Implementatie van FireSIGHT Management Center op VMware ESXi

Inhoud

Inleiding

In dit document wordt de eerste installatie beschreven van een FireSIGHT Management Center (ook bekend als Defense Center) dat op VMware ESXi draait. Met een FireSIGHT Management Center kunt u één of meer FirePOWER-applicaties, next-generation inbraakpreventiesysteem (NGIPS) virtuele applicaties en adaptieve security applicatie (ASA) met FirePOWER Services beheren.

> Opmerking: Dit document is een aanvulling op de FireSIGHT System Installatie Guide en de Gebruikersgids. Raadpleeg voor een ESXi-specifieke configuratie en probleemoplossing de VMware-kennisbasis en -documentatie.

Voorwaarden

Gebruikte componenten

De informatie op dit document is gebaseerd op de volgende platforms:

- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center virtuele applicatie
- VMware ESXI 5.0

In dit document verwijst een 'apparaat' naar deze platforms:

- Sourcefire FirePOWER 7000 Series-applicaties en 8000 Series applicaties
- Sourcefire NGIPS virtuele applicaties voor VMware ESXi
- Cisco ASA met FirePOWER Services

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van

elke opdracht begrijpen.

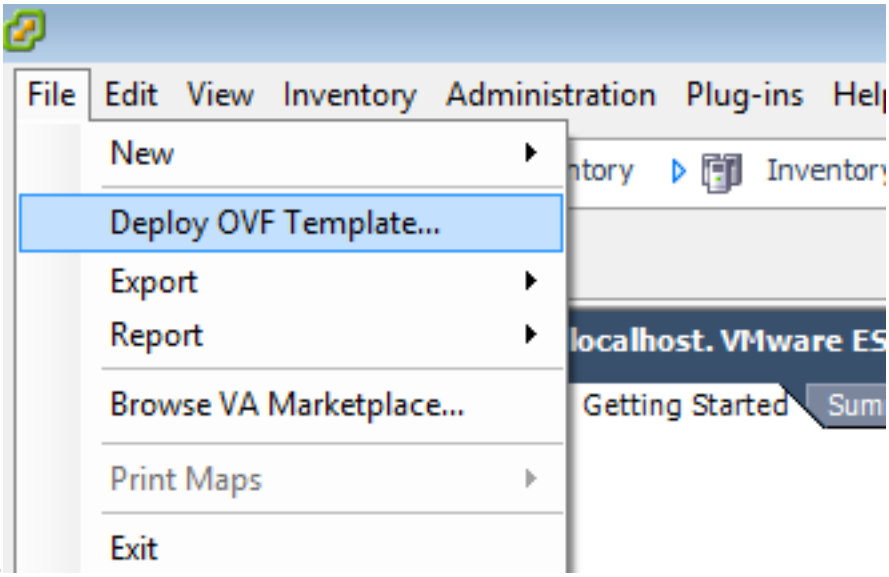
Configuratie

Een OVF-sjabloon implementeren

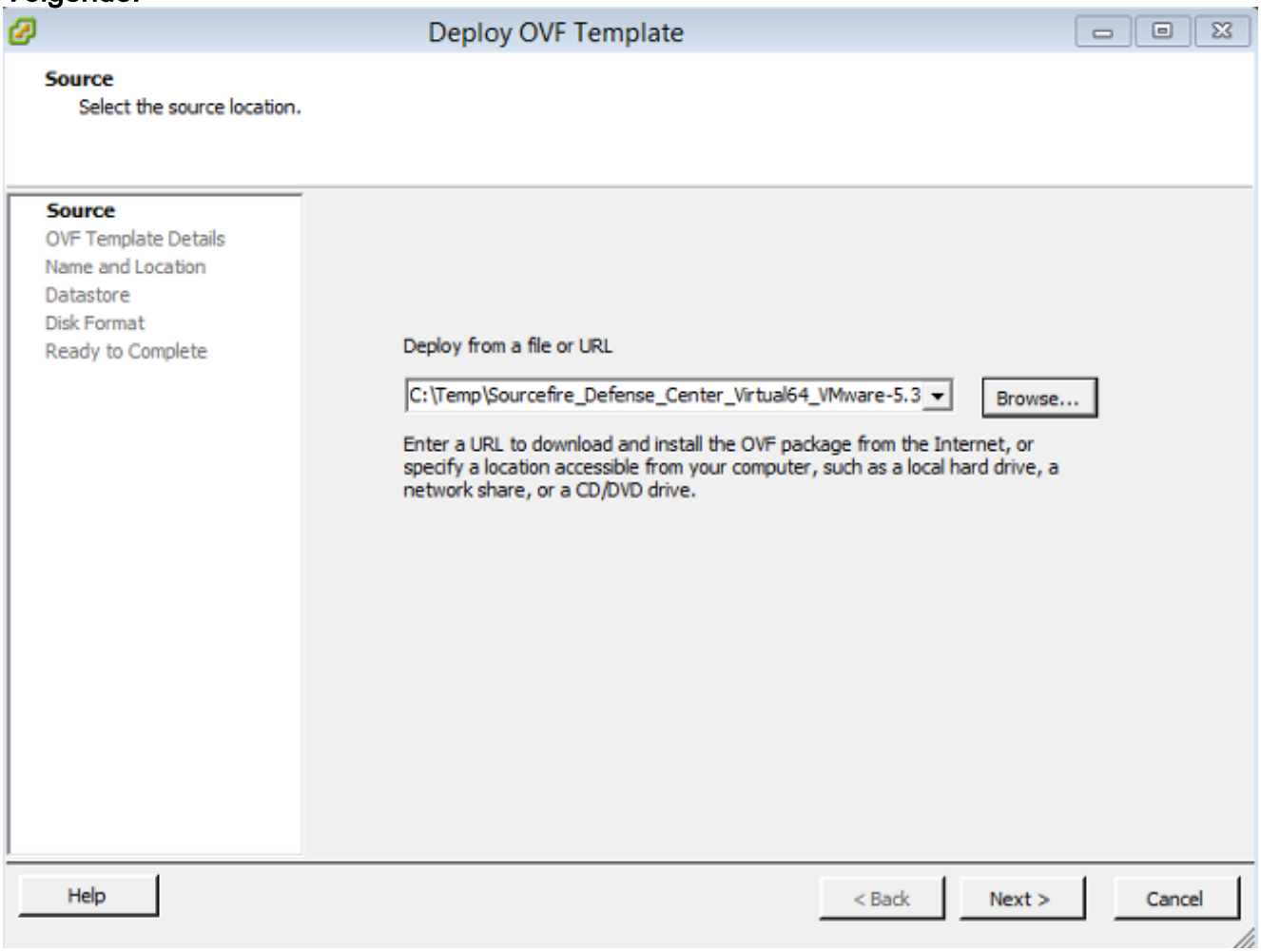
1. Download de **Cisco FireSIGHT Management Center virtuele applicatie** van de Cisco Support & Downloads-website.
2. Trek de inhoud van het tar.gz-bestand naar een lokale map.
3. Sluit aan op uw ESXi-server met een **VMware vSphere-client**.

