Implementación de FireSIGHT Management Center en VMware ESXi

Contenido

Introducción

Este documento describe la configuración inicial de un FireSIGHT Management Center (también conocido como Defense Center) que se ejecuta en VMware ESXi. FireSIGHT Management Center le permite administrar uno o varios appliances FirePOWER, dispositivos virtuales del sistema de prevención de intrusiones de última generación (NGIPS) y dispositivos de seguridad adaptable (ASA) con FirePOWER Services.

> **Nota:** Este documento es un suplemento de la guía de instalación del sistema FireSIGHT y de la guía del usuario. Para ver una pregunta específica de configuración y solución de problemas de ESXi, consulte la documentación y la base de conocimientos de VMware.

Prerequisites

Componentes Utilizados

La información de este documento se basa en estas plataformas:

- Cisco FireSIGHT Management Center
- Dispositivo virtual Cisco FireSIGHT Management Center
- VMware ESXI 5.0

En este documento, un "dispositivo" se refiere a estas plataformas:

- Appliances FirePOWER serie 7000 y dispositivos serie 8000 de Sourcefire
- Dispositivos virtuales NGIPS de Sourcefire para VMware ESXi
- Cisco ASA serie 5500-X con servicio FirePOWER

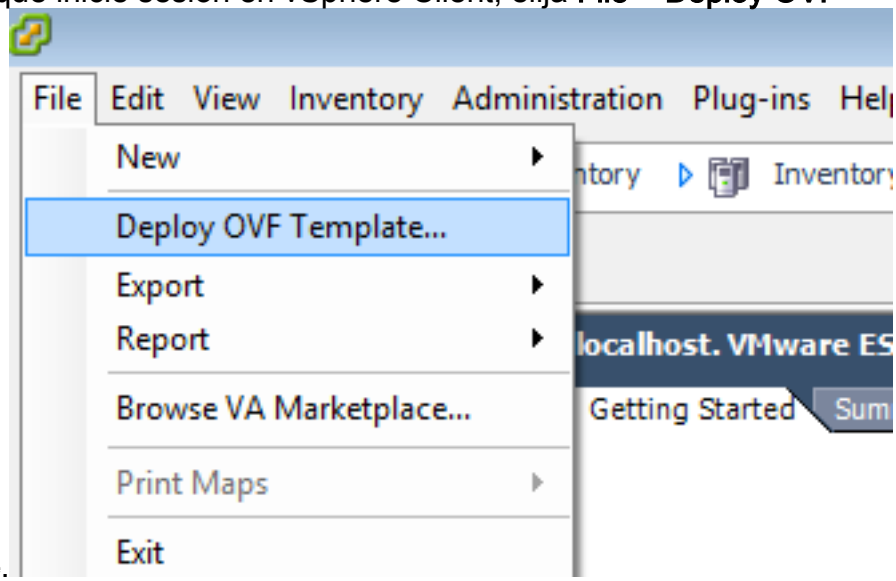
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuración

Implementar una plantilla OVF

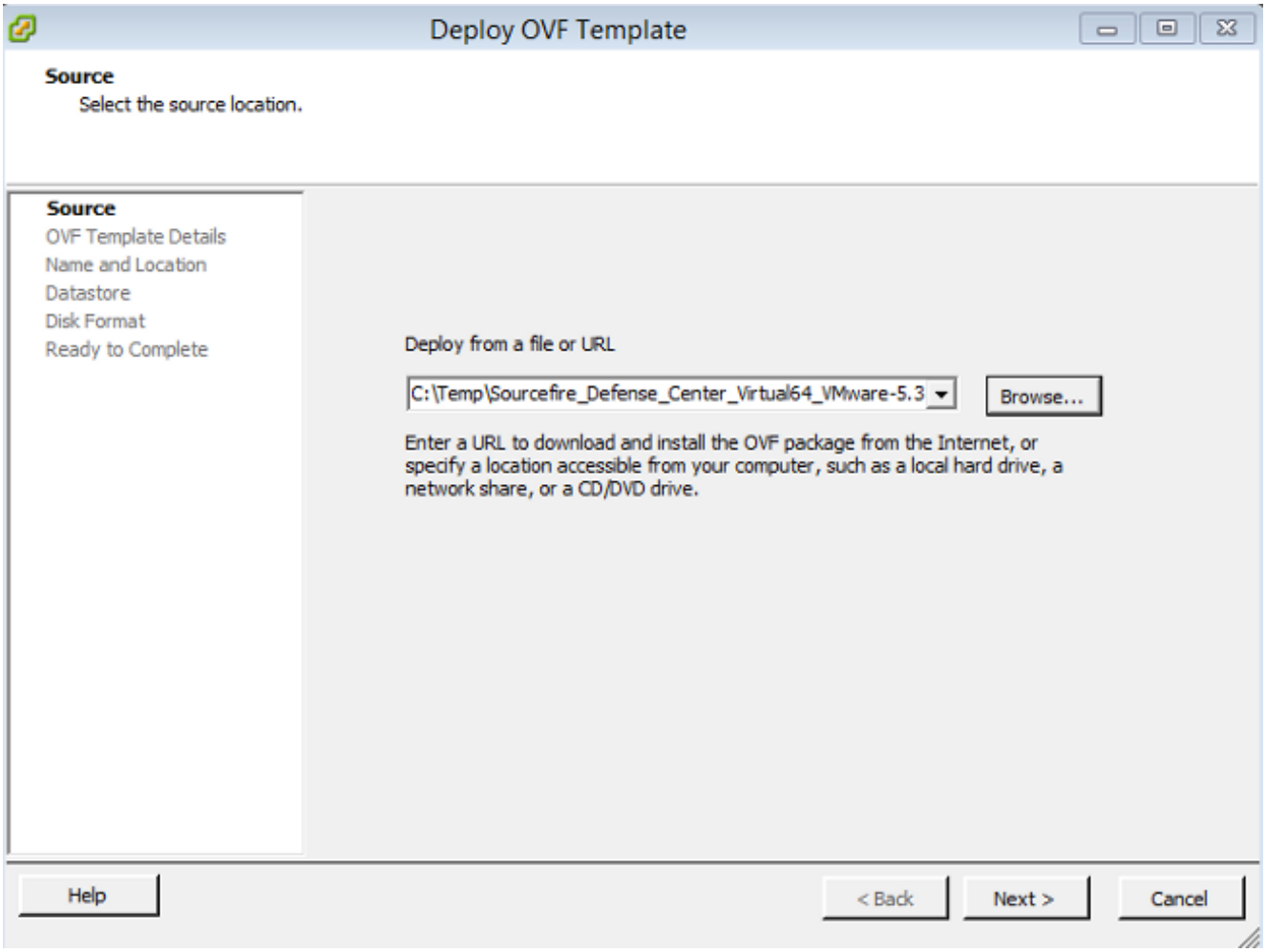
1. Descargue el **dispositivo virtual Cisco FireSIGHT Management Center** del sitio de soporte y descargas de Cisco.
2. Extraiga el contenido del archivo tar.gz a un directorio local.
3. Conéctese a su servidor ESXi con un **cliente VMware vSphere**.

