ViPNet Coordinator HW 4

Подготовка к работе

Версия продукта: 4.5.6

ViPNet Coordinator HW10
ViPNet Coordinator HW50
ViPNet Coordinator HW100
ViPNet Coordinator HW1000
ViPNet Coordinator HW2000
ViPNet Coordinator HW5000
ViPNet Coordinator VA

infotecs

ФРКЕ.00130-03 90 02

Версия продукта 4.5.6, документ обновлен 10.12.2024

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Документ содержит сведения о назначении и применении комплекса ViPNet Coordinator HW в составе защищенных сетей ViPNet, способах настройки и управления, описание исполнений ViPNet Coordinator HW и условий лицензирования. Также в документе приведен порядок действий по подготовке ViPNet Coordinator HW к работе.

Документ предназначен для администраторов сетей ViPNet.

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, путь, фрагмент кода или команда в командной строке

Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

Обозначения при описании команд в документе:

- Команды, которые участвуют в сценарии администратора, обозначены символом `#`

  ```
  hostname# admin config list
  ```

- Команды, которые участвуют в сценарии пользователя, обозначены символом `>`

  ```
  hostname> firewall local show
  ```

  Все команды, которые доступны пользователю, доступны и администратору.

- Параметры заключены в угловые скобки:

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

- Необязательные параметры или ключевые слова заключены в квадратные скобки:

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

- Допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:

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

Что нового в версии 4.5.6

- **Новая аппаратная платформа**

  Добавлена поддержка аппаратной платформы HW1000 Q10. Подробные характеристики приведены в разделе Аппаратная платформа HW1000 Q10.

- **Серийный номер аппаратной платформы**

  Теперь для исполнений на аппаратных платформах ПО ViPNet Coordinator HW поддерживает функцию добавления серийного номера. Данная информация доступна в командном интерпретаторе, веб-интерфейсе и может передаваться по протоколу SNMP во внешние системы.

- **Замена NTP-серверов по умолчанию и возможность их отключения**

  В предыдущих версиях локальный NTP-сервер синхронизировал время с публичными NTP-серверами по умолчанию из кластера pool.ntp.org. В новой версии ViPNet Coordinator HW кластер серверов по умолчанию заменен на vniiftri.ru. Также теперь при добавлении дополнительных NTP-серверов вы можете исключить из процесса синхронизации времени публичные NTP-серверы, заданные по умолчанию.

- **Добавление дополнительных адресов на интерфейсе в режиме автоматического получения параметров от DHCP-сервера**

  В предыдущих версиях дополнительные адреса можно было назначать только для интерфейсов, на которых настроены статические адреса. Теперь это ограничение снято.

- **Возможность указать идентификатор области маршрутизации в новом формате**

  В новой версии при настройке протокола OSPF идентификатор области маршрутизации можно задать в формате `A.B.C.D`, где `A,B,C,D` — целое число от 0 до 255.

- **Настройка хранения журнала транспортных конвертов**

  В новой версии вы можете настроить объем дискового пространства, доступного для хранения текстовых файлов, в которые выгружается информация из журнала транспортных конвертов. Подробнее см. документ «Справочник команд и конфигурационных файлов» описание параметра `max_log_space` секции `[journal]` файла `mftp.conf`.

Обратная связь

Контактная информация

- Единый многоканальный телефон:

  +7 (495) 737-6192,

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

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телеграм-канал поддержки: t.me/vhd21

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- О продуктах ViPNet.
- О решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется политикой ответственного разглашения.

1

Общая информация

Защищенная сеть ViPNet

Сеть ViPNet — виртуальная защищенная сеть, которая может быть развернута поверх локальных и глобальных IP-сетей. Технология ViPNet позволяет создать защищенные VPN-туннели между узлами сети ViPNet с помощью протоколов трех типов: IP/241, UDP и TCP, в которые инкапсулируются пакеты любых других IP-протоколов. Данные, передаваемые в VPN-туннелях, зашифровываются с помощью симметричных ключей; ключи шифрования создаются и распределяются централизованно. Каждая сеть ViPNet имеет свой уникальный идентификатор.

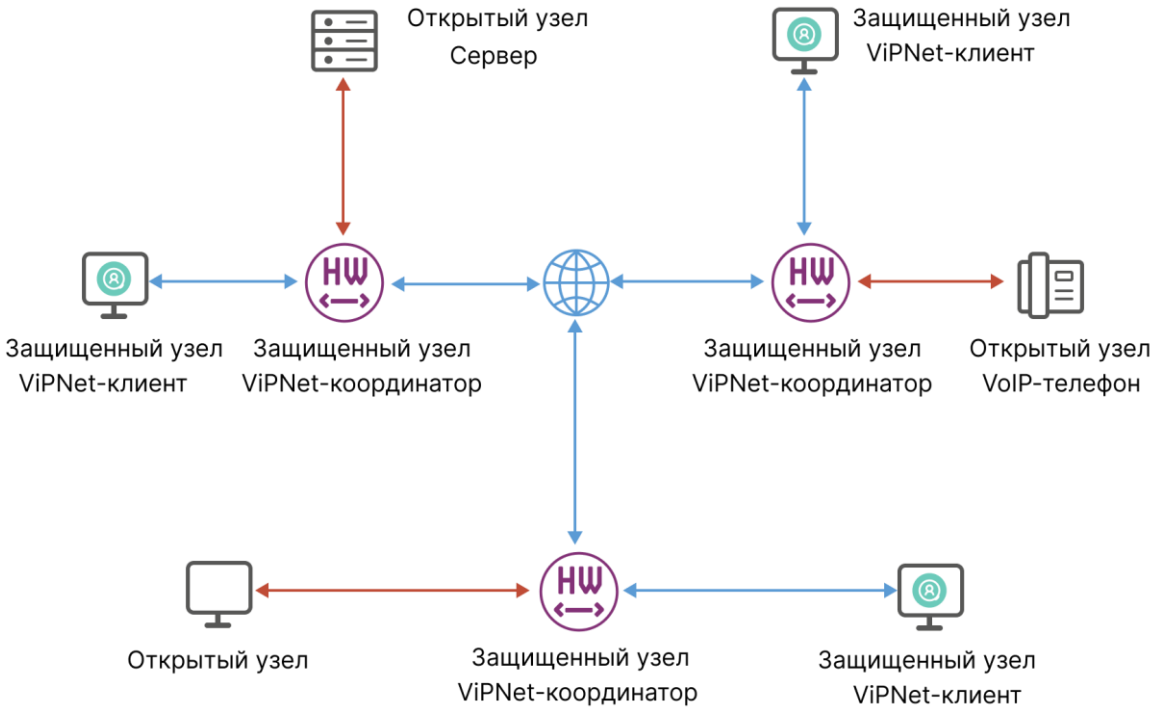


Рисунок 1. Типы узлов сети ViPNet

Типы узлов сети ViPNet:

- ViPNet-клиент — компьютер (Windows, Linux, macOS) или мобильное устройство (iOS, Android или Аврора) с установленным клиентским ПО ViPNet.
- ViPNet-координатор — сервер сети ViPNet. Аппаратная платформа с интегрированным ПО ViPNet или ПО ViPNet, развернутое на платформе виртуализации: например, ViPNet Coordinator HW на базе аппаратной платформы, ViPNet Coordinator VA на базе платформы виртуализации. В технологических сетях, например АСУ ТП, в роли ViPNet-координатора применяется ViPNet Coordinator IG, поддерживающий промышленные протоколы и интерфейсы.
- Открытый узел — компьютер или другое устройство (например SIP-телефон) без ПО ViPNet, расположенные в сети «за ViPNet-координатором».

Настройка и управление сетью ViPNet выполняется из управляющего ПО: ViPNet Administrator или ViPNet Prime. Основные функции:

- Создание узлов сети ViPNet и связей между ними.

- Настройка узлов сети ViPNet.
- Создание дистрибутивов ключей для узлов сети ViPNet.
- Централизованное обновление справочников и ключей.
- Централизованное обновление ПО ViPNet на узлах сети ViPNet.

Внимание! Одновременная работа сети ViPNet под управлением ViPNet Administrator и ViPNet Prime невозможна.

Управление политиками безопасности узлов сети ViPNet выполняется централизованно с помощью ViPNet Policy Manager или модулем ViPNet Prime Policy Management.

Для мониторинга состояния узлов сети ViPNet используется ViPNet StateWatcher или ViPNet NVS.

Основные функции ViPNet Coordinator HW

- Сервер IP-адресов. Обеспечивает взаимодействие защищенных узлов ViPNet. Сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.
- Маршрутизатор VPN-пакетов. Обеспечивает маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы.
- Сервер соединений. Обеспечивает соединение клиентов и координаторов друг с другом.
- VPN-шлюз. Позволяет организовать соединения между узлами сети и между сегментами сетей с помощью защищенных каналов (туннелей).
- Транспортный сервер MFTP. Обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из ViPNet ЦУС или Prime, а также обмен прикладными транспортными конвертами между узлами.
- Защищенный интернет-шлюз. Обеспечивает раздельный доступ защищенных узлов в интернет и к ресурсам защищенной сети ViPNet.
- Межсетевой экран. Фильтрует IP-трафик на основе заданных правил; транслирует адреса (NAT) для открытого IP-трафика.

Сервер IP-адресов

Клиенту для взаимодействия с другими защищёнными узлами требуется информация об адресах и параметрах доступа. Данную информацию клиент получает автоматически от координатора, который выполняет функцию сервера IP-адресов.

Принцип работы сервера IP-адресов:

- При появлении новой информации о клиенте, который использует данный координатор в качестве сервера IP-адресов, координатор рассылает её на связанные клиенты и координаторы.
- При появлении новой информации о клиентах других координаторов, координатор рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора.
- В случае взаимодействия координатора с другой сетью ViPNet на шлюзовой координатор 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 информацию на все координаторы своей сети, а также на свои клиенты, связанные с узлами другой сети.

Также сервер IP-адресов рассылает информацию о статусе сетевого узла:

- 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» и оповещает другие узлы, с которыми у данного клиента есть связь.
- Чтобы подтвердить свое присутствие в сети, координатор периодически (по умолчанию — каждые 15 минут) отсылает на другие связанные с ним координаторы подтверждение о своей активности.

По умолчанию для клиента в качестве сервера IP-адресов выступает координатор, на котором клиент зарегистрирован в ViPNet ЦУС или Prime. Сервер IP-адресов можно сменить, выбрав другой координатор, с которым у данного клиента есть связь.

Маршрутизатор VPN-пакетов

Клиенты, находящиеся в разных подсетях, связываются друг с другом через координаторы. Координатор при этом выполняет маршрутизацию защищённого трафика в сети ViPNet.

Защищённый трафик маршрутизируется на основе идентификаторов (ViPNet ID), которые присваиваются каждому узлу сети ViPNet и не меняются при смене IP-адреса узла. Это позволяет узлам защищённой сети взаимодействовать между собой независимо от изменений параметров и конфигурации физической сети.

Порядок взаимодействия клиентов через координатор:

- Клиент вставляет в открытую часть IP-пакета идентификатор узла назначения и отправляет IP-пакет координатору (идентификатор защищён от подмены).
- Координатор на основе идентификатора определяет маршрут доставки IP-пакета и отправляет его адресату или другому координатору, указав свой IP-адрес в качестве адреса источника (параметры трансляции адресов для защищённого трафика изменить нельзя).

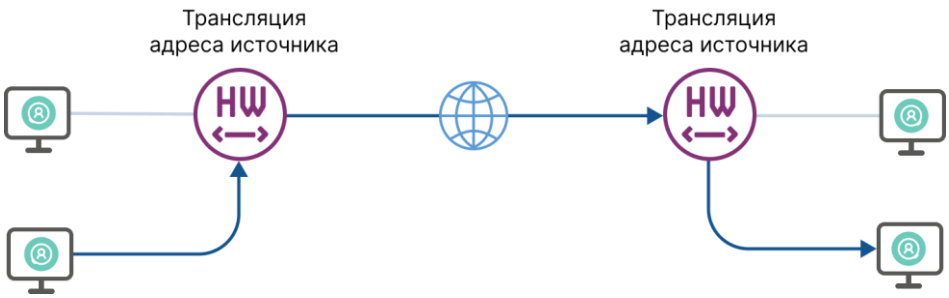


Рисунок 2. Функция маршрутизации защищенного трафика в сети ViPNet

Трафик маршрутизируется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями ViPNet.

Сервер соединений

Сервер соединений позволяет:

- Установить соединение между узлами, когда они не могут связаться напрямую (если на границе сети установлено стороннее устройство, выполняющее фильтрацию и трансляцию трафика). В таком случае соединение устанавливается через координатор, выполняющий функцию сервера соединений.

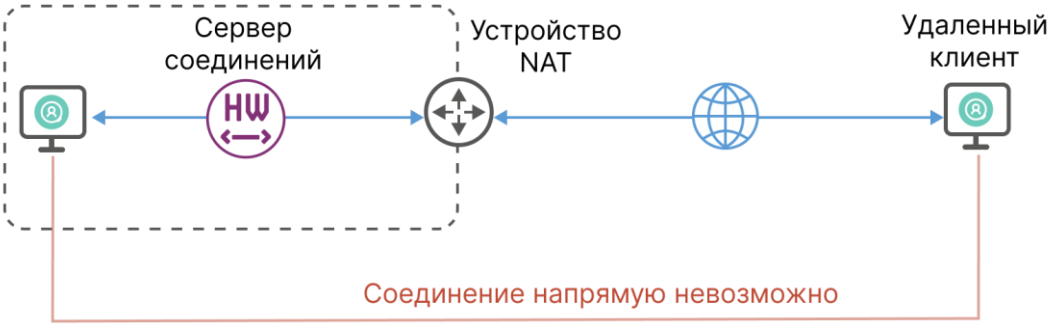


Рисунок 3. Организация соединений между сетевыми узлами ViPNet

- Установить TCP-туннель при блокировке протокола UDP.

  Когда удаленный клиент не может получить доступ к сети ViPNet по протоколу UDP (интернет-провайдер блокирует протокол 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.

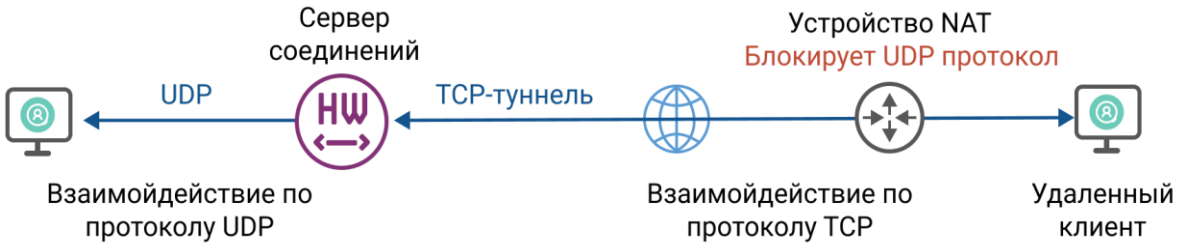


Рисунок 4. Доступ удаленного клиента к сети ViPNet через TCP-туннель

Для каждого сетевого узла (клиента и координатора) можно назначить свой сервер соединений. По умолчанию сервером соединений для клиента служит координатор, выполняющий функцию сервера IP-адресов.

VPN-шлюз

Координатор защищает соединения между узлами сети, которые обмениваются информацией через публичные сети. Для защиты соединения используется туннелирование. Координатор туннелирует узлы на сетевом (L3) или канальном (L2) уровнях модели OSI.

Туннелирование на сетевом уровне

Туннелирование на сетевом уровне позволяет организовать защищенное соединение между открытым и защищенным узлом или между двумя открытыми узлами, которые туннелируются разными координаторами. Выполняется следующим образом:

1. IP-пакеты от открытых узлов поступают на координатор и обрабатываются сетевыми фильтрами.
2. Обработанные IP-пакеты зашифровываются и инкапсулируются в новые IP-пакеты, после чего передаются:
   - На защищенные узлы назначения.
   - На другой координатор для открытых узлов назначения.
3. На другом координаторе из зашифрованных IP-пакетов извлекаются исходные IP-пакеты, расшифровываются, обрабатываются сетевыми фильтрами и передаются на открытые узлы назначения.

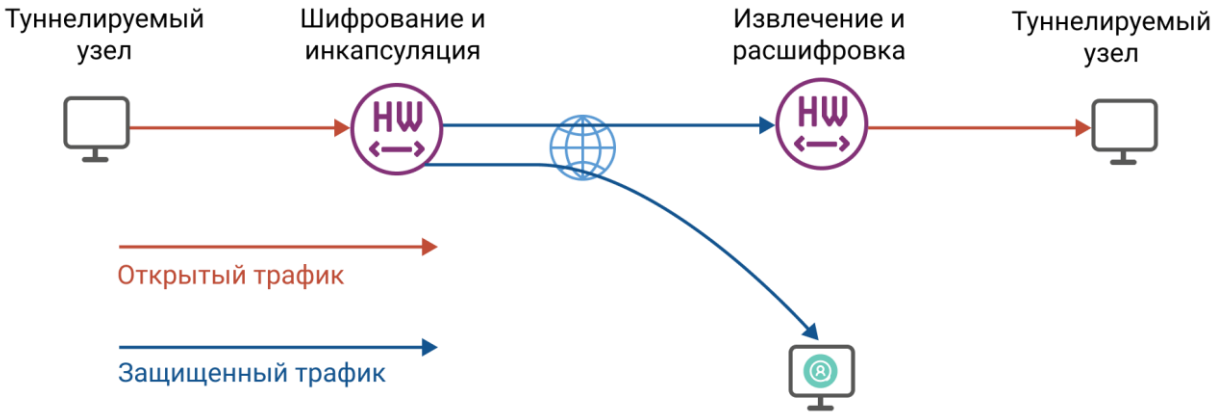


Рисунок 5. Защита соединения на сетевом уровне модели OSI

Туннелирование на канальном уровне (L2OverIP)

Туннелирование на канальном уровне, или L2OverIP, позволяет организовать защищенное соединение между узлами удаленных друг от друга сегментов сети так, что они находятся в одном широковещательном домене. На узлах сегментов сети, связанных через L2OverIP, используется адресное пространство в пределах одной IP-подсети. Выполняется следующим образом:

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

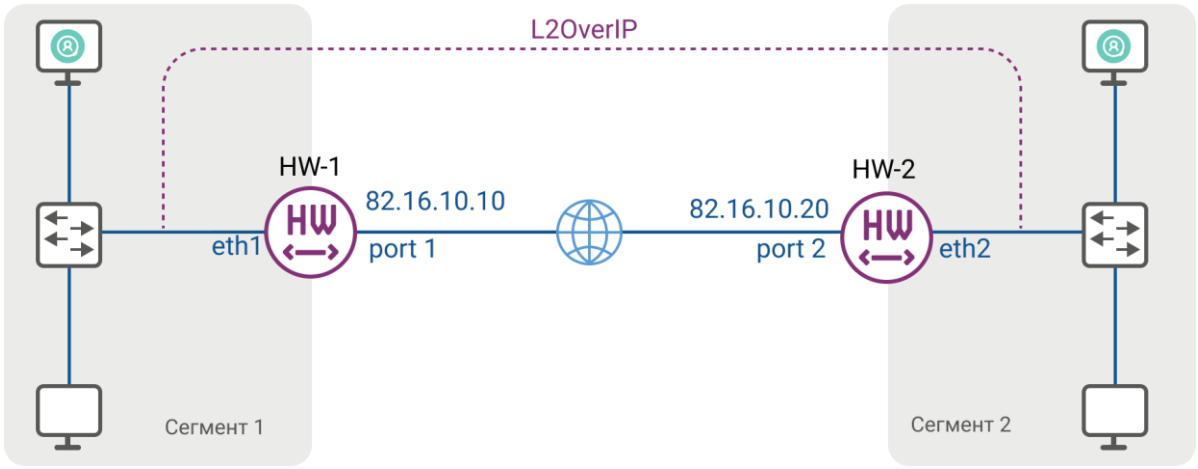


Рисунок 6. Защита соединения на канальном уровне модели OSI

Транспортный сервер MFTP

Защищенные сетевые узлы, поддерживающие работу с дистрибутивом ключей `dst`, обмениваются транспортными конвертами MFTP, в которых содержатся:

- управляющие сообщения;
- обновления программного обеспечения, справочников и ключей из системы управления;
- сообщения служб и приложений.

Транспортный сервер MFTP принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения.

