ViPNet Coordinator HW 5

Подготовка к работе

Версия продукта: 5.3.2

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

infotecs

ФРКЕ.465614.003РЭ

Версия продукта 5.3.2

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

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 общие сведения о многофункциональном шлюзе безопасности ViPNet Coordinator HW:

- поддерживаемые функции;
- описание исполнений;
- условия лицензирования;
- возможности управления.

Также в документе приведены сценарии:

- установки ViPNet Coordinator VA на платформы виртуализации;
- установки дистрибутива ключей;
- инициализации ViPNet Coordinator HW и ViPNet Coordinator VA.

Документ предназначен для администраторов сетей ViPNet.

Комплект документации ViPNet Coordinator HW:

- Подготовка к работе.
- Настройка с помощью командного интерпретатора.
- Настройка с помощью веб-интерфейса.
- Справочник команд и конфигурационных файлов.
- Лицензионные соглашения на компоненты сторонних производителей.
- История версий.
- Перечень совместимых трансиверов.

Соглашения документа

Внимание! Все сценарии работы с ViPNet Coordinator HW приведены для локального администратора `admin` в режимах просмотра или настройки.

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приемы и хорошие практики
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, службы, интерфейса, путь или команда

Описание команд:

- Приглашение команд, которые могут быть выполнены аудитором или администратором в режиме просмотра, заканчивается символом `>`:

  ```
  hostname> firewall local show
  ```

- Приглашение команд, которые могут быть выполнены администратором в режиме настройки, заканчивается символом `#`:

  ```
  hostname# admin upgrade software
  ```

- Параметры, которые должны быть заданы аудитором или администратором, заключены в угловые скобки `<>`:

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

  При вводе в командный интерпретатор параметры вводятся без угловых скобок:

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

- Необязательные параметры или ключевые слова заключены в квадратные скобки `[]`:

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

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

  ```
  hostname# firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude
  110.35.14.3,110.35.14.13
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки `{}` и разделены вертикальной чертой `|`:

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

  При вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок:

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

- Идентификатор сетевого узла ViPNet указывается в шестнадцатеричном формате с префиксом `0x`:

