# ViPNet xFirewall

## Подготовка к работе

infotecs

ФРКЕ.00217-01 90 13

Версия продукта 4.1.0



ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: https://infotecs.ru/

Служба технической поддержки: hotline@infotecs.ru

# Содержание

**Введение** ... **5**
О документе ... 6
Для кого предназначен документ ... 6
Соглашения документа ... 6
Связанные документы ... 8
О программно-аппаратном комплексе ViPNet xFirewall ... 9
Подготовка ViPNet xFirewall к работе ... 10
Обратная связь ... 11

**Глава 1. Развертывание ViPNet xFirewall xF-VA** ... **12**
Требования к платформе виртуализации ... 13
Установка ViPNet xFirewall xF-VA на платформу виртуализации ... 14
VMware vSphere ESXi ... 14
Oracle VM VirtualBox ... 19

**Глава 2. Установка, обновление и удаление справочников и лицензии** ... **22**
Способы установки и подготовка к установке справочников и лицензии ... 23
Подготовка к установке справочников и лицензии по протоколу TFTP ... 24
Подготовка к установке справочников и лицензии с помощью внешнего устройства ... 26
Установка справочников и лицензии ... 27
Начало установки ... 27
Настройка часового пояса, даты и времени ... 28
Установка дистрибутива лицензии на ViPNet xFirewall ... 30
Настройка DNS-сервера ... 32
Настройка сетевых интерфейсов ... 33
Настройка NTP-сервера ... 34
Настройка имени компьютера и диапазона виртуальных адресов ... 35
Завершение установки ... 36
Обновление и удаление справочников и лицензии ... 38

**Глава 3. Обновление программного обеспечения** ... **39**
Удаленное обновление ПО ... 40
Локальное обновление ПО ... 41
Обновление модуля DPI ... 43
Деактивация правил межсетевого экрана ... 45

Обновление ПО на кластере горячего резервирования ..... 47

**Глава 4. Резервное копирование и восстановление настроек ..... 49**

Назначение экспорта и импорта справочников, лицензии и настроек ..... 50

Экспорт справочников, лицензии и настроек ..... 51

Импорт справочников, лицензии и настроек ..... 53

**Приложение А. Глоссарий ..... 54**

# Введение


О документе 6

Связанные документы 8

О программно-аппаратном комплексе ViPNet xFirewall 9

Подготовка ViPNet xFirewall к работе 10

Обратная связь 11

# О документе

В документе описан порядок действий по подготовке ViPNet xFirewall к использованию, основные сценарии работы со справочниками и лицензией, порядок обновления ПО, резервное копирование и восстановление настроек.

## Для кого предназначен документ

Документ предназначен для администраторов, которые отвечают за эксплуатацию и сопровождение ViPNet xFirewall.

## Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

*Таблица 1. Обозначения, используемые в примечаниях*

| Обозначение | Описание |
|---|---|
|  | **Внимание!** Указывает на обязательное для исполнения или следования действие или информацию. |
|  | **Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию. |
|  | **Совет.** Содержит дополнительную информацию общего характера. |

*Таблица 2. Обозначения, используемые для выделения информации в тексте*

| Обозначение | Описание |
|---|---|
| **Название** | Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши. |
| **Клавиша+Клавиша** | Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу. |
| **Меню > Подменю > Команда** | Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации. |
| `Код` | Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки. |

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены только в режиме администратора, содержат приглашение с символом «#». Например:

  ```
  hostname# команда
  ```

- Команды, которые могут быть выполнены в режиме и пользователя, и администратора, содержат приглашение с символом «>». Например:

  ```
  hostname> команда
  ```

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки. Например:

  ```
  команда <параметр>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

  ```
  команда <обязательный параметр> [необязательный параметр]
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой. Например:

  ```
  команда {вариант-1 | вариант-2}
  ```

# Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ViPNet xFirewall помимо данного документа.

*Таблица 3. Связанные документы*

| Документ | Содержание |
|---|---|
| «ViPNet xFirewall. Общее описание» | Общая информации по ViPNet xFirewall, способы настройки и управления, описание существующих исполнений и характеристики аппаратных платформ |
| «ViPNet xFirewall. Настройка с помощью командного интерпретатора» | Описание основных сценариев настройки ViPNet xFirewall с помощью командного интерпретатора, работы с журналами и мониторинга ViPNet xFirewall |
| «ViPNet xFirewall. Настройка с помощью веб-интерфейса» | Описание основных сценариев настройки ViPNet xFirewall с помощью веб-интерфейса |
| «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам» | Описание команд ViPNet xFirewall<br>Описание конфигурационных файлов управляющего демона и системы защиты от сбоев |
| «ViPNet xFirewall. Лицензионные соглашения на компоненты сторонних производителей» | Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet xFirewall |

# О программно-аппаратном комплексе ViPNet xFirewall

ViPNet xFirewall представляет собой программно-аппаратный комплекс, который выступает в роли межсетевого экрана и предназначен для фильтрации трафика между внешней сетью и узлами локальной сети. ViPNet xFirewall выполняет фильтрацию трафика на сетевом и транспортном уровнях модели OSI (с контролем состояния сессий), а также реализует механизм расширенной инспекции IP-пакетов DPI (см. глоссарий, стр. 54) на уровнях 2 — 7 модели OSI и накопления статистики. Благодаря этому ViPNet xFirewall обеспечивает защиту локальной сети и контролирует работу пользователей с сетевыми приложениями.

ViPNet xFirewall производится в нескольких исполнениях, в том числе для развертывания на платформах виртуализации.

# Подготовка ViPNet xFirewall к работе

Для подготовки ViPNet xFirewall к эксплуатации выполните все действия из приведенной ниже таблицы в предложенном порядке.

*Таблица 4. Порядок действий при подготовке ViPNet xFirewall к работе*

| | Действие | Ссылка |
|---|---|---|
| ☐ | Установите и подключите ViPNet xFirewall к питанию и сетевому оборудованию. | |
| | Если вы используете ViPNet xFirewall xF-VA, разверните его на платформе виртуализации. | Развертывание ViPNet xFirewall xF-VA (на стр. 12) |
| ☐ | Получите лицензию сетевого узла (файл `*.dst`) и пароль у администратора вашей сети ViPNet. | |
| ☐ | Включите ViPNet xFirewall. | |
| ☐ | Выберите способ установки лицензии и выполните необходимые подготовительные действия перед установкой. | Способы установки и подготовка к установке справочников и лицензии (на стр. 23)<br>Подготовка к установке справочников и лицензии по протоколу TFTP (на стр. 24)<br>Подготовка к установке справочников и лицензии с помощью внешнего устройства (на стр. 26) |
| ☐ | Установите на ViPNet xFirewall справочники и лицензии. | Установка справочников и лицензии (на стр. 27) |
| ☐ | Во время установки справочников и лицензии выполните все необходимые настройки ViPNet xFirewall. | |

**Совет.** Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

# Обратная связь

## Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Информация о продуктах ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Часто задаваемые вопросы https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

## Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт https://infotecs.ru/support/request/.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения https://infotecs.ru/disclosure.php.

# 1

# Развертывание ViPNet xFirewall xF-VA


Требования к платформе виртуализации 13

Установка ViPNet xFirewall xF-VA на платформу виртуализации 14

# Требования к платформе виртуализации

ViPNet xFirewall имеет программное исполнение — ПО ViPNet xFirewall xF-VA, предназначенное для развертывания на платформе виртуализации. Преимуществом ViPNet xFirewall xF-VA является его независимость от изменений аппаратной платформы.

ViPNet xFirewall xF-VA можно установить на следующие платформы виртуализации, поддерживающие стандарт OVF (Open Virtualization Format):

- VMware vSphere 5.x (рекомендуемая версия — 5.5.0).
- VMware Workstation 11.x (рекомендуемая версия — 11.0.0).
- Oracle VM VirtualBox 4.x (рекомендуемая версия — 4.3.28).

Работа на других платформах виртуализации не гарантируется.

Виртуальная машина ViPNet xFirewall xF-VA должна быть сконфигурирована следующим образом:

- Процессор — один с количеством ядер 2.
- Объем оперативной памяти — не менее 2 Гбайт.
- Накопители — 2 диска: HDD не менее 2 Гбайт, HDD не менее 80 Гбайт.
- Сетевые интерфейсы — не менее 2.

Сетевому узлу, на который устанавливается ПО ViPNet xFirewall xF-VA, в программе ViPNet Центр управления сетью (далее — ЦУС) (см. глоссарий, стр. 55) должна быть назначена роль «ViPNet xFirewall xF-VA».

# Установка ViPNet xFirewall xF-VA на платформу виртуализации

Для установки ViPNet xFirewall xF-VA на платформу виртуализации вам потребуется файл с образом виртуальной машины (файл с расширением *.ova), который входит в комплект поставки.

В следующих разделах приведены примеры установки ViPNet xFirewall xF-VA на следующие платформы виртуализации: VMware vSphere ESXi и Oracle VM VirtualBox.

## VMware vSphere ESXi

Для установки ViPNet xFirewall xF-VA на платформу виртуализации VMware vSphere ESXi выполните следующие действия:

1 В главном окне программы vSphere Client в меню **File** выберите пункт **Deploy OVF Template**. Откроется окно **Deploy OVF Template**, которое представляет собой мастер развертывания виртуальных машин из образов формата OVF.

---

**Примечание.** Если в меню **File** нет пункта **Deploy OVF Template**, убедитесь, что установлено расширение Client Integration (http://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.vm_admin.doc/GUID-3FC8F86B-7F4A-450C-9D1F-0275E403F71C.html#GUID-3FC8F86B-7F4A-450C-9D1F-0275E403F71C), добавляющее поддержку образов формата OVF.

---

2 На странице **Source** укажите путь к файлу с расширением *.ova, содержащему образ виртуальной машины.