При поступлении прикладного или управляющего конверта транспортный сервер MFTP в соответствии с маршрутными таблицами определяет дальнейший путь передачи этого конверта. Получив конверт, транспортный сервер выполняет одно из действий, в зависимости от заданных параметров:

- Устанавливает соединение с защищенным 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.

Функцию транспортного сервера MFTP выполняет координатор, на котором зарегистрирован клиент. Транспортный сервер изменить нельзя.

Защищенный интернет-шлюз

Защищенный интернет-шлюз позволяет разделить доступ защищенных узлов в интернет и к корпоративным ресурсам сети ViPNet.

Клиенты, связанные с защищенным интернет-шлюзом, могут работать в одном из двух режимов:

- Работа в интернете. Корпоративные ресурсы недоступны.
- Работа в корпоративной сети. Доступ в интернет заблокирован.

Такое разделение обеспечивает доступ в интернет с максимальным уровнем безопасности, возможным без физического отключения компьютера от корпоративной сети.

Межсетевой экран

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. Также межсетевой экран защищает от одной из распространенных сетевых атак — спуфинга.

ViPNet Coordinator HW может осуществлять трансляцию сетевых адресов (NAT) для проходящего через него открытого трафика.

Примечание. Трансляция сетевых адресов для защищенного трафика выполняется автоматически (см. Маршрутизатор VPN-пакетов).

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

- Подключение локальной сети к интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг интернета количество публичных IP-адресов. В этом случае используется трансляция адреса источника, которая позволяет компьютерам с частными IP-адресами получать доступ к интернету от имени публичного IP-адреса координатора.
- Организация доступа к локальным ресурсам из внешней сети. В этом случае используется трансляция адреса назначения, которая позволяет узлам локальной сети, имеющим частные IP-адреса, быть доступными пользователям интернета по публичным IP-адресам.

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

Для поддержки пользовательских сетевых сервисов, например IP-телефонии, координатор выполняет обработку прикладных протоколов: FTP, DNS, H.323, SCCP, SIP.

Дополнительные функции ViPNet Coordinator HW

- Работа с виртуальными локальными сетями VLAN IEEE 802.1Q.
- Агрегирование сетевых интерфейсов IEEE 802.3ad.
- Доступ к мобильным и беспроводным сетям (для HW50 N2/N3, HW100 N2/N3).
- Статическая и динамическая (DHCP/PPP, OSPFv2) маршрутизация IP-трафика.
- Распределение нагрузки между каналами связи и резервирование каналов связи.
- Встроенные DHCP-, DNS- и NTP-серверы.
- Встроенный прокси-сервер с фильтрацией HTTP-трафика по его содержимому и антивирусной проверкой (через протокол ICAP).
- Система защиты от сбоев для контроля собственной работоспособности и создания кластера горячего резервирования на базе двух ViPNet Coordinator HW.
- Взаимодействие с ИБП (аппаратные исполнения).

Обработка сетевого трафика в соответствии с приоритетом

В ViPNet Coordinator HW реализована поддержка протокола классификации сетевого трафика DiffServ. Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена DSCP-метка, задающая приоритет обработки пакета.

Когда на ViPNet Coordinator HW 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 зашифровании и расшифровании (инкапсуляции 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 HW приходит открытый IP-пакет с DSCP-меткой, ViPNet Coordinator HW его зашифровывает и отправляет далее получателю. По пути следования IP-пакета его DSCP-метка может быть снята или изменена и останется такой после расшифрования.

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

Совместимое программное обеспечение

- ViPNet Prime:
  - для ViPNet Coordinator HW10 — версии 1.9.5,
  - для остальных — версии 1.7.2 и выше;
- ViPNet Administrator 4.6.9 и выше;
- ViPNet Client 4U 4.14 и выше;
- ViPNet Client for Windows 4.5.5 и выше.

2

Описание исполнений

ViPNet Coordinator HW10

Исполнение ViPNet Coordinator HW10 обладает небольшой производительностью, может быть использовано для защиты малых офисов. Исполнение ViPNet Coordinator HW10 поставляется на аппаратной платформе HW10 F1.

Таблица 1. Характеристики платформы HW10 F1

Характеристика	HW10 F1
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	94,5x30x68 мм
Масса	0,3 кг
Питание	Внешний блок питания, 220 В
Номинальная мощность	15 Вт
Порты Ethernet RJ-45	1 x 1 Гбит/с 2 x 2,5 Гбит/с
Порты ввода-вывода	HDMI 2 x USB 3.0

На передней панели HW10 F1 расположены сетевые порты Ethernet и порт HDMI. На задней панели HW10 F1 находятся два порта USB 3.0.

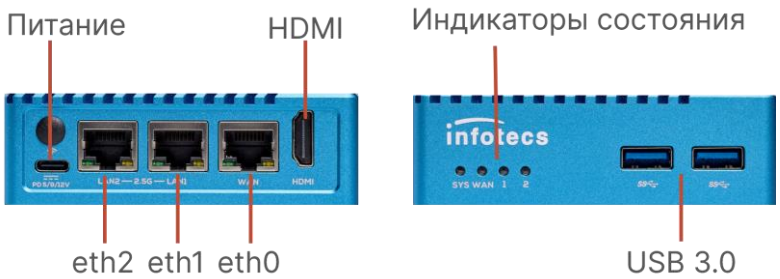


Рисунок 7. Передняя и задняя панели HW10 F1

Внимание! В связи с особенностями аппаратной платформы при каждой перезагрузке устройства на интерфейсе `eth2` генерируется случайный MAC-адрес. Учитывайте это при подключении сетевых устройств.

ViPNet Coordinator HW50

Исполнения ViPNet Coordinator HW50 имеют компактные размеры и небольшой вес, и поэтому их использование оправдано в местах, где физическое пространство ограничено. ViPNet Coordinator HW данного исполнения могут быть использованы для защиты небольших удаленных офисов и удаленных рабочих мест.

Аппаратные платформы HW50 представляют собой мини-компьютеры с низким уровнем тепловыделения и энергопотребления.

Аппаратные платформы HW50 N1, N2, N3, N4

Таблица 2. Характеристики платформ HW50 N1, N2, N3, N4

Характеристика	**HW50 N1, N2, N3**	**HW50 N4**
Форм-фактор	Мини-компьютер	Мини-компьютер
Размеры корпуса (ШхВхГ)	125,1x22,5x122 мм	137x22,5x122 мм
Масса	0,5 кг	0,5 кг
Питание	Внешний блок питания, 220 В	Внешний блок питания, 220 В
Номинальная мощность	36 Вт	36 Вт
Источник постоянного тока	12 В, 3 А	12 В, 3 А
Порты Ethernet RJ-45	3 x 1 Гбит/с	3 x 1 Гбит/с
3G-модем	Только в HW50 N3	нет
Адаптер Wi-Fi	Только в HW50 N2	нет
Порты ввода-вывода	HDMI Консольный порт (RJ-45) USB 2.0 USB 3.0	HDMI Консольный порт (RJ-45) USB 2.0 USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Для HW50 N2 — внешняя антенна Wi-Fi Для HW50 N3 — внешняя антенна 3G	

На передней панели аппаратных платформ HW50 расположены порты USB 2.0 и HDMI, а также консольный порт, предназначенный для подключения компьютера (ноутбука) при установке справочников и ключей.

Рисунок 8. Передняя панель HW50 N1, N2, N3, N4

Остальные коммуникационные разъемы находятся на задней панели:

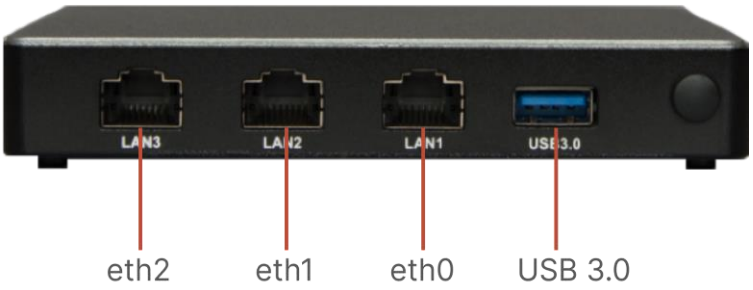


Рисунок 9. Задняя панель HW50 N1, N2, N3, N4

Примечание. Чтобы вставить SIM-карту оператора связи во встроенный модем аппаратной платформы HW50 N3, необходимо разобрать корпус мини-компьютера (см. Установка SIM-карты в HW50 N3 и HW100 N3).

Аппаратная платформа HW50 A1

Таблица 3. Характеристики платформы HW50 A1

Характеристика	HW50 A1
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	136x28x130 мм
Масса	1 кг
Питание	Внешний блок питания, 220 В
Номинальная мощность	36 Вт
Порты Ethernet RJ-45	3 x 1 Гбит/с
Порты ввода-вывода	HDMI

Характеристика	HW50 A1
	Консольный порт (RJ-45)
	USB 2.0
	USB 3.0

На передней панели HW50 A1 расположены сетевые порты Ethernet, USB-порты и индикаторы состояния.

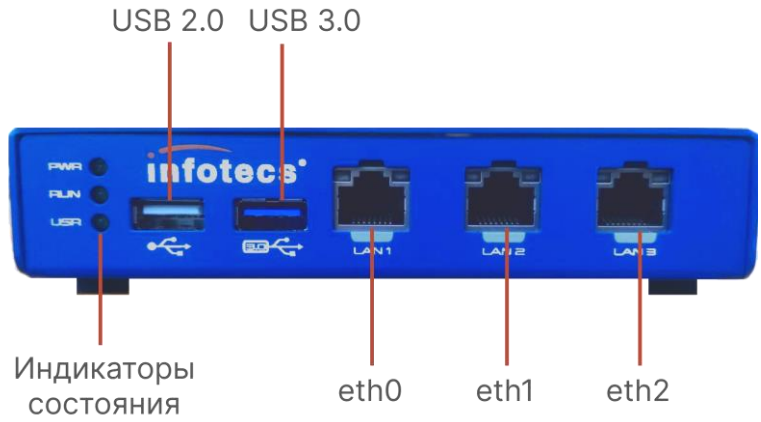


Рисунок 10. Передняя панель HW50 A1

Остальные разъемы находятся на задней панели.

Рисунок 11. Задняя панель HW50 A1

ViPNet Coordinator HW100

Исполнения ViPNet Coordinator HW100 имеют компактные размеры и небольшой вес, и поэтому их использование оправдано в местах, где физическое пространство ограничено. ViPNet Coordinator HW данных исполнений может быть использован для защиты филиалов компаний и небольших удаленных офисов.

Аппаратные платформы HW100 N1, N2, N3

Таблица 4. Характеристики платформ HW100 N1, N2, N3

Характеристика	**HW100 N1, N2, N3**
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	173,8x42x142,2 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Номинальная мощность	60 Вт
Источник постоянного тока	24 В, 2,5 А
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP	1 x 1 Гбит/с
3G-модем	Только в HW100 N3
Адаптер Wi-Fi	Только в HW100 N2
Порты ввода-вывода	VGA Консольный порт (RJ-45) USB 2.0 USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Консольный кабель COM-RJ-45 Для HW100 N2 — внешняя антенна Wi-Fi Для HW100 N3 — внешняя антенна 3G

Все коммуникационные разъемы расположены на передней панели компьютера. На конкретном устройстве расположение разъемов может немного отличаться от представленного на рисунке ниже.

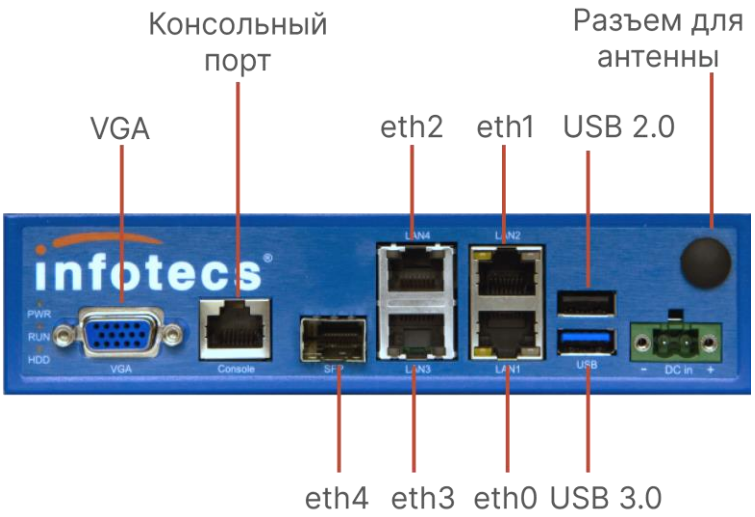


Рисунок 12. Передняя панель HW100 N1, N2, N3

Аппаратные платформы HW100 Q1, Q2

Таблица 5. Характеристики HW100 Q1, Q2

Характеристика	**HW100 Q1, Q2**
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	250 x 44 x 227,6 мм
Масса	1,9 кг
Питание	Внешний блок питания, 12 В
Номинальная мощность	60 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP	2 x 1 Гбит/с
Порты ввода-вывода	VGA Консольный порт (RJ-45) 2 x USB 3.0

Все коммуникационные разъемы расположены на передней панели HW100 Q1, Q2.

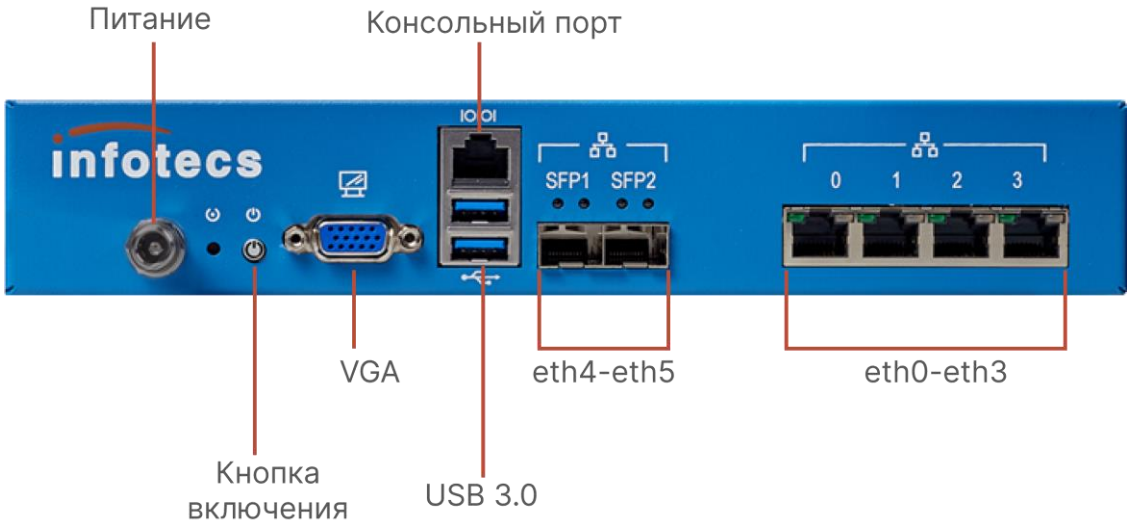


Рисунок 13. Передняя панель HW100 Q1, Q2

ViPNet Coordinator HW1000

Исполнения ViPNet Coordinator HW1000 устанавливаются в телекоммуникационную стойку 19" и могут быть использованы для защиты компьютерных сетей масштаба предприятия.

Аппаратные платформы HW1000 Q4, Q5, Q6

Таблица 6. Характеристики HW1000 Q4, Q5, Q6

Характеристика	HW1000 Q4	HW1000 Q5	HW1000 Q6
Форм-фактор	19" Rack 1U	19" Rack 1U	19" Rack 1U
Размеры корпуса (ШхВхГ)	430x44x380 мм	430x44x380 мм	430x44x380 мм
Масса	7,2 кг	7,2 кг	7,2 кг
Питание	Блок питания, 100–240 В	Блок питания, 100–240 В	Блок питания, 100–240 В
Номинальная мощность	250 Вт	250 Вт	250 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с	6 x 1 Гбит/с	4 x 1 Гбит/с
Порты Ethernet SFP+	нет	нет	2 x 1 Гбит/с
Порты ввода-вывода	2 x VGA PS/2 для подключения клавиатуры или мыши RS-232 4 x USB 2.0 2 x USB 3.0	2 x VGA PS/2 для подключения клавиатуры или мыши RS-232 4 x USB 2.0 2 x USB 3.0	2 x VGA PS/2 для подключения клавиатуры или мыши RS-232 4 x USB 2.0 2 x USB 3.0

На передней панели HW1000 Q4, Q5, Q6 расположены RS-232, два порта USB 2.0 и VGA.

Рисунок 14. Передняя панель HW1000 Q4, Q5, Q6

Остальные коммуникационные разъемы находятся на задней панели.

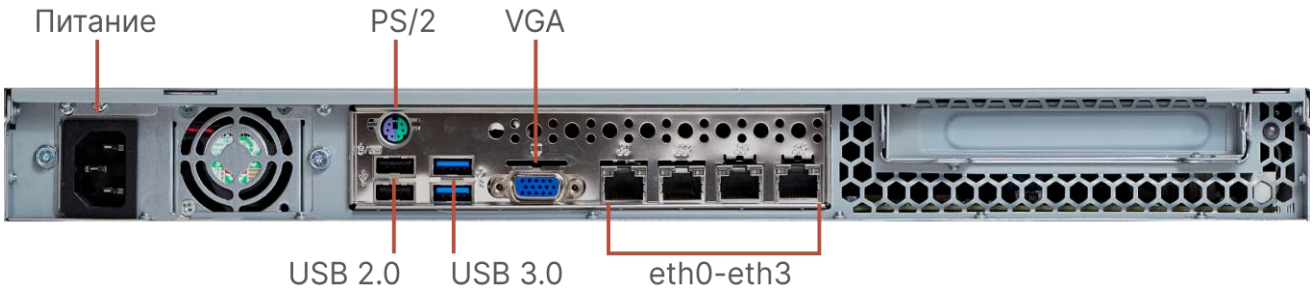


Рисунок 15. Задняя панель HW1000 Q4

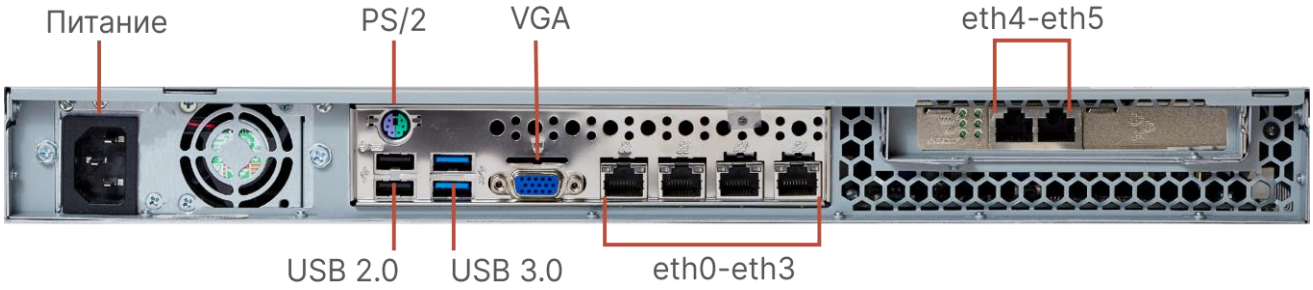


Рисунок 16. Задняя панель HW1000 Q5

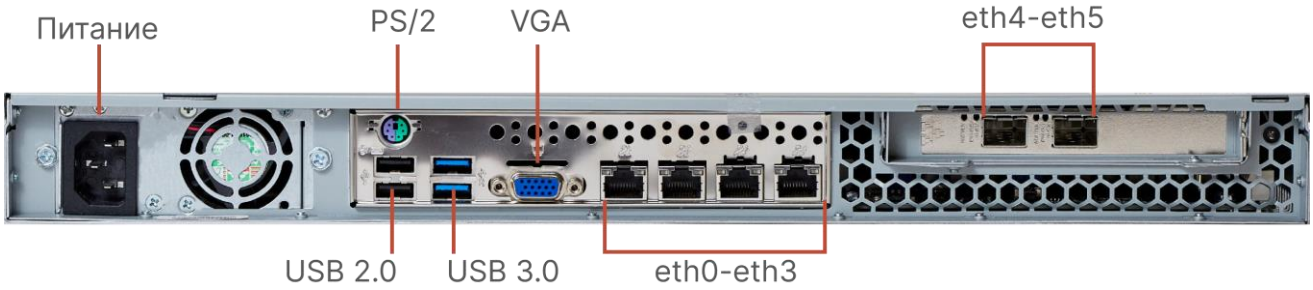


Рисунок 17. Задняя панель HW1000 Q6

Аппаратные платформы HW1000 Q7, Q8, Q9

Таблица 7. Характеристики HW1000 Q7, Q8, Q9

Характеристика	HW1000 Q7	HW1000 Q8	HW1000 Q9
Форм-фактор	19″ Rack 1U	19″ Rack 1U	19″ Rack 1U
Размеры корпуса (ШхВхГ)	430x44 x453 мм	430x44x453 мм	430x44x476 мм
Масса	6,8 кг	6,8 кг	7,8 кг
Питание	Блок питания, 100–240 В	Блок питания, 100–240 В	2 блока питания, 100–240 В
Номинальная мощность	250 Вт	250 Вт	2 x 300 Вт
Порты Ethernet RJ-45	6 x 1 Гбит/с	8 x 1 Гбит/с	8 x 1 Гбит/с

Характеристика	HW1000 Q7	HW1000 Q8	HW1000 Q9
Порты Ethernet SFP+	нет	нет	4 x 1 Гбит/с
Порты ввода-вывода	VGA RS-232 6 x USB 3.1	VGA RS-232 6 x USB 3.1	VGA RS-232 6 x USB 3.1
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку	2 кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

На передней панели HW1000 Q7 и HW1000 Q8 расположены: сетевые порты Ethernet, RS-232, порты USB 3.1 и VGA.