4. Una vez que inicie sesión en vSphere Client, elija **File > Deploy OVF Template**.

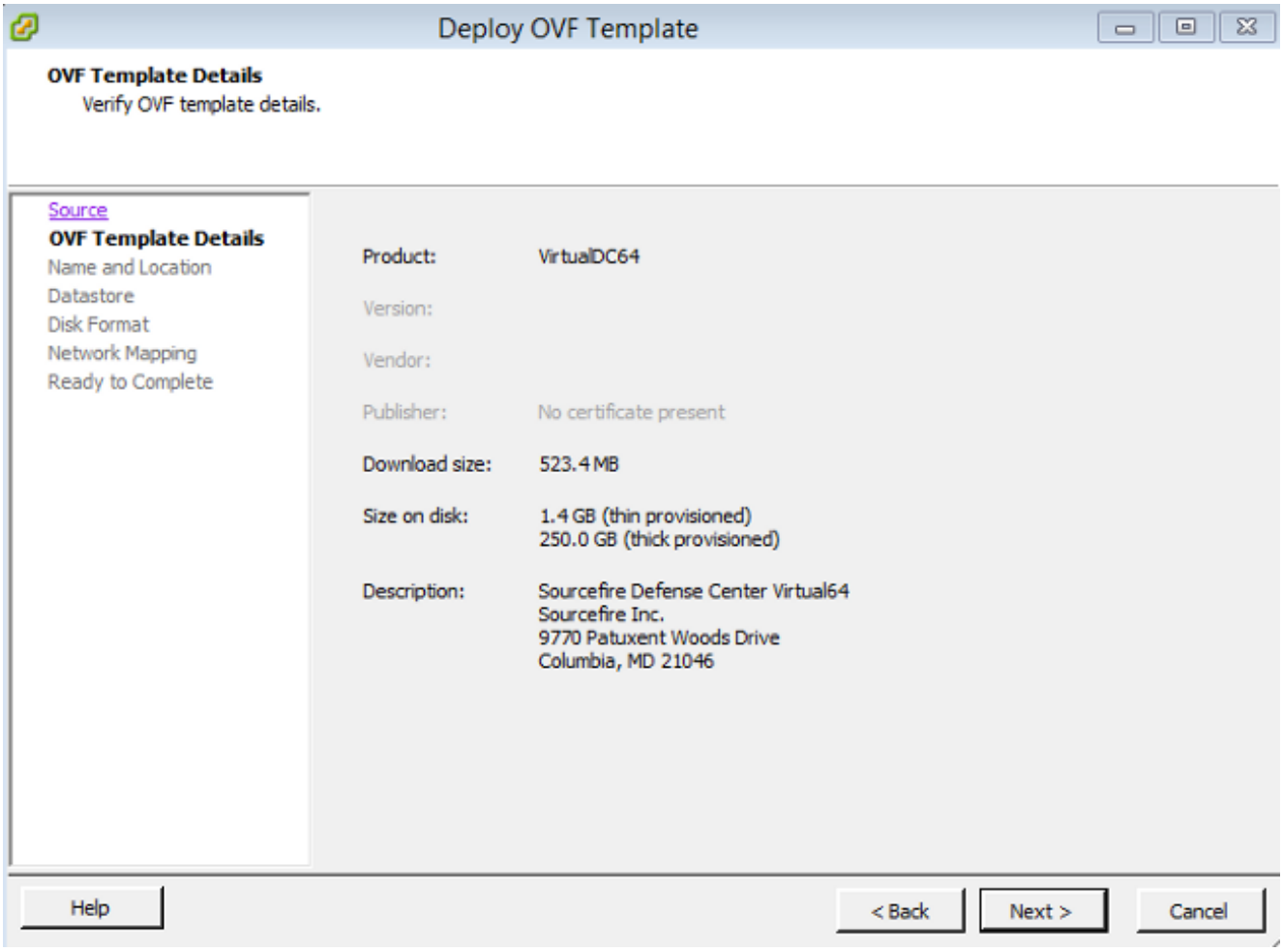


5. Haga clic en **Examinar** y busque los archivos que extrajo en el paso 2. Elija el archivo OVF

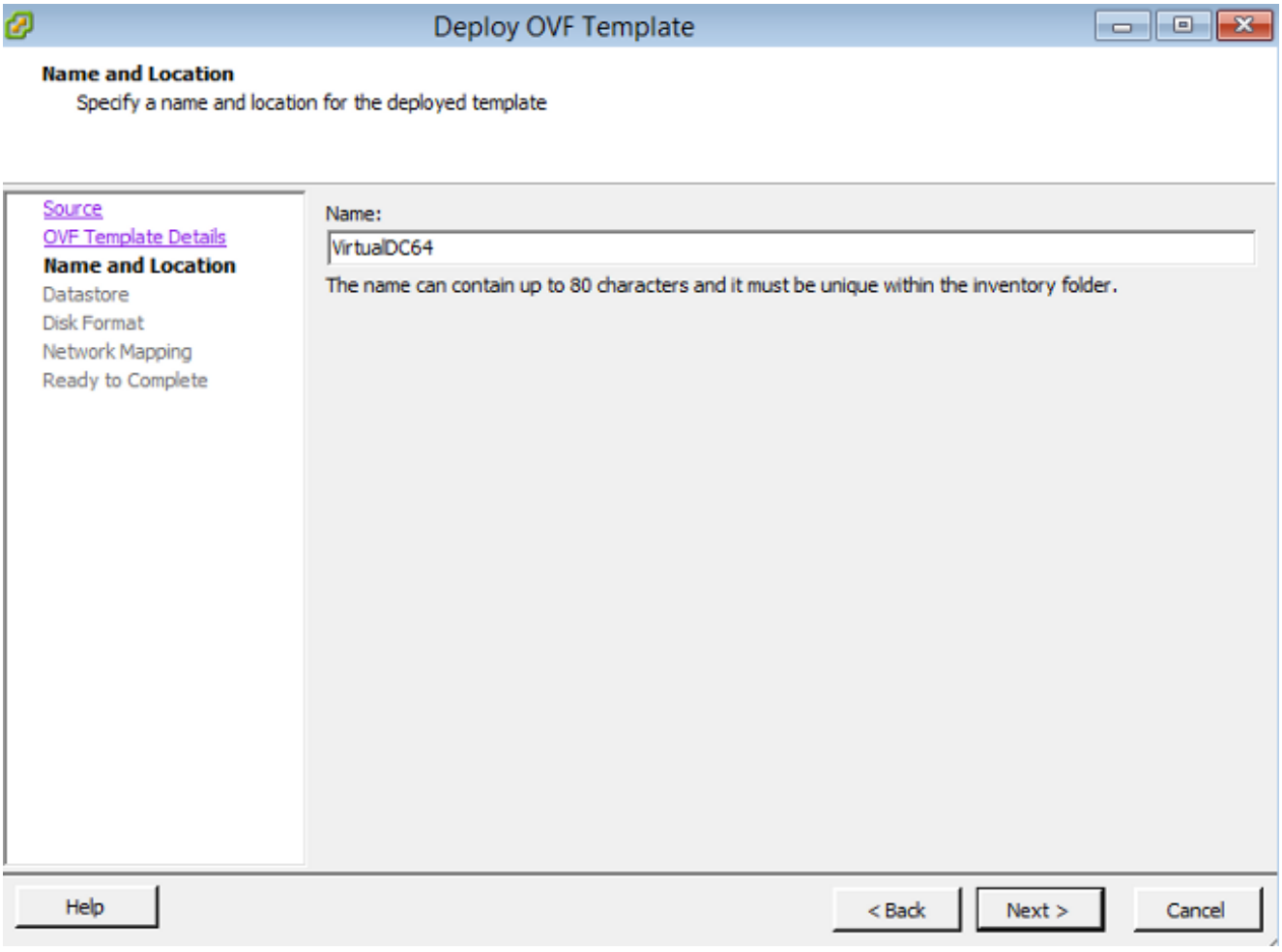