  ```
  hostname# iplir ping 0x270e000a
  ```

Что нового в версии 5.3.2

Повышена стабильность работы ViPNet Coordinator HW. Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий ViPNet Coordinator HW.

Совместимость с продуктами ViPNet

Таблица 1. Совместимость с продуктами VPN-сети

Продукт	Версия
ViPNet Client 4 (Windows)	4.5.5
ViPNet Client 4U for Linux	4.15
ViPNet Client 4U for Android	4.0.0
ViPNet Client 4U for Windows	4.12.2
ViPNet Client 4U for iOS	4.1.0
ViPNet Client 4U for macOS	4.1.1
ViPNet Client 4U for Aurora	4.0.2
ViPNet Coordinator VA	4.3.3, 4.5.0–4.5.6
ViPNet Coordinator HW 4	4.3.2, 4.5.0–4.5.6
ViPNet Coordinator HW 5	5.1.2–5.2.1 (алгоритм шифрования по ГОСТ 28147–89)

Таблица 2. Совместимость с другими продуктами

Продукт	Версия
ViPNet Prime	1.7.2 и 1.9.5
ViPNet xFirewall	5.4.1–5.7.1
ViPNet TIAS	3.7.1 и 3.8
ViPNet PKI Client for Windows	1.6.1–1.7.0
ViPNet PKI Client for Linux	1.4–1.7

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

Назначение

ViPNet Coordinator HW 5 — многофункциональный шлюз безопасности, реализующий концепцию межсетевого экрана нового поколения NGFW (Next-Generation Firewall). В одном устройстве ViPNet Coordinator HW объединены совместно работающие функции безопасности:

- межсетевой экран с контролем состояния сессий SPI (Stateful Packet Inspection);
- межсетевой экран уровня приложений DPI (Deep Packet Inspection);
- модуль идентификации пользователей Active Directory или LDAP;
- прокси-сервер;
- средство предотвращения вторжений (IPS);
- VPN-шлюз, обеспечивающий построение VPN-сети на сетевом (L3) и канальном (L2) уровнях модели OSI.

ViPNet Coordinator HW поддерживает дополнительный набор сетевых функций: кластер высокой доступности, агрегирование интерфейсов, VLAN, расширенная маршрутизация трафика, резервирование и балансировка каналов связи, обеспечение QoS.

ViPNet Coordinator HW выпускается в нескольких исполнениях, в том числе для платформ виртуализации. Может использоваться в сетях различного масштаба (малый офис, предприятие, ЦОД) и топологии («сеть-сеть», «точка-сеть»).

Лицензирование ViPNet Coordinator HW позволяет задействовать только нужные на текущий момент функции и расширять их по мере развития сети.

Межсетевой экран

В межсетевом экране ViPNet Coordinator HW реализованы следующие механизмы информационной безопасности, присущие межсетевым экранам нового поколения:

- фильтрация трафика на сетевом и транспортном уровнях модели OSI с контролем состояния сессий;
- расширенная инспекция трафика (Deep Packet Inspection) с целью отслеживания активности приложений и прикладных протоколов;
- возможность определения политик безопасности на уровне пользователей служб каталогов Active Directory или LDAP.

Примечание. ViPNet Coordinator HW классифицирует каждую сессию по типу прикладного протокола один раз до истечения времени жизни сессии. При изменении списка правил классификация сессий по прикладному протоколу заново не проводится.

С помощью сетевых фильтров можно не только заблокировать нежелательные соединения, но и разрешить соединения с открытыми узлами, не входящими в сеть ViPNet. Помимо настраиваемых фильтров имеется защита от одной из распространенных сетевых атак — спуфинга.

Межсетевой экран может выполнять трансляцию сетевых адресов (NAT) для проходящего через него открытого трафика.

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

NAT позволяет решить две задачи:

- 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 ViPNet Coordinator HW.
- Доступ 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.

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

Прокси-сервер

ViPNet Coordinator HW может выполнять роль прокси-сервера для узлов локальной сети. Встроенный прокси-сервер имеет следующие возможности:

- Поддержка протоколов HTTP и FTP.
- Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP.
- Проверка трафика внешним антивирусом по протоколу ICAP.

Средство предотвращения вторжений (IPS)

Обнаружение вторжений основано на анализе туннелируемого и транзитного трафика правилами сигнатурного и эвристического метода — правилами IPS:

- Сигнатурный метод основан на поиске последовательностей, характерных для сетевых угроз — сигнатур. Правила поиска содержат:
  - Заголовки транспортных протоколов, по которым необходимо анализировать пакеты (протокол, IP-адреса и порты источника и получателя).
  - Заголовки и параметры прикладных протоколов.
  - Сигнатуры сетевых атак, которые могут содержаться в теле пакета.
- Эвристический метод основан на предварительной обработке IP-пакетов в соответствии с набором эвристик (алгоритмов, идентифицирующих отдельные сетевые угрозы по параметрам трафика) и обнаруживает:
  - Аномалии в служебных заголовках IP-пакетов.
  - Аномалии при декодировании и фрагментации IP-пакетов.
  - Попытки сканирования портов и удаленного выполнения произвольного кода.

База правил IPS регулярно обновляется специалистами ИнфоТеКС.

При обнаружении характерных признаков вторжения (срабатывании правила IPS) IP-пакет может быть блокирован межсетевым экраном или пропущен для дальнейшей обработки с предупреждением. Событие срабатывания правила IPS регистрируется в журнале IP-пакетов.

Средство IPS выявляет и предотвращает:

- Попытки эксплуатации уязвимостей в ПО объектов защищаемой сети.
- Атаки на сетевые службы и серверы.
- Атаки типа «отказ в обслуживании» (DoS-атаки).
- Аномальный IP-трафик.
- Сетевую активность вирусов.

VPN-шлюз

ViPNet Coordinator HW выполняет роль VPN-шлюза в виртуальной защищенной сети ViPNet, которая может быть развернута поверх локальных и глобальных IP-сетей. VPN-шлюз:

- позволяет создавать VPN-туннели на сетевом (L3) и канальном (L2) уровнях модели OSI между узлами сети ViPNet с помощью протоколов UDP, TCP и IP/241, в которые инкапсулируются пакеты любых других IP-протоколов;
- обеспечивает поддержку служебных функций сети ViPNet: VPN-маршрутизатора, сервера IP-адресов, сервера соединений и транспорта.

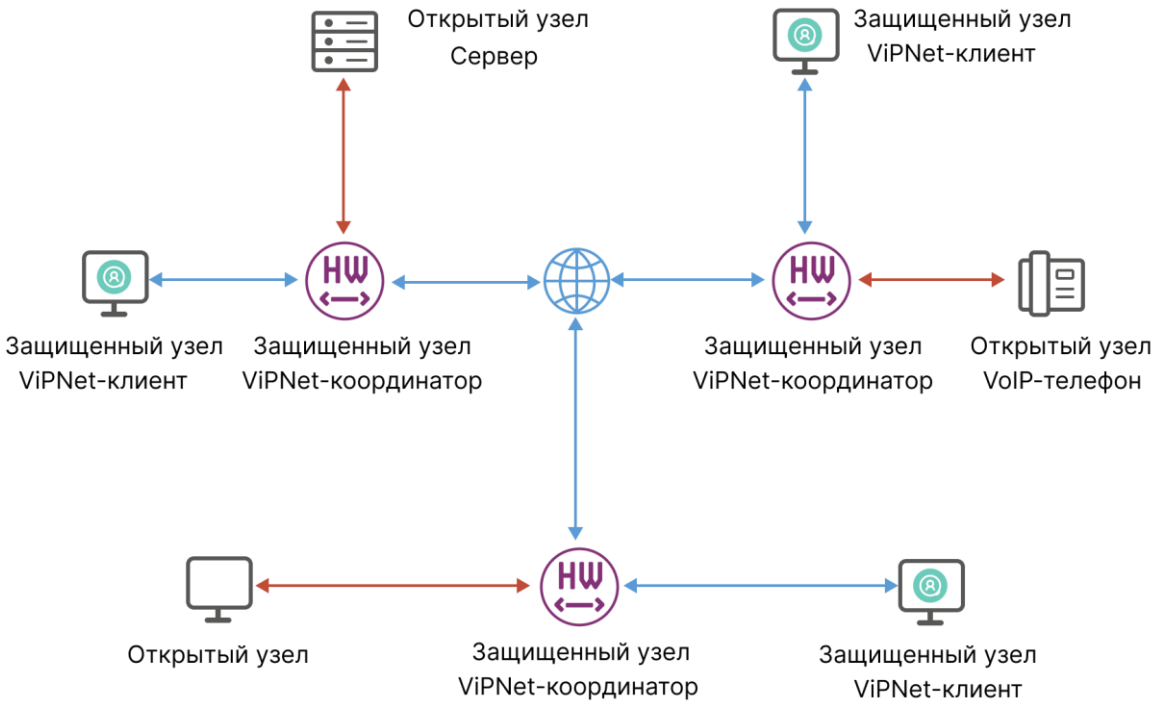

Рисунок 1. Типы узлов сети ViPNet

Туннелирование на сетевом уровне (L3)

На сетевом уровне VPN-туннели можно создавать между открытым и защищенным узлом или между двумя открытыми узлами, которые туннелируются разными координаторами. При этом:

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.

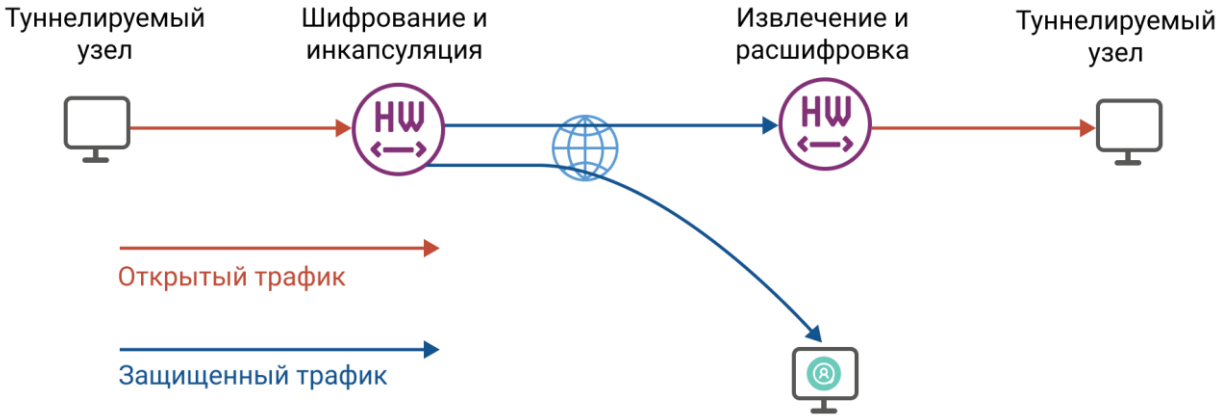

Рисунок 2. Защита соединения на сетевом уровне модели OSI

Туннелирование на канальном уровне (L2)

На канальном уровне VPN-туннели (L2OverIP) можно создавать между удаленными сегментами сети ViPNet так, что узлы сегментов будут находиться в одном широковещательном домене. При этом:

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.

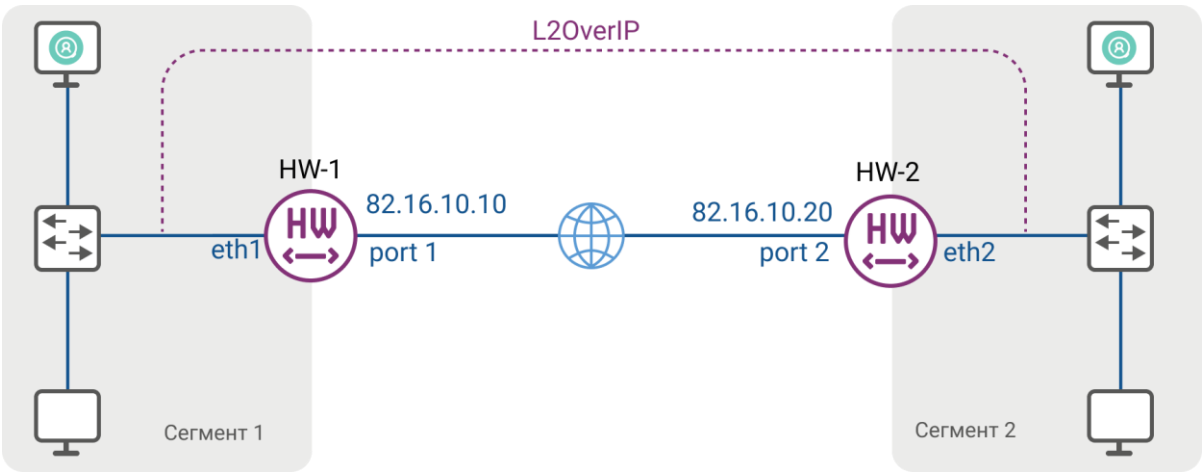

Рисунок 3. Защита соединения на канальном уровне модели OSI

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).

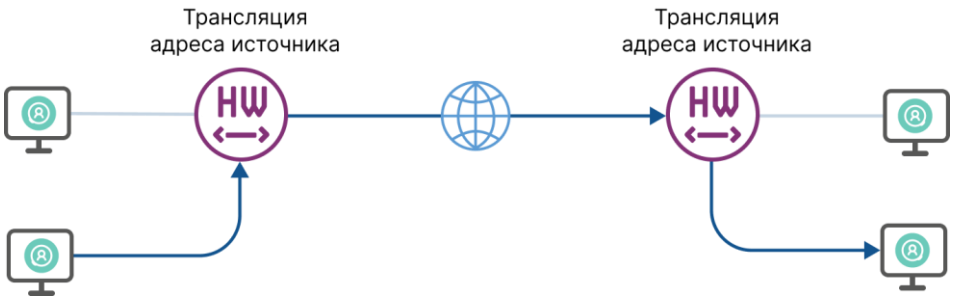

Рисунок 4. Функция маршрутизации защищенного трафика в сети ViPNet

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

