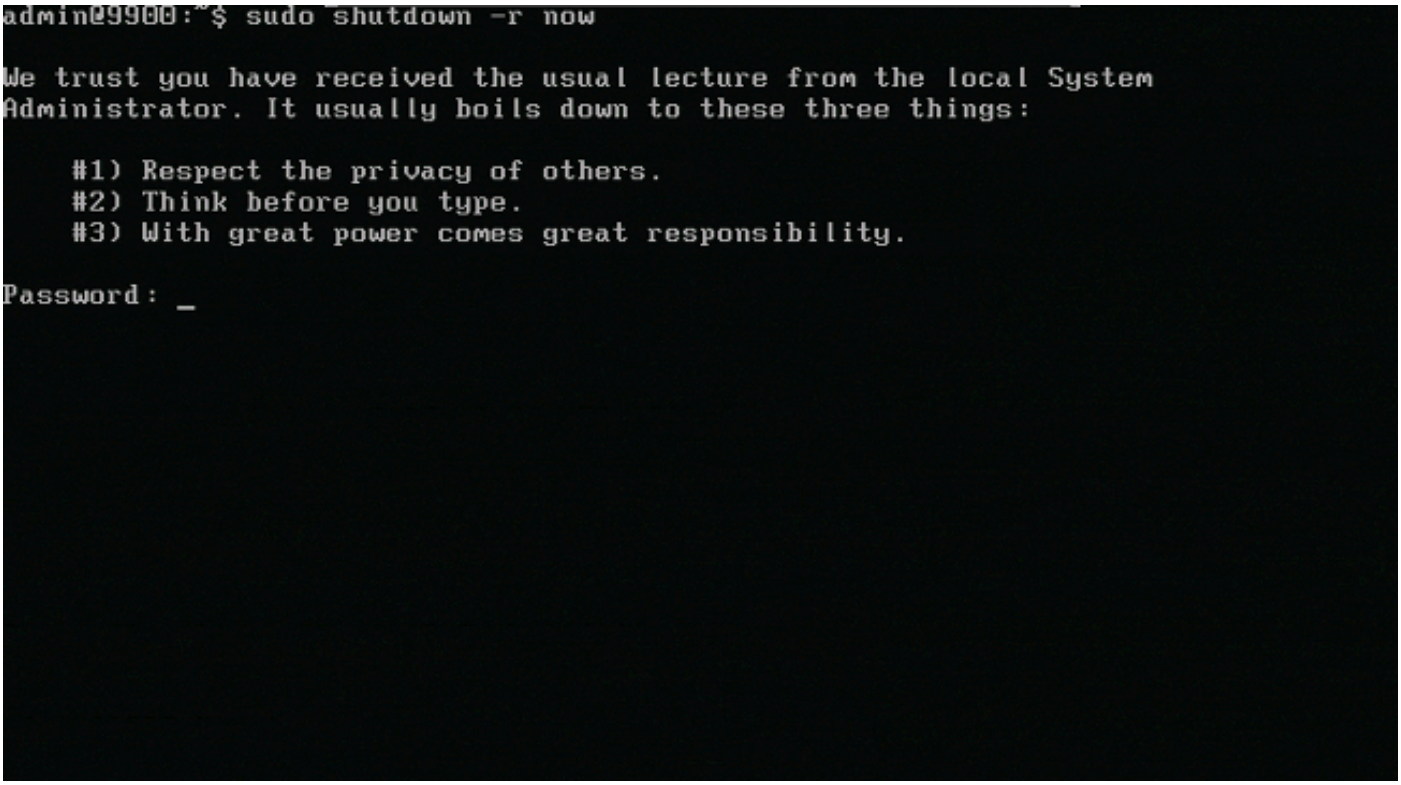


그림 1

그림 2 - 시스템이 재부팅될 때 카운트다운을 중지하려면 키보드의 화살표 키를 눌러 다음 화면에 대한 System_Restore 옵션을 선택합니다.

참고: System_Restore 프롬프트가 표시되지 않으면 부팅 순서를 변경하여 DOM(복원 파티션)으로 직접 부팅해야 합니다. 자세한 내용은 System_Restore LILO 메뉴 옵션이 없습니다.

그림 3

그림 4 - 키보드와 모니터를 사용하는 경우 옵션 0을 선택합니다.

참고: 경우에 따라 Restore(복원) 옵션의 메뉴는 Console(콘솔)이 연결된 경우에만 표시됩니다(키보드 플러그를 분리한 경우). 복구 옵션을 선택하면 바로 키보드를 다시 연결할 수 있습니다

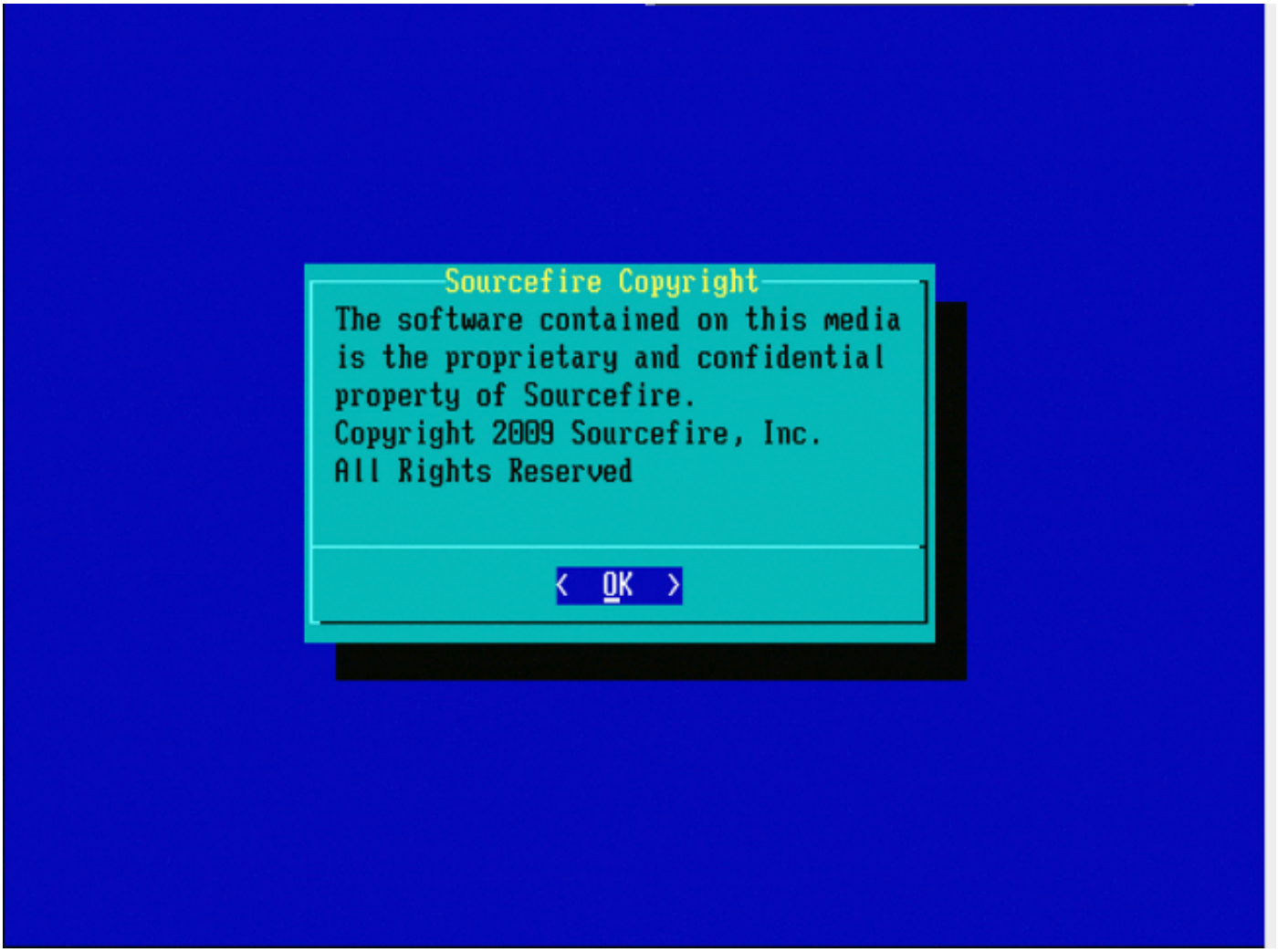


그림 5


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>

그림 6

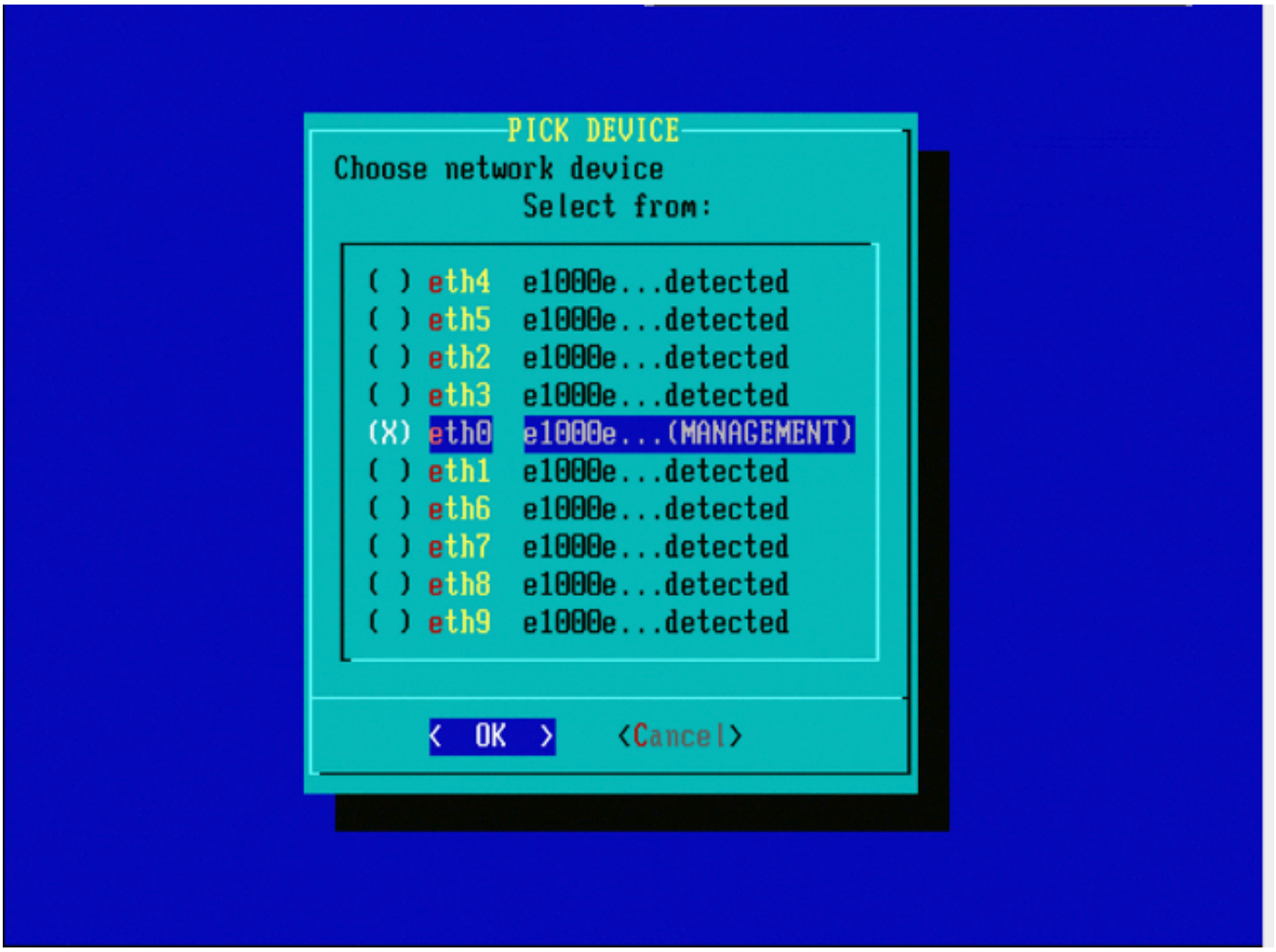


그림 7 - 네트워크 장치를 선택하려면 스페이스바를 누릅니다.

