Implantação do FireSIGHT Management Center no VMware ESXi

Contents

Introduction

Este documento descreve a configuração inicial de um FireSIGHT Management Center (também conhecido como Defense Center) executado no VMware ESXi. Um FireSIGHT Management Center permite que você gerencie um ou mais dispositivos FirePOWER, dispositivos virtuais do Next Generation Intrusion Prevention System (NGIPS) e Adaptive Security Appliance (ASA) com FirePOWER Services.

> **Note**: Este documento é um suplemento do Guia de instalação do sistema FireSIGHT e do Guia do usuário. Para uma pergunta específica sobre configuração e solução de problemas do ESXi, consulte a base de conhecimento e a documentação do VMware.

Prerequisites

Componentes Utilizados

As informações neste documento são baseadas nas seguintes plataformas:

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

Neste documento, um "dispositivo" refere-se a estas plataformas:

- Dispositivos Sourcefire FirePOWER 7000 Series e 8000 Series
- Dispositivos virtuais Sourcefire NGIPS para VMware ESXi
- Cisco ASA 5500-X Series com serviço FirePOWER

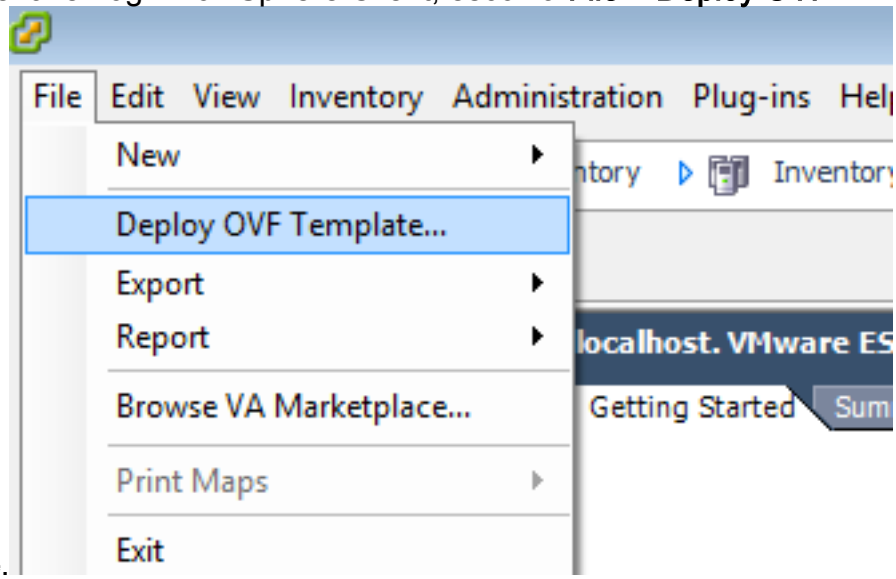
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuração

Implantar um modelo OVF

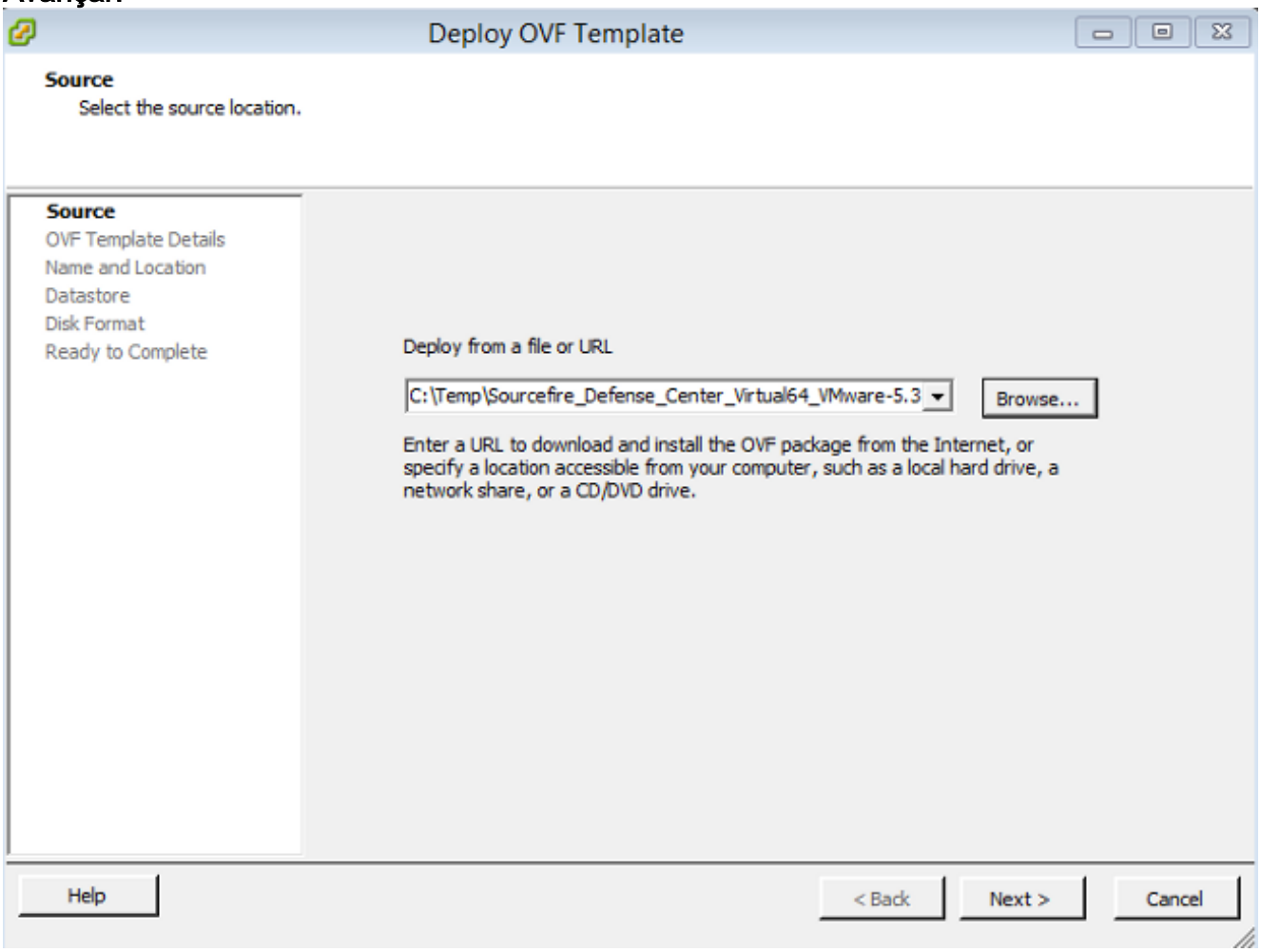
1. Baixe o **Cisco FireSIGHT Management Center Virtual Appliance** do site Cisco Support & Downloads.
2. Extraia o conteúdo do arquivo tar.gz para um diretório local.
3. Conecte-se ao servidor ESXi com um **cliente VMware vSphere**.