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 Prime. Сервер IP-адресов можно сменить, выбрав другой координатор, с которым у данного клиента есть связь.

Сервер соединений

Когда на границе сети ViPNet установлено стороннее устройство, выполняющее фильтрацию и трансляцию трафика, клиенты не могут установить соединение напрямую. В таком случае соединение устанавливается через координатор, выполняющий функцию сервера соединений.

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.

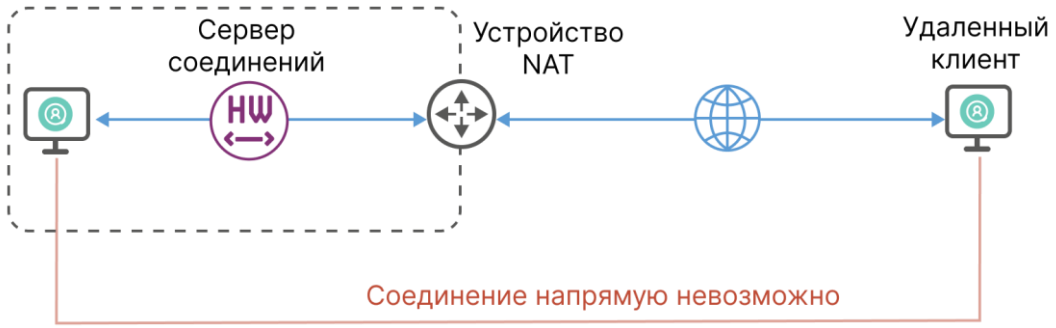

Рисунок 5. Организация соединений между сетевыми узлами ViPNet

Когда удалённый 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 по протоколу UDP.

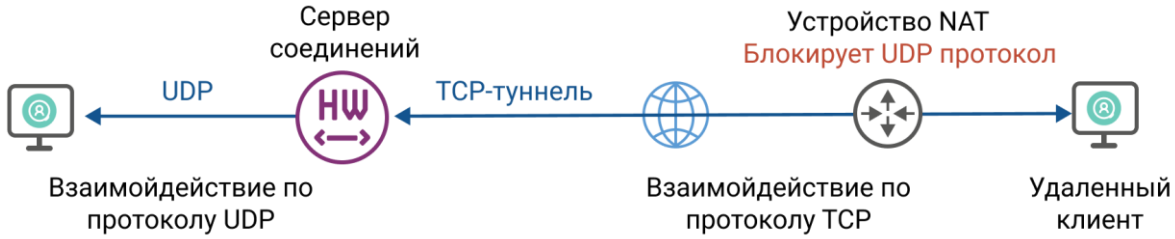

Рисунок 6. Доступ удаленного клиента к сети ViPNet через TCP-туннель

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.

Дополнительные сетевые функции

Дополнительные сетевые функции расширяют возможности обработки трафика, интеграции со сторонним оборудованием (коммутаторы, маршрутизаторы) и подключения к мобильным и беспроводным сетям:

- Поддержка VLAN IEEE 802.1Q.
- Агрегирование сетевых интерфейсов IEEE 802.3ad.
- Маршрутизация IP-трафика:
  - Статические маршруты.
  - Маршруты DHCP/PPP.
  - Динамическая маршрутизация: OSPFv2, BGP.
  - Маршрутизация на основе политик (PBR).
- Распределение нагрузки между каналами связи и резервирование каналов связи (MultiWAN).
- Обработка IP-трафика в соответствии с моделью QoS DiffServ.
- Встроенные DHCP-, DNS- и NTP-серверы.
- Подключение к 3G и Wi-Fi (IEEE 802.11 b/g) сетям (исполнения ViPNet Coordinator HW50 и ViPNet Coordinator HW100).

Кластер высокой доступности

Возможность отказоустойчивой работы обеспечивает объединение двух ViPNet Coordinator HW в кластер высокой доступности. Активный узел кластера выполняет функции ViPNet Coordinator HW, пассивный — находится в режиме ожидания. Особенности реализации кластера:

- Синхронизация сетевых фильтров, обеспечивающая полный набор фильтров активного узла на пассивном узле к моменту переключения кластера.
- Синхронизация открытых соединений, обеспечивающая непрерывную обработку транзитного трафика при переключении кластера.
- Использование виртуальных MAC-адресов сетевых интерфейсов кластера для быстрого восстановления соединения с сетевым оборудованием при переключении кластера.

Служебные функции

Транспортный клиент UT

Обеспечивает прием сообщений UT от транспортного сервера UT ViPNet Prime. Сообщение UT содержит один из компонентов:

- Политики безопасности.
- Обновление справочников и ключей ViPNet Coordinator HW.

Транспортный сервер MFTP

ViPNet-клиенты и ViPNet Coordinator HW версий ниже 5.0 обмениваются с ViPNet Prime транспортными конвертами MFTP. Если обмен настроен через ViPNet Coordinator HW, то для передачи конвертов используется транспортный сервер MFTP ViPNet Coordinator HW, работающий в транзитном режиме.

2

Описание исполнений

ViPNet Coordinator HW50

Исполнение ViPNet Coordinator HW50 может быть использовано для защиты небольших офисов и удаленных рабочих мест. Исполнение распространяется на аппаратных платформах HW50 N1, HW50 N2, HW50 N3 и HW50 N4.

Таблица 3. Характеристики HW50 N1, N2, N3, N4

Характеристика	HW50 N1, N2, N3	HW50 N4
Форм-фактор	Мини-компьютер	Мини-компьютер
Размеры корпуса (ШхВхГ)	125,1 x 22,5 x 122 мм	137 x 22,5 x 122 мм
Масса	0,5 кг	0,5 кг
Питание	Внешний блок питания, вх. 220 В, вых. 12 В, 3 А	Внешний блок питания, вх. 220 В, вых. 12 В, 3 А
Потребляемая мощность	9 Вт	9 Вт
Порты Ethernet RJ45	3 x 1 Гбит/с	3 x 1 Гбит/с
Wi-Fi	Только в HW50 N2	нет
3G	Только в HW50 N3	нет
Порты ввода-вывода	HDMI Консольный порт (RJ45) USB 2.0 USB 3.0	HDMI Консольный порт (RJ45) 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	

Рисунок 7. Передняя панель HW50 N1, N2, N3, N4

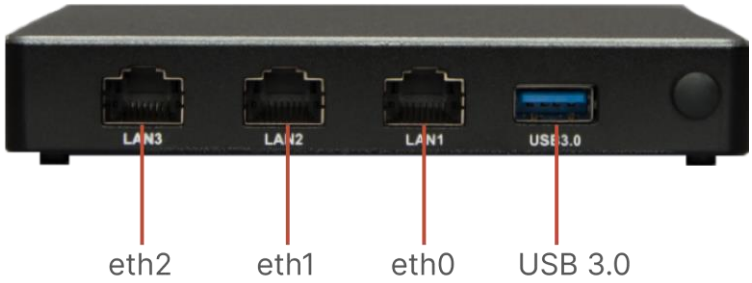

Рисунок 8. Задняя панель HW50 N1, N2, N3, N4

ViPNet Coordinator HW100

Исполнение ViPNet Coordinator HW100 применяется для защиты небольших офисов и удаленных рабочих мест. Исполнение распространяется на аппаратных платформах HW100 N1, HW100 N2, HW100 N3, HW100 Q1 и HW100 Q2.

Аппаратные платформы HW100 N1, N2, N3

Таблица 4. Характеристики HW100 N1, N2, N3

Характеристика	**HW100 N1, N2, N3**
Форм-фактор	Мини-компьютер
Размеры корпуса (ШхВхГ)	173,8 x 42 x 142,2 мм
Масса	0,5 кг
Блок питания	Внешний, вх. 220 В, вых. 24 В, 2,5 А
Потребляемая мощность	11 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP	1 x 1 Гбит/с
Wi-Fi	Только в HW100 N2
3G	Только в HW100 N3
Порты ввода-вывода	VGA Консольный порт (RJ45) USB 2.0 USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Консольный кабель COM-RJ45 Для HW100 N2 — внешняя антенна Wi-Fi Для HW100 N3 — внешняя антенна 3G

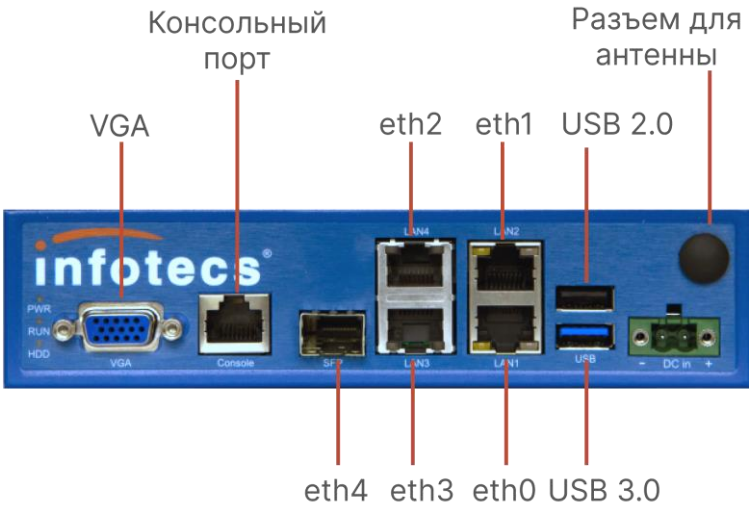

Рисунок 9. Передняя панель HW100 N1, N2, N3

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
Блок питания	Внешний, вх. 220 В, вых. 12 В
Потребляемая мощность	60 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP	2 x 1 Гбит/с
Порты ввода-вывода	VGA Консольный порт (RJ45) 2 x USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

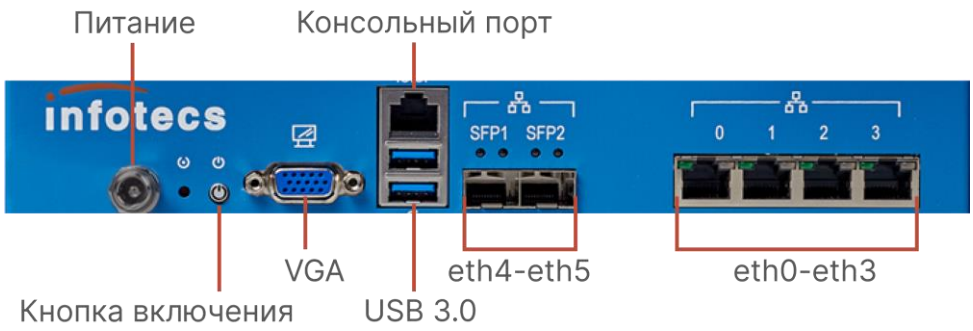

Рисунок 10. Передняя панель HW100 Q1, Q2

ViPNet Coordinator HW1000

Исполнения ViPNet Coordinator HW1000 могут быть использованы для защиты компьютерных сетей масштаба предприятия.

Таблица 6. Аппаратные платформы исполнений ViPNet Coordinator HW1000

Исполнение	Аппаратные платформы
ViPNet Coordinator HW1000	HW1000 Q4, Q7
ViPNet Coordinator HW1000 C	HW1000 Q5, Q8
ViPNet Coordinator HW1000 D	HW1000 Q6, Q9

Аппаратные платформы HW1000 Q4, Q5, Q6

Таблица 7. Характеристики HW1000 Q4, Q5, Q6

Характеристика	HW1000 Q4	HW1000 Q5	HW1000 Q6
Форм-фактор	19″ Rack 1U, укороченный корпус	19″ Rack 1U, укороченный корпус	19″ Rack 1U, укороченный корпус
Размеры корпуса (ШхВхГ)	430 x 44 x 380 мм	430 x 44 x 380 мм	430 x 44 x 380 мм
Масса	7,2 кг	7,2 кг	7,2 кг
Блок питания	250 Вт, 100–240 В	250 Вт, 100–240 В	250 Вт, 100–240 В
Потребляемая мощность	150 Вт	150 Вт	150 Вт
Порты Ethernet RJ45	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 Консольный порт (DB9-M) 4 x USB 2.0 2 x USB 3.0	2 x VGA Консольный порт (DB9-M) 4 x USB 2.0 2 x USB 3.0	2 x VGA Консольный порт (DB9-M) 4 x USB 2.0 2 x USB 3.0

Рисунок 11. Передняя панель HW1000 Q4, Q5, Q6

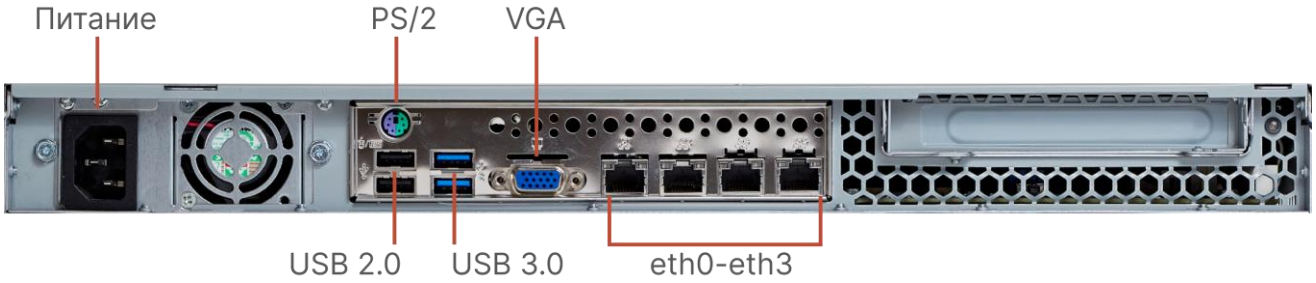

Рисунок 12. Задняя панель HW1000 Q4

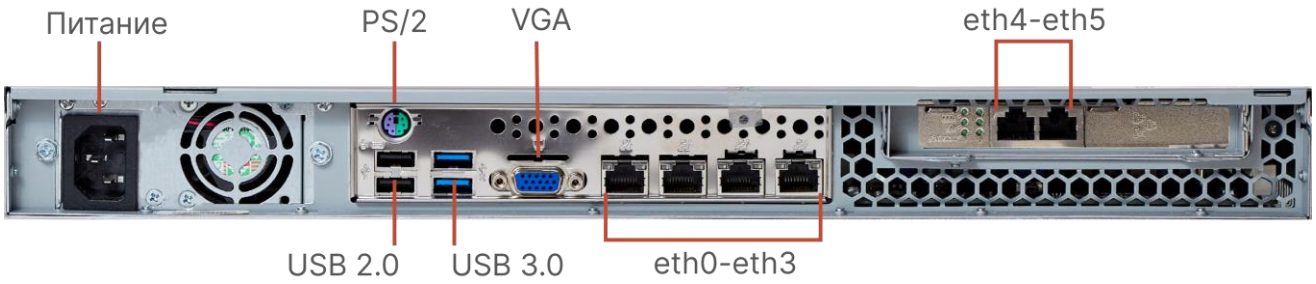

Рисунок 13. Задняя панель HW1000 Q5

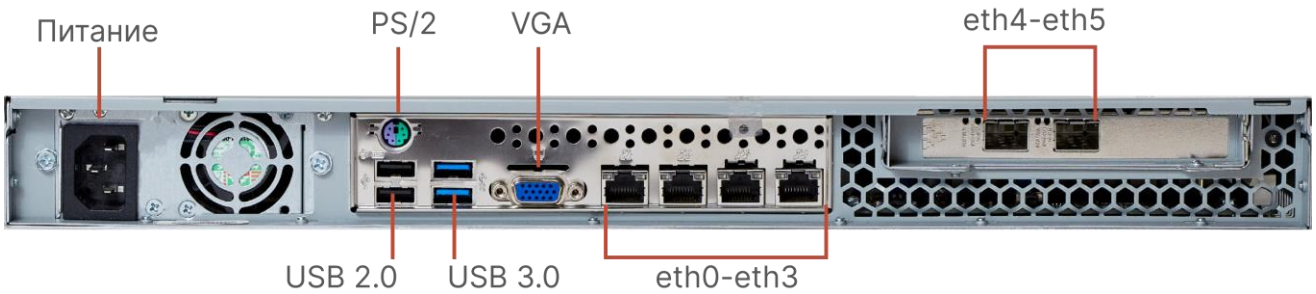

Рисунок 14. Задняя панель HW1000 Q6

Аппаратные платформы HW1000 Q7, Q8, Q9

Таблица 8. 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)	430 x 44 x 453 мм	430 x 44 x 453 мм	430 x 44 x 476 мм
Масса	7 кг	7 кг	8 кг
Блок питания	250 Вт	250 Вт	2 x 300 Вт с «горячей» заменой
Потребляемая мощность	215 Вт	230 Вт	230 Вт
Порты Ethernet RJ45	6 x 1 Гбит/с	8 x 1 Гбит/с	8 x 1 Гбит/с
Порты Ethernet SFP	нет	нет	4 x 1 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) 6 x USB 3.1	VGA Консольный порт (DB9-M) 6 x USB 3.1	VGA Консольный порт (DB9-M) 6 x USB 3.1
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку		Два кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