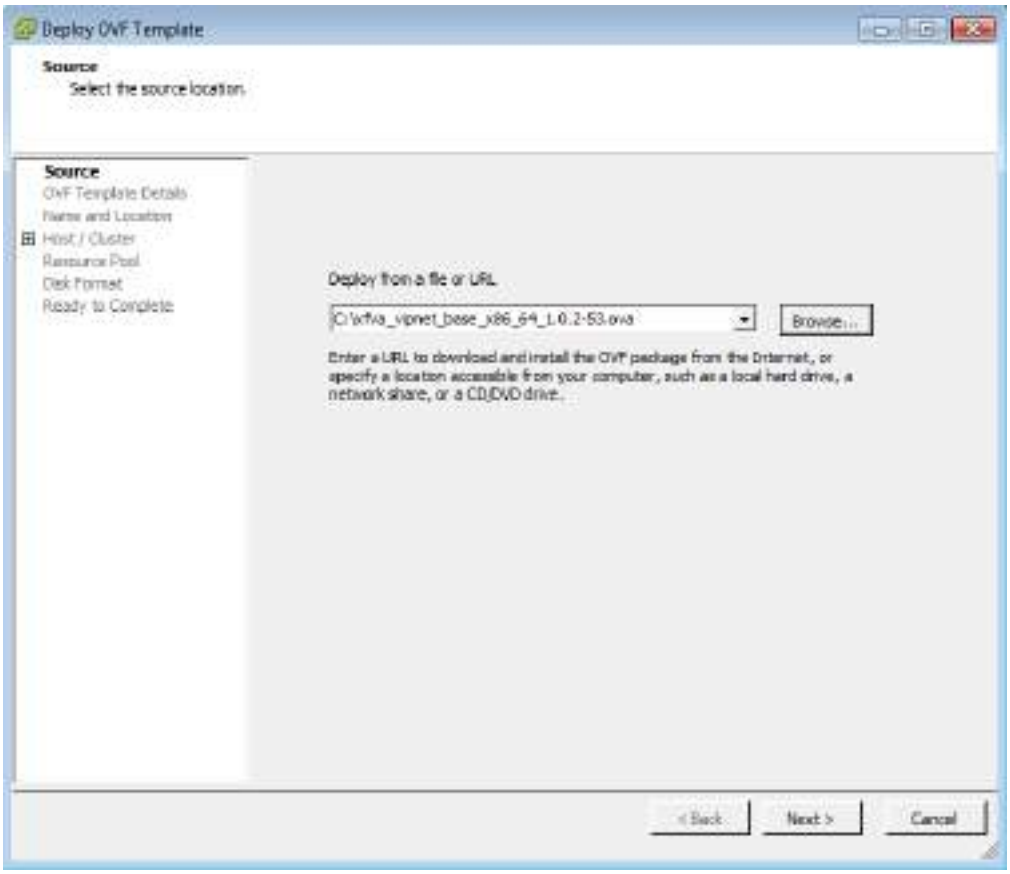


*Рисунок 1. Задание файла с образом виртуальной машины*

3 На странице **OVF Template Details** ознакомьтесь с параметрами виртуальной машины и убедитесь, что на ваших накопителях достаточно свободного места для развертывания.

4 На странице **Name and Location** выполните следующие действия:

- В поле **Name** измените, если необходимо, имя виртуальной машины.

---

**Примечание.** Имена виртуальных машин в папке не должны повторяться.

---

- Выберите папку, в которой будет располагаться виртуальная машина.

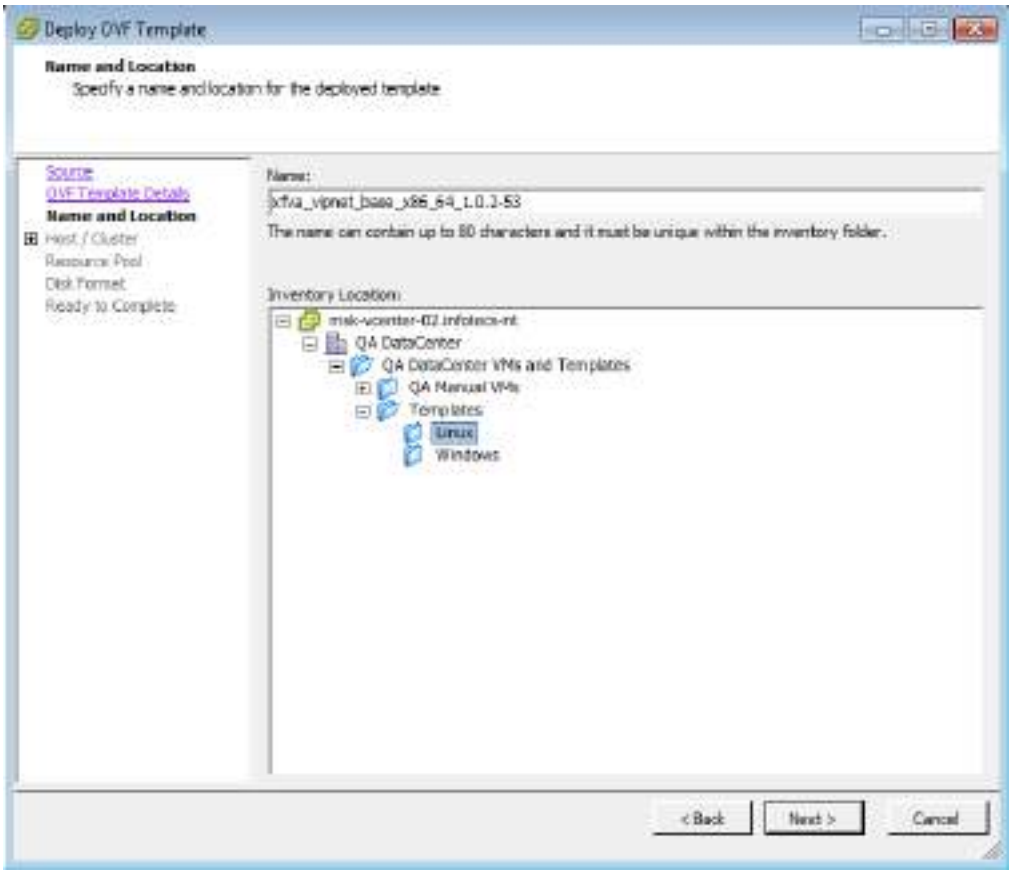


*Рисунок 2. Задание имени и расположения виртуальной машины*

5 При наличии на левой панели соответствующих пунктов выполните следующие действия:

**5.1** На странице **Host / Cluster** укажите сетевой узел, на котором будут храниться файлы виртуальной машины.

**5.2** На странице **Resource Pool** выберите «пул ресурсов», то есть группу носителей информации, выделяемых для хранения файлов виртуальной машины.

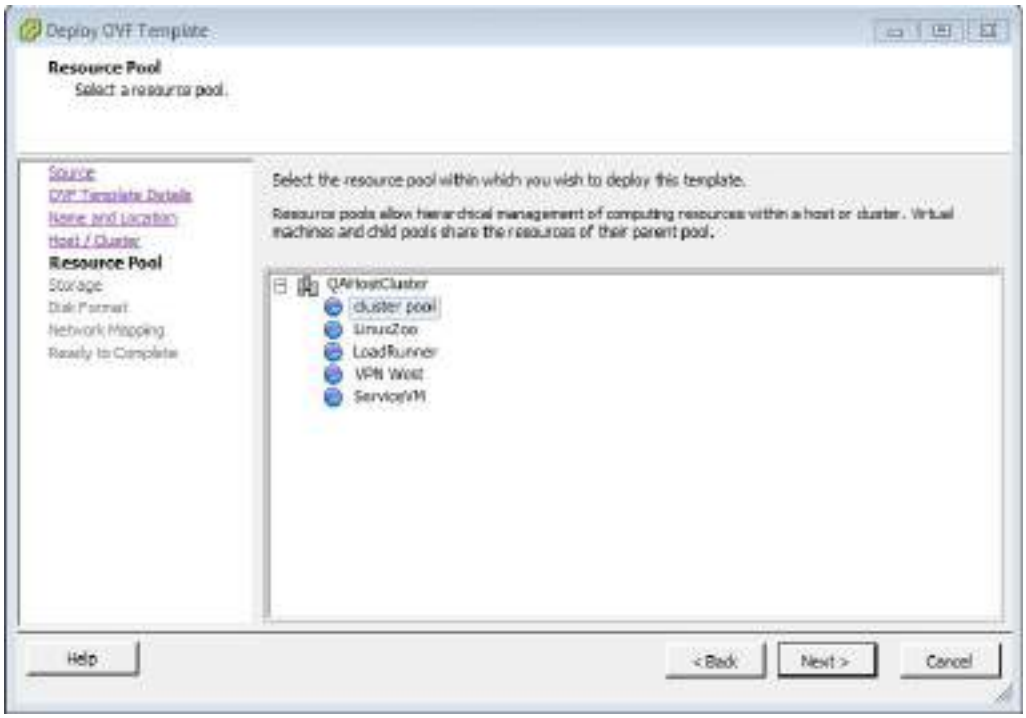


*Рисунок 3. Выбор пула ресурсов*

**5.3** На странице **Storage** укажите жесткий диск или твердотельный накопитель из выбранного пула ресурсов, на котором будут храниться файлы виртуальной машины.

**6** На странице **Disk Format** выберите необходимый формат виртуального диска (например, при выборе формата **Thin Provision** файл с виртуальным диском имеет переменный размер — файл увеличивается или уменьшается в зависимости от размера содержимого виртуального диска).

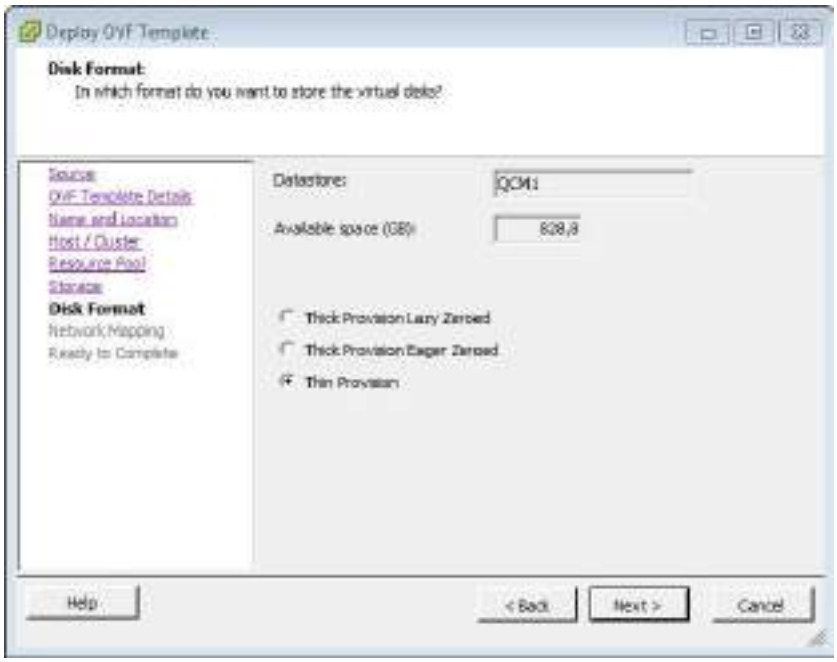


*Рисунок 4. Выбор формата виртуального диска*

**7** На странице **Network Mapping** задайте физический или виртуальный сетевой коммутатор ESXi, который будет по умолчанию сопоставлен всем сетевым интерфейсам вашей виртуальной

машины. Для этого сопоставьте его сети bridged. Впоследствии вам будет нужно сопоставить физический или виртуальный сетевой коммутатор каждому из сетевых интерфейсов ViPNet xFirewall xF-VA (см. шаг 10).