4. Depois de fazer login no vSphere Client, escolha **File > Deploy OVF Template**.

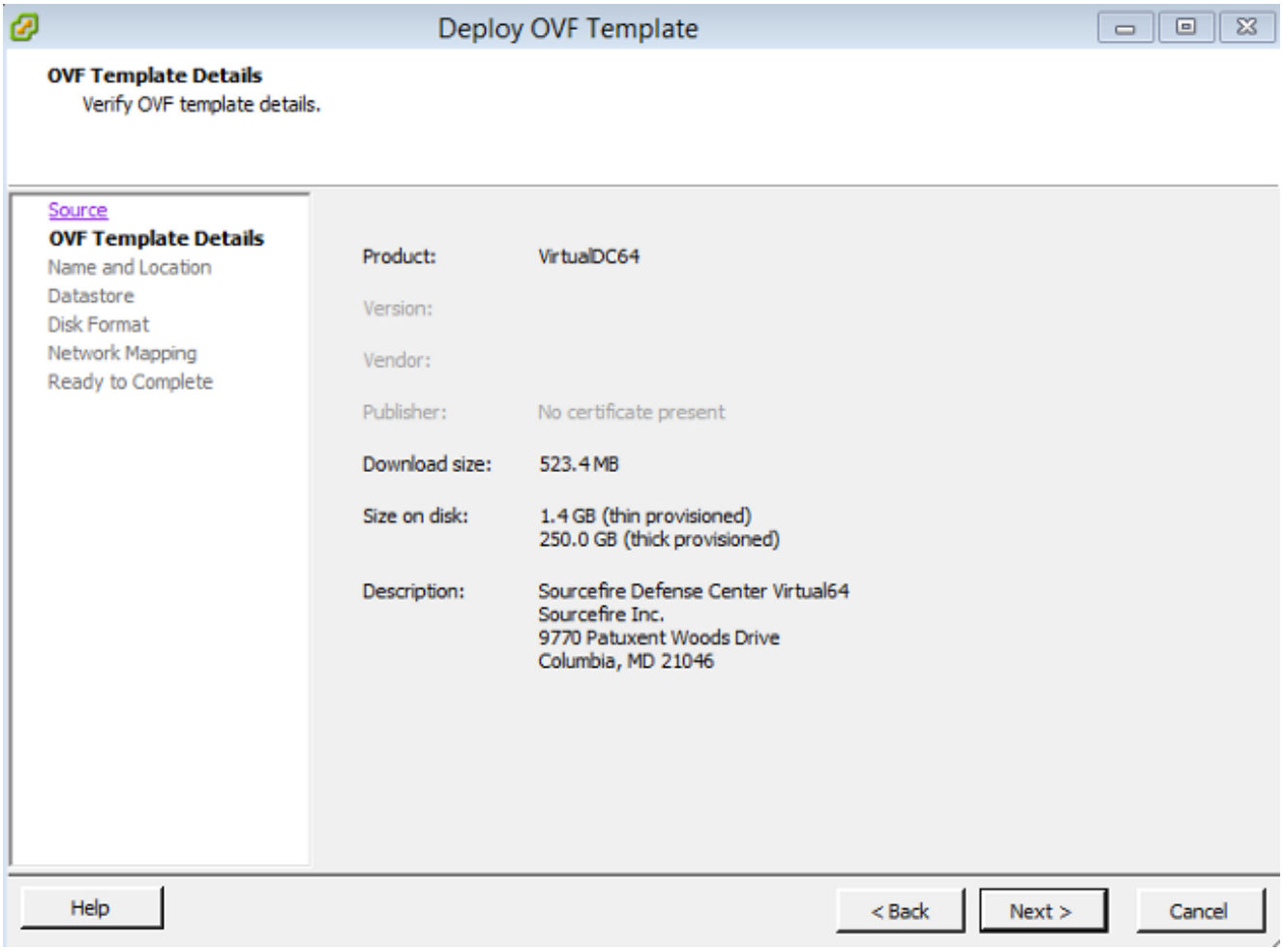


5. Clique em **Procurar** e localize os arquivos que você extraiu na etapa 2. Escolha o arquivo

