ViPNet Coordinator VA

Подготовка к работе

infotecs

ФРКЕ.00130-03 90 01

Версия продукта 4.3.3

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: infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В документе описывается назначение и применение программного координатора ViPNet Coordinator VA® (далее — ViPNet Coordinator VA) в составе защищенных сетей ViPNet, способы настройки и управления, приводится описание условий лицензирования. Также описано развертывание виртуального образа ViPNet Coordinator VA, основные сценарии работы со справочниками и ключами узла.

Для кого предназначен документ

Документ предназначен для администраторов ViPNet Coordinator VA.

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# admin config list
  ```

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

  ```
  hostname> alg restart
  ```

- При описании в документе параметры, которые должны быть заданы пользователем, заключены в угловые скобки «<>»:

  ```
  inet bonding delete <номер>
  ```

  При вводе в командный интерпретатор параметры, которые должны быть заданы пользователем, вводятся без угловых скобок:

  ```
  hostname# inet bonding delete 1
  ```

- При описании в документе необязательные параметры или ключевые слова заключены в квадратные скобки «[]». Например:

  ```
  firewall <тип> add name @<имя> <состав> [exclude <исключения>]
  ```

  При вводе в командный интерпретатор необязательные параметры или ключевые слова вводятся без квадратных скобок. Например:

  ```
  hostname# firewall interface-object add name @intgroup interface eth0 interface eth1
  ```

- Если при вводе команды можно указать один из нескольких параметров, при описании в документе допустимые варианты заключены в фигурные скобки «{}» и разделены вертикальной чертой «|». Например:

  ```
  inet ntp mode {on | off}
  ```

  Если при вводе команды можно указать один из нескольких параметров, то при вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок. Например:

  ```
  hostname# inet ntp mode off
  ```

Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ViPNet Coordinator VA помимо данного документа, и описаны основные сведения, которые содержит каждый из этих документов.

Таблица 3. Связанные документы

Документ и его назначение	Содержание
«ViPNet Coordinator VA. Настройка с помощью командного	Основные сведения по работе с командным интерпретатором Локальное и удаленное подключение к ViPNet Coordinator VA Настройка подключения к сети (настройка сетевых интерфейсов

Документ и его назначение	Содержание
интерпретатора». В документе описаны основные сценарии настройки ViPNet Coordinator VA с помощью командного интерпретатора, а также работа с журналами ViPNet Coordinator VA.	Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов, использование динамических интерфейсов) Настройка подключения ViPNet Coordinator VA к внешней сети через межсетевой экран Настройка VPN-функций (настройка виртуальных IP-адресов, настройка параметров туннелируемых узлов) Настройка туннелирования на канальном уровне (L2OverIP) Настройка сетевых фильтров Настройка групп объектов Настройка трансляции IP-адресов Тонкая настройка межсетевого экрана (антиспуфинг, дополнительные параметры межсетевого экрана) Настройка обработки прикладных протоколов Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, DHCP-relay, прокси-сервер) Настройка статической и динамической маршрутизации Настройка функции MultiWAN Настройка параметров безопасности Настройка системных параметров (параметры даты и времени, файла подкачки, резервное копирование и восстановление настроек) Настройка транспортного модуля MFTP Обновление ПО ViPNet Coordinator VA, в том числе на кластере горячего резервирования Настройка протоколирования событий и просмотр журналов (системный журнал, журнал IP-пакетов, журнал конвертов MFTP) Мониторинг ViPNet Coordinator VA (с помощью ViPNet StateWatcher, по протоколу SNMP) Список значений по умолчанию (сетевые фильтры, пользовательские группы протоколов) Список событий в журнале регистрации IP-пакетов и системном журнале Список демонов ПО ViPNet Coordinator VA Список MIME-типов, поддерживаемых при фильтрации содержимого трафика прокси-сервера
«ViPNet Coordinator VA. Настройка с помощью веб-интерфейса». В документе описана настройка ViPNet Coordinator VA с помощью	Подключение к веб-интерфейсу ViPNet Coordinator VA Настройка даты и времени Настройка подключения к сети (настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов, использование динамических интерфейсов

Документ и его назначение	Содержание
веб-интерфейса. Документ предназначен для администраторов и пользователей, которые планируют работать с ViPNet Coordinator VA, используя веб-интерфейс.	Настройка параметров VPN Работа со списком защищенных узлов, связанных с ViPNet Coordinator VA Настройка туннелирования на канальном уровне (L2OverIP) Настройка сетевых фильтров Настройка групп объектов Настройка трансляции IP-адресов Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, DHCP-relay, прокси-сервер) Настройка статической и динамической маршрутизации Настройка функции MultiWAN Мониторинг состояния ViPNet Coordinator VA, мониторинг по протоколу SNMP Просмотр журналов (системный журнал, журнал IP-пакетов, журнал конвертов MFTP) Список значений по умолчанию (сетевые фильтры, пользовательские группы протоколов) Список событий в журнале регистрации IP-пакетов и системном журнале Список демонов ПО ViPNet Coordinator VA Список MIME-типов, поддерживаемых при фильтрации содержимого трафика прокси-сервера
«ViPNet Coordinator VA. Справочное руководство по командному интерпретатору и конфигурационным файлам».	Описание команд ViPNet Coordinator VA Описание конфигурационных файлов управляющего демона и системы защиты от сбоев
«ViPNet Coordinator VA. Лицензионные соглашения на компоненты сторонних производителей»	Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet Coordinator HW и VA

Комплект поставки

В комплект поставки ViPNet Coordinator VA входят следующие компоненты:

- Файл с образом виртуальной машины:
  - `va_vipnet_base_x86_64_4.x.x-xxxx_vhd.tar.gz` (для развертывания в среде Microsoft Hyper-V);
  - `va_vipnet_base_x86_64_4.x.x-xxxx.raw.tar.gz` или `va_vipnet_base_x86_64_4.x.x-xxxx.qcow2.tar.gz` (для развертывания в среде KVM);
  - `va_vipnet_base_x86_64_4.x.x-xxxx.ova` (для развертывания в остальных средах виртуализации).
- Файл обновления в формате LZH, необходимый для обновления ПО ViPNet Coordinator VA с более ранней версии на текущую.
- Документация в формате PDF:
  - «ViPNet Coordinator VA. Подготовка к работе».
  - «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора».
  - «ViPNet Coordinator VA. Настройка с помощью веб-интерфейса».
  - «ViPNet Coordinator VA. Справочное руководство по командному интерпретатору и конфигурационным файлам».
  - «ViPNet Coordinator VA. Лицензионные соглашения на компоненты сторонних производителей».
  - «ViPNet Coordinator VA. История версий»

Что нового в версии 4.3.3

- **Разделение продукта на аппаратных исполнениях (HW) и на виртуальном исполнении (VA)**

  Начиная с версии 4.3.3, исполнение для виртуальных платформ получило имя ViPNet Coordinator VA и поставляется отдельно со своим комплектом документации. ViPNet Coordinator HW поставляется только в исполнениях на аппаратных платформах.

- **Добавлена поддержка Kernel-based Virtual Machine (KVM)**

  Теперь вы можете разворачивать ViPNet Coordinator VA на платформах виртуализации KVM. Подробнее о поддерживаемых гипервизорах см. Требования к виртуальной среде (на стр. 33).

- **Изменение в лицензировании**

  В новой версии изменилась система лицензирования, поэтому после обновления ПО потребуется назначить координатору новую роль в ViPNet ЦУС. Ранее для ViPNet Coordinator VA использовалась одна роль HW/VA, теперь в зависимости от исполнения роль может быть: VA100, VA500, VA1000, VA2000.

  При использовании кластера дополнительно потребуется назначить одну из ролей кластера: Failover100, Failover500, Failover1000 или Failover2000.

  Подробнее об особенностях каждого исполнения см. Лицензирование и функциональные ограничения (на стр. 28).

- **Поддержка современных высокоскоростных сетевых адаптеров**

  Теперь для работы ViPNet Coordinator VA на виртуальной платформе Microsoft Hyper-V не требуется использовать устаревший сетевой адаптер (**Legacy Network Adapter**), который поддерживает скорость до 100 Мбит/с.

  Поэтому при обновлении на новую версию ViPNet Coordinator VA измените тип сетевого адаптера на стандартный (**Network Adapter**). Подробнее об обновлении см. документ «Настройка с помощью командного интерпретатора», глава «Обновление программного обеспечения».

- **Экспорт журнала регистрации IP-пакетов по сети в формате CEF**

  Для интеграции ViPNet Coordinator VA в корпоративные информационные системы добавлена возможность экспорта журнала регистрации IP-пакетов формате CEF на удаленный сервер. Подробнее об экспорте журнала см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора», раздел «Экспорт журнала регистрации IP-пакетов по сети в формате CEF».

- **Новый дизайн веб-интерфейса**

  Выполнен переход на новый дизайн веб-интерфейса ViPNet Coordinator VA, в котором оптимизированы расположение элементов управления и навигация по ним. Поэтому работать с ViPNet Coordinator VA теперь удобнее.

- **Возможность увеличить размер дисков**

Теперь в настройках виртуальной платформы вы можете увеличить размер дисков для ViPNet Coordinator VA.

- **Запрет назначения разным сетевым интерфейсам IP-адресов из одного широковещательного диапазона**

  В новой версии добавлена проверка, запрещающая назначение разным сетевым интерфейсам IP-адресов, относящихся к одному широковещательному диапазону (broadcast).

- **Перенаправление запросов на основной DNS-сервер, когда DNS-серверы пересылки недоступны**

  Теперь в командном интерпретаторе и в веб-интерфейсе можно включить перенаправление запросов на основной DNS-сервер, если недоступны DNS-серверы пересылки.

- **Добавление DNS-серверов пересылки для определенных доменных зон без перенаправления на корневой DNS-сервер**

  Ранее при недоступности DNS-сервера пересылки, заданного для определенной доменной зоны, запросы перенаправлялись на корневой DNS-сервер. Теперь можно отключить перенаправление запросов на корневой сервер, когда это не требуется. Отключение возможно в командном интерпретаторе и веб-интерфейсе.

- **Поддержка Internet Explorer 11 для работы с веб-интерфейсом ViPNet Coordinator VA**

- **Дополнительный комплект документации на английском языке**

  Документация переведена и поддерживается на английском и русском языках.

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.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

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.

  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.

1

Общая информация

Назначение ViPNet Coordinator VA

ViPNet Coordinator VA представляет собой виртуализированное программное обеспечение, распространяемое в исполнениях VA100, VA500, VA1000 и VA2000, которые предназначены для развертывания на платформе виртуализации. Поддерживаемые платформы виртуализации перечислены в разделе Требования к виртуальной среде (на стр. 33).

Каждое исполнение ViPNet Coordinator VA представляет собой интегрированное решение на базе программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС GNU/Linux, а также роли, назначаемой сетевому узлу в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 83) и накладывающей определенные лицензионные ограничения.

ViPNet Coordinator VA выступает в роли VPN-сервера и предназначен для использования в IP-сетях, защита которых организуется с применением комплекса программных продуктов ViPNet. Описание всех основных функций ViPNet Coordinator VA приведено в разделе Функции координатора в защищенной сети (на стр. 17).

Защищенная сеть ViPNet

ViPNet Coordinator VA предназначен для использования в защищенной сети ViPNet, построенной на основе комплекса продуктов ViPNet.

Сеть ViPNet представляет собой виртуальную защищенную сеть (см. глоссарий, стр. 83), которая может быть развернута поверх локальных или глобальных сетей любой структуры. В отличие от многих популярных VPN-решений, технология ViPNet обеспечивает защищенное взаимодействие между сетевыми узлами по схеме «клиент-клиент».

Защита информации в сети ViPNet осуществляется с помощью специального программного обеспечения, которое выполняет две основные функции:

- Фильтрация всего IP-трафика сетевых узлов. Фильтрация трафика осуществляется в соответствии с заданными на узле правилами.
- Шифрование соединений между узлами сети ViPNet (см. глоссарий, стр. 87). Для шифрования трафика используются симметричные ключи, которые создаются и распределяются централизованно.

Для управления защищенной сетью ViPNet предназначено программное обеспечение ViPNet Administrator (см. глоссарий, стр. 83). С помощью ViPNet Administrator создаются сетевые узлы ViPNet и связи между ними, настраиваются параметры отдельных узлов, создаются дистрибутивы ключей (см. глоссарий, стр. 84) для каждого узла, выполняется централизованное обновление справочников, ключей (см. глоссарий, стр. 87) и программного обеспечения на узлах.

Сетевые узлы ViPNet делятся на два типа:

- Клиент (ViPNet-клиент) (см. глоссарий, стр. 84) — рабочее место пользователя сети ViPNet.
- Координатор (ViPNet-координатор) (см. глоссарий, стр. 85) — сервер сети ViPNet. Сетевой узел ViPNet Coordinator VA является координатором.

Также сеть ViPNet может включать открытые узлы (компьютеры без программного обеспечения ViPNet), соединения которых через Интернет или другие публичные сети защищаются ViPNet-координаторами с помощью туннелирования на сетевом уровне (см. глоссарий, стр. 88).

Функции координатора в защищенной сети

В защищенной сети ViPNet координатор выступает в роли VPN-сервера. Функции координатора определяются структурой и задачами корпоративной сети и могут быть следующими:

- Сервер IP-адресов (на стр. 17). Обеспечивает взаимодействие защищенных узлов ViPNet (см. глоссарий, стр. 84). Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.
- Маршрутизатор VPN-пакетов (на стр. 19). Обеспечивает маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы.
- Сервер соединений (на стр. 19). Обеспечивает соединение клиентов и координаторов друг с другом кратчайшим путем.
- VPN-шлюз (на стр. 20). Позволяет организовать защищенные соединения между узлами локальных сетей (на которых не установлено ПО ViPNet) и между сегментами сетей с помощью защищенных каналов (туннелей).
- Транспортный сервер (на стр. 22). Обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из программы ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 83), а также обмен прикладными транспортными конвертами (см. глоссарий, стр. 88) между узлами.
- Защищенный Интернет-шлюз (на стр. 23). Обеспечивает раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации.

Сервер IP-адресов