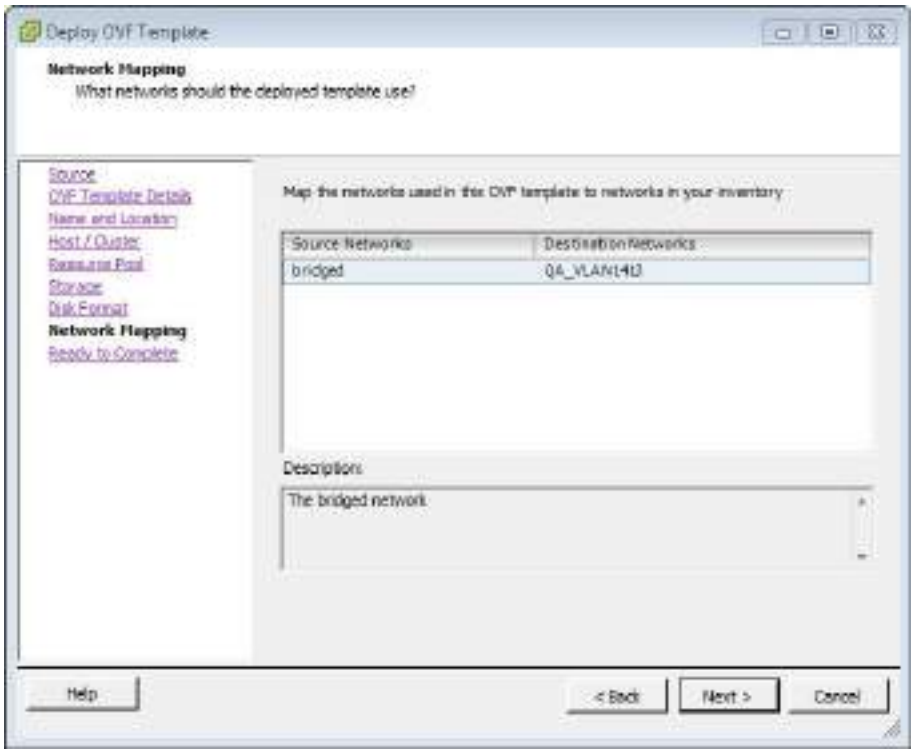


*Рисунок 5. Настройка сетевых интерфейсов*

8 На странице **Ready to Complete** выполните следующие действия:

- Проверьте настройки развертывания виртуальной машины.
- Если вы хотите, чтобы виртуальная машина запустилась автоматически после установки, установите флажок **Power on after deployment**.
- Чтобы начать развертывание, нажмите кнопку **Finish**.

9 Дождитесь окончания развертывания. В результате в папке, указанной на шаге 4, будет создана виртуальная машина с заданным именем.

10 В главном окне программы vSphere Client перейдите на страницу **VMs and Templates** и выполните следующие действия:

- Сопоставьте сетевым интерфейсам виртуальной машины физические или виртуальные сетевые коммутаторы. Параметры сетевых интерфейсов задаются в настройках виртуальной машины на вкладке **Hardware**.
- Запустите виртуальную машину. Начнется загрузка операционной системы и всех необходимых служб.

11 После завершения загрузки ViPNet xFirewall xF-VA выполните установку справочников и лицензии (см. Установка, обновление и удаление справочников и лицензии на стр. 22).

# Oracle VM VirtualBox

Для установки ViPNet xFirewall xF-VA на платформу виртуализации Oracle VM VirtualBox выполните следующие действия:

1 В главном окне программы Oracle VM VirtualBox в меню **Файл** выберите пункт **Импорт конфигураций**. Будет запущен мастер импорта конфигураций виртуальных машин.

2 На первой странице мастера укажите путь к файлу с расширением `*.ova`, содержащему образ виртуальной машины. Затем нажмите кнопку **Next**.

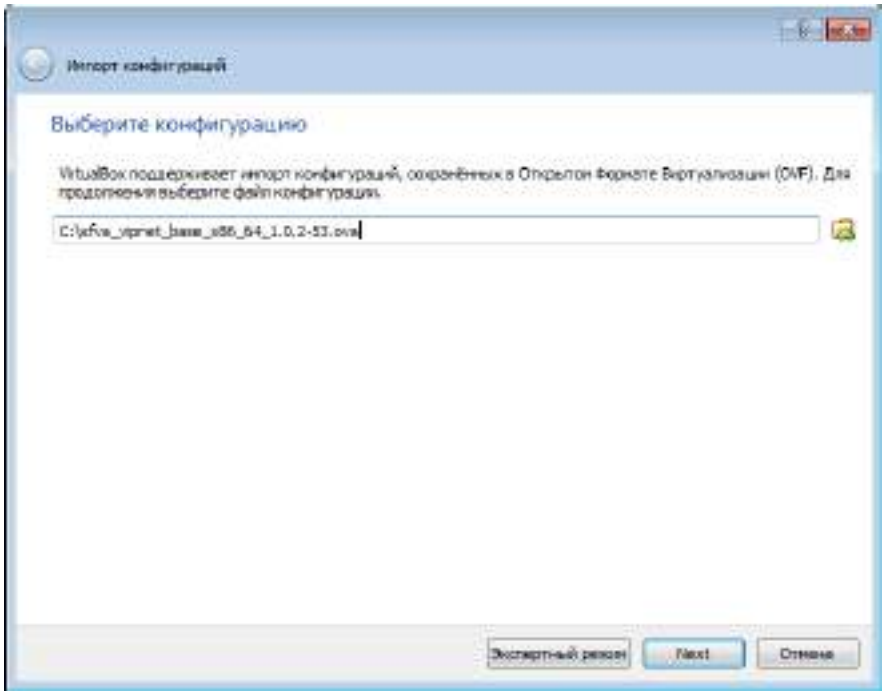


*Рисунок 6. Выбор файла с образом виртуальной машины*

3 На странице **Укажите параметры импорта** в поле **Имя** измените, если необходимо, имя виртуальной машины. Затем нажмите кнопку **Импорт**.

---

**Внимание!** Во время установки ViPNet xFirewall xF-VA на платформу виртуализации и при его дальнейшей эксплуатации не следует изменять используемый для виртуального образа контроллер жесткого диска. Корректная работа ViPNet xFirewall xF-VA гарантируется только при использовании IDE-контроллера жесткого диска.

---

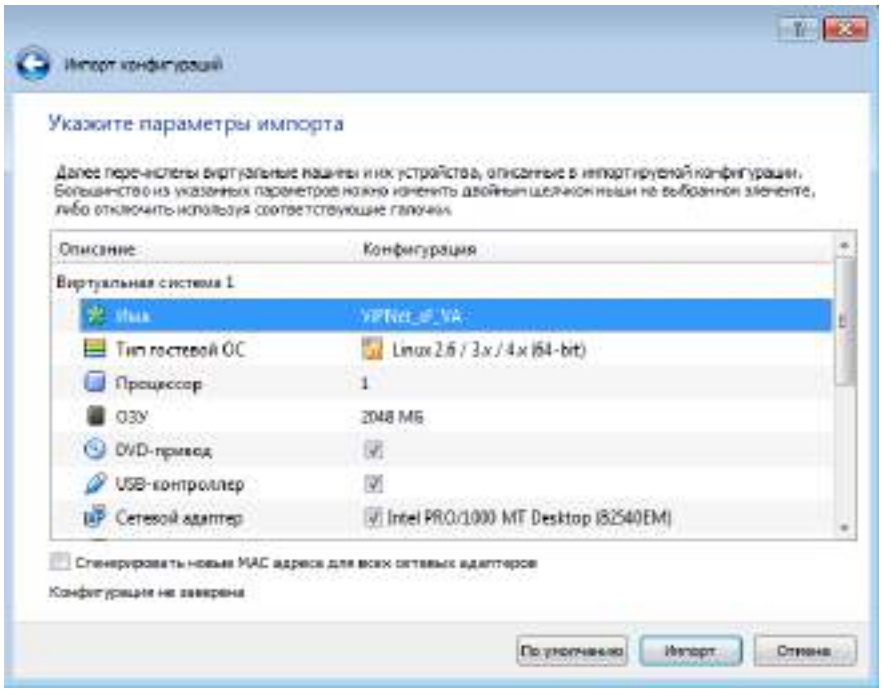


*Рисунок 7. Изменение параметров виртуальной машины*

В результате импорта будет создана виртуальная машина с указанным именем.

4 В настройках виртуальной машины включите поддержку процессором режима расширения физических адресов PAE (Physical Address Extension). Для этого в главном окне программы Oracle VM VirtualBox на панели инструментов нажмите кнопку **Настроить**, в окне **Настройки** выберите раздел **Система** и на вкладке **Процессор** установите флажок **Включить PAE/NX**.

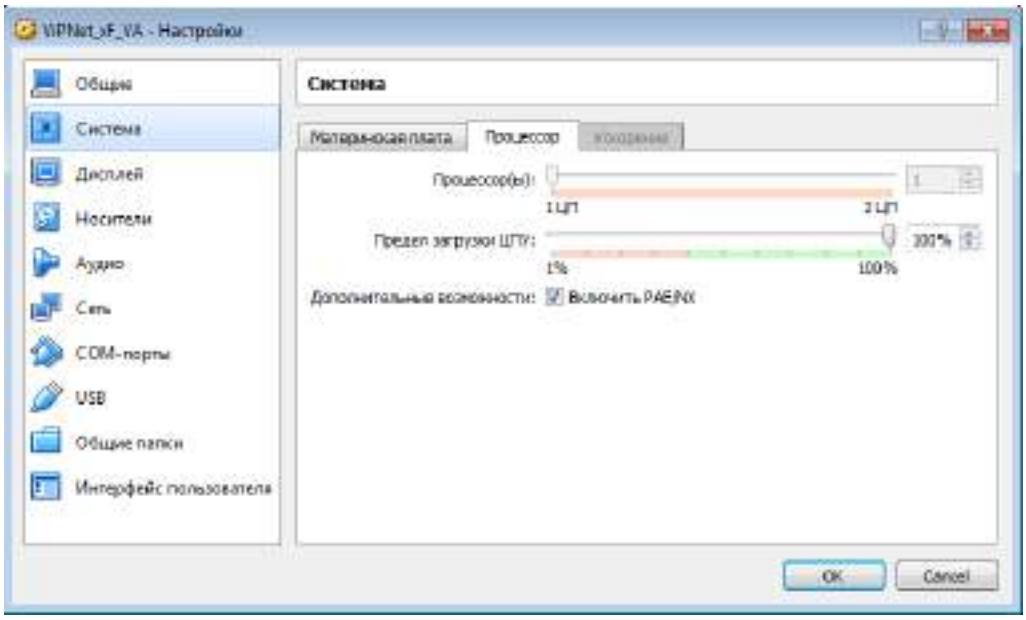


*Рисунок 8. Включение поддержки процессором режима PAE*

**Примечание.** На платформе виртуализации VMware Workstation поддержка режима PAE всегда включена.

5 Добавьте, если необходимо, сетевые интерфейсы. Параметры сетевых интерфейсов задаются в настройках виртуальной машины в разделе **Сеть**.

6 Запустите виртуальную машину. Начнется загрузка операционной системы и всех необходимых служб.

