Развертывания центра управления FireSIGHT на VMware ESXi

Содержание

Введение

Этот документ описывает начальную настройку Центра управления FireSIGHT (также известный как Центр Защиты), который работает на VMware ESXi. Центр управления FireSIGHT позволяет вам управлять одним или более Устройствами FirePOWER, Система предотвращения вторжений следующего поколения (NGIPS) устройства Viirtual и устройство адаптивной защиты (ASA) с FirePOWER Services.

> **Примечание:** Этот документ является дополнением Руководства по установке системы FireSIGHT и Руководства пользователя. Для определенного вопроса о конфигурации и устранении проблем ESXi обратитесь к базе знаний VMware и документации.

Предварительные условия

Используемые компоненты

Информация об этом документе основывается на этих платформах:

- Центр управления Cisco FireSIGHT
- Виртуальное устройство центра управления Cisco FireSIGHT
- VMware ESXI 5.0

В этом документе "устройство" обращается к этим платформам:

- Sourcefire FirePOWER устройства серии 7000 и устройства серии 8000
- Sourcefire виртуальные устройства NGIPS для VMware ESXi
- Cisco ASA 5500-X Series с сервисом FirePOWER

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить

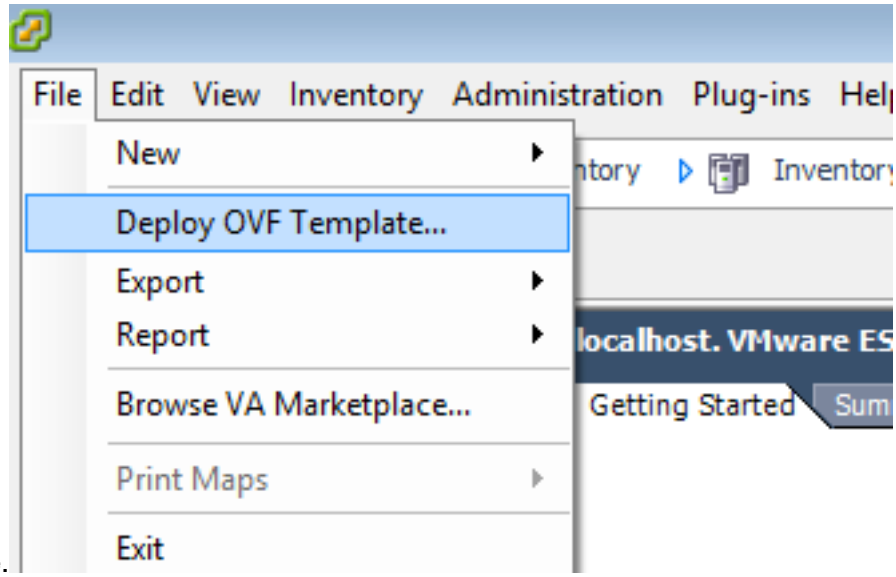
потенциальное воздействие всех команд до их использования.

!--- конфигурацию

Разверните шаблон OVF

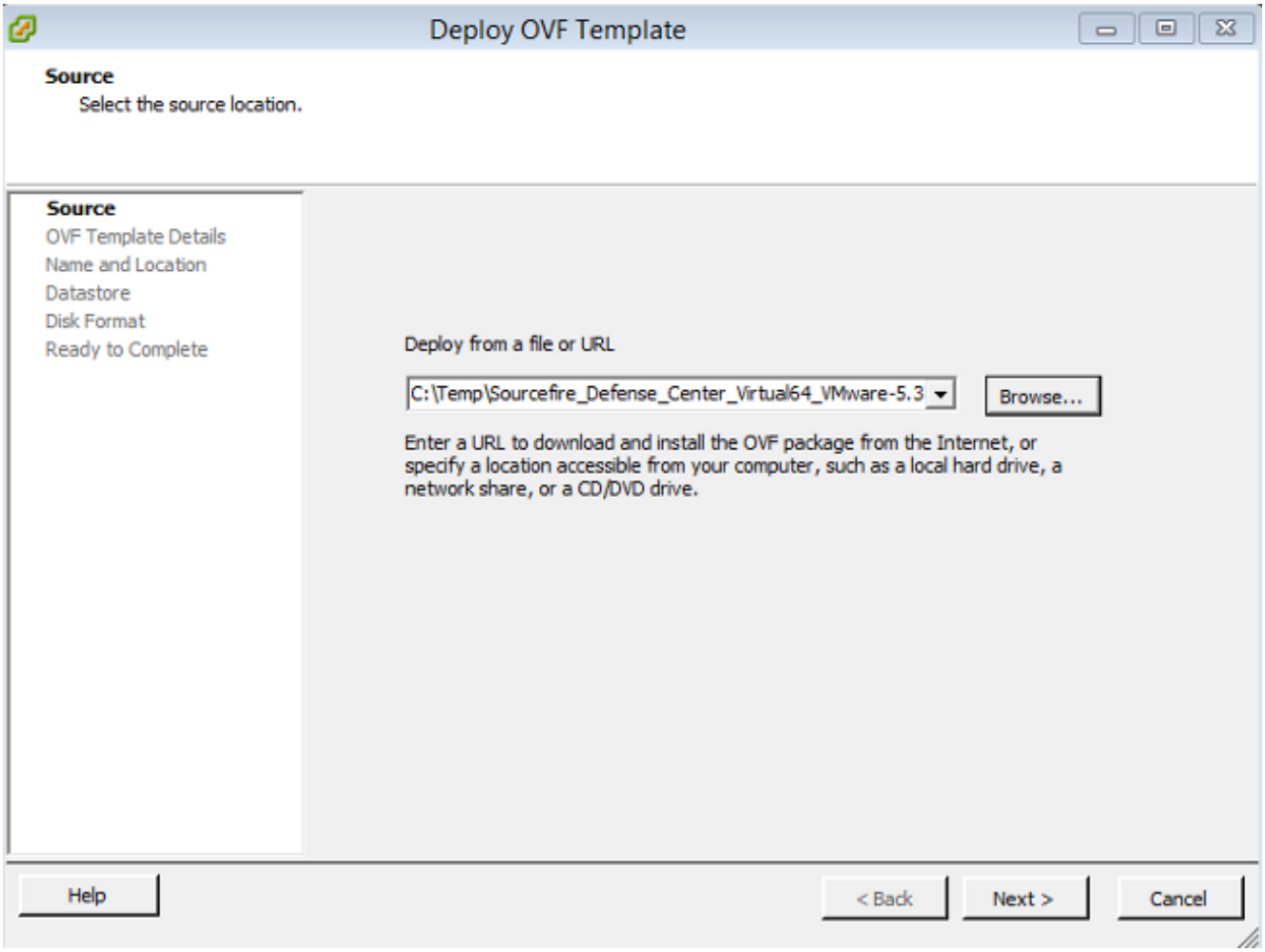
1. Загрузите **Виртуальное устройство Центра управления Cisco FireSIGHT** от узла Cisco Support & Downloads.
2. Извлеките содержание `tar.gz` файла к локальному каталогу.
3. Соединитесь со своим сервером ESXi с **Клиентом VMware vSphere**.