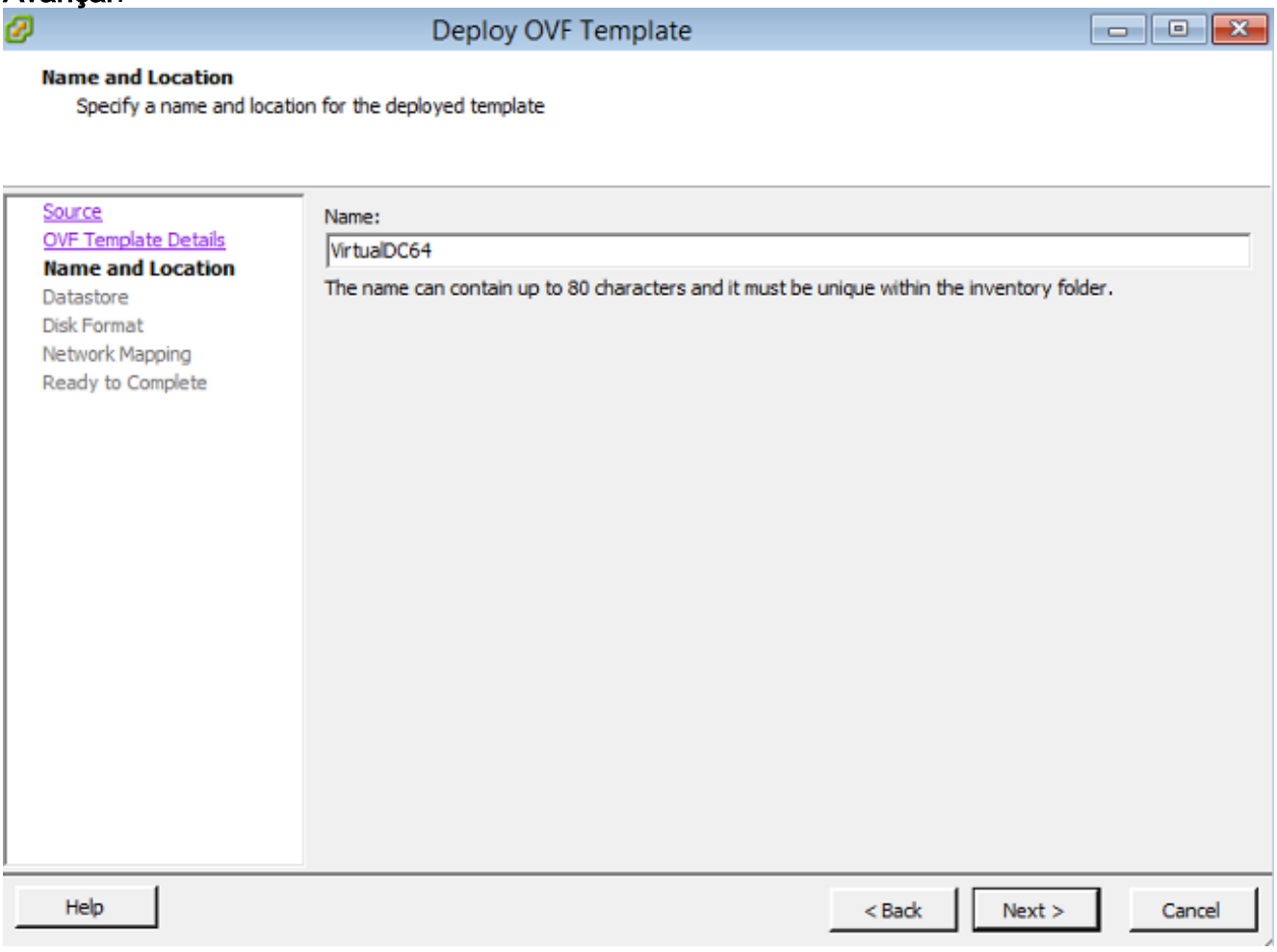
OVF Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf e clique em **Avançar.**



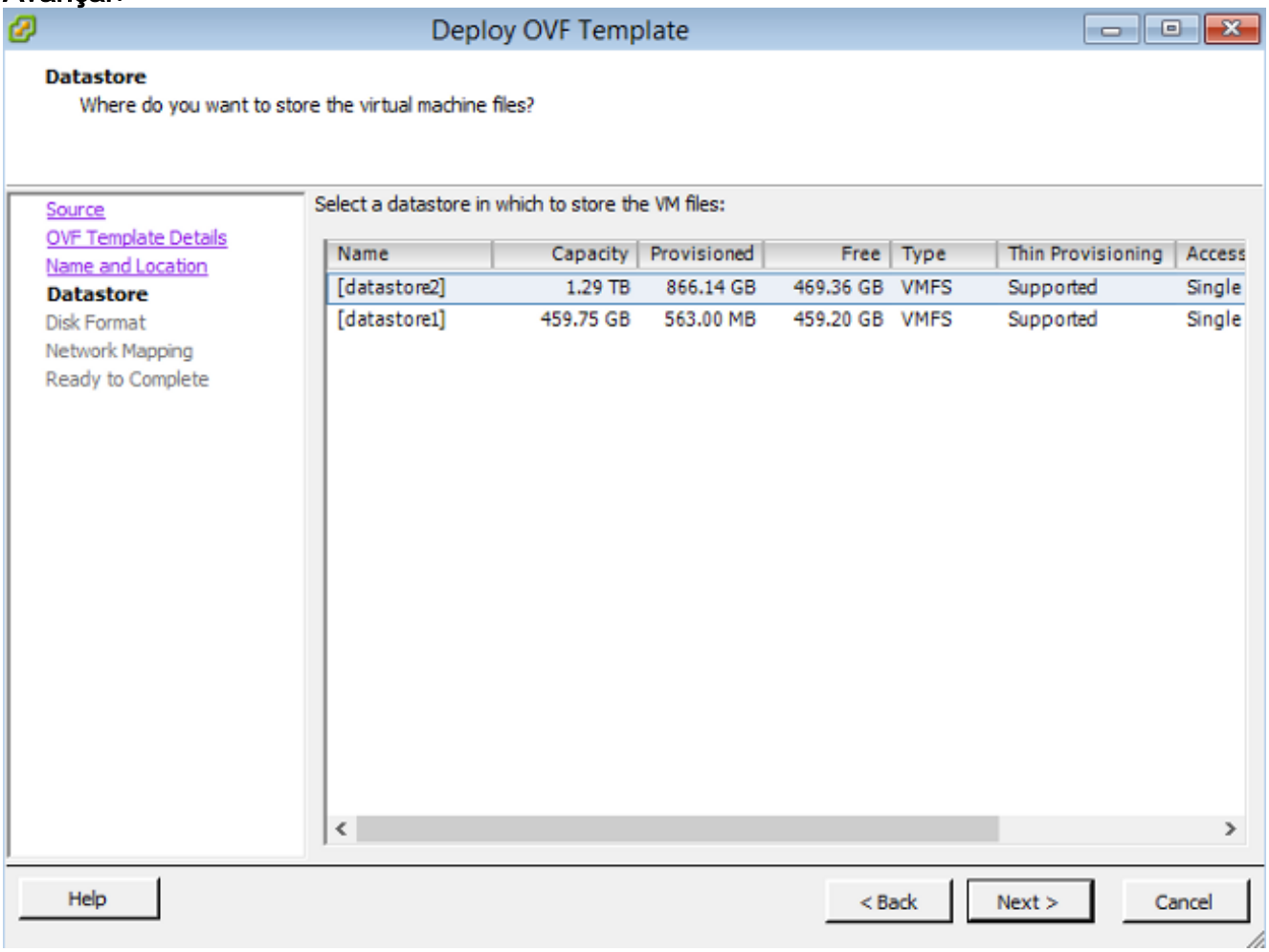
6. Na tela **OVF Template Details**, clique em **Next** para aceitar as configurações padrão.