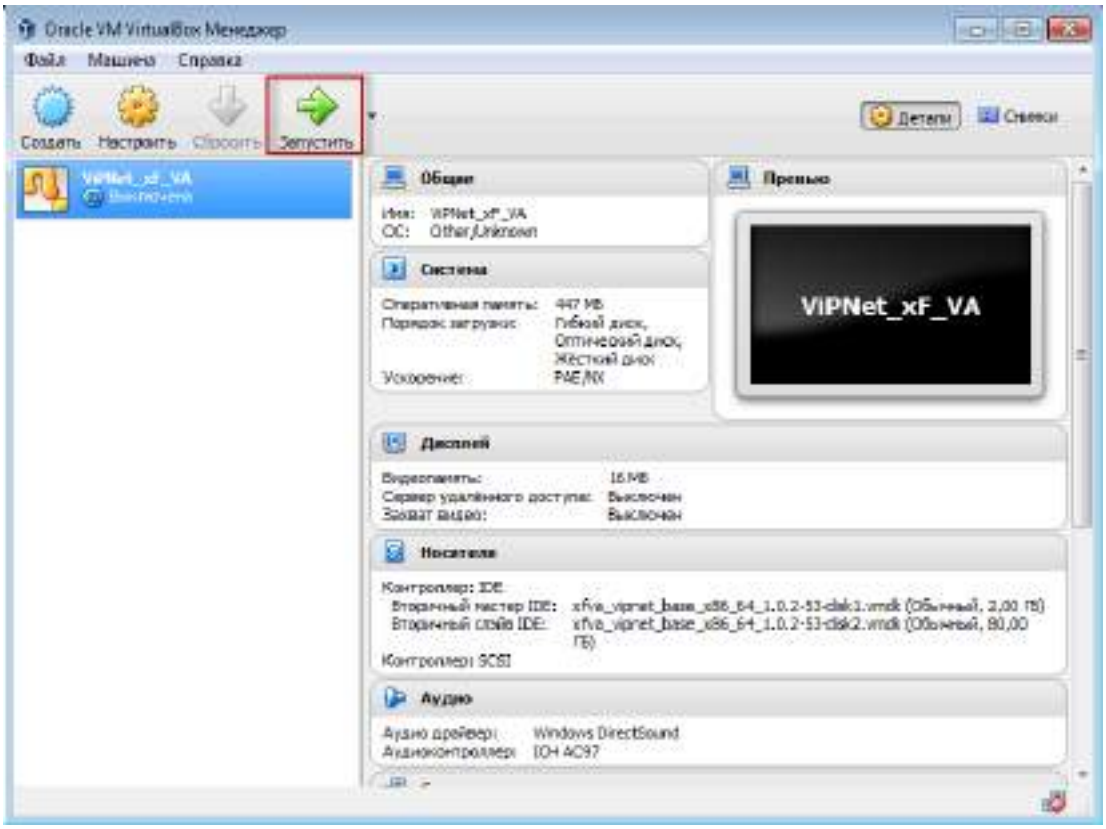


*Рисунок 9. Запуск виртуальной машины*

7 После завершения загрузки ViPNet xFirewall xF-VA выполните установку справочников и лицензии (см. Установка справочников и лицензии на стр. 27).

# 2

# Установка, обновление и удаление справочников и лицензии


Способы установки и подготовка к установке справочников и лицензии 23

Установка справочников и лицензии 27

Обновление и удаление справочников и лицензии 38

# Способы установки и подготовка к установке справочников и лицензии

Перед началом эксплуатации ViPNet xFirewall на нем необходимо установить справочники и лицензию сетевого узла ViPNet. Без этого работа ViPNet xFirewall и управление устройством будут невозможны. Вы можете установить справочники и лицензию в следующих случаях:

- Первоначальная инициализация справочников и лицензии с помощью дистрибутива лицензии сетевого узла (файла `*.dst`).

  Файл `*.dst` и пароль вы можете получить у администратора сети ViPNet.

- Восстановление справочников, лицензии и настроек на ViPNet xFirewall после некорректного обновления ПО или их перенос с другого ViPNet xFirewall того же исполнения (например, при замене аппаратной платформы). Для выполнения данных операций требуется файл `*.vbe`, в который были экспортированы справочники, лицензия и настройки с другого действующего ViPNet xFirewall. Подробнее об этом см. в главе Резервное копирование и восстановление настроек (на стр. 49).

Существует несколько способов установки справочников и лицензии на ViPNet xFirewall. Способ установки зависит от способа подключения к ViPNet xFirewall.


*Рисунок 10. Способы подключения и установки справочников и ключей на ViPNet xFirewall*

Вы можете выбрать один из следующих способов установки:

- Через ноутбук по каналу Ethernet и протоколу TFTP (см. Подготовка к установке справочников и лицензии по протоколу TFTP на стр. 24). Удобен, если вы подключаетесь к ViPNet xFirewall или виртуальному образу ViPNet xFirewall с ноутбука через сетевой кросс-кабель Ethernet и технологический адрес.
- Через внешнее устройство, которым может быть USB-носитель или CD-диск (см. Подготовка к установке справочников и лицензии с помощью внешнего устройства на стр. 26). Удобен, если вы подключаетесь к ViPNet xFirewall или виртуальному образу ViPNet xFirewall через обычную консоль (с использованием монитора и клавиатуры) или COM-консоль (с использованием ноутбука).

# Подготовка к установке справочников и лицензии по протоколу TFTP

Для установки справочников и лицензии данным способом вам понадобится следующее:

- ноутбук с сетевой картой Ethernet и ОС Windows или GNU/Linux любых версий;
- сетевой кросс-кабель Ethernet для соединения ноутбука с ViPNet xFirewall.

На ноутбуке должны быть включены стандартные службы Telnet (или SSH) и TFTP, которые необходимы для выполнения следующих функций:

- для подключения к ViPNet xFirewall (Telnet или SSH);
- для переноса дистрибутива лицензии на ViPNet xFirewall (TFTP).

В ОС Windows XP и GNU/Linux эти службы по умолчанию включены. В ОС Windows Vista и выше эти службы по умолчанию отключены и их необходимо включить вручную. Для включения служб в ОС Windows Vista и выше выполните следующее:

1. Выберите **Пуск** (**Start**) > **Панель управления** (**Control Panel**) > **Программы и компоненты** (**Programs and Features**).
2. Зайдите в меню **Включение или отключение компонентов Windows** (**Turn Windows features on or off**) и установите флажки рядом с названием служб **Клиент TFTP** (**TFTP Client**) и **Простые службы TCPIP** (**Simple TCPIP services**).

Кроме того, на время установки на ноутбуке с ОС Windows Vista отключите следующие службы безопасности (если они включены):

- Брандмауэр Windows (Windows Firewall);
- Защитник Windows (Windows Defender);
- Центр обновления Windows (Windows Update);
- в меню **Свойства обозревателя** (**Internet Options**) на вкладке **Безопасность** (**Security**) отключите защиту по всем параметрам.

Перед началом установки справочников и лицензии выполните следующие действия:

1. Перенесите на ноутбук дистрибутив лицензии (файл `*.dst`).
2. С помощью кросс-кабеля подключите ноутбук к порту Ethernet1 ПАК ViPNet xFirewall или компьютера, на котором развернут виртуальный образ ViPNet xFirewall xF-VA.
3. Если вы устанавливаете справочники и ключи на виртуальный образ ViPNet xFirewall xF-VA, установите сетевое соединение на виртуальном интерфейсе NetworkAdapter 1.
4. Установите вручную на сетевом интерфейсе ноутбука технологический IP-адрес `169.254.241.5`.
5. Подключитесь к ViPNet xFirewall по Telnet либо по протоколу SSH (с помощью стандартного Telnet- или SSH-клиента) по адресу `169.254.241.1`. Для корректной работы на Telnet- или SSH-клиенте должны быть заданы следующие параметры (далее для примера приведены настройки клиента PuTTY):
   - Тип терминала VT100 (**Terminal** > **Keyboard** > **VT100+**).
   - Кодировка символов KOI8-R (**Window** > **Translation**, в списке **Remote character set** выберите **KOI8-R** или **KOI8-U**).
   - Метод ввода linux (**Connection** > **Data** > **Terminal type string**, введите **linux**).
   - Ширина окна по умолчанию 120 (**Windows** > **Columns**, введите **120**).символов.

# Подготовка к установке справочников и лицензии с помощью внешнего устройства

Перед началом установки справочников и лицензии с помощью внешнего устройства выполните следующее:

1 При использовании USB-носителя:

1.1 Отформатируйте носитель в одну из поддерживаемых файловых систем: FAT32, ext2, ext3 или ext4.

1.2 Перенесите на носитель дистрибутив ключей (файл `*.dst`).

При использовании CD-диска запишите на него файл `*.dst`.

2 Подключитесь к ViPNet xFirewall через обычную или COM-консоль:

- Подключите монитор и клавиатуру к VGA-порту и PS/2-порту ПАК ViPNet xFirewall или компьютера, на котором развернут виртуальный образ ViPNet xFirewall.
- Подключите ноутбук к COM-порту RS-232 ПАК ViPNet xFirewall или компьютера, на котором развернут виртуальный образ ViPNet xFirewall.

**Примечание.** В аппаратной платформе xFirewall xF100 N1 вместо COM-порта присутствует служебный порт RJ45 для подключения ноутбука.

# Установка справочников и лицензии

Для установки справочников и лицензии на ViPNet xFirewall выполните все действия из приведенной ниже таблицы в предложенном порядке.

*Таблица 5. Последовательность установки справочников и лицензии*

| | Действие | Ссылка |
|---|---|---|
| ☐ | Запустите установку справочников и лицензии на ViPNet xFirewall | Начало установки (на стр. 27) |
| ☐ | Укажите часовой пояс, дату и время | Настройка часового пояса, даты и времени (на стр. 28) |
| ☐ | Выберите нужный дистрибутив лицензии | Установка дистрибутива лицензии на ViPNet xFirewall (на стр. 30) |
| ☐ | Настройте параметры всех сетевых интерфейсов ViPNet xFirewall | Настройка сетевых интерфейсов (на стр. 33) |
| ☐ | Настройте параметры DNS-сервера | Настройка DNS-сервера (на стр. 32) |
| ☐ | Настройте параметры NTP-сервера | Настройка NTP-сервера (на стр. 34) |
| ☐ | При необходимости измените настройки виртуальных адресов | Настройка имени компьютера и диапазона виртуальных адресов (на стр. 35) |
| ☐ | Завершите установку справочников и лицензии | Завершение установки (на стр. 36) |

**Совет.** Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

## Начало установки

Установка справочников и лицензии производится с помощью мастера установки, который запускается автоматически после авторизации в операционной системе. Мастер установки может работать в одном из двух режимов:

- обычный консольный режим;
- полноэкранный режим с эмуляцией графического интерфейса.

Выбрать режим работы предлагается сразу после запуска мастера. При описании установки справочников и лицензии приведены оба варианта работы с мастером — в консольном режиме и в полноэкранном режиме.

**Внимание!** При работе в полноэкранном режиме не поддерживаются «горячие клавиши».

В полноэкранном режиме для управления установкой предусмотрены следующие кнопки:

- **Next** — переход к следующему шагу;
- **Back** — возврат к предыдущему шагу;
- **Cancel** — прерывание установки. В случае прерывания установки состояние системы не изменяется — она остается в том состоянии, в котором была до начала установки.

Для управления установкой в полноэкранном режиме также могут использоваться следующие клавиши:

- **Tab** — переход между элементами интерфейса.
- «пробел» — выбор пункта меню.
- «стрелка вверх», «стрелка вниз», «+», «–» — задание числовых значений (например, времени), переход между элементами интерфейса.