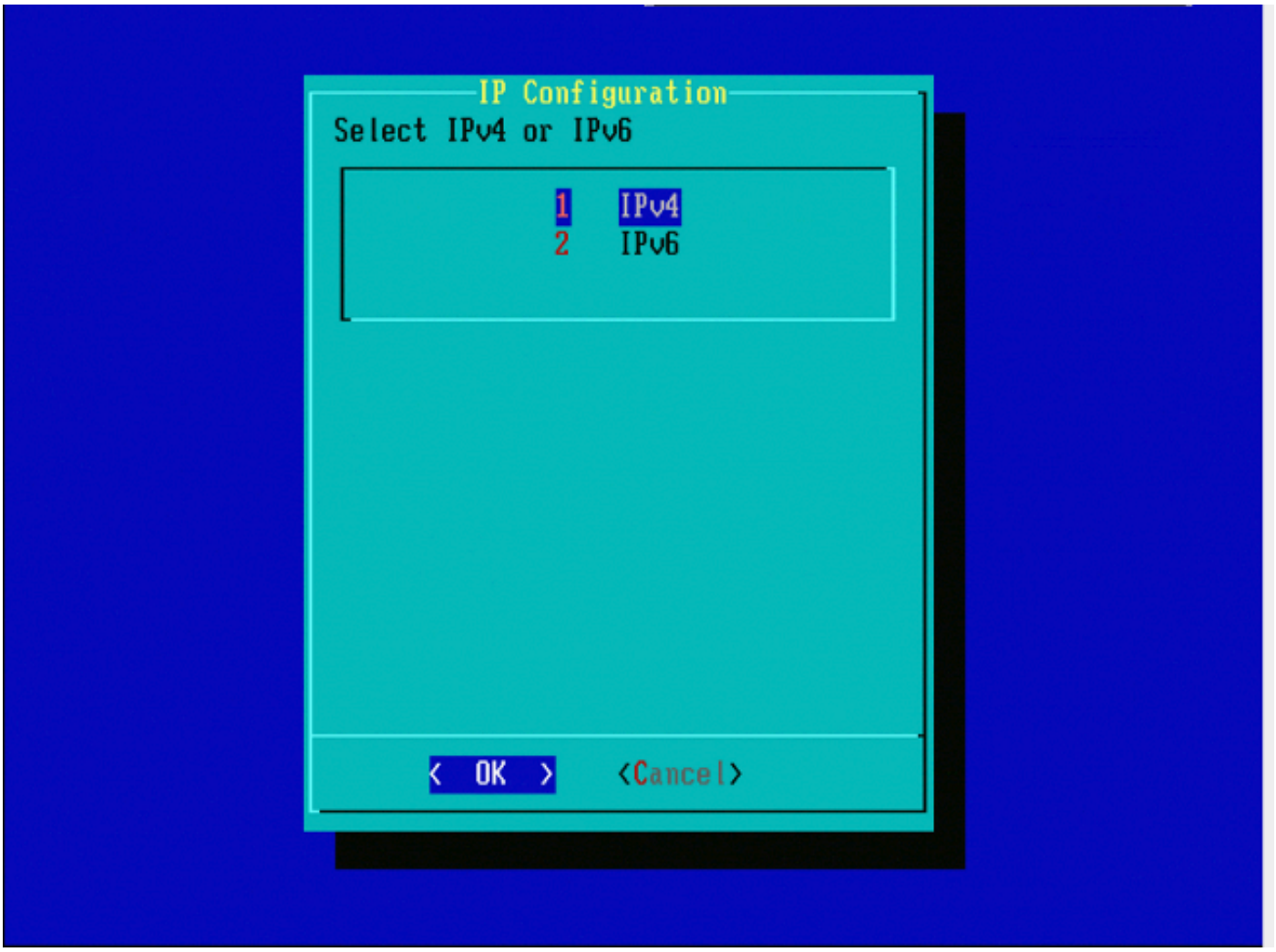


그림 8

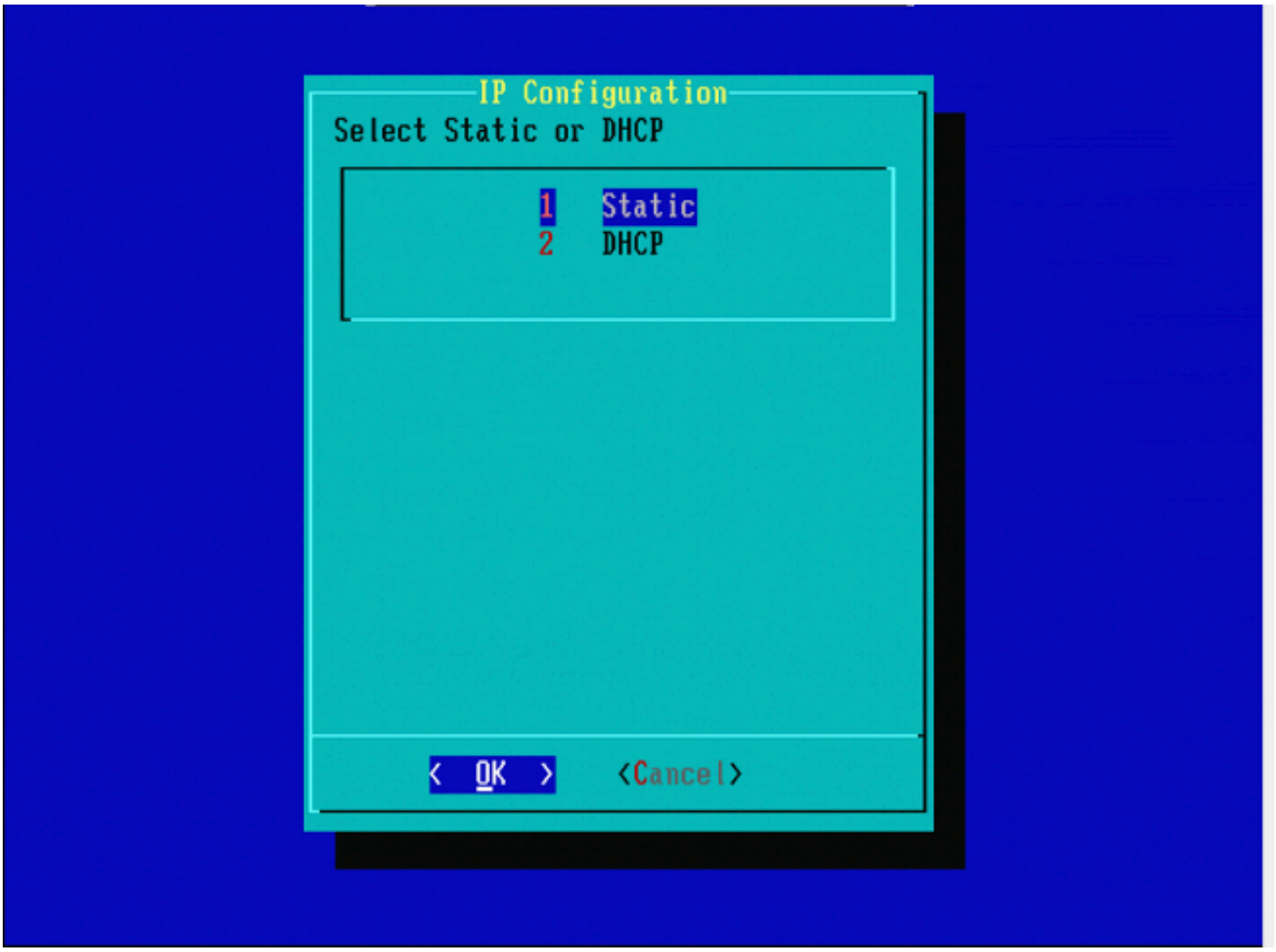

IP Configuration
Select Static or DHCP
1 Static
2 DHCP
< OK >
<Cancel>

그림 9


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

그림 10

그림 11

그림 12


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

그림 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>

그림 14

그림 15 - Cisco Support에서는 SCP(Secure Copy) 프로토콜을 사용할 것을 권장합니다.

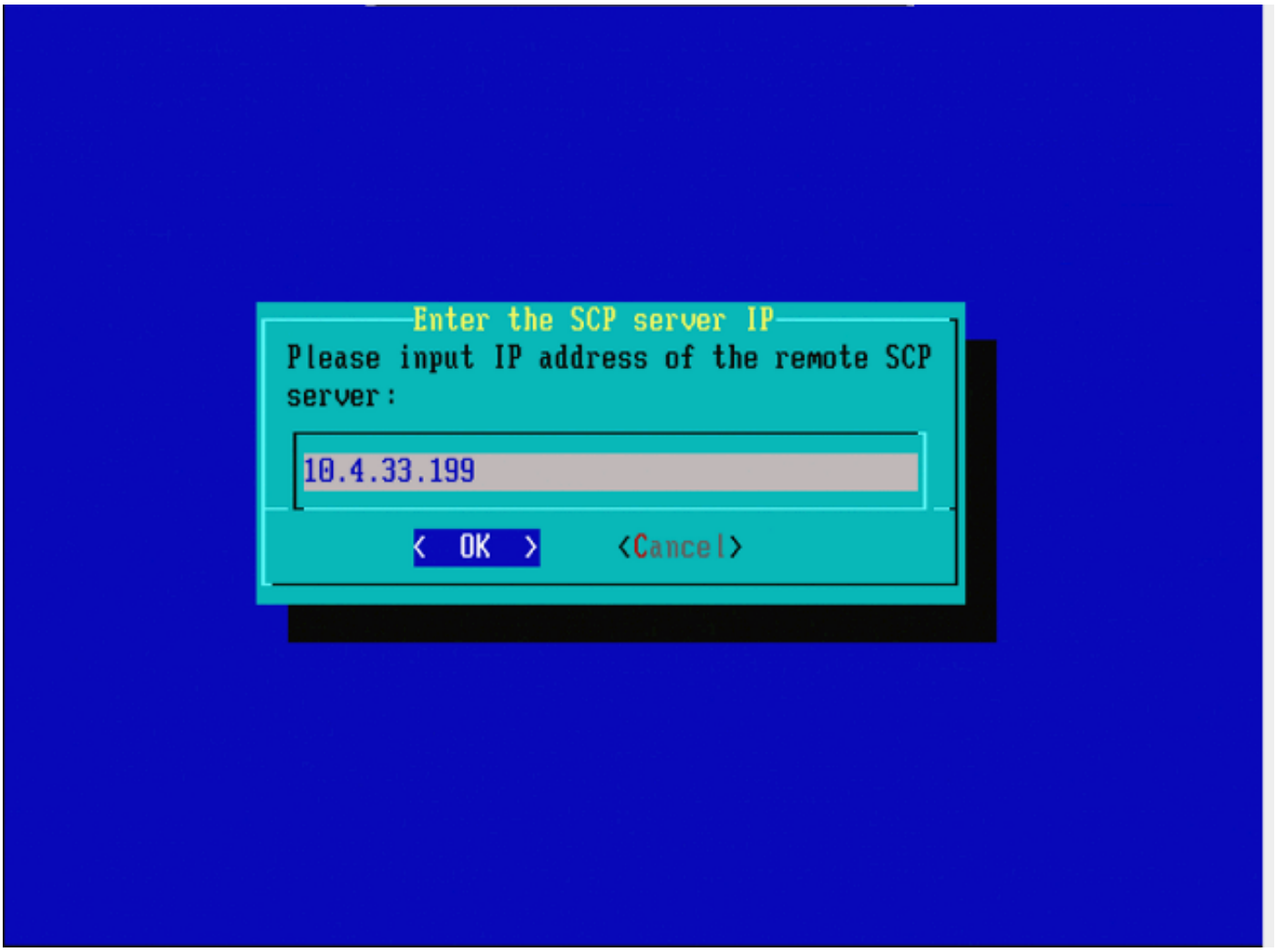


그림 16 - 이 단계의 SCP 서버로 FireSIGHT Management Center를 사용할 수 있습니다. 이 절차를 계속하고 Management Center의 IP 주소 및 자격 증명을 사용하여 System Restore(시스템 복원) 메뉴의 필드를 채웁니다. 추가 세부 정보

SCP(Secure Copy) 서버를 사용하여 파일을 안전하게 전송합니다. 경우 필요한 경우 Sourcefire DC(Defense Center)를 SCP 서버로 사용하여 파일을 다른 Sourcefire 디바이스에 전송할 수 있습니다. 이 기능은 리이미징을 위해 iso 이미지를 Sourcefire 디바이스에 전송해야 하지만 일반 SCP 서버에 연결할 수 없거나 해당 서버를 사용할 수 없는 경우에 유용합니다.

1단계. Sourcefire 지원 포털에서 적절한 .iso 파일을 데스크톱에 다운로드합니다.
2단계. SCP 클라이언트를 사용하여 데스크톱에서 Defense Center로 파일을 복사합니다.

팁: SCP 클라이언트는 일반적으로 Linux 또는 Mac 운영 체제에서 사용할 수 있습니다. 그러나 Windows 운영 체제에서는 서드파티 SCP 클라이언트 소프트웨어를 설치해야 할 수 있습니다. Sourcefire는 특정 SCP 클라이언트 소프트웨어를 설치하기 위한 권장사항이나 지원을 제공하지 않습니다.

다음 예에서는 Linux 시스템의 Downloads 디렉토리에서 Sourcefire Defense Center의 /var/tmpdirectory로 Sourcefire .iso 이미지 파일을 복사하는 방법을 보여 줍니다.