4. Selecteer **Bestand > OVF-sjabloon implementeren** als u hebt aangemeld bij de vSphere-

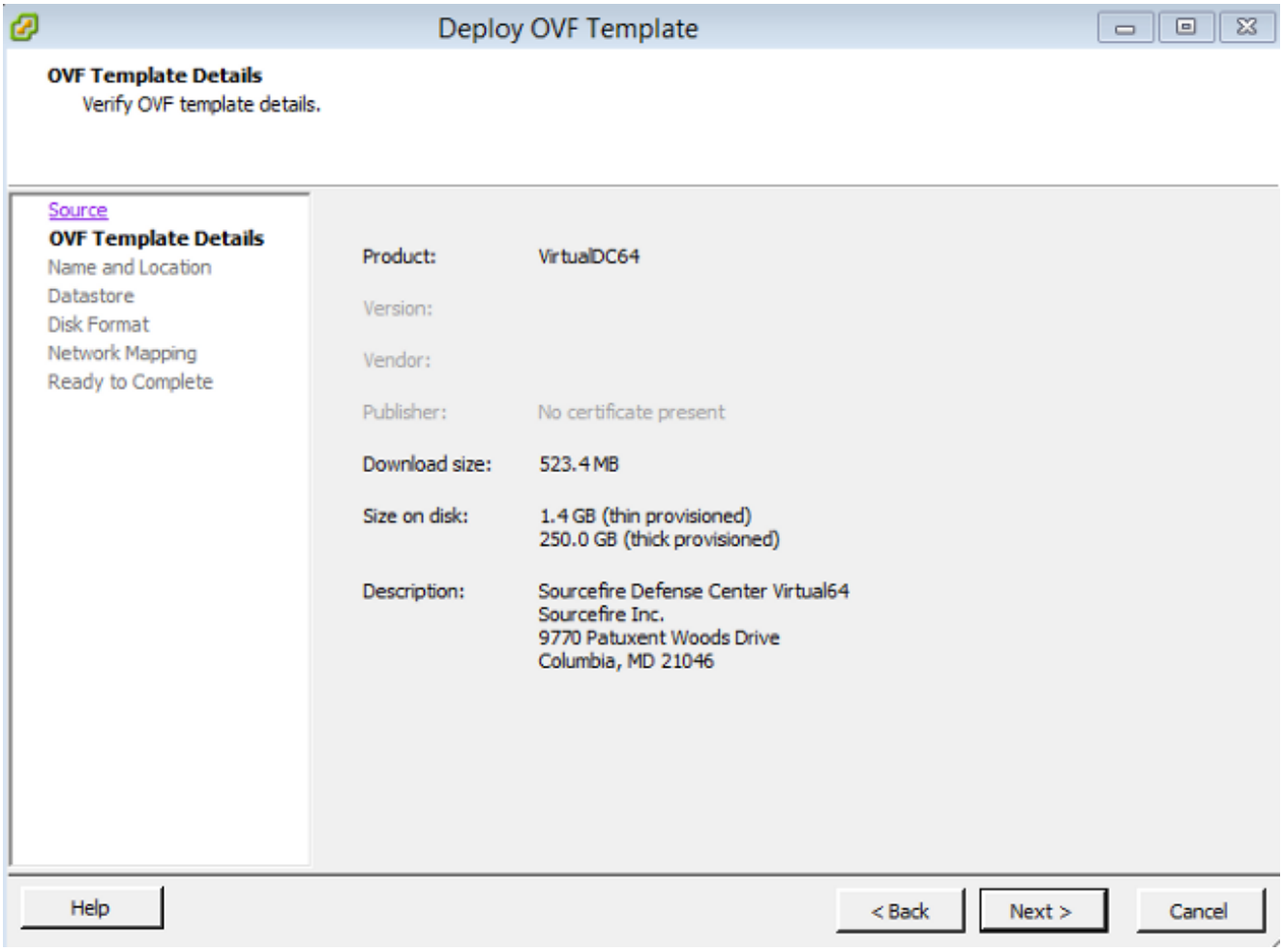
client.