Для начала установки справочников и лицензии выполните следующие действия:

1. Введите имя пользователя `user` и пароль `user`. После авторизации в системе автоматически будет запущен мастер установки.
2. Выберите режим работы мастера в ответ на сообщение `Please select setup wizard operating mode`:
   - `1` — консольный;
   - `2` — полноэкранный.
3. Ознакомьтесь с лицензионным соглашением с конечным пользователем на использование ПО ViPNet xFirewall. Для просмотра лицензионного соглашения вы можете использовать клавиши **PageUp** и **PageDown**. Введите символ `Y`, если вы согласны принять соглашение с пользователем, или символ `N` в противном случае.
4. В ответ на предложение начать установку в консольном режиме `Would you like to start installing keys or restoring configuration? [y/n]` введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.

# Настройка часового пояса, даты и времени

Следующие шаги предназначены для задания часового пояса (временной зоны), текущих даты и времени. Часовой пояс должен соответствовать географическому местоположению ViPNet

xFirewall. При установке справочников и лицензии из файла `*.vbe` эти шаги выполняются автоматически, так как настройки часового пояса импортируются из файла экспорта.

Для настройки часового пояса, даты и времени ViPNet xFirewall выполните следующие действия:

1 Выберите континент. Для этого введите номер континента из предложенного списка и нажмите клавишу **Enter**. В полноэкранном режиме выберите континент в списке и нажмите кнопку **Next**.

Если на ViPNet xFirewall необходимо установить время UTC, выберите в списке последний элемент. В этом случае сразу выводится информация о текущем времени UTC и запрашивается подтверждение на его установку.

2 Выберите страну. Для этого введите номер страны из предложенного списка и нажмите клавишу **Enter**. В полноэкранном режиме выберите страну в списке и нажмите кнопку **Next**. Список содержит страны, расположенные на выбранном континенте.

3 Выберите часовой пояс. Для этого введите номер пояса и нажмите клавишу **Enter**. В полноэкранном режиме выберите часовой пояс в списке и нажмите кнопку **Next**. Список содержит часовые пояса, имеющиеся в выбранной стране.

Если в выбранной на предыдущем шаге стране есть только один часовой пояс, он выбирается автоматически.

4 Подтвердите установку выбранного часового пояса. Если выбран нужный часовой пояс, в ответ на сообщение с информацией о текущем времени в этом поясе и вопросом `Is the above information OK?` введите символ `1` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**.

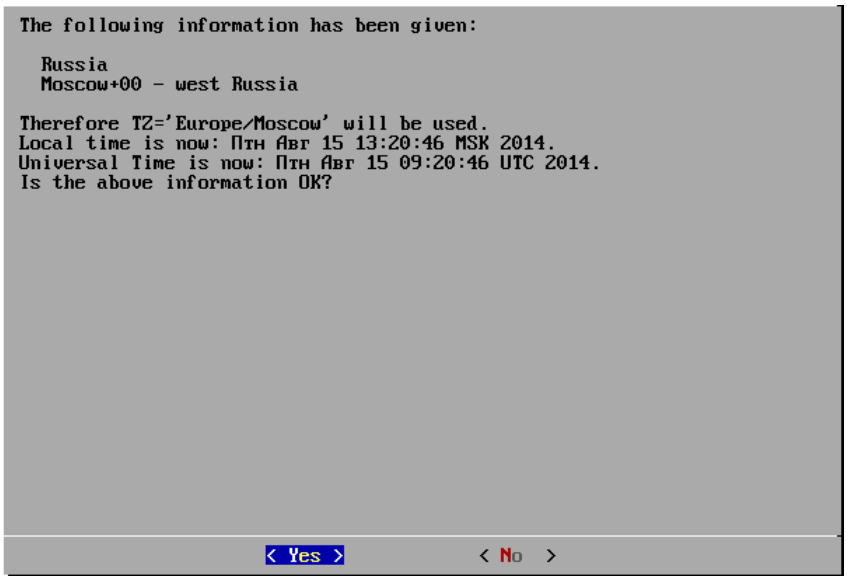


*Рисунок 11. Запрос на установку часового пояса*

Если необходимо установить другой часовой пояс, введите символ `2` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. После отказа от установки этого часового пояса мастер вернется к выбору континента.

5 Если требуется изменить текущую дату и время, введите их в формате `YYYY-MM-DD hh:mm:ss` (`год-месяц-день час-минуты-секунды`) и нажмите клавишу **Enter**.

**Примечание.** Если требуется изменить только время, то дату вы можете не вводить.

В полноэкранном режиме на одной странице установите нужную дату с помощью календаря, на следующей странице установите время с помощью клавиш «стрелка вверх», «стрелка вниз» или «+», «-», после чего нажмите кнопку **Next**.

Если дату и время изменять не нужно, нажмите клавишу **Enter**. В полноэкранном режиме 2 раза нажмите кнопку **Next**.

# Установка дистрибутива лицензии на ViPNet xFirewall

Для переноса и установки дистрибутива ключей `*.dst` или файла импорта `*.vbe` на ViPNet xFirewall выполните следующие действия:

1. Выберите один из предложенных способов переноса файла. Для этого в ответ на сообщение `Would you like installing keys from TFTP, USB or CD storage device? [t/u/c]` введите один из символов:
   - `t` — для переноса с ноутбука по протоколу TFTP;
   - `u` — для переноса с USB-носителя;
   - `c` — для переноса с CD-диска.

   В полноэкранном режиме установите переключатель в нужное положение с помощью клавиши «пробел» и нажмите кнопку **Next**.
2. Перенесите файл выбранным способом.

   Если вы выбрали способ переноса по TFTP, выполните на ноутбуке команду:

   `tftp -i 169.254.241.1 put <имя файла>`,

   после чего нажмите на консоли клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.

   Если вы выбрали способ переноса с USB-носителя или CD-диска, подключите устройство к одному из USB-разъемов ПАК ViPNet xFirewall или компьютера, на котором развернут виртуальный образ ViPNet xFirewall и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.
3. Если на USB-носителе или CD-диске будет обнаружен только один файл, то в консольном режиме он будет выбран для установки автоматически. В полноэкранном режиме список будет содержать только этот файл.

   Если обнаружено несколько файлов `*.dst` и `*.vbe`, появится пронумерованный список `Found several dst and vbe files`. Для файлов `*.dst` дополнительно указываются имена и

идентификаторы сетевых узлов, которым они соответствуют. В этом случае выберите файл для установки. Для этого введите номер файла из предложенного списка и нажмите клавишу **Enter**. Если номер не введен или введен некорректный номер, появится сообщение с предложением заново ввести номер файла. В полноэкранном режиме выберите файл в списке и нажмите кнопку **Next**.


*Рисунок 12. Выбор файла для установки справочников и лицензии*

В консольном режиме, если найдено больше 20 файлов, список выводится постранично по 20 файлов на странице. На каждой странице появляется предложение выбрать нужный файл либо перейти к следующей или первой странице.

---

**Совет.** В полноэкранном режиме длинные имена файлов могут быть не видны в списке полностью. Чтобы увидеть полное имя, выберите файл в списке — его имя будет отображено под окном мастера.

---

Если файлов нет, появится сообщение `DST or VBE files are not found`. Заново выберите способ переноса файла. В полноэкранном режиме нажмите в окне сообщения кнопку **Back**, произойдет возврат к предыдущему шагу.

4 Введите пароль к дистрибутиву ключей или пароль доступа к файлу экспорта в ответ на сообщение `Enter password` и нажмите клавишу **Enter**. В полноэкранном режиме после ввода пароля нажмите кнопку **Next**.

Если введенный пароль верен, то начнется установка справочников и лицензии из выбранного файла.

По завершении установки справочников и лицензии из дистрибутива лицензии появится информация об узле, и мастер перейдет к следующему шагу (см. Настройка сетевых интерфейсов на стр. 33). По завершении установки справочников и лицензии из файла экспорта мастер предложит перезагрузить компьютер (см. Завершение установки на стр. 36).

# Настройка DNS-сервера

Для настройки DNS-сервера выполните следующие действия:

1 Включите автоматический запуск DNS-сервера при загрузке ViPNet xFirewall, если это необходимо. Для этого в ответ на сообщение `Do you want to use DNS server? [y/n]` введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **ON (Enable starting the DNS server at boot)** и нажмите кнопку **Next**.

   После включения автоматического запуска DNS-сервера мастер перейдет к следующему шагу.

   Если DNS-сервер запускать не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **OFF (Disable starting the DNS server at boot)** и нажмите кнопку **Next**. В этом случае мастер перейдет к настройке NTP-сервера (см. Настройка NTP-сервера на стр. 34).

2 Появится сообщение, что при наличии подключения к Интернету в качестве DNS-серверов по умолчанию используются корневые DNS-серверы. При этом вы можете принять или отклонить предложение добавить DNS-сервер `Do you want to add custom DNS server? [y/n]`.

   - Если необходимо добавить конкретный DNS-сервер, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **Yes (Add custom DNS server)** и нажмите кнопку **Next**.

     После этого введите IP-адрес DNS-сервера и нажмите клавишу **Enter**. В полноэкранном режиме после ввода адреса нажмите кнопку **Next**.

   - Если DNS-сервер добавлять не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **No (Leave the default setting)** и нажмите кнопку **Next**. В этом случае будут использоваться либо настройки по умолчанию, либо текущие настройки (если это не первая установка справочников и лицензии).

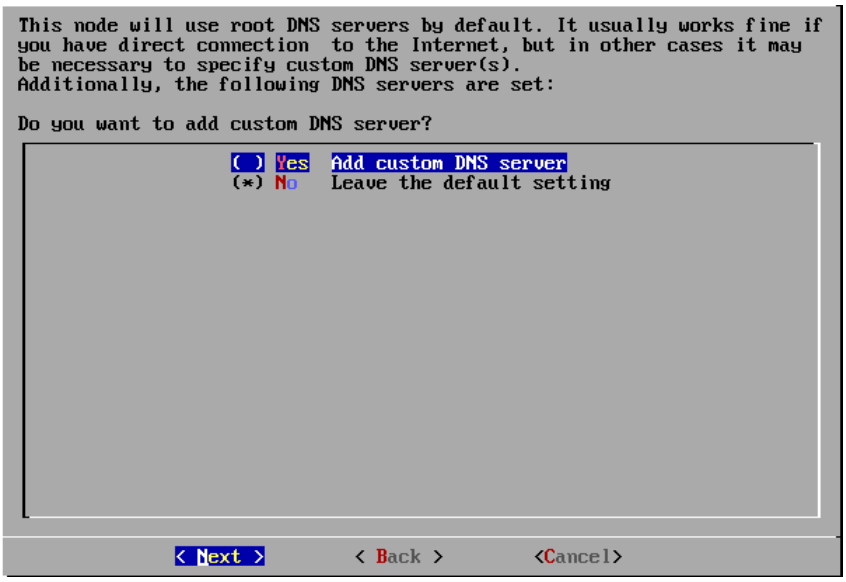


*Рисунок 13. Запрос на добавление адреса DNS-сервера*

После отказа от добавления DNS-сервера мастер перейдет к настройке NTP-сервера.

# Настройка сетевых интерфейсов

При импорте справочников и лицензии из файла `.vbe` следующие шаги вплоть до завершения установки пропускаются, так как все настройки импортируются из файла экспорта. В результате успешного импорта и после перезагрузки компьютера на ViPNet xFirewall будут установлены те настройки, которые были на момент выполнения экспорта (см. Завершение установки на стр. 36).