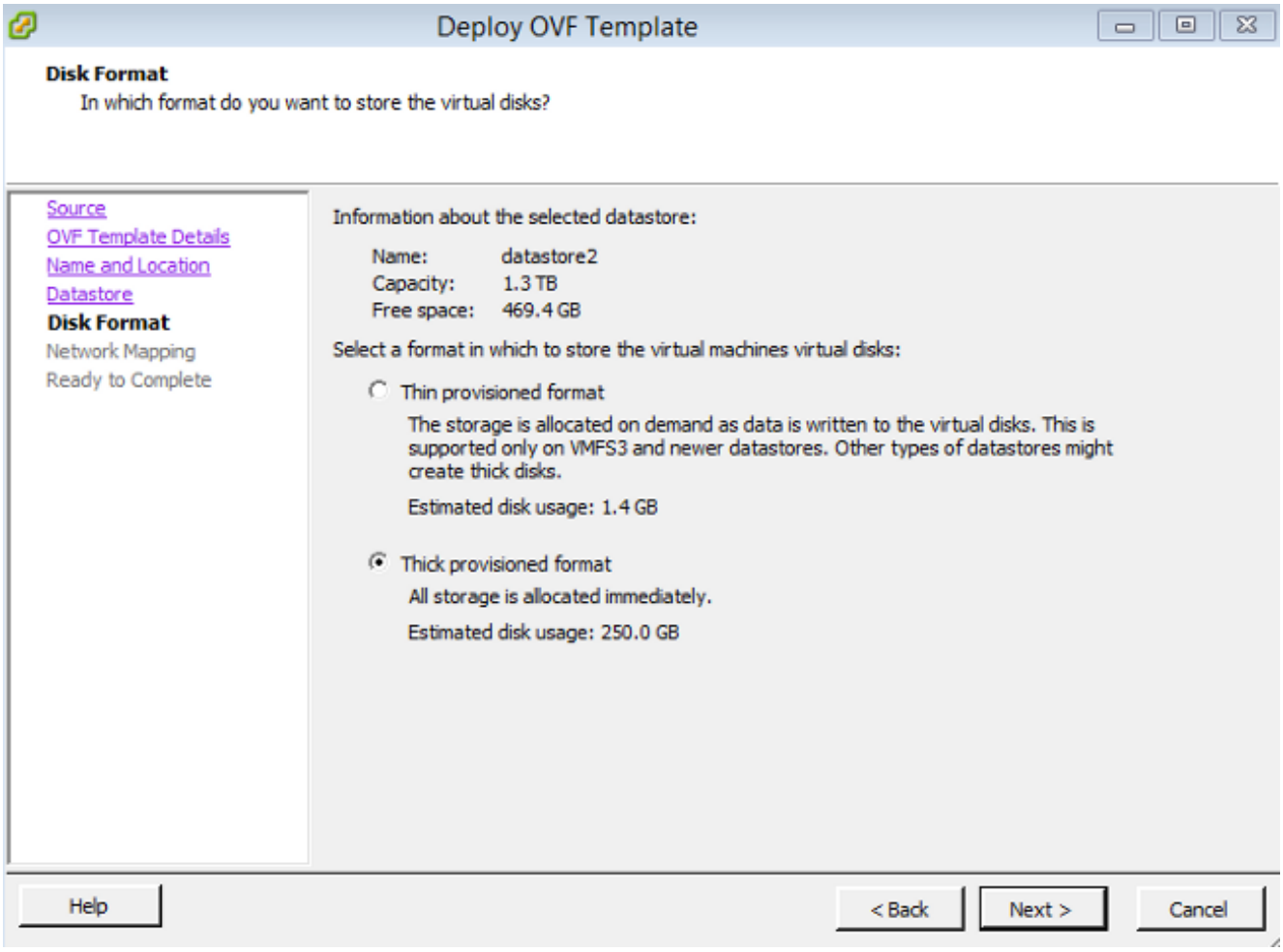
7. Forneça um nome para o Centro de Gerenciamento e clique em **Avançar**.