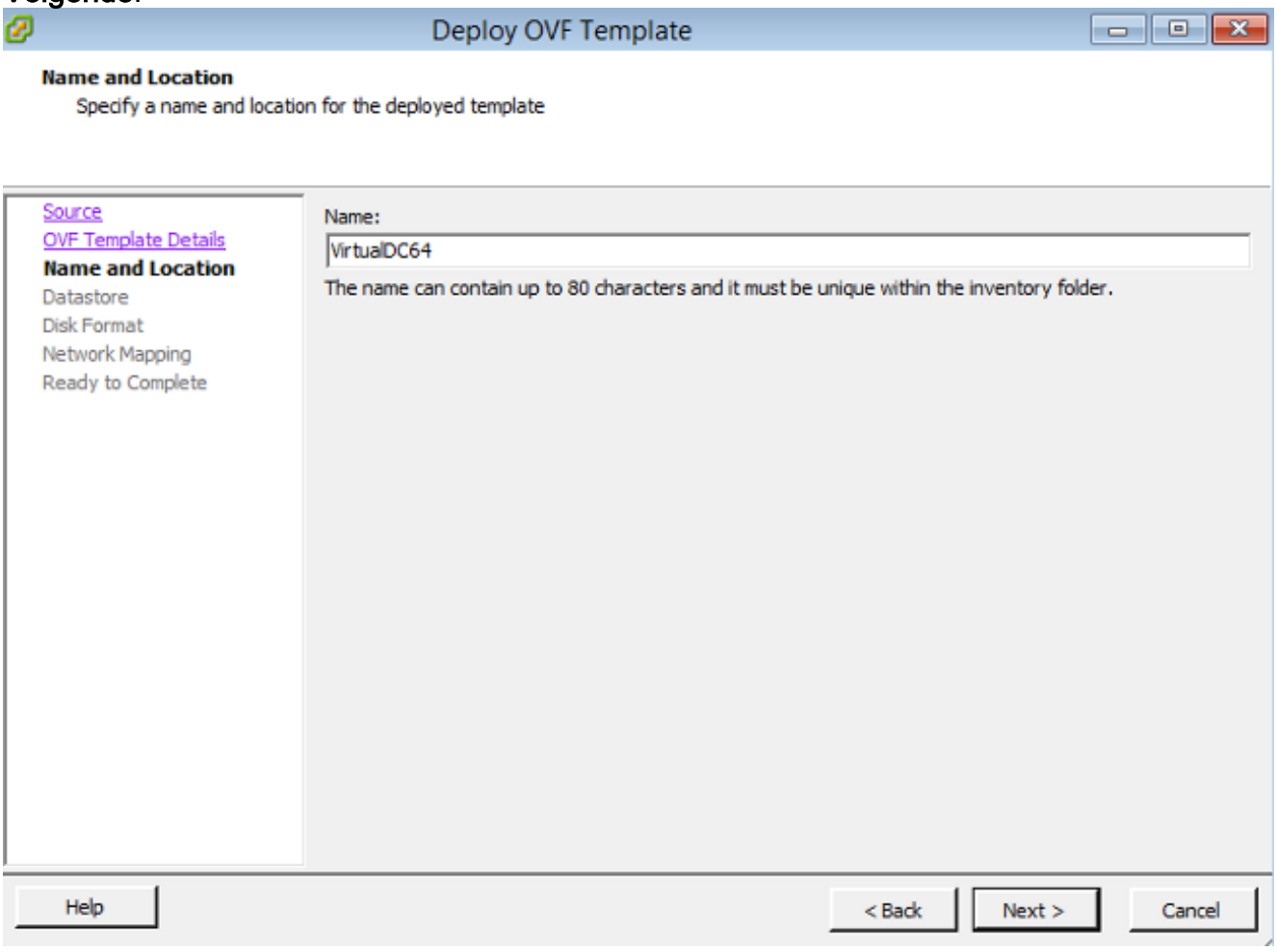
5. Klik op **Bladeren** en lokeer de bestanden die u in stap 2 hebt geëxtraheerd. Kies het OVF-bestand Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.x-xxx.ovf en klik op **Volgende.**



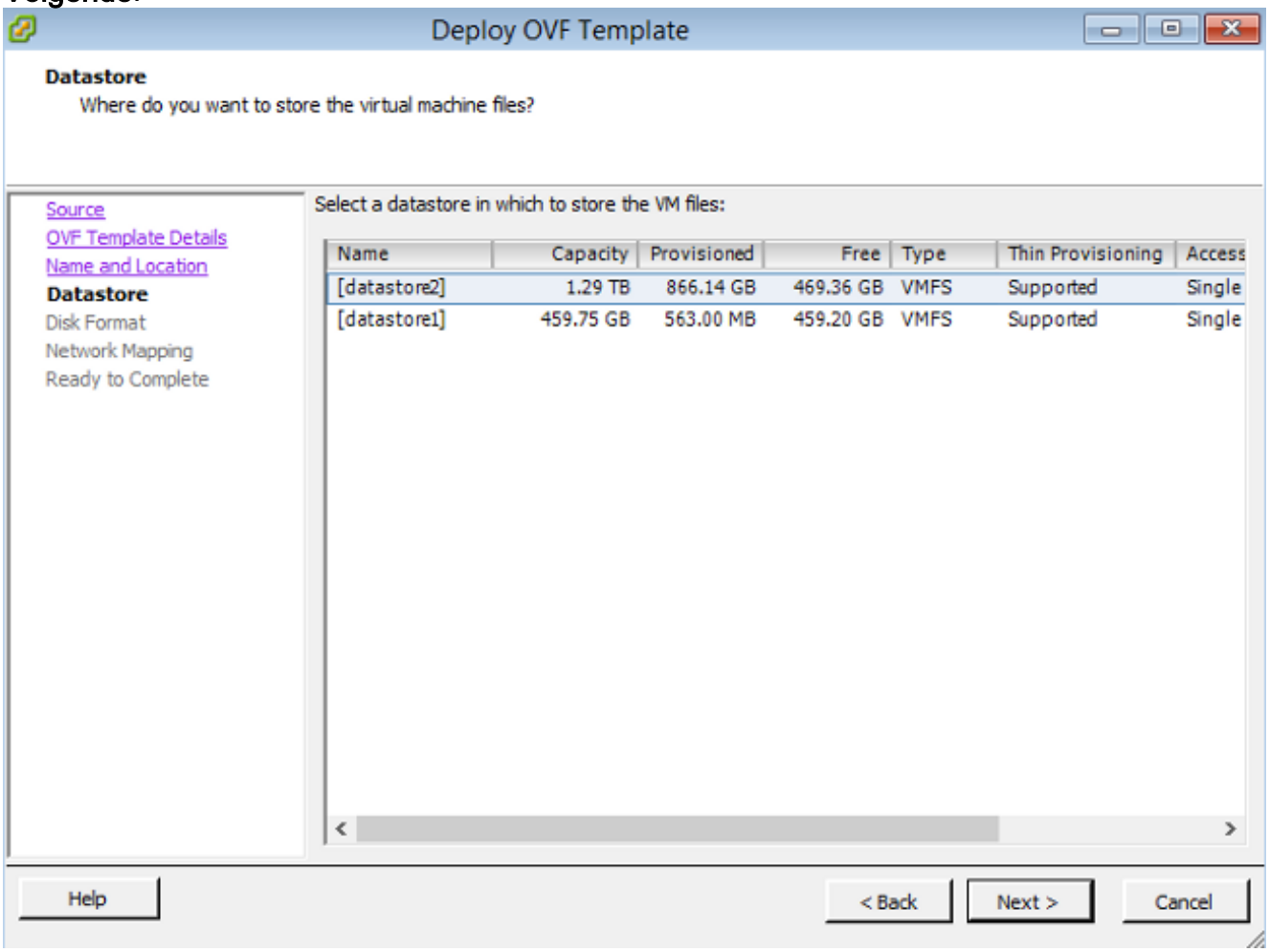
6. Klik in het scherm **OVF Sjabloongegevens** op **Volgende** om de standaardinstellingen te aanvaarden.