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf y haga clic en **Next.**



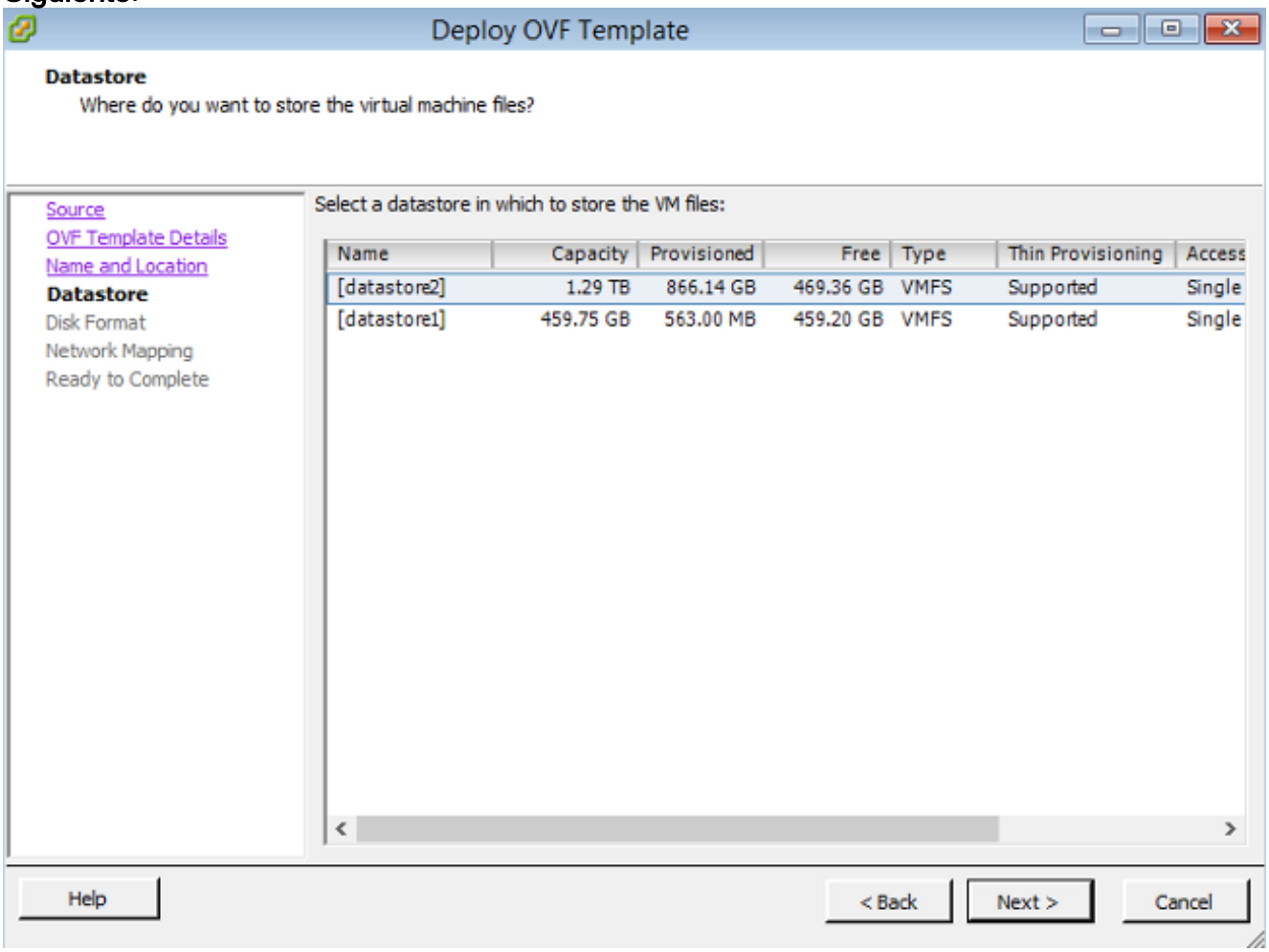
6. En la pantalla **Detalles de plantilla de OVF**, haga clic en **Siguiente** para aceptar la configuración predeterminada.