<#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
```

⚠ 주의: .iso 파일의 이름을 변경하지 마십시오. 이미지로 다시 설치하는 동안 파일 탐지에 문제가 발생할 수 있습니다.

이제 파일이 Defense Center로 복사됩니다. Sourcefire 디바이스의 재이미지화 프로세스를 진행할 수 있습니다. 필요한 경우 이미지로 다시 설치할 때 DC의 IP 주소와 사용자 이름 및 이전 지침과 함께 이미지 파일을 복사한 경로를 제공할 수 있습니다.

⚠ 경고: 디스크 공간의 사용률을 낮추려면 이미지로 다시 설치한 후 Defense Center의 /var/tmp 디렉토리에서 .iso 파일을 제거해야 합니다.

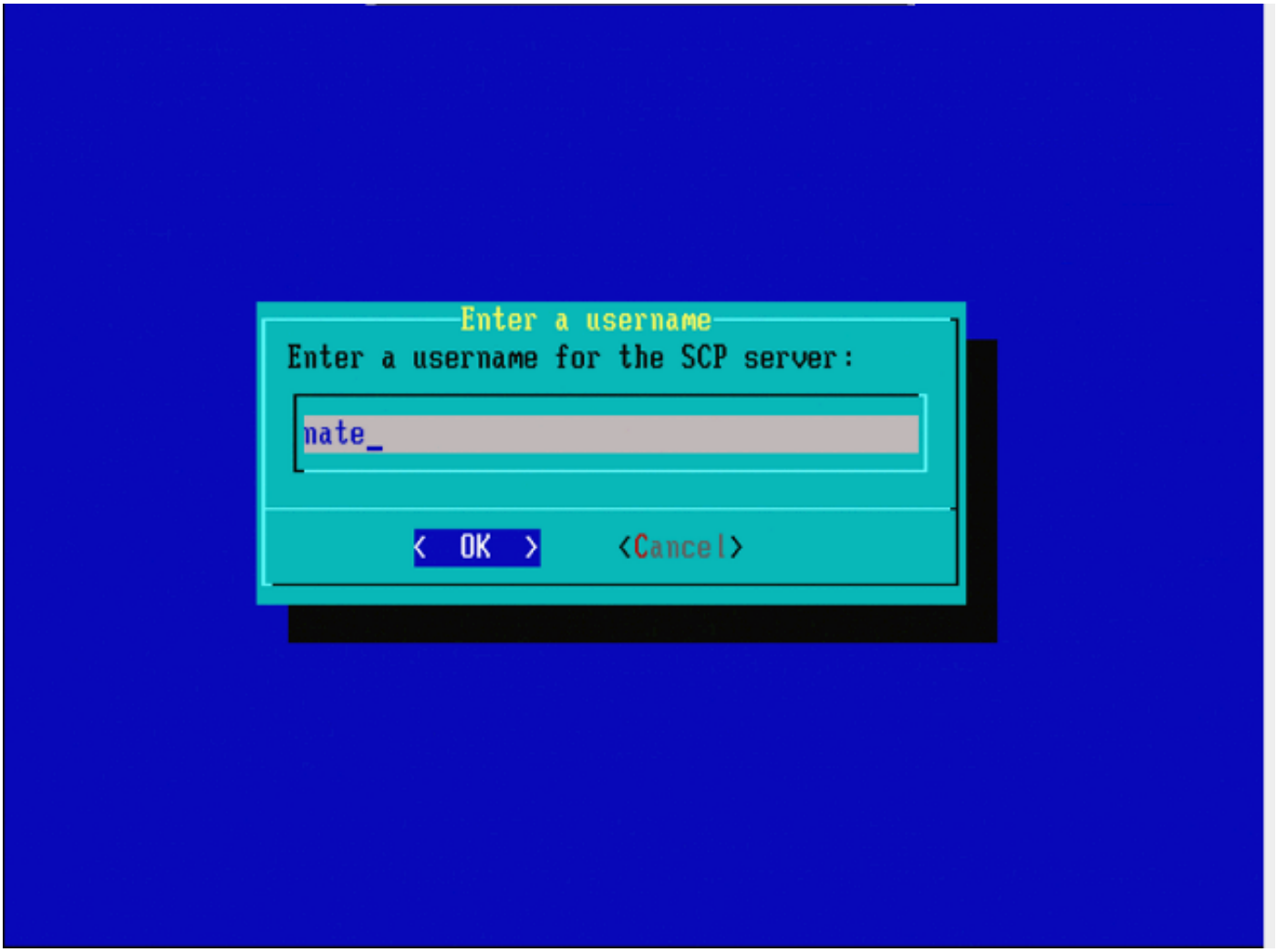


그림 17

그림 18

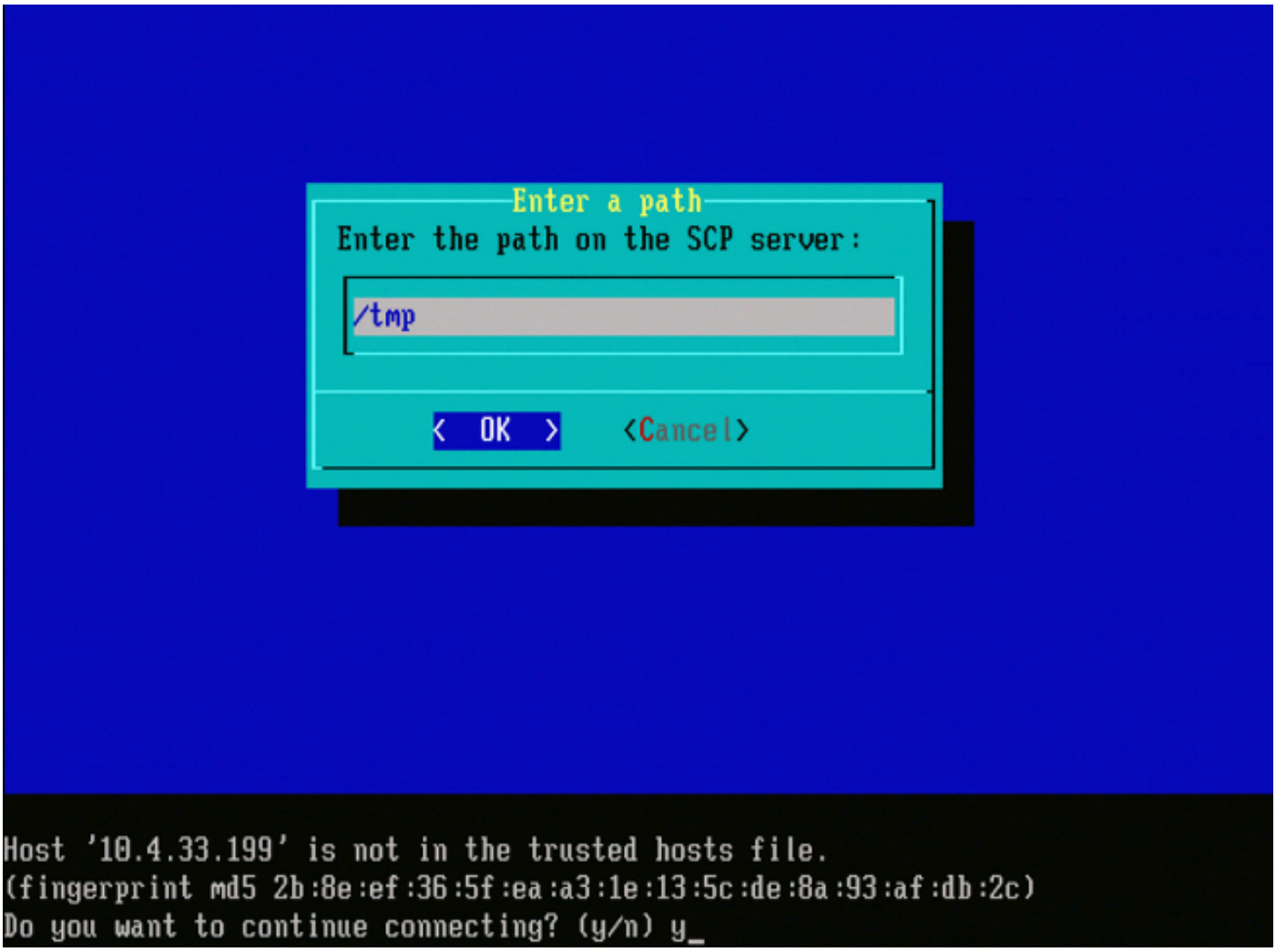


그림 19

참고: 이 시점에서 예상 메시지 대신 연결 오류가 발생하면 SSH 서버에 대한 연결을 확인하십시오.

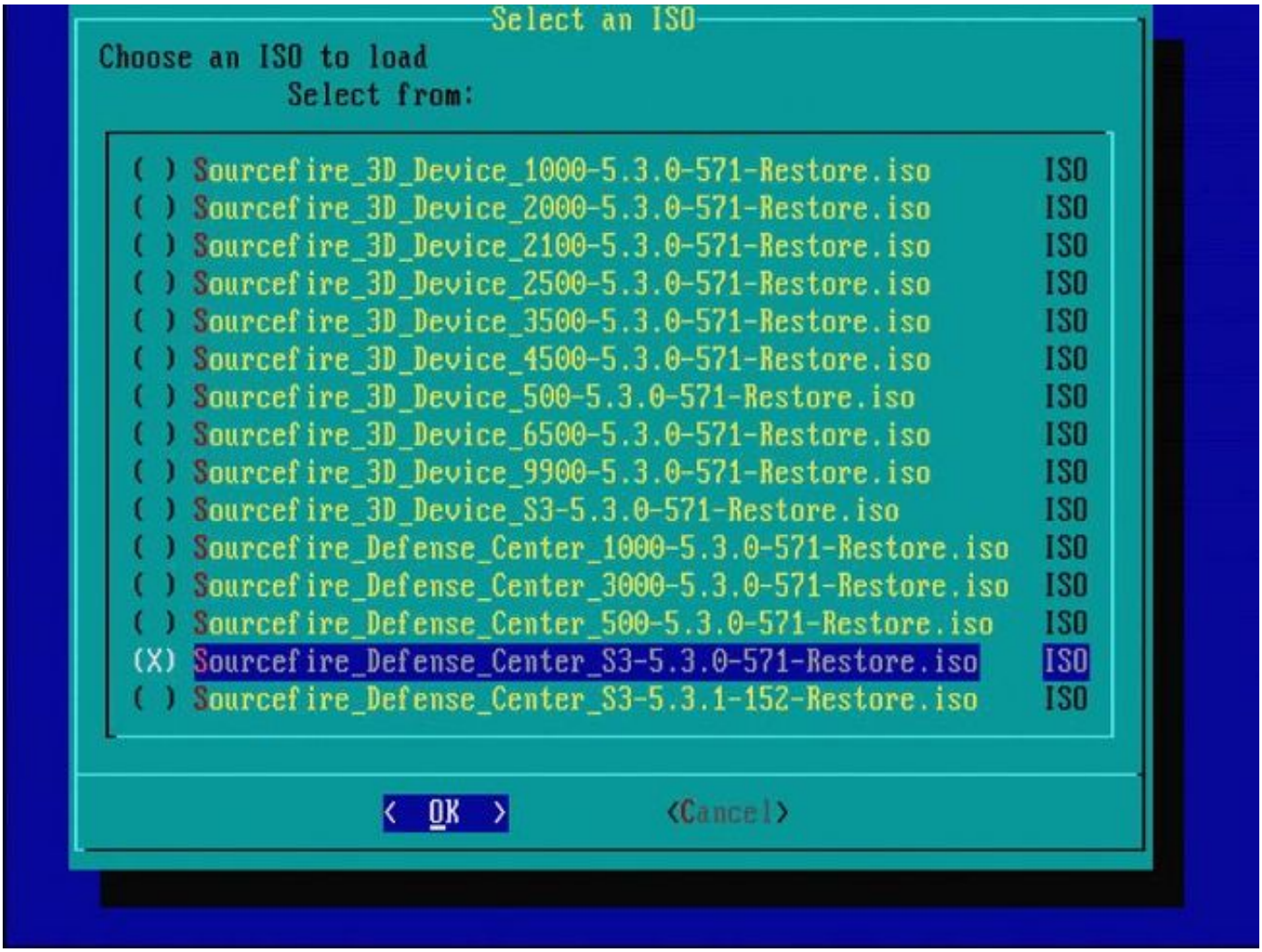


그림 20 - .iso 이미지를 선택하려면 스페이스바를 누릅니다.

참고: .iso 파일에 대한 기본 파일 이름을 사용해야 합니다. 그렇지 않으면 이 단계에서 파일이 감지되지 않을 수 있습니다.
오류: ISO 이미지가 없습니다.
버전 6.3에서 ISO 이름 규칙이 Sourcefire_3D_Device_S3-<ver>-<build>-Restore.iso에서 Cisco_Firepower_NGIPS_Appliance-<ver>-<build>-Restore.iso로 변경되었습니다. "ISO 이미지를 찾을 수 없음"이 표시되면 ISO 파일의 이름을 레거시 파일 이름으로 바꿉니다. 일반적으로 6.2.x 이전 버전을 6.3.0 이상 버전으로 이미지로 다시 설치하는 경우 이 문제가 발생합니다.

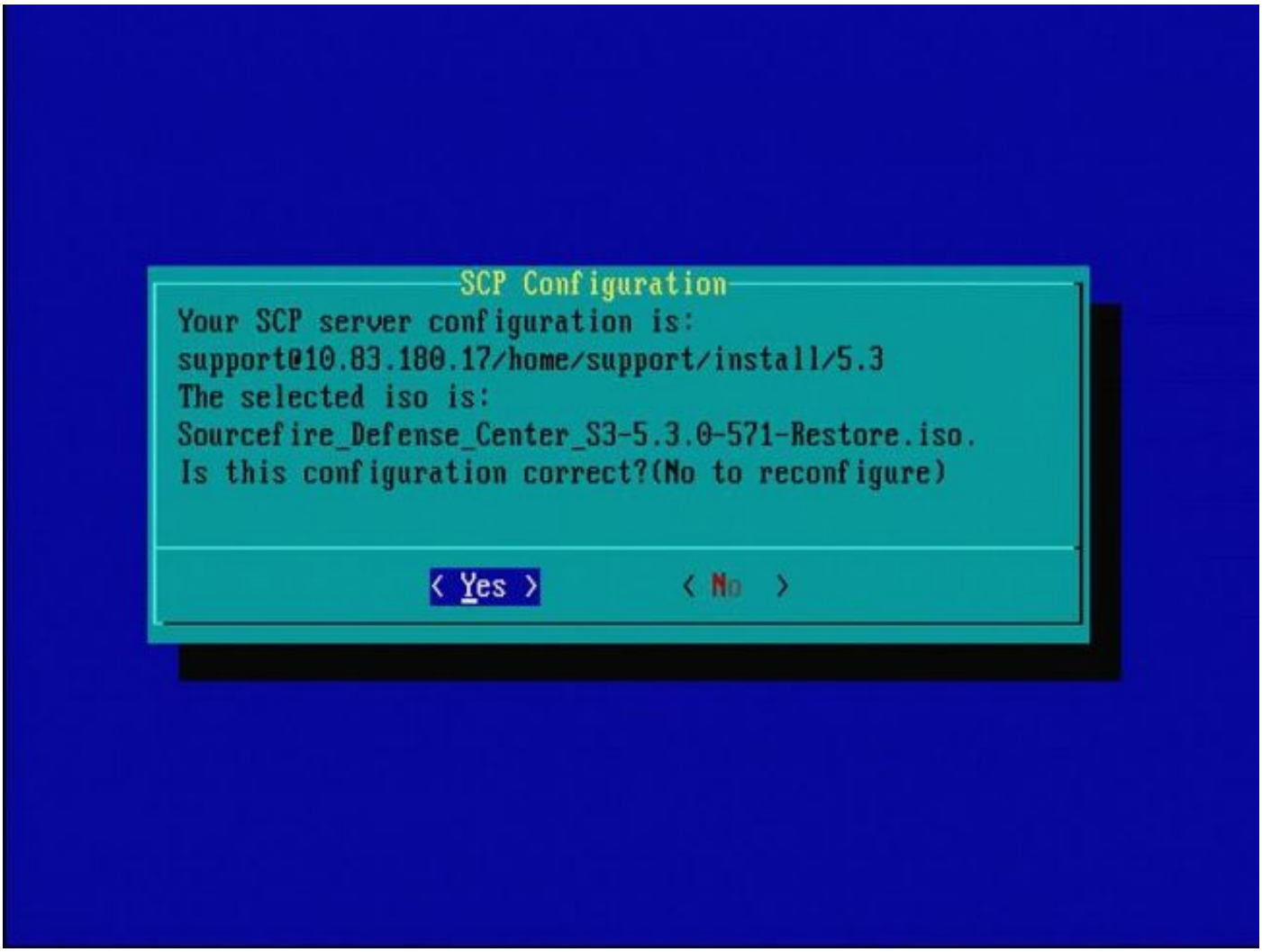

SCP Configuration
Your SCP server configuration is:
support@10.83.180.17/home/support/install/5.3