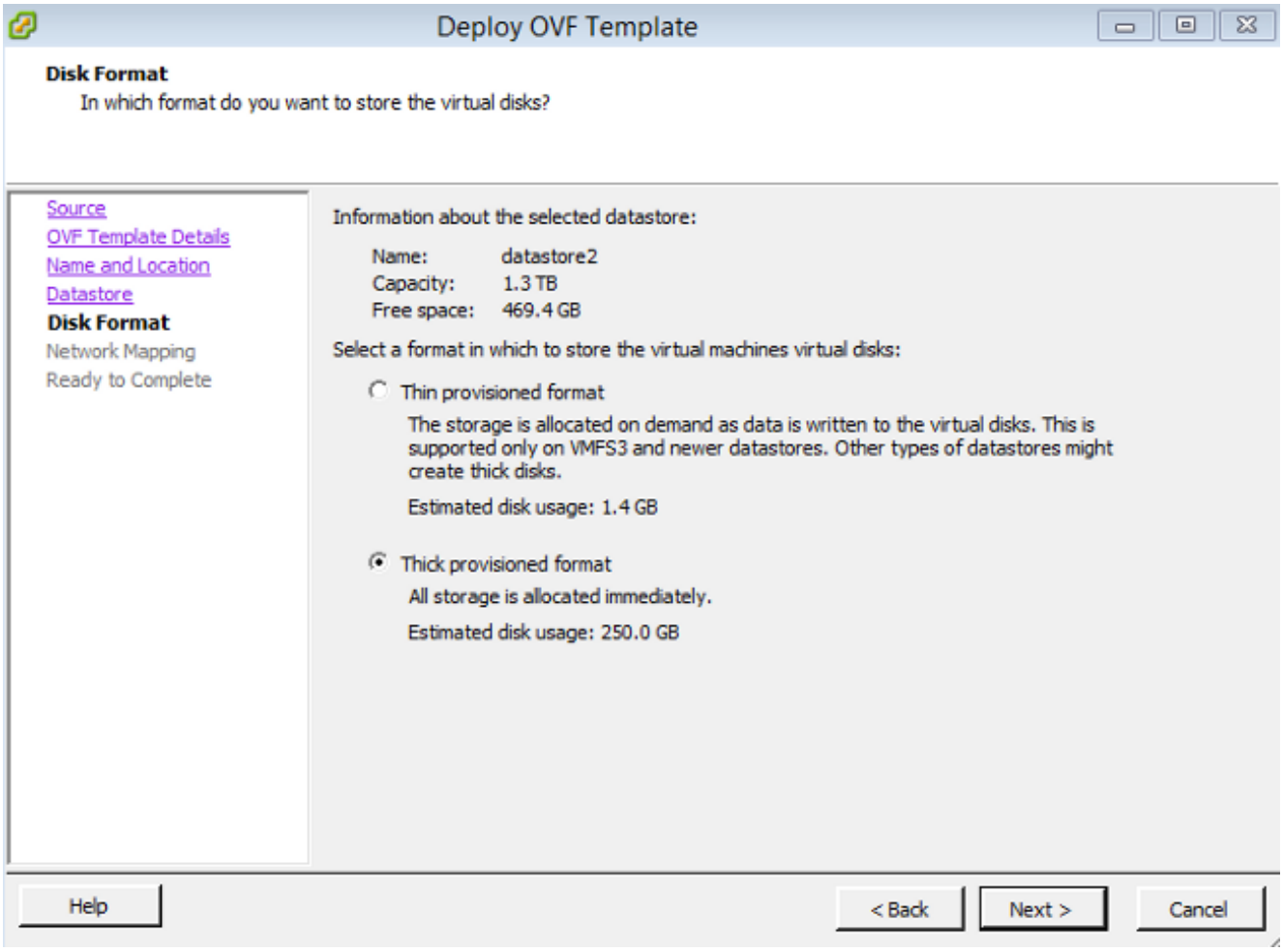
7. Typ een naam voor het beheercentrum en klik op **Volgende**.