4. Как только вы входите vSphere Клиенту, выбираете **File> Deploy OVF**

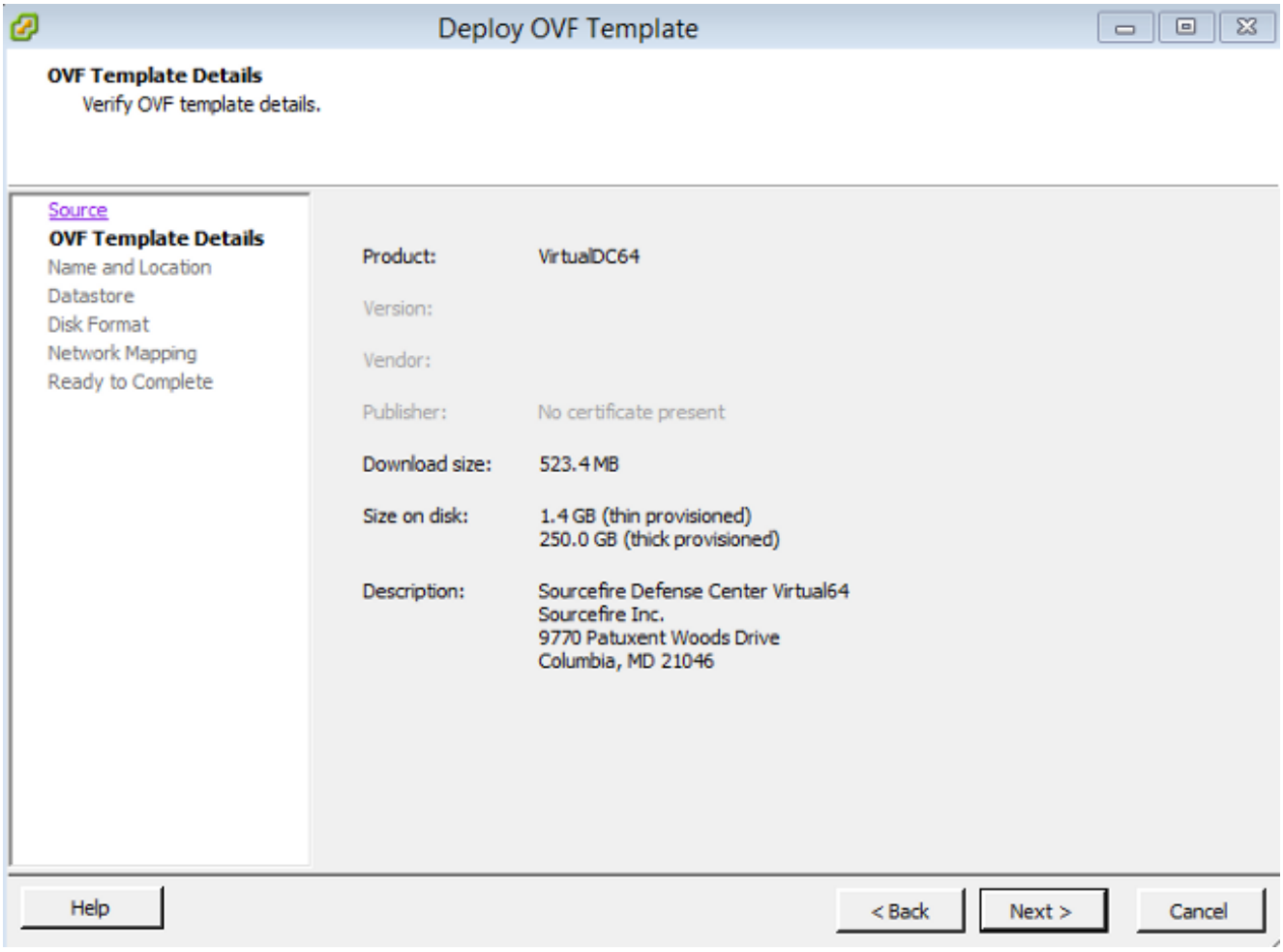


Template.