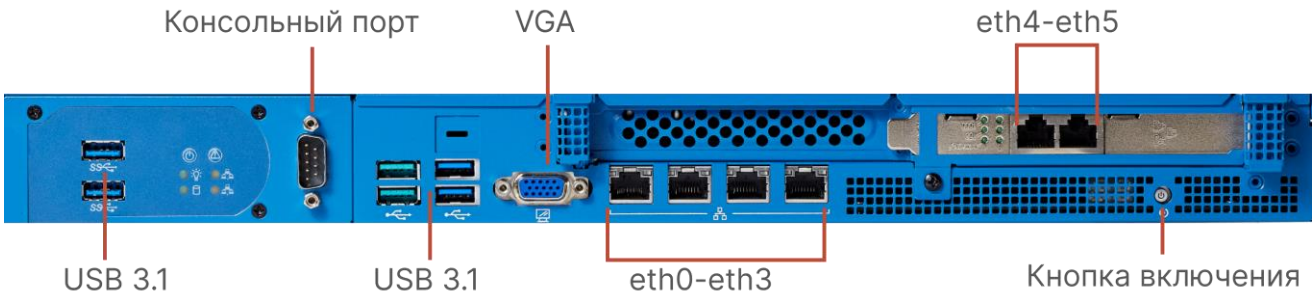

Рисунок 15. Передняя панель HW1000 Q7

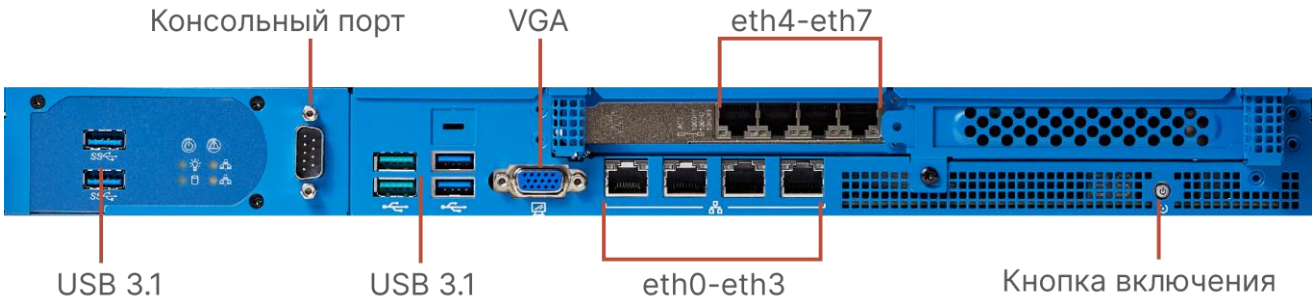

Рисунок 16. Передняя панель HW1000 Q8

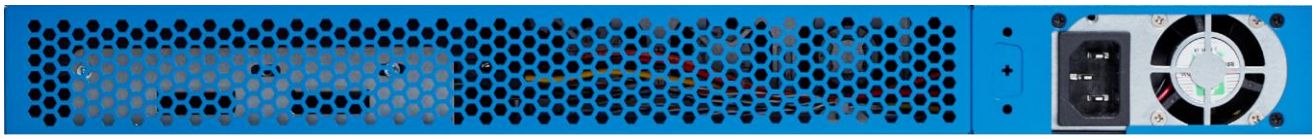

Рисунок 17. Задняя панель HW1000 Q7, Q8

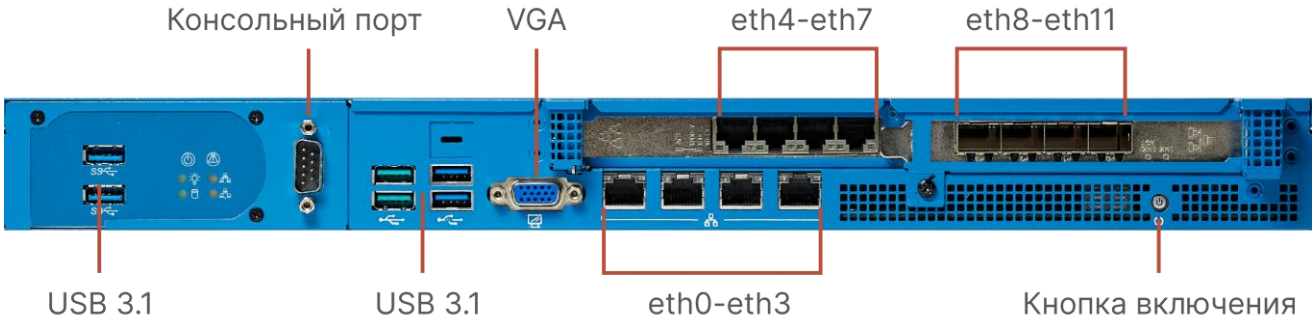

Рисунок 18. Передняя панель HW1000 Q9

Рисунок 19. Задняя панель HW1000 Q9

ViPNet Coordinator HW2000

Исполнение ViPNet Coordinator HW2000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных и к облачным ресурсам. Исполнение распространяется на аппаратных платформах HW2000 Q4 и HW2000 Q5.

Аппаратная платформа HW2000 Q4

Таблица 9. Характеристики HW2000 Q4

Характеристика	Описание
Форм-фактор	19" Rack 1U, укороченный корпус
Размеры корпуса (ШхВхГ)	444 x 44 x 380 мм
Масса	8 кг
Блок питания	500 Вт, 100-127 В/200-240 В
Потребляемая мощность	310 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) PS/2-порт для подключения клавиатуры или мыши 2 x USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

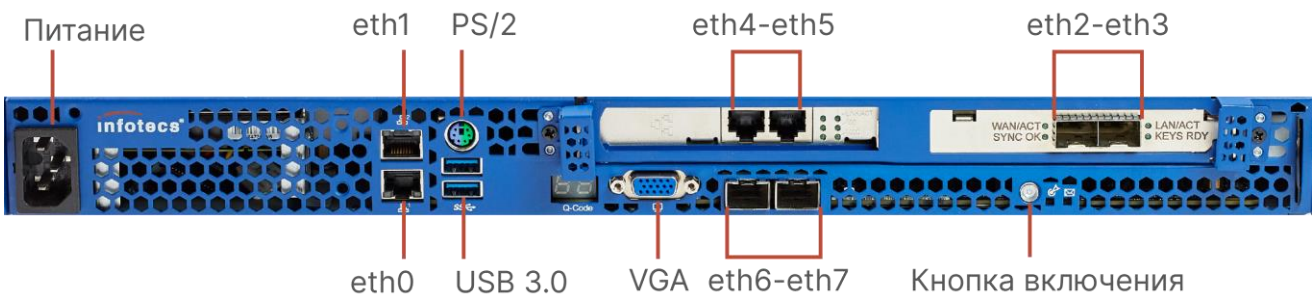

Рисунок 20. Передняя панель HW2000 Q4

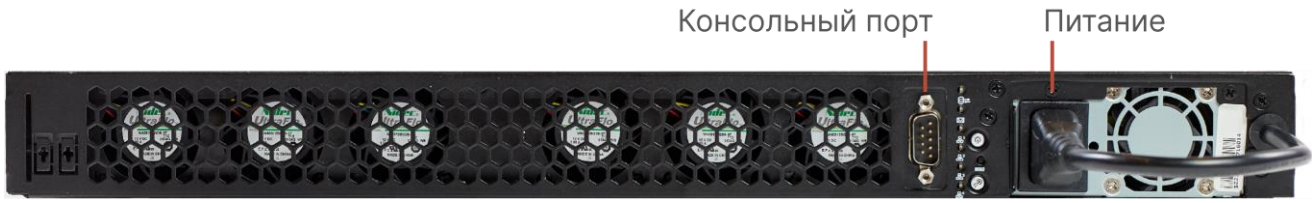

Рисунок 21. Задняя панель HW2000 Q4

Аппаратная платформа HW2000 Q5

Таблица 10. Характеристики HW2000 Q5

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	430 x 44 x 476 мм
Масса	8 кг
Блок питания	2x 300 Вт с «горячей» заменой
Потребляемая мощность	230 Вт
Порты Ethernet RJ45	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 Консольный порт (DB9-M) 6 x USB 3.1
Дополнительное оборудование	Два кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

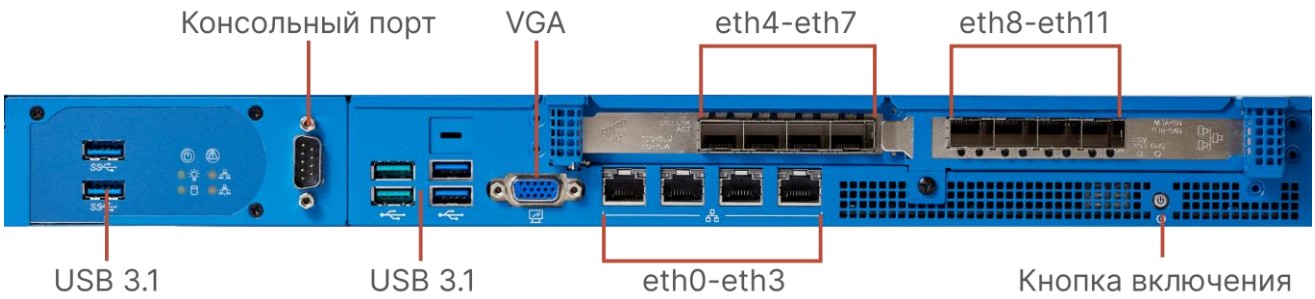

Рисунок 22. Передняя панель HW2000 Q5

На задней панели HW2000 Q5 расположены разъемы блоков питания.

Рисунок 23. Задняя панель HW2000 Q5

ViPNet Coordinator HW5000

Исполнение ViPNet Coordinator HW5000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных и к облачным ресурсам. Исполнение распространяется на аппаратных платформах HW5000 Q1 и HW5000 Q2.

Аппаратная платформа HW5000 Q1

Таблица 11. Характеристики HW5000 Q1

Характеристика	Описание
Форм-фактор	19″ Rack 1U, укороченный корпус
Размеры корпуса (ШхВхГ)	444 x 44 x 380 мм
Масса	8 кг
Блок питания	500 Вт, 100-127 В/200-240 В
Потребляемая мощность	310 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP+	4 x 10 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) PS/2-порт для подключения клавиатуры или мыши 2 x USB 3.0
Дополнительное оборудование	Кабель питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

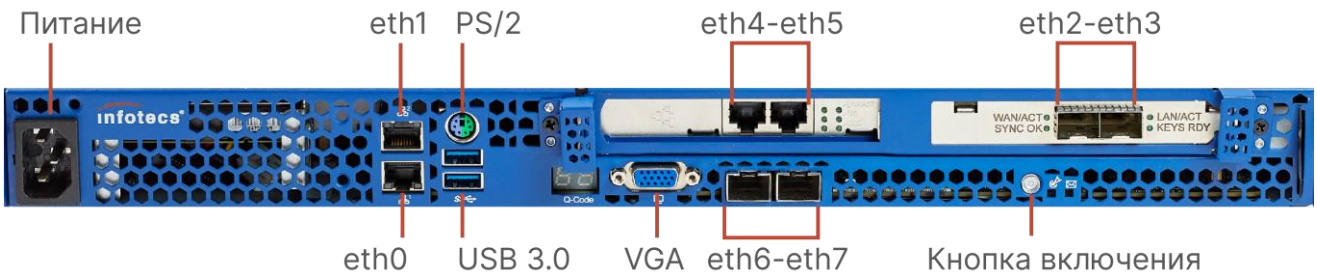

Рисунок 24. Передняя панель HW5000 Q1

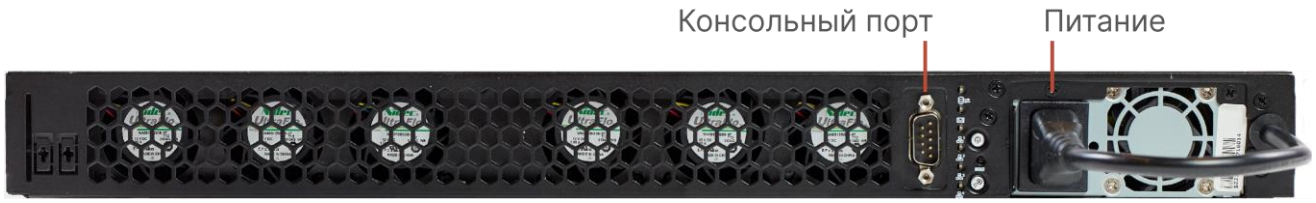

Рисунок 25. Задняя панель HW5000 Q1

Аппаратная платформа HW5000 Q2

Таблица 12. Характеристики HW5000 Q2

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры корпуса (ШхВхГ)	430 x 44 x 476 мм
Масса	8 кг
Блок питания	2x 300 Вт с «горячей» заменой
Потребляемая мощность	274 Вт
Порты Ethernet RJ45	4 x 1 Гбит/с
Порты Ethernet SFP+	8 x 10 Гбит/с
Порты ввода-вывода	VGA Консольный порт (DB9-M) 6 x USB 3.1
Дополнительное оборудование	2 кабеля питания CEE 7/7 Schuko - IEC-320-C13 Комплект для крепления в стойку

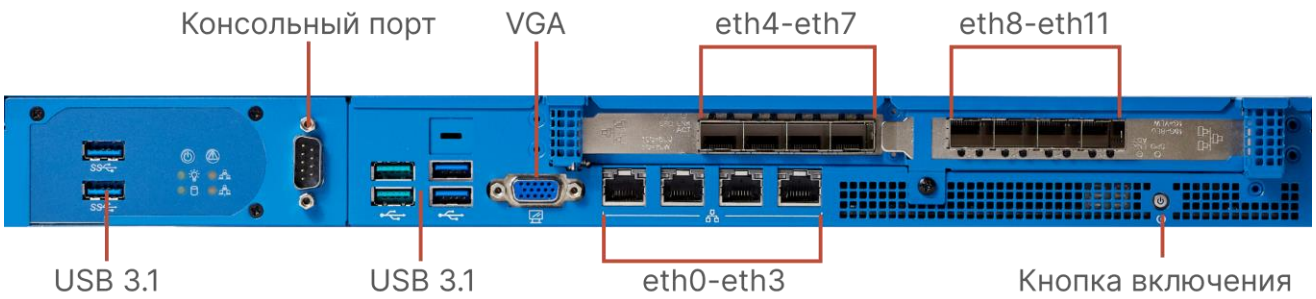

Рисунок 26. Передняя панель HW5000 Q2

На задней панели HW5000 Q2 расположены разъемы блоков питания.

Рисунок 27. Задняя панель HW5000 Q2

ViPNet Coordinator VA

ViPNet Coordinator VA распространяется в виде виртуальной машины, которая устанавливается на платформы виртуализации:

- KVM, например Qemu-KVM или Proxmox VE (см. Proxmox VE).
- VMware vSphere ESXi 6.7/7.0 (см. VMware vSphere ESXi).
- VMware Workstation Pro 15.x, 16.x (см. VMware Workstation Pro).
- Microsoft Hyper-V Server 2016/2019 (см. Microsoft Hyper-V).
- Oracle VM Server 3.4 (см. Oracle VM Server).
- Oracle VM VirtualBox 6.1.30 (см. Oracle VM VirtualBox).
- SharxBase 5.10.5 (см. SharxBase).

Внимание! Перед установкой виртуальной машины ViPNet Coordinator VA обновите ПО платформы виртуализации до последней версии и установите рекомендуемые обновления безопасности.

Виртуальная машина поставляется в виде файлов форматов `VHD`, `AMI`, `RAW`, `Qcow2` и `OVA` с частично предустановленным профилем аппаратных средств:

- Количество ядер процессора — 2 шт.
- Оперативная память — 2 Гбайт.
- Основной HDD — 4 Гбайт.
- Дополнительный HDD — 80 Гбайт.
- Сетевые интерфейсы — 4 шт.

Производительность исполнения ViPNet Coordinator VA определяется лицензией. При установке ViPNet Coordinator VA на платформу виртуализации настройте профиль аппаратных средств виртуальной машины в соответствии с рекомендуемыми параметрами. Установка параметров, превышающих рекомендованные, не приведет к увеличению производительности.

Таблица 13. Рекомендуемые параметры профиля аппаратных средств для объектов лицензирования: основной + VPN

Основной объект лицензирования	Количество ядер процессора, шт.	Оперативная память, Гбайт	Скорость интерфейсов, Гбит/с
Coordinator VA100	2	4	1
Coordinator VA500	4	4	10
Coordinator VA1000	6	6	10
Coordinator VA2000	8	8	10
Coordinator VA5000	12	12	10

Таблица 14. Рекомендуемые параметры профиля аппаратных средств для объектов лицензирования: основной + VPN +DPI + IPS

Основной объект лицензирования	Количество ядер процессора, шт.	Оперативная память, Гбайт	Скорость интерфейсов, Гбит/с
Coordinator VA100	4	4	1
Coordinator VA500	4	8	10
Coordinator VA1000	8	12	10
Coordinator VA2000	12	16	10
Coordinator VA5000	16	32	10

Дополнительные настройки:

- Если на ViPNet Coordinator VA планируется использование агрегированного сетевого интерфейса, настройте его на платформе виртуализации.
- Для достижения заявленной производительности ViPNet Coordinator VA:
  - Сопоставьте сетевому интерфейсу ViPNet Coordinator VA физический сетевой адаптер средствами платформы виртуализации.
  - Используйте функции платформ виртуализации DirectPath или SR-IOV с сетевыми адаптерами, поддерживающими разделение RSS.

Функциональные ограничения исполнений

Сетевые интерфейсы

Максимальное количество сетевых интерфейсов:

- для всех исполнений, кроме ViPNet Coordinator HW50 — 128;
- ViPNet Coordinator HW50 — 32.

Количество сетевых интерфейсов определенных типов:

- `eth` — физические интерфейсы Ethernet аппаратной платформы или интерфейсы Ethernet виртуальной машины;
- `bond` — до 8;
- `wlan` — 1;
- `vlan` и `alias` — в сумме с другими интерфейсами не превышает максимального количества интерфейсов.

Туннелирование на канальном уровне

Не поддерживается в исполнении ViPNet Coordinator HW50.

Динамическая маршрутизация

Протокол OSPF не поддерживается в исполнении ViPNet Coordinator HW50.

Рекомендованное количество сетевых фильтров

Рекомендованное количество сетевых фильтров ViPNet Coordinator HW зависит от их сложности. Превышение этого количества может нарушить работоспособность ViPNet Coordinator HW.

- **Малая сложность**. В фильтре вы можете указать по одному адресу источника и получателя IP-пакетов или одно приложение. В качестве адреса вы можете использовать IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску подсети, доменное имя сети и др.