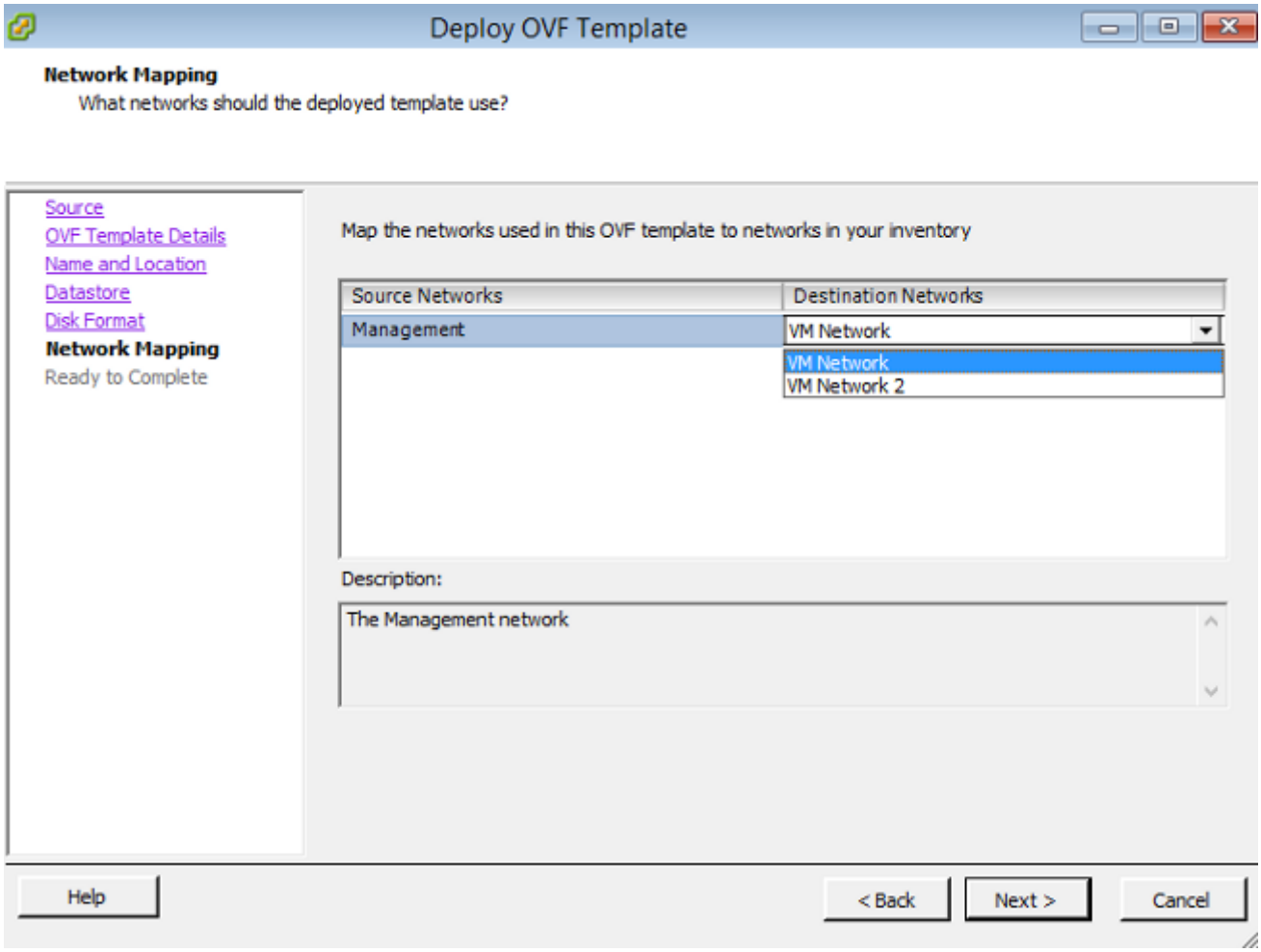
8. Kies een **Datastore** waarop u de virtuele machine wilt maken en klik op **Volgende**.



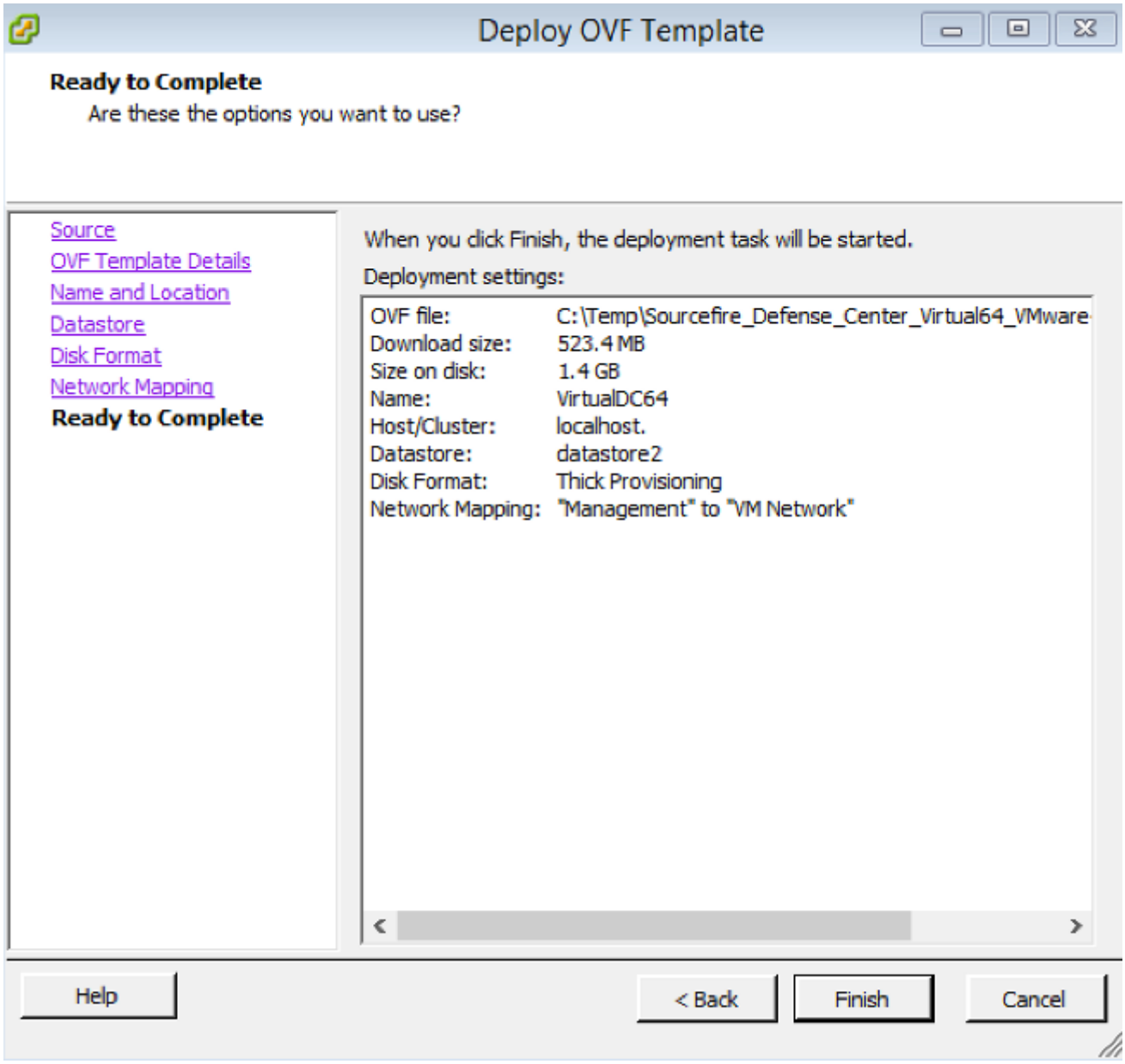
9. Klik op de radioknop **voor dikke** bestandsindeling voor de **schijf** en klik op **Volgende**. Het dikke leveringsformaat wijst de benodigde schijfruimte toe op het moment dat een virtuele schijf wordt gemaakt, terwijl het dunne provisioningformaat op verzoek ruimte gebruikt.