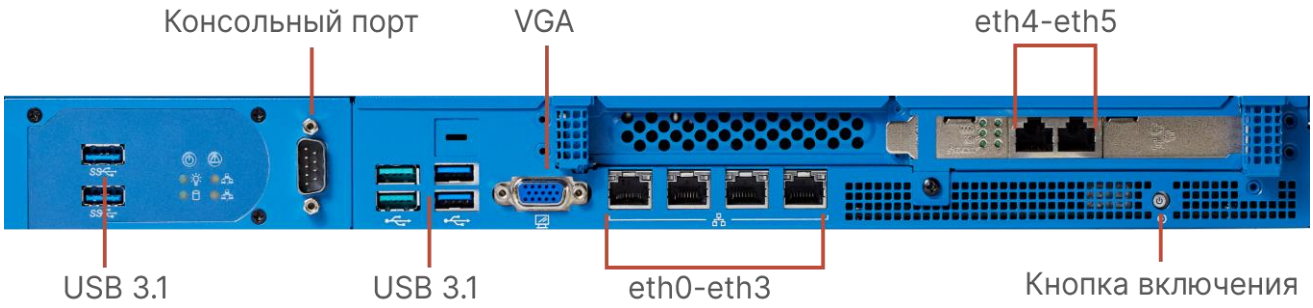


Рисунок 18. Передняя панель HW1000 Q7

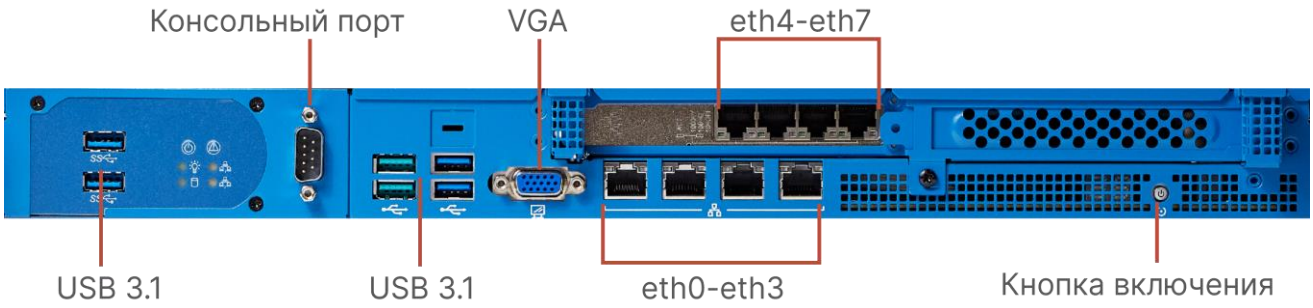


Рисунок 19. Передняя панель HW1000 Q8

На задней панели HW1000 Q7, Q8 находится разъем блока питания.

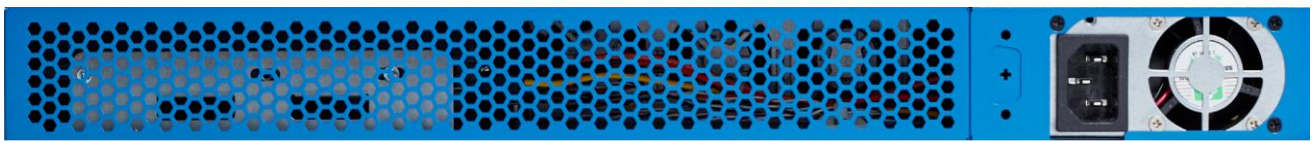


Рисунок 20. Задняя панель HW1000 Q7, Q8

На передней панели HW1000 Q9 расположены: сетевые порты Ethernet (`eth0` - `eth7`) и Ethernet SFP (`eth8` - `eth11`), RS-232, порты USB 3.1 и VGA.

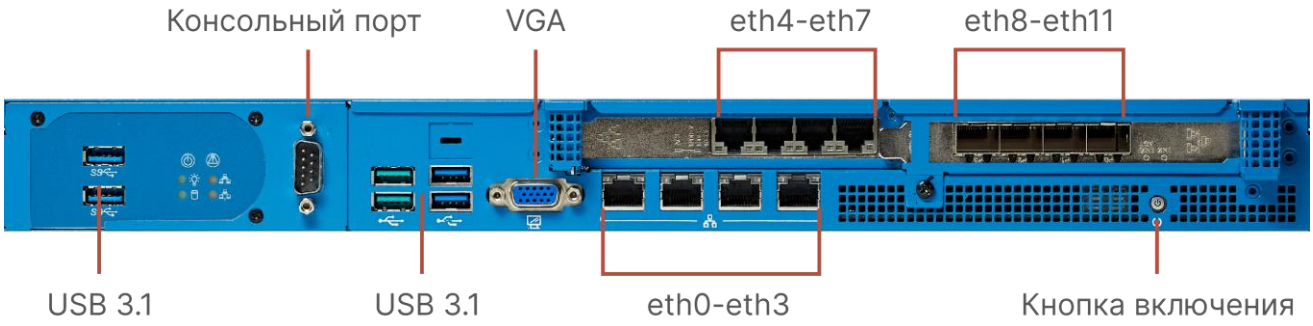


Рисунок 21. Передняя панель HW1000 Q9

На задней панели HW1000 Q9 расположены разъемы блоков питания.

Рисунок 22. Задняя панель HW1000 Q9

Аппаратная платформа HW1000 Q10

Таблица 8. Характеристики HW1000 Q10

Характеристика	HW1000 Q10
Форм-фактор	19” Rack 1U
Размеры корпуса (ШхВхГ)	428x44x466 мм
Масса	7,2 кг
Питание	Блок питания, 220В
Номинальная мощность	250 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP	2 x 1 Гбит/с
Порты ввода-вывода	VGA 2 x USB 3.0 Консольный порт (RJ-45)

На передней панели HW1000 Q10 расположены: сетевые порты Ethernet (`eth0` - `eth3`) и Ethernet SFP (`eth4` - `eth5`), VGA, порты USB 3.0.

Внимание! Не используйте разъём питания на передней панели. Это может привести к неработоспособности ViPNet Coordinator HW.

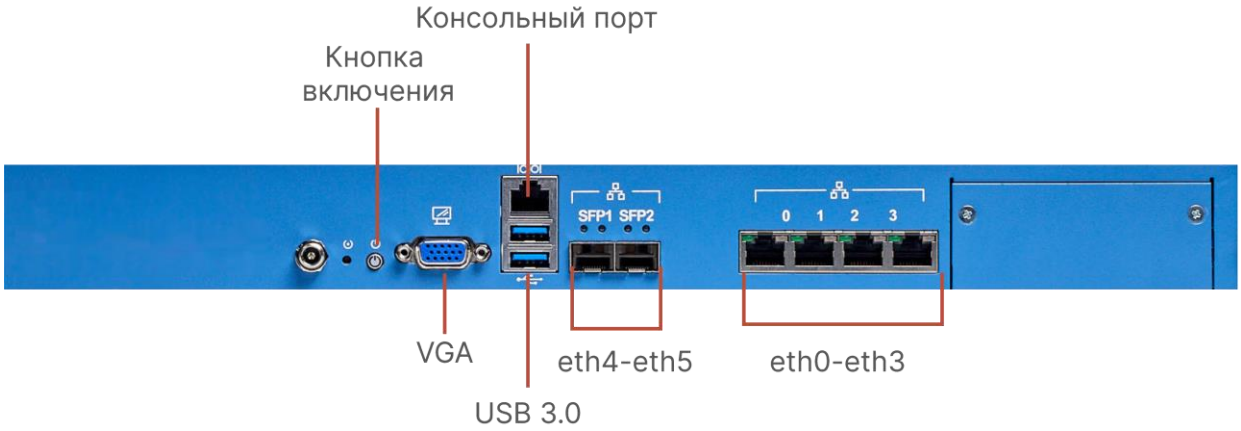


Рисунок 23. Передняя панель HW1000 Q10

Рисунок 24. Задняя панель HW1000 Q10

ViPNet Coordinator HW2000

Исполнение ViPNet Coordinator HW2000 устанавливается в телекоммуникационную стойку 19”. Благодаря использованию серверов с производительными процессорами и высокоскоростных сетевых адаптеров, исполнение ViPNet Coordinator HW2000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных и к облачным ресурсам.

Аппаратная платформа HW2000 Q4

Таблица 9. Характеристики HW2000 Q4

Характеристика	HW2000 Q4
Форм-фактор	1U в укороченном корпусе
Размеры корпуса (ШхВхГ)	444x44x380 мм
Масса	8 кг
Питание	Блок питания, 100-127 В/200-240 В
Номинальная мощность	500 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши RS-232 2 x USB 3.0

На задней панели HW2000 Q4 расположен RS-232. Остальные коммуникационные разъемы находятся на передней панели.

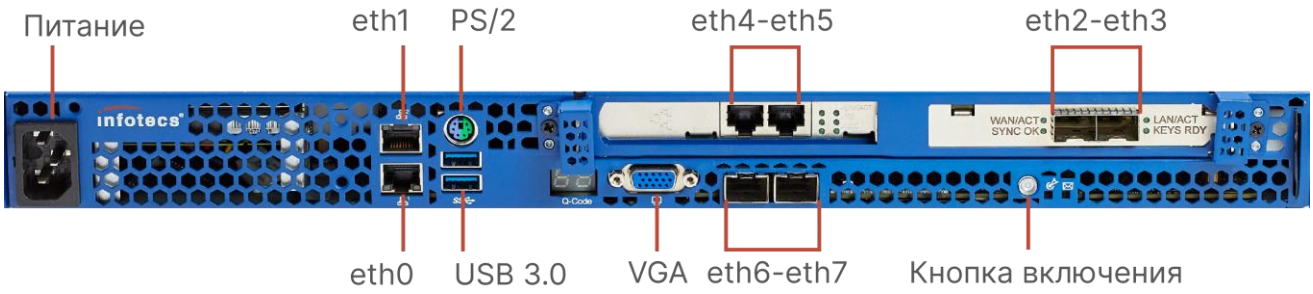


Рисунок 25. Передняя панель HW2000 Q4

Аппаратная платформа HW2000 Q5

Таблица 10. Характеристики аппаратной платформы HW2000 Q5

Характеристики	HW2000 Q5
Форм-фактор	1U
Размеры корпуса (ШхВхГ)	430x44x476 мм
Масса	8 кг
Питание	2 блока питания с «горячей» заменой
Номинальная мощность	2 x 300 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA RS-232 6 x USB 3.1
Дополнительное оборудование	2 кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

На передней панели HW2000 Q5 находятся: сетевые порты Ethernet (`eth0 - eth3`), Ethernet SFP (`eth4 - eth7`) и Ethernet SFP+ (`eth8 - eth11`), порты USB 3.1, VGA и RS-232.

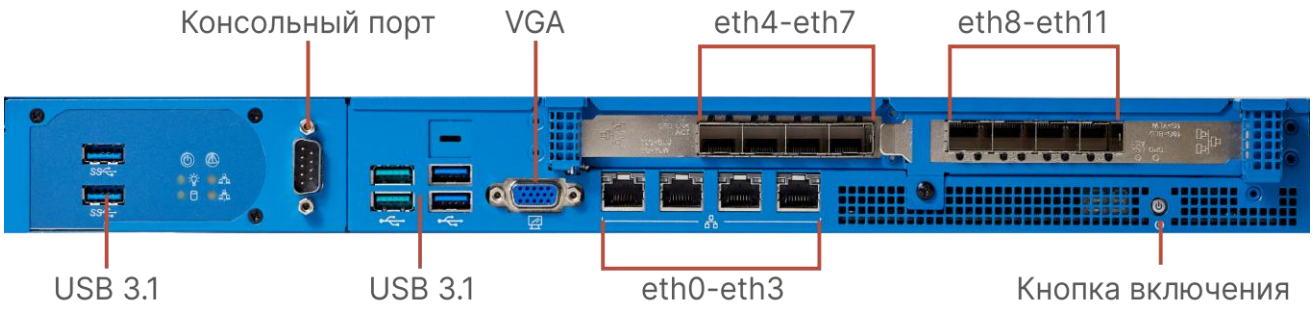


Рисунок 26. Передняя панель HW2000 Q5

На задней панели HW2000 Q5 расположены разъемы блоков питания.

Рисунок 27. Задняя панель HW2000 Q5

ViPNet Coordinator HW5000

Исполнение ViPNet Coordinator HW5000 устанавливается в телекоммуникационную стойку 19”. Благодаря использованию серверов с многоядерными процессорами и высокоскоростных сетевых адаптеров, исполнение ViPNet Coordinator HW5000 подходит для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных и к облачным ресурсам.

Аппаратная платформа HW5000 Q1

Таблица 11. Характеристики HW5000 Q1

Характеристика	HW5000 Q1
Форм-фактор	19” Rack 1U (в укороченном корпусе)
Размеры корпуса (ШхВхГ)	444x44x380 мм
Масса	8 кг
Питание	Блок питания, 100-127 В/200-240 В
Номинальная мощность	500 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши 2 x USB 3.0 RS-232
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

На передней панели HW5000 Q1 находятся: сетевые порты Ethernet (`eth0`, `eth1`, `eth4`, `eth5`) и Ethernet SFP+ (`eth2`, `eth3`, `eth6`, `eth7`), порты PS/2, USB 3.0, VGA и дублирующий разъем блока питания.

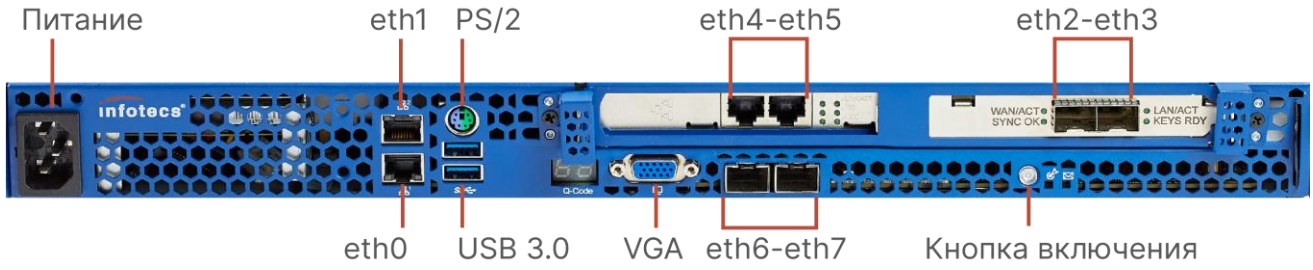


Рисунок 28. Передняя панель HW5000 Q1

На задней панели HW5000 Q1 расположены RS-232 и разъем блока питания.

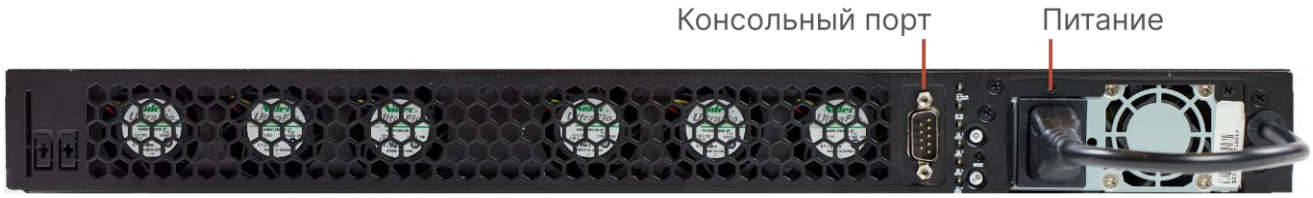


Рисунок 29. Задняя панель HW5000 Q1

Аппаратная платформа HW5000 Q2

Таблица 12. Характеристики аппаратной платформы HW5000 Q2

Характеристики	HW5000 Q2
Форм-фактор	1U
Размеры корпуса (ШхВхГ)	430x44x476 мм
Масса	8 кг
Питание	2 блока питания с «горячей» заменой
Номинальная мощность	2 x 300 Вт
Порты Ethernet RJ-45	4 x 1 Гбит/с
Порты Ethernet SFP+	8 x 10 Гбит/с
Порты ввода-вывода	VGA RS-232 6 x USB 3.1
Дополнительное оборудование	2 кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

На передней панели HW5000 Q2 расположены: сетевые порты Ethernet (`eth0` - `eth3`) и Ethernet SFP+ (`eth4` - `eth11`), порты USB 3.1, VGA и RS-232.

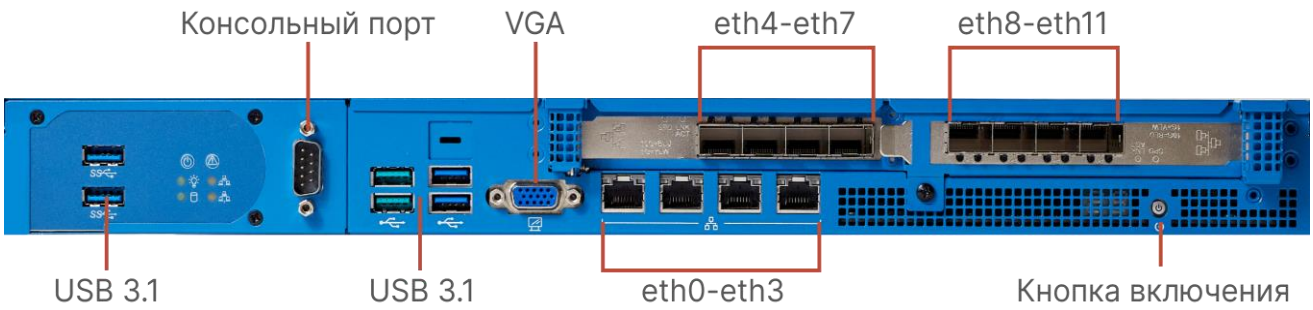


Рисунок 30. Передняя панель HW5000 Q2

На задней панели HW5000 Q2 расположены разъемы блоков питания.

Рисунок 31. Задняя панель HW5000 Q2

ViPNet Coordinator VA

ViPNet Coordinator VA — виртуализированное программное обеспечение, которое предназначено для развертывания на платформе виртуализации.

Поддерживаемые платформы виртуализации

ViPNet Coordinator VA поставляется в виде образа виртуальной машины, который можно установить на платформы виртуализации:

- KVM (Kernel-based Virtual Machine), например Qemu-KVM или Proxmox.
- VMware vSphere 6.7, 7.0.
- VMware Workstation Pro 15.x, 16.x.
- Microsoft Hyper-V Server 2019.
- Oracle VM Server 3.4.
- Oracle VM VirtualBox 6.x.

Работа на других платформах виртуализации не гарантируется.

Параметры виртуальной машины

Таблица 13. Минимальные параметры виртуальной машины ViPNet Coordinator VA

Название роли	Накопители	Количество сетевых интерфейсов	Количество ядер процессора	Оперативная память (Гбайт)
ViPNet Coordinator VA100 ViPNet Coordinator VA500	2 диска, 4 и 80 Гбайт	1	2	2
ViPNet Coordinator VA1000	2 диска, 4 и 80 Гбайт	1	4	4
ViPNet Coordinator VA2000	2 диска, 4 и 80 Гбайт	1	8	8

Примечание. Рекомендуем использовать не менее двух сетевых интерфейсов. Если сетевых интерфейсов меньше, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники с помощью компьютера по протоколу TFTP.