The selected iso is:
Sourcefire_Defense_Center_S3-5.3.0-571-Restore.iso.
Is this configuration correct?(No to reconfigure)
< Yes >
< No >

그림 21

그림 22 - Cisco Support에서는 이 프로세스의 3단계를 건너뛸 것을 권장합니다. 패치 및 SRU(Snort Rule Update)는 리이미지 작업이 완료된 후 설치할 수 있습니다.

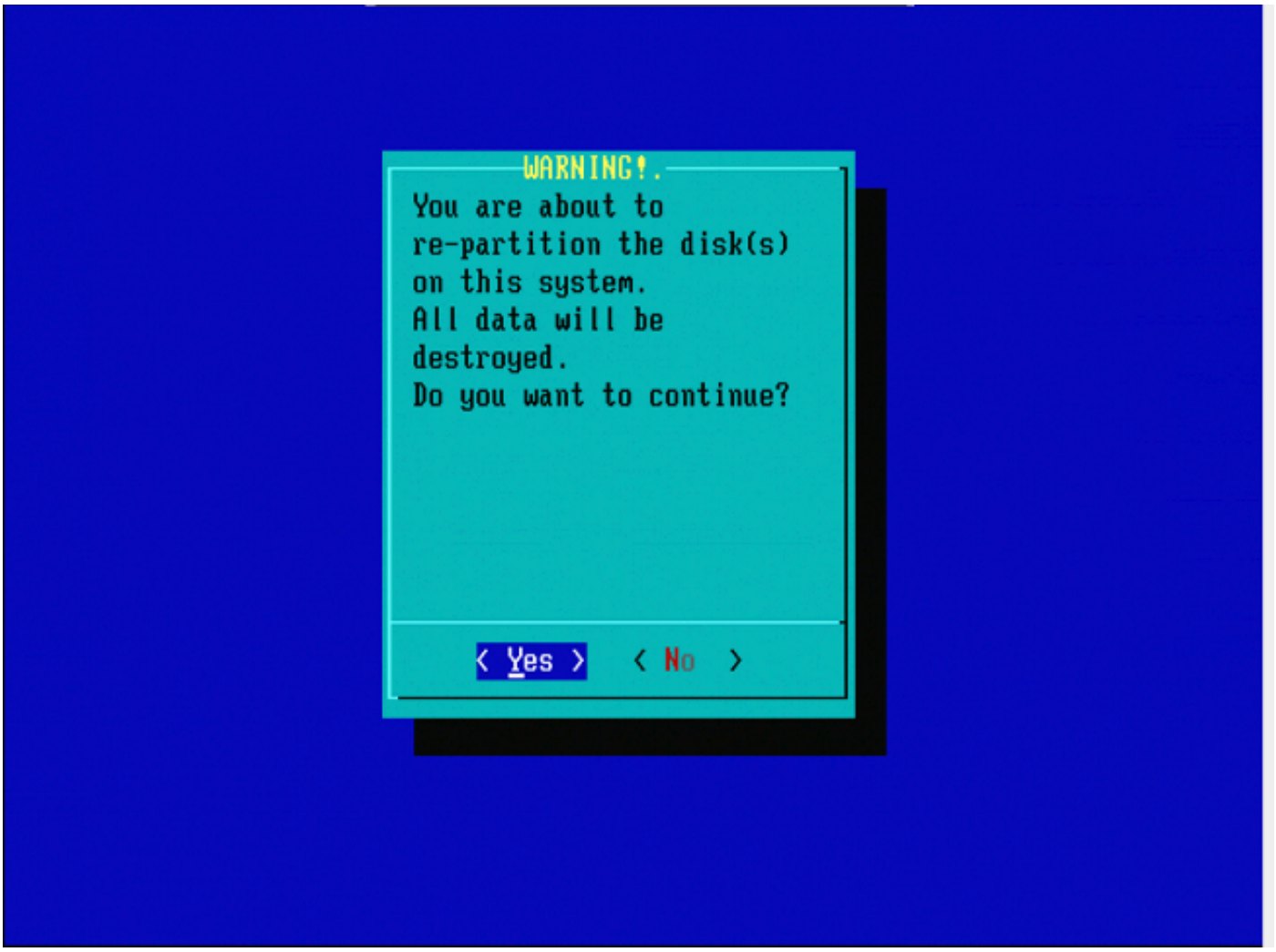
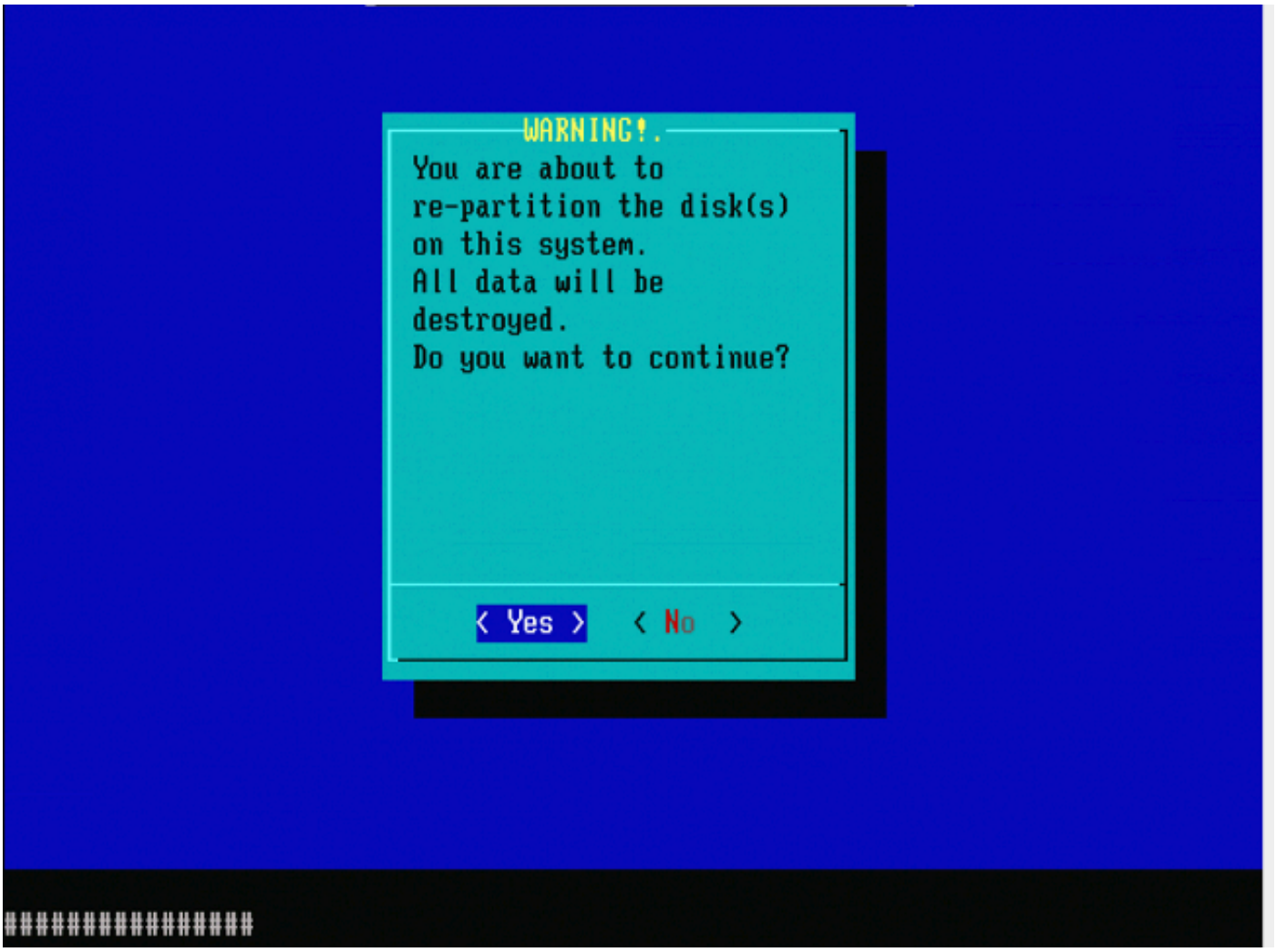

WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >

그림 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 >
##################
그림 24

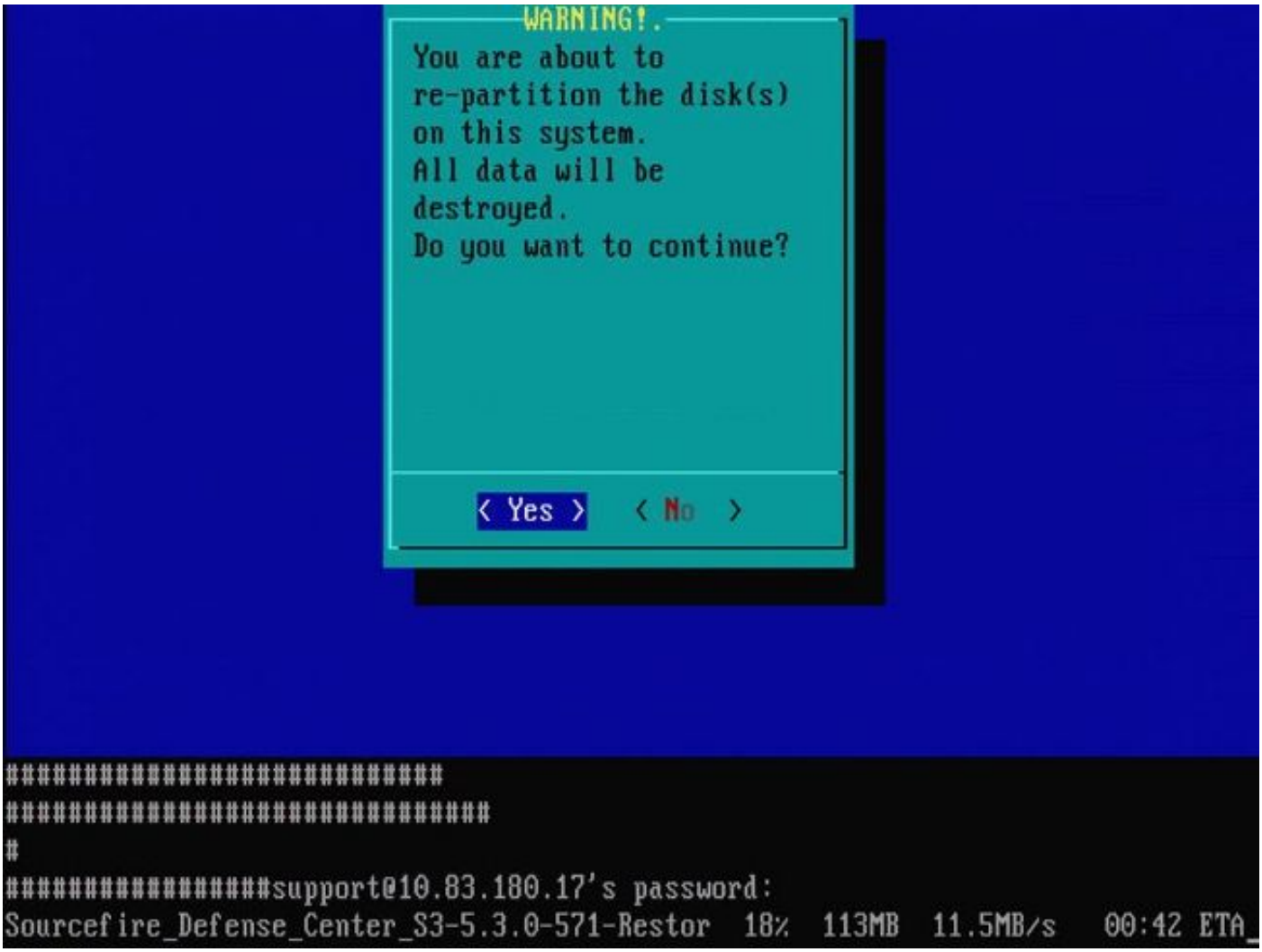

WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >
##############################
##################################
#
##################support@10.83.180.17's password:
Sourcefire_Defense_Center_S3-5.3.0-571-Restor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

그림 25

그림 26

다른 주요 소프트웨어 버전의 이미지로 다시 설치하는 것과 관련된 중요 참고 사항: 5.1 > 5.2, 5.2 > 5.3, 5.3 > 5.2 등을 이미지로 다시 설치하는 경우와 같이 이전에 다른 주요 소프트웨어 버전을 실행한 디바이스를 다시 이미지화하려는 경우 그림 1 - 26에 나와 있는 단계를 두 번 완료해야 합니다.

1. 이미지 26과 같이 프롬프트에서 OK를 선택하면 System Restore 파티션이 새 버전으로 깜박이며 어플라이언스가 재부팅됩니다.
2. 재부팅 후 처음부터 다시 이미지로 다시 설치 프로세스를 시작하고 그림 27b ~ 31에 나와 있는 프로세스를 계속 진행해야 합니다.