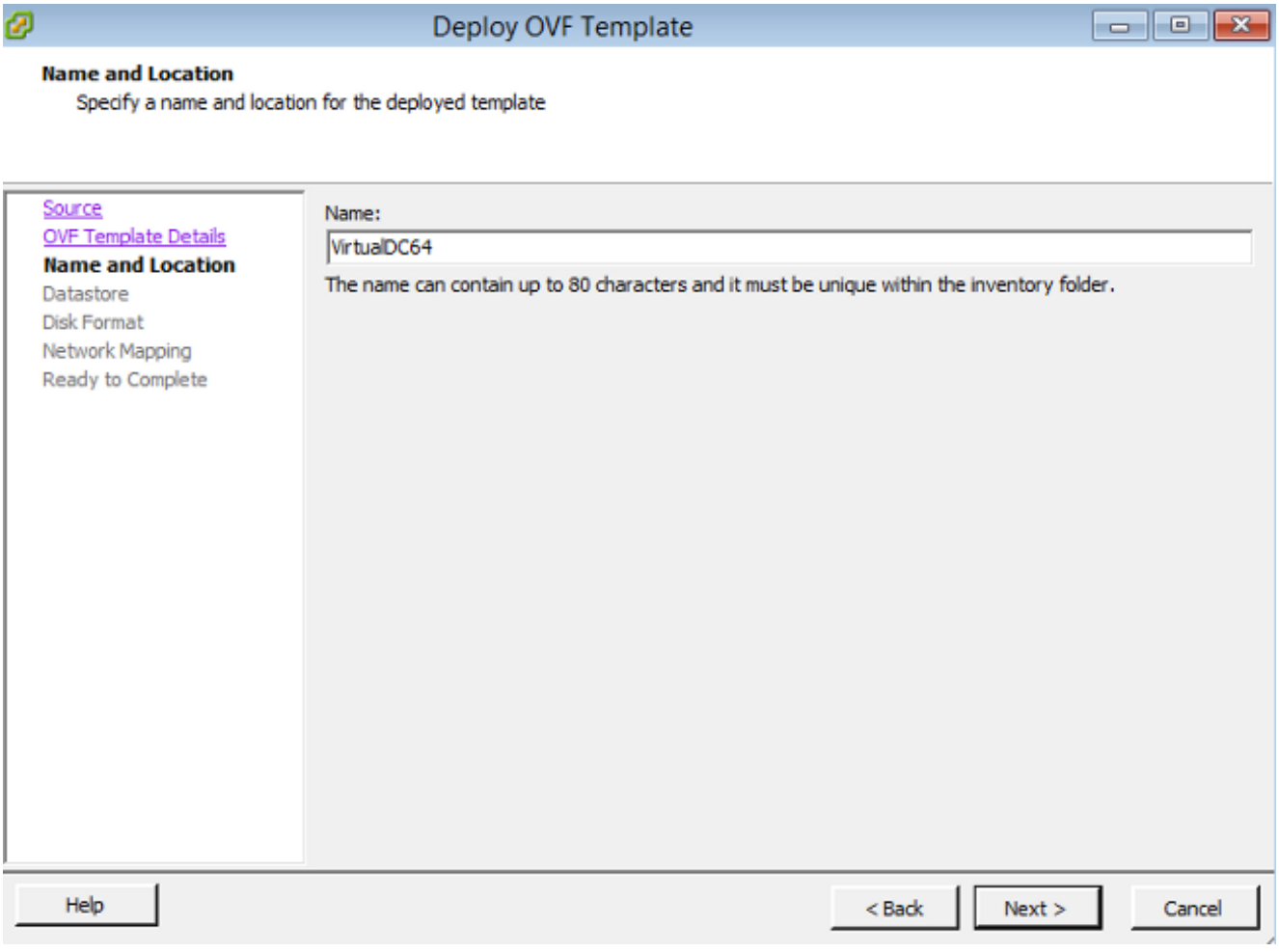
5. Нажмите **Browse** и найдите файлы, которые вы извлекли в шаге 2. Выберите файл OVF `Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf` и нажмите **Next.**



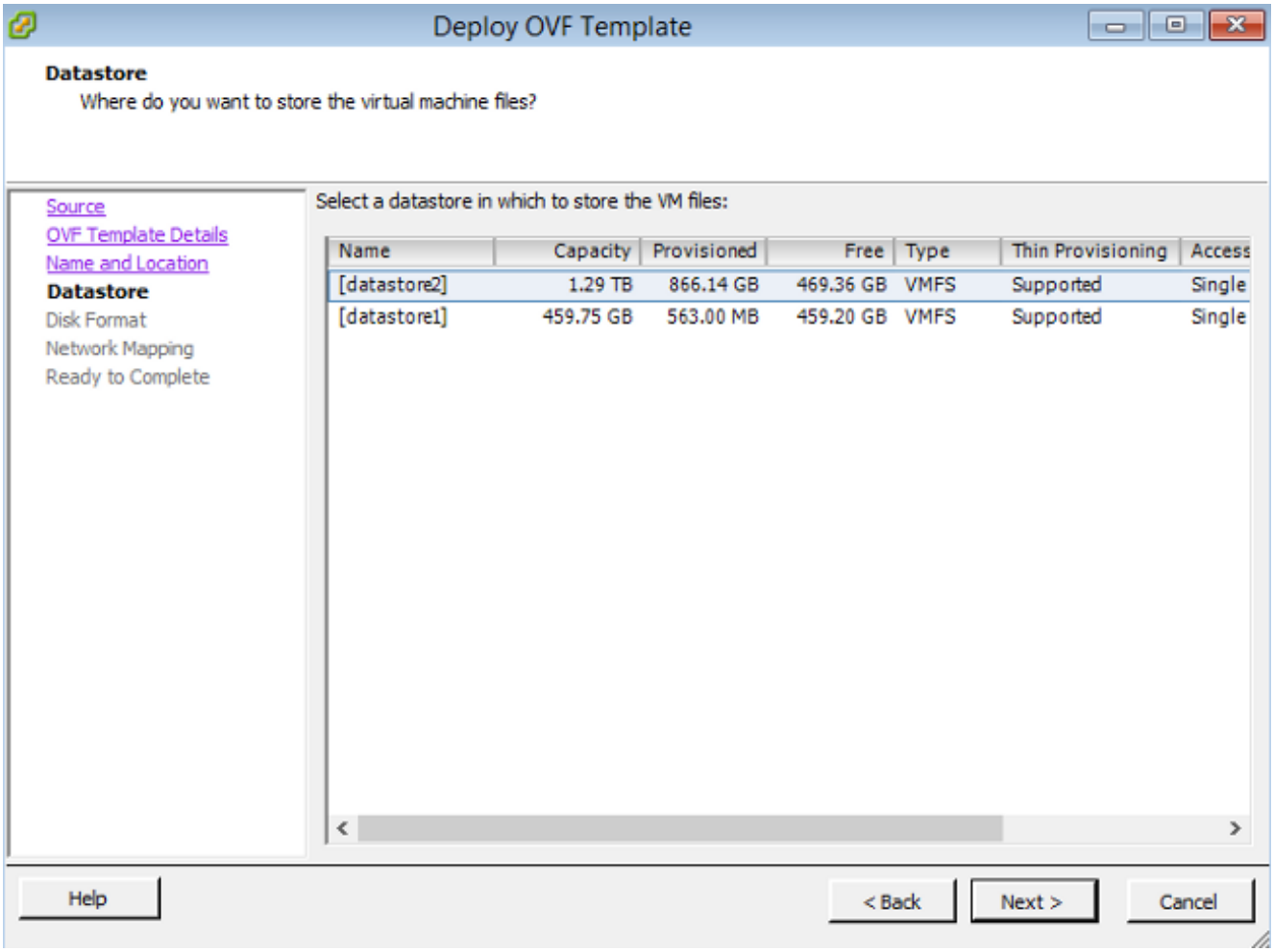
6. На экране **OVF Template Details** нажмите **Next** для принятия настроек по умолчанию.