Дополнительные настройки:

- Если на ViPNet Coordinator VA предполагается регистрация более 1000 ViPNet-клиентов, в настройках виртуальной машины укажите тип диска виртуальной машины **Фиксированный жесткий диск (Thick Provision)**.
- Если на ViPNet Coordinator VA планируется использование агрегированного сетевого интерфейса, настройте его на платформе виртуализации.
- Для уменьшения расходов на виртуализацию сопоставьте сетевому интерфейсу ViPNet Coordinator VA физический сетевой адаптер средствами платформы виртуализации. Для максимальной производительности используйте функции SR-IOV или DirectPath с сетевыми картами поддерживающими разделение RSS (при их наличии).

3

Лицензирование и функциональные ограничения

Лицензирование

Функции ViPNet Coordinator HW в сети ViPNet и возможности по обработке трафика определяются ролью (лицензией), которая назначается сетевом узлу в управляющем ПО (ViPNet Administrator или ViPNet Prime).

При выпуске лицензии на сеть ViPNet указывается максимальная версия продуктов ViPNet. Максимальная версия для ViPNet Coordinator HW должна быть не менее 4.7. Проверьте в управляющем ПО, что лицензия на вашу сеть ViPNet соответствует этому требованию. Если в ViPNet ЦУС не указана максимальная версия для ViPNet Coordinator HW, то она совпадает с максимальной версией ViPNet Administrator.

Соответствие исполнения назначенной роли (лицензии) проверяется при установке на ViPNet Coordinator HW дистрибутива ключей.

Аппаратные исполнения

Таблица 14. Роли (лицензии) исполнений ViPNet Coordinator HW в ViPNet ЦУС (ViPNet Prime)

Исполнение	Аппаратные платформы	Роль (лицензия)	Роль для использования в кластере
HW10	HW10 F1	Coordinator HW10	-
HW50 A	HW50 N1, N2, N3, N4, A1	Coordinator HW50 A, Coordinator HW50 AU	Failover100
HW50 B	HW50 N1, N2, N3, N4, A1	Coordinator HW50 B	Failover100
HW 100 C	HW100 N1, N2, N3, Q1, Q2	Coordinator HW100 C Coordinator HW100 CU	Failover100
HW1000	HW1000 Q4, Q7, Q10	Coordinator HW1000	Не требуется
HW1000 C	HW1000 Q5, Q8	Coordinator HW1000 C	Не требуется
HW1000 D	HW1000 Q6, Q9	Coordinator HW1000 D	Не требуется
HW2000	HW2000 Q4, Q5	Coordinator HW2000	Не требуется
HW5000	HW5000 Q1, Q2	Coordinator HW5000	Не требуется

В кластере горячего резервирования вы можете использовать только одинаковые аппаратные платформы. Например, вы можете использовать в кластере два ViPNet Coordinator HW на аппаратной платформе HW1000 Q5 или два ViPNet Coordinator HW на аппаратной платформе HW1000 Q8.

Виртуализированное исполнение

Таблица 15. Роли (лицензии) исполнения ViPNet Coordinator VA

Роль (лицензия)	Роль для использования в кластере
Coordinator VA100	Failover100
Coordinator VA500	Failover500
Coordinator VA1000	Failover1000
Coordinator VA2000	Failover2000

В кластере горячего резервирования вы можете использовать ViPNet Coordinator VA только с одинаковой ролью.

Функциональные ограничения

Поддержка функций транспортного сервера и туннелирования

Таблица 16. Лицензионные ограничения, накладываемые ролью (лицензией)

Роль (лицензия)	Транспортный сервер	Макс. число туннелируемых соединений на сетевом уровне (ЦУС)	Туннелирование на канальном уровне
Coordinator HW10	Нет	65535	Нет
Coordinator HW50 A	Нет	2	Нет
Coordinator HW50 B	Нет	5	Нет
Coordinator HW50 AU	Нет	65535	Нет
Coordinator HW100 C	Да	10	Да
Coordinator HW100 CU	Да	65535	Да
Coordinator HW1000	Да	65535	Да
Coordinator HW1000 C	Да	65535	Да
Coordinator HW1000 D	Да	65535	Да
Coordinator HW2000	Да	65535	Да
Coordinator HW5000	Да	65535	Да
Coordinator VA100	Да	65535	Да
Coordinator VA500	Да	65535	Да
Coordinator VA1000	Да	65535	Да
Coordinator VA2000	Да	65535	Да

В исполнениях ViPNet Coordinator HW10, HW50 A, B не поддерживаются функции шлюзового координатора и транспортного сервера. Поэтому возникают ограничения при формировании структуры сети ViPNet:

- Координатор нельзя регистрировать в качестве шлюзового в другие сети ViPNet. Иначе его работоспособность может быть нарушена.
- За координатором нельзя регистрировать ViPNet-клиентов. В данном случае он может использоваться для туннелирования открытого IP-трафика.

Количество сетевых интерфейсов

- `eth` — по количеству физических интерфейсов Ethernet.
- `wlan` — 1, если присутствует.

- `localhost` — 1.
- `bond` — 3, если созданы агрегированные интерфейсы.
- `vlan` и `alias` — в сумме с другими интерфейсами не превышает максимального количества интерфейсов для аппаратной платформы.

Максимальное количество сетевых интерфейсов:

- 32 — для аппаратных платформ HW10, HW50.
- 128 — для остальных платформ.

Количество связей с ViPNet-узлами

Таблица 17. Количество ViPNet-клиентов и связей ViPNet Coordinator HW

Исполнение / Роль	Рекомендованное число клиентов на координаторе	Макс. количество связей с ViPNet-узлами	Макс. количество связей с туннелирующими координаторами	Макс. количество заданных диапазонов туннелируемых узлов
ViPNet Coordinator HW10	0	500	50	1000
ViPNet Coordinator HW50 A, 50 B	0	500	50	1000
ViPNet Coordinator HW100 C	10	1000	50	1000
ViPNet Coordinator HW1000	500	5000	100	1000
ViPNet Coordinator HW1000 C, 1000 D	1000	10000	1000	1000
ViPNet Coordinator HW2000	5000	15000	5000	1000
ViPNet Coordinator HW5000	6000	15000	5000	1000
ViPNet Coordinator VA100	100	100	50	1000
ViPNet Coordinator VA500	500	500	250	1000
ViPNet Coordinator VA1000	1000	1000	500	1000
ViPNet Coordinator VA2000	2000	2000	1000	1000

Число соединений МСЭ

Таблица 18. Число соединений МСЭ

Аппаратная платформа	Значение по умолчанию	Макс. значение
HW10 F1	150 000	150 000

Аппаратная платформа	Значение по умолчанию	Макс. значение
HW50 (все платформы)	150 000	150 000
HW100 (все платформы)	150 000	150 000
HW1000 (все платформы)	800 000	1 000 000
HW2000 Q4	2 500 000	3 000 000
HW5000 Q1, Q2	6 000 000	6 500 000
VA100	150 000	150 000
VA500	400 000	500 000
VA1000	800 000	1 000 000
VA2000	2 500 000	3 000 000

4

Возможности управления

Способы управления

Управляющее ПО ViPNet

- ViPNet ЦУС или Prime. Удаленная настройка ViPNet Coordinator HW:
  - централизованное обновление ключей и программного обеспечения;
  - настройка адресов доступа к ViPNet Coordinator HW;
  - настройка туннелируемых узлов;
  - настройка параметров подключения ViPNet Coordinator HW к внешней сети.
- ViPNet Policy Manager или ViPNet Prime Policy Management. Формирование политик безопасности и их рассылка на узлы по сети ViPNet. Политики безопасности могут включать в себя сетевые фильтры и правила трансляции IP-адресов. Фильтры и правила трансляции, полученные из ViPNet Policy Manager (ViPNet Prime Policy Management), недоступны для редактирования на узлах. Подробнее о политиках безопасности см. в документах «ViPNet Policy Manager. Руководство администратора» или «ViPNet Prime Policy Management. Руководство администратора».

Веб-интерфейс ViPNet Coordinator HW

В веб-интерфейсе вы можете:

- Настроить дату и время.
- Настроить подключение ViPNet Coordinator HW к сети, сетевые интерфейсы.
- Управлять сетевыми фильтрами и правилами трансляции адресов.
- Управлять туннелированием адресов.
- Настроить обработку прикладных протоколов.
- Настроить сетевые службы: встроенный DHCP-, DNS-, NTP- и прокси-сервер, DHCP-relay.
- Настроить L2OverIP, MultiWAN.
- Настроить статическую и динамическую маршрутизацию.
- Настроить удаленный мониторинг по протоколу SNMP.
- Следить за состоянием ViPNet Coordinator HW.
- Настроить видимость сетевых узлов.
- Перевыпустить самоподписанный сертификат для подключения к веб-интерфейсу.
- Сформировать запрос на выпуск серверного сертификата, загрузить серверный сертификат и списки аннулированных сертификатов.

- Посмотреть системный журнал, журнал регистрации IP-пакетов, транспортных конвертов, переключений режимов кластера (в режиме кластера).
- Настроить журнал регистрации IP-пакетов.
- Посмотреть список сетевых узлов ViPNet.

В веб-интерфейсе доступны не все настройки ViPNet Coordinator HW. Полный набор настроек есть только в командном интерпретаторе.

Командный интерпретатор ViPNet Coordinator HW

В дополнение к настройкам из веб-интерфейса в командном интерпретаторе доступны:

- Настройка режимов подключения ViPNet Coordinator HW к сети через межсетевой экран.
- Управление конфигурациями VPN.
- Настройка системы защиты от сбоев.
- Настройка транспортного сервера MFTP в транзитном режиме.
- Резервирование справочников, ключей и настроек ViPNet Coordinator HW, обновление ПО ViPNet Coordinator HW.
- Локальное обновление справочников и ключей.
- Настройка подключения к веб-интерфейсу ViPNet Coordinator HW по протоколу HTTP или HTTPS.

Подключение к ViPNet Coordinator HW

Локальное подключение

При локальном подключении доступно управление ViPNet Coordinator HW с помощью командного интерпретатора. Командный интерпретатор запускается автоматически после аутентификации.

Удаленное подключение

Удаленное подключение к ViPNet Coordinator HW доступно после установки справочников и ключей. Управление происходит через командный интерпретатор по протоколу SSH или через веб-интерфейс.

Подробное описание процесса подключения описано в документах «Настройка в веб-интерфейсе» и «Настройка с помощью командного интерпретатора».

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких узлов. Количество одновременных сессий зависит от исполнения ViPNet Coordinator HW:

- 5 — для всех исполнений HW10, HW50, HW100 и ViPNet Coordinator VA.
- 30 — для остальных исполнений.

Только в одной удаленной сессии можно работать в режиме администратора.

Внимание! Не предоставляйте доступ к ViPNet Coordinator HW с незащищенных узлов. Для рабочего места администратора на ViPNet Coordinator HW настройте фильтры, которые разрешают только удаленное управление и передачу данных по служебным протоколам ViPNet.

Удаленное подключение по SSH

Для удаленного подключения вы можете использовать любой SSH-клиент с парольным типом аутентификации.

Подключение через веб-интерфейс

Вы можете подключиться к веб-интерфейсу ViPNet Coordinator HW с браузеров Microsoft Edge, Google Chrome или Firefox последних версий.

Чтобы подключение к ViPNet Coordinator HW через веб-интерфейс было безопасным:

- Подключайтесь с защищенного узла ViPNet. Между этим узлом и ViPNet Coordinator HW должна быть создана связь в управляющем ПО.
- Подключайтесь по протоколу HTTPS. Подключение происходит автоматически с помощью самоподписанного сертификата. Также вы можете установить на ViPNet Coordinator HW серверный сертификат, выданный УЦ.

Способы аутентификации пользователя

- «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.
- «Устройство». При аутентификации требуется ввести имя учетной записи, подключить устройство, на котором сохранен персональный ключ, и ввести ПИН доступа к устройству.

Особенности и ограничения

- Способ аутентификации «Устройство» применим только при локальном подключении к ViPNet Coordinator HW с помощью консоли. При подключении с помощью протокола SSH или веб-интерфейса применяется способ аутентификации «Пароль».
- При управлении с помощью ViPNet Prime возможен только один способ аутентификации — «Пароль».
- Платформы виртуализации Microsoft Hyper-V и Oracle VM Server не поддерживают подключение USB-устройств к виртуальной машине. Поэтому аутентификация с помощью устройства на этих платформах невозможна.
- Для аутентификации могут использоваться только внешние устройства Рутокен Lite производства компании «Актив».
- При управлении с помощью ViPNet ЦУС способ аутентификации можно изменить локально на ViPNet Coordinator HW. При этом изменить можно только способ аутентификации «Пароль» на «Устройство». Подробнее см. в документе «Настройка с помощью командного интерпретатора».
- При подключении через веб-интерфейс или удаленном подключении по SSH с защищенного узла аутентификация состоит из двух этапов:
    - Аутентификация в ПО ViPNet, которое установлено на удаленном рабочем месте для защиты канала передачи данных с ViPNet Coordinator HW.
    - Аутентификация при непосредственном подключении к ViPNet Coordinator HW через веб-интерфейс или по SSH.

5

Подготовка к работе

Установка SIM-карты в HW50 N3 и HW100 N3

1 Убедитесь, что ViPNet Coordinator HW выключен.

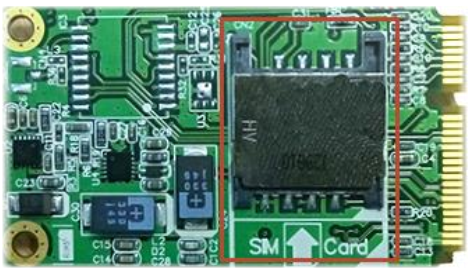
2 Открутите крепежные винты и разберите корпус ViPNet Coordinator HW.

3 На материнской плате найдите плату mini-PCIe, открутите крепежный винт и снимите ее.

Рисунок 32. Плата mini-PCIe

4 Установите SIM-карту в разъем:

- На HW50 разъем для SIM-карты находится на плате mini-PCIe.
- На HW100 N3 разъем для SIM-карты расположен на материнской плате под платой mini-PCIe.



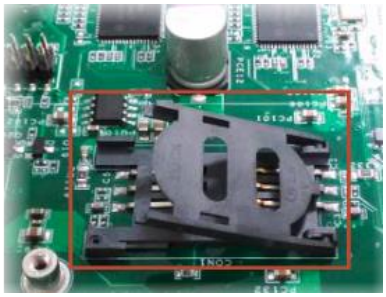


Рисунок 33. Разъемы для SIM-карты

5 Установите плату mini-PCIe в исходное положение и зафиксируйте ее крепежным винтом.

6 Соберите корпус ViPNet Coordinator HW.

«Горячая замена» блоков питания

Платформы HW2000 Q5 и HW5000 Q2 поставляются с двумя блоками питания с функцией «горячая замена». Данная функция позволяет:

- заменить вышедший из строя блок питания без выключения ViPNet Coordinator HW;
- обеспечить работу ViPNet Coordinator HW при перерыве подачи электропитания на один из блоков.

Подключать в сеть необходимо оба блока питания. При этом нагрузка делится поровну между ними.

При пропадании электропитания или неисправности на каком-либо из блоков питания перестанет гореть индикатор на нём. При этом ViPNet Coordinator HW будет продолжать работу в штатном режиме.

Коммутация портов 10GE в HW2000 и HW5000

Аппаратные платформы HW2000 и HW5000 имеют сетевые адаптеры Ethernet SFP+ 10G. Для подключения этих адаптеров к сети можно использовать SFP-трансиверы или кабели.

Требования к кабелям:

- SFP+ пассивный медный кабель спецификаций SFF-8431 v4.1 и SFF-8472 v10.4.
- Идентификатор по спецификации SFF-8472 — 03h (SFP или SFP+).
- Максимальная длина кабеля — 7 метров.

Примечание. Кабель прямого подключения нельзя использовать для соединения с портом коммутатора, к которому можно подключать SFP-модули.

Таблица 19. Коды для заказа совместимых кабелей Intel

Название продукции	Код продукции
Intel Ethernet SFP+ твинаксиальный кабель, 1 метр	XDACBL1M
Intel Ethernet SFP+ твинаксиальный кабель, 3 метра	XDACBL3M
Intel Ethernet SFP+ твинаксиальный кабель, 5 метров	XDACBL5M

Установка ViPNet Coordinator VA на платформу виртуализации

VMware vSphere ESXi

1 Запустите vSphere Client и выберите **Actions** > **Deploy OVF Template**.

Примечание. Если в меню **File** нет пункта **Deploy OVF Template**, установите расширение Client Integration, добавляющее поддержку образов формата OVF.

2 На странице **Select an OVF template** укажите путь к образу виртуальной машины `*.ova`.

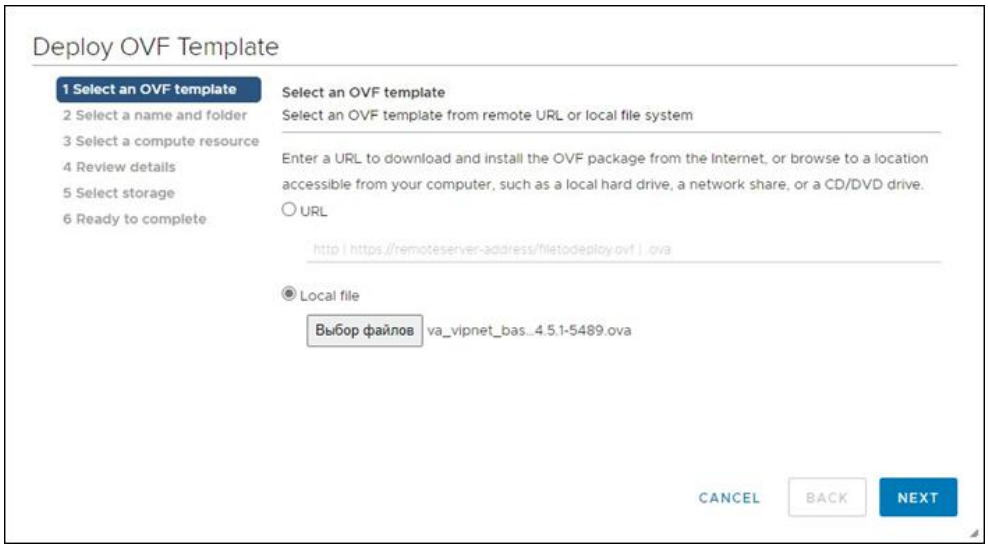


Рисунок 34. Задание файла с образом виртуальной машины

3 На странице **Select a name and folder** укажите произвольное имя и папку для файлов виртуальной машины.

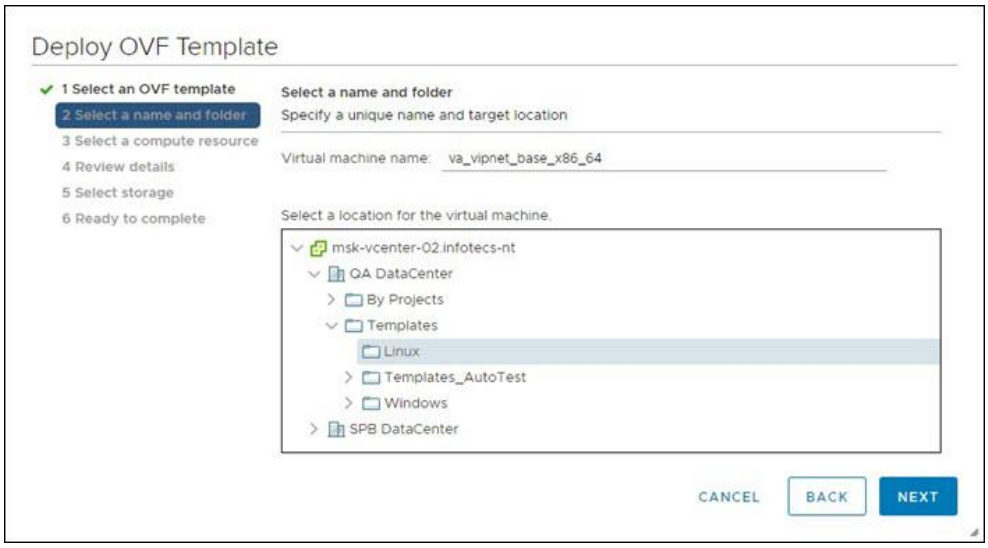


Рисунок 35. Задание имени и расположения виртуальной машины

4 На странице **Select a compute resource** выберите «пул ресурсов», то есть группу носителей информации, выделяемых для хранения файлов виртуальной машины.