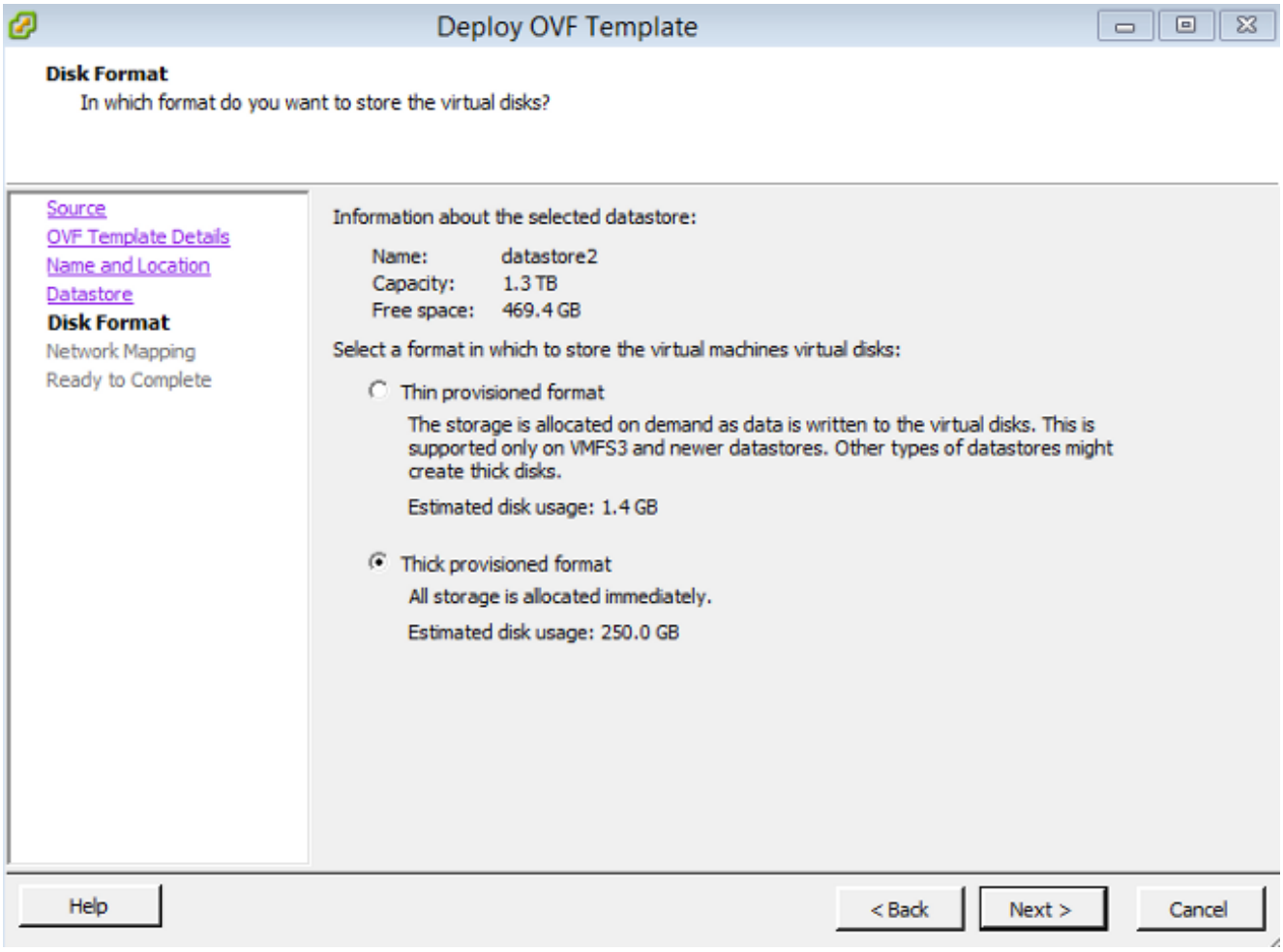
7. Proporcione un nombre para el Management Center y haga clic en **Next**.