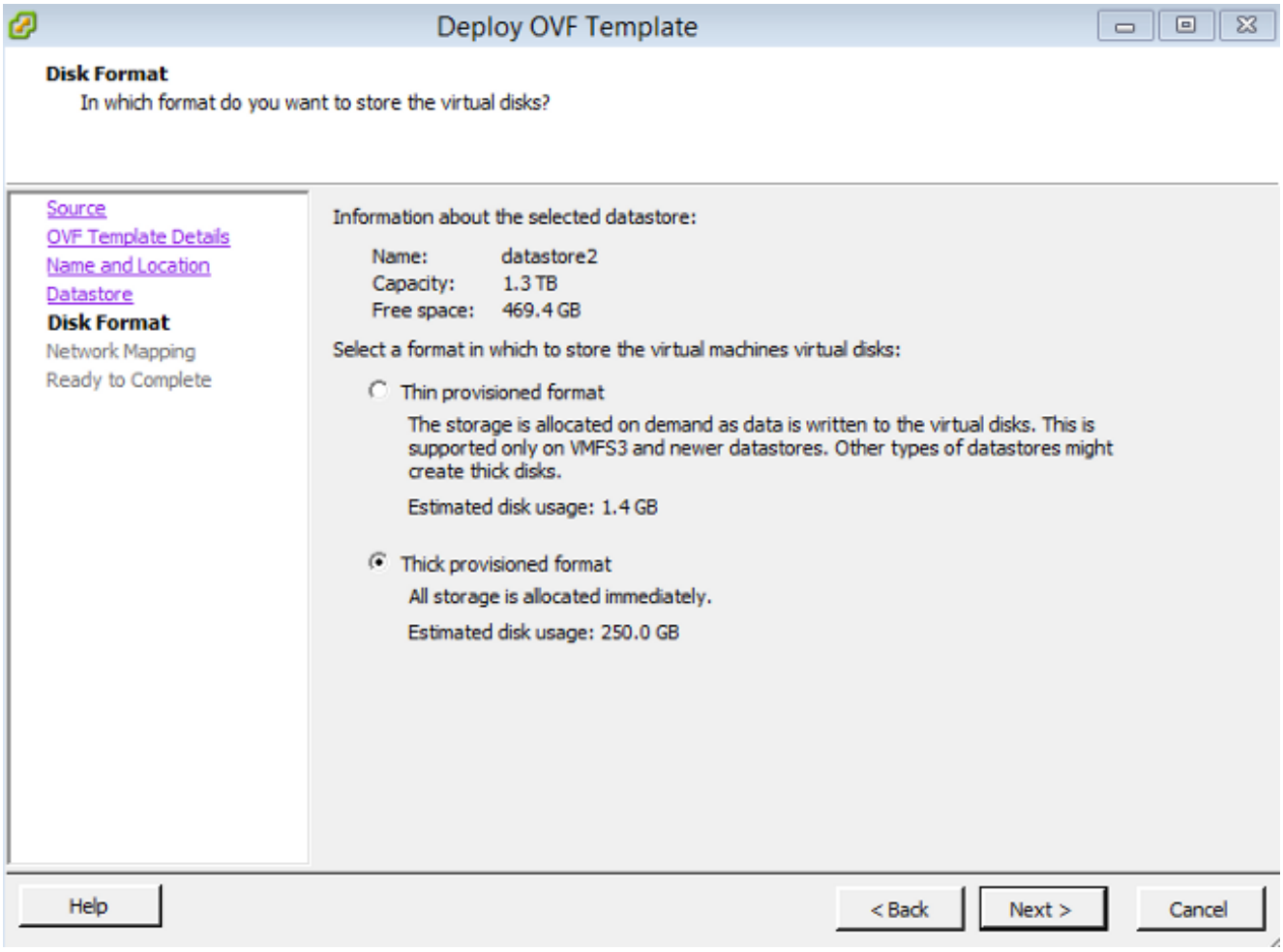
7. Предоставьте название для Центра управления и нажмите **Next**.