При подключении любого клиента с программой ViPNet Client (см. глоссарий, стр. 84) к сети или изменении его параметров подключения эти параметры сообщаются координатору, который играет роль сервера IP-адресов для данного клиента. В свою очередь, сервер IP-адресов отправляет на клиент информацию о параметрах подключения и о состоянии всех узлов, с которыми у данного клиента имеется связь.

Таким образом, роль сервера IP-адресов заключается:

- в сборе сведений о сетевых узлах;
- в информировании о параметрах доступа и состоянии тех узлов сети, с которыми у данного клиента имеется связь.

Рисунок 1. Сервер IP-адресов в сети ViPNet

Чтобы подтвердить свое присутствие в сети, клиент периодически (по умолчанию — каждые 5 минут) отправляет на сервер сообщение о своей активности. Если такое сообщение не поступило, координатор переводит клиент в статус «Недоступен».

Аналогичным образом происходит обмен информацией о параметрах доступа между координаторами. Периодически (по умолчанию — каждые 15 минут) координатор отсылает на другие связанные с ним координаторы подтверждение о своей активности. Кроме того, координаторы обеспечивают рассылку информации об узлах, для которых они выполняют функцию сервера IP-адресов.

Сервер IP-адресов работает по следующей логике:

- При появлении новой информации о своем клиенте (то есть о клиенте, который использует данный координатор в качестве сервера IP-адресов) координатор рассылает ее на другие свои клиенты и связанные координаторы.
- При появлении новой информации о клиентах других координаторов рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора.
- При отсутствии информации от своего клиента по истечении периода опроса координатор считает этот клиент недоступным и рассылает информацию об этом.
- В случае взаимодействия координатора с другой сетью ViPNet на шлюзовой координатор (см. глоссарий, стр. 88) другой сети высылается информация о состоянии всех узлов своей сети, связанных с узлами другой сети ViPNet. При получении такой информации из другой сети ViPNet координатор рассылает эту информации на все координаторы своей сети, а также на свои клиенты, связанные с узлами другой сети.

По умолчанию для клиента роль сервера IP-адресов выполняет его транспортный сервер (координатор, на котором клиент зарегистрирован в программе ViPNet Центр управления сетью). В отличие от транспортного сервера, сервер IP-адресов можно сменить, выбрав любой другой координатор, с которым у данного клиента есть связь.

Маршрутизатор VPN-пакетов

Координатор выполняет маршрутизацию транзитного защищенного трафика, передаваемого на другие защищенные сетевые узлы. Маршрутизация осуществляется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями ViPNet.

Рисунок 2. Функция маршрутизации защищенного трафика в сети ViPNet

Маршрутизация защищенного трафика осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется трансляция сетевых адресов (NAT) (см. глоссарий, стр. 88). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора. Трансляция адресов для защищенного трафика выполняется автоматически в соответствии с параметрами, которые не могут быть изменены.

Если на границе сети ViPNet установлено стороннее устройство, выполняющее фильтрацию и трансляцию трафика, то в этом случае координатор может выступать в роли сервера соединений. С помощью сервера соединений клиенты устанавливают соединения друг с другом в том случае, если напрямую установить соединения они не могут. Для каждого клиента может быть назначен свой сервер соединений. По умолчанию сервер соединений для клиента служит также сервером IP-адресов (см. Сервер IP-адресов на стр. 17).

Сервер соединений

Координатор может выступать в качестве сервера соединений (см. глоссарий, стр. 87) и устанавливать соединения между клиентами и координаторами по кратчайшему пути, если они находятся в разных подсетях и не могут соединиться друг с другом напрямую. Для каждого клиента может быть назначен свой сервер соединений. По умолчанию сервер соединений для клиента служит также сервером IP-адресов. Для координаторов также при необходимости может быть выбран сервер соединений.

Рисунок 3. Организация соединений между сетевыми узлами ViPNet

На сервере соединений можно настроить TCP-туннель, который будет соединять клиентов из внешних сетей с другими узлами ViPNet в том случае, если интернет-провайдер блокирует протокол UDP.

Рисунок 4. Функция TCP-туннеля

Таким образом, когда удаленный клиент не может получить доступ к сети ViPNet по протоколу UDP, он автоматически устанавливает связь через TCP-туннель своего сервера соединений. На сервере полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.

VPN-шлюз

Координаторы в роли VPN-шлюзов защищают соединения между узлами локальных сетей, которые обмениваются информацией через публичные сети. Защита реализуется с помощью технологии туннелирования (см. Туннелирование на стр. 88), в основе которой лежит инкапсуляция и шифрование проходящего через координаторы трафика. При этом координатор может выполнять туннелирование как на сетевом уровне (уровень 3 модели OSI), так и на канальном уровне (уровень 2 модели OSI).

Туннелирование трафика на сетевом уровне позволяет организовать защищенное соединение между открытым узлом и защищенным узлом ViPNet или между двумя открытыми узлами, которые туннелируются разными координаторами. В результате это позволяет включить открытые узлы в

защищенную сеть ViPNet без установки на них программного обеспечения ViPNet. Туннелирование трафика на сетевом уровне выполняется следующим образом:

- На координатор поступают открытые IP-пакеты от туннелируемых узлов, которые обрабатываются сетевыми фильтрами.
- Обработанные IP-пакеты на координаторе зашифровываются и упаковываются в новые IP-пакеты, после чего передаются на защищенные узлы назначения либо на другой координатор.
- Если на координатор поступают зашифрованные IP-пакеты, предназначенные для туннелируемых узлов, из них извлекаются исходные IP-пакеты, расшифровываются, обрабатываются сетевыми фильтрами и передаются на узлы назначения в открытом виде.

Рисунок 5. Защита соединения на сетевом уровне модели OSI

Чтобы координатор мог осуществлять туннелирование на сетевом уровне, администратор сети ViPNet в программе ViPNet Центр управления сетью (ЦУС) задает максимальное разрешенное число одновременных туннелируемых соединений на данном координаторе. Также в ЦУСе либо на самом координаторе задаются IP-адреса туннелируемых устройств.

Туннелирование на канальном уровне (или технология L2OverIP (см. глоссарий, стр. 82)) позволяет организовать защищенное соединение между узлами удаленных друг от друга сегментов сети, обеспечивая прямую связь между ними по протоколу Ethernet. С помощью этой технологии можно связывать различные сегменты в единую сеть вне зависимости от того, какие сетевые протоколы будут использоваться в этой сети (IP, IPX, MPLS, IEEE 802.2 и другие). При использовании протокола IP связанные через L2OverIP сегменты образуют единое адресное пространство в пределах одной IP-подсети.

Технология L2OverIP работает следующим образом:

- Координаторы, установленные на границе разных сегментов сети, перехватывают Ethernet-кадры, передаваемые между сегментами.
- Перехваченные Ethernet-кадры на координаторах упаковываются в IP-пакеты специального формата и передаются по защищенному каналу.
- Из полученных IP-пакетов на координаторах извлекаются исходные кадры и передаются узлам сегмента назначения.

Рисунок 6. Защита соединения на канальном уровне модели OSI

Для туннелирования требуется выполнить ряд специальных настроек на координаторах, установленных на границе удаленных сегментов сети.

Транспортный сервер

В программе ViPNet Центр управления сетью каждый создаваемый клиент регистрируется на координаторе. Этот координатор является для клиента транспортным сервером. Пользователь сетевого узла не может изменить заданный транспортный сервер на какой-либо другой.

Роль транспортного сервера в сети ViPNet состоит в доставке на сетевые узлы ViPNet управляющих сообщений, обновлений справочников и ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами (см. глоссарий, стр. 88) между узлами.

Маршрутизация прикладных и управляющих конвертов осуществляется с помощью транспортного модуля ViPNet MFTP, работающего на прикладном уровне. Транспортный модуль на координаторе принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения.

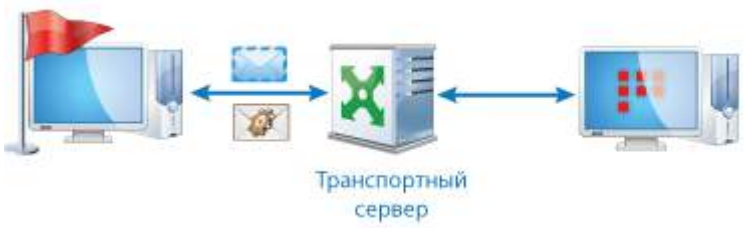

Рисунок 7. Роль транспортного сервера в сети ViPNet

При поступлении прикладного или управляющего конверта транспортный сервер в соответствии с маршрутными таблицами определяет дальнейший путь передачи этого конверта. Если конверт многоадресный, он дробится сервером на соответствующие части. Получив конверт, транспортный сервер выполняет одно из действий, в зависимости от заданных параметров:

- Устанавливает соединение с сетевым узлом (по умолчанию такая логика действует при отправке конверта на другой транспортный сервер).

- Ожидает, когда соединение установит получатель конверта (по умолчанию эта логика действует при наличии конвертов для клиентов).

Кроме того, можно задать период опроса других узлов независимо от наличия для них конвертов. При разрывах соединений передача информации всегда продолжается с точки разрыва, что особенно важно на коммутируемых каналах.

Защищенный Интернет-шлюз

Технология «Открытый Интернет» позволяет разделить доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet. Таким образом обеспечивается доступ в Интернет с максимальным уровнем безопасности, возможным без физического отключения компьютера от корпоративной сети.

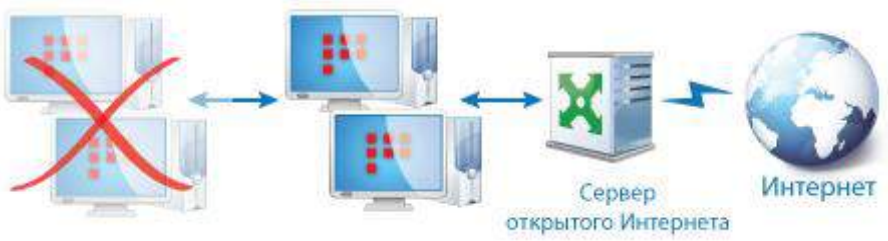

Рисунок 8. Роль сервера открытого Интернета в сети ViPNet

Клиенты, имеющие связь с сервером открытого Интернета, могут работать только в одном из двух режимов:

- Работа в Интернете, при этом ресурсы корпоративной защищенной сети недоступны, хотя компьютер не отключен от сети физически.
- Работа в локальной сети, при этом доступ в Интернет полностью заблокирован, но без физического отключения от внешней сети.

Такое разделение на два непересекающихся режима исключает любые атаки в реальном времени на компьютеры корпоративной сети через компьютеры, имеющие доступ к Интернету.

Чтобы использовать на координаторе технологию «Открытый Интернет», в программе ViPNet Центр управления сетью для этого координатора следует включить функцию сервера открытого Интернета. Подробнее см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора».

Функции межсетевого экрана ViPNet Coordinator VA

Координатор выполняет фильтрацию IP-пакетов на каждом сетевом интерфейсе по адресам, протоколам и портам в соответствии с настроенными сетевыми фильтрами. С помощью сетевых фильтров можно не только заблокировать нежелательные соединения, но и разрешить соединения с открытыми узлами, не входящими в сеть ViPNet.

Помимо настраиваемых фильтров имеется система защиты от одной из распространенных сетевых атак — спуфинга.

Рисунок 9. Роль межсетевого экрана в сети ViPNet

Координатор также может осуществлять трансляцию сетевых адресов (NAT) для проходящего через него открытого трафика (см. глоссарий, стр. 88).

Примечание. Трансляция сетевых адресов для защищенного трафика осуществляется автоматически (см. Маршрутизатор VPN-пакетов на стр. 19).

Функция NAT для открытого трафика позволяет задать правила трансляции сетевых адресов для решения двух основных задач:

- Для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов. Таким образом, NAT позволяет компьютерам с локальными IP-адресами получать доступ к Интернету от имени публичного IP-адреса координатора.

  Для решения этой задачи используется трансляция адреса источника.

- Для организации доступа к локальным ресурсам из внешней сети. В результате применения технологии NAT узлы локальной сети, имеющие частные IP-адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

  Для решения этой задачи используется трансляция адреса назначения.

Подробнее об использовании NAT для открытого трафика см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора» и «ViPNet Coordinator VA. Настройка с помощью веб-интерфейса».

Также межсетевой экран ViPNet Coordinator VA обладает следующими возможностями:

- Обработка протоколов прикладного уровня: FTP, DNS, H.323, SCCP, SIP.
- Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q).
- Объединение нескольких физических сетевых интерфейсов в один логический — агрегированный интерфейс — для увеличения пропускной способности, повышения надежности, резервирования каналов связи.
- Приоритизация обработки IP-трафика в соответствии с протоколом DiffServ (см. Обработка сетевого трафика в соответствии с его приоритетом на стр. 26).
- Функции DHCP-, DNS- и NTP-сервера.
- Реализация функций прокси-сервера с возможностью фильтрации HTTP-трафика по его содержимому и антивирусной проверки.
- Функции маршрутизатора IP-пакетов с возможностью настройки статической и динамической маршрутизации.
- Функции кластера горячего резервирования.
- Совместимость с программным обеспечением для управления и мониторинга: ViPNet Administrator, ViPNet Policy Manager, ViPNet StateWatcher.

Обработка сетевого трафика в соответствии с его приоритетом