При установке справочников и лицензии из файла `*.dst` следующие шаги вам необходимо выполнить для каждого сетевого интерфейса ViPNet xFirewall.

Для настройки сетевых интерфейсов ViPNet xFirewall выполните следующие действия:

1. Включите интерфейс, если это необходимо. Для этого в консоли в ответ на сообщение `Configure interface eth<номер>? [y/n]` введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **UP** с помощью клавиши «пробел» и нажмите кнопку **Next**.

   После включения интерфейса мастер перейдет к следующему шагу.

   Если интерфейс включать не надо, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **DOWN** и нажмите кнопку **Next**. Мастер предложит настроить следующий сетевой интерфейс. В случае отказа от конфигурации последнего сетевого интерфейса, мастер перейдет к настройке DNS-сервера (см. Настройка DNS-сервера на стр. 32).

2. Установите для интерфейса режим DHCP, если это необходимо. Для этого в ответ на сообщение `Use dhcp on the interface eth<номер>? [y/n]` введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **DHCP** и нажмите кнопку **Next**.

   Если для интерфейса нужно задать статические параметры, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **StaticIP** и нажмите кнопку **Next**.

3. Если для интерфейса не был выбран режим DHCP, введите последовательно IP-адрес и маску интерфейса и нажмите клавишу **Enter**. В полноэкранном режиме введите параметры интерфейса в соответствующие поля, используя для перехода между полями ввода клавишу «стрелка вниз», после чего нажмите кнопку **Next**.

   Если сконфигурированный на данном шаге интерфейс не последний, мастер переходит к конфигурированию следующего интерфейса.

4. Если ни для одного включенного интерфейса не был задан режим DHCP, введите IP-адрес шлюза по умолчанию и нажмите клавишу **Enter**. В полноэкранном режиме после ввода адреса нажмите кнопку **Next**.

# Настройка NTP-сервера

Для настройки NTP-сервера выполните следующие действия:

1 Включите автоматический запуск NTP-сервера при загрузке ViPNet xFirewall, если это необходимо. Для этого в ответ на сообщение `Do you want to use NTP daemon to synchronize the time? [y/n]` введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **ON (Enable starting the NTP server at boot)** и нажмите кнопку **Next**.

После включения автоматического запуска NTP-сервера мастер перейдет к следующему шагу.

Если NTP-сервер запускать не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **OFF (Disable starting the NTP server at boot)** и нажмите кнопку **Next**. В этом случае мастер перейдет к настройке имени компьютера (см. Настройка имени компьютера и диапазона виртуальных адресов на стр. 35).

2 Появится сообщение, что для синхронизации системного времени по умолчанию будут использоваться публичные NTP-серверы точного времени. При этом вы можете принять или отклонить предложение добавить NTP-сервер `Do you want to add custom NTP server? [y/n]`.

- Если необходимо добавить конкретный NTP-сервер, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **Yes (Add custom NTP server)** и нажмите кнопку **Next**.

  После этого введите IP-адрес или DNS-имя NTP-сервера и нажмите клавишу **Enter**. В полноэкранном режиме после ввода нажмите кнопку **Next**.

  **Примечание.** IP-адрес NTP-сервера должен соответствовать следующим требованиям:

  - первый октет должен быть больше 0 и меньше 224;
  - остальные октеты должны быть не больше 255.

- Если NTP-сервер добавлять не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **No (Leave the default setting)** и нажмите кнопку **Next**. В этом случае будут использоваться либо настройки по умолчанию, либо текущие настройки (если это не первая установка справочников и лицензии).

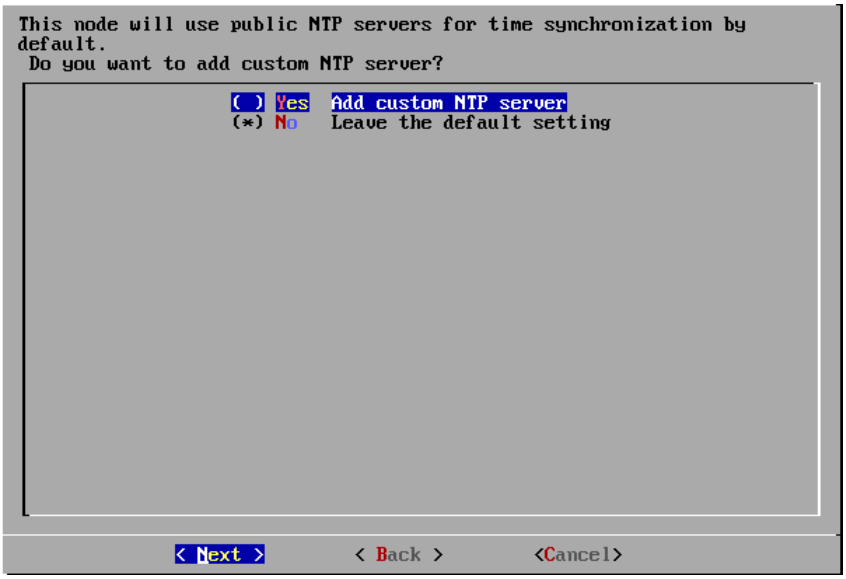


*Рисунок 14. Запрос на добавление NTP-сервера*

После отказа от добавления NTP-сервера мастер перейдет к установке имени компьютера.

# Настройка имени компьютера и диапазона виртуальных адресов

Для настройки имени компьютера и диапазона виртуальных адресов выполните следующие действия:

1 Введите имя компьютера, если вы не хотите оставить имя, заданное по умолчанию, и нажмите клавишу **Enter**. В полноэкранном режиме введите нужное имя и нажмите кнопку **Next**.

По умолчанию предлагается имя, сформированное по шаблону `<исполнение ViPNet xFirewall>-<идентификатор узла ViPNet>`. Например: `xF1000-270E033A`.

Если имя изменять не нужно, нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.

2 Мастер перейдет к настройке виртуальных адресов. Появится текущий диапазон виртуальных адресов, назначаемых узлам сети, и предложение его изменить `Do you want to specify custom virtual IP address range? [y/n]`.

---

**Примечание.** По умолчанию предлагается диапазон виртуальных адресов 11.0.0.1-11.0.254.254. Если этот диапазон пересекается с диапазоном IP-адресов, который используется для адресации в вашей сети, измените его.

---

Подробнее о виртуальных адресах см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Принципы назначения виртуальных адресов».

Выполните одно из действий:

- Если необходимо задать другой диапазон виртуальных адресов, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **Yes (Set custom virtual IP range)** и нажмите кнопку **Next**.

  После этого введите начальный и конечный адреса нового диапазона виртуальных адресов и нажмите клавишу **Enter**. Например: 11.0.0.1-11.0.254.254. В полноэкранном режиме после ввода нажмите кнопку **Next**.

- Если диапазон виртуальных адресов изменять не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **No (Leave the default setting)** и нажмите кнопку **Next**.

3 Если на предыдущем этапе вы настроили хотя бы один сетевой интерфейс, мастер предложит завершить установку.

# Завершение установки

Для завершения установки справочников и лицензии выполните следующие действия:

1 Если производится импорт справочников, лицензии и настроек из файла `.vbe`, то появится сообщение с предложением перезагрузить компьютер для корректного применения настроек. Для перезагрузки введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Reboot**. Работа мастера будет завершена, и компьютер перезагрузится.

   Если вы хотите отказаться от немедленной перезагрузки, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Continue**.

**Примечание.** Применение всех настроек, импортированных из файла `*.vbe`, произойдет только после перезагрузки. В случае отказа перезагрузите компьютер вручную.

2 Появится сообщение с предложением автоматически запустить драйверы и демоны ViPNet xFirewall после завершения установки `Do you want to start VPN services before leaving the installation wizard? [y/n]`. Для запуска введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**.

   Если драйверы и демоны запускать не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. В этом случае после установки лицензии необходимо вручную запустить демоны и драйверы с помощью команды:

   ```
   hostname# vpn start
   ```

3 Появится сообщение об успешном завершении установки, и мастер предложит запустить командный интерпретатор: `Do you want to start the command shell now? [y/n]`. Чтобы запустить командный интерпретатор, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Run Command shell**.

   Если командный интерпретатор запускать не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Finish**. Работа мастера будет завершена без запуска командного интерпретатора.

4 Если при установке лицензии были настроены DNS- и NTP-серверы, запустите их с помощью команд:

```
hostname# inet dns start
hostname# inet ntp start
```

# Обновление и удаление справочников и лицензии

Если администратор сети ViPNet вносит какие-либо изменения в структуру сети или настройки отдельных сетевых узлов, например, создает новые связи между сетевыми узлами, то автоматически изменяются справочники и лицензия, и их требуется обновить на сетевых узлах.

Обновления справочников и лицензии могут быть созданы и централизованно отправлены на сетевые узлы, которых коснулись изменения, администратором сети с помощью программы ViPNet Administrator. Поступившие обновления справочников и лицензии на ViPNet xFirewall будут приняты в автоматическом режиме.

Информация о принятых обновлениях записывается в журнал обновления справочников и лицензии. Для просмотра этого журнала выполните команду:

```
hostname# iplir show keys-upgrade-log
```

Если по каким-либо причинам обновление справочников и лицензии не может быть принято по сети, вы можете обновить справочники и лицензию вручную с помощью дистрибутива лицензии.

---

**Внимание!** После обновления справочников и лицензии с помощью дистрибутива лицензии будут потеряны все настройки ViPNet xFirewall, произведенные вручную, и их необходимо будет задать заново. Некоторые настройки вы можете задать в процессе установки справочников и лицензии из нового дистрибутива, остальные необходимые настройки потребуется задать после завершения обновления.

---

Для этого выполните следующие действия:

1. Получите новый дистрибутив лицензии у администратора сети ViPNet.
2. Завершите работу демонов `iplircfg`, `failoverd` и `mftpd` с помощью команды:

   ```
   hostname# vpn stop
   ```
3. Удалите текущие справочники и лицензию с помощью команды:

   ```
   hostname# admin remove keys
   ```
4. Установите справочники и лицензию из нового дистрибутива лицензии (см. Установка, обновление и удаление справочников и лицензии на стр. 22). В конце процедуры установки согласитесь с запуском демонов и командного интерпретатора.
5. Задайте настройки, которые были потеряны в процессе обновления справочников и лицензии.

# 3

# Обновление программного обеспечения


Удаленное обновление ПО 40

Локальное обновление ПО 41

Обновление модуля DPI 43

Деактивация правил межсетевого экрана 45

Обновление ПО на кластере горячего резервирования 47

# Удаленное обновление ПО

Удаленное обновление ПО ViPNet xFirewall производится с помощью программы ViPNet Центр управления сетью (далее — ЦУС) (см. глоссарий, стр. 55). Администратор сети ViPNet получает у представителей ОАО «ИнфоТеКС» файл формата LZH с новой версией ПО и из ЦУСа рассылает файл обновления на все узлы ViPNet xFirewall, на которых необходимо выполнить обновление.