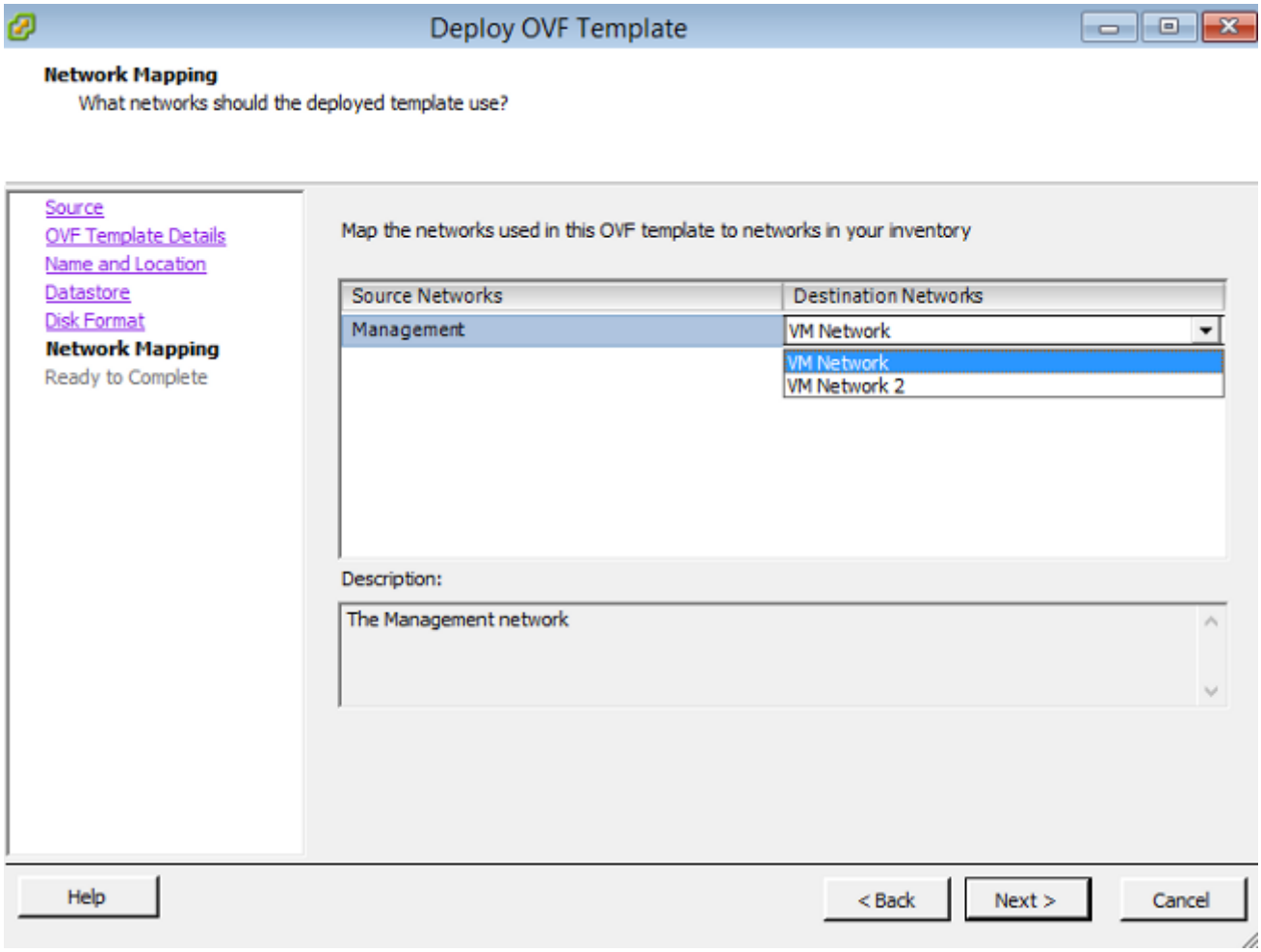
8. Выберите **Datastore**, на котором вы хотите создать виртуальную машину и нажать **Next**.