В ViPNet Coordinator VA реализована поддержка протокола классификации сетевого трафика DiffServ (см. глоссарий, стр. 81). Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена DSCP-метка, задающая приоритет обработки пакета.

Когда на ViPNet Coordinator VA поступают IP-пакеты с DSCP-метками, по значению метки определяется принадлежность каждого IP-пакета к одному из 8 классов приоритета. IP-пакеты, принадлежащие к классу с более высоким приоритетом, всегда обрабатываются раньше пакетов, принадлежащих к менее приоритетным классам.

При этом, при зашифровании и расшифровании (инкапсуляциии и декапсуляции) IP-пакета DSCP-метка перемещается соответственно из закрытой в открытую или из открытой в закрытую часть IP-пакета. Поэтому в случае, когда на ViPNet Coordinator VA приходит открытый IP-пакет с DSCP-меткой, ViPNet Coordinator VA его шифрует и отправляет далее получателю, по пути следования IP-пакета его DSCP-метка может быть снята или изменена и останется такой после расшифрования.

ViPNet Coordinator VA поддерживает следующие политики обработки трафика с учетом приоритета в соответствии с RFC 2474 и RFC 2475:

- Assured Forwarding — гарантированная переадресация.
- Class Selector — политика, обеспечивающая обратную совместимость с полем IP Precedence.
- Default PHB (Best Effort) — негарантированная доставка.

ViPNet Coordinator VA гарантирует обработку трафика в соответствии с его приоритетом в том случае, если на сетевом оборудовании (например, коммутаторе), подключенном к ViPNet Coordinator VA, поддерживается эта функция, а также включено управление потоком передачи данных (Ethernet Flow Control).

Примечание. Если количество поступающего трафика более чем на 20% превышает пропускную способность ViPNet Coordinator VA, обработка трафика с заданным приоритетом не гарантируется.

Система защиты от сбоев и кластер горячего резервирования

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNet Coordinator VA и создания отказоустойчивого решения на базе узлов ViPNet Coordinator VA. Данная система может работать в одиночном режиме или в режиме кластера горячего резервирования.

По умолчанию в ViPNet Coordinator VA система защиты от сбоев работает в одиночном режиме и выполняет следующие функции:

- контроль собственной работоспособности;
- контроль работоспособности демонов и драйверов ViPNet Coordinator VA, ведение статистики использования системных ресурсов;
- контроль сбоев при обработке IP-пакетов драйвером ViPNet.

Кластер горячего резервирования состоит из двух взаимосвязанных ViPNet Coordinator VA, которые являются его узлами:

- активный узел — выполняет фильтрацию трафика;
- пассивный узел — находится в режиме ожидания.

В режиме кластера горячего резервирования система защиты от сбоев также осуществляет контроль работоспособности ViPNet Coordinator VA, а при сбоях переключает пассивный узел кластера в активный режим.

2

Лицензирование и функциональные ограничения

Лицензирование ViPNet Coordinator VA

Распределение лицензии для ViPNet Coordinator VA и кластера выполняется в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 83). Для каждого исполнения ViPNet Coordinator VA администратор ЦУС назначает одну из ролей: VA100, VA500, VA1000 или VA2000. При использовании кластера горячего резервирования администратор дополнительно назначает роль кластера: Failover100, Failover500, Failover1000, Failover2000. Затем администратор ЦУС отправляет лицензию на узел в составе обновлений справочников и ключей или передает в файле первичного развертывания DST.

Соответствие исполнения назначенной роли проверяется при установке на ViPNet Coordinator VA справочников и ключей.

Роль накладывает ограничения на количество потоков ядра для шифрования трафика и определят роль на использование кластера горячего резервирования. В таблице приведены роли и их параметры для различных исполнений ViPNet Coordinator VA.

Таблица 4. Лицензионные параметры ролей ViPNet Coordinator VA

Название роли	Роль для использования в кластере	Максимальное количество потоков ядра для шифрования трафика	Максимальное число соединений МСЭ
VA100	Failover100	2	150 000
VA500	Failover500	2	500 000
VA1000	Failover1000	4	1 000 000
VA2000	Failover2000	7	3 000 000

Максимальное количество сетевых интерфейсов

На ViPNet Coordinator VA можно одновременно использовать не более 128 сетевых интерфейсов.

Типы сетевых интерфейсов:

- eth — количество, не превышающее в сумме с другими интерфейсами 128 (не зависит от числа физических разъемов компьютера, на котором развернут ViPNet Coordinator VA);
- loopback-интерфейс (localhost) — 1;
- vlan и alias (интерфейс, который создается при добавлении дополнительного адреса для интерфейса eth) — количество, не превышающее в сумме с другими интерфейсами 128.

Количество связей ViPNet Coordinator VA с ViPNet-узлами

В таблице ниже указано максимальное количество сетевых узлов, с которыми ViPNet Coordinator VA может быть связан, в зависимости от назначенной роли.

Превышение указанного количества связей может привести к снижению производительности ViPNet Coordinator VA.

Таблица 5. Ограничения на количество связей и клиентов ViPNet Coordinator VA

Роль	Максимальное число клиентов	Максимальное количество связей с ViPNet-узлами	Максимальное количество связей с туннелирующими координаторами	Максимальное количество заданных диапазонов туннелируемых узлов
VA100	100	100	50	1000
VA500	500	500	250	1000
VA1000	1000	1000	500	1000
VA2000	2000	2000	1000	1000

3

Подготовка к работе

Развертывание виртуального образа ViPNet Coordinator VA

Требования к виртуальной среде

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

- VMware vSphere 6.5, 6.7;
- VMware Workstation 12.x, 14.x, 15.x;
- Oracle VM VirtualBox 6.x;
- Oracle VM Server 3.4;

> **Примечание.** Для Oracle VM Server не поддерживается перезапуск ViPNet Coordinator VA с помощью кнопки **Restart** и остановка — **Suspend**.
>
> Для перезапуска виртуальной машины воспользуйтесь кнопками **Stop** и **Start**, либо перезагрузите ViPNet Coordinator через командный интерпретатор или веб-интерфейс.

- Microsoft Hyper-V Server 2019;
- среды на базе Linux с поддержкой KVM, Qemu-KVM и Libvirt.

Работа на других платформах виртуализации не гарантируется.

> **Внимание!** Сетевому узлу, на который устанавливается ПО ViPNet Coordinator VA, в программе ViPNet Центр управления сетью (далее — ЦУС) должна быть назначена роль «VA».

Конфигурации виртуальных машин в зависимости от исполнения ViPNet Coordinator VA представлены в таблице.

Таблица 6. Параметры виртуальных машин для работы ViPNet Coordinator VA

Исполнение	Количество потоков процессора	Оперативная память (Гб)
ViPNet Coordinator VA100	2	2
ViPNet Coordinator VA500	2	2
ViPNet Coordinator VA1000	4	4
ViPNet Coordinator VA2000	8	8

Общие требования для всех исполнений ViPNet Coordinator VA:

- Накопители — 2 диска: HDD не менее 4 Гбайт, HDD не менее 80 Гбайт.
- Сетевые интерфейсы — не менее 4.

Примечание. В связи с особенностями виртуализации сетевых интерфейсов, при увеличении числа потоков одновременной обработки данных может снижаться пропускная способность координатора. В таком случае сопоставьте виртуальному сетевому интерфейсу физический сетевой адаптер средствами выбранной платформы виртуализации.

Если на координаторе будет зарегистрировано более 1000 клиентов, то для виртуального диска укажите тип **Thick Provision** или **Фиксированный жесткий диск**.

Установка ViPNet Coordinator VA на платформу виртуализации

Для установки ViPNet Coordinator VA на платформу виртуализации вам потребуется файл с образом виртуальной машины (`*.ova`, `*.raw.tar.gz`, `*.vhd.tar.gz` или `*.qcow2.tar.gz`), который входит в комплект поставки.

В следующих разделах приведены примеры установки ViPNet Coordinator VA на платформы виртуализации: VMware vSphere ESXi (на стр. 34), Oracle VM VirtualBox (на стр. 38), Oracle VM Server (на стр. 42), Microsoft Hyper-V (на стр. 45) и KVM (на стр. 47).

VMware vSphere ESXi

Для установки ViPNet Coordinator VA на платформу виртуализации VMware vSphere ESXi:

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, добавляющее поддержку образов формата OVF.

---

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

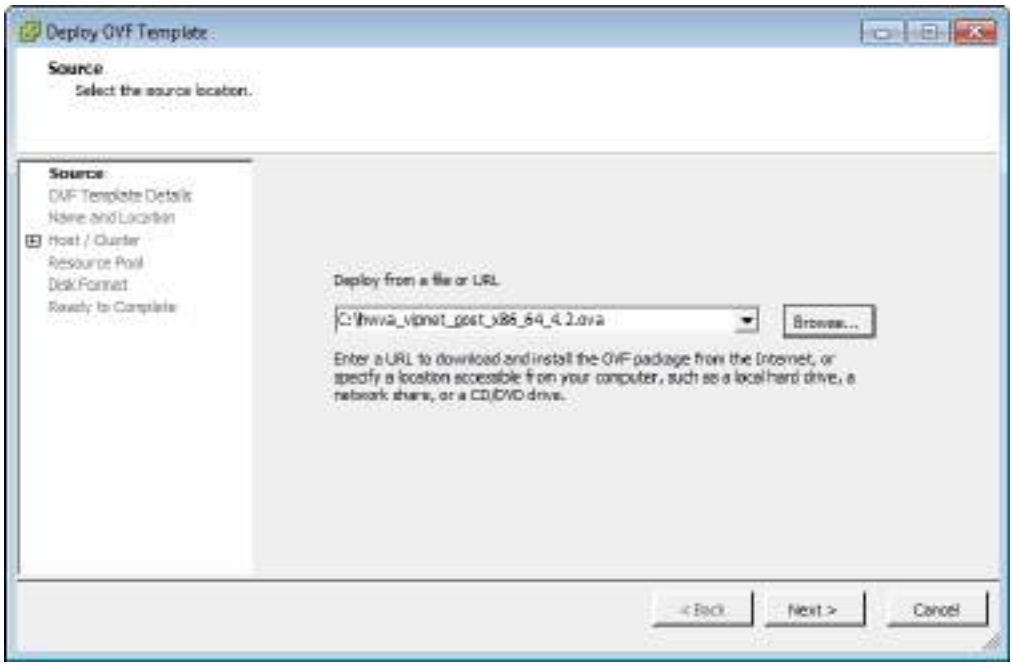

Рисунок 10. Задание файла с образом виртуальной машины

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.

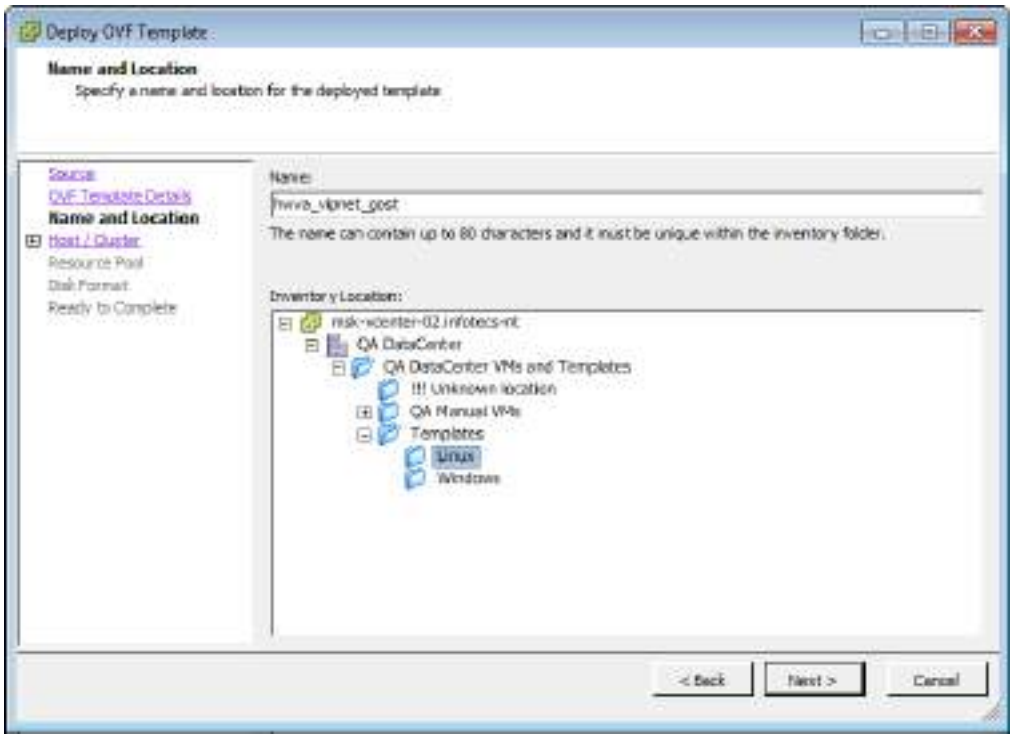

Рисунок 11. Задание имени и расположения виртуальной машины

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.

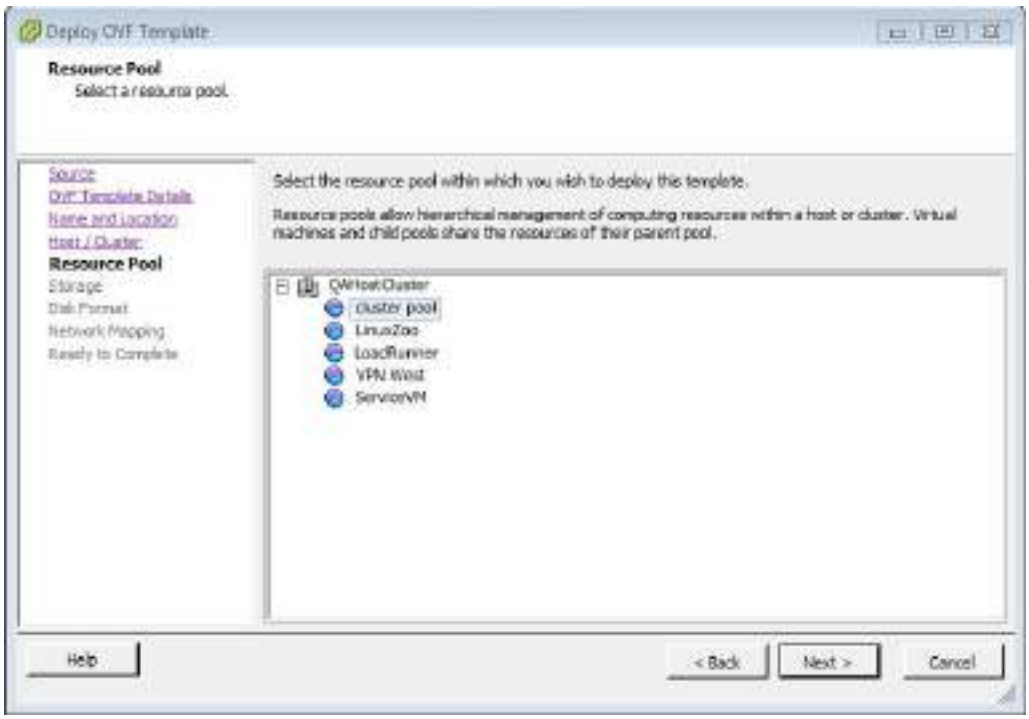

Рисунок 12. Выбор пула ресурсов

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 формат виртуального диска.

Формат **Thin Provision** подходит для небольших по объему дисков или для небольших сетей ViPNet. Поскольку файл с виртуальным диском имеет переменный размер — файл увеличивается или уменьшается в зависимости от размера содержимого виртуального диска.

Если на координаторе будет зарегистрировано более 1000 клиентов, то для виртуального диска укажите тип **Thick Provision**, иначе работа в сети ViPNet будет существенно замедлена.

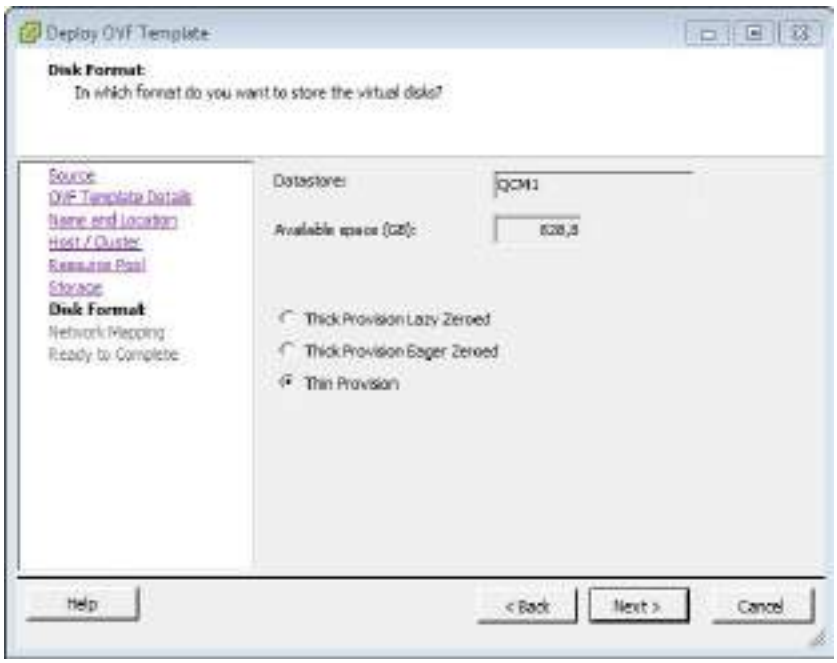

Рисунок 13. Выбор формата виртуального диска

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 Coordinator VA (см. шаг 10).

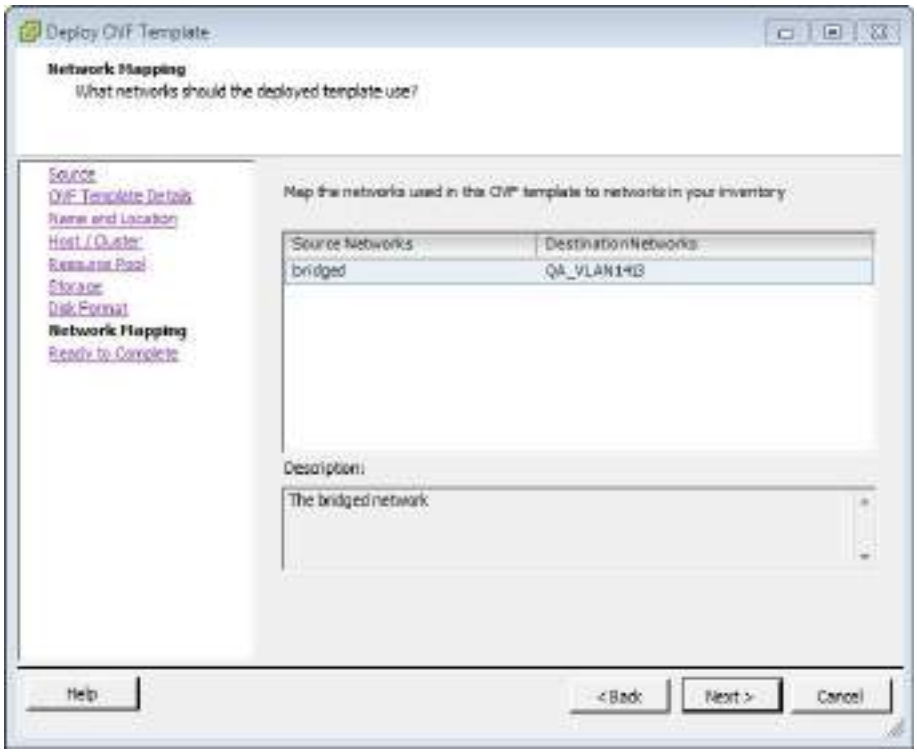

Рисунок 14. Настройка сетевых интерфейсов

8 На странице **Ready to Complete** проверьте настройки виртуальной машины и нажмите кнопку **Finish**.

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

10 Перейдите в настройки виртуальной машины и на вкладке **Hardware** добавьте не менее 4 сетевых интерфейсов.

Если сетевых интерфейсов будет меньше, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники через ноутбук по каналу Ethernet (см. Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP на стр. 50).

11 Обновите уровень совместимости созданной виртуальной машины на **ESXi 6.7 and later (VM version 14)**.

Для этого в свойствах виртуальной машины выберите **Compatibility** > **Upgrade VM Compatibility**.

12 Укажите тип операционной системы **Other 4.x or later Linux (64-bit)**.

13 Запустите виртуальную машину и установите справочники и ключи (см. Способы установки и подготовка к установке справочников и ключей на стр. 50).

Oracle VM VirtualBox

Для установки ViPNet Coordinator VA на платформу виртуализации Oracle VM VirtualBox:

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**.

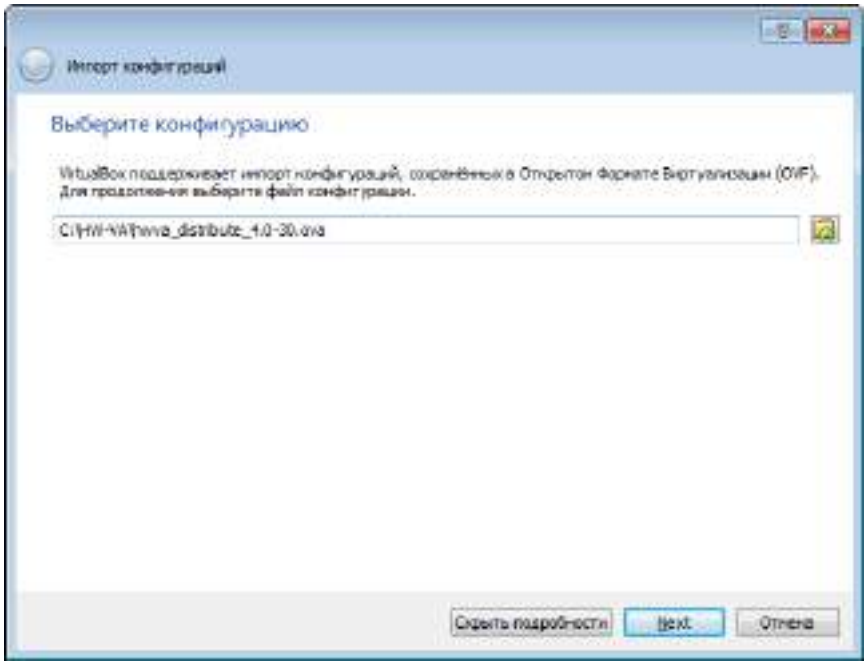

Рисунок 15. Выбор файла с образом виртуальной машины

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

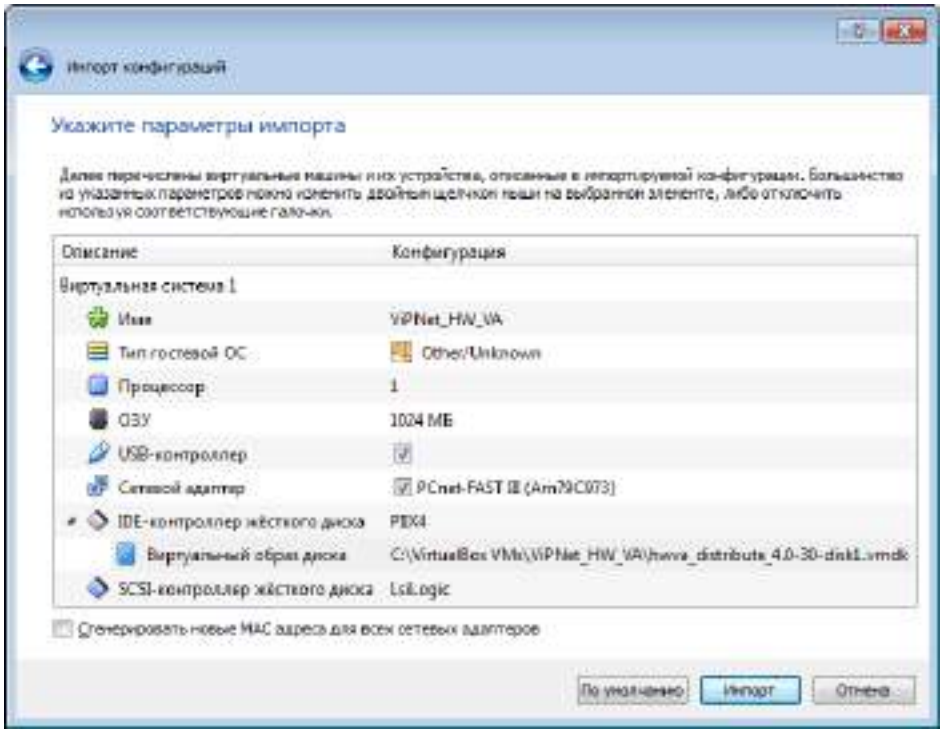

Рисунок 16. Изменение параметров виртуальной машины

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**.

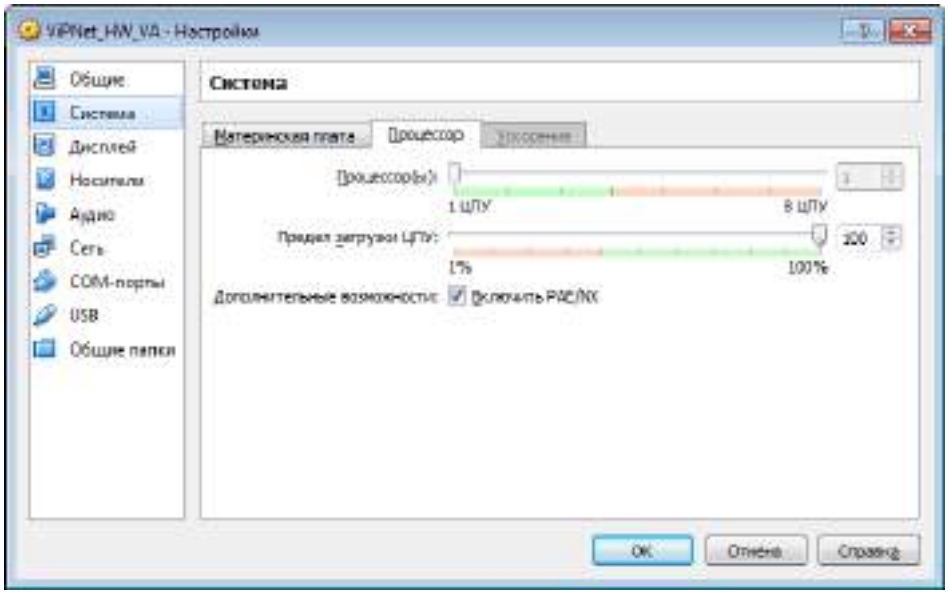

Рисунок 17. Включение поддержки процессором режима PAE

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

5 На вкладке **Материнская плата** установите флажок **Часы в системе UTC**.

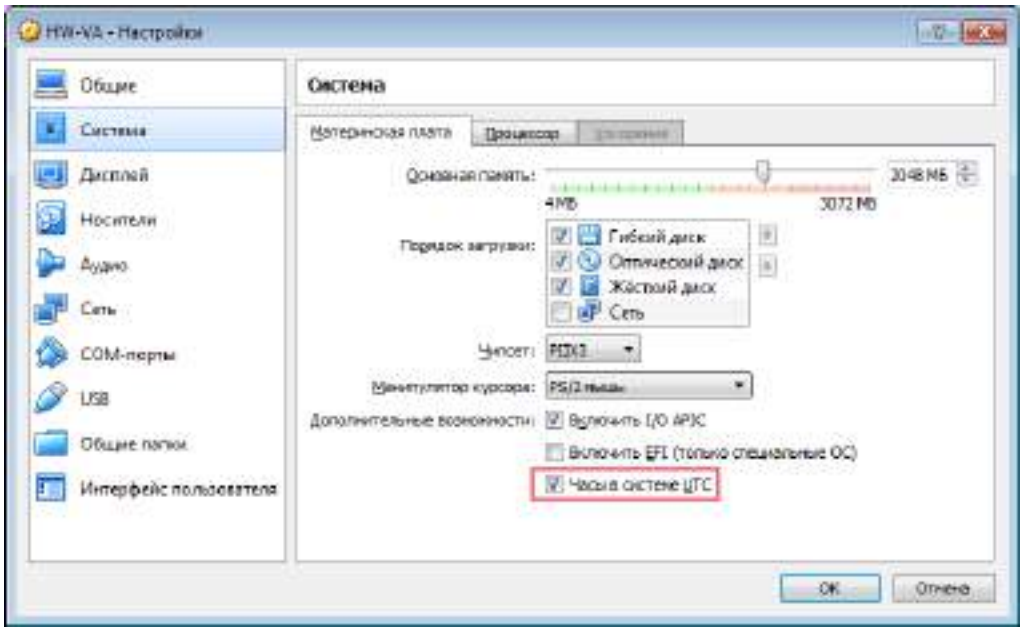

Рисунок 18. Включение режима UTC для аппаратных часов в VirtualBox

---

Примечание. Если в VirtualBox вы ставите на паузу виртуальную машину с ViPNet Coordinator VA, то после возобновления работы часы не будут синхронизированы. Поэтому вместо режима паузы используйте выключение и включение виртуальной машины.

---

6 Если на координаторе будет зарегистрировано более 1000 клиентов, то для виртуального диска укажите формат хранения — **Фиксированный виртуальный жесткий диск**, иначе работа в сети ViPNet будет существенно замедлена.

7 Перейдите в настройки виртуальной машины и на вкладке **Сеть** добавьте не менее 4 сетевых интерфейсов.

Если сетевых интерфейсов будет меньше, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники через ноутбук по каналу Ethernet (см. Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP на стр. 50).

8 Запустите виртуальную машину и установите справочники и ключи (см. Установка справочников и ключей на стр. 52).

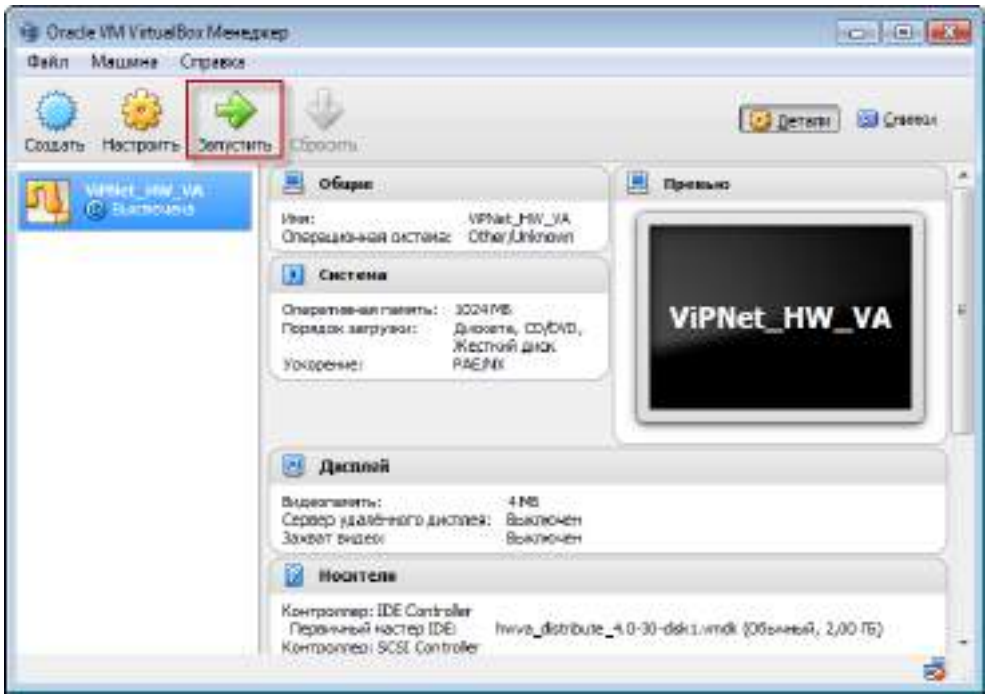

Рисунок 19. Запуск виртуальной машины

Oracle VM Server

Особенности работы на Oracle VM Server

Oracle VM Server не поддерживает подключение USB-устройств к виртуальной машине, поэтому:

- установка дистрибутива ключей возможна только с помощью TFTP (см. Установка дистрибутива ключей на ViPNet Coordinator VA на стр. 55) или CD;
- в командном интерпретаторе не будут выполняться команды, использующие USB-носитель:
  - `admin add spare keys`
  - `admin export keys binary-encrypted usb`
  - `admin export logs usb`
  - `admin export packetdb usb`
  - `admin upgrade software usb`

После перезагрузки сервера с виртуальной платформой или виртуальной машины ViPNet Coordinator VA существенно снижается скорость передачи данных на ViPNet Coordinator VA.

Чтобы скорость сетевых интерфейсов не снижалась, после каждой перезагрузки для всех сетевых интерфейсов выполняйте команды:

- После перезагрузки виртуальной машины на ViPNet Coordinator VA выполните:

  `ip li set vif<идентификатор виртуальной машины>.<номер интерфейса> qlen 1000`
- После перезагрузки сервера на Oracle VM Server выполните:

  `ethtool -K eth<номер интерфейса> gro off gso off`

На ViPNet Coordinator VA выполните:

```
ip li set vif<идентификатор виртуальной машины>.<номер интерфейса> qlen 1000
```

Если проблема не решена, см. документ «Настройка с помощью командного интерпретатора», раздел «Низкая скорость работы сетевых интерфейсов на Oracle VM Server».

Установка ViPNet Coordinator VA на Oracle VM Server

Для установки ViPNet Coordinator VA на платформу виртуализации Oracle VM Server:

1. Загрузите файл `*.ova` на FTP- или HTTP-сервер, развернутый в вашей сети.
2. В браузере откройте страницу доступа к Oracle VM Manager.
3. На вкладке **Repositories** нажмите кнопку **Import Virtual Appliance**.

Рисунок 20. Импорт образа вируальной машины

4. В окне **Import Virtual Appliance**:
   - В поле **Virtual Appliance download location** укажите сетевой путь к файлу `*.ova`, загруженному на шаге 1.
   - Установите флажок **Create VM**.
   - В списке **Server Pool** выберите область, в которой будут сохранены файлы виртуальной машины.
   - Нажмите кнопку **OK**.

Рисунок 21. Задание пути к образу виртуальной машины

5 На вкладке **Servers and VMs** выберите новую виртуальную машину и нажмите кнопку **Edit**.

Рисунок 22. Задание пути к образу виртуальной машины

6 В окне **Edit Virtual Machine**:

- На вкладке **Configuration tab**, в списке **Domain Type** выберите **Xen HVM PV Drivers**.
- Укажите параметры CPU, RAM, HDD (см. Требования к виртуальной среде на стр. 33).
- На вкладке **Networks** добавьте не менее 4 сетевых сетевых интерфейсов.

  Если сетевых интерфейсов будет меньше, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники через ноутбук по каналу Ethernet (см. Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP на стр. 50).
- Нажмите кнопку **OK**.

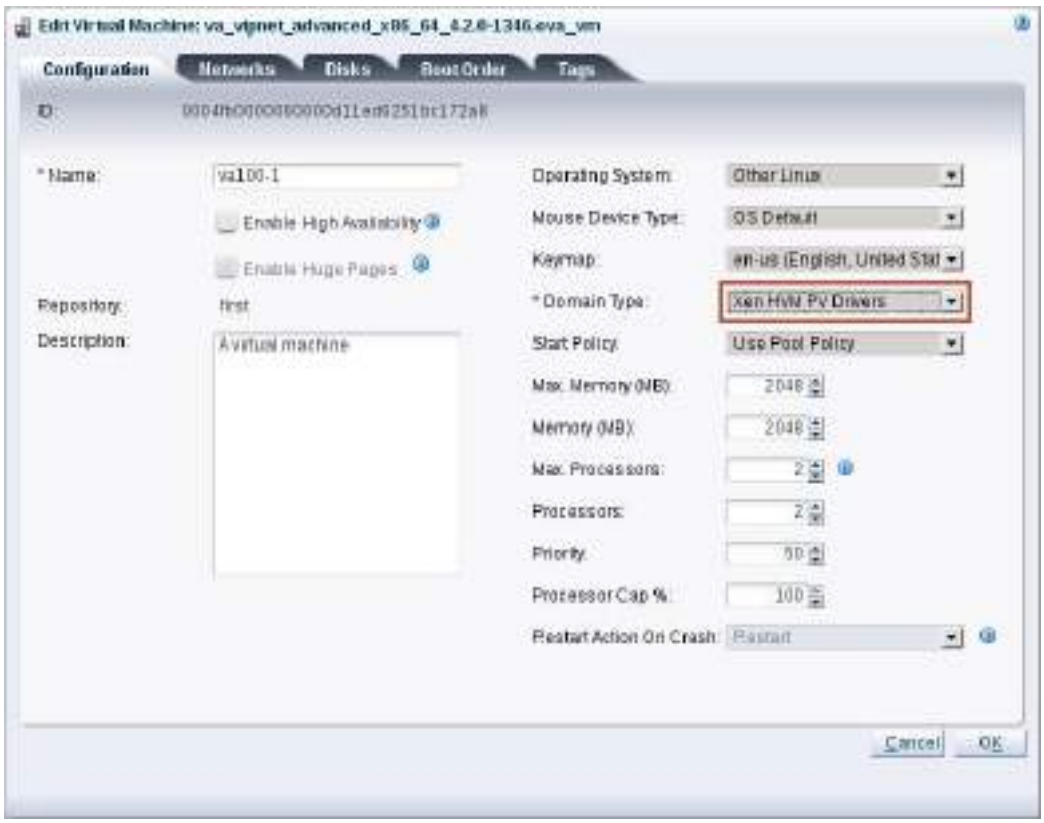

Рисунок 23. Настройка виртуальной машины

7 Запустите виртуальную машину и установите справочники и ключи (см. Способы установки и подготовка к установке справочников и ключей на стр. 50).

Внимание! При установке ключей и справочников используйте образ CD-диска для передачи дистрибутива ключей или файла импорта. Для этого скопируйте этот образ на FTP- или HTTP-сервер в вашей сети и укажите адрес этого файла в окне параметров виртуальной машины **Edit Virtual Machine** > **Disk**.

Microsoft Hyper-V

Microsoft Hyper-V не поддерживает подключение USB-устройств к виртуальной машине, поэтому:

- установка дистрибутива ключей возможна только с помощью TFTP (см. Установка дистрибутива ключей на ViPNet Coordinator VA на стр. 55) или CD;
- в командном интерпретаторе не будут выполняться команды, использующие USB-носитель:
  - `admin add spare keys`
  - `admin export keys binary-encrypted usb`
  - `admin export logs usb`
  - `admin export packetdb usb`
  - `admin upgrade software usb`

Для установки ViPNet Coordinator VA на платформу виртуализации Microsoft Hyper-V:

1 Распакуйте архив с расширением `.tar.gz`, содержащий два образа диска ViPNet Coordinator VA для Microsoft Hyper-V.

2 В программе Hyper-V Manager в меню **Actions** выберите **Virtual Switch Manager** и создайте новую виртуальную сеть.

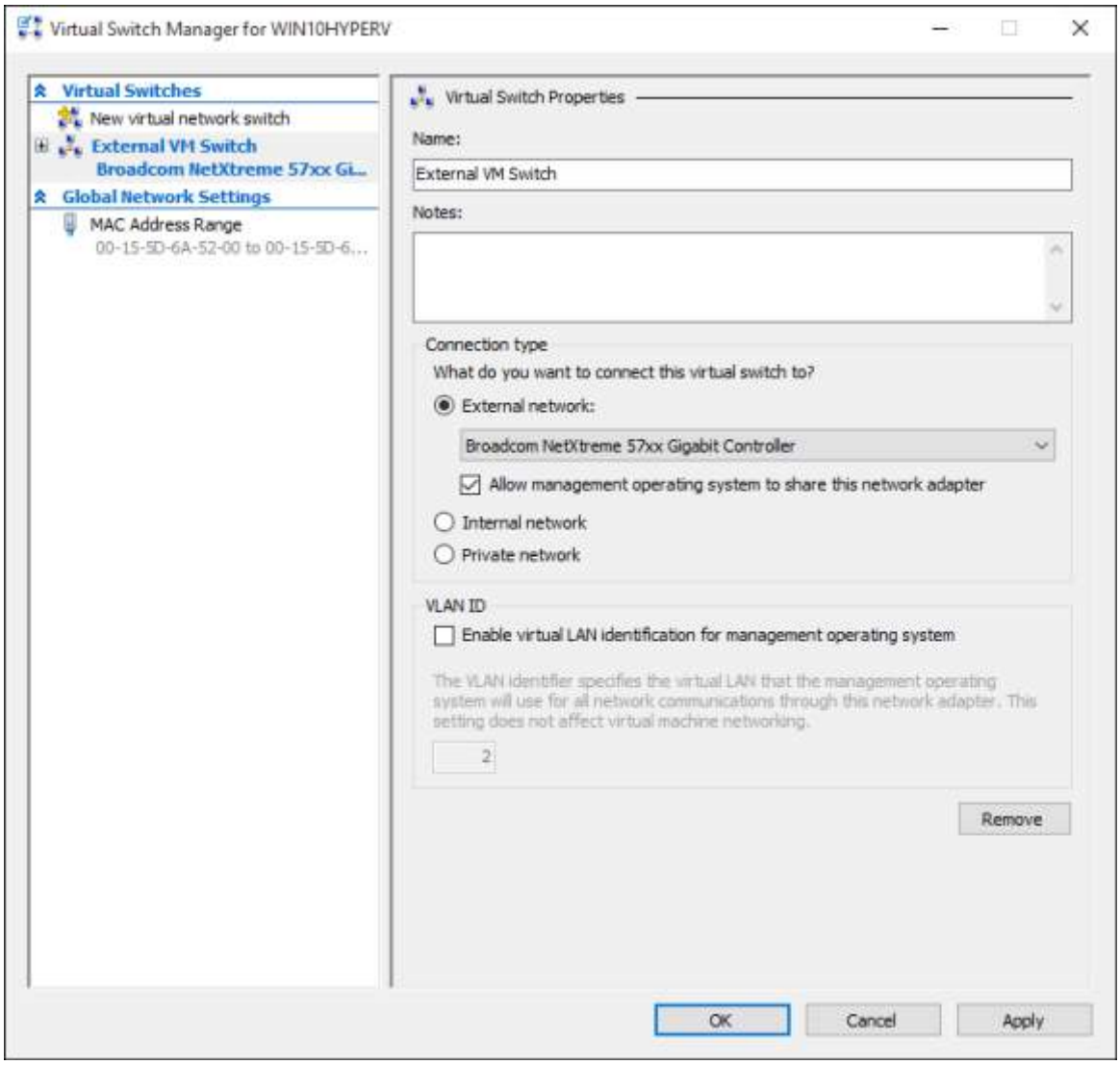

Рисунок 24. Создание виртуальной сети в Virtual Switch Manager

3 В программе Hyper-V Manager создайте новую виртуальную машину.

4 В настройках виртуальной машины в качестве жесткого диска укажите путь к первому образу ViPNet Coordinator VA для Microsoft Hyper-V (файл с расширением .vhd).

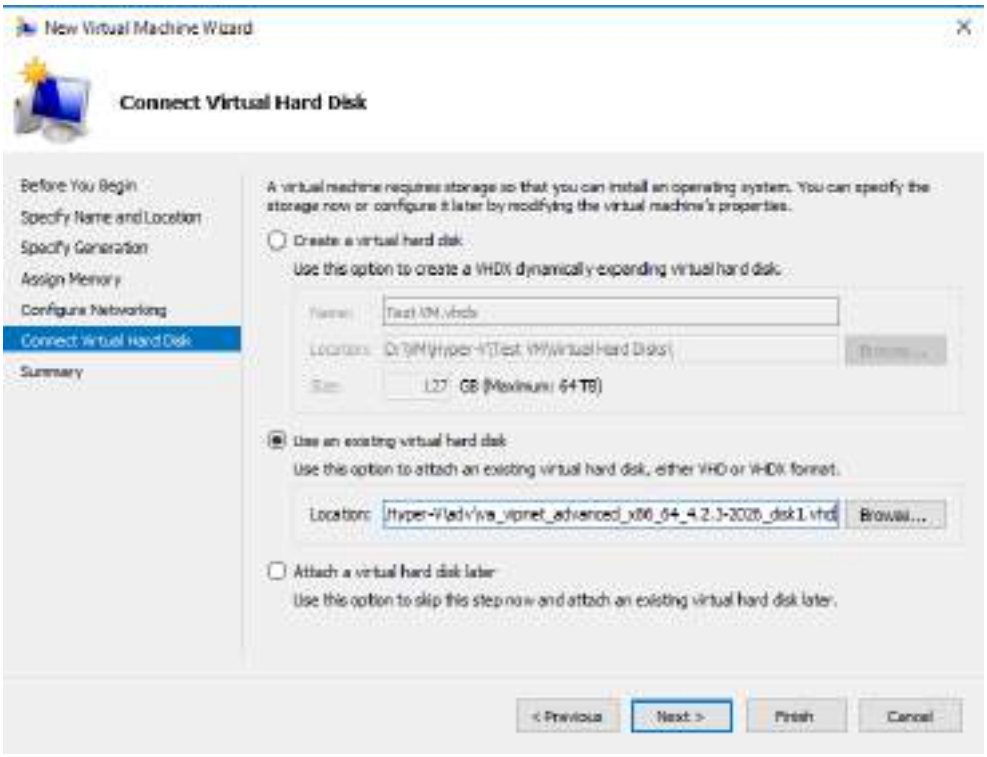

Рисунок 25. Выбор образа .vhd ViPNet Coordinator VA

5 После создания виртуальной машины в ее свойствах добавьте второй жесткий диск, указав путь ко второму образу ViPNet Coordinator VA для Microsoft Hyper-V (файл с расширением .vhd).

6 В свойствах виртуальной машины добавьте не менее 4 сетевых интерфейсов.

Если сетевых интерфейсов будет меньше, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники через ноутбук по каналу Ethernet (см. Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP на стр. 50).

7 Если на координаторе будет зарегистрировано более 1000 клиентов, то для виртуального диска укажите тип — **Fixed size**, иначе работа в сети ViPNet будет существенно замедлена

8 Запустите созданную виртуальную машину.

Примечание. При первой загрузке ViPNet Coordinator VA в журнале может появиться критическая ошибка с кодом 18590. Она связана с особенностью платформы Microsoft Hyper-V и не влияет на работоспособность координатора.

---

9 После загрузки ViPNet Coordinator VA установите справочники и ключи (см. Способы установки и подготовка к установке справочников и ключей на стр. 50).

KVM (Kernel-based Virtual Machine)

Для установки ViPNet Coordinator VA на платформу виртуализации KVM рекомендуется использовать графическую среду управления гипервизором. В качестве примера ниже

рассмотрена установка ViPNet Coordinator VA с помощью системы Proxmox, представляющей собой среду управления виртуализацией на базе KVM.

Примечание. Подробнее о ПО Proxmox см. на сайте поддержки proxmox.com). В зависимости от настроек платформы параметры развертывания могут отличаться от приведенных ниже.

Для установки ViPNet Coordinator VA на платформу виртуализации:

1 Подготовьте файл `*.raw` или `*.qcow2` с образом виртуальной машины ViPNet Coordinator VA.

Примечание. Шаги 3 и 4 (создание и развертывание виртуальной машины) можно выполнить в графическом интерфейсе менеджера виртуальных машин.

Шаг 5 (подключение дисков) выполняется только в командной строке.

2 Запустите командную строку и войдите в режим суперпользователя.

3 Создайте новое расположение для виртуальной машины и укажите ее параметры:

```
qm create <номер VM> --name va --net0 virtio,bridge=vmbr0 --serial0 \
--bootdisk scsi0 --scsihw virtio-scsi-pci
```

`<номер VM>` — произвольный номер виртуальной машины, в командах ниже он будет 110.

4 Запустите развертывание образа виртуальной машины:

```
qm importdisk 110 <путь к файлу с образом> local-lvm
```

5 После развертывания подключите диски виртуальной машины к SCSI-контроллерам:

```
qm set 110 --scsi0 local-lvm:vm-110-disk-0
qm set 110 --scsi1 local-lvm:vm-110-disk-1
```

6 Откройте менеджер виртуальных машин и выберите созданную виртуальную машину **110(va)**.

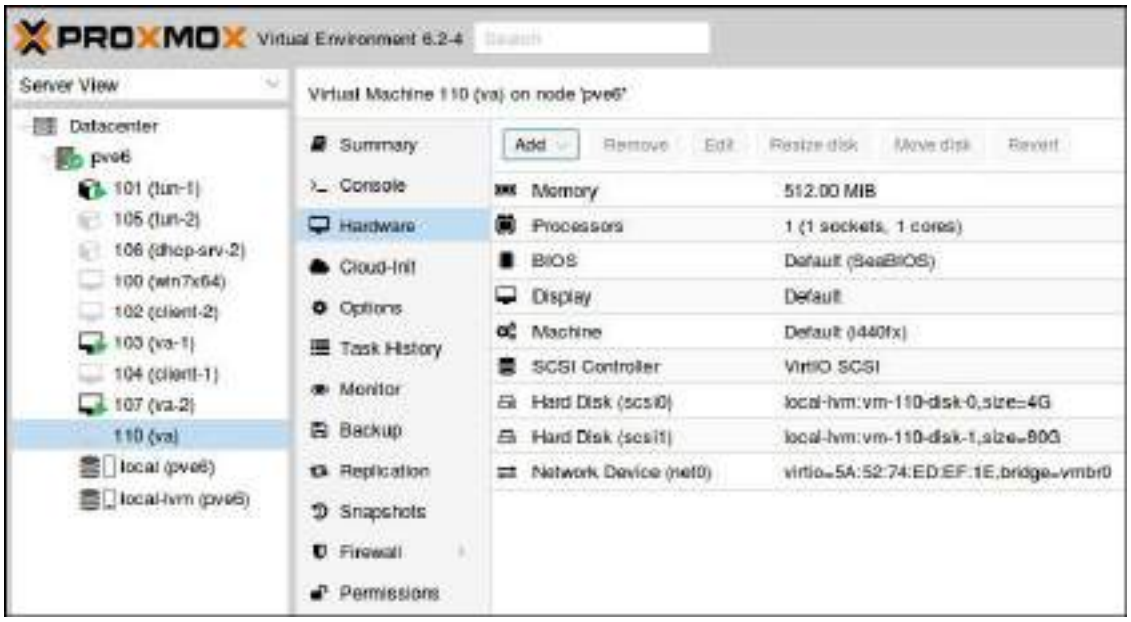

Рисунок 26. Запуск виртуальной машины ViPNet Coordinator VA

7 В разделе **Hardware** добавьте не менее 4 сетевых интерфейсов.

Если сетевых интерфейсов будет меньше, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники через ноутбук по каналу Ethernet (см. Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP на стр. 50).

8 Запустите виртуальную машину и установите справочники и ключи (см. Способы установки и подготовка к установке справочников и ключей на стр. 50).

Установка, обновление и удаление справочников и ключей

Способы установки и подготовка к установке справочников и ключей

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

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

  Файл `*.dst` и пароль вы можете получить у администратора сети ViPNet. Если администратор сети при создании дистрибутива ключей указал для пользователя ViPNet Coordinator VA способ аутентификации «Устройство», получите также внешнее устройство, на котором сохранен персональный ключ пользователя (см. глоссарий, стр. 86).

- Восстановление справочников, ключей и настроек на ViPNet Coordinator VA после некорректного обновления ПО или их перенос с другого ViPNet Coordinator VA того же исполнения.

  Для выполнения данных операций требуется файл `*.vbe`, в который были экспортированы справочники, ключи и настройки с другого действующего ViPNet Coordinator VA. Подробнее об этом см. в документе «Настройка с помощью командного интерпретатора», разделе «Резервное копирование и восстановление настроек».

Существует несколько способов установки справочников и ключей на ViPNet Coordinator VA. Способ установки зависит от способа подключения к ViPNet Coordinator VA.

Вы можете выбрать один из следующих способов установки:

- Через ноутбук по каналу Ethernet и протоколу TFTP. Удобен, если вы подключаетесь к компьютеру, на котором развернут виртуальный образ ViPNet Coordinator VA.
- Через внешнее устройство, которым может быть USB-носитель или CD-диск. Удобен, если вы подключаетесь к компьютеру, на котором развернут виртуальный образ ViPNet Coordinator VA, через обычную консоль (с использованием монитора и клавиатуры).

Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP

Для установки справочников и ключей вам понадобится:

- ноутбук с сетевой картой Ethernet и Windows или GNU/Linux любых версий;

- сетевой кросс-кабель Ethernet для соединения ноутбука с ViPNet Coordinator VA.

На ноутбуке должны быть включены стандартные службы Telnet (или SSH) и TFTP, которые необходимы для подключения к ViPNet Coordinator VA (Telnet или SSH) и для переноса дистрибутива ключей на ViPNet Coordinator VA (TFTP).

В GNU/Linux эти службы по умолчанию включены. В Windows эти службы по умолчанию отключены, чтобы их включить:

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**).

На время установки на ноутбуке с Windows:

1. Отключите ноутбук от внешней сети.
2. Отключите службы безопасности:
   - 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.
3. Отключите защиту ViPNet. Для этого в программе ViPNet Client выберите **Файл** > **Конфигурации** > **Отключить защиту**.

Перед началом установки справочников и ключей:

1. Перенесите на ноутбук дистрибутив ключей (файл `*.dst`).
2. С помощью кросс-кабеля подключите ноутбук к порту Ethernet1 компьютера, на котором развернут виртуальный образ ViPNet Coordinator VA.
3. 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 Coordinator VA по Telnet либо по протоколу SSH (с помощью Telnet- или SSH-клиента) по адресу `169.254.241.1`.

   На Telnet- или SSH-клиенте должны быть заданы следующие параметры (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 символов (**Windows** > **Columns**, введите **120**).

Примечание. Если ViPNet Coordinator VA недоступен по адресу `169.254.241.1`, значит при развертывании образа не добавлено нужное количество сетевых интерфейсов.

Для решения проблемы заново разверните виртуальный образ ViPNet Coordinator VA (см. Установка ViPNet Coordinator VA на платформу виртуализации на стр. 34) и добавьте не менее 4 сетевых интерфейсов.

Установка с помощью внешнего устройства

Перед началом установки справочников и ключей:

1. При использовании USB-носителя отформатируйте носитель в одну из поддерживаемых файловых систем: FAT32, ext3 или ext4.
2. Перенесите на USB-носитель или CD-диск дистрибутив ключей (файл `*.dst`).
3. Подключитесь к ViPNet Coordinator VA через обычную консоль: подключите монитор и клавиатуру к VGA-порту и PS/2-порту компьютера, на котором развернут виртуальный образ ViPNet Coordinator VA.

Установка справочников и ключей

Для установки справочников и ключей на координатор ViPNet Coordinator VA выполните все действия из приведенной таблицы.

Таблица 7. Последовательность установки справочников и ключей

	Действие	Ссылка
☐	Инициируйте установку справочников и ключей на ViPNet Coordinator VA	Начало установки (на стр. 53)
☐	Укажите часовой пояс, дату и время	Настройка часового пояса, даты и времени (на стр. 54)
☐	Выберите нужный дистрибутив ключей	Установка дистрибутива ключей на ViPNet Coordinator VA (на стр. 55)
☐	Настройте параметры всех сетевых интерфейсов ViPNet Coordinator VA	Настройка сетевых интерфейсов (на стр. 58)
☐	Настройте параметры DNS-сервера	Настройка DNS-сервера (на стр. 59)
☐	Настройте параметры NTP-сервера	Настройка NTP-сервера (на стр. 60)
☐	При необходимости измените настройки виртуальных адресов	Настройка имени компьютера и диапазона виртуальных адресов (на стр. 61)

	Действие	Ссылка
☐	Выберите режим подключения ViPNet Coordinator VA к внешней сети через межсетевой экран	Настройка подключения к внешней сети через межсетевой экран (на стр. 62)
☐	Проверьте связь с одним или несколькими узлами сети ViPNet	Проверка связи с другим сетевым узлом (на стр. 66)
☐	Завершите установку справочников и ключей	Завершение установки (на стр. 68)

Начало установки

Установка справочников и ключей 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 ключей 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 ключей 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 Coordinator VA. 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.

Примечание. Текст лицензионного соглашения отображается в кодировке KOI8-R, поэтому в случае, если вы подключены к ViPNet Coordinator VA через Telnet или SSH и текст лицензионного соглашения отображается неверно, убедитесь, что на вашем консольном клиенте заданы верные параметры.

4 В ответ на предложение начать установку в консольном режиме `Would you like to start installing keys or restoring configuration? [Yes/No]` введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**. Следуйте указаниям мастера.

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 компьютера, на котором развернут виртуальный образ ViPNet Coordinator VA, либо время должно быть задано в формате UTC, если местоположение установить невозможно. При установке справочников и ключей из файла `*.vbe` эти шаги выполняются автоматически, так как настройки часового пояса импортируются из файла экспорта.

Для настройки часового пояса, даты и времени ViPNet Coordinator VA 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 Coordinator VA 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**.

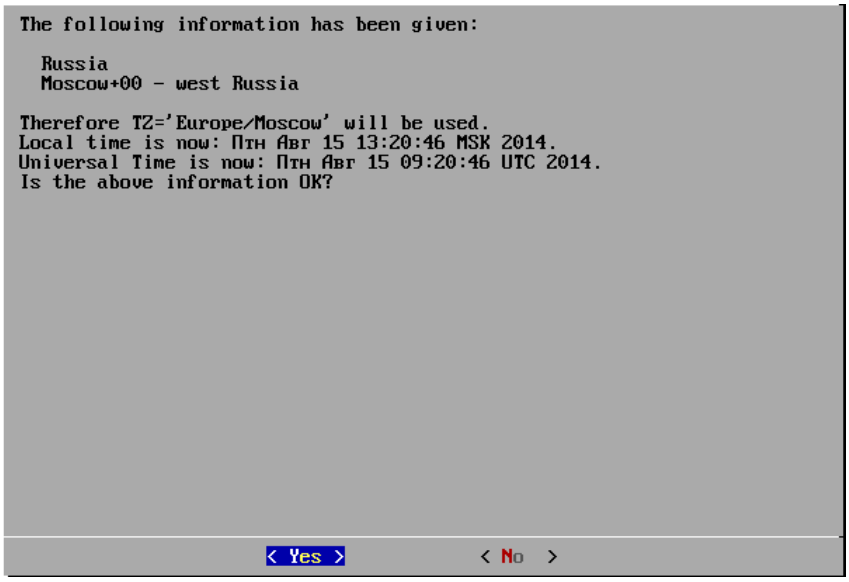

Рисунок 27. Запрос на установку часового пояса в полноэкранном режиме

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 часы-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 ключей на ViPNet Coordinator VA

Для переноса и установки дистрибутива ключей `*.dst` или файла экспорта `*.vbe` на ViPNet Coordinator VA 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**.

3. Если вы выбрали способ переноса с USB-носителя или CD-диска, подключите устройство к одному из USB-разъемов компьютера, на котором развернут виртуальный образ ViPNet Coordinator VA или вставьте диск в привод и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.
   Если на USB-носителе 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**.

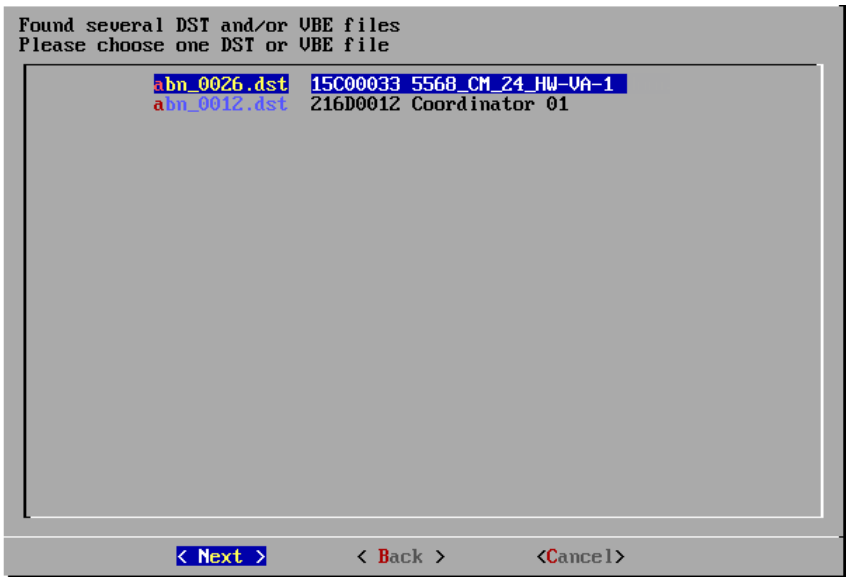

Рисунок 28. Выбор файла для установки справочников и ключей

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 ключей из выбранного файла.

5 Если администратор сети при создании дистрибутива ключей указал для пользователя ViPNet Coordinator VA способ аутентификации «Устройство», в ответ на сообщение `Insert token and enter PIN Code` выполните следующие действия:

- Подключите к одному из USB-разъемов компьютера, на котором развернут виртуальный образ ViPNet Coordinator VA токен, на котором сохранен персональный ключ пользователя (см. глоссарий, стр. 86).
- Введите ПИН-код доступа к подключенному устройству. ПИН-код вы можете получить у администратора вашей сети ViPNet.

Внимание! На подключенном токене должен быть только один контейнер, в котором содержится персональный ключ пользователя. При наличии нескольких контейнеров на устройстве персональный ключ пользователя не удастся найти, поэтому установка ключей не будет продолжена, о чем оповестит появившееся сообщение.

Если введенный ПИН-код верен, то появится соответствующее сообщение и установка справочников и ключей из выбранного файла будет продолжена.

По завершении установки справочников и ключей из дистрибутива ключей появится информация об узле, и мастер перейдет к следующему шагу (см. Настройка сетевых интерфейсов на стр. 58). По завершении установки справочников и ключей из файла экспорта мастер предложит перезагрузить компьютер (см. Завершение установки на стр. 68).

Настройка сетевых интерфейсов

При импорте справочников и ключей 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 Coordinator VA будут установлены те настройки, которые были на момент выполнения экспорта (см. Завершение установки на стр. 68).

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

Для настройки сетевых интерфейсов ViPNet Coordinator VA выполните следующие действия:

1. Включите интерфейс, если это необходимо. Для этого в консоли в ответ на сообщение `Configure interface eth<номер>? [Yes/No]` 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. 59).

2. Установите для интерфейса режим DHCP, если это необходимо. Для этого в ответ на сообщение `Use dhcp on the interface eth<номер>? [Yes/No]` 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**.

Внимание! При задании IP-адреса действуют следующие ограничения:

- нельзя задать IP-адрес 0.0.0.0;
- нельзя задать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255;
- для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети.

Также невозможно установить файл конфигурации (`*.vbe`), если он содержит настройки IP-адресов сетевых интерфейсов, в которых не соблюдаются описанные ограничения.

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**.

Внимание! Если хотя бы для одного включенного интерфейса задан режим DHCP, после установки справочников и ключей проверьте, что от DHCP-сервера был получен маршрут по умолчанию (см. глоссарий, стр. 85). Для этого выполните одно из действий:

- Выполните команду `hostname> inet show routing`. Если маршрут по умолчанию не был получен, будет выведено соответствующее предупреждение. В этом случае задайте статический маршрут по умолчанию (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка маршрутизации»).