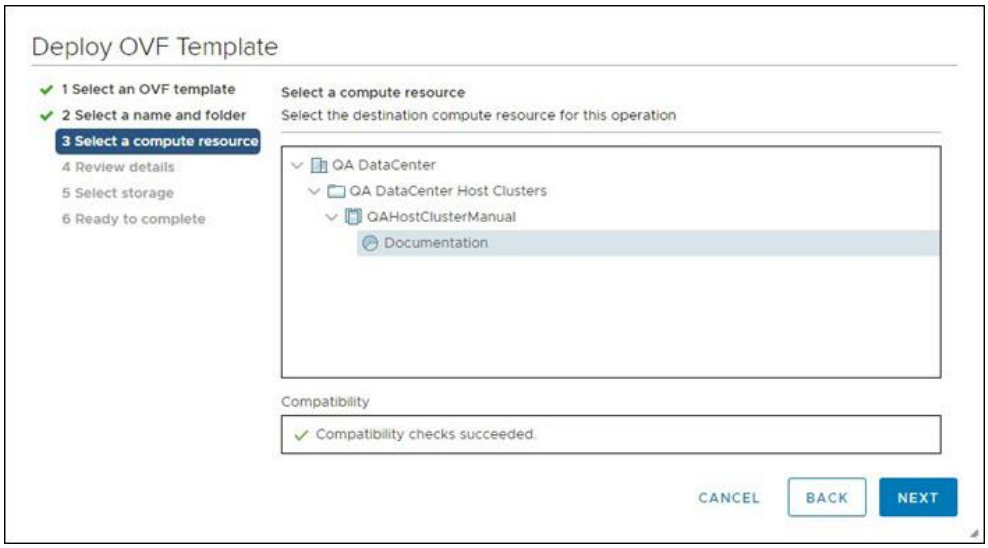


Рисунок 36. Выбор пула ресурсов

5 На странице **Select storage** выберите накопитель из выбранного пула ресурсов, на котором будут храниться файлы виртуальной машины и укажите формат виртуального диска.

Формат **Thin Provision** подходит для небольших по объему дисков или для небольших сетей ViPNet: 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.

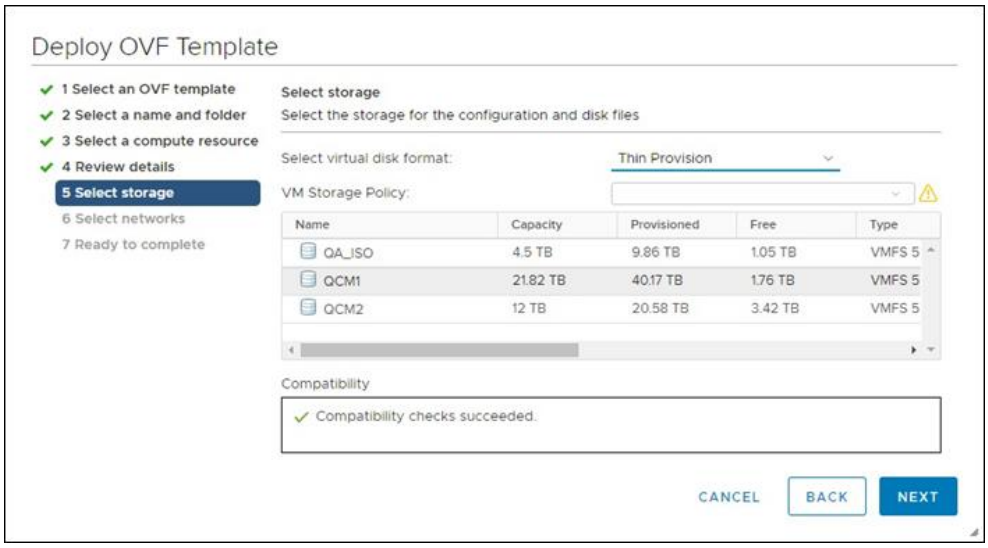


Рисунок 37. Выбор формата виртуального диска

6 На странице **Select networks** 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).

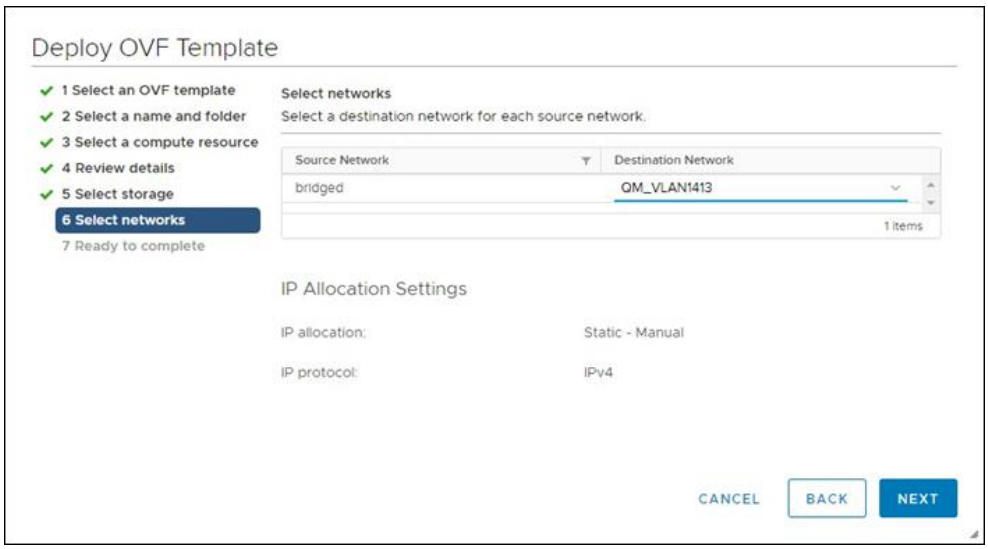


Рисунок 38. Настройка сетевых интерфейсов

7 На странице **Ready to complete** проверьте настройки виртуальной машины и нажмите кнопку **Finish**.

8 Дождитесь окончания развертывания — в папке будет создана виртуальная машина.

9 Перейдите в настройки виртуальной машины и на вкладке **Edit Settings** > **Virtual Hardware** добавьте сетевые интерфейсы.

Если сетевых интерфейсов будет меньше двух, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники с помощью компьютера по протоколу TFTP.

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

Для этого в свойствах перейдите **Actions** > **Compatibility** > **Upgrade VM Compatibility**.

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

12 Запустите виртуальную машину и инициализируйте ViPNet Coordinator HW.

VMware Workstation Pro

Для установки ViPNet Coordinator VA на платформу виртуализации VMware Workstation Pro:

1 Запустите VMware Workstation Pro и выберите **File** > **Open**.

2 Укажите путь к файлу с расширением `*.ova`, содержащему образ виртуальной машины и нажмите **Открыть**.

3 В окне **Import Virtual Machine** укажите имя и папку для размещения виртуальной машины. Нажмите **Import**.

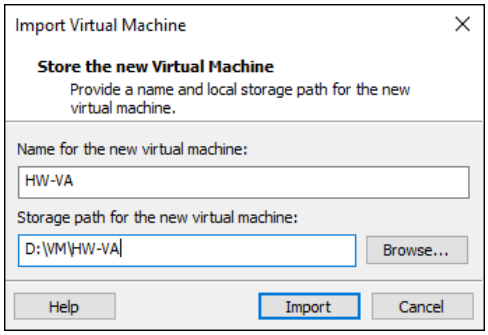


Рисунок 39. Указание имени и расположения виртуальной машины

4 Дождитесь завершения развертывания виртуальной машины.

5 В главном окне программы в контекстном меню созданной виртуальной машины выберите пункт **Settings**.

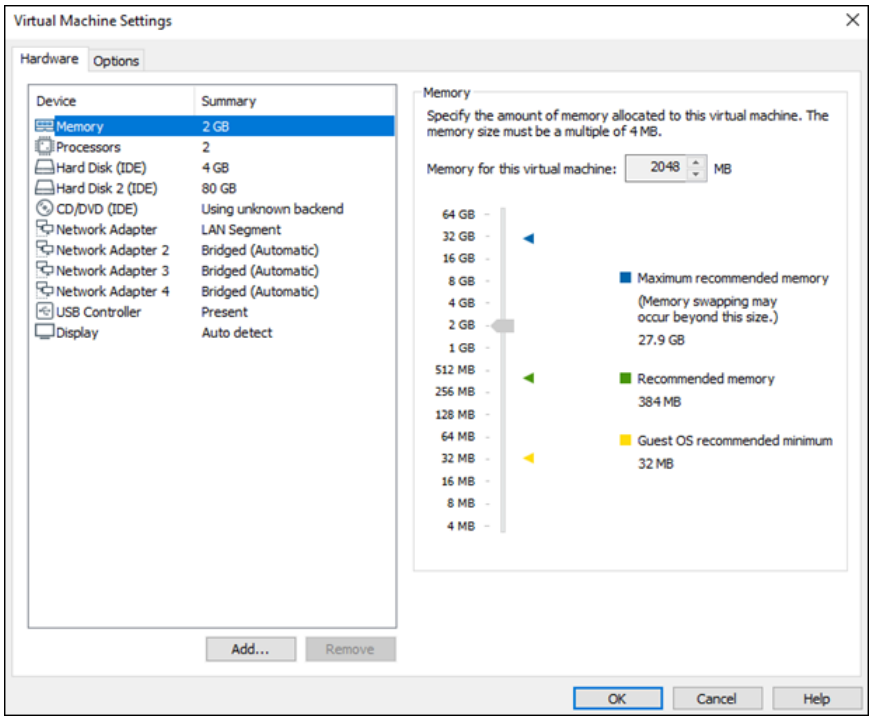


Рисунок 40. Настройка параметров виртуальной машины

6 В окне настройки виртуальной машины **Virtual Machine Settings** на вкладке **Hardware**:

6.1 Настройте конфигурацию виртуальной машины в соответствии с вашей лицензией.

6.2 Настройте виртуальные сетевые интерфейсы.

Примечание. Чтобы подключать к виртуальной машине USB-носители, настройте тип USB-контроллера (вкладка **USB Controller**).

---

7 Запустите виртуальную машину и установите справочники и ключи.

Oracle VM Server

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

- Установка дистрибутива ключей возможна только с помощью компьютера по протоколу TFTP или внешнего CD-привода.
- В командном интерпретаторе не будут выполняться команды, использующие USB-носитель.

После запуска или перезагрузки Oracle VM Server или виртуальной машины ViPNet Coordinator VA снижается скорость передачи данных на сетевых интерфейсах ViPNet Coordinator VA. Чтобы скорость передачи не снижалась, для всех сетевых интерфейсов:

- После запуска или перезагрузки Oracle VM Server в Oracle VM CLI выполните команду:

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

- После запуска или перезагрузки виртуальной машины ViPNet Coordinator VA в Oracle VM CLI выполните команды:

  ```
  ip li set vif<идентификатор виртуальной машины>.<номер интерфейса> qlen 1000
  ethtool -K vif<идентификатор виртуальной машины>.<номер интерфейса> tx off
  ```

В Oracle VM Server не поддерживается перезапуск и приостановка виртуальной машины ViPNet Coordinator VA с помощью кнопок **Restart** и **Suspend**. Для перезапуска виртуальной машины используйте кнопки **Stop** и **Start**, либо перезагружайте ViPNet Coordinator VA с помощью командного интерпретатора или веб-интерфейса.

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 **Import Virtual Appliance**.

Рисунок 41. Импорт образа виртуальной 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 **OK**.

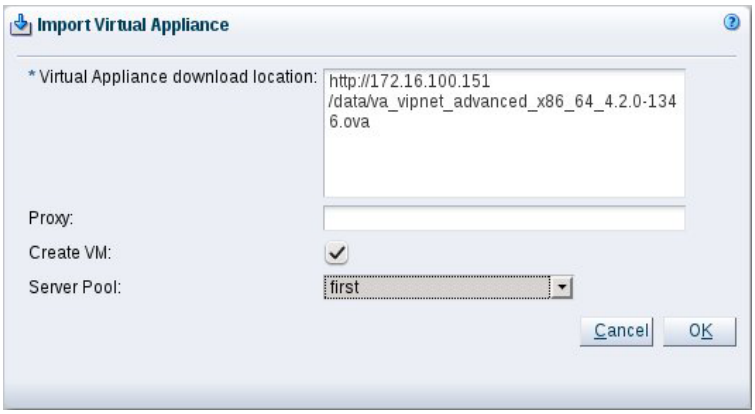


Рисунок 42. Задание пути к образу виртуальной машины

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

Рисунок 43. Редактирование настроек виртуальной машины

6 В окне **Edit Virtual Machine**:

- На вкладке **Configuration**, в списке **Domain Type** выберите **Xen HVM PV Drivers**.
- Укажите параметры CPU, RAM, HDD.
- На вкладке **Networks** добавьте сетевые интерфейсы.

  Если сетевых интерфейсов будет меньше двух, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники с помощью компьютера по протоколу TFTP.
- Нажмите **OK**.

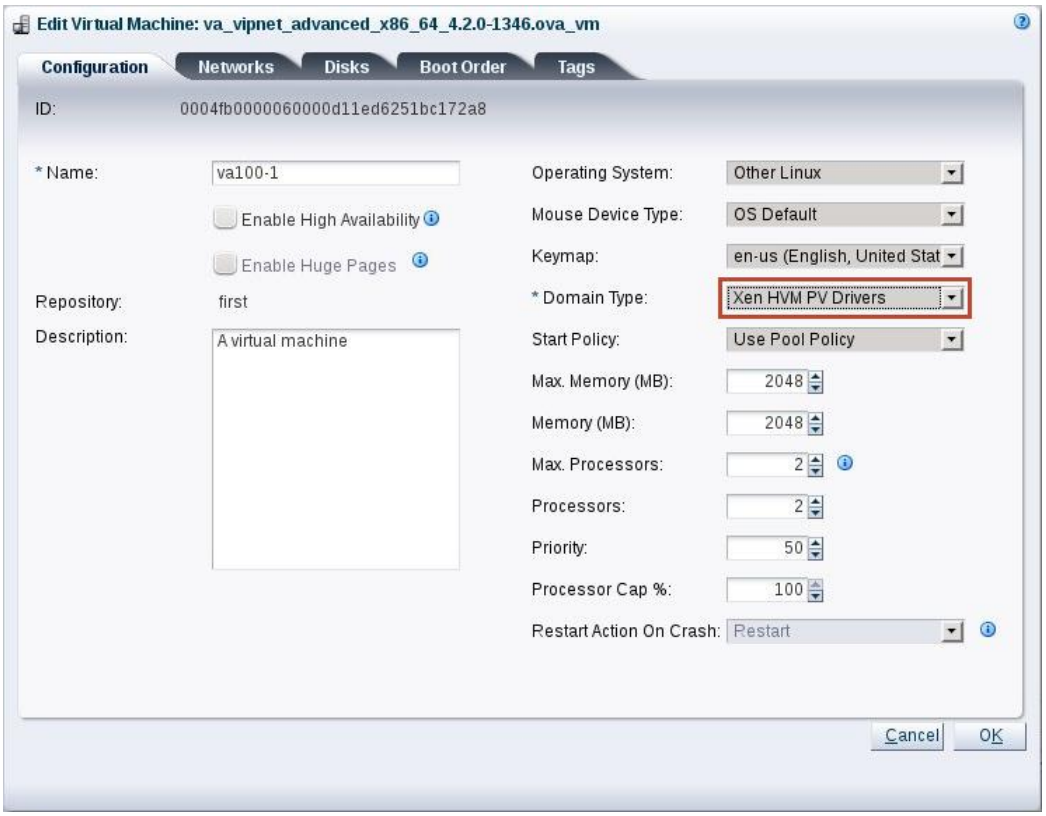


Рисунок 44. Настройка виртуальной машины

7 Запустите виртуальную машину и установите справочники и ключи.

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** > **Disks**.

Oracle VM VirtualBox

1 Выберите **Файл** > **Импорт конфигураций**.

2 На первой странице мастера укажите путь к образу виртуальной машины `*.ova`.

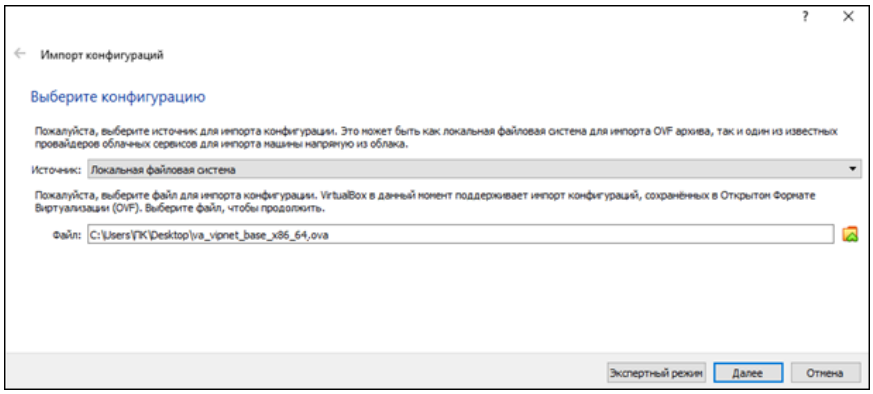


Рисунок 45. Выбор файла с образом виртуальной машины

3 На странице **Укажите параметры импорта** в поле **Имя** вы можете изменить имя виртуальной машины. Затем нажмите **Импорт**.

Внимание! Во время установки ViPNet Coordinator VA на платформу виртуализации и при его дальнейшей эксплуатации не меняйте тип контроллера жесткого диска. Корректная работа ViPNet Coordinator VA гарантируется только при использовании IDE-контроллера жесткого диска.

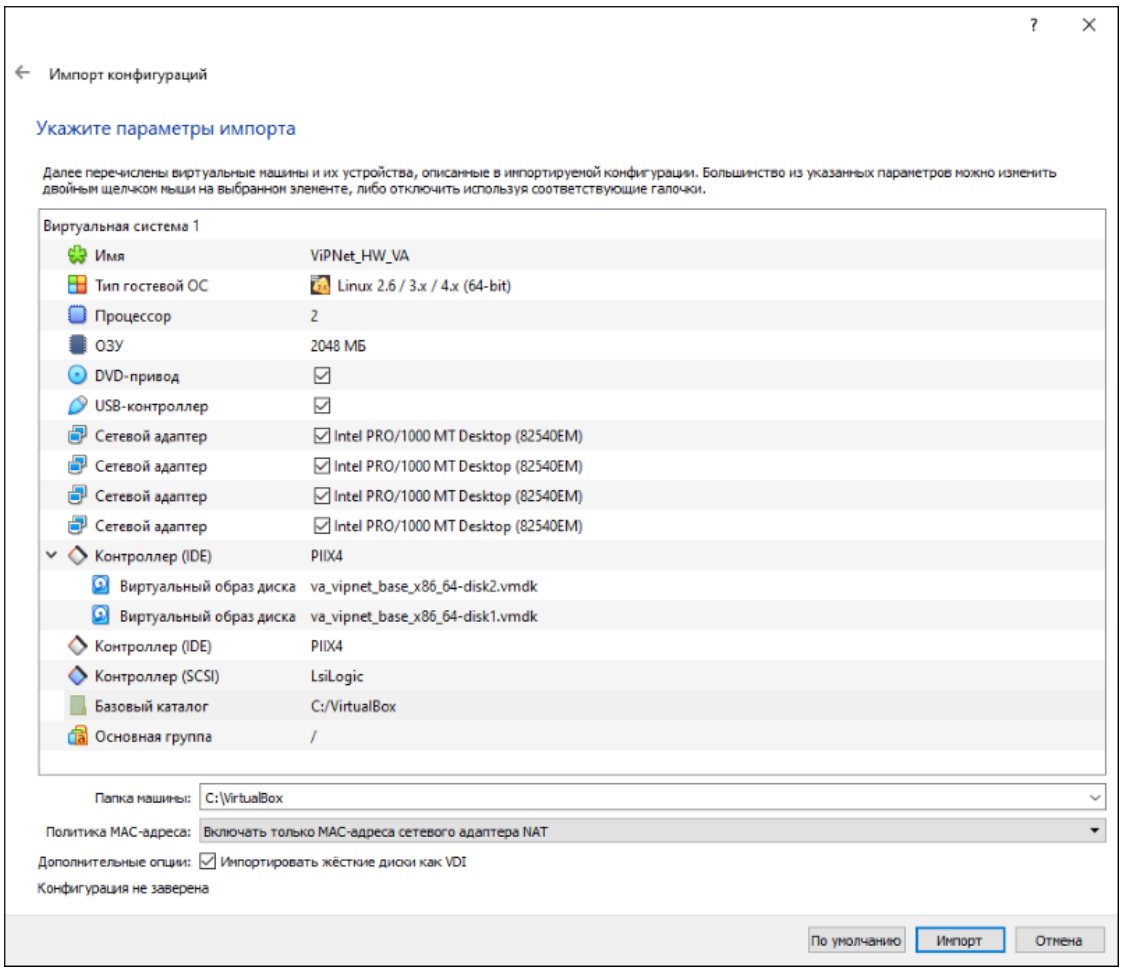


Рисунок 46. Изменение параметров виртуальной машины

4 Настройте виртуальную машину — нажмите **Настроить** .