다른 주요 소프트웨어 버전으로부터의 첫 번째 리이미지인 경우, 이미지 27a, 그림 31 및 32와 같은 화면이 표시됩니다.

⚠ 주의: 이 화면이 표시되면 "하드웨어 확인" 후 "USB 장치..." 전에 출력이 표시되지 않을 수 있습니다. 지금 아무 키나 누르지 마십시오. 그렇지 않으면 디바이스가 사용할 수 없는 상태로 재부팅되어 다시 이미징해야 합니다.

그렇지 않은 경우 그림 27b에서 그림 32의 화면을 볼 수 있습니다.

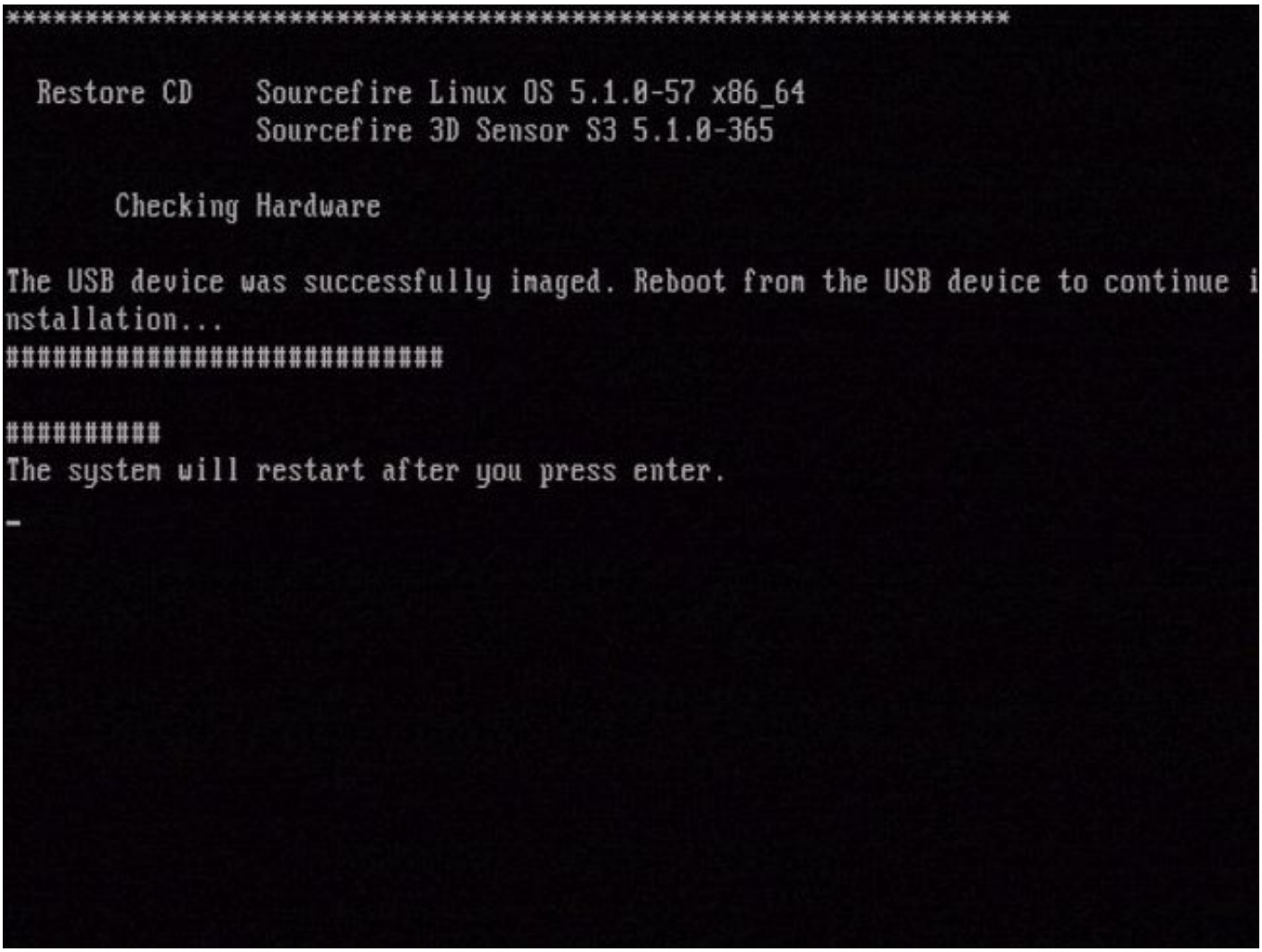


그림 27a

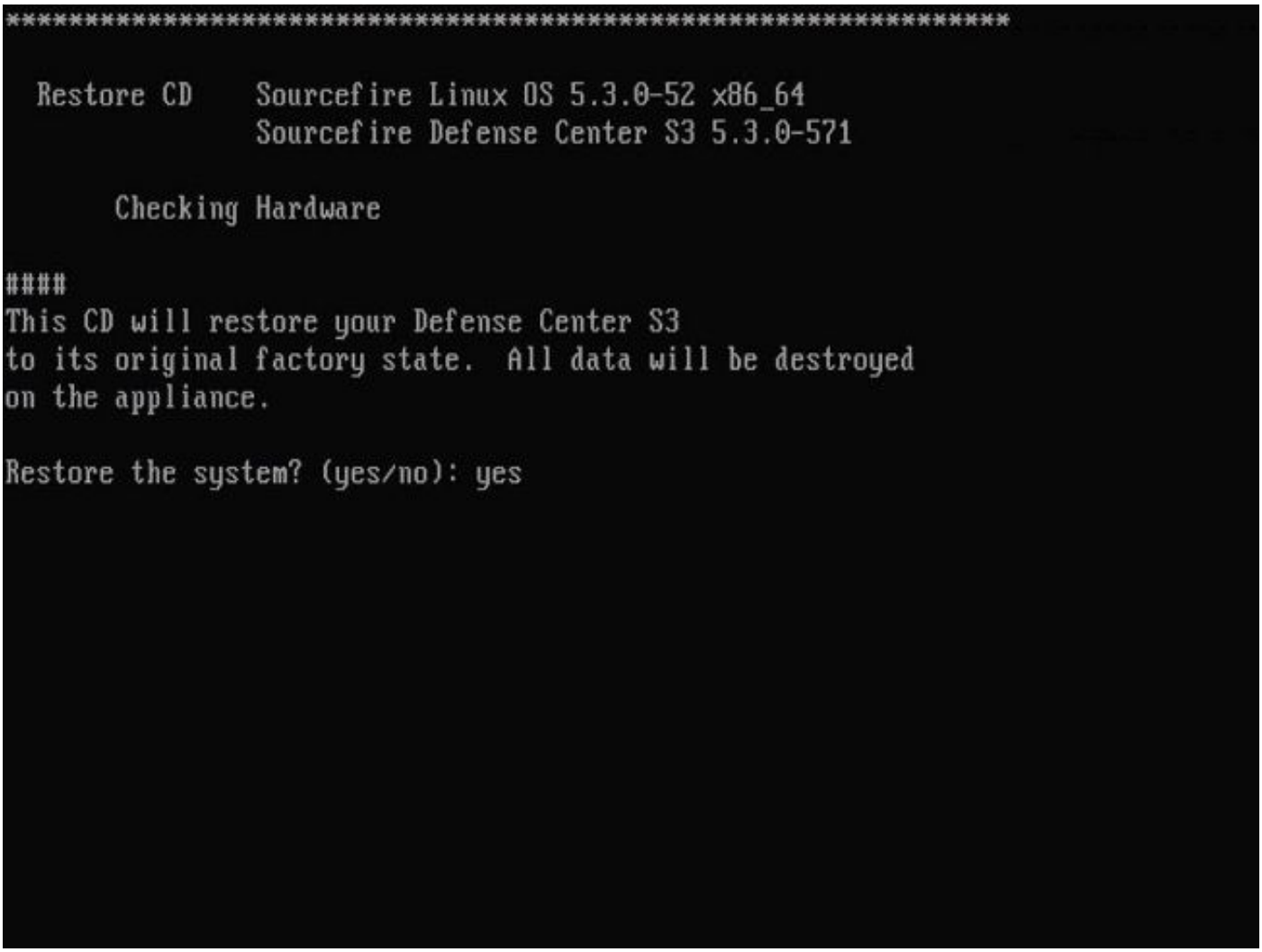

****
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes

그림 27b

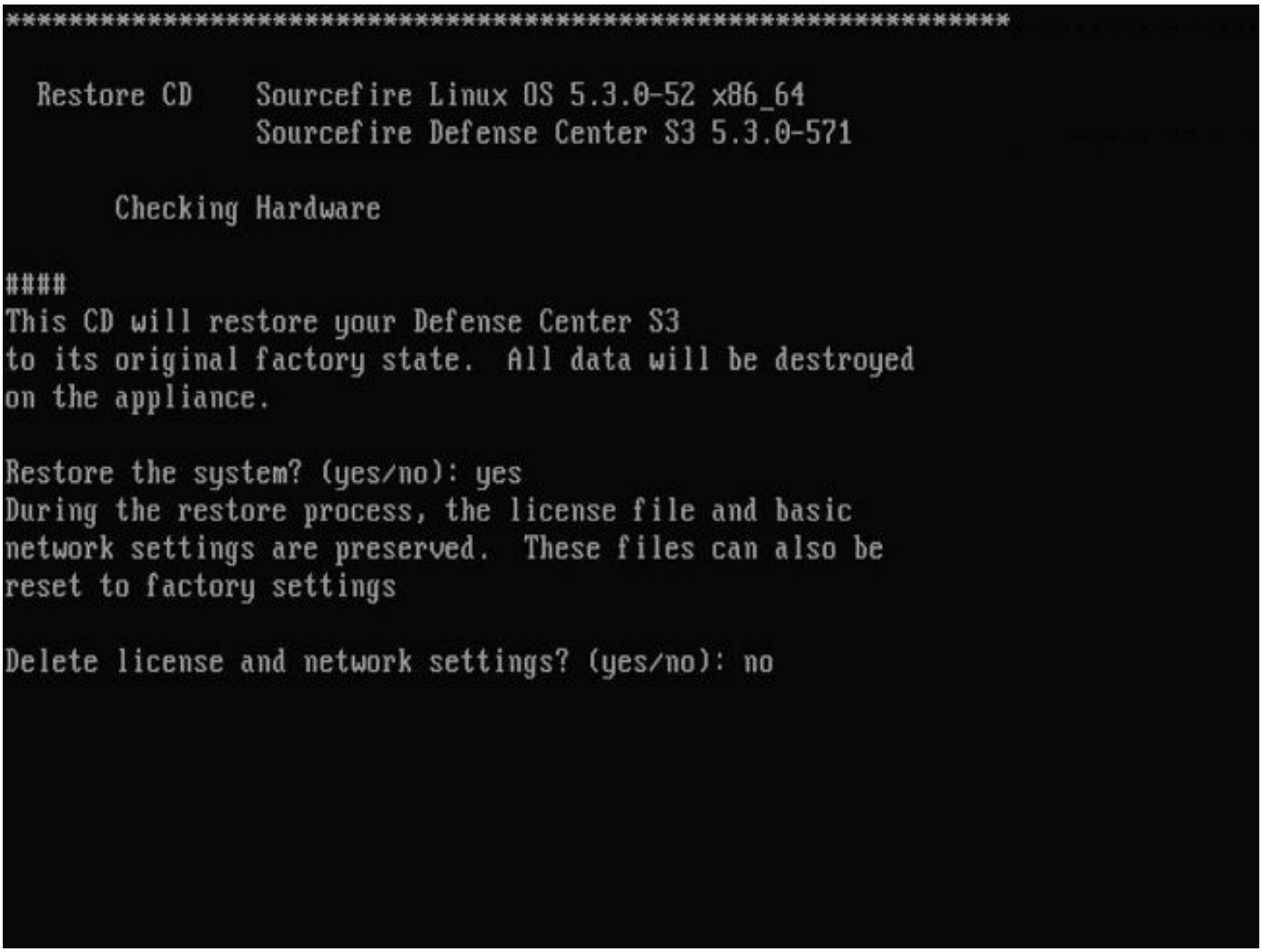
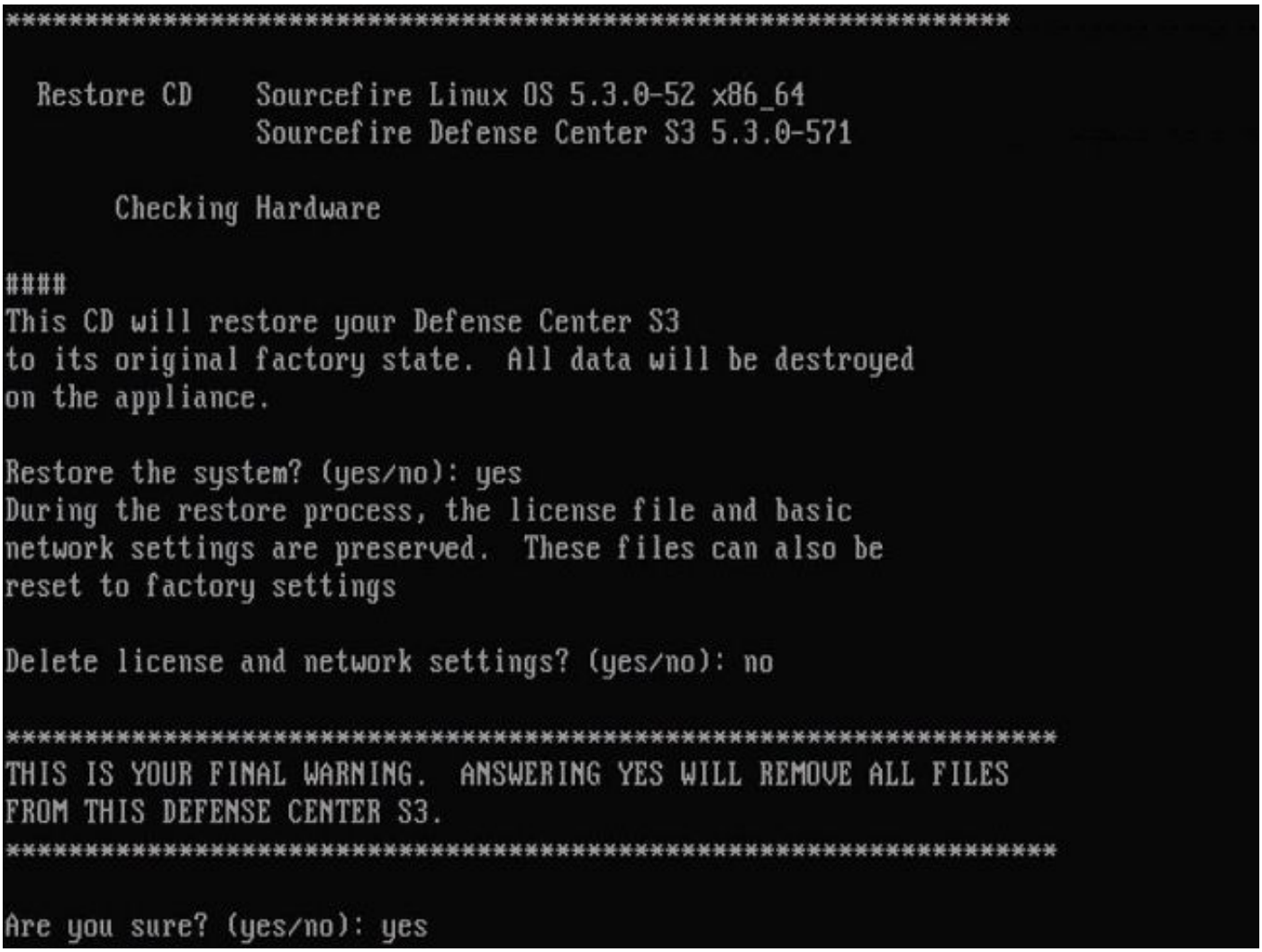

****
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes
During the restore process, the license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

그림 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
그림 29

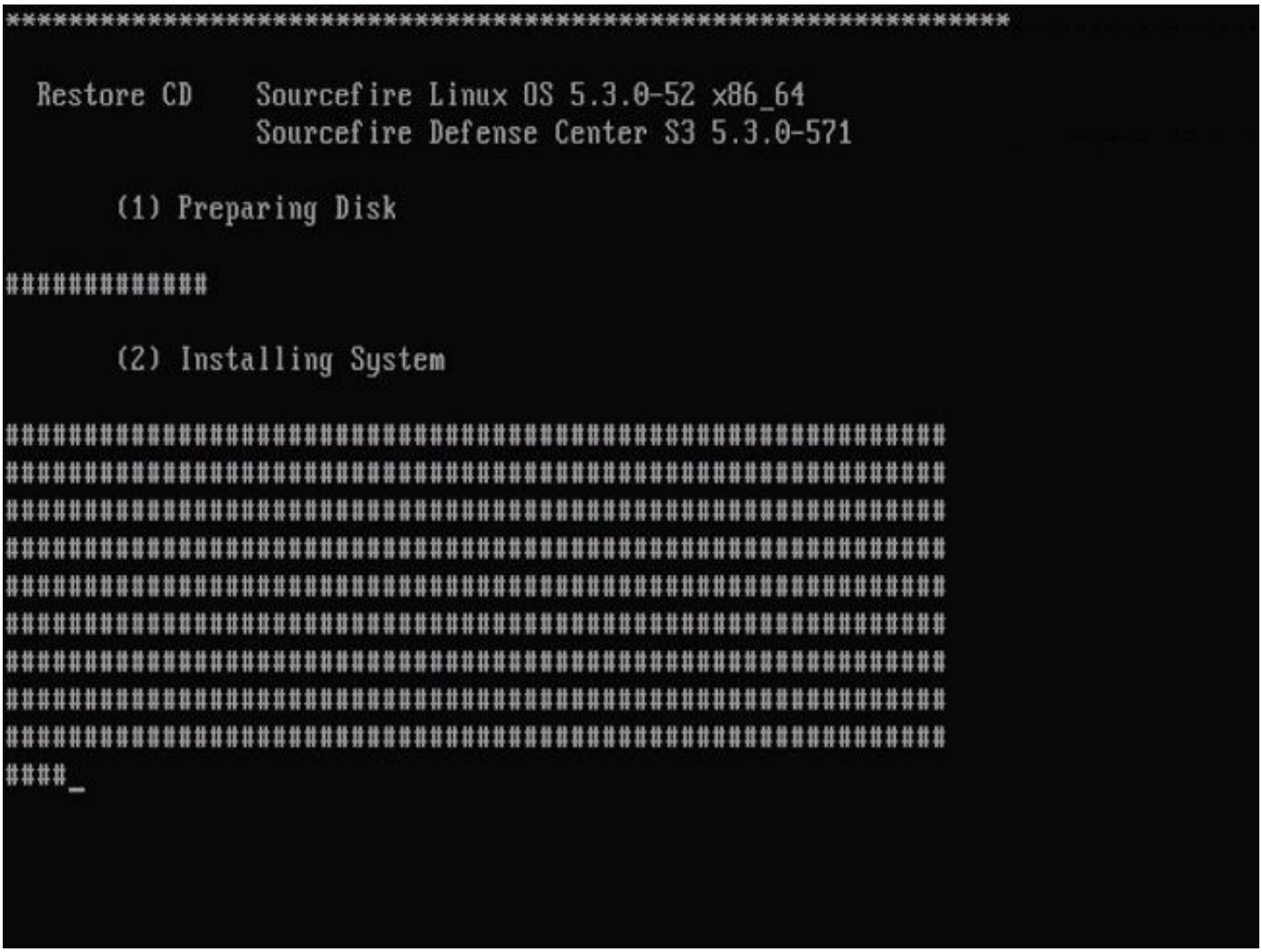

Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
(1) Preparing Disk
(2) Installing System

그림 30

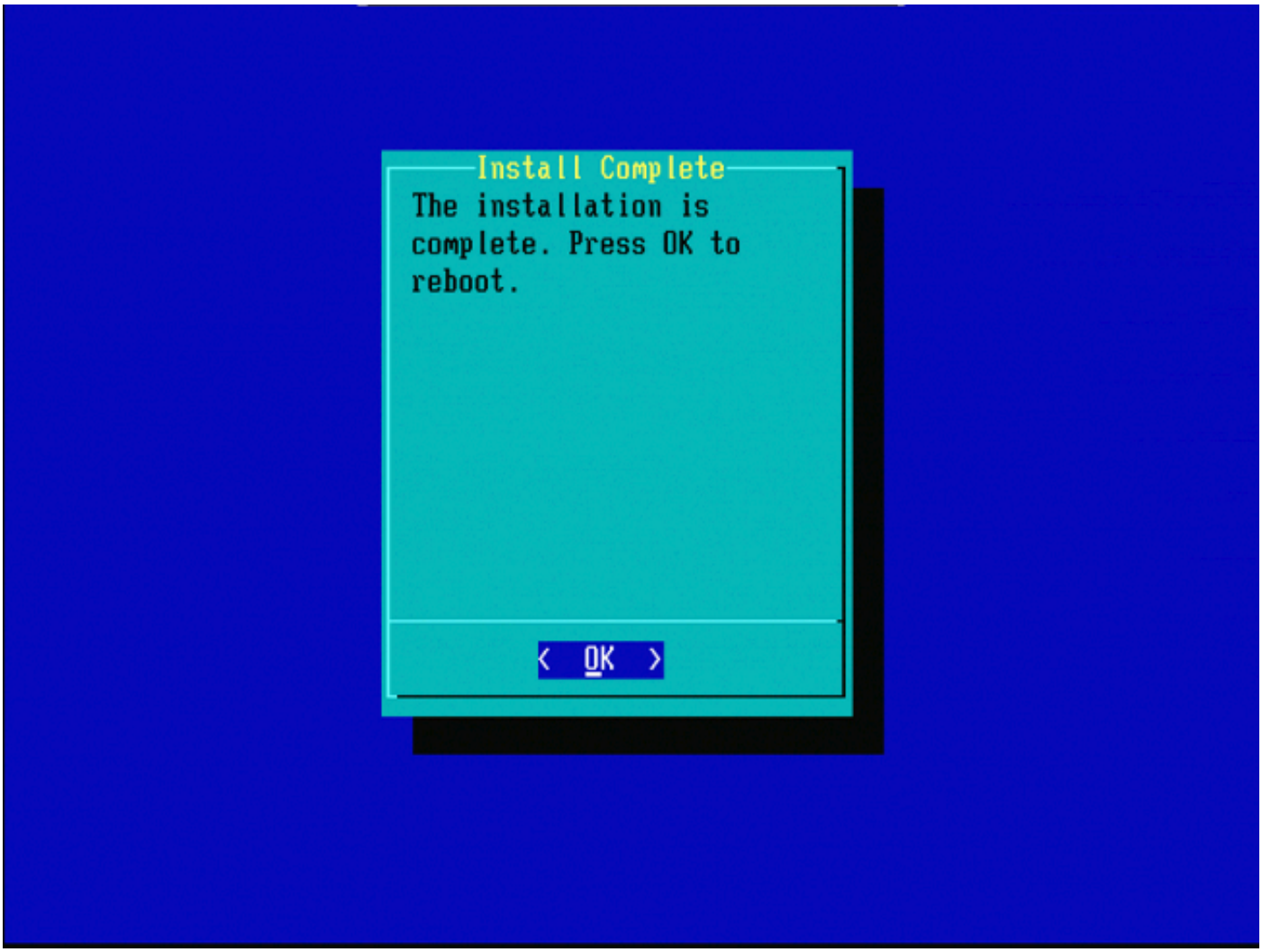

Install Complete
The installation is
complete. Press OK to
reboot.
< OK >

그림 31

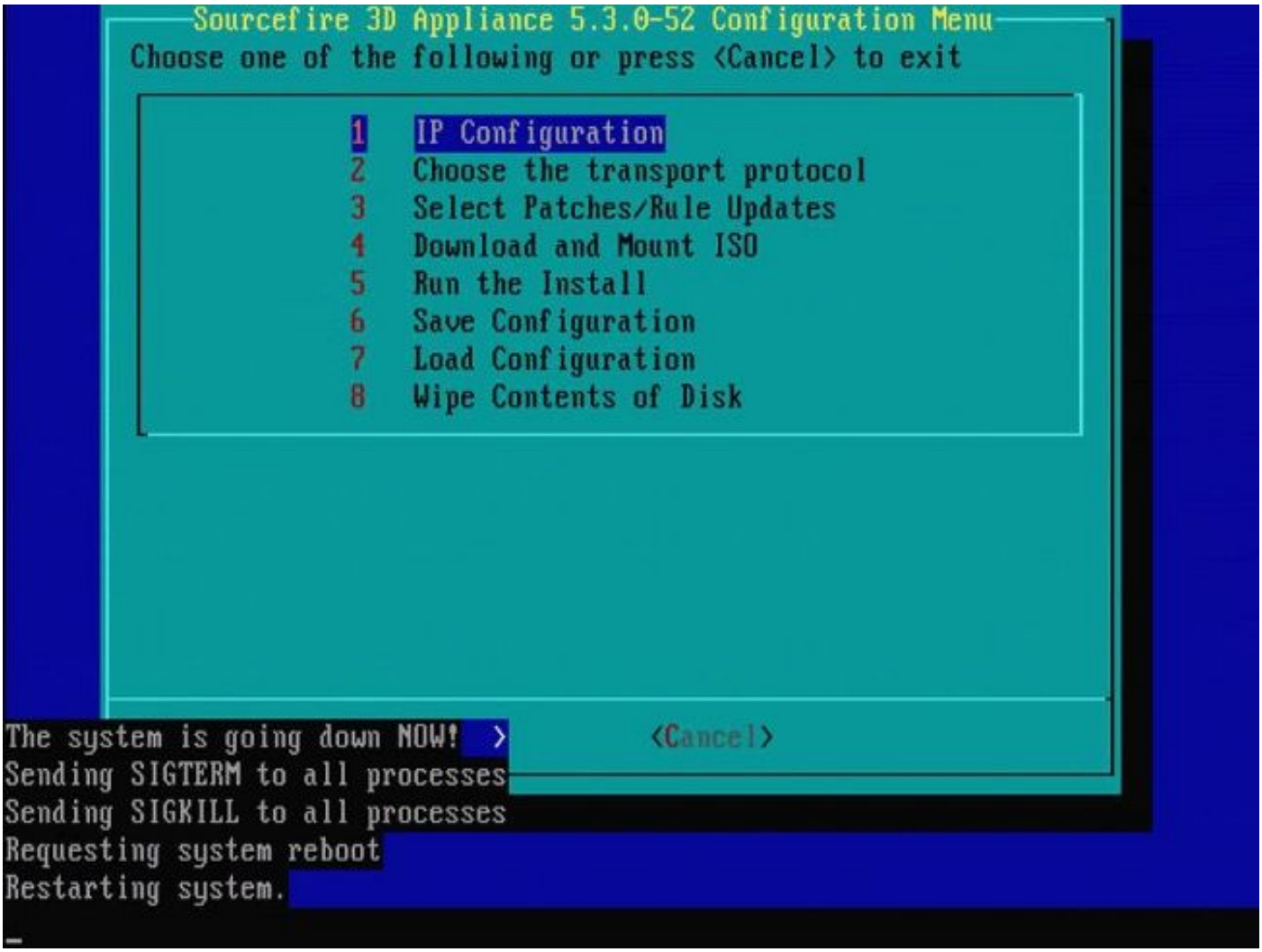


그림 32

Cisco Firepower Management Center 1000, 2500 및 4500