  ```
  firewall forward add src 172.168.13.33 dst yandex.ru pass
  ```

  В качестве приложения вы можете указывать прикладные приложения, например, Skype или Facebook.

  ```
  firewall forward add src @any dst @any dpiapp Skype pass
  ```

- **Средняя сложность**. В фильтре вы можете указать до пятнадцати адресов источника и получателя (одиночные или в составе групп IP-адресов), протоколы (одиночные или в составе групп протоколов) и приложения.

  ```
  firewall forward add src 172.168.13.33,17.18.1.66,@Accountants dst @any service SSH
  dpiapp Skype,Facebook,Youtube pass
  ```

- **Высокая сложность**. В фильтре вы можете указать до тридцати пользователей Active Directory или Captive Portal, одну группу приложений и до сорока приложений.

  ```
  firewall forward add src @any dst @any dpigroup Messaging dnuser
  Ivanov.I,Petrov.P,Sidoriv.S pass
  ```

  ```
  firewall forward add src @any dst @any dpiapp
  Gadu-Gadu,Facebook,Paltalk,VK,WeChat,WhatsApp,Zalo dnuser
  Ilyina.E,Ivanov.I,Pavlov.K,Petrova.P,Popov.D.A.,Sidorov.S,Smirnova.D,Sokolov.P
  pass
  ```

Таблица 15. Рекомендованное количество сетевых фильтров ViPNet Coordinator HW

Аппаратная платформа	Малая сложность	Средняя сложность	Высокая сложность
HW50 N1, N2, N3, N4	1500	300	10
HW100 N1, N2, N3, Q1, Q2	2900	600	30
HW1000 Q4, Q7	20000	4000	150
HW1000 Q5, Q6, Q8, Q9	27000	5500	160
HW2000 Q4, Q5	30000	6000	170
HW5000 Q1, Q2	32000	7000	180

Таблица 16. Рекомендованное количество сетевых фильтров ViPNet Coordinator VA

Базовая лицензия	Малая сложность	Средняя сложность	Высокая сложность
Coordinator VA100	1500	300	10
Coordinator VA500	2900	600	30
Coordinator VA1000	20000	4000	150
Coordinator VA2000	27000	5500	160
Coordinator VA5000	30000	6000	170

Рекомендованное количество ViPNet-клиентов и связей с ViPNet-узлами

Таблица 17. Рекомендованное количество ViPNet-клиентов и связей ViPNet Coordinator HW

Аппаратная платформа	Оптим. число клиентов на координаторе	Макс. количество связей с ViPNet-узлами	Макс. количество связей с туннелирующими координаторами	Макс. количество заданных диапазонов туннелируемых узлов
HW50 N1, N2, N3, N4	0	500	50	1000
HW100 N1, N2, N3, Q1, Q2	10	1000	50	1000
HW1000 Q4, Q7	500	5000	100	1000
HW1000 Q5, Q6, Q8, Q9	1000	10000	1000	1000
HW2000 Q4, Q5	5000	15000	5000	1000
HW5000 Q1, Q2	6000	15000	5000	1000

Таблица 18. Рекомендованное количество ViPNet-клиентов и связей ViPNet Coordinator VA

Базовая лицензия	Оптим. число клиентов на координаторе	Макс. количество связей с ViPNet-узлами	Макс. количество связей с туннелирующими координаторами	Макс. количество заданных диапазонов туннелируемых узлов
Coordinator VA100	100	100	50	1000
Coordinator VA500	500	500	250	1000
Coordinator VA1000	1000	1000	500	1000
Coordinator VA2000	2000	2000	1000	1000
Coordinator VA5000	3000	3000	1500	1000

Меры безопасности при эксплуатации исполнений на аппаратных платформах

1. Исполнения ViPNet Coordinator HW в форм-факторе 1U предназначены для установки в телекоммуникационные 19" стойки. Во избежание повреждения ViPNet Coordinator HW используйте для монтажа в стойку специальные направляющие.
2. Не загораживайте и не накрывайте вентиляционные отверстия на передней и задней панелях ViPNet Coordinator HW. В исполнениях ViPNet Coordinator HW в форм-факторе 1U забор воздуха выполняется со стороны передней панели, отвод — со стороны задней панели. Для обеспечения надлежащей вентиляции необходимо обеспечить зазор не менее 15 см до передней и задней панелей. Зазоры для обеспечения вентиляции не требуются со стороны боковых, верхней и нижней частей ViPNet Coordinator HW.
3. Для подключения ViPNet Coordinator HW к электросети используйте кабели, входящие в комплект поставки. Подключение допускается только с использованием предназначенных для этого разъёмов.
4. ViPNet Coordinator HW должен быть заземлен. Не используйте для подключения незаземлённые электрические розетки.
5. При подключении электропитания к ViPNet Coordinator HW сначала подключайте кабели к оборудованию, затем к электрической сети.
6. Не допускайте воздействия на ViPNet Coordinator HW сильных магнитных полей, пыли, жидкостей, дождя и прямого солнечного света.

3

Лицензирование

Объекты лицензирования

Функции ViPNet Coordinator HW в сети ViPNet и возможности по обработке трафика определяются лицензией. Она состоит из основного и дополнительных объектов лицензирования. Лицензия назначается в ViPNet Prime.

Основной объект лицензирования соответствует определенному исполнению ViPNet Coordinator HW и разрешает:

- Установку VPN-соединения с ViPNet Prime.
- Настройку сетевых интерфейсов.
- Настройку маршрутизации.
- Настройку фильтрации открытого локального и открытого транзитного трафика по IP-адресам и транспортным протоколам.
- Настройку DHCP-, NTP-, DNS-серверов и DHCP-relay.
- Обновление ПО и лицензий ViPNet Coordinator HW.

Дополнительные объекты лицензирования разрешают:

- VPN:
  - Регистрацию ViPNet-клиентов.
  - Установку туннелируемых соединений на сетевом и канальном уровнях.
  - Настройку фильтрации защищенного трафика.
- DPI:
  - Идентификацию прикладных протоколов, приложений и их групп.
  - Идентификацию пользователей Active Directory и Captive Portal.
  - Фильтрацию туннельного и транзитного трафика по прикладным протоколам, приложениям и их группам, а также идентифицированным пользователям сети.
- Обновление DPI: обновление подсистемы DPI для идентификации новых, ранее не определяемых прикладных протоколов, приложений и их групп.
- IPS: обработку транзитного и туннелируемого трафика правилами IPS для обнаружения и предотвращения вторжений.
- Обновление IPS: обновление базы правил IPS для обнаружения и предотвращения новых, ранее не определяемых типов вторжений.
- Кластер высокой доступности: работу системы защиты от сбоев в режиме кластера.

Ограничения по окончании срока действия объектов лицензирования

Лицензии на использование ViPNet Coordinator HW могут быть срочными (с ограничением срока действия) и бессрочными. В случае истечения срока действия лицензии ViPNet Coordinator HW будет работать с ограничениями.

Таблица 19. Функциональные ограничения работы ViPNet Coordinator HW по окончании срока действия объектов лицензирования

Объект лицензирования	Функциональные ограничения
Основной	• Блокируется транзитный открытый и защищенный трафик • Заканчивается действие дополнительных лицензий • Разрешено удаленное обновление лицензий
VPN	• Прекращается обслуживание зарегистрированных ViPNet-клиентов и регистрация новых • Закрываются установленные туннелируемые соединения сетевого и канального уровней; установка новых соединений запрещается • Блокируется защищенный трафик
DPI	• Сетевые фильтры с параметрами прикладных протоколов, приложений и их групп, а также идентифицированными пользователями AD и CP — далее параметрами DPI, деактивируются • Запрещено создание новых сетевых фильтров с параметрами DPI
Обновление DPI	• Прекращается обновление подсистемы DPI
IPS	• Прекращается обработка транзитного и туннелируемого трафика правилами IPS
Обновление IPS	• Прекращается обновление базы правил IPS
Кластер	• Сохраняется работоспособность узлов кластера и синхронизации настроек, кроме автоматического переключения • Возможно ручное переключение узлов кластера в командном интерпретаторе

4

Возможности управления

Способы управления

Управление с помощью ViPNet Prime

ViPNet Prime используется администратором сети ViPNet для формирования структуры сети ViPNet, задания основных параметров сетевых узлов, централизованной отправки справочников, ключей и обновлений ПО на сетевые узлы ViPNet.

Также с помощью ViPNet Prime вы можете:

- задать адреса доступа к ViPNet Coordinator HW, параметры подключения ViPNet Coordinator HW к внешней сети, адреса туннелируемых узлов;
- сформировать и переслать на ViPNet Coordinator HW политики безопасности.

Подробнее об управлении ViPNet Coordinator HW см. документ «ViPNet Prime. Руководство администратора».

Управление с помощью веб-интерфейса

Подключение к ViPNet Coordinator HW с помощью веб-интерфейса по протоколам HTTP и HTTPS разрешено только с защищенных узлов ViPNet, связанных с ним.

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких узлов ViPNet с различными типами учетных записей; количество подключений не ограничено.

В веб-интерфейсе доступна частичная настройка ViPNet Coordinator HW:

- Настройка подключения ViPNet Coordinator HW к сети, настройка сетевых интерфейсов и параметров подключения к сетям 3G/4G, Wi-Fi.
- Настройки сетевых фильтров и правил трансляции адресов.
- Настройка подключения к домену AD и сервису аутентификации CP.
- Настройка туннелирования адресов.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера, DHCP-relay.
- Настройка L2OverIP.
- Настройка предотвращения вторжений IPS; обновление базы правил IPS.
- Настройка маршрутизации: статические маршруты, DHCP/PPP, OSPF, BGP.
- Настройка MultiWAN.
- Просмотр списка сетевых узлов ViPNet.
- Настройка параметров удаленного мониторинга по протоколу SNMP.
- Настройка даты и времени.

- Управление ключами локального SSH-сервера.
- Управление локальными учетными записями администратора (`admin`) и аудитора (`user`).
- Создание резервной копии индивидуальной конфигурации на внешнем устройстве.
- Настройка расписания резервного копирования индивидуальной конфигурации на ViPNet Prime.
- Восстановление из резервной копии индивидуальной конфигурации.
- Экспорт и импорт настроек индивидуальной конфигурации.
- Мониторинг состояния ViPNet Coordinator HW, настройка ведения журналов и их просмотр.

Управление с помощью командного интерпретатора

Командный интерпретатор запускается автоматически после аутентификации на ViPNet Coordinator HW. При этом он может быть запущен как локально с помощью COM-консоли или обычной консоли, так и удаленно при подключении по SSH с других узлов сети ViPNet, связанных с ViPNet Coordinator HW.

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких защищенных узлов с различными типами учетных записей; количество подключений — не более 32.

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

- Настройка VPN: режимы подключения ViPNet Coordinator HW к сети и управление конфигурациями VPN.
- Настройка системы защиты от сбоев.
- Настройка транспортного сервера MFTP в транзитном режиме.
- Обновление ПО ViPNet Coordinator HW.
- Обновление подсистемы DPI.

Роли и учетные записи пользователей

Для разграничения доступа к ViPNet Coordinator HW используются роли:

- Администратор — наделяет полномочиями:
  - изменения настроек;
  - обновления ПО ViPNet Coordinator HW;
  - просмотра настроек и аудита событий.
- Аудитор — наделяет полномочиями просмотра настроек и аудита событий.

ViPNet Coordinator HW поддерживает учетные записи пользователей двух типов:

- Локальные — две встроенные учетные записи пользователей `user` и `admin`, которым назначены роли аудитора и администратора соответственно:
  - Учетная запись `user` (пароль по умолчанию — `user`) используется на шаге 2 инициализации ViPNet Coordinator HW. После инициализации учетная запись блокируется, а ее пароль сбрасывается. Если вы предполагаете использовать учетную запись `user` для аудита ViPNet Coordinator HW, разблокируйте ее (см. После инициализации).
  - Учетная запись `admin` (пароль по умолчанию не задан) используется для просмотра и настройки параметров, обновления ПО и аудита событий ViPNet Coordinator HW. Пароль учетной записи `admin` необходимо задать при инициализации ViPNet Coordinator HW.

  

  Примечание. Изменить имена локальных учетных записей `user` и `admin`, их роли или добавить другие локальные учетные записи невозможно.
- Централизованные — учетные записи пользователей ViPNet Coordinator HW с ролями аудитора и администратора, созданные в ViPNet Prime. Ограничения на количество централизованных учетных записей нет.

Аутентификация пользователей

ViPNet Coordinator HW поддерживает два способа аутентификации пользователей — по паролю или по сертификату. Способ аутентификации устанавливается в ViPNet Prime для всей сети ViPNet.

Для аутентификации по сертификату применяются USB-токены:

- Рутокен ЭЦП 2.0 (2000, 2100, 2200, 3000, 4500);
- Рутокен ЭЦП 3.0 (3100);
- JaCarta-2 ГОСТ.

На USB-токене хранятся сертификат и закрытый ключ пользователя. Для доступа к USB-токену используются:

- ПИН администратора — задается средствами изготовителя USB-токена.
- ПИН пользователя:
  - Для локальных пользователей `user` и `admin` задается на ViPNet Coordinator HW.
  - Для централизованных пользователей задается средствами изготовителя USB-токена.

Для исполнения ViPNet Coordinator VA аутентификация по сертификату доступна на платформах виртуализации, поддерживающих работу с USB-устройствами.

В зависимости от типа учетной записи пользователя аутентификация различается как:

- Локальная — с использованием локальных учетных записей `user` и `admin`.
- Централизованная — с учетными записями пользователей, созданными в ViPNet Prime; возможна только при наличии доступа ViPNet Coordinator HW к ViPNet Prime. Если имя централизованной учетной записи совпадает с одним из локальных, то в командном интерпретаторе необходимо использовать префикс: `center\user` или `center\admin`.

При аутентификации по сертификату:

- Удаленное подключение централизованных пользователей по SSH запрещено.
- При удаленном подключении локальных пользователей по SSH и HTTP/HTTPS используются пароли их учетных записей.

Многопользовательский режим работы

ViPNet Coordinator HW поддерживает многопользовательский режим работы — одновременно могут быть открыты несколько сессий локальных и централизованных пользователей. В рамках сессий пользователи могут выполнять команды по просмотру и изменению настроек ViPNet Coordinator HW из разных групп.

Таблица 20. Распределение команд ViPNet Coordinator HW по группам настроек

Группа настроек	Команды
Системные	• Настройка даты и времени • Настройка сетевых интерфейсов • Перезагрузка ViPNet Coordinator HW • Резервное копирование конфигурации • Настройка системы защиты от сбоев • Настройка транспортного сервера MFTP • Другие общесистемные настройки
VPN	Настройка параметров работы в защищенной сети ViPNet
МЭ	Настройка сетевых фильтров и правил трансляции адресов

Администраторы могут бесконфликтно изменять настройки, относящиеся к командам разных групп. Для предотвращения конфликта, возникающего при изменении одних и тех же настроек, применяется блокировка. Она устанавливается сессией администратора, который начал вносить изменения первым, и продолжается до их применения в ViPNet Coordinator HW. Другие администраторы могут снять эту блокировку и установить свою; при этом первый администратор получит уведомление, а его изменения будут потеряны. На время блокировки все пользователи, как администраторы, так и аудиторы, могут просматривать настройки.

Например, если локальный администратор `admin` начал вносить изменения в сетевые фильтры, то настройка сетевых фильтров и правил трансляции адресов (группа настроек МЭ) другим администратором будет заблокирована до тех пор, пока `admin` не применит изменения. При этом администратор может снять блокировку `admin` для изменения настроек межсетевого экрана. В этом случае `admin` получит уведомление, а сделанные им изменения будут потеряны.

Отдельные команды, связанные с системными процессами, устанавливают глобальную блокировку, на время которой:

- Блокируются команды всех групп настроек, в том числе команды просмотра настроек.
- На сессии пользователей накладывают ограничения.

Таблица 21. Команды, устанавливающие глобальную блокировку

Команда	Ограничения
`admin remove keys` — удаление ключей	Завершение сессий всех пользователей
`admin upgrade software` — обновление ПО	Завершение сессий всех пользователей, новые сессии не открываются
`iplir set performance-mode` — выбор профиля производительности	Завершение сессий всех пользователей, новые сессии не открываются
`machine backup export` — экспорт конфигурации	Текущие сессии пользователей сохраняются, новые сессии не открываются
`machine halt` — завершение работы	Завершение сессий всех пользователей
`machine reboot` — перезагрузка	Завершение сессий всех пользователей
`machine self-test` — проверка целостности ПО	Текущие сессии пользователей сохраняются, новые сессии не открываются
`service dpi update usb` — обновление подсистемы DPI	Завершение сессий всех пользователей
`admin escape` — выход в shell	Для остальных сессий администратора, выполнившего выход в shell, доступны только команды просмотра параметров; сессии других пользователей завершаются

Особенности применения блокировок

- Блокировки не синхронизируются в кластере: непримененные изменения на активном узле будут потеряны после переключения кластера.
- Глобальная блокировка не всегда проверяется до начала выполнения интерактивной команды, что может привести к прерыванию ее выполнения после окончания интерактивного ввода.

Автоматическое завершение сессии

Помимо завершения работы сессии самим пользователем, она завершается автоматически в двух случаях:

- По истечении допустимого времени неактивности сессии, одинакового для сессий всех пользователей.
- При переключении кластера.

Если команда запущена и выполняется, то завершение сессии не отменяет выполнение этой команды.

Режимы работы командного интерпретатора и веб-интерфейса

- Режим просмотра — позволяет просматривать настройки и выполнять аудит событий.
- Режим настройки — позволяет просматривать настройки, изменять их, обновлять ПО и выполнять аудит событий.

Командный интерпретатор

Пользователю с ролью аудитора доступен только режим просмотра.

Пользователю с ролью администратора сразу после аутентификации доступен режим просмотра. Для перехода в режим настройки выполните:

```
hostname> enable
hostname#
```

Чтобы вернуться в режим просмотра, выполните:

```
hostname# exit
hostname>
```

Веб-интерфейс

Пользователю с ролью аудитора доступен только режим просмотра.

Пользователю с ролью администратора режим настройки доступен сразу после аутентификации, за исключением работы в разделах, требующих глобальной блокировки. Такие разделы, например, настройка сетевых интерфейсов, помечены значком  . Чтобы изменить настройки раздела:

1. Нажмите  .
2. Внесите изменения.
3. Нажмите  .

5

Подготовка к работе

Порядок действий

1 У администратора сети ViPNet:

   1.1 Получите дистрибутив ключей и пароль к нему.

   1.2 Выясните доменное имя и ViPNet ID ViPNet Prime.

   1.3 Если на ViPNet Coordinator HW (ViPNet Coordinator VA) будет использоваться аутентификация по сертификату, получите USB-токен. В ходе инициализации на USB-токене будут сохранены сертификат и закрытый ключ локального администратора `admin`.

2 В зависимости от исполнения:

   - Разверните виртуальную машину ViPNet Coordinator VA на платформе виртуализации (см. Развертывание виртуальной машины ViPNet Coordinator VA).
   - Установите SIM-карту для исполнений на аппаратных платформах HW50 N3 и HW100 N3 (см. Установка SIM-карты в HW50 N3 и HW100 N3).

3 Чтобы во время инициализации проверить связь с каким-либо из связанных узлов сети ViPNet, например с ViPNet Prime, подключите ViPNet Coordinator HW (виртуальную машину ViPNet Coordinator VA) к коммутационному оборудованию сети ViPNet.

4 Подключитесь к ViPNet Coordinator HW (ViPNet Coordinator VA) одним из способов (см. Способы установки дистрибутива ключей).

5 Выполните инициализацию в одном из режимов:

   - Инициализация в консольном режиме.
   - Инициализация в полноэкранном режиме.

6 Подключитесь к ViPNet Coordinator HW (ViPNet Coordinator VA) с помощью веб-интерфейса или командного интерпретатора, чтобы выполнить дополнительные настройки (см. После инициализации).

Развертывание виртуальной машины ViPNet Coordinator VA

Proxmox VE

1 Создайте новую виртуальную машину:

```
#qm create <номер VM> --name va --net0 intelE1000,bridge=vmbr0 --serial0 socket
--bootdisk scsi0 --scsihw virtio-scsi-pci
```

`<номер VM>` — номер виртуальной машины, далее в сценарии `110`.

2 Добавьте файл виртуальной машины ViPNet Coordinator VA:

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

`<путь к файлу>` — путь к файлу виртуальной машины ViPNet Coordinator VA в формате `*.raw` или `*.qcow2`

3 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
```

4 Откройте менеджер виртуальных машин в веб-интерфейсе.

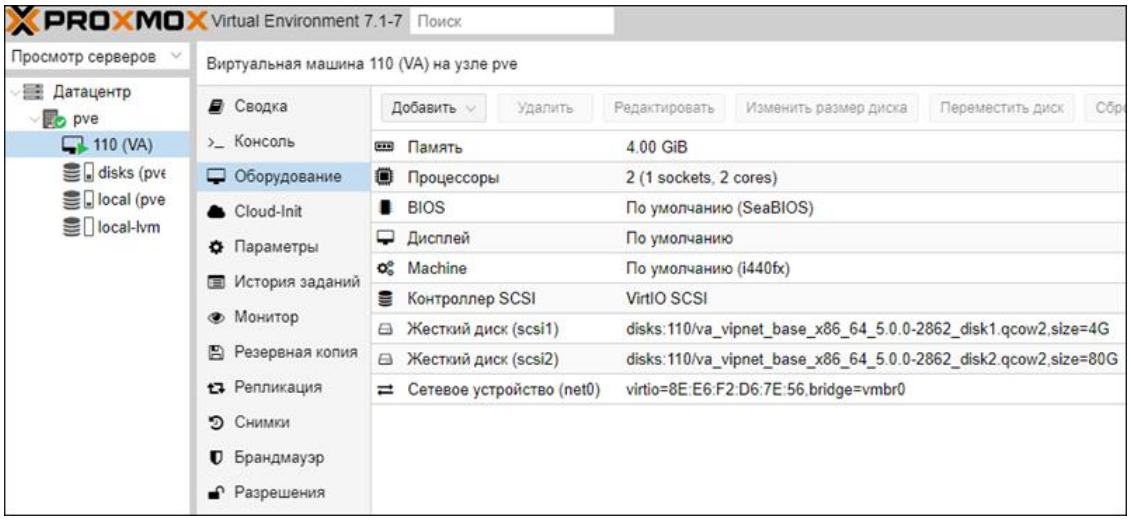

Рисунок 28. Настройки виртуальной машины

5 Задайте параметры профиля аппаратных средств виртуальной машины (см. ViPNet Coordinator VA):

5.1 Выберите **Память** и задайте размер ОЗУ.

5.2 Выберите **Процессоры**:

5.2.1 Задайте количество ядер процессоров.

5.2.2 В списке **Тип** выберите **host**.

5.2.3 Нажмите **OK**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.

VMware vSphere ESXi

1 Подключитесь к **VM vSphere**.

2 Выберите **VM and Templates** > **Actions** > **Deploy OVF Template**.

3 На странице **Select an OVF template** мастера укажите путь к файлу виртуальной машины ViPNet Coordinator VA с расширением `ova`.

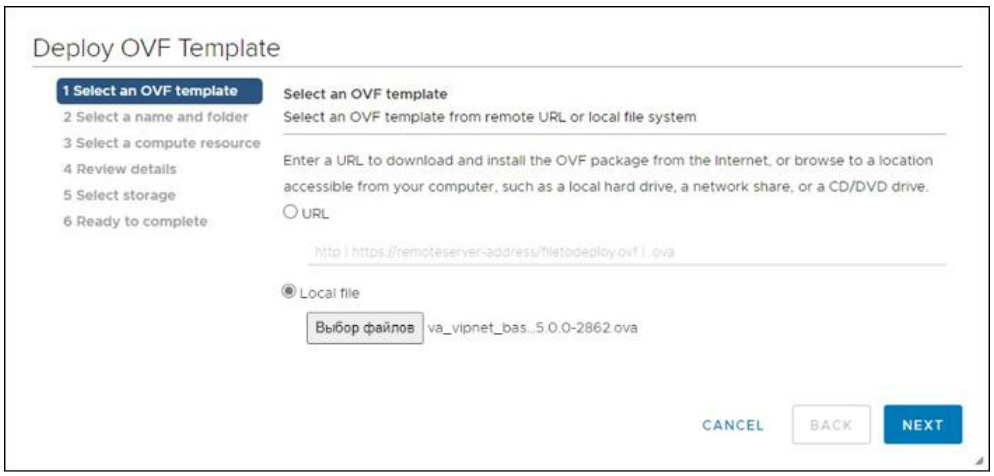

Рисунок 29. Выбор файла виртуальной машины

4 На странице **Select a name and folder** укажите имя виртуальной машины и выберите папку ее размещения.

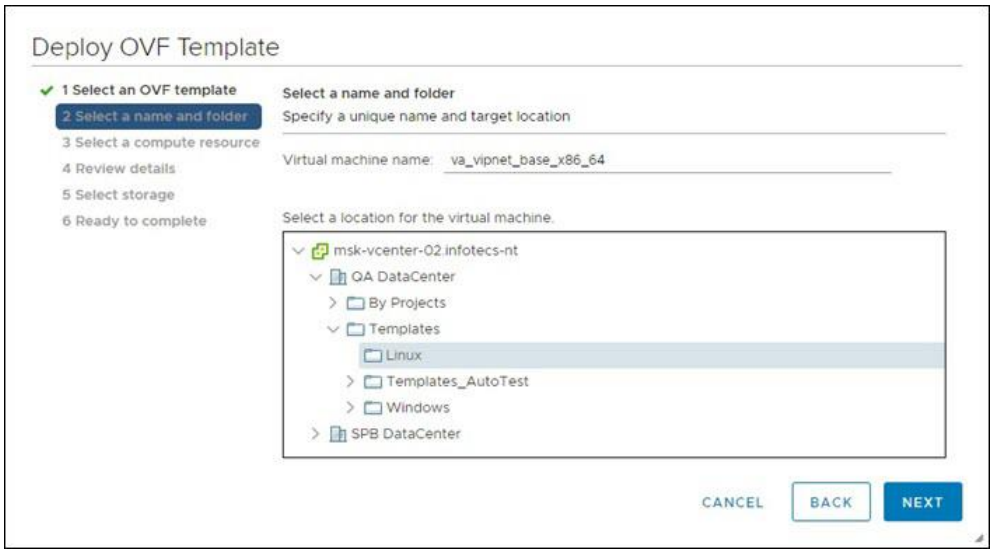

Рисунок 30. Задание имени и расположения виртуальной машины

5 На странице **Select a computer resource** выберите пул ресурсов, выделяемых виртуальной машине.

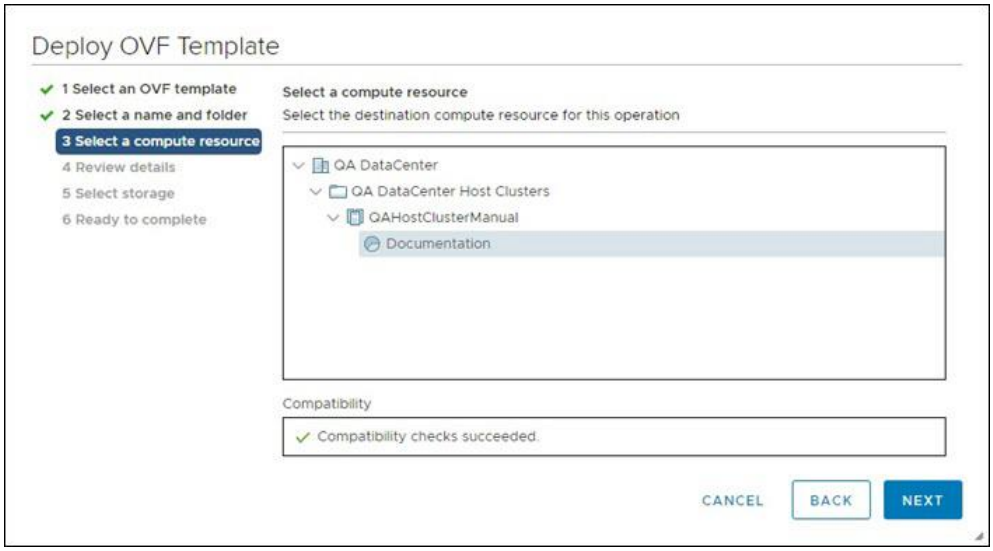

Рисунок 31. Выбор пула ресурсов

6 На странице **Review details** проверьте параметры виртуальной машины.

7 На странице **Select storage** выберите накопитель из пула ресурсов и укажите формат виртуального диска.