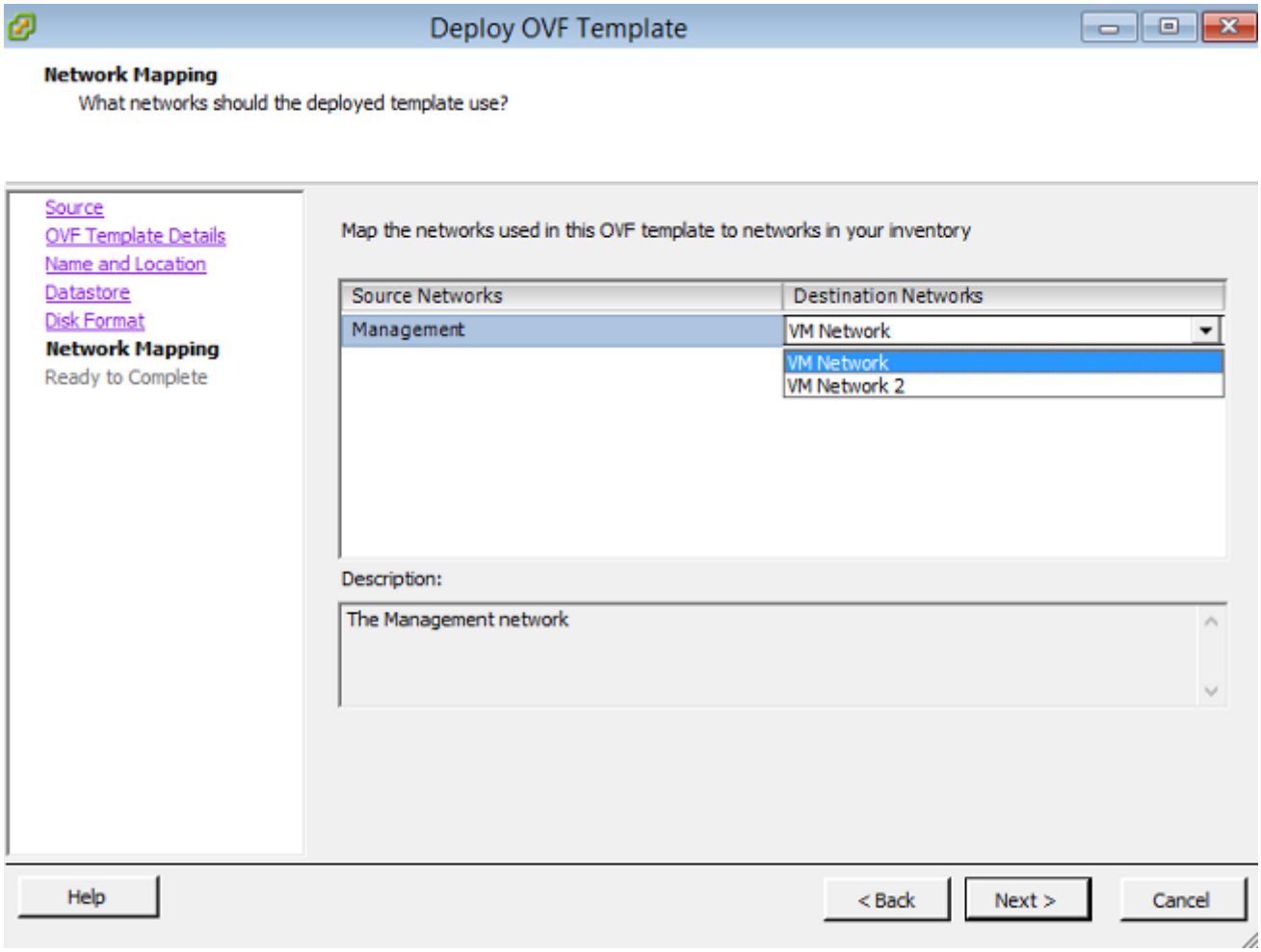
8. Elija un **almacén de datos** en el que desea crear la máquina virtual y haga clic en **Siguiente**.



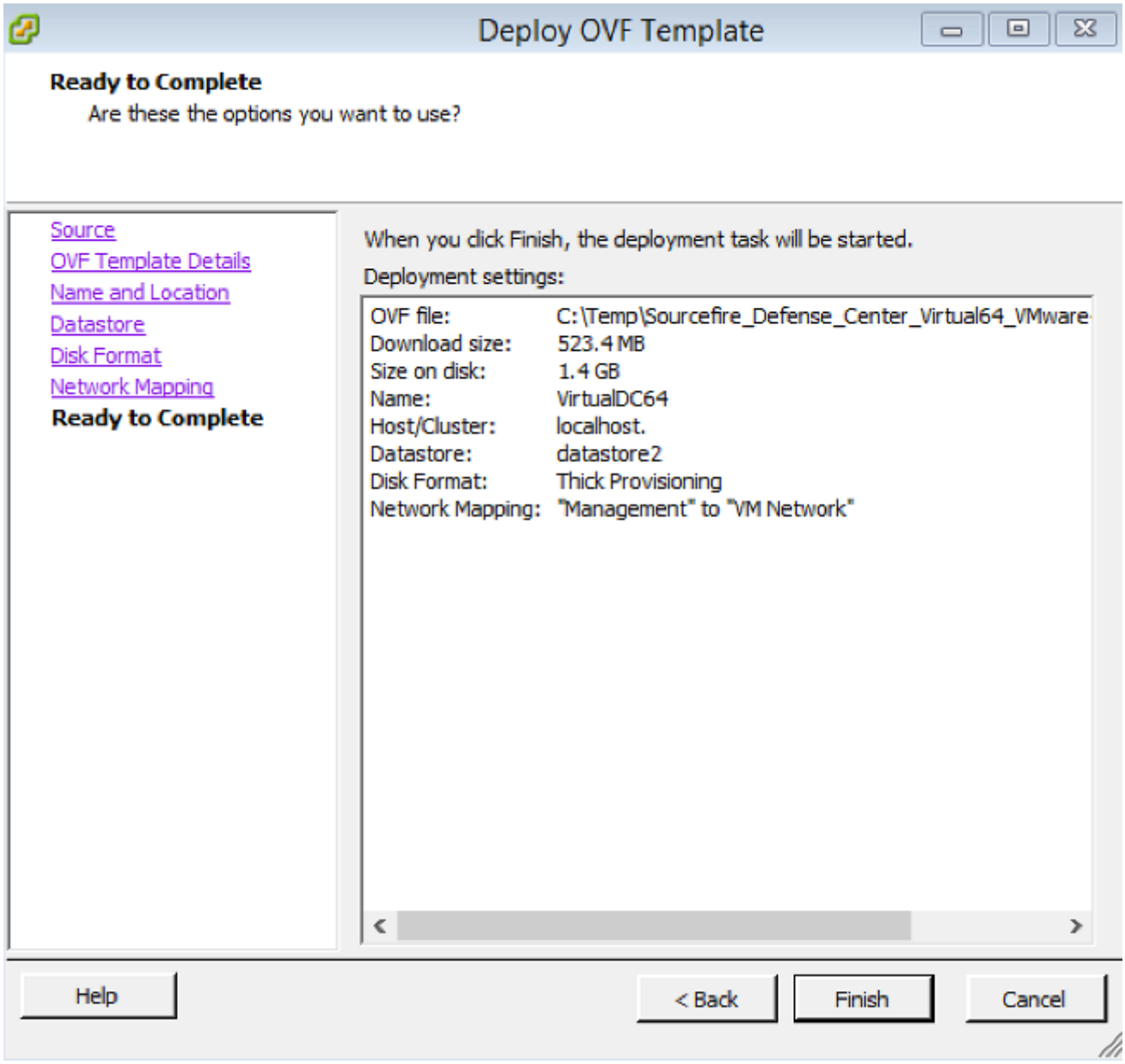
9. Haga clic en el botón de opción **Thick provisioned format** para el **Formato de disco** y haga clic en **Siguiente**. El formato de aprovisionamiento grueso asigna el espacio de disco necesario en el momento de crear un disco virtual, mientras que el formato de aprovisionamiento ligero utiliza espacio a demanda.