FMC 1000, 2500 및 4500에서는 옵션이 서로 다릅니다. KVM 스위치 또는 CIMC를 사용하면 디바이스가 시작될 때 다음 옵션이 표시됩니다.

1 - Cisco Firepower Management Console VGA 모드

2 - Cisco Firepower Management Console 시리얼

3 - Cisco Firepower Management Console 시스템 복원 모드

4 - Cisco Firepower Management Console 비밀번호 복원 모드

UI를 사용하여 복원 모드를 시작하려면 'Cisco Firepower Management Console 시스템 복원 모드'(옵션 3)와 'Cisco Firepower Management Console 시스템 복원 VGA 모드'(옵션 1)를 차례로 선택합니다

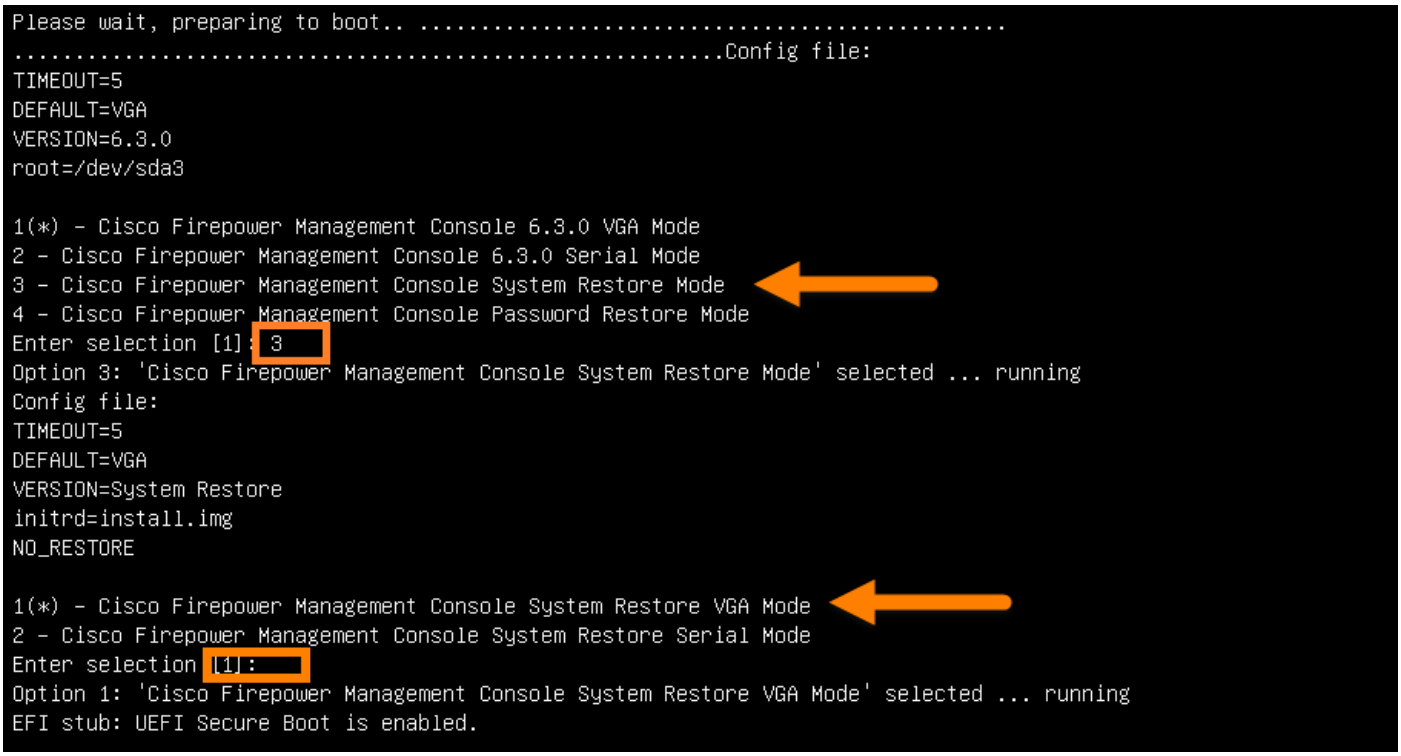


그림 33

나머지 프로세스는 다른 FMC 어플라이언스와 동일합니다.

문제 해결

System_Restore LILO 메뉴 옵션이 나열되지 않음

FireSIGHT Management Center 및 Firepower 7000 및 8000 Series 어플라이언스에는 리이미지 시스템이 포함된 통합 플래시 드라이브가 있습니다. "System_Restore" 옵션이 LILO(Linux Loader) 부팅 메뉴에 나열되지 않으면 이 드라이브에 액세스하여 리이미지를 완료할 수 있습니다.

7010, 7020 및 7030 디바이스

70XX 시리즈 디바이스를 사용하는 경우 부팅 디바이스를 선택하려면 다음 단계를 완료하십시오.

1. 어플라이언스의 전원을 안전하게 끕니다.

2. 부팅 디바이스 선택 화면에 액세스하기 위해 어플라이언스 전원을 켜고 어플라이언스가 부팅되는 동안 Delete 키를 반복해서 누릅니다. 다음 위치에서 이미지를 참조하십시오.

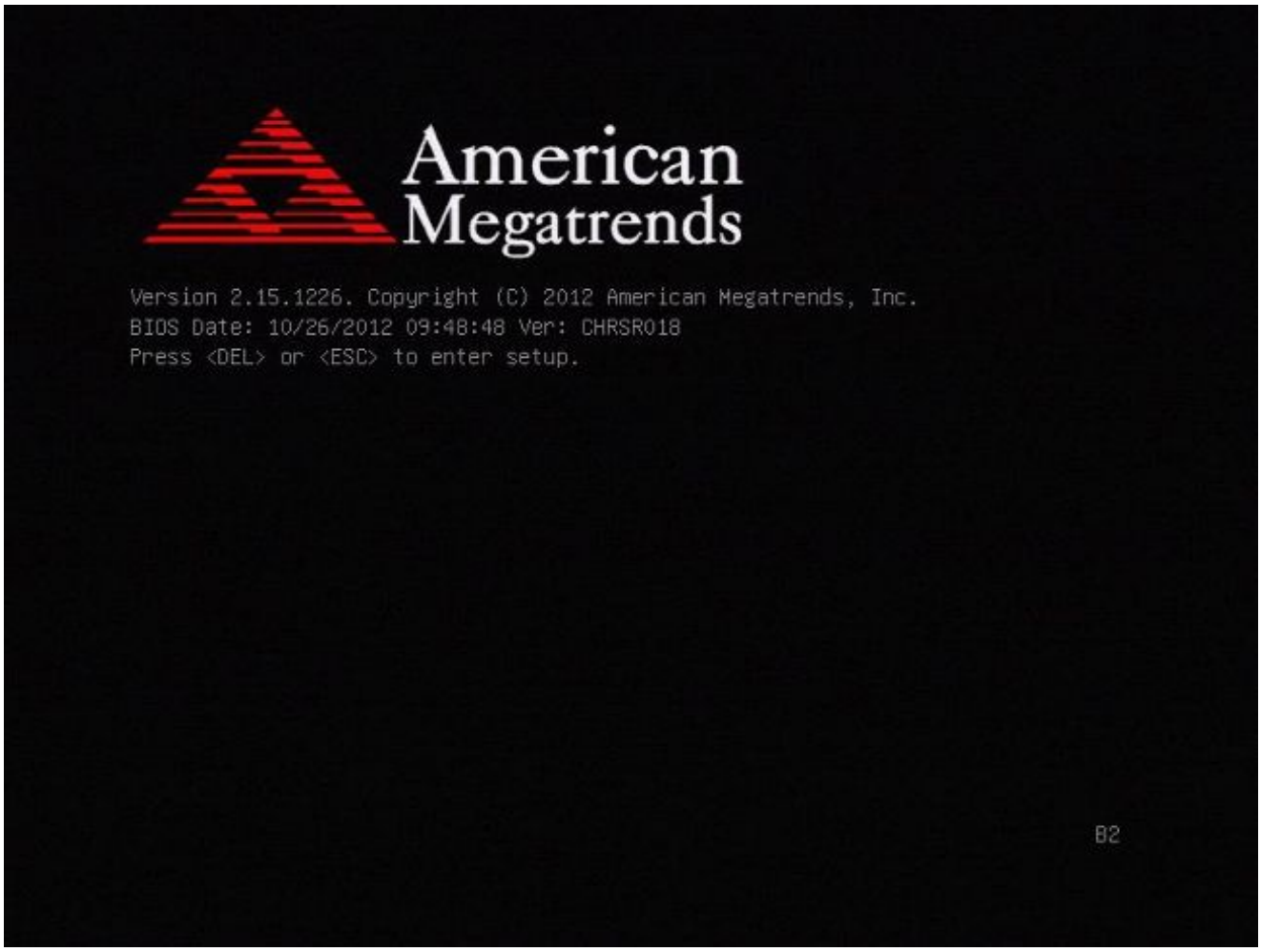

American
Megatrends
Version 2.15.1226. Copyright (C) 2012 American Megatrends, Inc.
BIOS Date: 10/26/2012 09:48:48 Ver: CHRSR018