10. Koppel in het gedeelte **Network mapping** de beheerinterface van het FireSIGHT Management Center aan een VMware-netwerk en klik op **Volgende**.

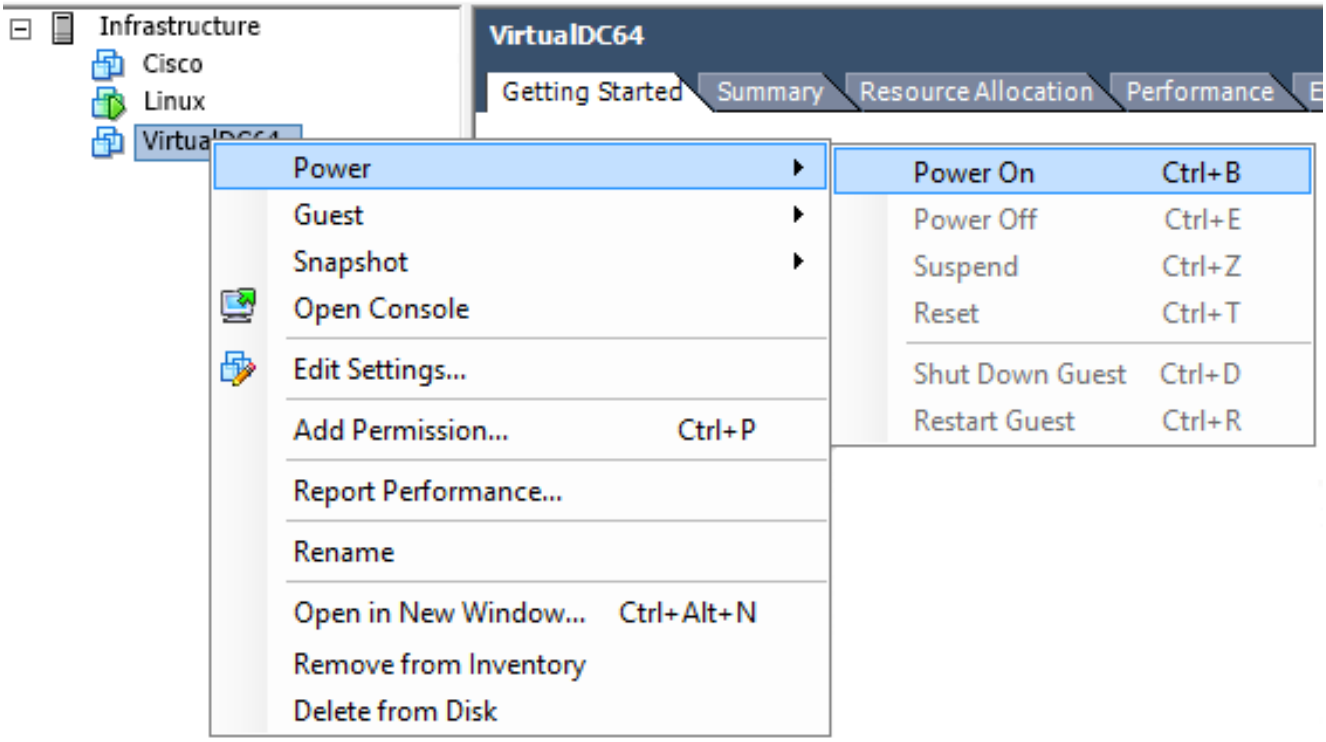


11. Klik op **Voltooien** om de OVF-modelplaatsing te voltooien.

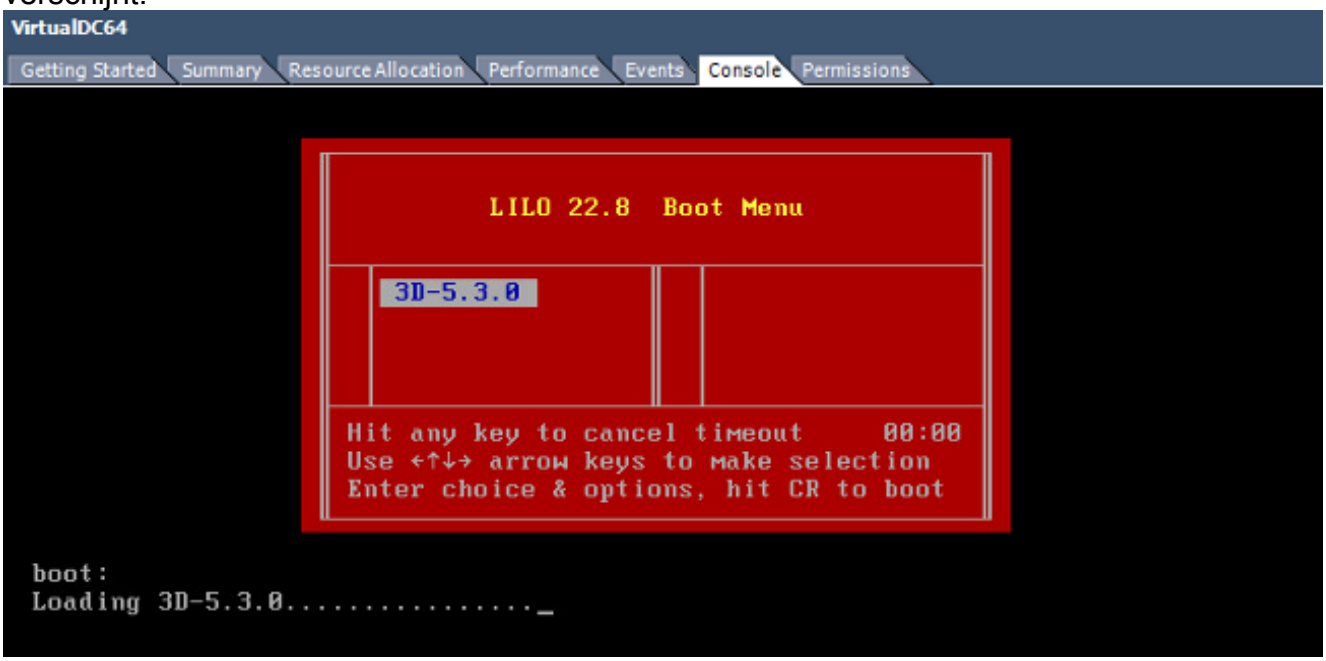


Inschakelen en initialiseren

1. Navigeren naar de nieuwe virtuele machine. Klik met de rechtermuisknop op de servernaam en kies **Aan/uit > Aan/uit** om de server voor het eerst op te starten.