- В веб-интерфейсе в разделе **Сетевые настройки** > **Маршрутизация** проверьте наличие маршрута по умолчанию (он имеет вид `0.0.0.0/0`). Если такого маршрута нет, задайте статический маршрут по умолчанию (см. документ «Настройка с помощью веб-интерфейса», раздел «Настройка маршрутизации»).

Настройка DNS-сервера

Для настройки DNS-сервера (см. глоссарий, стр. 81) выполните следующие действия:

1 Включите автоматический запуск DNS-сервера при загрузке ViPNet Coordinator VA, если это необходимо. Для этого в ответ на сообщение `Do you want to use DNS server? [Yes/No]` 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. 60).

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? [Yes/No]`.

- 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 ключей).

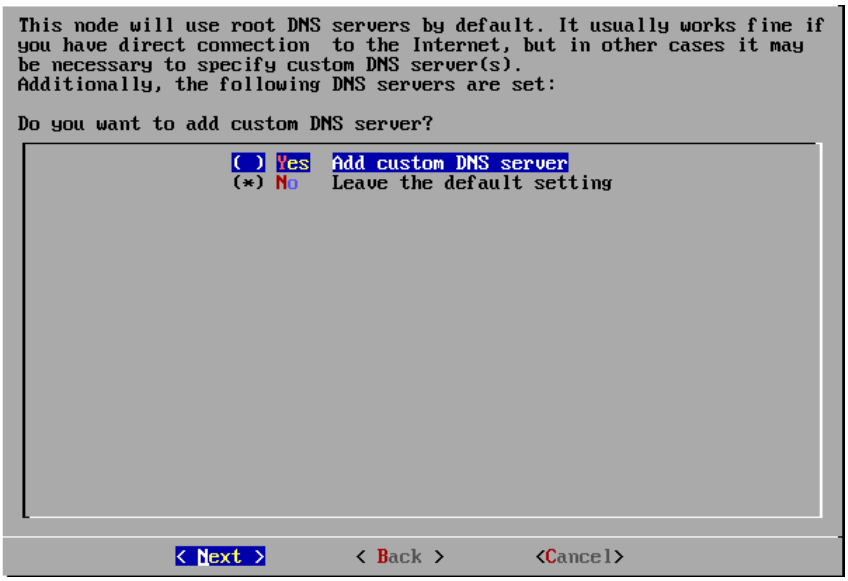

Рисунок 29. Запрос на добавление IP-адреса DNS-сервера в полноэкранном режиме

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

Настройка NTP-сервера

Для настройки NTP-сервера выполните следующие действия:

1 Включите автоматический запуск NTP-сервера при загрузке ViPNet Coordinator VA, если это необходимо. Для этого в ответ на сообщение `Do you want to use NTP daemon to synchronize the time? [Yes/No]` 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. 61).

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? [Yes/No]`.

- 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**.

- 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 ключей).

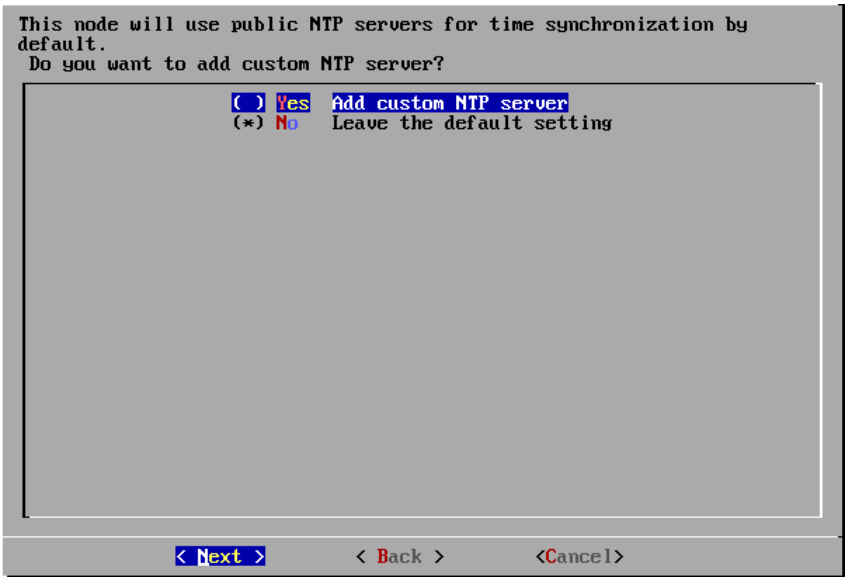

Рисунок 30. Запрос на добавление NTP-сервера в полноэкранном режиме

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 VA-<идентификатор узла>. Например: VA-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? [Yes/No]`.

Примечание. По умолчанию предлагается диапазон виртуальных адресов 11.0.0.1/8 (в нотации CIDR, что соответствует диапазону 11.0.0.1-11.255.255.254) Если этот диапазон пересекается с диапазоном IP-адресов, который используется для адресации в вашей сети, измените его.

Подробнее о виртуальных адресах см. документ «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора», раздел «Общие принципы назначения виртуальных адресов».

Виртуальные адреса из указанного диапазона будут назначаться одиночным туннелируемым адресам. Для диапазонов туннелируемых узлов адреса берутся из следующего интервала: <x+1>.0.0.1–<x+1>.255.255.254, где x — первый октет заданного диапазона виртуальных адресов.

Подробнее о задании виртуальных адресов для туннелируемых узлов см. документ «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора», раздел «Настройка видимости туннелируемых узлов».

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 (или только начальный адрес в нотации CIDR) нового диапазона виртуальных адресов и нажмите клавишу **Enter**. Например: 11.0.0.1-11.0.255.254 (или 11.0.0.1/16). 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 проверить соединение с узлом сети ViPNet (см. Проверка связи с другим сетевым узлом на стр. 66) и при необходимости настроить подключение к внешней сети через межсетевой экран (см. Настройка подключения к внешней сети через межсетевой экран на стр. 62).

Настройка подключения к внешней сети через межсетевой экран

Настроить подключение ViPNet Coordinator VA к внешней сети через межсетевой экран вы можете только в том случае, если на предыдущих этапах были выполнены следующие действия:

1 Настроен хотя бы один сетевой интерфейс (см. Настройка сетевых интерфейсов на стр. 58).

2 Дано согласие проверить соединение с одним из сетевых узлов ViPNet (см. Проверка связи с другим сетевым узлом на стр. 66).

Чтобы настроить подключение ViPNet Coordinator VA к внешней сети, выполните следующие действия:

1 После того, как вы согласились выполнить проверку соединения с узлом ViPNet, появится сообщение с предложением задать режим подключения ViPNet Coordinator VA к сети через межсетевой экран `Do you want to configure firewall mode? [Yes/No]`.

- Если вы хотите использовать настройки подключения к сети через межсетевой экран, заданные в файле дистрибутива ключей, режим подключения ViPNet Coordinator VA через межсетевой экран задавать не нужно. В этом случае введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**.

  После отказа от задания режима подключения ViPNet Coordinator VA к сети через межсетевой экран появляется сообщение с предложением выбрать сетевой интерфейс, через который необходимо проверить соединение с другим узлом.

- Если необходимо задать режим подключения ViPNet Coordinator VA к сети через межсетевой экран, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**.

2 Выберите режим подключения ViPNet Coordinator VA к внешней сети через межсетевой экран.

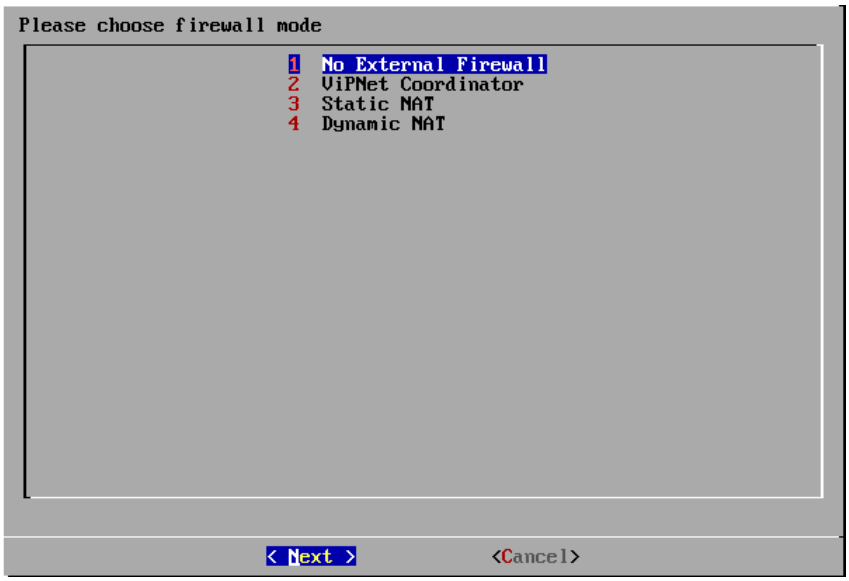

Рисунок 31. Выбор режима работы ViPNet Coordinator VA через межсетевой экран

- Чтобы выбрать режим «Без использования межсетевого экрана», введите цифру `1` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **1 (No External Firewall)** и нажмите кнопку **Next**.
- Чтобы выбрать режим «Координатор», введите цифру `2` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **2 (ViPNet Coordinator)** и нажмите кнопку **Next**.
- Чтобы выбрать режим «Со статической трансляцией адресов», введите цифру `3` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **3 (Static NAT)** и нажмите кнопку **Next**.

- Чтобы выбрать режим «С динамической трансляцией адресов», введите цифру `4` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **4 (Dynamic NAT)** и нажмите кнопку **Next**.

  Подробнее о режимах подключения к сети через межсетевой экран см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора».

3 Если был выбран режим **Без использования межсетевого экрана**, то перейдите к проверке связи с другим узлом ViPNet (см. Проверка связи с другим сетевым узлом на стр. 66).

4 Если был выбран режим **Координатор**, выполните следующие действия:

4.1 В ответ на сообщение `Please choose the network interface which will be use as external` выберите сетевой интерфейс, который будет являться внешним. Для этого введите цифру, соответствующую нужному сетевому интерфейсу в предложенном списке, и нажмите клавишу **Enter**. В полноэкранном режиме выберите нужный сетевой интерфейс и нажмите кнопку **Next**.

4.2 В ответ на сообщение `Please choose the ViPNet Coordinator` выберите координатор, через который ViPNet Coordinator VA будет подключаться к сети. Для этого введите номер координатора, приведенный в списке, и нажмите клавишу **Enter**. В полноэкранном режиме выберите нужный координатор и нажмите кнопку **Next**.

В списке выводятся только те координаторы, с которыми у ViPNet Coordinator VA есть связи. Информация о связях содержится в справочниках, установленных на ViPNet Coordinator VA.

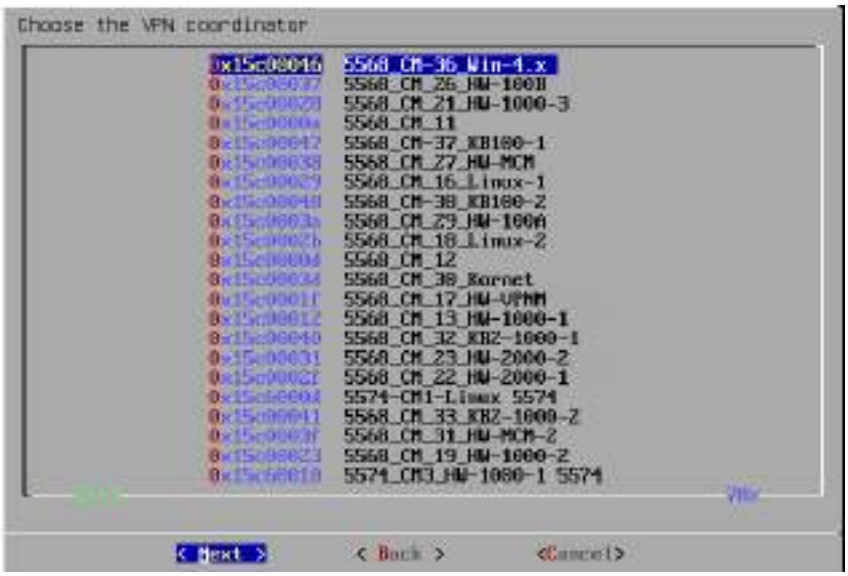

Рисунок 32. Выбор координатора для подключения к внешней сети

4.3 Если в справочниках не указан IP-адрес для выбранного координатора, мастер предложит вручную задать IP-адрес для него `The IP address of the ViPNet host has not been found. Do you want to specify one? [Yes/No]`.

Примечание. Если в установленных справочниках не будут обнаружены связи ViPNet Coordinator VA с другими координаторами сети ViPNet, появится сообщение `Your VPN host has no links with VPN coordinators`. В этом случае вы можете отменить настройку режима подключения или настроить другой режим.

Чтобы задать IP-адрес координатора, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите IP-адрес и нажмите клавишу **Enter**. В полноэкранном режиме введите IP-адрес и нажмите кнопку **Next**.

4.4 После этого перейдите к проверке связи с другим узлом ViPNet.

5 Если был выбран режим **Со статической трансляцией адресов**, выполните следующие действия:

5.1 В ответ на сообщение `Do you want to specify custom UDP port? [Yes/No]` укажите, следует ли изменить номер порта отправки (порт источника) и порта получения (порт назначения) IP-пакетов, преобразованных в UDP-формат, на ViPNet Coordinator VA. По умолчанию используется порт 55777.

Примечание. Изменять номер порта нужно в том случае, если внутри локальной сети через один межсетевой экран (или NAT-устройство) работает несколько узлов с ПО ViPNet. У всех таких узлов номера портов должны быть разными.

Если необходимо изменить номер порта, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите номер порта и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.

Если номер порта менять не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**.

5.2 В ответ на сообщение `Do you want to specify fixed IP address of the external firewall? [Yes/No]` укажите, следует ли задать фиксированный IP-адрес внешнего межсетевого экрана.

Примечание. Фиксированный IP-адрес межсетевого экрана нужно задавать тогда, когда требуется, чтобы входящие пакеты поступали на определенный адрес межсетевого экрана независимо от того, с какого адреса были отправлены исходящие пакеты.

Если необходимо задать IP-адрес, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите IP-адрес и нажмите клавишу **Enter**. В полноэкранном режиме введите IP-адрес и нажмите кнопку **Next**.

Если IP-адрес задавать не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. После этого перейдите к проверке связи с другим узлом ViPNet.

5.3 Выберите сетевой интерфейс, который будет являться внешним (аналогично п. 4.1).

6 Если был выбран режим **С динамической трансляцией адресов**, выполните следующие действия:

6.1 Выберите координатор, через который ViPNet Coordinator VA будет подключаться к сети (аналогично п. 4.2).

6.2 Задайте IP-адрес координатора, через который будет производиться подключение, если в установленных справочниках не обнаружены связи ViPNet Coordinator VA с другими координаторами сети ViPNet (аналогично п. 4.3).

6.3 Выберите сетевой интерфейс, который будет являться внешним (аналогично п. 4.1).

Проверка связи с другим сетевым узлом

Проверить связь с другим узлом ViPNet вы можете только в том случае, если на предыдущем этапе был настроен хотя бы один сетевой интерфейс (см. Настройка сетевых интерфейсов на стр. 58).

Для проверки связи с узлом ViPNet выполните следующие действия:

1 Если в процессе установки ключей вы изменяли параметры сетевых интерфейсов, то после настройки диапазона виртуальных адресов (см. Настройка имени компьютера и диапазона виртуальных адресов на стр. 61) появится сообщение с предложением выполнить проверку связи с одним из узлов сети ViPNet `Do you want to probe VPN-connection with some host in order to verify the configuration you've just made? [Yes/No]`. Выполните одно из действий:

- Если проверку связи с узлами выполнять не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. В этом случае установка справочников и ключей будет завершена.
- Если необходимо выполнить проверку связи с другим узлом, введите символ y и нажмите клавишу Enter. В полноэкранном режиме нажмите кнопку **Yes**.

Примечание. Проверку связи с другими узлами сети ViPNet рекомендуется выполнять во избежание возможной потери доступа к ViPNet Coordinator VA при завершении установки справочников и ключей.

В этом случае мастер предложит настроить подключение ViPNet Coordinator VA к внешней сети. Если требуется, выполните данную настройку (см. Настройка подключения к внешней сети через межсетевой экран на стр. 62). В противном случае настройки подключения к сети будут скопированы из дистрибутива ключей без изменения.

2 Появится список сетевых узлов ViPNet, с которыми ViPNet Coordinator VA имеет связи. Информация о связях содержится в справочниках, установленных на ViPNet Coordinator VA.

Выберите сетевой узел, связь с которым вы хотите проверить. Для этого в ответ на сообщение