Для разных исполнений ViPNet xFirewall передаются следующие файлы обновления ПО:

- для xFirewall xF100 — `xf100_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh`;
- для xFirewall xF1000 — `xf1000_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh`;
- для xFirewall xF5000 — `xf5000_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh`;
- для xFirewall xF-VA — `xfva_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh`.

Процедура удаленного обновления ПО подробно описана в документе «ViPNet Центр управления сетью. Руководство администратора». На ViPNet xFirewall обновление принимается и выполняется автоматически, после обновления выполняется перезагрузка. Перед обновлением настоятельно рекомендуется сделать экспорт справочников, лицензии и настроек ViPNet xFirewall в файл `*.vbe`. Это позволит вам восстановить их на ViPNet xFirewall, если обновление ПО пройдет некорректно (см. Импорт справочников, лицензии и настроек на стр. 53).

# Локальное обновление ПО

Прежде чем начать локальное обновление ПО на ViPNet xFirewall, выполните следующие действия:

- У администратора сети получите файл дистрибутива ПО ViPNet xFirewall новой версии (файл формата LZH) и запишите его на USB-носитель.

**Примечание.** На один USB-носитель можно записать несколько файлов обновления, предназначенных для различных исполнений ViPNet xFirewall (разместив их в разных каталогах). При выполнении локального обновления производится анализ содержимого USB-носителя и становится доступным для использования только тот дистрибутив, которые соответствуют данному исполнению ViPNet xFirewall.

- Выполните экспорт справочников, лицензии и настроек ViPNet xFirewall в файл `*.vbe`. Это позволит вам восстановить их на ViPNet xFirewall, если обновление ПО пройдет некорректно (см. Импорт справочников, лицензии и настроек на стр. 53).

Для локального обновления ПО выполните следующие действия:

1. На ViPNet xFirewall выполните команду:

   ```
   hostname# admin upgrade software usb
   ```

   При этом появится предложение подключить USB-носитель.

2. Подключите USB-носитель к USB-разъему ViPNet xFirewall или компьютера, на котором развернут виртуальный образ ViPNet xFirewall, и подтвердите подключение.

   Если USB-носитель не найден, появится соответствующее сообщение, выполнение команды завершается, обновление не производится.

3. На USB-носителе производится поиск файлов LZH:
   - Если файлов нет, появляется соответствующее сообщение и выполнение команды завершается, обновление не производится.
   - Если файлы найдены:
     - Проверяется целостность архива LZH каждого из файлов.
     - Для каждого файла, прошедшего проверку целостности, также проверяется, соответствует ли он данному исполнению ViPNet xFirewall.
     - Выводится пронумерованный список отобранных файлов. Выберите файл, в имени которого указана нужная версия обновления ПО.
4. Введите номер выбранного файла обновления и нажмите клавишу **Enter**.

**Внимание!** При использовании кластера горячего резервирования локальное обновление ПО должно быть произведено на обоих серверах кластера (см. Обновление ПО на кластере горячего резервирования на стр. 47).

5 Дождитесь появления сообщения о результате обновления.

6 После обновления перезагрузите ViPNet xFirewall, чтобы обновление вступило в силу.

# Обновление модуля DPI

Для поддержания актуального набора приложений и прикладных протоколов, а также групп приложений необходимо регулярно обновлять модуль DPI (см. глоссарий, стр. 54). Обновление можно выполнять двумя способами:

- Централизованно с помощью ПО ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 55). Подробнее см. документ «ViPNet Administrator. Руководство администратора».
- Вручную с помощью командного интерпретатора.

**Внимание!** При обновлении модуля DPI будут прерваны все сетевые соединения и ViPNet xFirewall будет перезагружен. Правила межсетевого экрана, в которых заданы приложения, прикладные протоколы и группы приложений, не поддерживаемые в новой версии модуля DPI, будут деактивированы (см. Деактивация правил межсетевого экрана на стр. 45).

Вы можете выполнить откат к версии модуля DPI, вплоть до версии, которая входила в состав ПО ViPNet xFirewall 4.1.0 при поставке. В этом случае будут деактивированы (см. Деактивация правил межсетевого экрана на стр. 45) правила межсетевого экрана, в которых заданы приложения, прикладные протоколы и группы приложений, не поддерживаемые новой версией модуля DPI или отсутствующие в предыдущей версии.

Для ручного обновления модуля DPI выполните следующие действия:

1. Отформатируйте USB-носитель в одну из поддерживаемых файловых систем: FAT32, ext2, ext3 или ext4.
2. Скопируйте на носитель файл обновления модуля DPI. Имя файла должно иметь формат `<platform>_<vipnet>_<base>_<architecture>_<version>_<DPI_base_release_date>.lzh`, например:

   ```
   xf100_vipnet_base_i386_1.0_16.01.31_dpi.lzh
   ```
3. Выполните команду:

   ```
   hostname# admin upgrade dpi usb
   ```

**Внимание!** Выполнить команду необходимо через COM-консоль (см. глоссарий, стр. 54) или обычную консоль (см. глоссарий, стр. 56). Удаленное выполнение команды по протоколу SSH невозможно.

4. На вопрос об остановке сетевого экрана и блокировке всех соединений ответьте утвердительно (введите символ «y» и нажмите клавишу **Enter**).
5. Подключите USB-носитель к USB-разъему ViPNet xFirewall или компьютера, на котором развернут виртуальный образ ViPNet xFirewall, и подтвердите подключение (нажмите клавишу **Enter**).

Если USB-носитель не найден, появится соответствующее сообщение, выполнение команды завершается, обновление не производится.

6 На USB-носителе производится поиск файлов LZH:

- Если файлов нет или найденные файлы не являются файлами обновления модуля DPI, появляется соответствующее сообщение и выполнение команды завершается, обновление не производится.
- Если файлы найдены:
  - Проверяется целостность каждого из файлов.
  - Выводится пронумерованный список отобранных файлов. Выберите файл, в имени которого указана нужная версия обновления модуля DPI.

7 Введите номер выбранного файла обновления и нажмите клавишу **Enter**.

8 Дождитесь появления сообщения о результате обновления.

9 После обновления извлеките USB-носитель и нажмите клавишу **Enter**, чтобы перезагрузить ViPNet xFirewall.

# Деактивация правил межсетевого экрана

При обновлении программного обеспечения ViPNet xFirewall или обновлении модуля DPI (включая откат к предыдущей версии) возможно изменение схемы описания прикладных протоколов, приложений и групп приложений. В этом случае:

- Правила межсетевого экрана, содержащие прикладной протокол, приложение или группу приложений, которые отсутствуют в новой схеме, применяться не будут.
- Если в правиле обнаружены неподдерживаемые прикладные протоколы, приложения или группы приложений, то они отмечается как **Unsupported**.
- Если в правиле не остается ни одного работающего прикладного протокола, приложения, группы приложений, то правило отмечается как **Inactive**.

## Действия в веб-интерфейсе

При отображении в веб-интерфейсе неподдерживаемый прикладной протокол, приложение, группа приложений выделяется красным цветом.

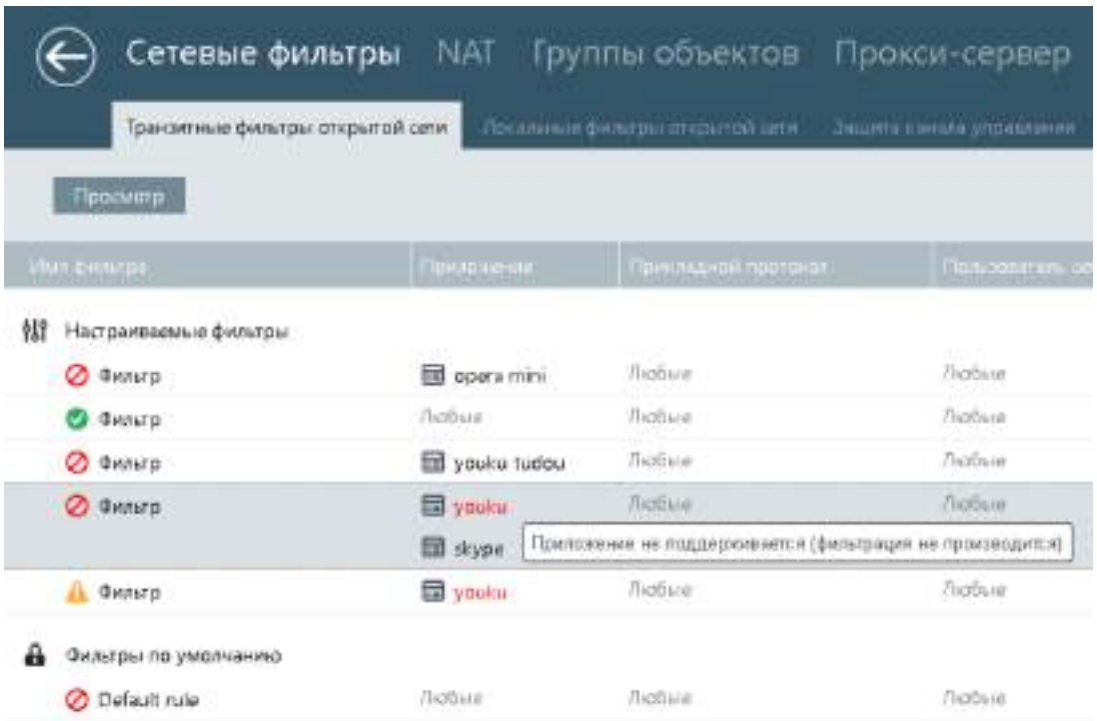


*Рисунок 15. Отображение неподдерживаемых параметров правила в веб-интерфейсе*

Вы можете отредактировать неактивное правило и затем активировать его (см. документ «ViPNet xFirewall. Настройка с помощью веб-интерфейса», раздел «Создание и изменение сетевого фильтра»).

## Действия в интерфейсе командного интерпретатора

При отображении в интерфейсе командного интерпретатора неподдерживаемый прикладной протокол, приложение, группа приложений и название неактивного правила выделяются инверсией.


*Рисунок 16. Отображение неактивного правила в интерфейсе командного интерпретатора*

Вы можете отредактировать неактивное правило (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Изменение сетевого фильтра»), но не можете его активировать.

# Обновление ПО на кластере горячего резервирования

Для обеспечения отказоустойчивой фильтрации трафика вы можете настроить работу ViPNet xFirewall в режиме кластера горячего реферирования (подробнее см. документ «ViPNet. Настройка с помощью командного интерпретатора», раздел «Работа системы защиты от сбоев в режиме кластера горячего резервирования»).

Обновление ПО ViPNet xFirewall на кластере горячего резервирования может выполняться удаленно или локально. Удаленное обновление выполняется автоматически на обоих серверах кластера. Локальное обновление на кластере имеет ряд особенностей, порядок его выполнения приведен ниже.

Для локального обновления ПО на кластере выполните следующие действия:

1. Выключите интерфейс резервного канала на обоих серверах кластера с помощью команды:

   `hostname# inet ifconfig <интерфейс> down`

   Затем отсоедините кросс-кабель от компьютеров.