5 Выберите **Система** > **Процессор** и установите **Включить PAE/NX** (поддержка режима расширения физических адресов PAE — Physical Address Extension).

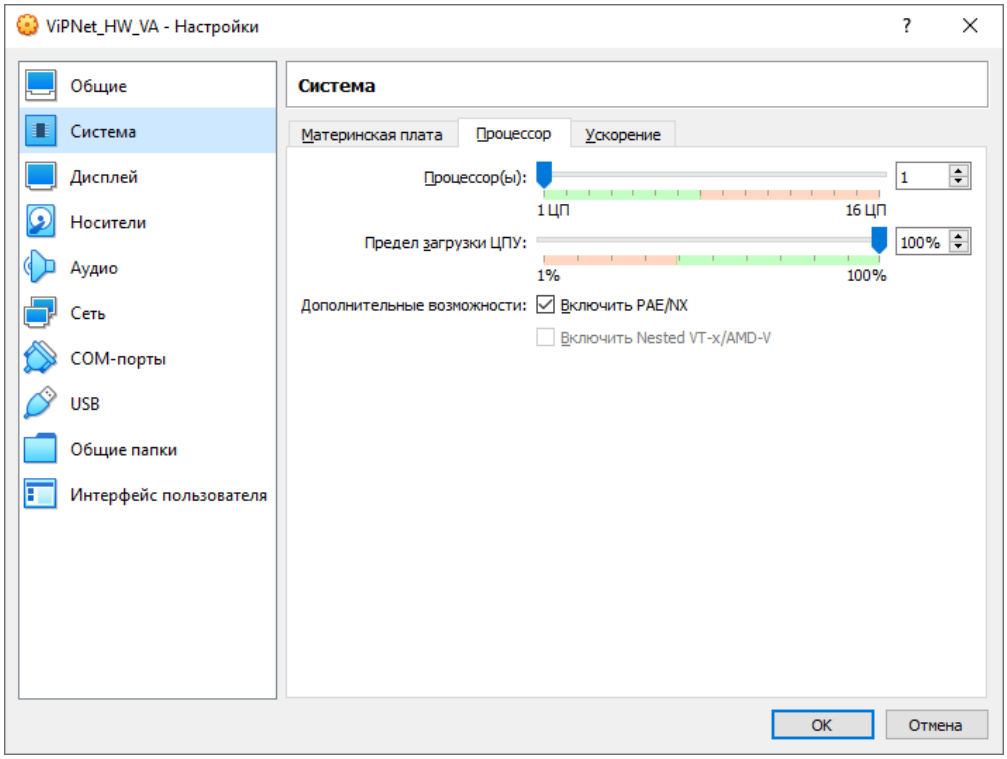


Рисунок 47. Включение поддержки процессором режима PAE

6 На вкладке **Материнская плата** установите **Часы в системе UTC**.

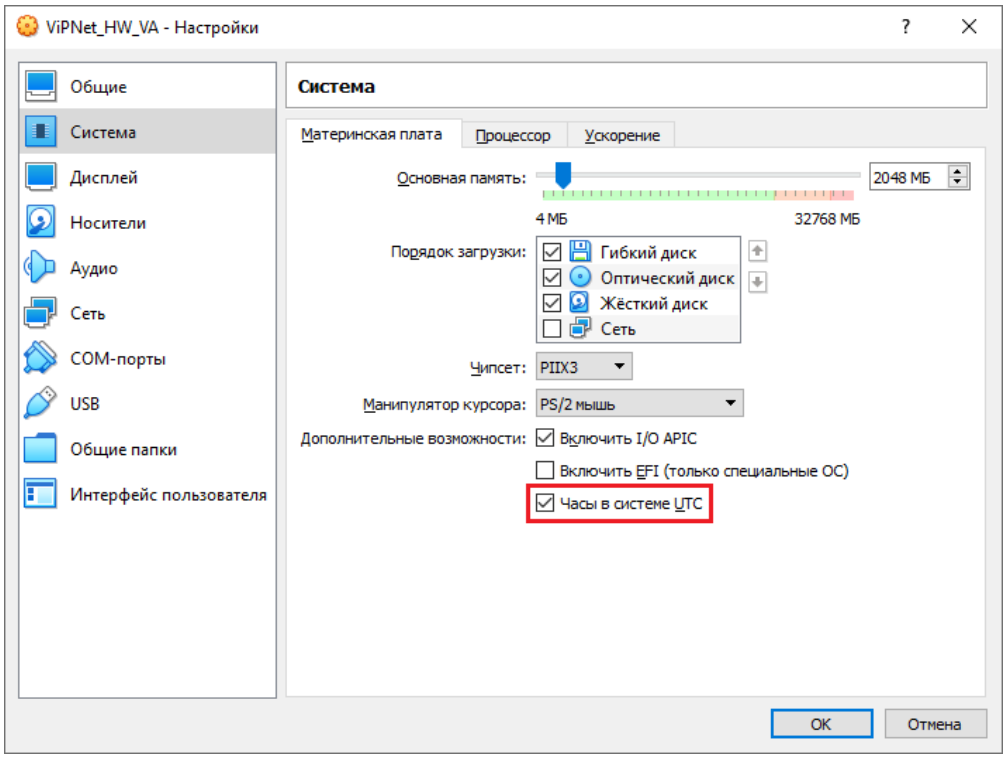


Рисунок 48. Включение режима UTC для аппаратных часов в VirtualBox

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 Выберите **Сеть** и добавьте сетевые интерфейсы. Если сетевых интерфейсов будет меньше двух, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники с помощью компьютера по протоколу TFTP.

Для сетевых интерфейсов укажите:

- **Тип подключения** — **Сетевой мост**, **Внутренняя сеть**, либо **Виртуальный адаптер хоста**.
- **Тип адаптера** — любое значение кроме **Паравиртуальная сеть (virtio-net)**.

8 Чтобы запустить виртуальную машину, нажмите **Запустить**.

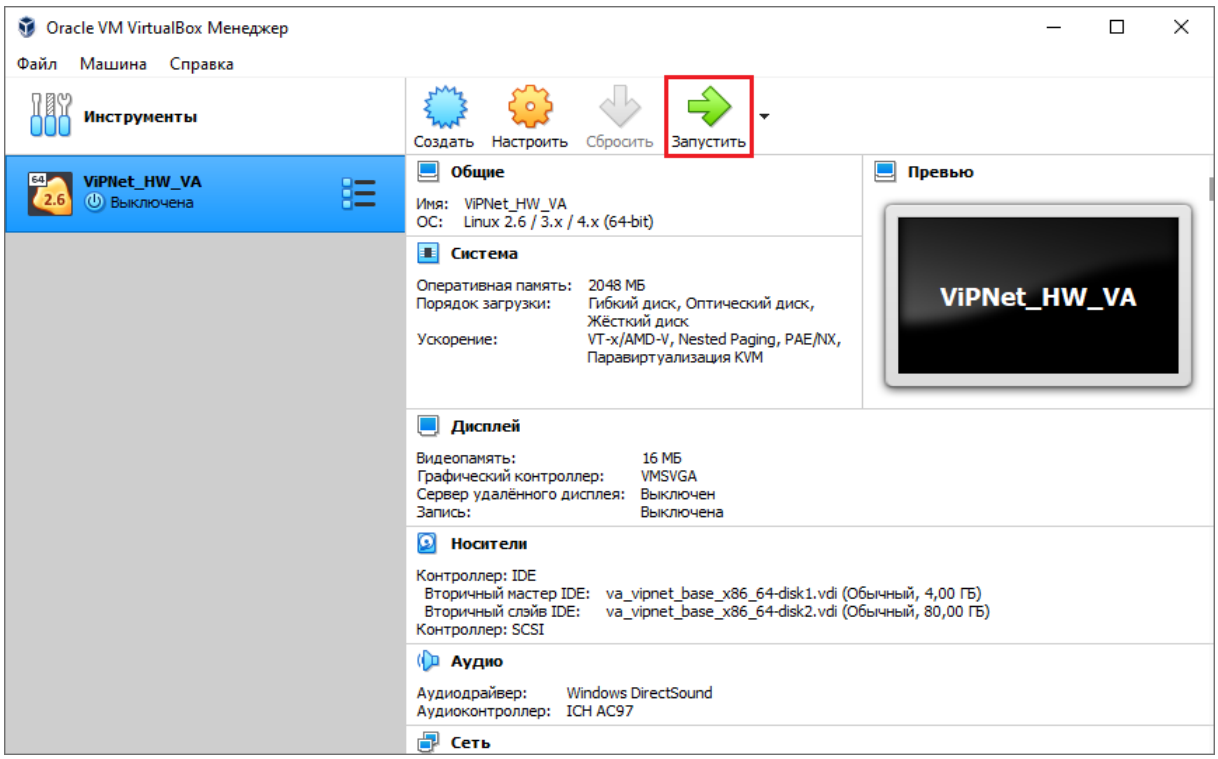


Рисунок 49. Запуск виртуальной машины

После загрузки ViPNet Coordinator VA установите справочники и ключи.

Microsoft Hyper-V

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

- Установка дистрибутива ключей возможна только с помощью компьютера по протоколу TFTP или внешнего CD-привода.
- В командном интерпретаторе не будут выполняться команды, использующие USB-носитель.

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

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

2 В программе Диспетчер Hyper-V выберите **Действие** > **Диспетчер виртуальных коммутаторов** и создайте новую виртуальную сеть.

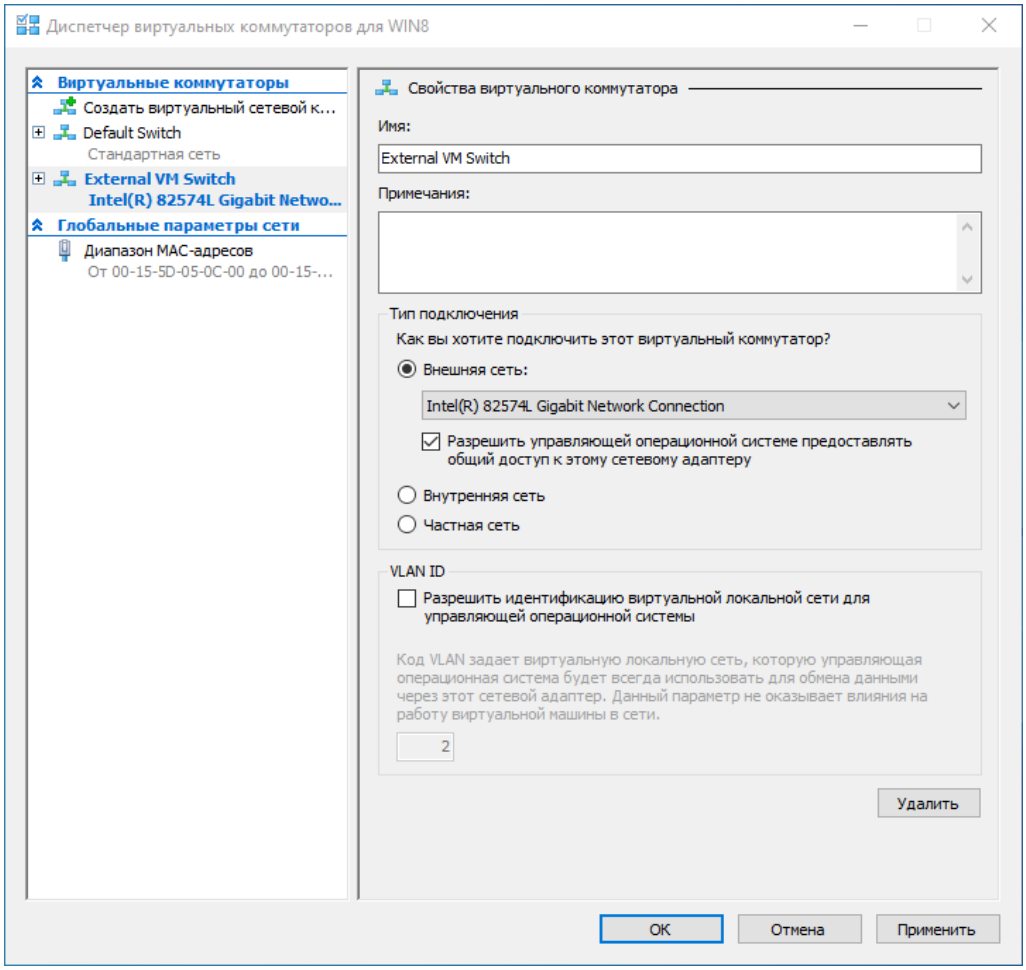


Рисунок 50. Создание виртуальной сети в Virtual Switch Manager

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

4 На вкладке **Укажите поколение** выберите **Поколение 1**.

5 На вкладке **Подключить виртуальный жесткий диск** выберите **Использовать имеющийся виртуальный жесткий диск** и укажите путь к первому образу ViPNet Coordinator VA для Microsoft Hyper-V (файл с расширением `.vhdx`).

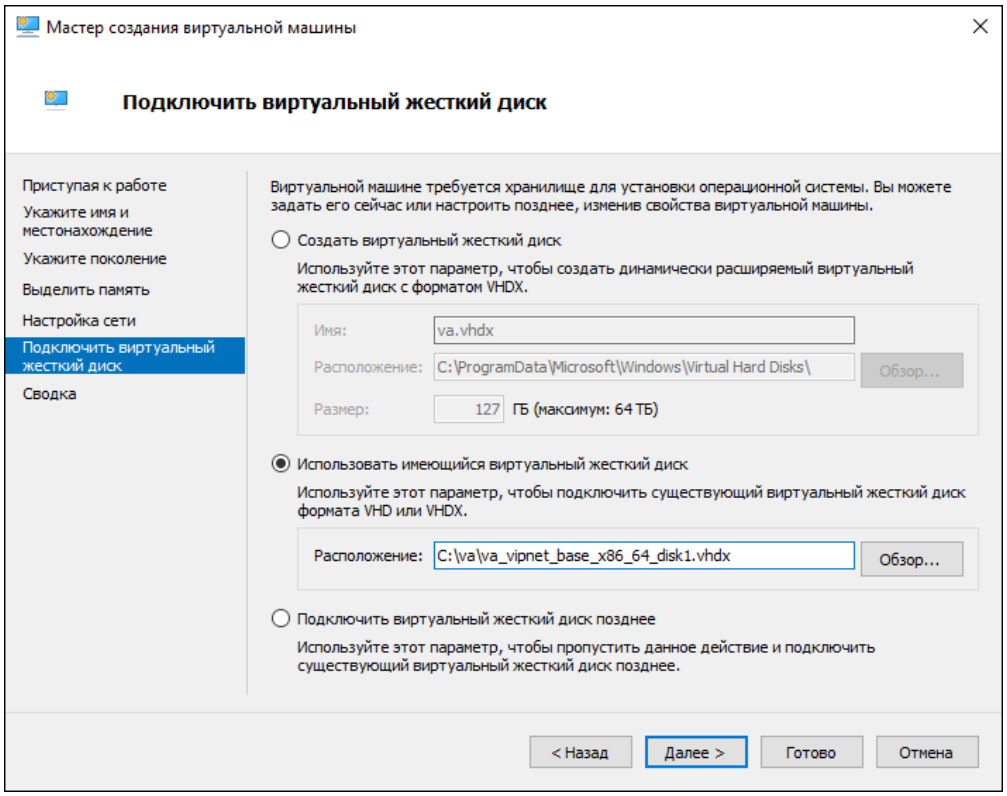


Рисунок 51. Выбор образа .vhdx

6 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 `.vhdx`).

7 В свойствах виртуальной машины добавьте сетевые интерфейсы.

Если сетевых интерфейсов будет меньше двух, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники с помощью компьютера по протоколу TFTP.

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

9 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.

---

10 После загрузки ViPNet Coordinator VA установите справочники и ключи.

Proxmox

Примечание. Сценарий установки представлен для Proxmox версии 7.3-3.

Шаги 3 и 5 (создание и подключение дисков) можно выполнить в графическом интерфейсе менеджера виртуальных машин Proxmox.

Шаг 4 (развертывание образов) выполняется только в командной строке..

1 Подготовьте файлы `*.raw`, `*vhdx` или `*.qcow2` с образами виртуальной машины ViPNet Coordinator VA.

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 socket --bootdisk scsi0 --scsihw virtio-scsi-pci
```

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

4 Запустите развертывание образов виртуальной машины:

```
qm disk import 110 <путь к первому образу> local-lvm
```

```
qm disk import 110 <путь ко второму образу> 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)**.

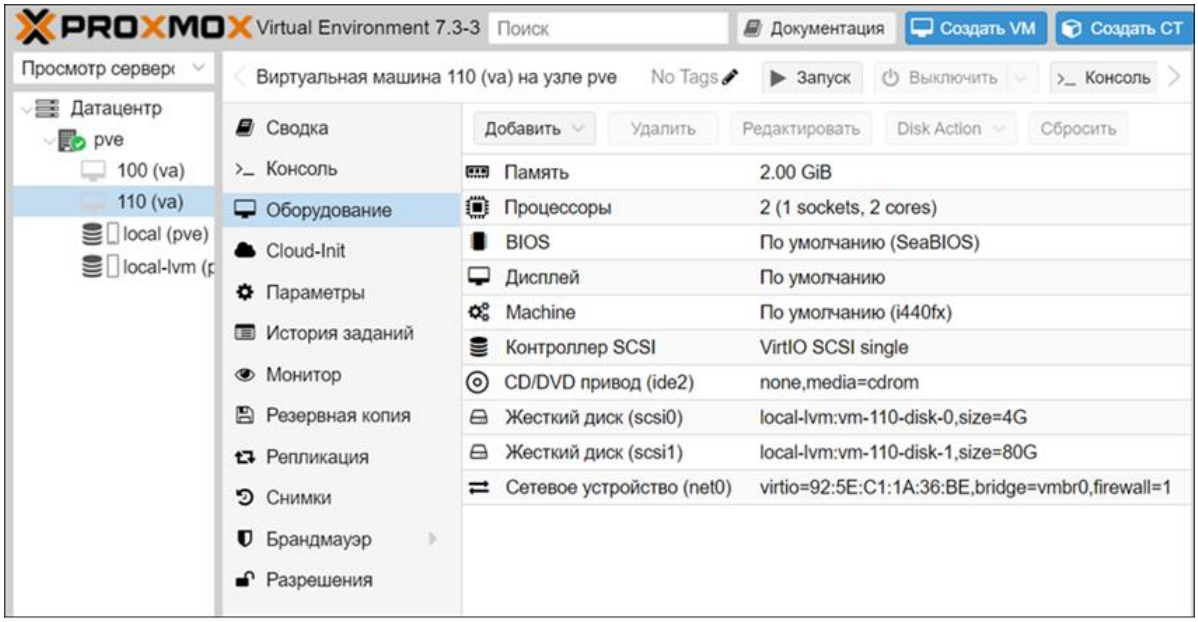


Рисунок 52. Запуск виртуальной машины

7 В разделе **Оборудование** добавьте сетевые интерфейсы.

Если сетевых интерфейсов будет меньше двух, то ViPNet Coordinator VA будет недоступен по технологическому адресу. Это означает, что вы не сможете установить ключи и справочники с помощью компьютера по протоколу TFTP.

8 В разделе **Параметры** установите **Порядок загрузки**. Система должна устанавливаться с наименьшего жесткого диска.