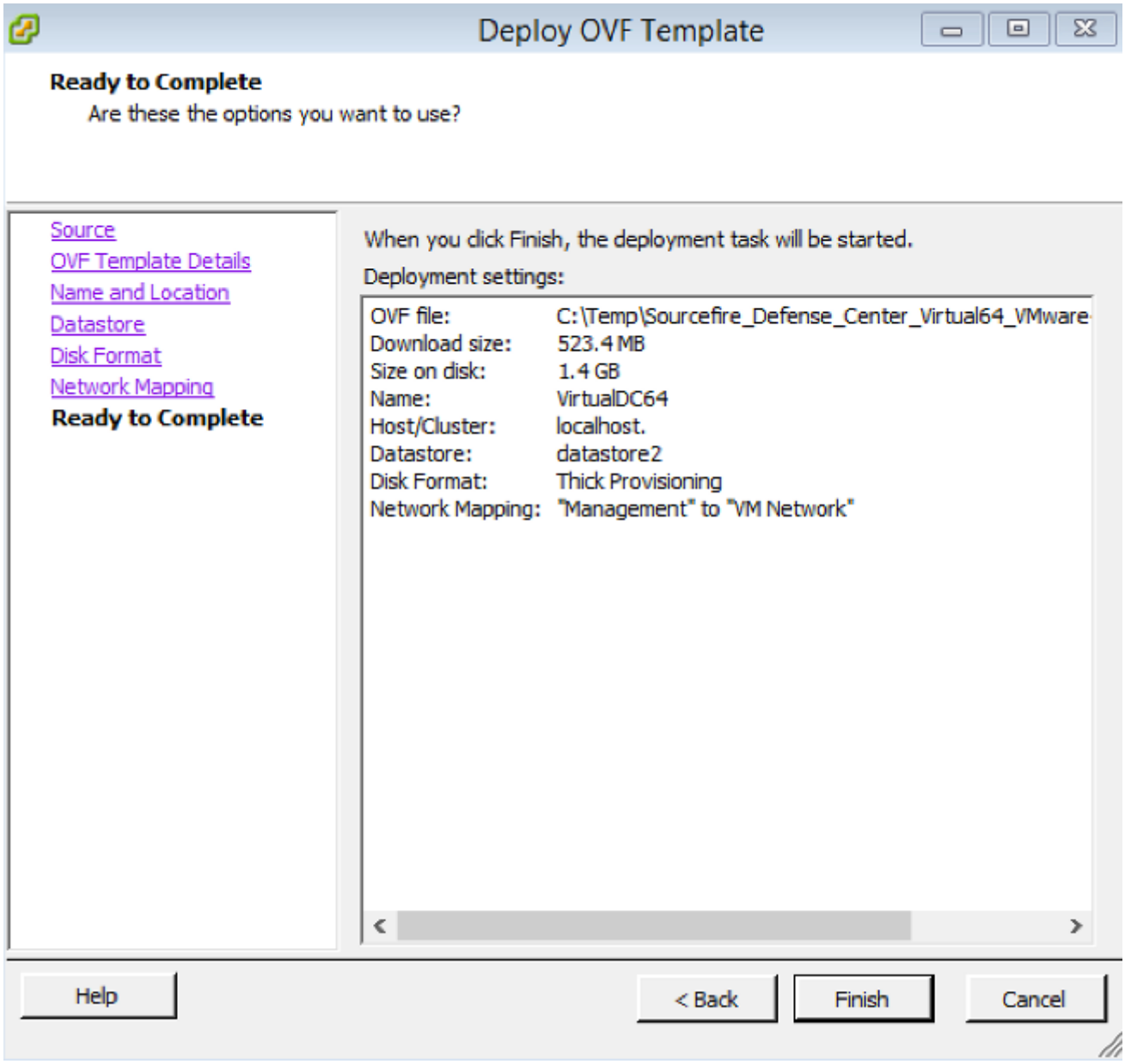
9. Нажмите кнопку с зависимой фиксацией **Толстого выделенного формата** для **Формата диска** и нажмите **Next**. Толстый формат инициализации выделяет необходимое дисковое пространство во время создания виртуального диска, тогда как тонкий формат инициализации использует пространство по требованию.



10. На разделе **Сопоставления Сети** привяжите интерфейс управления Центра управления FireSIGHT к сети VMware и нажмите **Next**.

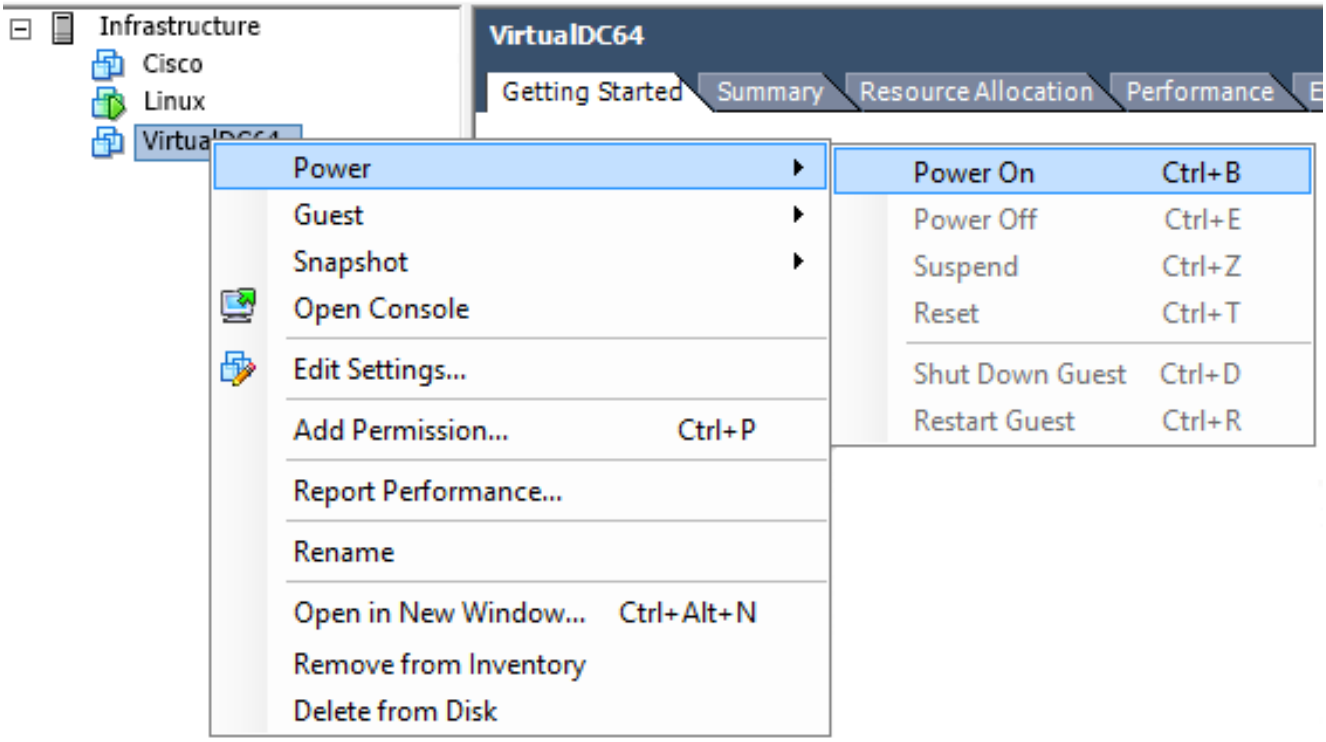


11. Нажмите **Finish** для завершения развертываний шаблона OVF.