Press <DEL> or <ESC> to enter setup.
B2

그림 A1

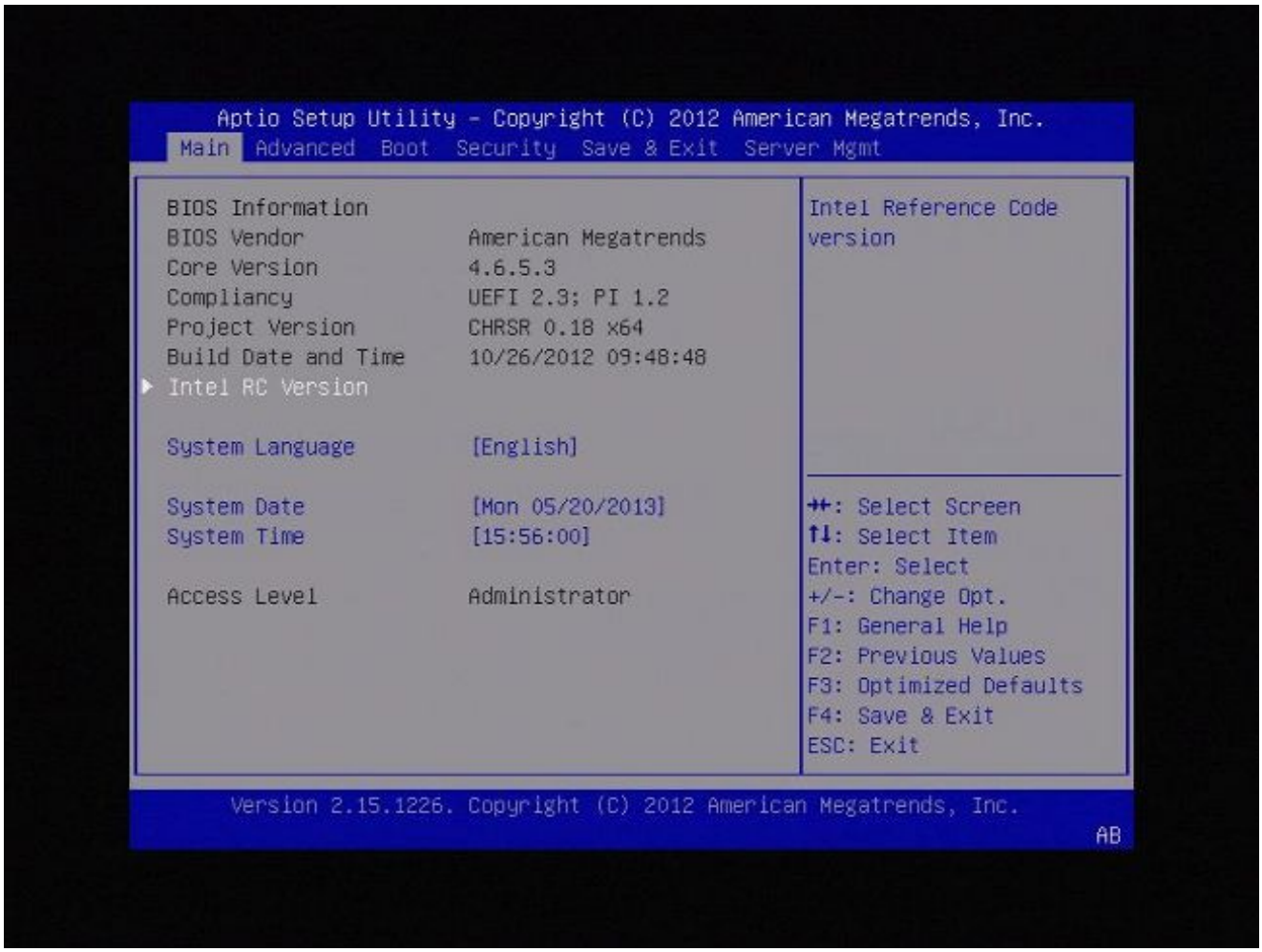


그림 A2

3. Save & Exit 탭을 선택하려면 오른쪽 화살표 키를 사용합니다. 이 탭에서 아래쪽 화살표 키를 사용하여 SATA SM: InnoDisk를 선택합니다. - InnoLite를 누르고 Enter 키를 누릅니다.

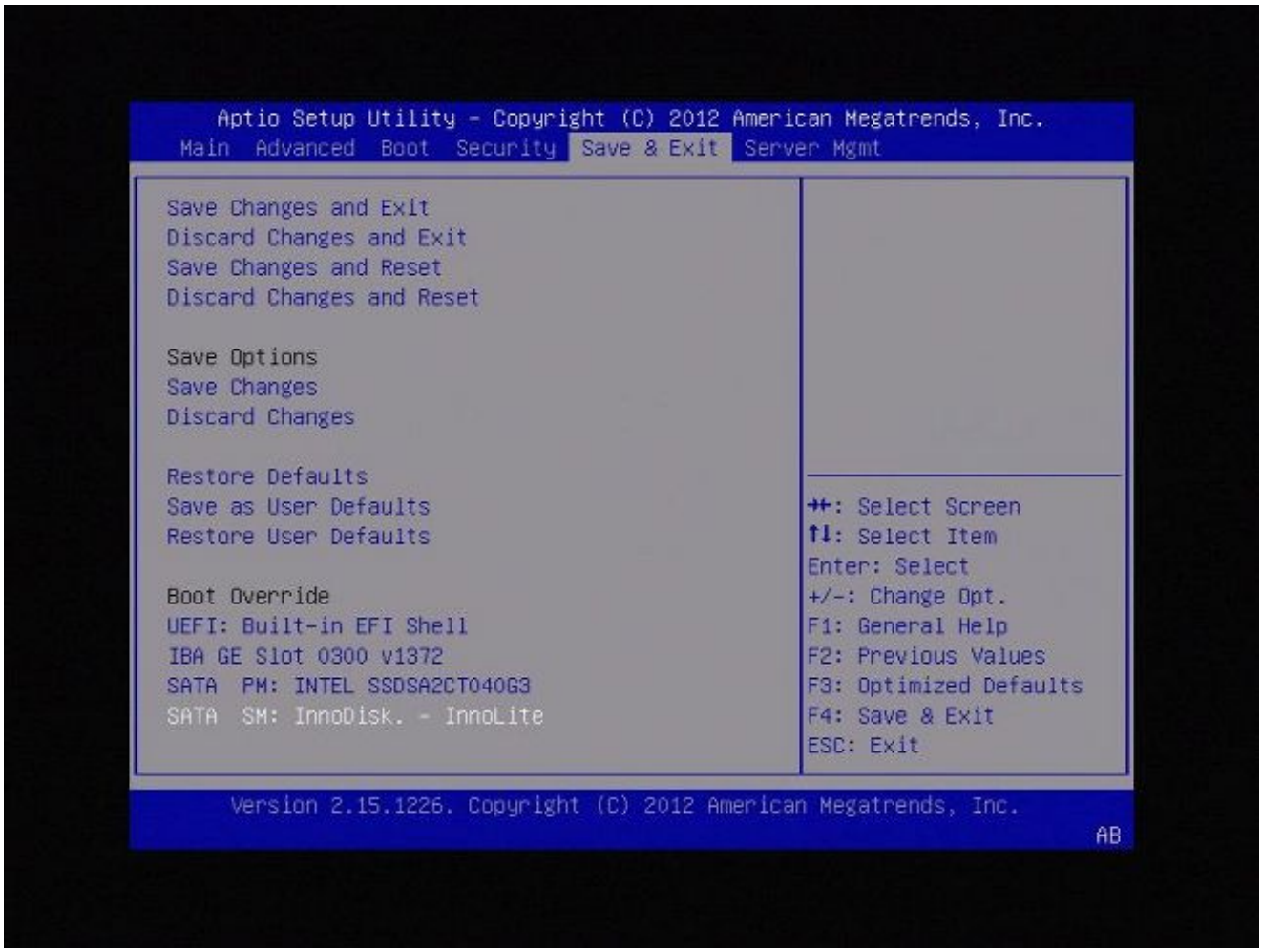


그림 A3

4. 키보드와 모니터를 사용하는 경우 옵션 0을 선택합니다.

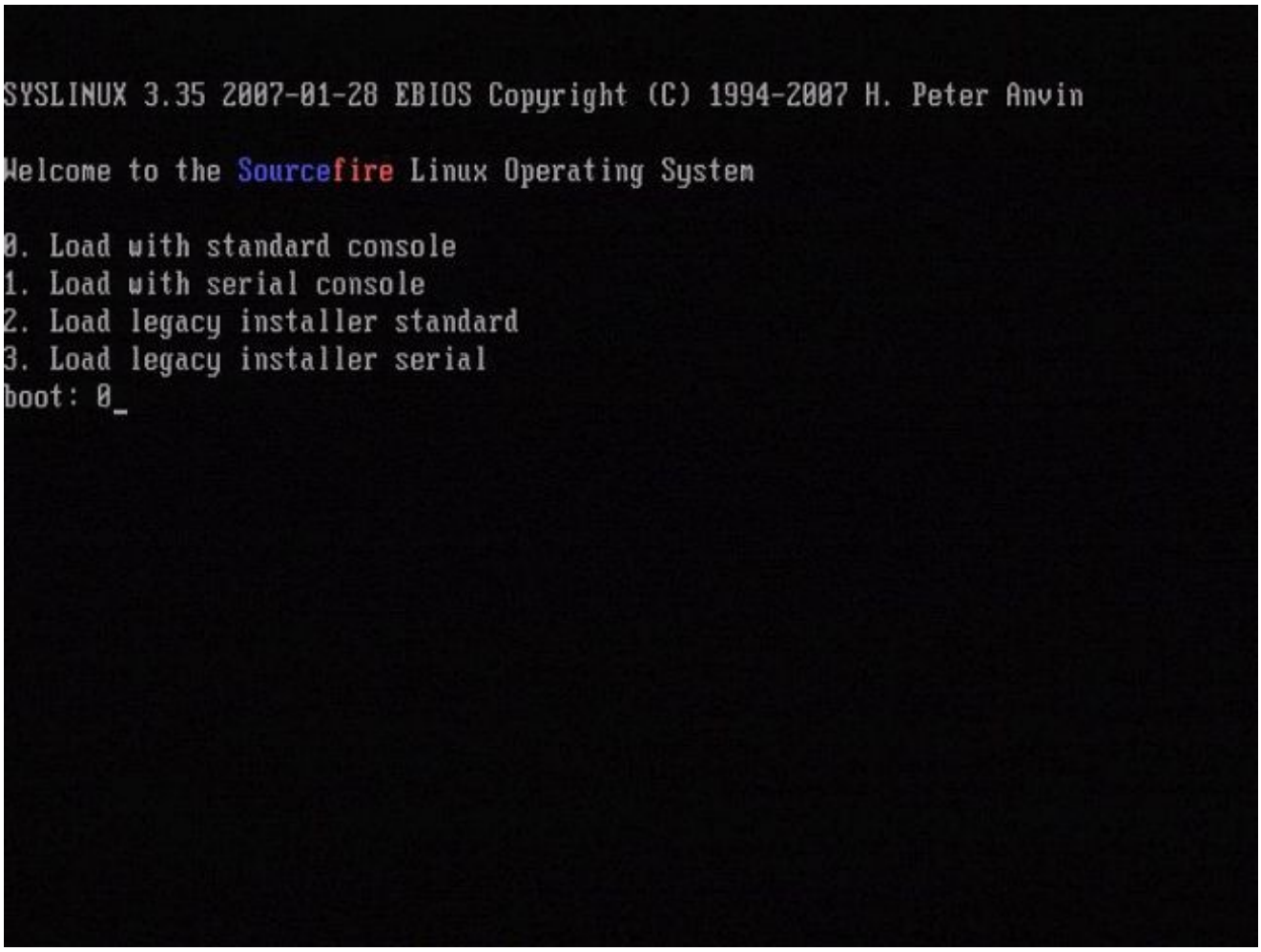

SYSLINUX 3.35 2007-01-28 EBIOS Copyright (C) 1994-2007 H. Peter Anvin
Welcome to the Sourcefire Linux Operating System
0. Load with standard console
1. Load with serial console
2. Load legacy installer standard
3. Load legacy installer serial
boot: 0_

그림 A4

그림 A5

7110 및 7120 디바이스

71XX 시리즈 디바이스를 사용하는 경우, 부팅 디바이스를 선택하려면 다음 단계를 완료하십시오.

1. 어플라이언스의 전원을 안전하게 끕니다.

2. 부트 장치 선택 화면에 액세스하기 위해 어플라이언스를 켜고 어플라이언스가 부팅하는 동안 F11 키를 반복적으로 누릅니다. 여기에 표시된 이미지를 참조하십시오.

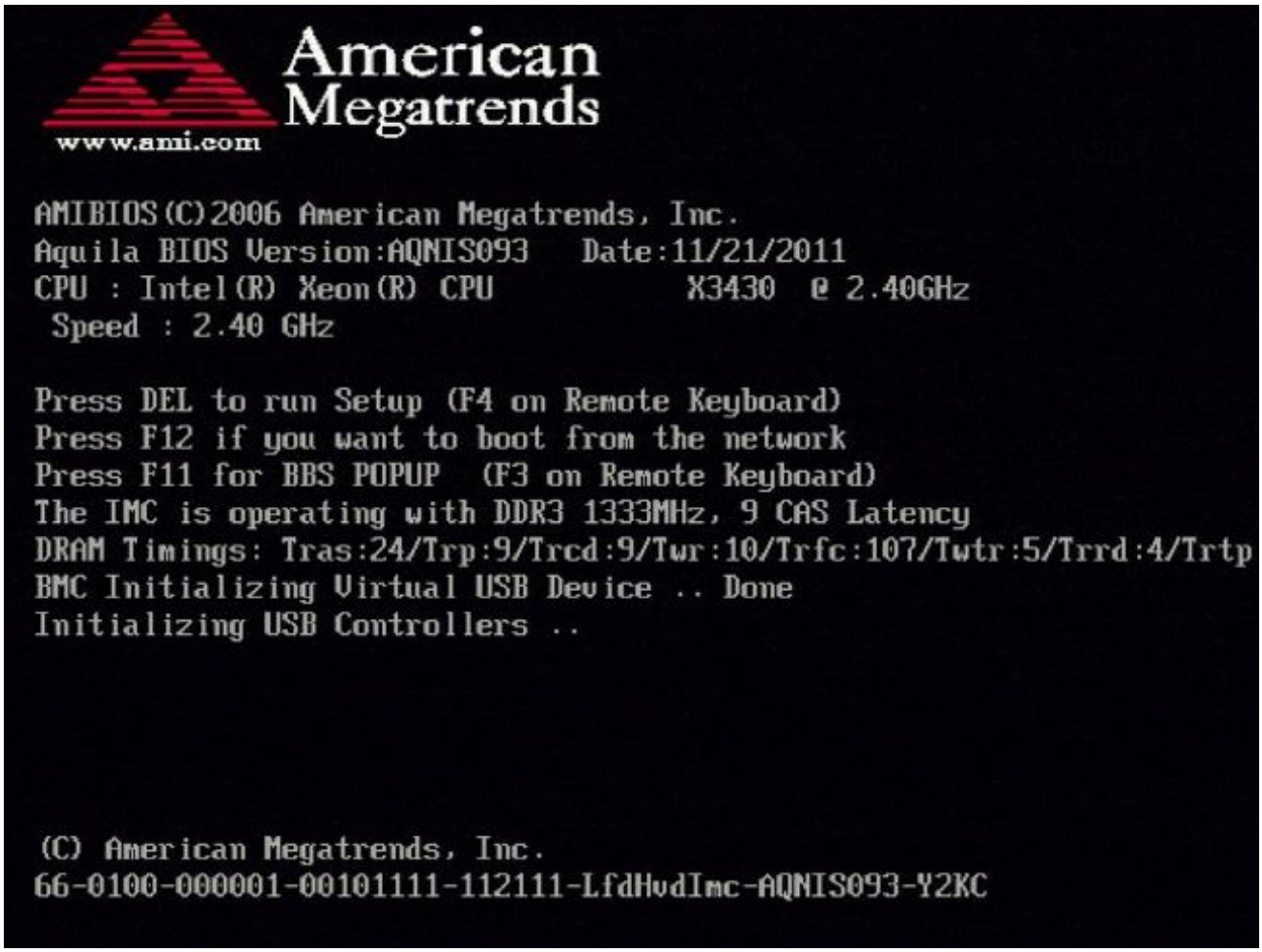


그림 B1

3. 옵션 HDD:P1-SATADOM을 선택하고 Enter를 눌러 System_Restore 파티션으로 부팅합니다.


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

그림 B2

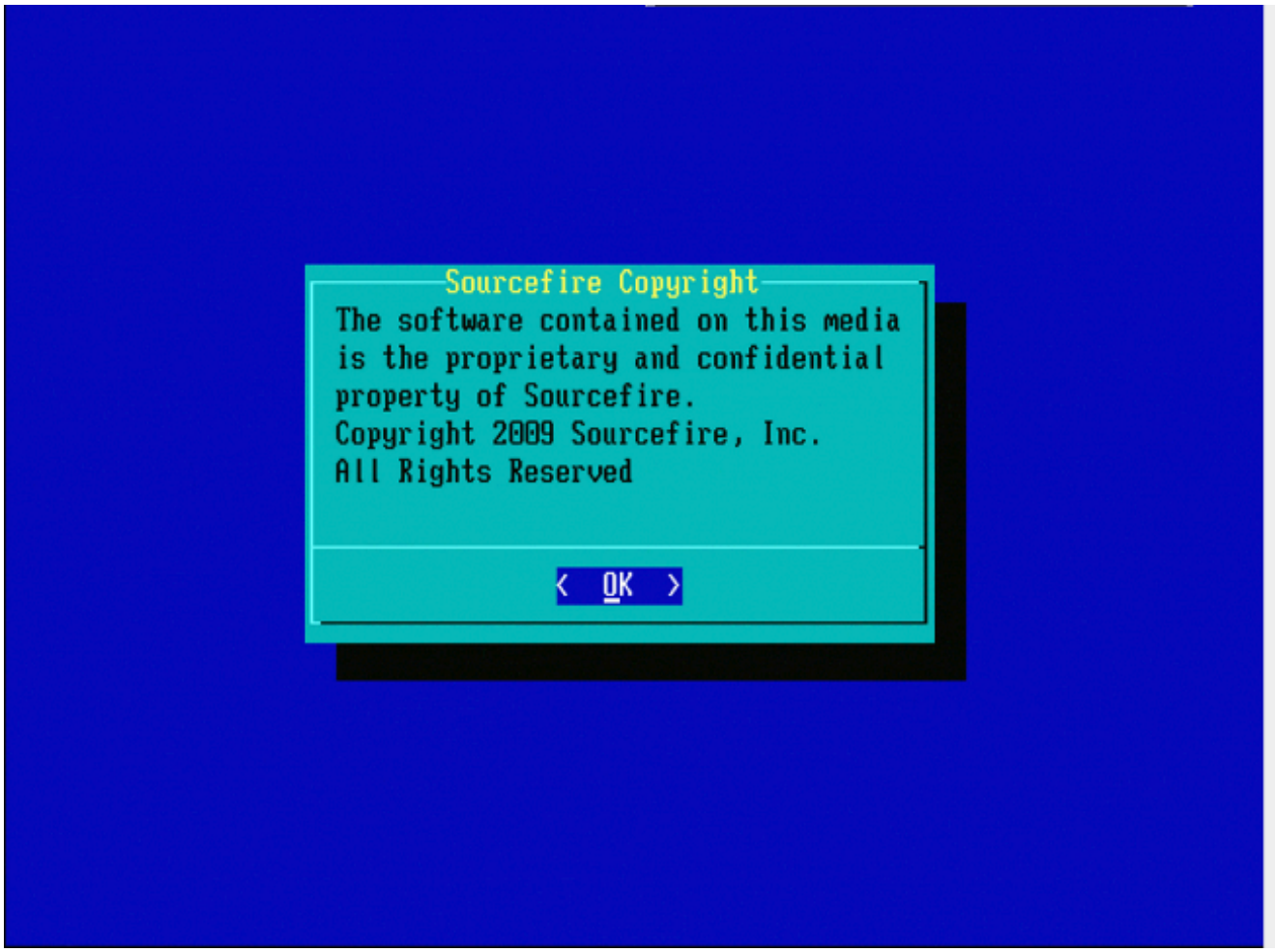


그림 B3

8000 Series 디바이스 또는 Management Center 모델 FS750, FS1500 또는 FS3500