```
Please choose the ViPNet host by number [<диапазон цифр, соответствующих узлам в списке>] or [q] to cancel or press Enter for next page
```

введите цифру, соответствующую сетевому узлу в списке, и нажмите клавишу **Enter**. В полноэкранном режиме выберите нужный сетевой узел и нажмите кнопку **Next**.

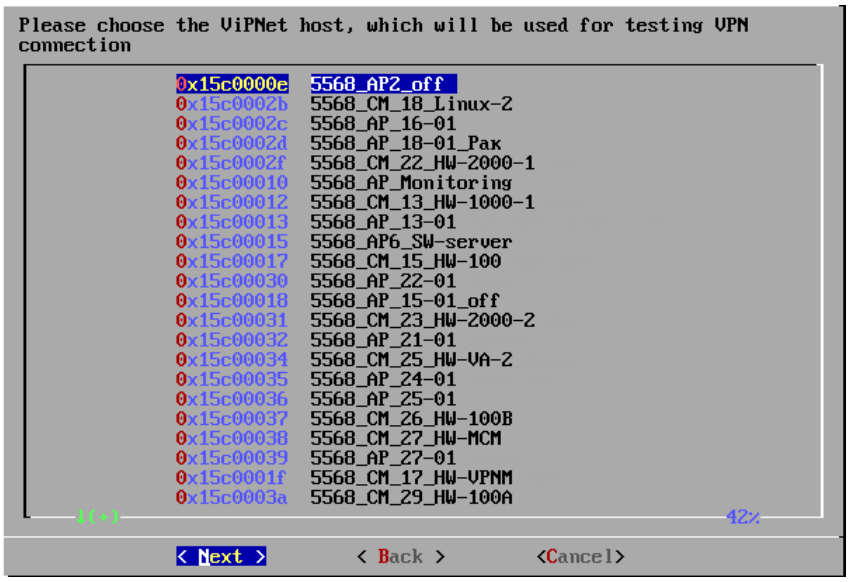

Рисунок 33. Выбор узла ViPNet для проверки связи

3 Если в справочниках не указан IP-адрес для выбранного сетевого узла, появится сообщение с предложением вручную задать для этого узла IP-адрес `The IP address of the ViPNet host has not been found. Do you want to specify one? [Yes/No]`.

Чтобы задать IP-адрес для сетевого узла, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите IP-адрес и нажмите клавишу **Enter**. В полноэкранном режиме введите IP-адрес и нажмите кнопку **Next**.

4 Начнется проверка связи с выбранным сетевым узлом ViPNet.

Примечание. Проверка связи с сетевым узлом ViPNet может занять несколько минут.

---

5 По окончании появляется сообщение о результатах проверки связи с выбранным узлом.

- Если связь с узлом была установлена, все выполненные настройки сохраняются в конфигурационный файл `iplir.conf`. Подробнее о файле `iplir.conf` см. в документе «ViPNet Coordinator VA. Справочное руководство по командному интерпретатору и конфигурационным файлам».

  Нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **OK**. Мастер предложит запустить драйверы и демоны (см. Завершение установки на стр. 68).

- Если установить связь с сетевым узлом не удалось, появляется сообщение с предложением просмотреть журнал регистрации IP-пакетов `Do you want to view IP packet log in order to investigate the issue? [Yes/No]`.

  - Для просмотра журнала введите символ y. На экране появится окно журнала IP-пакетов. Подробнее о работе с журналом см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора».
  - Для отказа от просмотра журнала введите символ n.

После этого будет предложено выполнить повторную проверку связи с другим узлом сети ViPNet.

Завершение установки

Для завершения установки справочников и ключей выполните следующие действия:

1 Если производится импорт справочников, ключей и настроек из файла `.vbe`, то для корректного применения настроек появится сообщение с предложением перезагрузить ViPNet Coordinator VA.

Для перезагрузки введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Reboot**. Работа мастера будет завершена, и ViPNet Coordinator VA 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 ViPNet Coordinator VA вручную.

2 Появится сообщение с предложением автоматически запустить драйверы и демоны ViPNet Coordinator VA после завершения установки `Do you want to start VPN services before leaving the installation wizard? [Yes/No]`. 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 ключей 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? [Yes/No]`. 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 ключей были настроены DNS- и NTP-серверы, запустите их с помощью команд:

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

Теперь вы можете выполнить необходимую настройку ViPNet Coordinator VA с помощью командного интерпретатора или веб-интерфейса в соответствии с требуемыми сценариями

использования. Подробнее см. документы «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора» и «ViPNet Coordinator VA. Настройка с помощью веб-интерфейса».

4

Возможности управления ViPNet Coordinator VA

Способы управления ViPNet Coordinator VA

Для настройки параметров ViPNet Coordinator VA вы можете использовать следующие средства:

- Административное программное обеспечение ViPNet — программы ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 83) и ViPNet Policy Manager (см. глоссарий, стр. 83).

  Выполнение настроек в ЦУСе облегчает управление ViPNet Coordinator VA и позволяет оповестить об изменении параметров сетевые узлы ViPNet, связанные с ViPNet Coordinator VA, путем отправки на эти узлы справочников и ключей. Программа Policy Manager позволяет централизованно управлять встроенными сетевыми экранами узлов, в том числе координаторов ViPNet Coordinator VA (см. Управление с помощью административного ПО ViPNet на стр. 76).

- Веб-интерфейс.

  Вы можете подключиться с удаленного компьютера и настроить ViPNet Coordinator VA с помощью веб-браузера. Возможности управления ViPNet Coordinator VA с помощью веб-интерфейса ограничены (см. Управление с помощью веб-интерфейса на стр. 77).

- Командный интерпретатор ViPNet Coordinator VA.

  Вы можете использовать командную оболочку ViPNet локально или удаленно через протокол SSH. Командный интерпретатор предоставляет наиболее полные возможности по администрированию ViPNet Coordinator VA (см. Управление с помощью командного интерпретатора на стр. 79).

Полномочия при различных способах управления

Примечание. Microsoft Hyper-V и Oracle VM Server не поддерживают подключение USB-устройств к виртуальной машине. Поэтому аутентификация с помощью токена на этих платформах невозможна.

Таблица 8. Основные действия, доступные при различных способах управления ViPNet Coordinator VA

	Режимы подключения		
	Пользователь узла	**Администратор узла**	**Администратор сети**
	Доступ		
Интерфейс для управления ViPNet Coordinator VA	веб-интерфейс (удаленное управление) командный интерпретатор (локальное или удаленное управление)		программа ViPNet Центр управления сетью или ViPNet Policy Manager (удаленное управление)
Способ аутентификации	пароль пользователя или аутентификация с помощью токена	пароль пользователя, пароль администратора узла ViPNet	пароль администратора ViPNet Центр управления сетью или ViPNet Policy Manager
	Установка		
Локальное обновление ПО ViPNet	–	+	–
Удаленное обновление ПО ViPNet	–	–	+
	Обслуживание		
Настройка системных параметров	–	+	–
Настройка параметров сетевых интерфейсов	–	+	-
Настройка подключения к внешнему межсетевому экрану	–	+	+

	Режимы подключения		
	Пользователь узла	**Администратор узла**	**Администратор сети**
Настройка IP-адресов ViPNet Coordinator VA и туннелируемых им IP-адресов	–	+	+
Настройка встроенного межсетевого экрана	–	+	+
Запуск и завершение работы демонов и драйверов	+ (только для командного интерпретатора)	+	–
Настройка системных служб	–	+	–
Просмотр журналов и настроек	–	+	–

Режимы работы в командном интерпретаторе и веб-интерфейсе

Вы можете работать с командным интерпретатором и веб-интерфейсом ViPNet Coordinator VA в одном из двух режимов:

- Режим пользователя. Данный режим становится активным по умолчанию после аутентификации на ViPNet Coordinator VA. При работе с командным интерпретатором или веб-интерфейсом в данном режиме пользователю недоступно изменение настроек ViPNet Coordinator VA. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ >.
- Режим администратора. В этом режиме в командном интерпретаторе и веб-интерфейсе доступны все настройки. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ #. Чтобы перейти в режим администратора, в командном интерпретаторе или веб-интерфейсе требуется авторизоваться с использованием пароля администратора сетевого узла.

Способы аутентификации пользователя

Прежде чем начать работу с ViPNet Coordinator VA с помощью командного интерпретатора или веб-интерфейса, требуется пройти аутентификацию. Возможно два способа аутентификации:

- «Пароль». При аутентификации требуется ввести имя учетной записи и пароль пользователя. Каждый раз при вводе пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу (см. глоссарий, стр. 86).
- «Устройство». При аутентификации требуется ввести имя учетной записи, подключить устройство, на котором сохранен персональный ключ, и ввести ПИН-код доступа к устройству. Этот способ аутентификации применим только при подключении к ViPNet Coordinator VA с помощью обычной консоли (см. глоссарий, стр. 86).

Внимание! Для аутентификации могут использоваться только внешние устройства Rutoken Lite производства компании «Актив».

Microsoft Hyper-V и Oracle VM Server не поддерживают подключение USB-устройств к виртуальной машине. Поэтому аутентификация «Устройство» на этих платформах невозможна.

Способ аутентификации задается администратором сети в программе ViPNet Удостоверяющий и ключевой центр. Впоследствии он может быть изменен на самом ViPNet Coordinator VA с помощью командного интерпретатора. Причем изменить способ аутентификации на ViPNet Coordinator VA можно только на «Устройство». Изменение способа аутентификации с «Устройство» на «Пароль» запрещено по требованиям безопасности. Подробнее об изменении способа аутентификации см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора».

При локальном подключении к ViPNet Coordinator VA аутентификация производится в командном интерпретаторе (см. Управление с помощью командного интерпретатора на стр. 79).

При подключении через веб-интерфейс (см. Управление с помощью веб-интерфейса на стр. 77) или удаленном подключении по протоколу SSH (см. Удаленное подключение с помощью протокола SSH на стр. 80) аутентификация состоит из двух этапов:

1. Вначале в соответствии с заданным способом выполняется аутентификация в ПО ViPNet, которое установлено на удаленном рабочем месте для защиты канала передачи данных с ViPNet Coordinator VA.
2. Затем выполняется аутентификация по паролю при непосредственном подключении к ViPNet Coordinator VA через веб-интерфейс или по протоколу SSH.

Управление с помощью административного ПО ViPNet

Для удаленной настройки параметров ViPNet Coordinator VA может использоваться следующее управляющее программное обеспечение ViPNet:

- ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 83).

  Данная программа, входящая в состав программного комплекса ViPNet Administrator (см. глоссарий, стр. 83), предназначена для формирования структуры сети ViPNet, задания основных параметров сетевых узлов, централизованной отправки справочников, ключей и программного обеспечения на сетевые узлы ViPNet (подробнее см. в документе «ViPNet Центр управления сетью. Руководство администратора»).

  В ЦУСе администратор сети ViPNet может настроить адреса доступа к ViPNet Coordinator VA, параметры подключения узла ViPNet Coordinator VA к внешней сети через межсетевой экран, адреса туннелируемых узлов. Настройки, выполненные в ЦУСе, применяются на узле ViPNet Coordinator VA после установки полученного доверенным способом файла `*.dst`, либо после получения справочников или ключей на этом узле по сети ViPNet.

- ViPNet Policy Manager (см. глоссарий, стр. 83).

  Данная программа предназначена для формирования политик безопасности (см. глоссарий, стр. 86) и их рассылки на узлы по сети ViPNet (подробнее см. в документе «ViPNet Policy Manager. Руководство администратора»). Политики безопасности могут включать в себя сетевые фильтры и правила трансляции IP-адресов. Фильтры и правила трансляции, полученные из программы ViPNet Policy Manager, недоступны для редактирования на узлах.

Управление с помощью веб-интерфейса

Для удаленного управления и частичной настройки ViPNet Coordinator VA вы можете использовать веб-интерфейс, который входит в его состав. С помощью веб-интерфейса ViPNet Coordinator VA вы можете выполнять следующие действия:

- Настройка даты и времени.
- Настройка подключения ViPNet Coordinator VA к сети, настройка сетевых интерфейсов.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов.
- Настройка туннелирования адресов.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера, DHCP-relay.
- Настройка защиты соединения по технологии L2OverIP.
- Настройка статической и динамической маршрутизации.
- Настройка функции MultiWAN.
- Работа со списком сетевых узлов ViPNet.
- Настройка параметров удаленного мониторинга по протоколу SNMP.
- Мониторинг состояния ViPNet Coordinator VA, настройка параметров протоколирования событий, просмотр системного журнала, журналов регистрации IP-пакетов, транспортных конвертов, переключений режимов кластера (в режиме кластера).

Подключение к веб-интерфейсу ViPNet Coordinator VA следует осуществлять только с других защищенных узлов ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 83)).

Внимание! Предоставлять удаленный доступ к ViPNet Coordinator VA с незащищенных узлов запрещено. С помощью фильтров защищенной сети следует ограничить соединения между ViPNet Coordinator VA и рабочими местами администраторов, разрешив только удаленное управление и передачу данных по служебным протоколам ViPNet.

Возможно одновременное подключение к ViPNet Coordinator VA с нескольких защищенных узлов. Одновременно с веб-интерфейсом могут работать не более 5 пользователей, причем только один из них — в режиме администратора.

Примечание. Для подключения к веб-интерфейсу ViPNet Coordinator VA используйте браузеры Internet Explorer 11, Microsoft Edge, Google Chrome и Mozilla Firefox последних версий. В настройка браузера укажите следующие разрешения:

- разрешить сайтам сохранять и просматривать данные файлов Cookie;
- разрешить загружать с сайта и выполнять сценарии JavaScript.

Установите разрешение экрана 1360x768 пикселей или выше.

После обновления ViPNet Coordinator VA с предыдущей версии рекомендуется очистить кэш браузера. В противном случае возможны проблемы с подключением и использованием веб-интерфейса.

Подробнее о работе с веб-интерфейсом см. в документе «ViPNet Coordinator VA. Настройка с помощью веб-интерфейса».

Управление с помощью командного интерпретатора

Командный интерпретатор обеспечивает наиболее полные возможности администрирования ViPNet Coordinator VA по сравнению с другими вариантами управления. С помощью командного интерпретатора ViPNet вы можете выполнять следующие действия:

- Настройка системных функций ViPNet Coordinator VA: настройка даты и времени, создание копий конфигурации и другое.
- Настройка подключения ViPNet Coordinator VA к сети, настройка сетевых интерфейсов.
- Настройка режимов подключения ViPNet Coordinator VA к сети через межсетевой экран.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов.
- Управление обработкой прикладных протоколов.
- Настройка VPN: настройка видимости узлов, туннелирования адресов, работа со списком сетевых узлов ViPNet и другие.
- Настройка защиты соединения по технологии L2OverIP.
- Настройка транспортного модуля: выбор канала передачи конвертов между узлами, настройка протоколирования событий транспортного модуля и другое.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера, DHCP-relay.
- Настройка статической и динамической маршрутизации.
- Настройка системы защиты от сбоев.
- Настройка функции MultiWAN.
- Резервирование справочников, ключей и настроек ViPNet Coordinator VA, обновление ViPNet Coordinator VA.
- Настройка параметров протоколирования событий, просмотр системного журнала, журналов регистрации IP-пакетов, транспортных конвертов.
- Настройка параметров удаленного мониторинга по протоколу SNMP и другое.

Командный интерпретатор запускается автоматически после аутентификации пользователя ViPNet Coordinator VA. При этом он может быть запущен как локально с помощью обычной консоли (см. глоссарий, стр. 86), так и удаленно при подключении с других узлов сети ViPNet, связанных с ViPNet Coordinator VA, по протоколу SSH (см. Удаленное подключение с помощью протокола SSH на стр. 80).

Подробнее о настройке и обновлении ПО ViPNet Coordinator VA с помощью командного интерпретатора, а также об остальных операциях в командном интерпретаторе см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора».

Удаленное подключение с помощью протокола SSH

Настройку и управление ViPNet Coordinator VA с помощью командного интерпретатора можно производить не только через локальную консоль, но также с помощью удаленного подключения по протоколу SSH. Удаленное подключение к ViPNet Coordinator VA следует осуществлять только с других защищенных узлов ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 83)).

Внимание! Предоставлять удаленный доступ к ViPNet Coordinator VA с незащищенных узлов запрещено. С помощью фильтров защищенной сети следует ограничить соединения между ViPNet Coordinator VA и рабочими местами администраторов, разрешив только удаленное управление и передачу данных по служебным протоколам ViPNet.

Возможно одновременное подключение к ViPNet Coordinator VA с нескольких узлов. При этом одновременно может быть запущено не более 30 удаленных сессий, и только в одной удаленной сессии можно работать в режиме администратора.

Подробнее об удаленном подключении и его особенностях см. в документе «ViPNet Coordinator VA. Настройка с помощью командного интерпретатора», в разделе «Работа с командным интерпретатором».

Глоссарий

DAD (Duplicate address detection)

Duplicate address detection (обнаружение дублирования адреса) — метод проверки уникальности IP-адреса с помощью отправки специального ARP-запроса с указанием проверяемого IP-адреса и ожиданием ответа от этого IP-адреса. Результатом является получение от устройства с указанным IP-адресом ответа. Если в течение определенного времени ответ не поступил, считается, что такой адрес в сети не используется.

DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса серверов DNS, IP-адреса серверов WINS.

DHCP-сервер

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

DiffServ (Differentiated Service)

Протокол, обеспечивающий классификацию сетевого трафика при помощи DSCP-меток, добавляемых в заголовки IP-пакетов.

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам сетевых узлов 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.

L2OverIP

Технология, которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов сети смогут взаимодействовать друг с другом так, как будто они находятся в одном сегменте с прямой видимостью по MAC-адресам. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

MIME-тип

Тип данных, которые могут быть переданы с помощью Интернета с применением стандарта MIME.

MTU (Maximum Transmission Unit)

Максимальный размер полезного блока данных пакета, который может быть передан через сетевой интерфейс без фрагментации.

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.

OSPF (Open Shortest Path First)

Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала для нахождения кратчайшего маршрута. Распространяет информацию о доступных маршрутах внутри автономной системы.

PPP (Point-to-Point Protocol)

Протокол канального уровня, использующийся для установления прямой связи между двумя узлами сети.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

TCP-туннель настраивается на координаторе, который является для клиента сервером соединений.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Policy Manager

Программа для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Центр управления сетью (ЦУС)

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.

VPN-сервер

Функция координатора, включающая в себя задачи сервера IP-адресов и транспортного сервера сети ViPNet.

Административная дистанция

Характеристика маршрута. Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

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.

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям

благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

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 сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Динамический сетевой интерфейс

Разновидность сетевого интерфейса, который добавляется в процессе работы при наступлении некоторого события (например, при подключении USB-модема, предоставляющего данный интерфейс).

Динамические интерфейсы объединяются в группы по типу интерфейса. Поэтому иногда может встречаться термин «групповой динамический интерфейс».

Дистрибутив ключей

Файл с расширением `*.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Маршрут по умолчанию

Путь следования IP-пакетов, для которых не был найден подходящий маршрут в таблице маршрутизации.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Мастер-ключ

Ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена;
- мастер-ключ ключей защиты ключей обмена;
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

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 IP-адресов в адреса, доступные из внешней сети (выполняет NAT).

Метрика маршрута

Параметр, определяющий приоритет маршрута передачи IP-трафика.

Обычная консоль

Монитор и клавиатура, которые используются для локальной настройки ViPNet Coordinator VA.

Открытый интернет (Защищенный интернет-шлюз)

Технология, реализованная в программном обеспечении ViPNet. При подключении к интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

Начиная с версии ПО ViPNet Administrator ЦУС 4.6.3, технология «Открытый Интернет» называется «Защищенный интернет-шлюз».

Открытый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

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.

ПК ViPNet StateWatcher

Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher, который предназначен для наблюдения за состоянием узлов сетей ViPNet, мониторинга событий безопасности, происходящих на сетевых узлах, своевременного выявления неполадок в работе узлов и оперативного оповещения пользователей о возникающих проблемах.

Политика безопасности

Набор параметров, регулирующих безопасность сетевого узла. В технологии ViPNet безопасность сетевых узлов обеспечивается с помощью сетевых фильтров и правил трансляции сетевых адресов.

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ создает для пользователя. Имя этого файла имеет маску AAAA.pk, где AAAA — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее устройствами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Статический сетевой интерфейс

Сетевой интерфейс, для работы которого требуется задать секцию `[adapter]` в файле `iplir.conf` с описанием параметров этого интерфейса. К таким интерфейсам относятся физические (Ethernet) и виртуальные (VLAN) интерфейсы.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки конверта.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на сетевые узлы ViPNet транспортным модулем ViPNet MFTP.

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Транспортный сервер

Функциональность координатора, обеспечивающая маршрутизацию транспортных конвертов между узлами сети ViPNet.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ЦУСе каждой сети при организации взаимодействия между двумя различными сетями ViPNet.