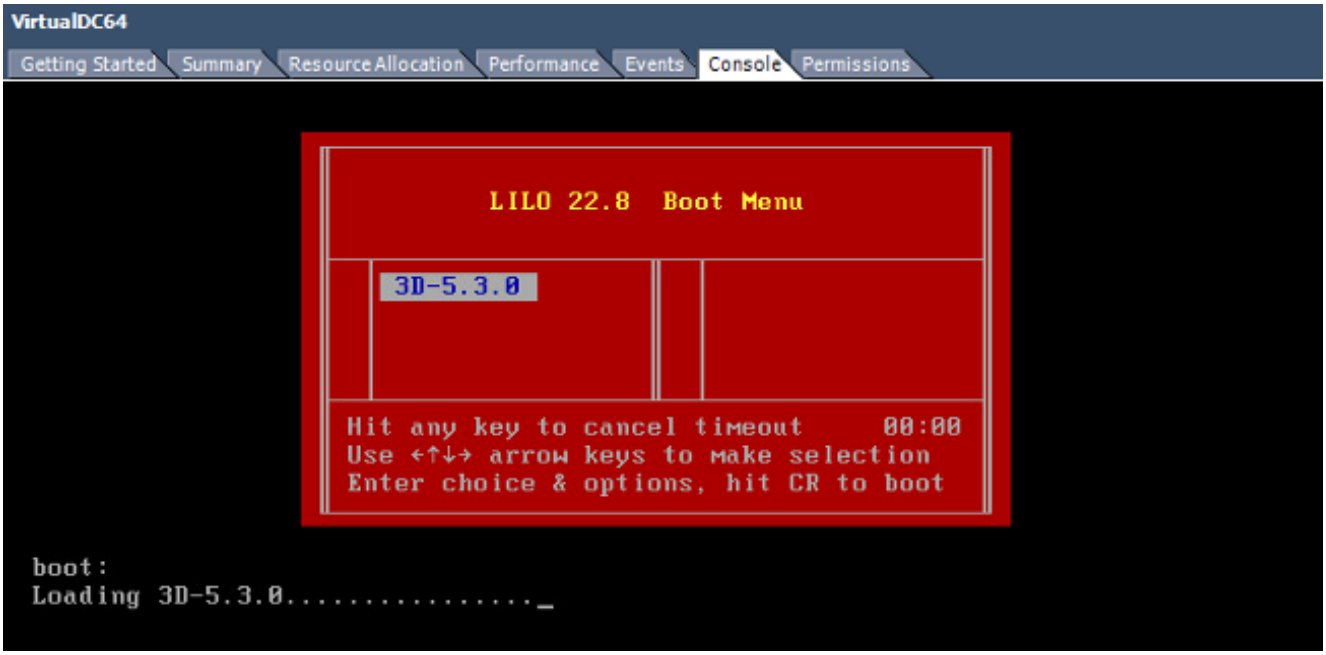


Включите и завершите инициализацию

1. Перейдите к недавно созданной виртуальной машине. Щелкните правой кнопкой мыши имя сервера и выберите **Power> Power On** для начальной загрузки сервера впервые.



2. Перейдите к вкладке **Console** для мониторинга консоли сервера. Меню начальной загрузки LILO
появляется.



Как только проверка данных BIOS успешна, процесс инициализации запускается. Первая начальная загрузка могла бы занять время для завершения, поскольку база данных конфигурации инициализируется
впервые.

```
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
_
```

Однажды завершенный, вы могли бы видеть сообщение ни для `Какого такого устройства`.

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

3. Нажмите **Enter** для получения приглашения регистрации.

```
 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: _
```

Примечание: Сообщение "`ЗАПИСЬ ТО ЖЕ отказало. Вручную обнуление`". может появиться после того, как система загружена впервые. Это не указывает на дефект, он правильно указывает, что драйвер хранилища VMware не поддерживает команду `WRITE SAME`. Система отображает это сообщение и продолжает команду нейтрализации выполнять ту же операцию.

Настройте настройки сети

1. На приглашении регистрации `Sourcefire3D` используйте эти учетные данные для регистрации: Для версии 5. xUsername: **admin**Password: **Sourcefire**Для версии 6.x и позжеUsername: **admin**Password: **Admin123Совет:** Вы будете в состоянии изменить пароль по умолчанию в процессе начальной настройки в GUI.
2. Начальная конфигурация сети сделана со сценарием. Необходимо выполнить сценарий как `пользователь маршрута`. Для коммутации `пользователю маршрута` введите **sudo su -** команда наряду с паролем **Sourcefire или Admin123** `(для 6.x` . Проявите осторожность, когда вошли командная строка Центра управления как пользователь маршрута. `admin@Sourcefire3D:~$ sudo su -`
`Password:`
3. Для начала конфигурации сети введите **сеть configure** сценарий как `root`.