8000 Series 디바이스 또는 Management Center 모델 FS750, FS1500 또는 FS3500을 사용하는 경우 다음 단계를 완료하여 부팅 디바이스를 선택합니다.

1. 어플라이언스의 전원을 안전하게 끕니다.

2. 부트 디바이스 선택 화면에 액세스하기 위해 어플라이언스를 켜고 어플라이언스가 부팅되는 동안 F6 키를 반복적으로 누릅니다. 여기에 표시된 이미지를 참조하십시오.

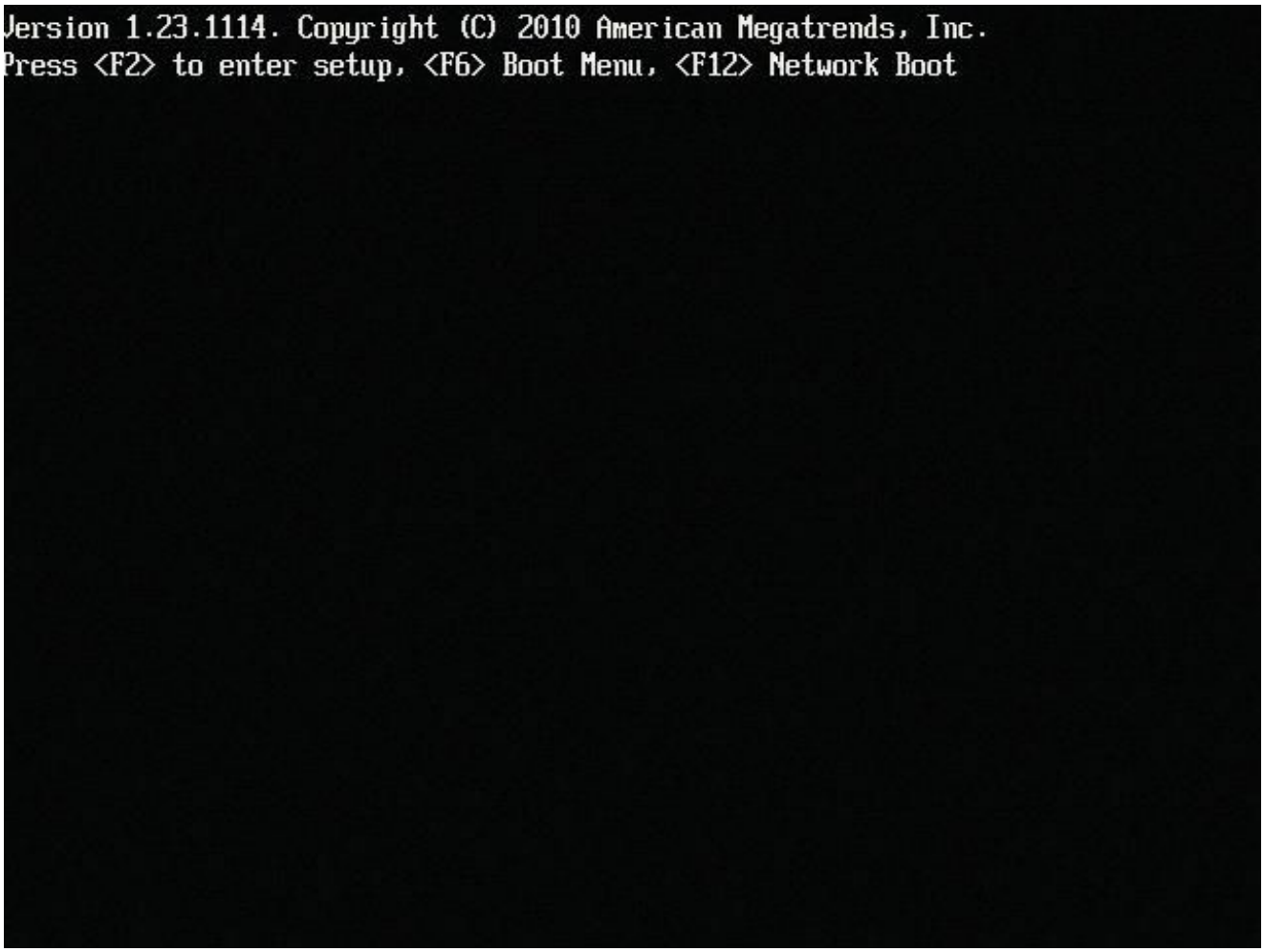


그림 C1

3. USB 옵션을 선택합니다.

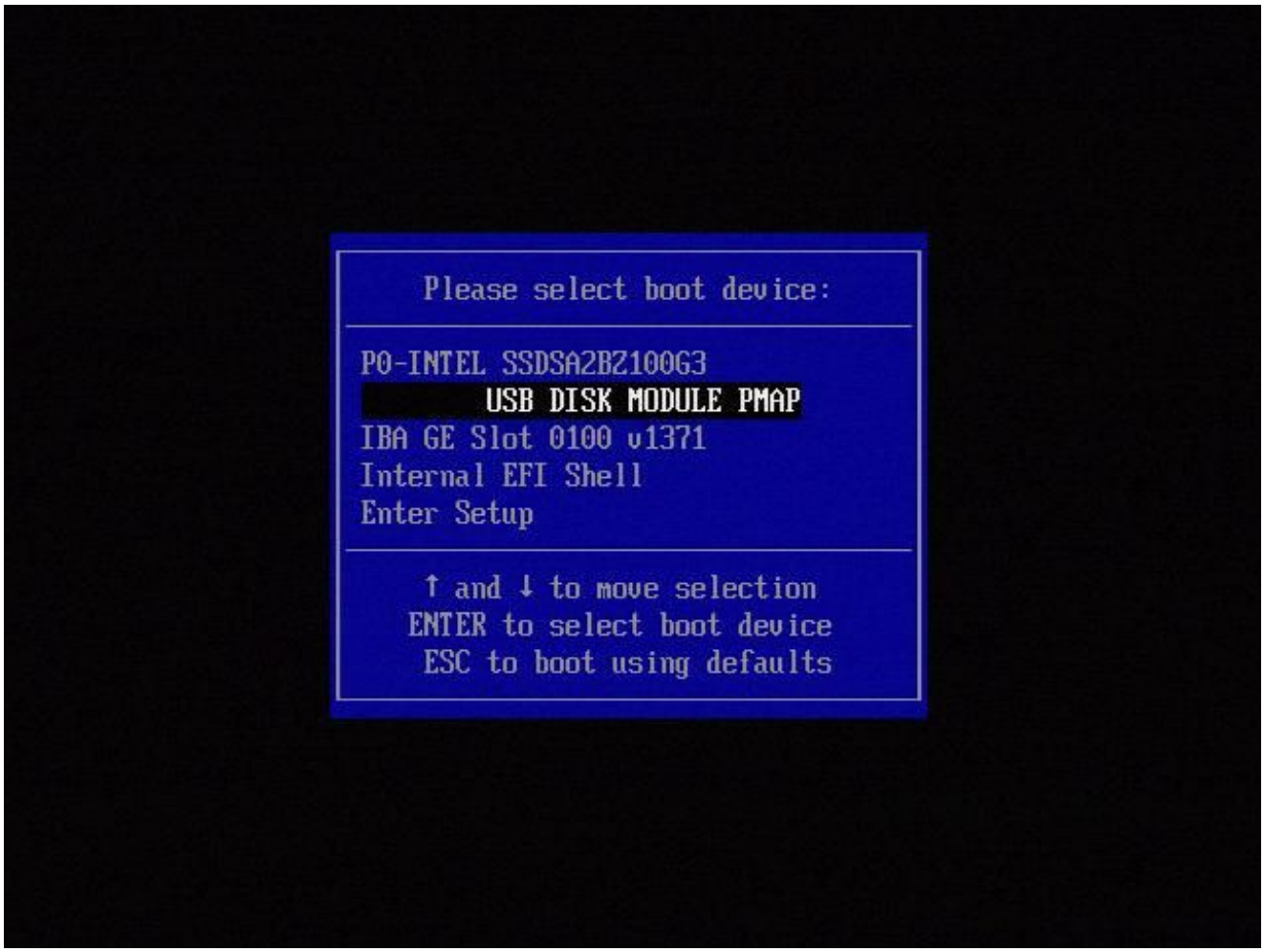


그림 C2

4. 어플라이언스가 System_Restore 파티션에서 부팅되고 System_Restore 메뉴가 표시됩니다.

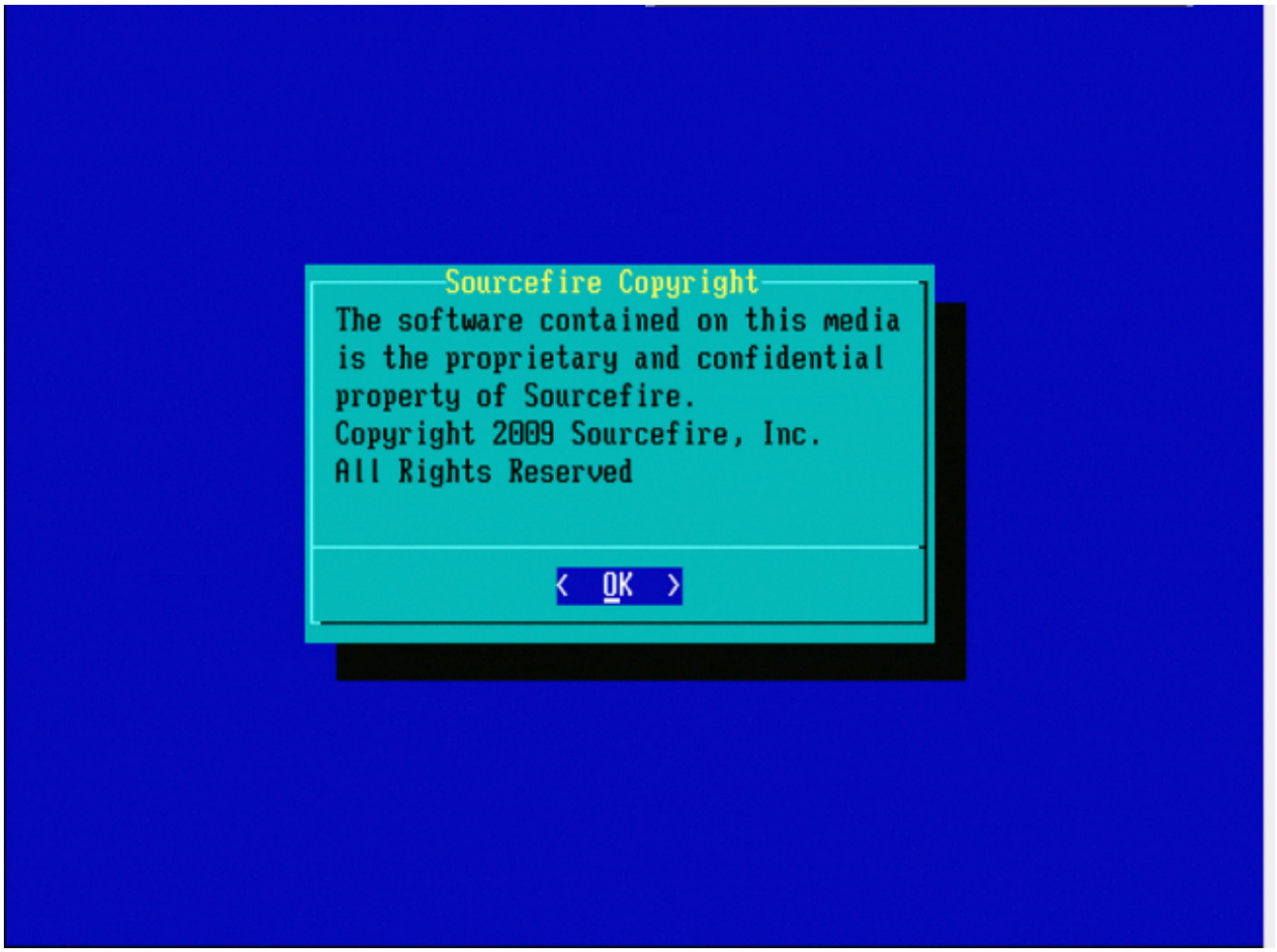


그림 C3

모델 FMC1000, FMC2500, FMC4500(M4 기반 FMC)에 대한 시스템 복원

참고: FMC4500의 경우 이 모델에는 다른 부팅 메뉴가 있으며 자세한 내용은 다음 링크에 나와 있습니다.

시스템 복원을 선택하라는 프롬프트는 FMC1000, FMC2500, FMC4500 모델에 대해 다르게 나타납니다

1. 부팅하는 동안 이 화면을 5초 동안 볼 수 있습니다.

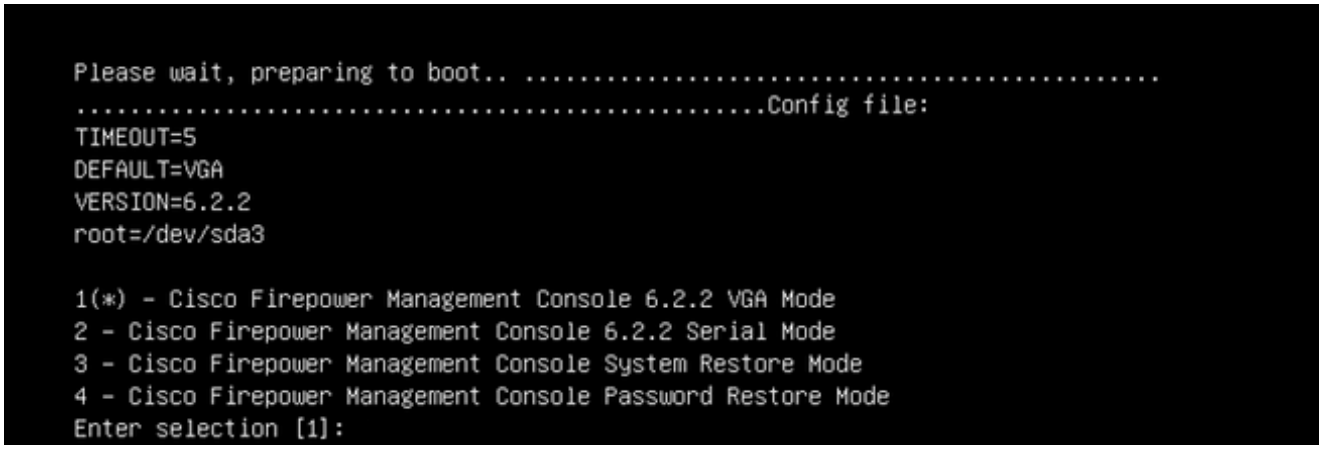


그림 D1

2. 시스템 복원 옵션을 선택합니다(이 #3의 경우).

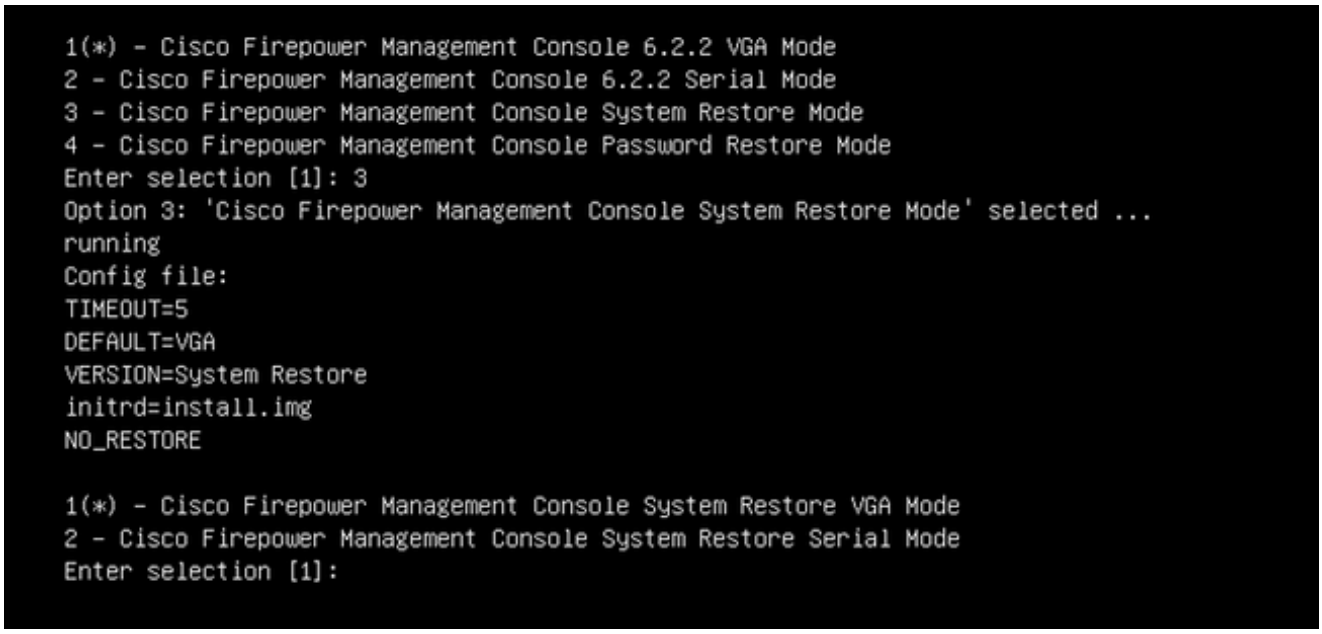


그림 D2

3. 시스템 복원에 대한 표시 방법을 선택합니다(이 #1는 VGA용).

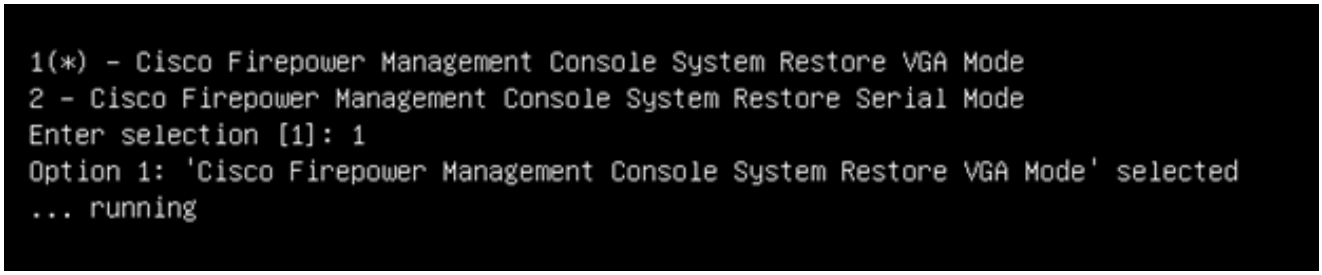


그림 D3

4. 그런 다음 그림 5에서 볼 수 있는 프롬프트에 도달하며 프로세스는 정상적으로 계속됩니다.

부팅 옵션이 나열되지 않음

재이미지 파티션으로 부팅하는 옵션이 BIOS 또는 boot 메뉴에 나열되지 않을 수 있습니다. 이 경우 이미지로 다시 설치하는 시스템이 포함된 드라이브가 없거나 손상되었을 수 있습니다. RMA가 필요할 수 있습니다.

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.