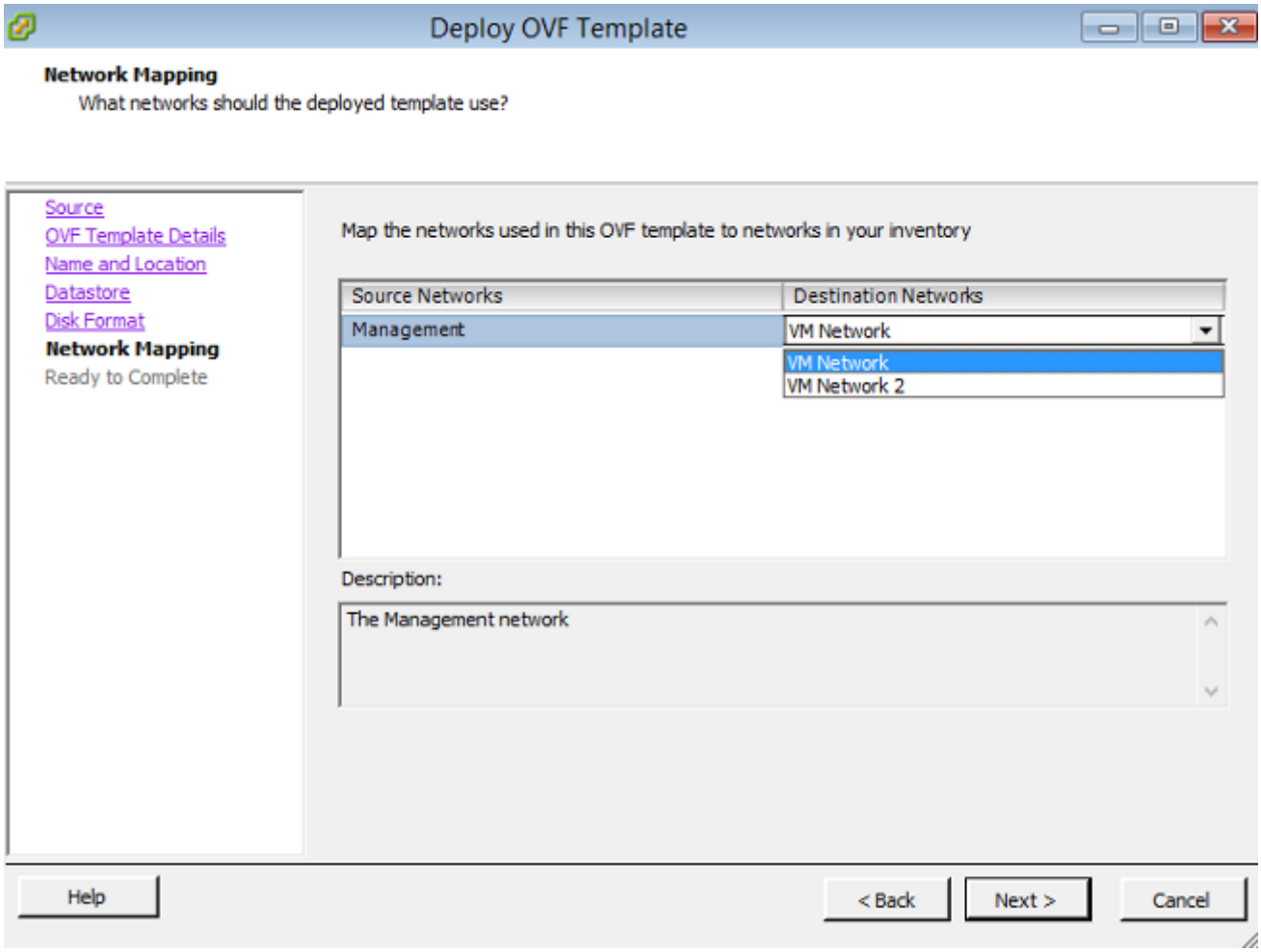
8. Escolha um **Armazenamento de Dados** no qual deseja criar a máquina virtual e clique em **Avançar**.



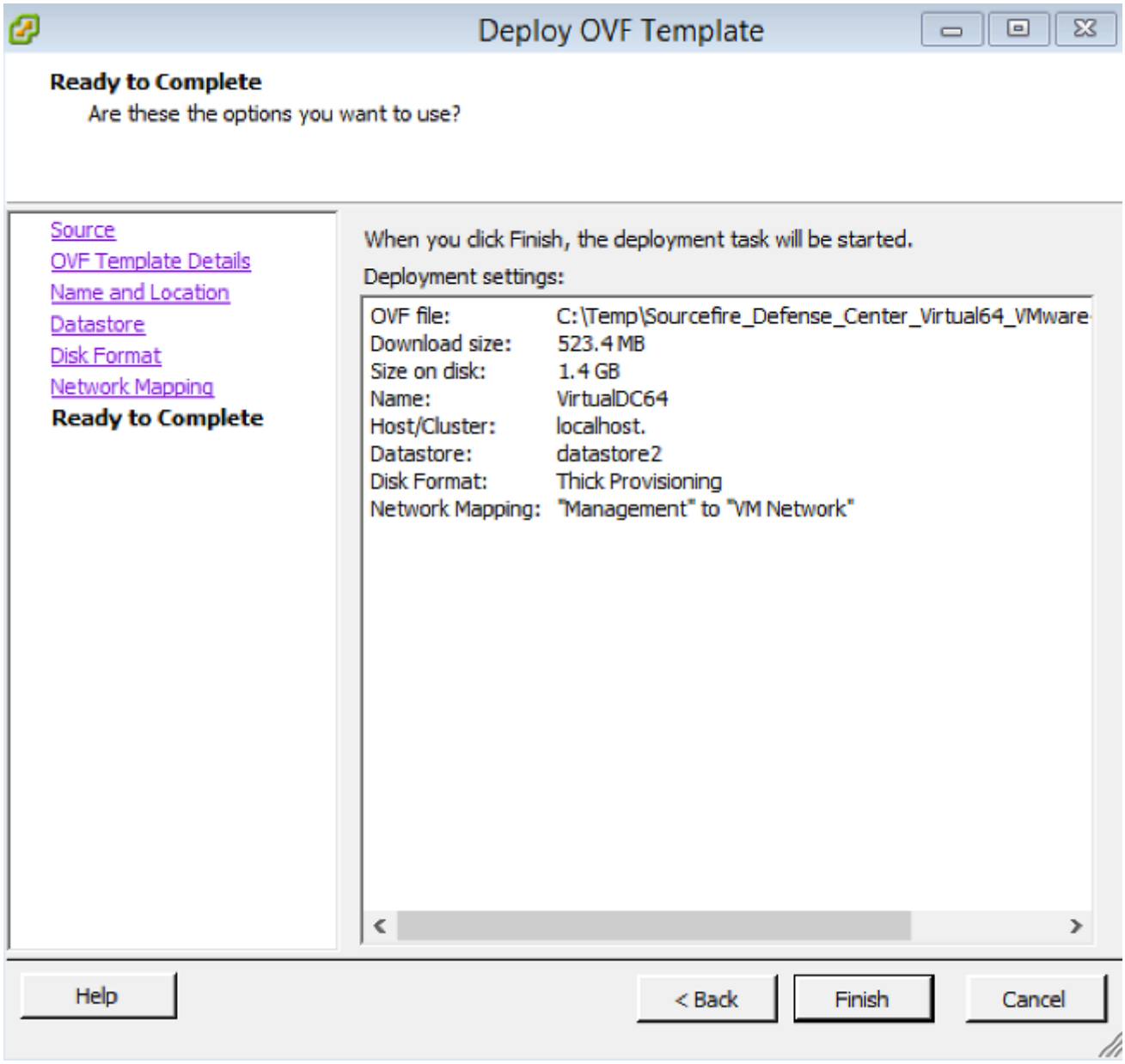
9. Clique no botão de opção **Thick provisioned format** para o **formato do disco** e clique em **Next**. O formato de provisionamento grosso aloca o espaço em disco necessário no momento da criação de um disco virtual, enquanto o formato de provisionamento thin usa espaço sob
demanda.