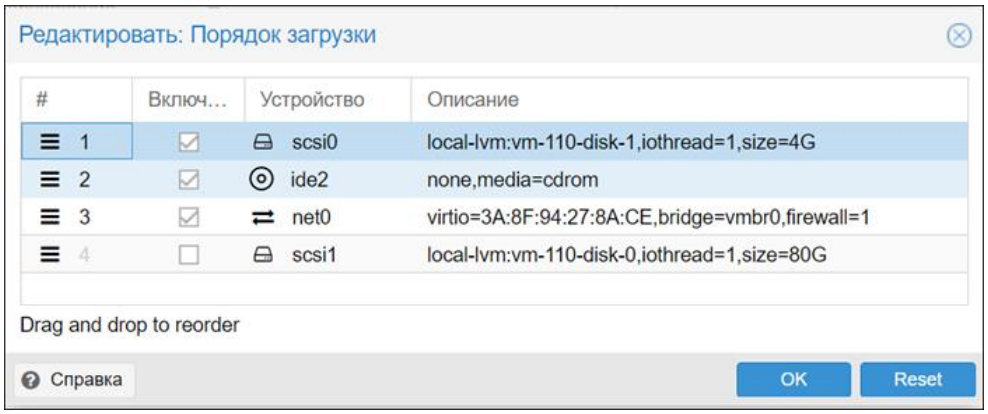


Рисунок 53. Порядок загрузки

9 Запустите виртуальную машину и установите справочники и ключи.

Способы установки дистрибутива ключей

В процессе первичной настройки ViPNet Coordinator HW необходимо установить дистрибутив ключей, в котором содержатся справочники, ключи и лицензия ViPNet Coordinator HW. Без выполнения этого этапа работа ViPNet Coordinator HW в сети ViPNet невозможна. Существует несколько способов установки дистрибутива ключей, которые зависят от способа подключения к ViPNet Coordinator HW.

- С помощью внешнего устройства — USB-носителя или CD-привода. Файл дистрибутива ключей располагается на USB-носителе или CD-диске, которые подключены к ViPNet Coordinator HW.

  Способ удобен, если вы подключаетесь к ViPNet Coordinator HW локально с помощью консоли (аппаратные исполнения) или если платформа виртуализации поддерживает подключение внешних носителей (виртуализированное исполнение).

- С помощью компьютера по протоколу TFTP. Файл дистрибутива ключей располагается в папке на компьютере.

  Способ удобен, если вы подключаете компьютер к сетевому интерфейсу `eth1` ViPNet Coordinator HW напрямую (для аппаратных платформ используйте сетевой кабель RJ-45 Cat. 5).

Установка с помощью внешнего устройства

Для установки дистрибутива ключей данным способом:

1. Отформатируйте USB-носитель в одну из файловых систем: FAT32, ext2, ext3 или ext4.
2. Запишите на USB-носитель или CD-диск файл дистрибутива ключей.
3. Подключите USB-носитель или CD-привод к ViPNet Coordinator HW; вставьте CD-диск в привод.

Примечание. Подключение USB-носителя или CD-привода к ViPNet Coordinator VA производится средствами платформы виртуализации.

---

4. Для аппаратных исполнений ViPNet Coordinator HW:
   - подключите монитор (к VGA или HDMI порту) и клавиатуру (к PS/2 или USB порту).
   - подключите компьютер к консольному порту ViPNet Coordinator HW (кроме HW10 F1).

Примечание. Разъем консольного порта может отличаться на разных аппаратных платформах ViPNet Coordinator HW.

Для корректной работы задайте параметры подключения консоли:

- Speed (скорость обмена данными) — 38400.
- Data (размер данных) — 8.
- Parity (четность) — None.
- Stopbits (стоповые биты) — 1.
- Тип терминала — VT100+.
- Flow Control — None.
- Remote character set (кодировка) — KOI8-R.

Установка с помощью компьютера по протоколу TFTP

Для установки дистрибутива ключей вам понадобятся:

- Компьютер с сетевой картой Ethernet и Windows или Linux любых версий.
- Сетевой кабель RJ-45 Cat. 5 для подключения компьютера к ViPNet Coordinator HW.

На компьютере должны быть включены стандартные службы, необходимые для установки дистрибутива ключей:

- Telnet или SSH — для подключения к ViPNet Coordinator HW.
- TFTP — для переноса дистрибутива ключей на ViPNet Coordinator HW.

В Linux эти службы включены по умолчанию.

В Windows эти службы по умолчанию отключены, чтобы их включить:

1. В меню **Пуск** начните вводить «компоненты» и выберите **Включение или отключение компонентов Windows** (**Turn Windows features on or off**).
2. Выберите **Клиент TFTP** (**TFTP Client**) и **Простые службы TCPIP** (**Simple TCPIP services**).
3. Нажмите **OK**.

На время установки дистрибутива ключей:

1. Отключите компьютер от внешней сети.
2. Если на компьютере установлен ViPNet Client — отключите защиту ViPNet. Для этого в основном меню ViPNet Client выберите **Файл** > **Конфигурации** > **Отключить защиту**.
3. На компьютере с Windows:
   - 3.1 Отключите службы безопасности и обновления:
     - Брандмауэр Windows (Windows Firewall).
     - Защитник Windows (Windows Defender).

- Центр обновления Windows (Windows Update).

3.2 На панели управления Windows выберите **Сеть и Интернет (Network and Internet)** > **Свойства браузера (Manage browser add-ons)** > **Безопасность (Security)** > **Интернет (Internet)** > **Другой (Custom level)** и отключите защиту по всем параметрам. Нажмите **OK**.

Перед началом установки дистрибутива ключей:

1 Перенесите на компьютер файл дистрибутива ключей.

2 С помощью сетевого кабеля подключите компьютер к порту `eth1` ViPNet Coordinator HW.

3 Установите на сетевом интерфейсе компьютера IP-адрес `169.254.241.5`.

4 Подключитесь к ViPNet Coordinator HW с помощью Telnet- или SSH-клиента по IP-адресу `169.254.241.1`; в параметрах подключения укажите (приведены настройки PuTTY):

- Тип терминала VT100 (**Terminal** > **Keyboard** > **VT100+**).
- Кодировка символов KOI8-R (**Window** > **Translation**, в списке **Remote character set** выберите **KOI8-R**).
- Метод ввода linux (**Connection** > **Data** > **Terminal type string**, введите **linux**).
- Ширина окна по умолчанию 120 символов (**Windows** > **Columns**, введите **120**).

Первичная настройка ViPNet Coordinator HW

Первичная настройка позволяет задать параметры, необходимые для подключения ViPNet Coordinator HW к существующей сети ViPNet или использования ViPNet Coordinator HW в качестве первого координатора новой сети ViPNet. Первичная настройка выполняется с помощью мастера установки дистрибутива ключей. До выполнения первичной настройки:

1. Получите у администратора сети ViPNet файл дистрибутива ключей и пароль доступа к нему. Если при создании дистрибутива ключей был задан способ аутентификации пользователя «Устройство», получите у администратора сети ViPNet внешнее устройство аутентификации и ПИН доступа к нему.
2. Подключитесь к ViPNet Coordinator HW локально одним из способов.
3. Если для установки файла дистрибутива ключей будет использоваться внешнее устройство, подготовьте его.

Внимание! Не отключайте питание ViPNet Coordinator HW до завершения процесса установки дистрибутива ключей, так как это может привести к неработоспособности ViPNet Coordinator HW.

Вы можете остановить установку дистрибутива и сбросить ViPNet Coordinator HW к заводским настройкам нажав **Ctrl+C** в процессе первичной настройки. Данный способ будет работать до шага загрузки основных драйверов и служб.

Выполните первичную настройку ViPNet Coordinator HW:

1. Включите ViPNet Coordinator HW.
2. В строке приглашения Linux введите имя пользователя `user` и пароль `user`. При успешной авторизации будет запущен мастер установки дистрибутива ключей.
3. Выберите режим работы мастера:
   - `1` — консольный.
   - `2` — полноэкранный.

Примечание. Далее, в каждом шаге работы мастера приведены действия для двух режимов: сначала для консольного, затем для полноэкранного.

---

4. Ознакомьтесь с лицензионным соглашением. Для продолжения установки примите условия соглашения.

   Если вы не примете лицензионное соглашение, ViPNet Coordinator HW будет выключен. Вы можете сбросить ViPNet Coordinator HW к заводским настройкам и выключить его на любом

шаге до установки дистрибутива ключей. Для этого нажмите **Ctrl**+**C** и откажитесь от принятия лицензионного соглашения.

Примечание. Текст лицензионного соглашения отображается в кодировке KOI8-R, поэтому если вы подключились к ViPNet Coordinator HW через консоль, Telnet или SSH, а текст лицензионного соглашения отображается некорректно, убедитесь, что заданы верные параметры.

5 Начните установку:

- В строке `Would you like to start installing keys/restoring configuration? [Yes/No]` введите `y` и нажмите **Enter**.
- Нажмите **Next**.

6 Выберите континент или время UTC из списка:

- Введите номер континента или UTC и нажмите **Enter**.
- Выберите континент или UTC в списке и нажмите **Next**.

7 Выберите страну из списка:

- Введите номер страны и нажмите **Enter**.
- Выберите страну в списке и нажмите **Next**.

Список содержит страны, расположенные на выбранном континенте.

8 Выберите часовой пояс из списка:

- Введите номер пояса и нажмите **Enter**.
- Выберите часовой пояс в списке и нажмите **Next**.

Список содержит часовые пояса выбранной страны. Если в стране только один часовой пояс, то он будет выбран автоматически.

9 Подтвердите установку часового пояса:

- В строке `Is the above information OK?` введите `1` и нажмите **Enter**.
- Нажмите **Yes**.

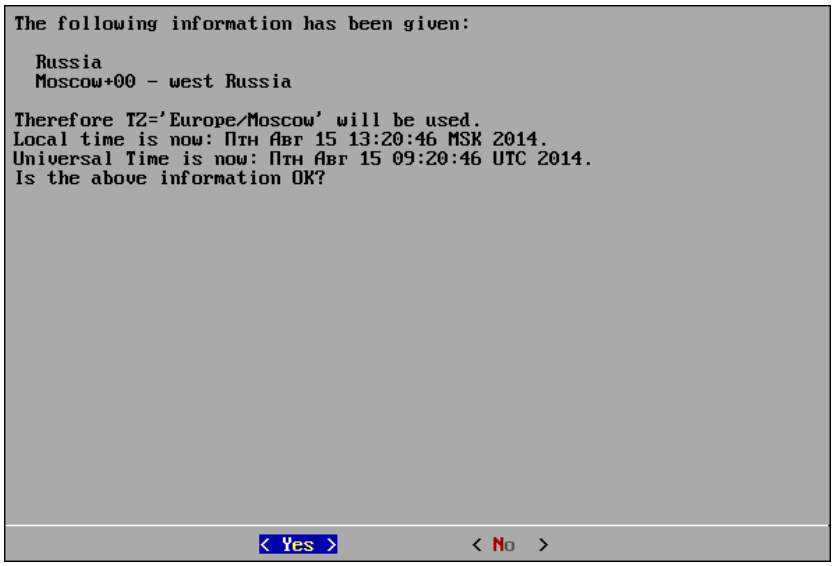


Рисунок 54. Запрос на установку часового пояса в полноэкранном режиме

10 Если требуется изменить текущую дату и время:

- Введите дату и время в формате `YYYY-MM-DD hh:mm:ss` и нажмите **Enter**.
- Установите дату и время с помощью календаря, нажмите **Next**.

11 Выберите способ установки файла дистрибутива ключей:

- В строке `Would you like to install keys from TFTP, USB or CD storage device? [t/u/c]` введите:
  - `t` — с компьютера по протоколу TFTP.
  - `u` — с USB-носителя.
  - `c` — с CD-диска.
- Установите переключатель в нужное положение с помощью пробела и нажмите **Next**.

12 Для установки с компьютера по протоколу TFTP:

12.1 На компьютере выполните команду:

```
tftp -i 169.254.241.1 put <имя_файла>
```

12.2 В мастере установки подтвердите установку файла дистрибутива ключей — нажмите **Enter** или **Next**.

13 Для установки с USB-носителя или CD-диска:

13.1 Подключите USB-носитель или CD-привод к USB-разъему ViPNet Coordinator HW; вставьте CD-диск в привод.

13.2 Чтобы найти файлы `dst`, в мастере установки нажмите **Enter** или **Next**.

Если на USB-носителе или CD-диске обнаружен только один файл `dst`, то он будет выбран для установки.

Если обнаружено несколько файлов `dst`:

- Введите номер файла из списка `Found several DST and VBE files` и нажмите **Enter**.

- Выберите файл в списке и нажмите **Next**.

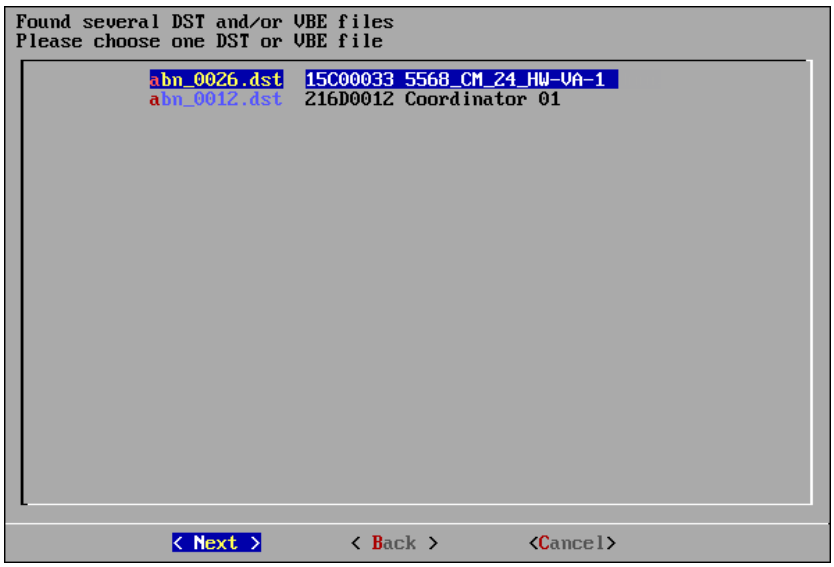


Рисунок 55. Выбор файла для установки справочников и ключей в полноэкранном режиме

Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы `dst`.

Если в консольном режиме найдено больше 20 файлов, список выводится постранично.

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

Если файлов `dst` не обнаружено, мастер предложит заново выбрать способ переноса дистрибутива ключей (шаг 11).

14 Введите пароль к файлу дистрибутива ключей:

- В строке `Enter password` введите пароль и нажмите **Enter**.
- Введите пароль и нажмите **Next**.

15 Если способ аутентификации пользователя на ViPNet Coordinator HW — «Устройство»:

15.1 Подключите к USB-разъему ViPNet Coordinator HW устройство аутентификации.

15.2 Введите ПИН доступа к устройству:

- В строке `Insert token and enter PIN Code` введите ПИН и нажмите **Enter**.
- Введите ПИН и нажмите **Next**.

Внимание! На устройстве аутентификации должен быть только один контейнер, в котором содержится персональный ключ пользователя. При наличии нескольких контейнеров на устройстве мастер установки дистрибутива ключей завершит работу.

---

16 Настройте сетевые интерфейсы последовательно, начиная с `eth0`. Чтобы настроить интерфейс, включите его:

- В строке `Configure interface eth<номер>? [Yes/No]` введите `y` и нажмите **Enter**.
- Установите переключатель в положение **UP** с помощью пробела и нажмите **Next**.

Чтобы пропустить настройку интерфейса и перейти к следующему:

- Введите `n` и нажмите **Enter**.
- Установите переключатель в положение **DOWN** и нажмите **Next**.

В случае отказа от настройки последнего сетевого интерфейса, мастер перейдет к настройке DNS-сервера (шаг 20).

17 Установите для интерфейса режим DHCP:

- В строке `Use dhcp on the interface eth<номер>? [Yes/No]` введите `y` и нажмите **Enter**.
- Установите переключатель в положение **DHCP** и нажмите **Next**.

Или установите режим статического адресации:

- Введите `n` и нажмите **Enter**.
- Установите переключатель в положение **StaticIP** и нажмите **Next**.

18 Если был выбран режим статической адресации, задайте IP-адрес:

- Введите последовательно IP-адрес и маску интерфейса и нажмите **Enter**.
- Введите IP-адрес и маску интерфейса в соответствующие поля и нажмите **Next**.

Внимание! Ограничения при задании IP-адреса:

- Запрещено задавать IP-адрес 0.0.0.0.
- Запрещено задать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов запрещено задать IP-адреса, относящиеся к одной подсети.

Если интерфейс не последний, мастер перейдет к настройке следующего интерфейса (шаг 16).

19 Если ни для одного интерфейса не был задан режим DHCP, задайте шлюз по умолчанию: введите IP-адрес шлюза и нажмите **Enter** или **Next**.

20 Включите автоматический запуск DNS-сервера при загрузке ViPNet Coordinator HW:

- В строке `Do you want to enable DNS server? [Yes/No]` введите `y` и нажмите **Enter**.
- Установите переключатель в положение **ON (Enable starting the DNS server at boot)** и нажмите **Next**.

Если DNS-сервер запускать не нужно:

- Введите `n` и нажмите **Enter**.

- Установите переключатель в положение **OFF (Disable starting the DNS server at boot)** и нажмите **Next**.

  Мастер перейдет к настройке NTP-сервера (шаг 22).

21 При подключении к интернету в качестве DNS-серверов по умолчанию используются корневые DNS-серверы. Чтобы добавить DNS-сервер:

- В строке `Do you want to add custom DNS server? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес DNS-сервера и нажмите **Enter**.
- Установите переключатель в положение **Yes (Add custom DNS server)** и нажмите **Next**. Введите IP-адрес DNS-сервера и нажмите **Next**.

Если DNS-сервер добавлять не нужно:

- Введите `n` и нажмите **Enter**.
- Установите переключатель в положение **No (Leave the default setting)** и нажмите **Next**.

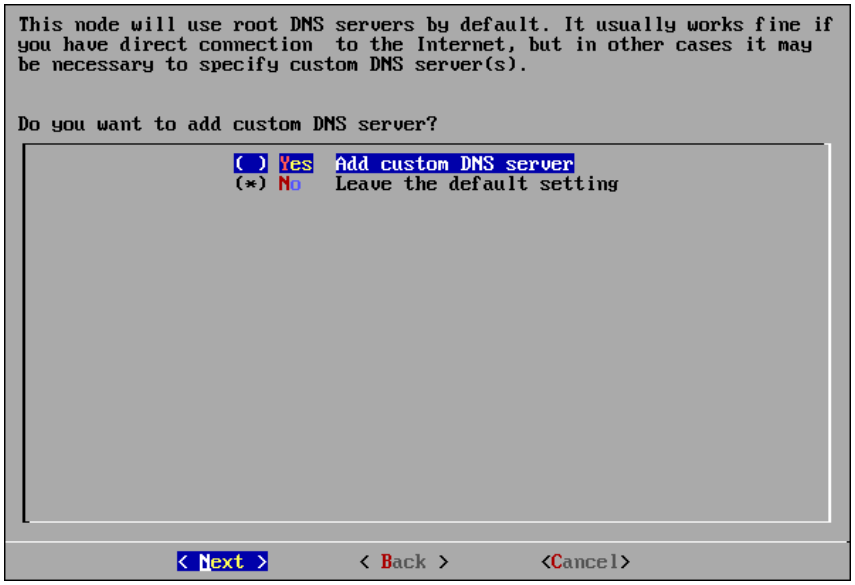


Рисунок 56. Запрос на добавление IP-адреса DNS-сервера в полноэкранном режиме

22 Включите автоматический запуск NTP-сервера при загрузке ViPNet Coordinator HW:

- В строке `Do you want to enable NTP server? [Yes/No]` введите `y` и нажмите **Enter**.
- Установите переключатель в положение **ON (Enable starting the NTP server at boot)** и нажмите **Next**.

Если NTP-сервер запускать не нужно:

- Введите `n` и нажмите **Enter**.
- Установите переключатель в положение **OFF (Disable starting the NTP server at boot)** и нажмите **Next**.

  Мастер перейдет к настройке имени компьютера (шаг 23).

23 Для синхронизации системного времени по умолчанию используются публичные NTP-серверы. Чтобы добавить NTP-сервер:

- В строке `Do you want to add custom NTP server? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес или DNS-имя NTP-сервера и нажмите **Enter**.
- Установите переключатель в положение **Yes (Add custom NTP server)** и нажмите **Next**. Введите IP-адрес или DNS-имя NTP-сервера и нажмите **Next**.

Если NTP-сервер добавлять не нужно:

- Введите `n` и нажмите **Enter**.
- Установите переключатель в положение **No (Leave the default setting)** и нажмите **Next**.