10. En la sección **Asignación de red**, asocie la interfaz de administración de FireSIGHT Management Center a una red VMware y haga clic en **Siguiente**.

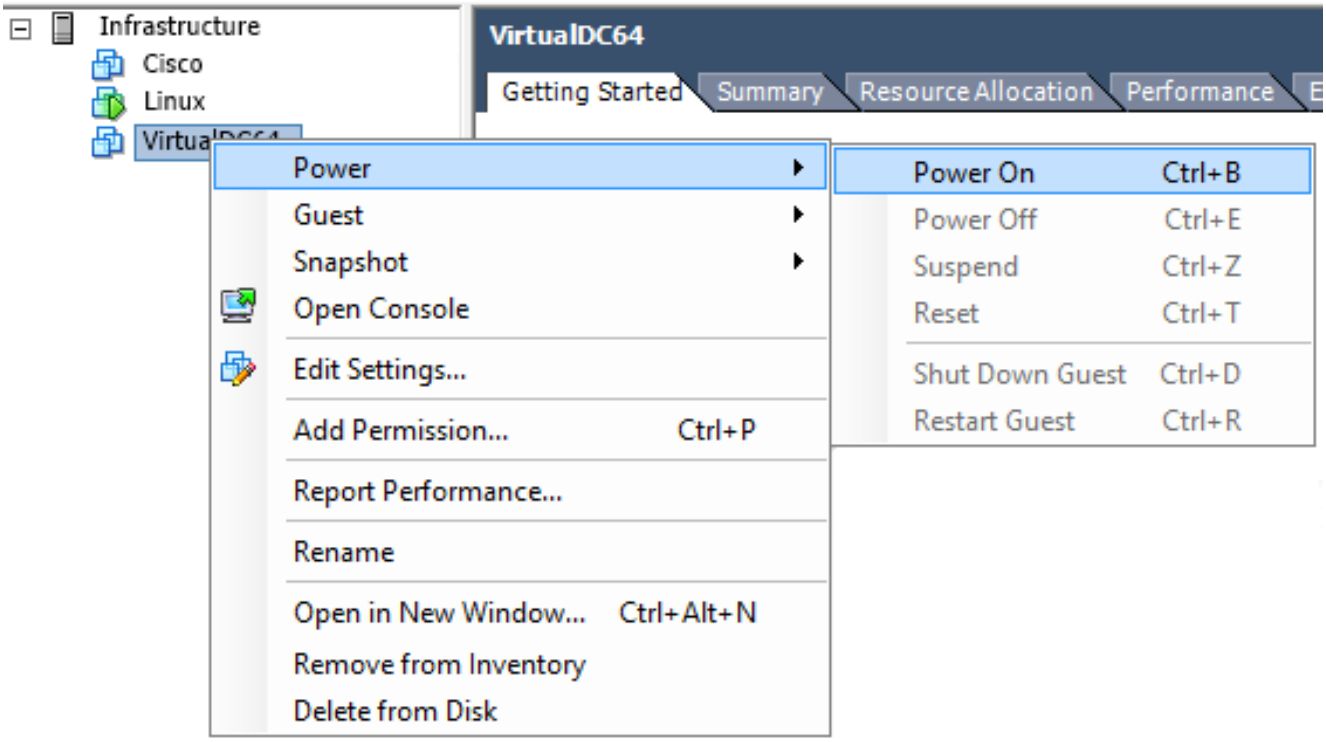


11. Haga clic en **Finalizar** para completar la implementación de la plantilla OVF.

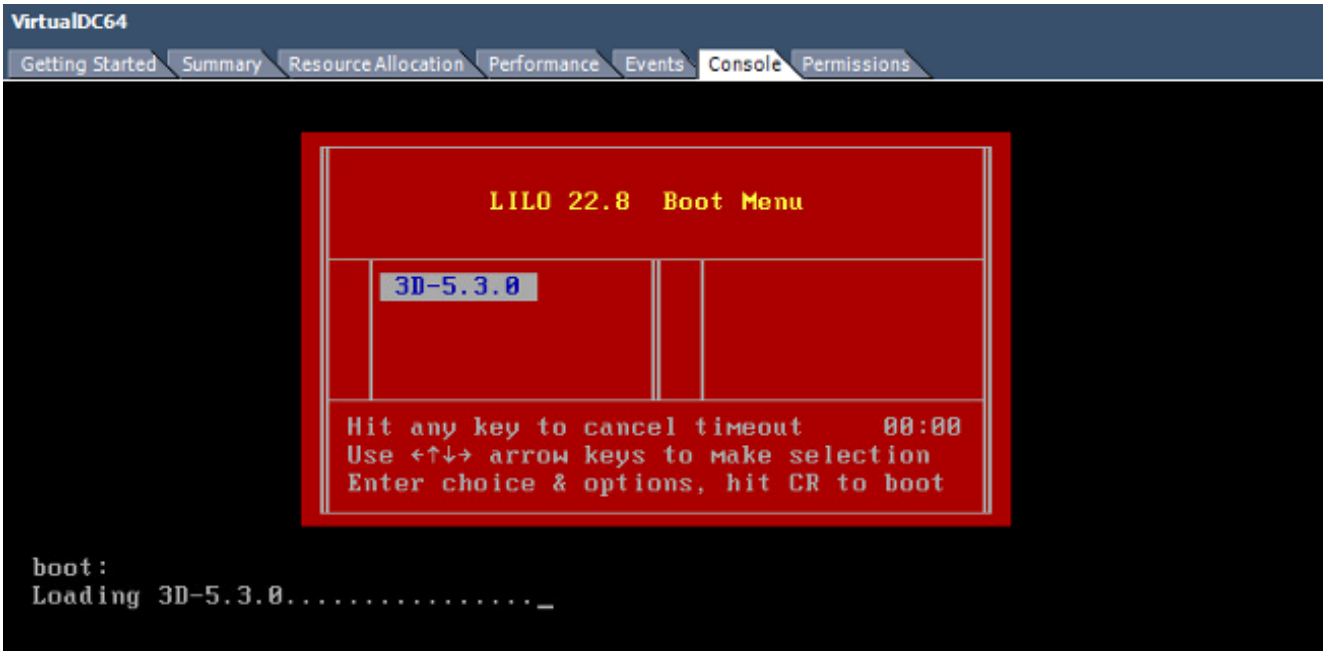


Activación e inicialización completa

1. Navegue hasta la máquina virtual recién creada. Haga clic con el botón derecho en el nombre del servidor y elija **Power > Power On** para iniciar el servidor por primera vez.