10. Na seção **Mapeamento de rede**, associe a interface de gerenciamento do FireSIGHT Management Center a uma rede VMware e clique em **Avançar**.

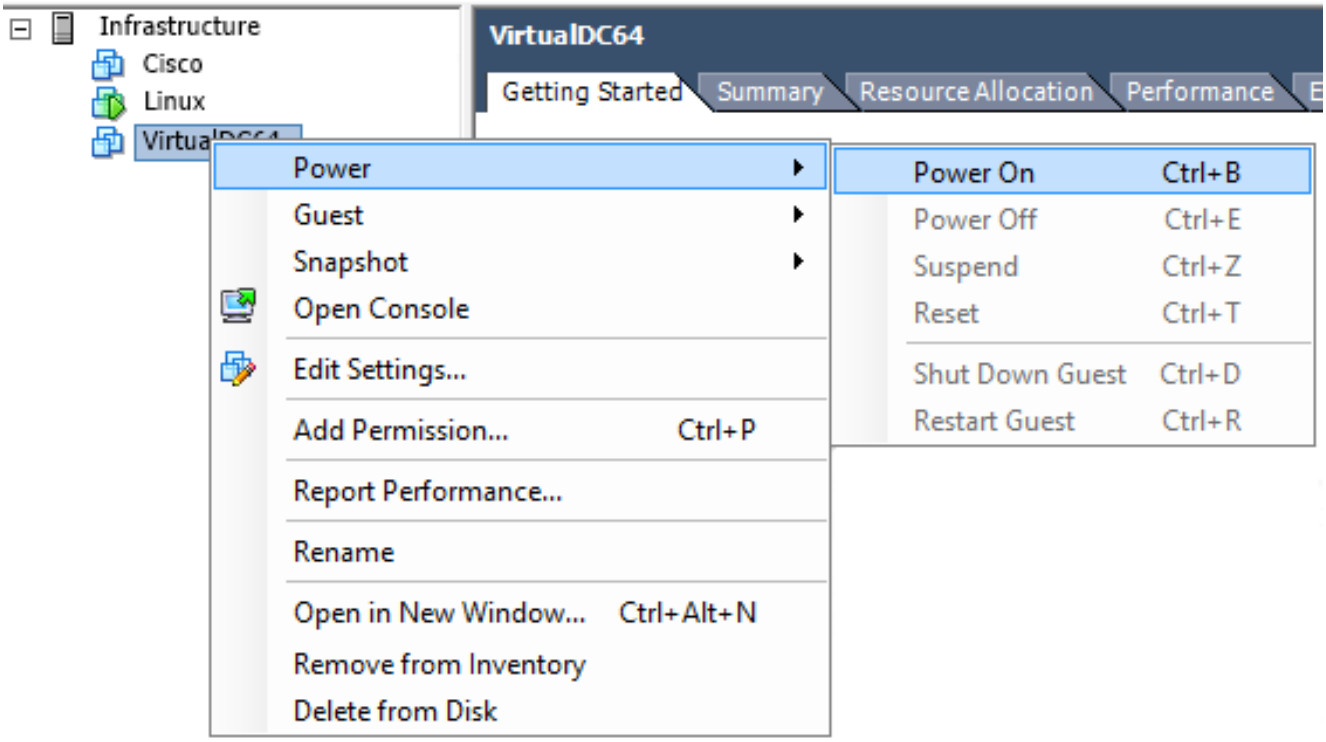


11. Clique em **Finish** para concluir a implantação do modelo OVF.

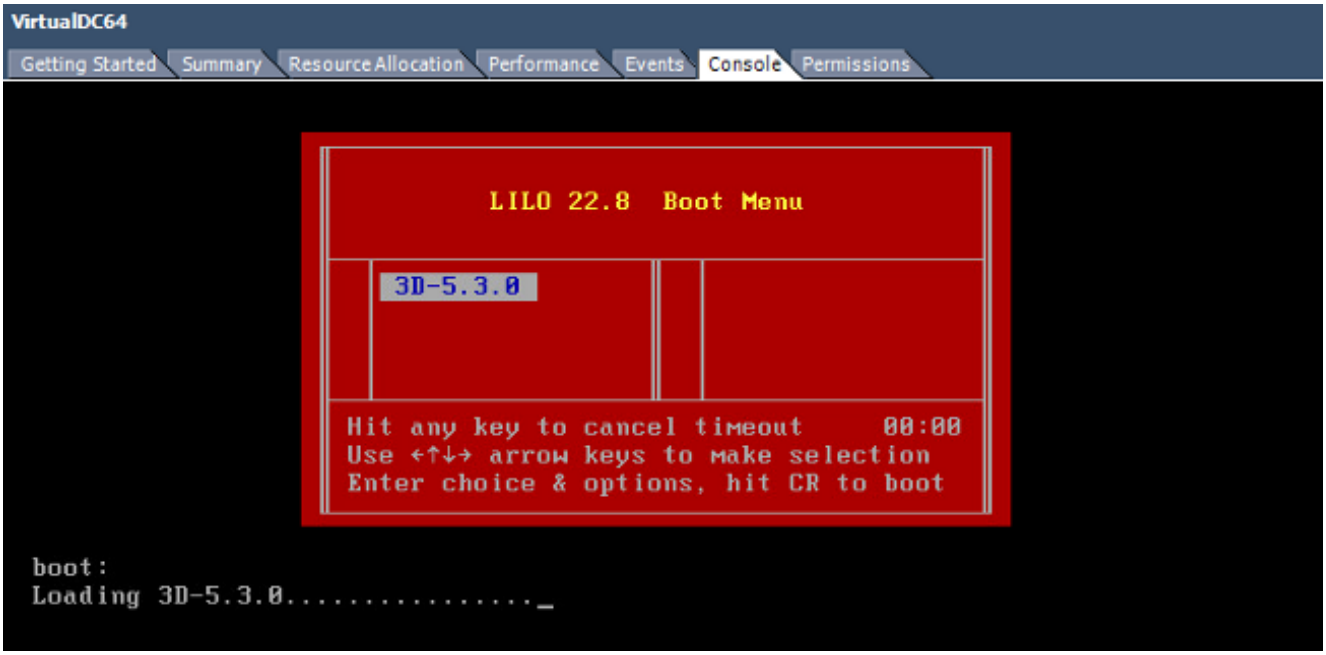


Ligar e concluir a inicialização

1. Navegue até a máquina virtual recém-criada. Clique com o botão direito do mouse no nome do servidor e escolha **Power > Power On** para inicializar o servidor pela primeira vez.



2. Navegue até a guia **Console** para monitorar o console do servidor. O menu de inicialização LILO é
exibido.



Quando a verificação de dados do BIOS for bem-sucedida, o processo de inicialização será iniciado. A primeira inicialização pode levar mais tempo para ser concluída, pois o banco de dados de configuração é inicializado pela primeira
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
_
```

Depois de concluído, você poderá ver uma mensagem para Nenhum dispositivo desse tipo.

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

3. Pressione **Enter** para obter um prompt de login.