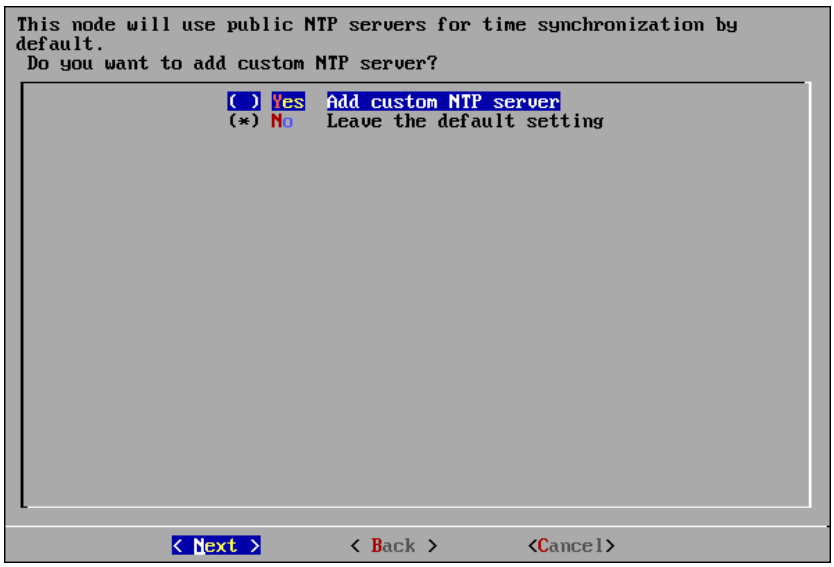


Рисунок 57. Запрос на добавление NTP-сервера в полноэкранном режиме

24 По умолчанию имя компьютера ViPNet Coordinator HW формируется по шаблону `<исполнение ViPNet Coordinator HW>-<идентификатор узла>`, например, `HW1000-270E033A`. Чтобы изменить имя, введите новое и нажмите **Enter** или **Next**. Если имя изменять не нужно, нажмите **Enter** или **Next**.

25 Текущий диапазон виртуальных адресов может пересекаться с диапазоном IP-адресов, который используется для адресации в вашей сети. Чтобы изменить диапазон виртуальных адресов:

- В строке `Do you want to specify custom virtual IP address range? [Yes/No]` введите `y` и нажмите **Enter**. Введите начальный и конечный адреса (или только начальный адрес в нотации CIDR) нового диапазона виртуальных адресов, например, 11.0.0.1-11.0.254.254 или 11.0.0.1/16 и нажмите **Enter**.
- Установите переключатель в положение **Range (Set custom virtual IP range)** или **CIDR (Set custom virtual IP range in the CIDR notation)** и нажмите **Next**. Введите начальный и конечный адреса (или только начальный адрес в нотации CIDR) нового диапазона виртуальных адресов и нажмите **Next**.

Если диапазон виртуальных адресов изменять не нужно:

- Введите `n` и нажмите **Enter**.
- Установите переключатель в положение **No (Leave the default setting)** и нажмите **Next**.

Примечание. По умолчанию мастер предлагает диапазон виртуальных адресов 11.0.0.1-11.255.255.254 (в нотации CIDR 11.0.0.1/8).

Подробнее о виртуальных адресах см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка виртуальных IP-адресов».

Виртуальные адреса из указанного диапазона будут назначаться одиночным туннелируемым адресам. Для диапазонов туннелируемых узлов адреса назначаются из 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 «Настройка с помощью командного интерпретатора», раздел «Настройка видимости узлов».

26 Если был настроен хотя бы один сетевой интерфейс, проверьте связь ViPNet Coordinator HW с узлом сети ViPNet:

- В строке `Do you want to probe VPN-connection with some host in order to verify the configuration you've just made? [Yes/No]` введите `y` и нажмите **Enter**.
- Нажмите **Yes**.

Примечание. Проверку связи с другими узлами сети ViPNet рекомендуется выполнять во избежание возможной потери доступа к ViPNet Coordinator HW по завершении первичной настройки.

Если проверять связь с узлом сети ViPNet не нужно:

- Введите `n` и нажмите **Enter**.
- Нажмите **No**.

  Мастер установки дистрибутива ключей перейдет к запуску драйверов и служб (шаг 34).

27 Задайте режим подключения ViPNet Coordinator HW к внешней сети:

- В ответ на сообщение `Do you want to configure firewall mode? [Yes/No]` введите символ `y` и нажмите **Enter**.
- В полноэкранном режиме нажмите **Yes**.

Если вы хотите использовать настройки подключения ViPNet Coordinator HW к внешней сети из файла дистрибутива ключей:

- Введите `n` и нажмите **Enter**.
- Нажмите **No**.

  Мастер перейдет к проверке связи с другим узлом сети ViPNet (шаг 31).

28 Выберите режим подключения ViPNet Coordinator HW к внешней сети:

Внимание! Не рекомендуем использовать режимы подключения «Без использования межсетевого экрана» и «Координатор», так как они являются устаревшими и будут удалены в следующих версиях продукта. При выборе этих режимов возможна потеря связи с узлами.

Если вы выбрали один из этих режимов, внесите изменения в файл `iplir.conf`. Подробнее см. в документе «Настройка с помощью командного интерпретатора» раздел «Настройка параметров сетевого подключения координатора».

Вместо устаревших режимов рекомендуем использовать:

- режим «Со статической трансляцией адресов» вместо режима «Без межсетевого экрана»;
- режим «С динамической трансляцией адресов» вместо режима «Координатор».

- Чтобы выбрать режим **Без использования межсетевого экрана**:
  - Введите 1 и нажмите **Enter**.
  - Выберите режим **1 (No External Firewall)** и нажмите **Next**.
- Чтобы выбрать режим **Координатор**:
  - Введите 2 и нажмите **Enter**.
  - Выберите режим **2 (VPN Coordinator)** и нажмите **Next**.
- Чтобы выбрать режим **Со статической трансляцией адресов**:
  - Введите `3` и нажмите **Enter**.
  - Выберите режим **3 (Static NAT)** и нажмите **Next**.
- Чтобы выбрать режим **С динамической трансляцией адресов**:
  - Введите `4` и нажмите **Enter**.
  - Выберите режим **4 (Dynamic NAT)** и нажмите **Next**.

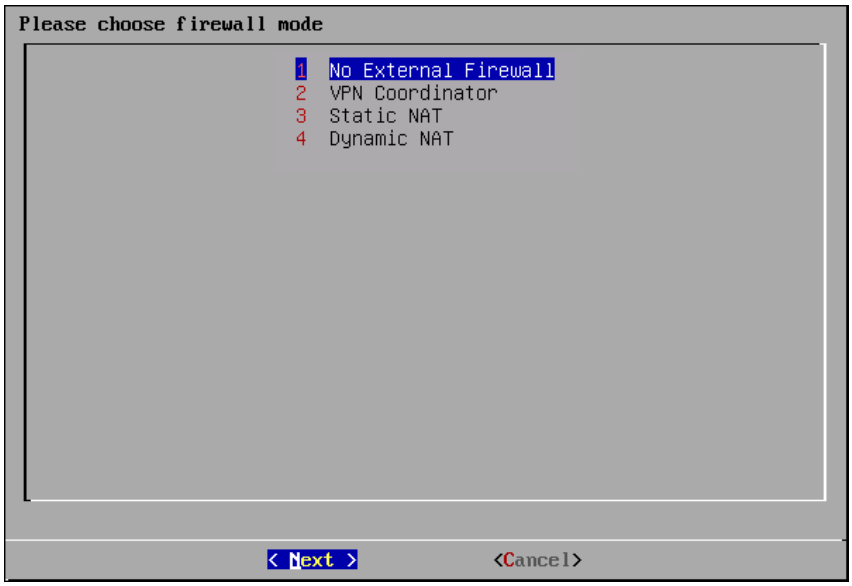


Рисунок 58. Выбор режима работы через межсетевой экран в полноэкранном режиме

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

29 Если вы выбрали режим **Со статической трансляцией адресов**:

29.1 По умолчанию для отправки и получения UDP-пакетов используется порт 55777. Чтобы изменить номер порта:

- В строке `Do you want to specify custom UDP port? [Yes/No]` введите `y` и нажмите **Enter**. Введите номер UDP-порта и нажмите **Enter**.
- Нажмите **Yes**. Введите номер UDP-порта и нажмите **Next**.

Примечание. Если через один межсетевой экран (или NAT-устройство) подключены несколько ViPNet Coordinator HW, то их номера UDP-портов должны быть разными.

29.1 Задайте фиксированный IP-адрес внешнего межсетевого экрана:

Внимание! При задании фиксированного адреса возможна потеря связи с узлами, находящимися за межсетевым экраном с динамической трансляцией адресов. Режим со статической трансляцией и фиксированным IP-адресом внешнего межсетевого экрана является устаревшим и будет удален в следующих версиях продукта.

- В строке `Do you want to specify fixed IP address of the external firewall? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес и нажмите **Enter**.
- Нажмите **Yes**. Введите IP-адрес и нажмите **Next**.

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

Мастер перейдет к проверке связи с другим узлом сети ViPNet (шаг 31).

30 Если вы выбрали режим **С динамической трансляцией адресов**:

30.1 Выберите координатор, через который ViPNet Coordinator HW будет подключаться к сети, как на шаге 29.2.

30.2 Если для выбранного координатора не указан IP-адрес, задайте его вручную, как на шаге 29.3.

Мастер перейдет к проверке связи с другим узлом сети ViPNet (шаг 31).

31 Выберите из списка сетевых узлов ViPNet, с которыми ViPNet Coordinator HW имеет связи, узел для проверки:

- В строке `Specify the sequence number of the VPN host [<диапазон цифр, соответствующих узлам в списке>] or [q] to cancel or press Enter for next page :` введите номер сетевого узла в списке и нажмите **Enter**.
- Выберите сетевой узел и нажмите **Next**.

Примечание. Информация о связях содержится в справочниках устанавливаемого дистрибутива ключей.

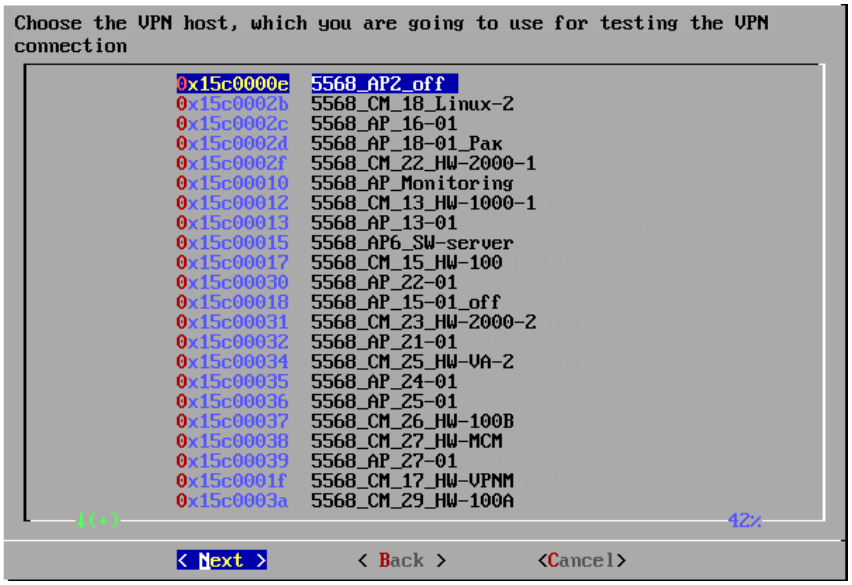


Рисунок 59. Выбор узла сети ViPNet для проверки связи в полноэкранном режиме

32 Если в справочниках устанавливаемого дистрибутива ключей не указан IP-адрес выбранного узла сети ViPNet, задайте его вручную:

- В строке `The IP address of the ViPNet host has not been found. Do you want to specify one? [Yes/No]` введите `y` и нажмите **Enter**. Введите IP-адрес и нажмите **Enter**.
- Нажмите **Yes**. Введите IP-адрес и нажмите **Next**.

33 Проверка связи с узлом сети ViPNet может занять несколько минут. Дождитесь сообщение о результатах проверки:

- Если связь с узлом сети ViPNet была установлена, все настройки, выполненные до проверки, сохраняются в конфигурационном файле `iplir.conf` ViPNet Coordinator HW. Для продолжения работы мастера нажмите **Enter** или **OK**.
- Если связь с узлом сети ViPNet установить не удалось, то для выяснения причины, просмотрите журнал регистрации IP-пакетов. Подробнее о работе с журналом регистрации IP-пакетов см. в документе «Настройка с помощью командного интерпретатора».

34 Запустите драйверы и службы ViPNet Coordinator HW перед завершением работы мастера:

- В строке `Do you want to start VPN services before leaving the installation wizard? [Yes/No]` введите `y` и нажмите **Enter**.
- Нажмите **Yes**.

35 Запустите командный интерпретатор ViPNet Coordinator HW:

- В строке `Do you want to start the command shell now? [Yes/No]` введите `y` и нажмите **Enter**.

- Нажмите **Run Command shell**.

Первичная настройка завершена, выполнено подключение к ViPNet Coordinator HW в режиме пользователя.

Теперь вы можете подключиться к ViPNet Coordinator HW в режиме администратора и использовать для настройки командный интерпретатор или веб-интерфейс. Подробнее см. документы «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса».

Если для сетевого интерфейса был задан режим DHCP, проверьте, что от DHCP-сервера получен маршрут по умолчанию:

- В командном интерпретаторе просмотрите таблицу маршрутизации:

  ```
  hostname> inet show routing
  ```

  Если маршрут по умолчанию не был получен, будет выведено предупреждение. В этом случае задайте статический маршрут по умолчанию (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка маршрутизации»).

- В разделе **Сетевые настройки** > **Маршрутизация** веб-интерфейса 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»).

Внимание! Убедитесь, что заданный в маршруте шлюз по умолчанию доступен для сетевого узла ViPNet Coordinator HW. Если шлюз по умолчанию окажется недоступен, некоторые функции ViPNet Coordinator HW не будут работать, например, виртуальные IP-адреса, обработка прикладных протоколов, сетевые службы и другие.

A

Термины и сокращения

DiffServ (Differentiated Service)

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

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 в одном широковещательном домене. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

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 Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задает связи между ними.
- ViPNet Rollout Center — модуль быстрого развертывания защищенных устройств ViPNet в больших распределенных сетях.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet StateWatcher

Программный комплекс 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.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

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 Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями.

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.

Дистрибутив ключей

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

Защищенный интернет-шлюз (открытый интернет)

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.

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.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В 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.

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).

Модуль ViPNet Network Visibility System

Функциональный модуль системы управления ViPNet Prime для сбора информации о состоянии устройств.

Модуль ViPNet Policy Management

Функциональный модуль системы ViPNet Prime для управления политиками безопасности устройств защищенной сети ViPNet.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

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 Prime. 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.

Политики безопасности

Набор параметров — сетевых фильтров и правил трансляции сетевых адресов, регулирующих безопасность сетевого узла.

Роль

Функциональность сетевого узла, которая решает целевые и служебные задачи 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.

Набор ролей для каждого сетевого узла задает администратор 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

Сетевой узел с ПО ViPNet, зарегистрированный в ViPNet Prime VPN.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на защищенные узлы ViPNet транспортным сервером MFTP.

Транспортный сервер MFTP

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

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Шлюзовой координатор

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

B

Изменения в документации

- **11.12.2024 — обновлены документы:**
  - **«Настройка с помощью командного интерпретатора»:**
    - Обновлены разделы «Локальное подключение к ViPNet Coordinator HW с помощью консоли», «Удаленное подключение к ViPNet Coordinator HW с помощью протокола SSH» и «Обновление ключей при истечении срока их действия». Уточнено примечание об истечении срока действия ключей. Добавлена информация о том, что для обновления ключей необходимо обращаться к администратору сети ViPNet.
    - Обновлены разделы «Параметры статической маршрутизации» и «Особенности обновления ПО» — добавлено примечание про проверку параметров маршрутизации при обновлении с версии 4.3.2.
    - Обновлен раздел «Развертывание кластера горячего резервирования» — добавлено описание ролей для использования ViPNet Coordinator VA в кластере.
    - В список терминов и сокращений добавлен термин «ключ обмена».
  - **«Настройка в браузере»:**
    - Обновлен раздел «Подключение к веб-интерфейсу». Уточнено примечание об истечении срока действия ключей.
    - Обновлен раздел «Параметры статической маршрутизации» — добавлено примечание о необходимости убедиться в том, что пакеты проходят от источника до пункта назначения и обратно через координатор.
    - В список терминов и сокращений добавлен термин «ключ обмена».
  - **«Подготовка к работе»:**
    - Актуализирована информация о поддержке ViPNet Coordinator HW10 в ViPNet Prime.
    - Обновлен раздел «Горячая замена» блоков питания». Актуализирована информация об индикации при неисправности блока питания.

- **«Смена мастер-ключей»:**

  Обновлен раздел «Подготовка к смене мастер ключей» — актуализирована информация о создании частичной резервной копии.

- **27.09.2024 — обновлен документ «Подготовка к работе»:**

  Обновлён раздел «Аппаратная платформа HW1000 Q10» — добавлено примечание о том, что нельзя использовать разъём питания на передней панели платформы.

- **19.09.2024 — обновлены документы «Настройка с помощью командного интерпретатора», «Настройка с помощью веб-интерфейса» и «Справочник команд и конфигурационных файлов»:**

  В разделы «Создание сетевого фильтра», «Создание и изменение сетевых фильтров» и «firewall add» соответственно добавлена информация о том, что в названии фильтра нельзя использовать символы на кириллице.

- **09.07.2024 — обновлен документ «Настройка с помощью командного интерпретатора»:**

  Обновлен раздел «Настройка подключения к веб-интерфейсу по протоколу HTTPS» — добавлен сценарий выгрузки самоподписанного сертификата и добавления сертификата в браузер как доверенного.

- **02.07.2024 — обновлены документы:**
  - **«Настройка с помощью командного интерпретатора»:**
    - Обновлено описание параметра checkonlyidle в разделе «Развертывание кластера горячего резервирования», добавлен раздел «Настройка параметра checkonlyidle» с описанием особенностей настройки.
    - Обновлен раздел «Особенности реализации L2OverIP» — добавлены особенности обработки туннелируемого трафика при настроенном L2OverIP.
  - **«Справочник команд и конфигурационных файлов»:**

    Обновлено описание параметра checkonlyidle в разделе «Файл failover.ini» > «Секция [channel]».

- **27.06.2024 — обновлены документы:**
  - **«Подготовка к работе»:**

    Добавлен раздел «Совместимое программное обеспечение».
  - **«Справочник команд и конфигурационных файлов»:**

    Обновлен раздел «inet show dhcp server» — актуализирован вывод команды в примере использования.

- **24.05.2024 — обновлен документ «Настройка с помощью командного интерпретатора»:**

  Обновлен раздел «Проверка ЭП файла обновления» — актуализирован список корневых и аннулированных сертификатов, которые нужны при проверке файла обновления.

- **17.05.2024 — обновлены документы:**
  - **«Подготовка к работе»:**

Обновлен раздел «Описание исполнений».

- **«Настройка с помощью командного интерпретатора»**:

  Обновлены разделы «Настройка модема вручную», «Создание пользовательской группы объектов».

- **«Справочник команд и конфигурационных файлов»**:

  Обновлен раздел «firewall add name».

- **13.05.2024 — обновлен документ «Перечень совместимых трансиверов».**
- **03.05.2024 — обновлены документы**:
  - **«Настройка с помощью командного интерпретатора»**

    Обновлен раздел «Установка серийного номера».

  - **«Справочник команд и конфигурационных файлов»**

    Раздел «serial» переименован в «machine serial» и перенесен в раздел «Команды группы machine».

  - **«Лицензионные соглашения на компоненты сторонних производителей»**
- **27.04.2024 — обновлен документ «Перечень совместимых трансиверов».**
- **19.04.2024 — обновлен документ «Справочник команд и конфигурационных файлов»:**

  Обновлен раздел «admin passwd».

- **26.03.2024 — обновлен документ «Перечень совместимых трансиверов».**
- **05.03.2024 — обновлен документ «Подготовка к работе»:**

  Обновлен раздел «Аппаратные платформы HW100 Q1/Q2».

- **29.02.2024 — обновлен документ «Подготовка к работе»:**

  Обновлены разделы «Аппаратная платформа HW2000 Q5», «Первичная настройка ViPNet Coordinator HW».

- **09.02.2024 — обновлен документ «Справочник команд и конфигурационных файлов»:**

  Обновлен раздел «service http-proxy cache».

- **02.02.2024 — выпущена документация к версии 4.5.6.**