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

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

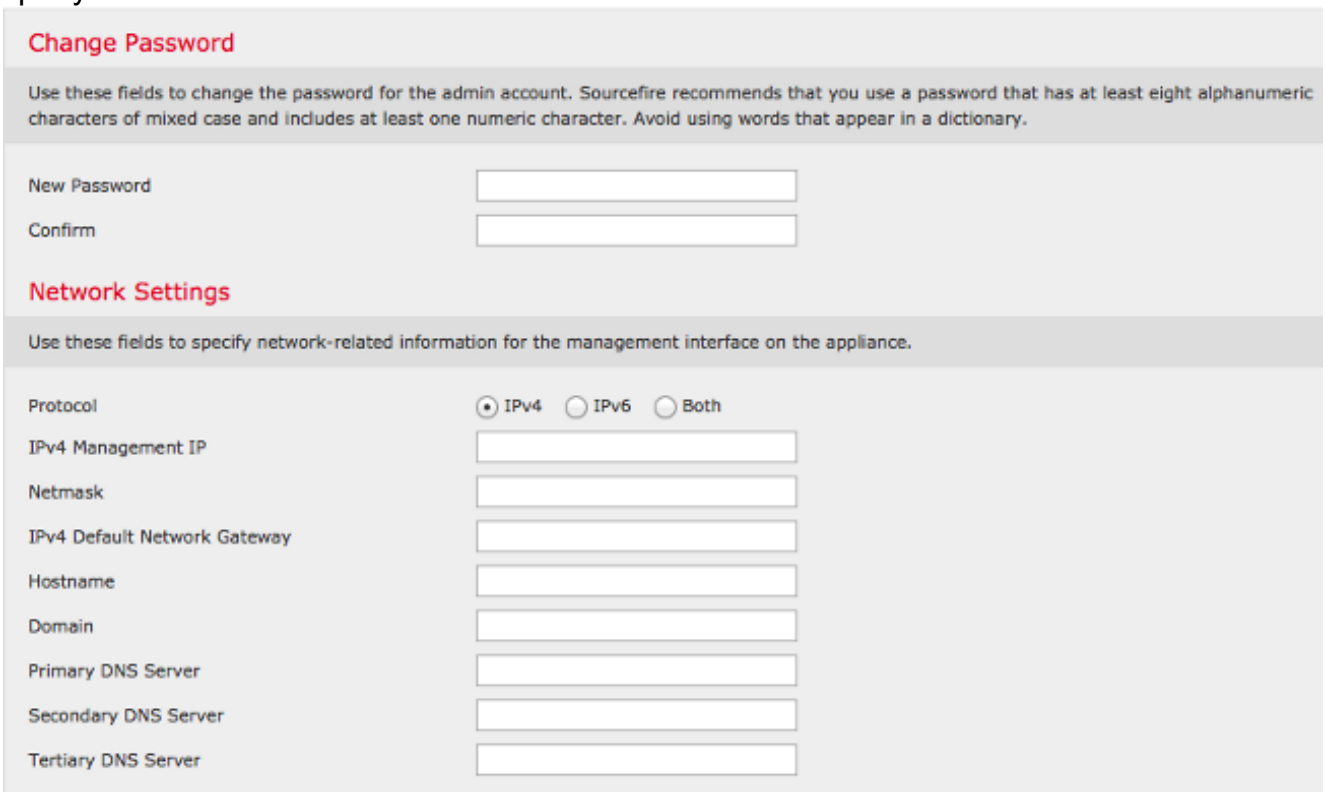
Вас попросят предоставить Управление IP-адресами, маску подсети и шлюз по умолчанию. Как только вы подтверждаете параметры настройки, перезапуски сетевого сервиса. В результате интерфейс управления выключается и затем возвращается.

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

Management IP address? [192.168.45.45] 192.0.2.2
Management netmask? [255.255.255.0]
Management default gateway? 192.0.2.1

Management IP address?         192.0.2.2
Management netmask?            255.255.255.0
Management default gateway?    192.0.2.1

Are these settings correct? (y or n) y

Do you wish to configure IPv6? (y or n) n
e1000: eth0: e1000_watchdog_task: NIC Link is Up 1000 Mbps Full Duplex, Flow Con
trol: None
ADDRCONF(NETDEV_UP): eth0: link is not ready
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

Updated network configuration.

Updated comms. channel configuration.

Please go to https://192.0.2.2/ or https://[]/ to finish installation.
root@Sourcefire3D:~# _
```

Выполните начальную настройку

1. После того, как настройки сети настроены, открывают web-браузер и переходят к настроенному IP через HTTPS (https://192.0.2.2 в данном примере). Аутентифицируйте сертификат SSL по умолчанию, если предложено. Используйте эти учетные данные для регистрации:Для версии 5. x Username: **admin**Password: **Sourcefire**Для версии 6.x и позжеUsername: **admin**Password: **`Admin123`**
2. На экране, который придерживается, все разделы конфигурации GUI являются дополнительными за исключением изменения пароля и принятия условий предоставления услуг. Если информация известна, рекомендуется использовать мастера настройки для упрощения начальной конфигурации Центра управления. После того, как настроенный, нажмите **Apply** для применения конфигурации к Центру управления и зарегистрированным устройствам. Краткий обзор параметров конфигурации следующие:**Пароль изменения:** Позволяет вам изменять пароль для учетной записи администратора по умолчанию. Это требуется, чтобы изменять пароль. **Параметры сети:** Позволяет вам модифицировать ранее настроенный IPv4 и настройки сети IPv6 для интерфейса управления устройства или виртуальной машины.**Настройки времени:** рекомендуется синхронизировать Центр управления с надежным NTP source. Сенсоры IPS могут быть настроены через системную политику для синхронизации их времени с Центром управления. Дополнительно, время и часовой пояс показа могут быть установлены вручную.**Повторяющийся Импорт Обновления Правила:** Позвольте возвратиться обновления правила Фырканья и дополнительно установите теперь во время начальной настройки.**Повторяющиеся Обновления Геолокации:** Включите повторяющиеся обновления правила геолокации и

дополнительно установите теперь во время начальной настройки.**Автоматические Резервные копии:** резервные копии автоматической конфигурации Списка.**Настройки лицензии:** Добавьте характеристику лицензирования.**Регистрация устройства:** Позволяет вам добавлять, лицензировать, и применять политику контроля за начальным доступом к предзарегистрированным устройствам. ИМЯ ХОСТА/IP-АДРЕС и регистрационный ключ должны совпасть с IP-адресом и регистрационным ключом, настроенным на Модуле ips FirePOWER.**Лицензионное соглашение с конечным пользователем:** Принятие EULA
требуется.



Дополнительные сведения

- [Центр управления огневой мощи действительное Краткое руководство по началу работы для VMware, версии 6.0]
- [Cisco Systems – техническая поддержка и документация]