2. Navigeer naar het tabblad **console** om de serverconsole te bewaken. Het LILO Boot Menu verschijnt.



Nadat de door het systeem ingestelde gegevens zijn gecontroleerd, wordt het initialisatieproces gestart. De eerste start kan extra tijd in beslag nemen om te voltooien aangezien de configuratiedatabase voor het eerst wordt geformatteerd.

```
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
_
```

Zodra dit is voltooid, ziet u mogelijk een bericht voor Geen dergelijk apparaat.

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

3. Druk op **ENTER** om een aanmelding te verkrijgen.

```
 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: _
```

Opmerking: Een bericht "SCHRIJF DEZELFDE. handmatig op nul stellen." Mogelijk verschijnt nadat het systeem voor het eerst is opgestart. Dit wijst niet op een defect, het geeft juist aan dat de VMware-opslagstuurprogramma de opdracht SCHRIFTELIJK SAME niet ondersteunt. Het systeem geeft dit bericht weer en gaat met een back-upopdracht verder om dezelfde bewerking uit te voeren.

Netwerkinstellingen configureren

1. Gebruik de inlognaam Sourcefire3D om in te loggen op deze aanmeldingsgegevens: Voor versie 5.xUsername: **besturen**Wachtwoord: **Sourcefire**Voor versie 6.x en laterUsername: **besturen**Wachtwoord: **Admin123Tip**: U kunt het standaardwachtwoord tijdens de eerste installatie in de GUI wijzigen.
2. De eerste configuratie van het netwerk gebeurt met een script. U moet het script als wortel gebruiker uitvoeren. Om op de root gebruiker te kunnen overschakelen, voert u de **sudo su -** opdracht in samen met het wachtwoord **Sourcefire of Admin123** (voor 6.x). Wees voorzichtig met inloggen in de opdrachtregel van het beheercentrum als basisgebruiker.

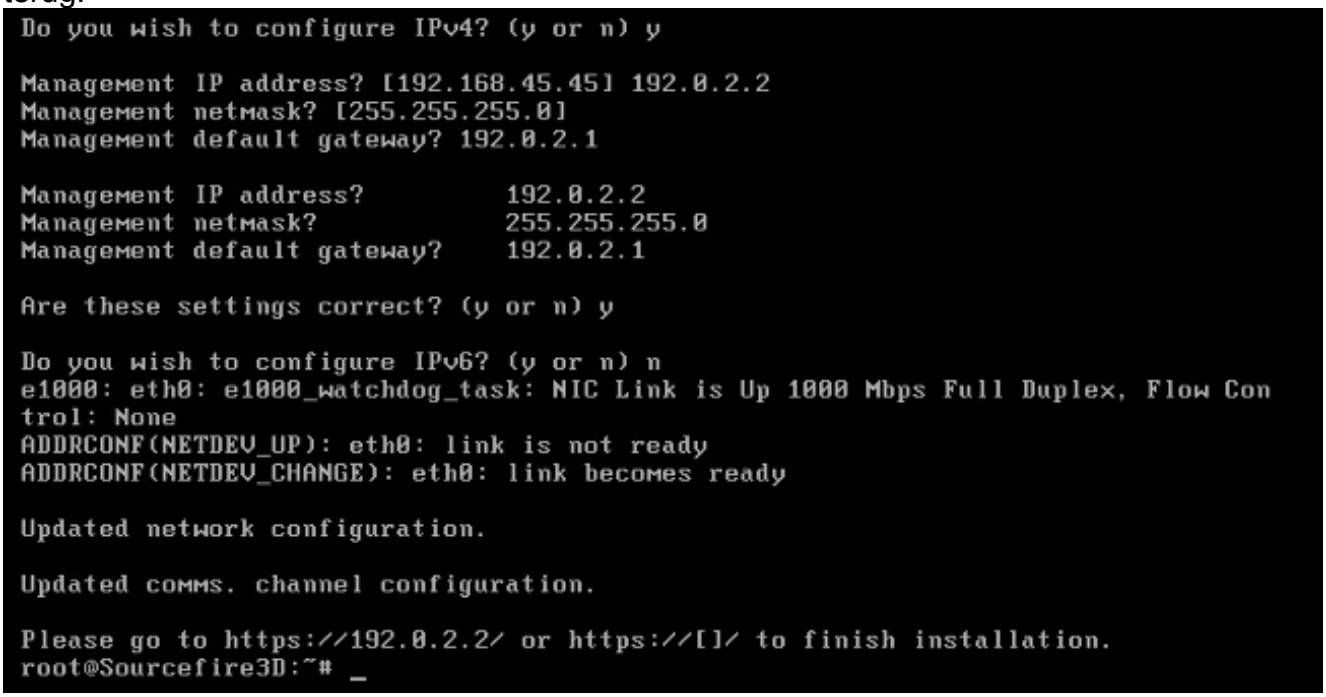
```
admin@Sourcefire3D:~$ sudo su -
Password:
```