```
 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: _
```

Note: Uma mensagem "WRITE SAME failed. Zerando manualmente." pode aparecer após o sistema ser inicializado pela primeira vez. Isso não indica um defeito, indica corretamente que o driver de armazenamento VMware não suporta o comando WRITE SAME. O sistema exibe essa mensagem e continua com um comando fallback para executar a mesma operação.

Definir as configurações de rede

1. No prompt de login Sourcefire3D, use estas credenciais para fazer login: Para a versão 5.xNome de usuário: **admin**Senha: **Sourcefire**Para a versão 6.x e posteriorNome de usuário: **admin**Senha: **Admin123Tip**: Você poderá alterar a senha padrão no processo de configuração inicial na GUI.
2. A configuração inicial da rede é feita com um script. Você precisa executar o script como um usuário raiz. Para alternar para o usuário raiz, digite o **comando sudo su -** junto com a senha **Sourcefire ou Admin123** (para 6.x). Tenha cuidado ao fazer login na linha de comando do Management Center como um usuário raiz.

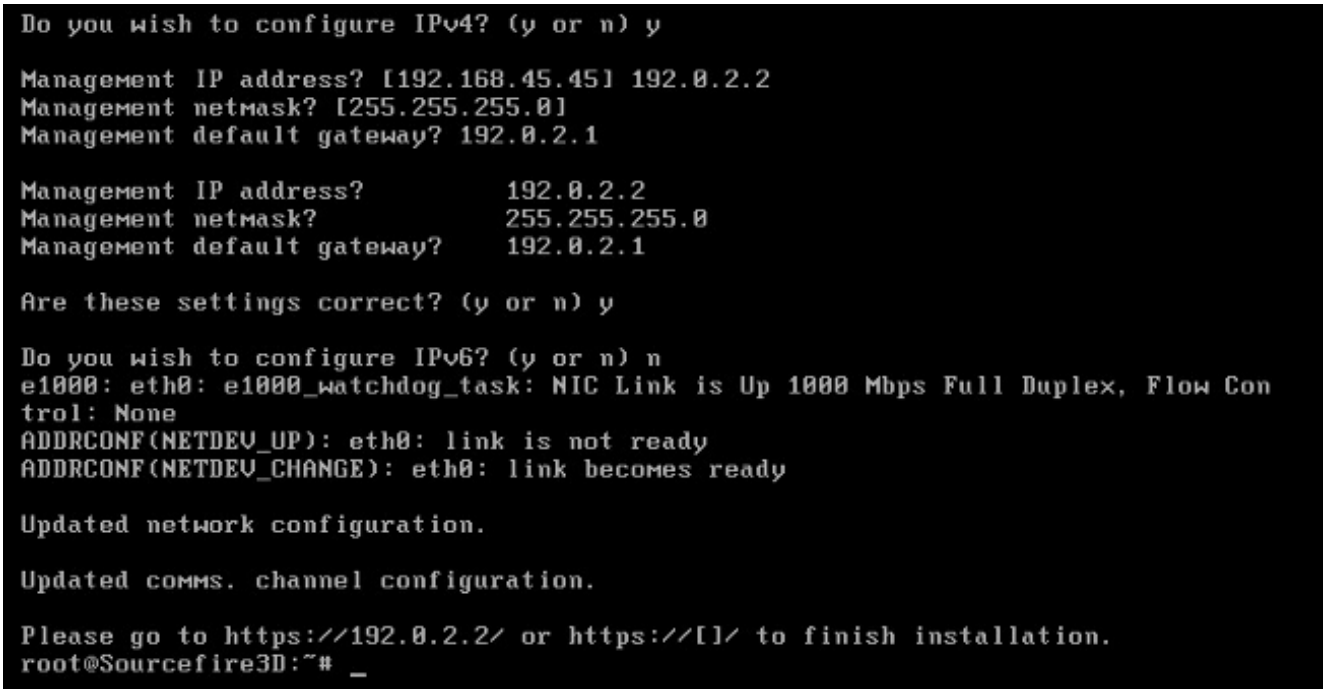
```
admin@Sourcefire3D:~$ sudo su -
Password:
```

3. Para iniciar a configuração de rede, insira o script **configure-network** como root.

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

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

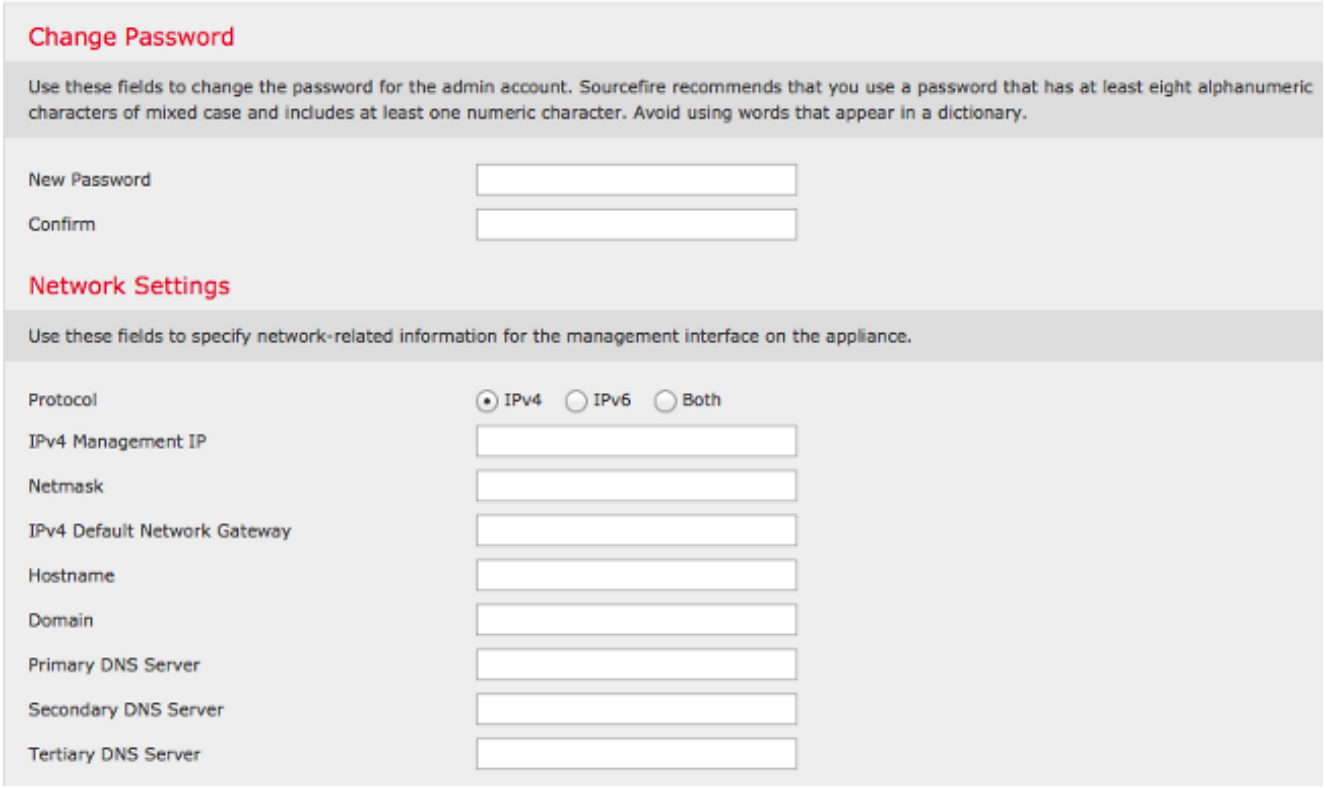
Você será solicitado a fornecer um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão. Depois de confirmar as configurações, o serviço de rede será reiniciado. Como resultado, a interface de gerenciamento fica inativa e volta.



Executar configuração inicial

1. Depois que as configurações de rede estiverem configuradas, abra um navegador da Web e navegue até o IP configurado via HTTPS (https://192.0.2.2 neste exemplo). Autentique o certificado SSL padrão, se solicitado. Use estas credenciais para fazer login:Para a versão 5.x Nome de usuário: **admin**Senha: **Sourcefire**Para a versão 6.x e posteriorNome de usuário: **admin**Senha: **Admin123**