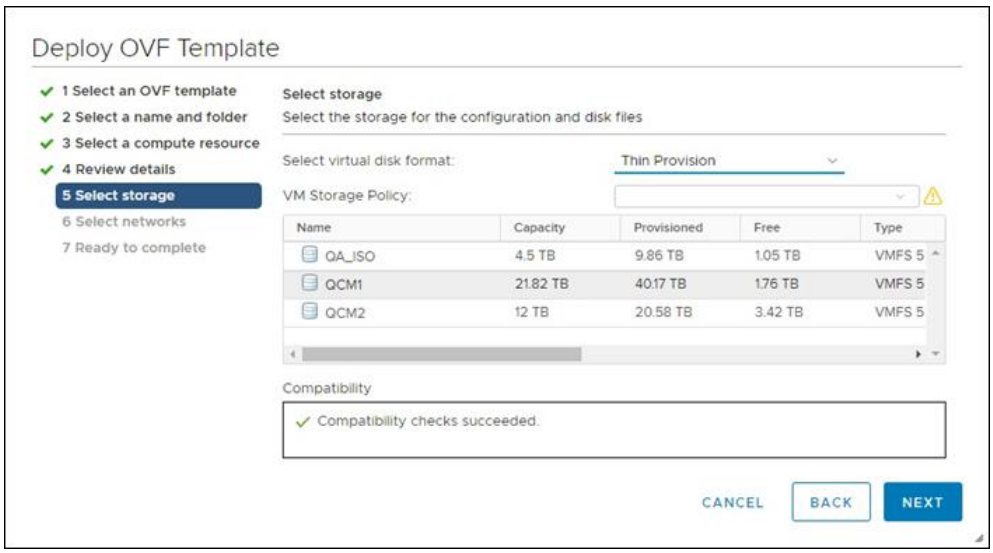

Рисунок 32. Выбор формата виртуального диска

- 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 ViPNet-клиентов, то для виртуального диска укажите тип **Thick Provision**, иначе работа в сети ViPNet будет существенно замедлена.

8 На странице **Select networks** выберите физический или виртуальный коммутатор ESXi для сети **bridged**.

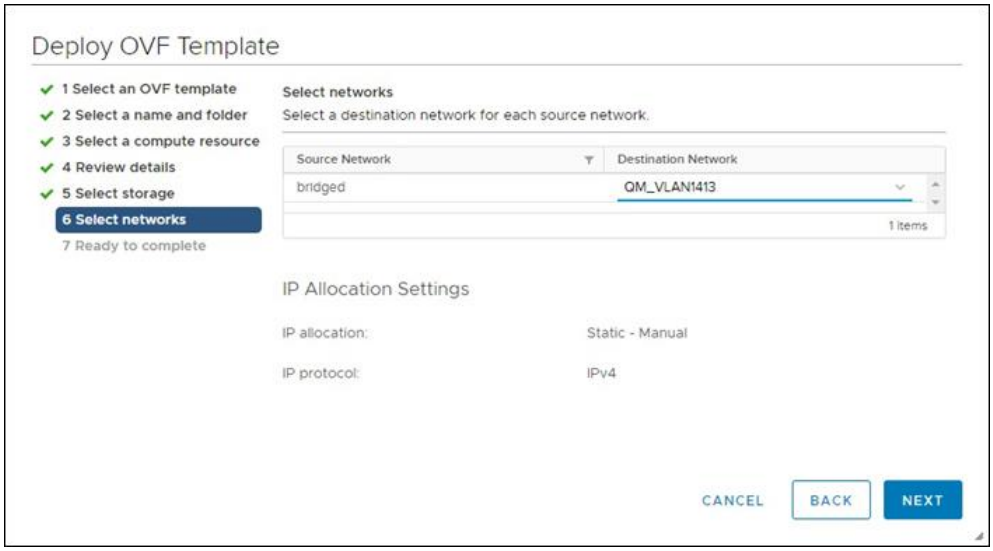

Рисунок 33. Настройка сетевых интерфейсов

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

10 Задайте параметры профиля аппаратных средств виртуальной машины (см. ViPNet Coordinator VA):

10.1 Выберите **Actions** > **Edit Settings** > **Virtual Hardware**.

10.2 Задайте параметры **CPU** и **Memory**.

10.3 Нажмите **OK**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.

VMware Workstation Pro

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

2 Укажите путь к файлу виртуальной машины ViPNet Coordinator VA с расширением `ova`.

3 В окне **Import Virtual Machine** задайте имя виртуальной машины и папку для ее размещения, нажмите **Import**.

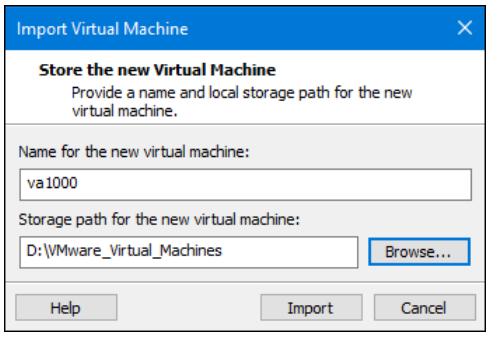

Рисунок 34. Выбор расположения виртуальной машины

4 Задайте параметры профиля аппаратных средств виртуальной машины (см. ViPNet Coordinator VA):

4.1 Перейдите на вкладку **Hardware**.

4.2 Задайте параметры **Memory** и **Processors**.

4.3 Нажмите **OK**.

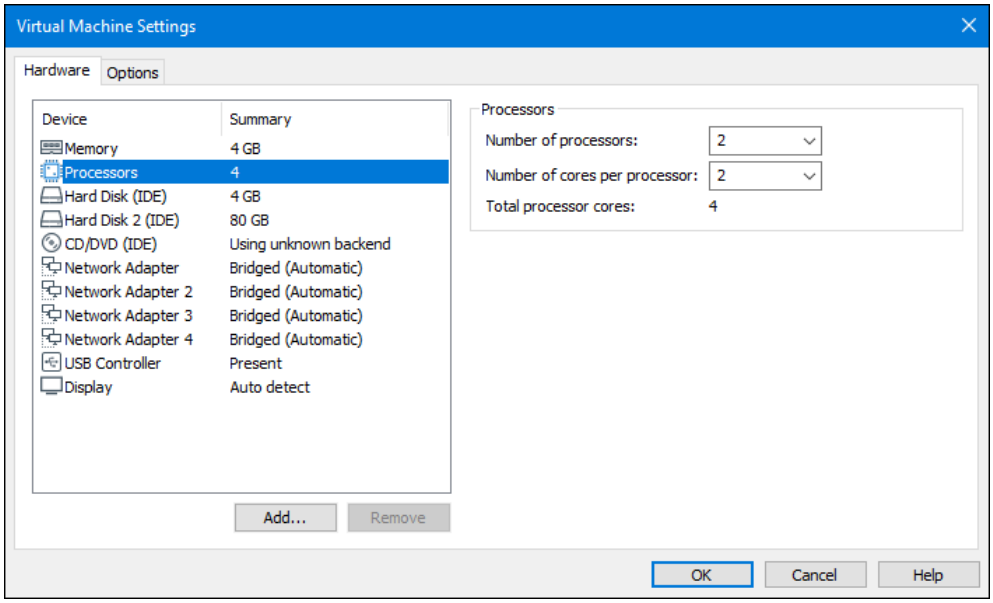

Рисунок 35. Настройки виртуальной машины

Виртуальная машина ViPNet Coordinator VA готова к использованию.

Microsoft Hyper-V

Внимание! Microsoft Hyper-V не поддерживает подключение USB-носителей к виртуальной машине, поэтому:

1 Установка дистрибутива ключей возможна только с помощью компьютера по протоколу TFTP или внешнего CD-привода.

2 Не поддерживаются команды с обращением к USB-носителю.

Предварительно распакуйте архив с расширением `tar.gz`, содержащий два файла виртуальной машины ViPNet Coordinator VA формата `vhd` с метками `disk1` и `disk2`, например:

- `va_vipnet_base_x86_64_5.1.0-3064_disk1.vhd`
- `va_vipnet_base_x86_64_5.1.0-3064_disk2.vhd`

Далее:

1. Запустите **Диспетчер Hyper-V**.
2. Выберите **Действие** > **Создать** > **Виртуальная машина** и задайте ее имя.
3. Не изменяйте поколение виртуальной машины, размер отведенной ей памяти, и подключение к сети, заданные по умолчанию.
4. Выберите **Подключить виртуальный жесткий диск позднее**.
5. Нажмите **Готово**.
6. Задайте параметры профиля аппаратных средств виртуальной машины (см. ViPNet Coordinator VA):
   - **6.1** Выберите **Установка оборудования** > **Сетевой адаптер** > **Добавить** и увеличьте общее количество адаптеров до четырех.
   - **6.2** Выберите **Память** и задайте размер ОЗУ.
   - **6.3** Выберите **Процессор** и задайте количество ядер процессоров.
   - **6.4** Выберите **Контроллер 0 IDE** > **Жесткий диск** > **Добавить** и укажите файл виртуальной машины с меткой `disk1`.
   - **6.5** Выберите **Контроллер 0 IDE** > **Жесткий диск** > **Добавить** и укажите файл виртуальной машины с меткой `disk2`.
   - **6.6** Нажмите **OK**.

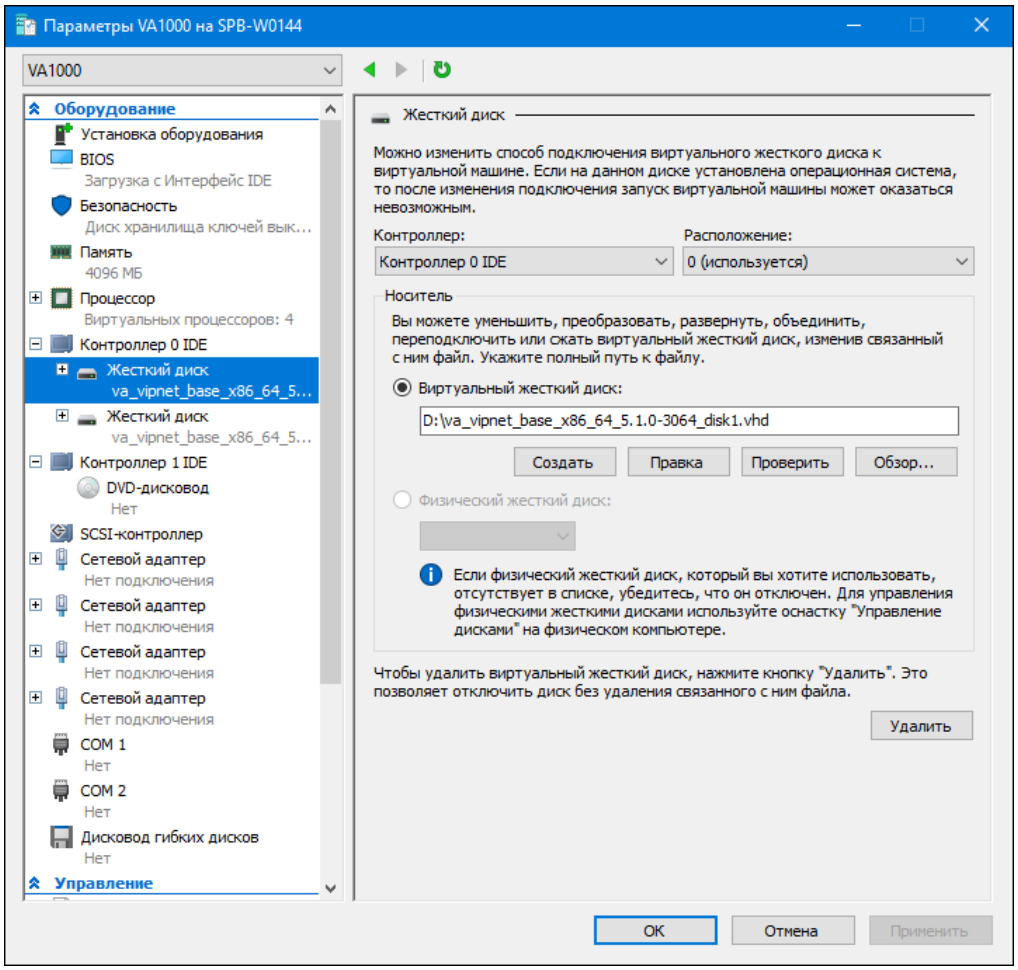

Рисунок 36. Настройки виртуальной машины

Виртуальная машина ViPNet Coordinator VA готова к использованию.

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.

Oracle VM Server

Внимание! Oracle VM Server не поддерживает подключение USB-носителей к виртуальной машине, поэтому:

1. Установка дистрибутива ключей возможна только с помощью компьютера по протоколу TFTP или внешнего CD-привода.
2. Не поддерживаются команды с обращением к USB-носителю.

1. Загрузите файл виртуальной машины ViPNet Coordinator VA с расширением `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 37. Импорт образа виртуальной машины

4 В окне **Import Virtual Appliance**:

4.1 В поле **Virtual Appliance download location** укажите сетевой путь к файлу `*.ova`, загруженному на шаге 1.

4.2 Установите флажок **Create VM**.

4.3 В списке **Server Pool** выберите область, в которой будут сохранены файлы виртуальной машины.

4.4 Нажмите **OK**.