3. Om met de netwerkconfiguratie te beginnen, voer het **configuratie-netwerk** script als root in.

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

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

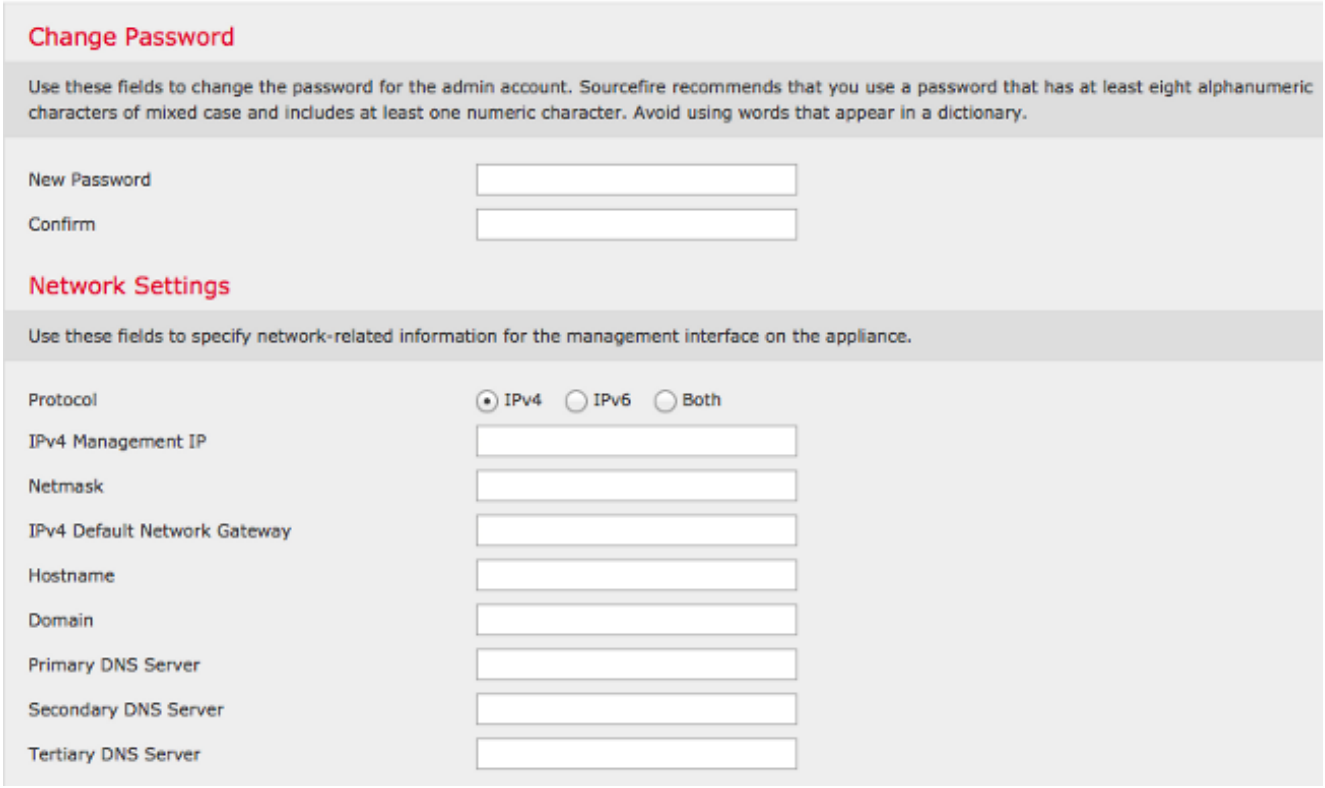
U zal worden gevraagd een IP-adres, netmasker en standaardgateway te verstrekken. Zodra u de instellingen hebt bevestigd, start de netwerkservice opnieuw. Als resultaat hiervan gaat de managementinterface omlaag en komt dan
terug.



Eerste installatie uitvoeren

1. Nadat de netwerkinstellingen zijn ingesteld, opent u een webbrowser en bladert u naar de geconfigureerde IP via HTTPS (https://192.0.2.2 in dit voorbeeld). Verifieer het standaard SSL-certificaat indien dit wordt gevraagd. Gebruik deze aanmeldingsgegevens om in te loggen:Voor versie 5.x Username: **besturen**Wachtwoord: **Sourcefire**Voor versie 6.x en laterUsername: **besturen**Wachtwoord: **Admin123**
2. Op het volgende scherm zijn alle GUI-configuratiesecties optioneel, behalve de wachtwoordwijziging en de acceptatie van de servicebepalingen. Als de informatie bekend is, wordt het aanbevolen de installatiewizard te gebruiken om de eerste configuratie van het Management Center te vereenvoudigen. Klik na configuratie op **Toepassen** om de configuratie toe te passen op het Management Center en de geregistreerde apparaten. Een kort overzicht van de configuratieopties is als volgt:**Wachtwoord wijzigen** Hiermee kunt u het wachtwoord wijzigen voor de standaard-beheeraccount. Het wachtwoord moet worden gewijzigd. **Netwerkinstellingen:** Hiermee kunt u de eerder ingestelde IPv4- en IPv6-netwerkinstellingen aanpassen voor de beheerinterface van het apparaat of de virtuele machine.**Tijdinstellingen:** Aanbevolen wordt om het Management Center te synchroniseren met een betrouwbare NTP-bron. De IPS sensoren kunnen via systeembeleid worden geconfigureerd om hun tijd met het Management Center te synchroniseren. Optioneel kan de tijd- en weergavetijdzone handmatig worden ingesteld.**Recurring Rule Update:** Kunt u terugkerende updates voor de kortregel inschakelen en desgewenst tijdens de eerste installatie nu installeren.**Herstel van geolocatie-updates:** Schakel terugkerende geo-locatiereedschappen in en installeer nu optioneel tijdens de eerste instelling.**Automatische back-ups:** Schema's voor automatische configuratie.**Instellingen licentie:** Voeg de functiekaart toe.**Apparaatregistratie:** Hier kunt u beleid voor toegangscontrole toevoegen, licentiëren en toepassen op gepreregistreerde apparaten. De hostname/IP-adres en de

registratiesleutel moeten overeenkomen met het IP-adres en de registratiesleutel die in de FirePOWER IPS-module zijn ingesteld.**Gebruiksrechtovereenkomst:** Aanvaarding van de EULA is
vereist.



Gerelateerde informatie

- [Firepower Management Center Virtual Quick Start Guide voor VMware, versie 6.0]
- [Technische ondersteuning en documentatie – Cisco Systems]