2. Обновите ПО на пассивном ViPNet xFirewall (так же, как при работе в одиночном режиме (см. Локальное обновление ПО на стр. 41)) с помощью команды:

   `hostname# admin upgrade software usb`

   Информацию о текущем режиме ViPNet xFirewall можно получить с помощью команды `hostname> failover show info`.

3. После обновления перезагрузите пассивный ViPNet xFirewall. Для этого в ответ на предложение перезагрузки нажмите клавишу **Enter**.

   Убедитесь в стабильной работе ViPNet xFirewall:

   - Проверьте текущее состояние служб ViPNet с помощью команды:

     `hostname> failover show info`

     Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера.

   - В течение некоторого времени (около 15 минут) последите за работой пассивного ViPNet xFirewall и убедитесь, что он не перезагружается.

4. Перезагрузите активный ViPNet xFirewall, для этого выполните команду:

   `hostname> machine reboot`

   В результате пассивный ViPNet xFirewall (с обновленным ПО) перейдет в активный режим, а ViPNet xFirewall со старой версией ПО окажется в пассивном режиме.

5. Обновите ПО на пассивном ViPNet xFirewall, для этого выполните команду:

   `hostname# admin upgrade software usb`

6 После обновления перезагрузите пассивный ViPNet xFirewall и убедитесь в его стабильной работе (как на шаге 3).

7 Соедините оба ViPNet xFirewall (или оба компьютера, на которых развернуты виртуальные образы ViPNet xFirewall xF-VA) кросс-кабелем и включите интерфейс резервного канала с помощью команды:

```
hostname# inet ifconfig <интерфейс> up
```

8 Убедитесь, что резервный канал функционирует нормально. Для этого измените какую-либо настройку в файле конфигурации на активном ViPNet xFirewall и через некоторое время проверьте наличие этих же изменений на пассивном ViPNet xFirewall. Чтобы изменения попали на пассивный ViPNet xFirewall, необходимо включить резервирование группы файлов конфигурации в файле `failover.ini` в секции `[sendconfig]`.

# 4

# Резервное копирование и восстановление настроек


Назначение экспорта и импорта справочников, лицензии и настроек 50

Экспорт справочников, лицензии и настроек 51

Импорт справочников, лицензии и настроек 53

# Назначение экспорта и импорта справочников, лицензии и настроек

Вы можете использовать экспорт и импорт справочников, лицензии и настроек ViPNet xFirewall в следующих ситуациях:

- Сохранение и восстановление данных на ViPNet xFirewall в случае некорректного обновления ПО.
- Перенос справочников, лицензии и настроек с одного сервера ViPNet xFirewall на другой, например, в случае замены аппаратной платформы. Это позволяет упростить подготовку нового ViPNet xFirewall к работе, так как не требуется выполнять установку справочников и лицензии и необходимые настройки вручную.

  В этом случае оба сервера ViPNet xFirewall должны иметь одинаковые исполнение и тип лицензии. Кроме этого, по завершении импорта сервер, с которого переносятся данные, должен быть отключен от сети или на нем должны быть удалены справочники и лицензии. Это связано с тем, что в сети ViPNet не допускается функционирование нескольких узлов с одинаковыми справочниками и лицензиями.

В состав экспортируемой информации входят следующие данные:

- файлы, содержащие информацию о связанных с ViPNet xFirewall узлах (справочники);
- настройки подключения к сети ViPNet (файл `iplir.conf`);
- настройки сетевых интерфейсов (IP-адрес, маска подсети, файл `iplir.conf-<интерфейс>`);
- настройки динамической маршрутизации и статические маршруты, если такие созданы;
- настройки часового пояса;
- сетевые фильтры и правила трансляции адресов;
- настройки параметров обработки прикладных протоколов;
- настройки системы защиты от сбоев (файл `failover.ini`);
- настройки транспортного модуля (файл `mftp.conf`);
- настройки протоколирования;
- настройки дополнительных сервисов (DHCP-сервера и других);
- настройки взаимодействия с UPS;
- текущие ключи для соединений по протоколу SSH2.

# Экспорт справочников, лицензии и настроек

Экспорт справочников, лицензии и настроек требуется выполнять в следующих случаях:

- Перед обновлением ПО на ViPNet xFirewall (см. Обновление программного обеспечения на стр. 39), а также периодически для возможности восстановления данных в случае сбоев в работе.

---

**Примечание.** Периодичность резервирования данных на ViPNet xFirewall определяется регламентом безопасности вашей организации.

---

- При переносе справочников, лицензии и настроек на другой ViPNet xFirewall аналогичного исполнения (например, при замене аппаратной платформы).

Экспорт справочников, лицензии и настроек вы можете выполнить только при непосредственном доступе к ViPNet xFirewall или виртуальному образу ViPNet xFirewall одним из следующих способов:

- На ноутбук, подключенный через сетевой кросс-кабель Ethernet и технологический адрес.
- На USB-носитель при подключении через обычную консоль (с использованием монитора и клавиатуры) или COM-консоль (с использованием ноутбука). Перед началом экспорта этим способом отформатируйте USB-носитель в одну из поддерживаемых файловых систем: FAT32, ext2, ext3 или ext4.

---

**Внимание!** Экспортировать справочники, лицензию и настройки в удаленной SSH-сессии запрещено.

---

На время выполнения экспорта с использованием ноутбука (после ввода команды) автоматически изменяются настройки сетевых интерфейсов ViPNet xFirewall: на интерфейсе Ethernet1 устанавливается технологический IP-адрес `169.254.241.1`, все остальные интерфейсы ViPNet xFirewall выключаются. Восстановление настроек интерфейсов ViPNet xFirewall производится только при успешном завершении экспорта.

Для экспорта справочников, лицензии и настроек выполните следующие действия:

1. Завершите работу демонов iplircfg и mftpd с помощью команд:

   ```
   hostname# iplir stop
   hostname# mftp stop
   ```

2. Выберите место сохранения файла экспорта с помощью команды:

   `hostname# admin export keys binary-encrypted {tftp | usb}`, где:

   - `tftp` — экспорт на ноутбук по протоколу TFTP.

- usb — экспорт на USB-носитель.

При успешном выполнении команды появится сообщение, что файл экспорта сформирован и сохранен в каталоге `/tmp/vipnet`:

```
Configuration file will be saved to tmp/vipnet/<имя файла экспорта>
```

**Примечание.** Имя файла экспорта формируется по следующему шаблону: `<название ViPNet xFirewall>-<идентификатор узла ViPNet>-<дата экспорта>.vbe`,

где `<название ViPNet xFirewall>` — наименование исполнения.

Файл экспорта автоматически зашифровывается на текущем пароле пользователя.

3 Перенесите сформированный файл экспорта на ноутбук или USB-носитель.

Для переноса файла на ноутбук выполните на нем команду:

```
tftp -i 169.254.241.1 get <имя файла экспорта>
```

Для переноса файла на USB-носитель выполните следующие действия:

3.1 Подключите USB-носитель к одному из USB-разъемов ViPNet xFirewall или компьютера, на котором развернут виртуальный образ ViPNet xFirewall в ответ на предложение

```
Put <имя файла экспорта> file onto USB drive.
```

```
Insert USB drive and press Enter.
```

3.2 Появится пронумерованный список всех обнаруженных устройств. Выберите USB-носитель для переноса на него файла экспорта. Для этого в ответ на сообщение `Select target partition [1-1] or 0 to abort` введите цифру, соответствующую USB-носителю в списке, и нажмите клавишу **Enter**.

3.3 При успешной записи файла экспорта на USB-носитель появится сообщение с разрешением извлечь устройство:

```
You may remove the USB drive.
```

**Внимание!** Необходимо дождаться этого сообщения прежде, чем извлечь USB-носитель из разъема.

4 Запустите демоны iplircfg и mftpd с помощью команд:

```
hostname# iplir start
```

```
hostname# mftp start
```

# Импорт справочников, лицензии и настроек

Импорт справочников, лицензии и настроек требуется выполнять в следующих случаях:

- Для восстановления данных при некорректном обновлении ПО на ViPNet xFirewall (см. Обновление программного обеспечения на стр. 39).
- Для загрузки справочников, лицензии и настроек с одного ViPNet xFirewall на другой (например, при замене аппаратной платформы).

Способы импорта справочников, лицензии и настроек на ViPNet xFirewall описаны в разделе Способы установки и подготовка к установке справочников и лицензии (на стр. 23).

Перед началом импорта убедитесь в наличие файла `*.vbe`, полученного в результате экспорта справочников, лицензии и настроек на действующем ViPNet xFirewall. Вместе с файлом `*.vbe` вам должен быть предоставлен пароль, на котором он зашифрован. Данный пароль потребуется ввести при выполнении импорта данных из файла `*.vbe`.

---

**Примечание.** При экспорте файл `*.vbe` автоматически зашифровывается на текущем пароле пользователя.

---

Кроме этого, если импорт справочников, лицензии и настроек выполняется на ViPNet xFirewall, на котором уже установлены справочники и лицензия, то удалите их перед началом импорта с помощью команды:

```
hostname# admin remove keys
```

В противном случае импорт данных будет невозможен.

Для импорта справочников, лицензии и настроек на ViPNet xFirewall выполните все действия из приведенной ниже таблицы в предложенном порядке.

*Таблица 6. Последовательность импорта справочников, лицензии и настроек*

| | Действие | Ссылка |
|---|---|---|
| ☐ | Инициируйте импорт справочников, лицензии и настроек на ViPNet xFirewall | Начало установки (на стр. 27) |
| ☐ | Укажите часовой пояс, дату и время | Настройка часового пояса, даты и времени (на стр. 28) |
| ☐ | Выберите файл экспорта `*.vbe` | Установка дистрибутива лицензии на ViPNet xFirewall (на стр. 30) |
| ☐ | Перезагрузите компьютер | Завершение установки (на стр. 36) |

# Глоссарий

## COM-консоль

Ноутбук, подключенный к COM-порту, который используется для локальной настройки ViPNet xFirewall.

## DHCP-сервер

Сервер, автоматически администрирующий IP-адреса DHCP-клиентов и выполняющий соответствующую настройку для сети.

## DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам компьютеров в интернет-домене. Например, ns.domain.net. Как правило, информация о домене хранится на двух DNS-серверах, называемых «Primary DNS» и «Secondary DNS» (дублирование делается для повышения отказоустойчивости системы).

Также DNS-сервер называют сервером доменных имен, сервером имен DNS.

## DPI (Deep Packet Inspection)

Технология расширенной инспекции содержимого трафика сетевых приложений на уровнях 2 — 7 модели OSI и накопления статистики.

На основании анализа полученных данных выполняется фильтрация трафика.

## NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между

эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

### ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

### Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

### Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

### Дистрибутив лицензии

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы ПО ViPNet xFirewall.

### Ключи узла ViPNet xFirewall

Совокупность ключей, с использованием которых производится шифрование служебной информации, передаваемой между ViPNet xFirewall и узлами сети ViPNet. Шифрование трафика клиентов сети ViPNet на ключах узла ViPNet xFirewall не производится.

### Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

### Обычная консоль

Монитор и клавиатура, которые используются для локальной настройки ViPNet xFirewall.

### Пароль пользователя

Индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

### Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

### Справочники и лицензия

Справочники, ключи узла и ключи пользователя.