2. Na tela a seguir, todas as seções de configuração da GUI são opcionais, exceto a alteração de senha e a aceitação dos termos de serviço. Se as informações forem conhecidas, é recomendável usar o assistente de configuração para simplificar a configuração inicial do Management Center. Depois de configurado, clique em **Apply** para aplicar a configuração ao Management Center e aos dispositivos registrados. Uma breve visão geral das opções de configuração é a seguinte:**Alterar Senha:** Permite alterar a senha da conta admin padrão. É necessário alterar a senha. **Configurações de rede:** Permite modificar as configurações de rede IPv4 e IPv6 previamente configuradas para a interface de gerenciamento do dispositivo ou da máquina virtual.**Configurações de horário:** é recomendável sincronizar o Management Center com uma fonte NTP confiável. Os sensores IPS podem ser configurados por meio de política de sistema para sincronizar seu tempo com o Management Center. Opcionalmente, o fuso horário e o fuso horário de exibição podem ser definidos manualmente.**Importações de atualização de regra recorrente:** Habilite atualizações de regra de Snort recorrentes e, opcionalmente, instale agora durante a configuração inicial.**Atualizações recorrentes da localização geográfica:** ativar atualizações recorrentes da regra de localização geográfica e, opcionalmente, instalar agora durante a configuração inicial.**Backups automáticos:** agende backups automáticos de configuração.**Configurações da licença:** Adicione a licença do recurso.**Device Registration:** permite que você adicione, licencie e aplique as políticas iniciais de controle de acesso aos dispositivos pré-registrados. O nome do host/endereço IP

e a chave de registro devem corresponder ao endereço IP e à chave de registro configurados no módulo IPS do FirePOWER.**Contrato de licença de usuário final:** é necessária a aceitação do
EULA.



Informações Relacionadas

- [Guia de início rápido virtual do Firepower Management Center para VMware, versão 6.0]
- [Suporte Técnico e Documentação - Cisco Systems]