2. Navegue hasta la pestaña **Consola** para monitorear la consola del servidor. Aparece el menú de arranque
LILO.



Una vez que la verificación de datos del BIOS se realiza correctamente, se inicia el proceso de inicialización. El primer inicio puede tardar más tiempo en completarse, ya que la base de datos de configuración se inicializa por primera
vez.

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh                                  [  OK  ]
Executing S04async_syslog_dc.sh                                    [  OK  ]
Executing S04fix-httpd.sh                                          [  OK  ]
Executing S05set-mgmnt-port                                        [  OK  ]
Executing S06addusers                                              [  OK  ]
Executing S07uuid-init                                             [  OK  ]
Executing S09configure_mysql                                       [  OK  ]

************ Attention **********

   Initializing the configuration database.  Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.

************ Attention **********

Executing S10database
_
```

Una vez completado, es posible que vea un mensaje para No tal dispositivo.

```
  Copyright (c) 1999-2010 Intel Corporation.
  Silicom Bypass-SD Control driver v5.0.39.5
  No such device
  _
```

3. Presione **Enter** para obtener un mensaje de inicio de sesión.

```
 Copyright (c) 1999-2010 Intel Corporation.
 Silicom Bypass-SD Control driver v5.0.39.5
 No such device

 Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)
 Sourcefire3D login: _
```

Nota: Un mensaje "WRITE SAME failed" (Falló la ESCRITURA EN LA MISMA). Manualmente cero." puede aparecer después de arrancar el sistema por primera vez. Esto no indica un defecto, indica correctamente que el driver de almacenamiento VMware no soporta el comando WRITE SAME. El sistema muestra este mensaje y continúa con un comando de reserva para realizar la misma operación.

Configuración de los parámetros de red

1. En el mensaje de inicio de sesión Sourcefire3D, utilice estas credenciales para iniciar sesión: Para la versión 5.xNombre de usuario: **admin**Contraseña **Sourcefire**Para la versión 6.x y posterioresNombre de usuario: **admin**Contraseña **Admin123Consejo:** Podrá cambiar la contraseña predeterminada en el proceso de configuración inicial en la GUI.
2. La configuración inicial de la red se realiza con un script. Debe ejecutar el script como usuario raíz. Para cambiar al usuario root, ingrese el **comando sudo su -** junto con la contraseña **Sourcefire o Admin123** (para 6.x). Tenga cuidado cuando inicie sesión en la línea de comandos del Management Center como usuario raíz.

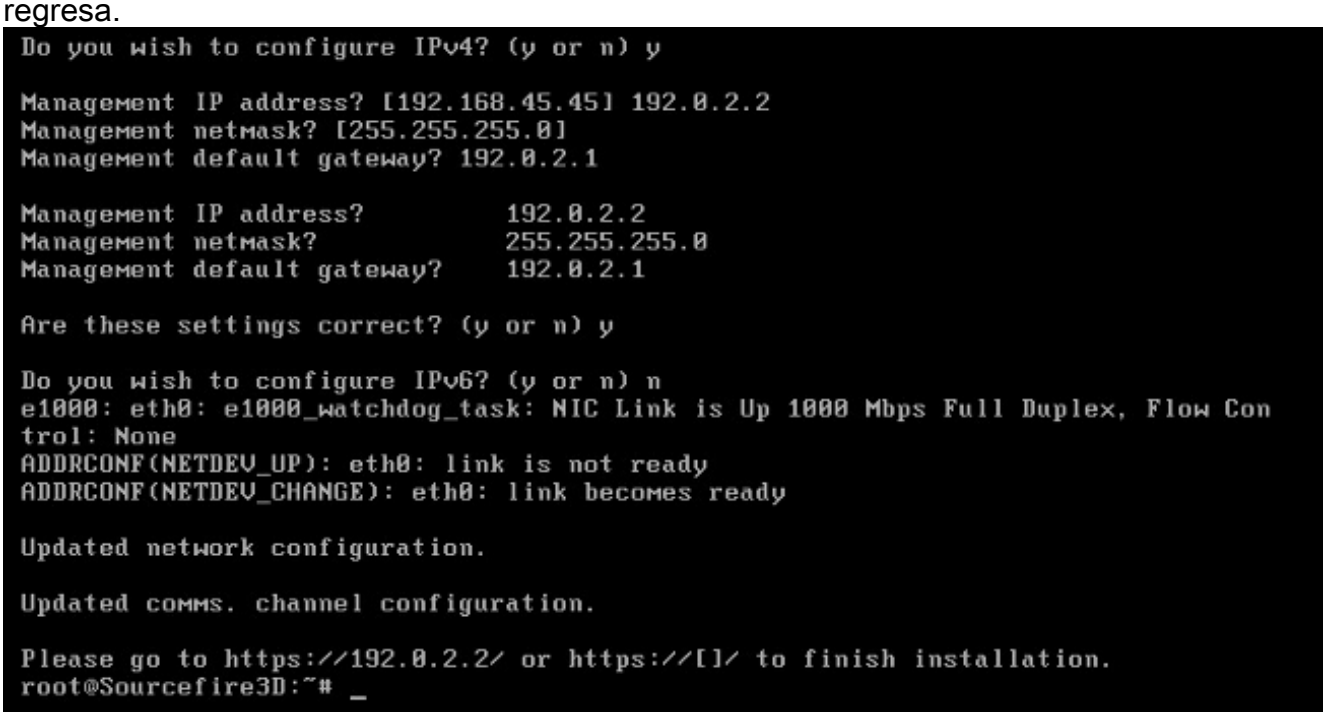
```
admin@Sourcefire3D:~$ sudo su -
Password:
```

3. Para comenzar la configuración de la red, ingrese el script **configure-network** como root.

```
root@Sourcefire3D:~# configure-network

Do you wish to configure IPv4? (y or n) y
```

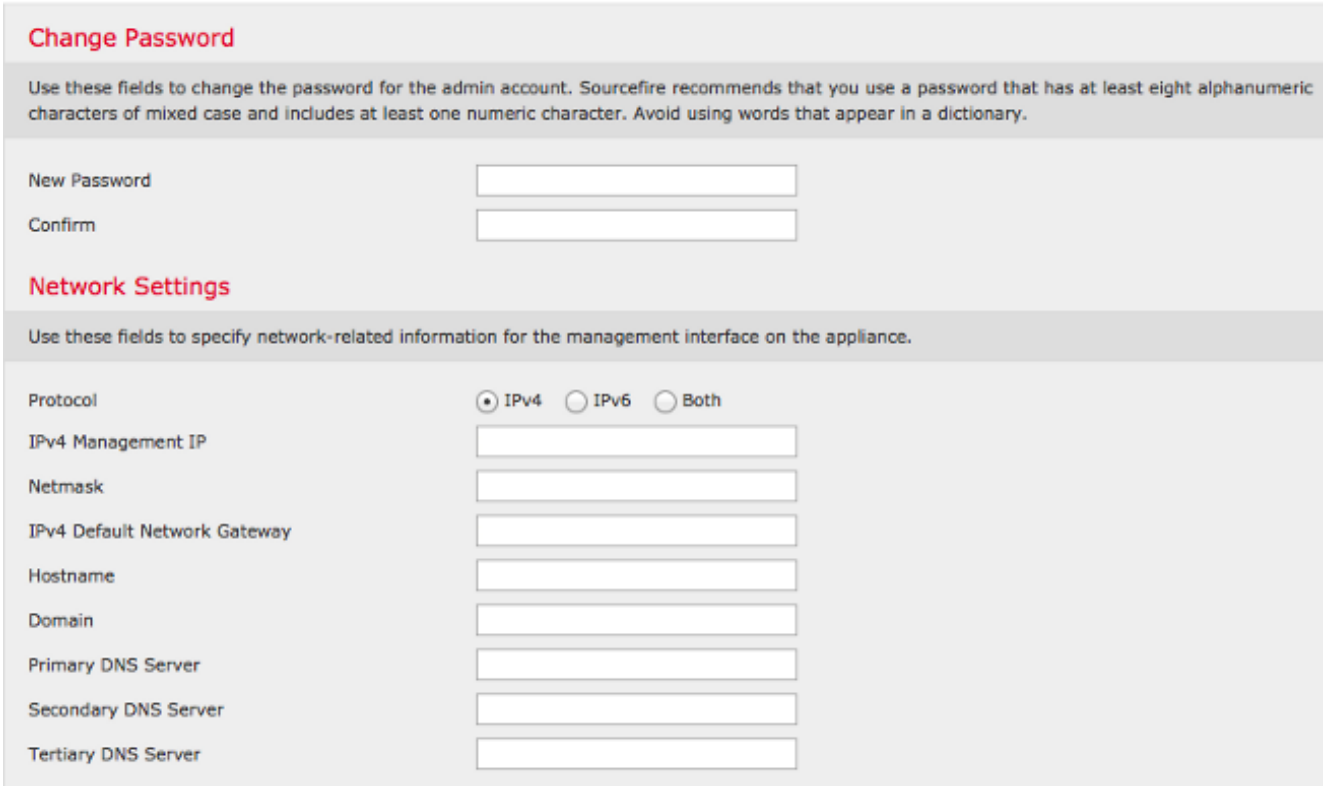
Se le solicitará que proporcione una dirección IP de administración, una máscara de red y una gateway predeterminada. Una vez que confirme los parámetros, el servicio de red se reiniciará. Como resultado, la interfaz de administración se desactiva y regresa.



Realizar configuración inicial

1. Después de configurar los parámetros de red, abra un navegador web y busque la IP configurada a través de HTTPS (https://192.0.2.2 en este ejemplo). Autentique el certificado SSL predeterminado si se le solicita. Utilice estas credenciales para iniciar sesión:Para la versión 5.x Nombre de usuario: **admin**Contraseña **Sourcefire**Para la versión 6.x y posterioresNombre de usuario: **admin**Contraseña **Admin123**
2. En la pantalla que aparece a continuación, todas las secciones de configuración de la GUI son opcionales excepto el cambio de contraseña y la aceptación de los términos de servicio. Si se conoce la información, se recomienda utilizar el asistente de configuración para simplificar la configuración inicial del Management Center. Una vez configurado, haga clic en **Aplicar** para aplicar la configuración al Centro de administración y a los dispositivos registrados. A continuación se ofrece una breve descripción general de las opciones de configuración:**Cambiar contraseña:** Permite cambiar la contraseña de la cuenta de administrador predeterminada. Es necesario cambiar la contraseña. **Network Settings (Parámetros de red)** Permite modificar los parámetros de red IPv4 e IPv6 configurados previamente para la interfaz de administración del dispositivo o la máquina virtual.**Configuración de hora:** Se recomienda sincronizar el Management Center con un origen NTP fiable. Los sensores IPS se pueden configurar mediante la política del sistema para sincronizar su tiempo con el Management Center. Opcionalmente, la zona horaria y de visualización se pueden establecer manualmente.**Importaciones recurrentes de actualización de reglas:** Habilitar actualizaciones recurrentes de reglas de Snort e instalar opcionalmente ahora durante la configuración inicial.**Actualizaciones recurrentes de geolocalización:** Habilitar actualizaciones recurrentes de reglas de geolocalización e instalar opcionalmente ahora durante la configuración inicial.**Copias de seguridad automáticas:** Programar copias de seguridad automáticas de la configuración.**Configuración de licencia:** Agregue la licencia de

función.**Registro de dispositivos:** Permite agregar, licenciar y aplicar políticas de control de acceso iniciales a dispositivos registrados previamente. El nombre de host/dirección IP y la clave de registro deben coincidir con la dirección IP y la clave de registro configuradas en el módulo IPS FirePOWER.**Acuerdo de licencia del usuario final:** Se requiere la aceptación del CLUF.



Información Relacionada

- [Guía de inicio rápido virtual de Firepower Management Center para VMware, versión 6.0]
- [Soporte Técnico y Documentación - Cisco Systems]