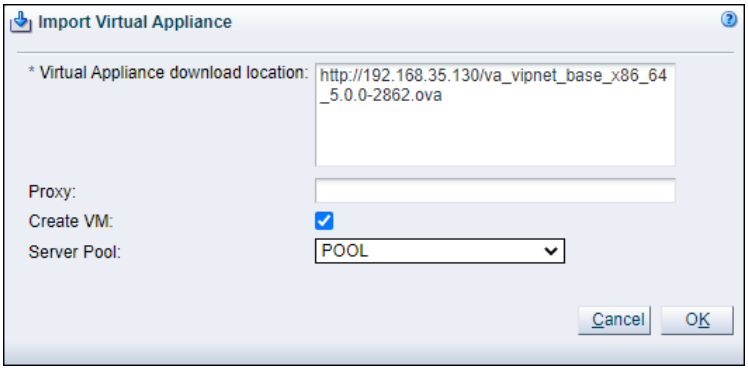

Рисунок 38. Выбор файла виртуальной машины

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

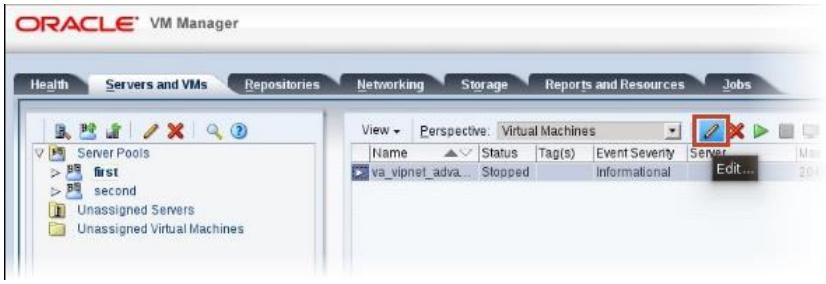

Рисунок 39. Редактирование настроек виртуальной машины

6 Задайте параметры профиля аппаратных средств виртуальной машины (см. ViPNet Coordinator VA):

6.1 Перейдите на вкладку **Configuration**.

6.2 В списке **Domain Type** выберите **Xen HVM PV Drivers**.

6.3 Задайте параметры **Memory** и **Processors**.

6.4 Нажмите **OK**.

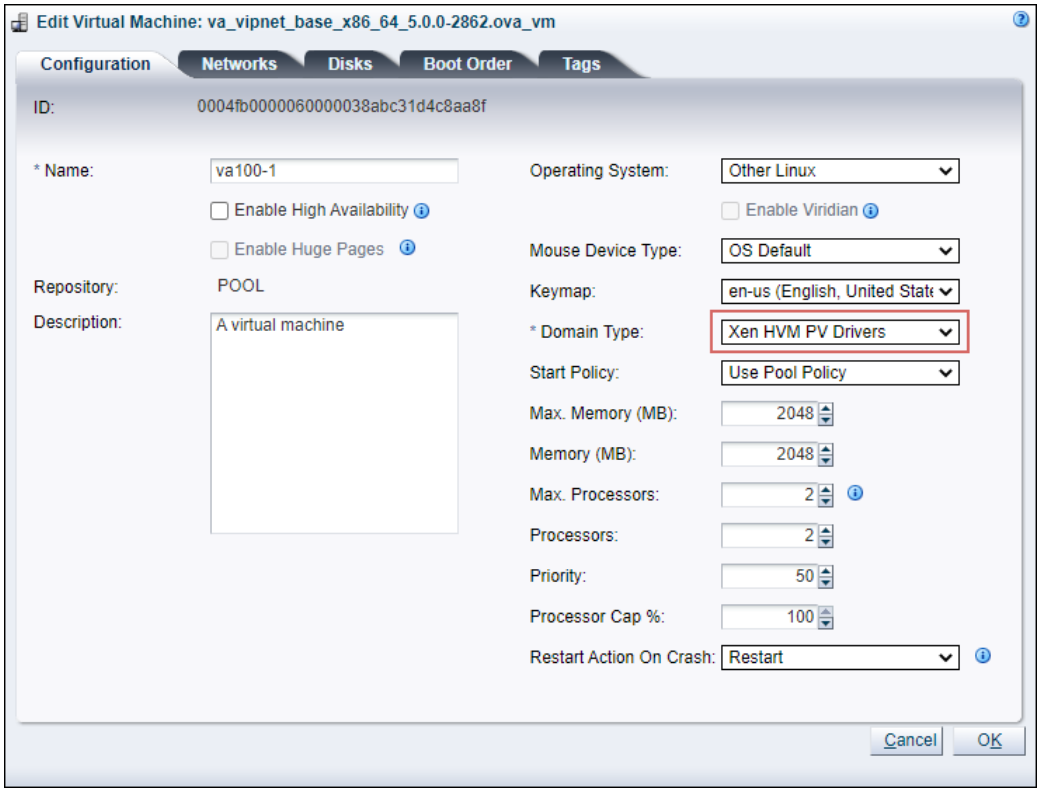

Рисунок 40. Настройки виртуальной машины

Виртуальная машина ViPNet Coordinator VA готова к использованию.

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**.

Особенности работы

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** или перезагружайте ViPNet Coordinator VA с помощью командного интерпретатора или веб-интерфейса.

Oracle VM VirtualBox

1 Запустите **Oracle VM VirtualBox** и выберите **File** > **Импорт конфигураций**.

2 Укажите путь к файлу виртуальной машины ViPNet Coordinator VA с расширением `ova`.

3 Настройте параметры импорта:

  3.1 Задайте имя виртуальной машины.

  3.2 Задайте параметры профиля аппаратных средств виртуальной машины (см. ViPNet Coordinator VA):

  3.2.1 ОЗУ.

  3.2.2 Процессор.

4 Нажмите **Импорт**.

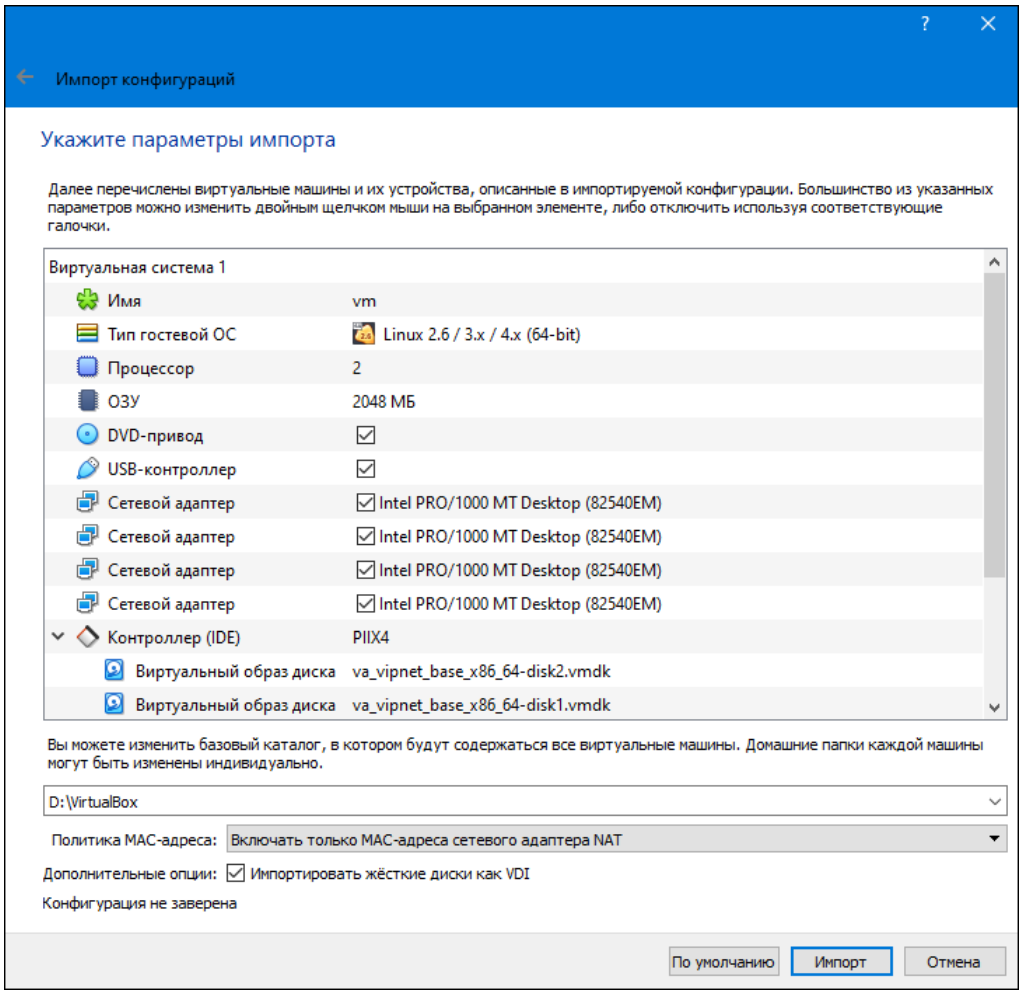

Рисунок 41. Настройка параметров импорта

5 По завершении импорта конфигурации виртуальной машины:

5.1 Выберите **Настроить** > **Система** > **Материнская плата** и установите флажок **Часы в системе UTC**.

5.2 Нажмите **OK**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.

Внимание! Во время эксплуатации ViPNet Coordinator VA не меняйте тип контроллера жесткого диска. Корректная работа гарантируется только при использовании IDE-контроллера.

SharxBase

Предварительно распакуйте архив с расширением `tar.gz`, содержащий два файла виртуальной машины ViPNet Coordinator VA формата `qcow2` с метками `disk1` и `disk2`, например:

- `va_vipnet_base_x86_64_5.2.0-5104_disk1.qcow2`
- `va_vipnet_base_x86_64_5.2.0-5104_disk2.qcow2`

Далее:

1 Подключитесь к SharxBase.

2 В настройке **Представления (kvm)** учетной записи подключения к SharxBase проверьте вид интерфейса: если установлен **cloud** — выберите **user**.

3 Выберите **Хранилище** > **Образы дисков ВМ**.

4 Создайте образ для файла с меткой `disk1`:

4.1 Нажмите +, затем **Создать**.

4.2 Укажите имя образа, например va_disk1.

4.3 В списке **Тип** выберите **Блочное устройство**.

4.4 В списке **Постоянный образ** выберите **Да**.

4.5 В разделе **Расположение образа** выберите **Загрузить** и укажите путь к файлу с меткой `disk1`.

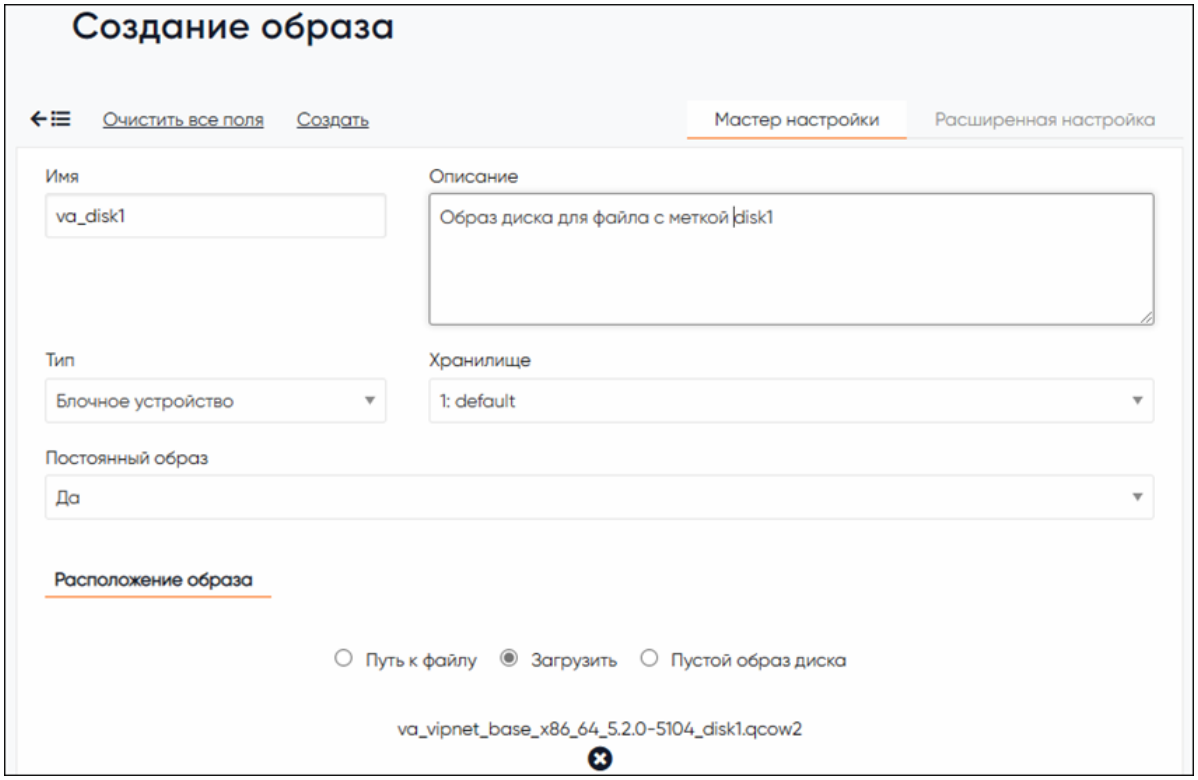

Рисунок 42. Создание образа диска

4.6 На панели инструментов нажмите **Создать**.

Загрузка файла и регистрация его образа выполняются в фоновом режиме.

5 Чтобы создать образ для файла с меткой `disk2`, повторите шаги 4.1–4.6.

6 Выберите **Шаблоны** > **Виртуальные машины**.

7 Создайте шаблон виртуальной машины ViPNet Coordinator HW:

7.1 Нажмите +, затем **Создать** и на вкладке **Общие** укажите:

7.1.1 Имя шаблона, например VA1000.

7.1.2 **ОЗУ** — объем ОЗУ профиля аппаратных средств виртуальной машины (см. ViPNet Coordinator VA).

7.1.3 **ЦПУ** — 1.

7.1.4 **Виртуальные ЦПУ** — количество ядер процессора профиля аппаратных средств виртуальной машины.

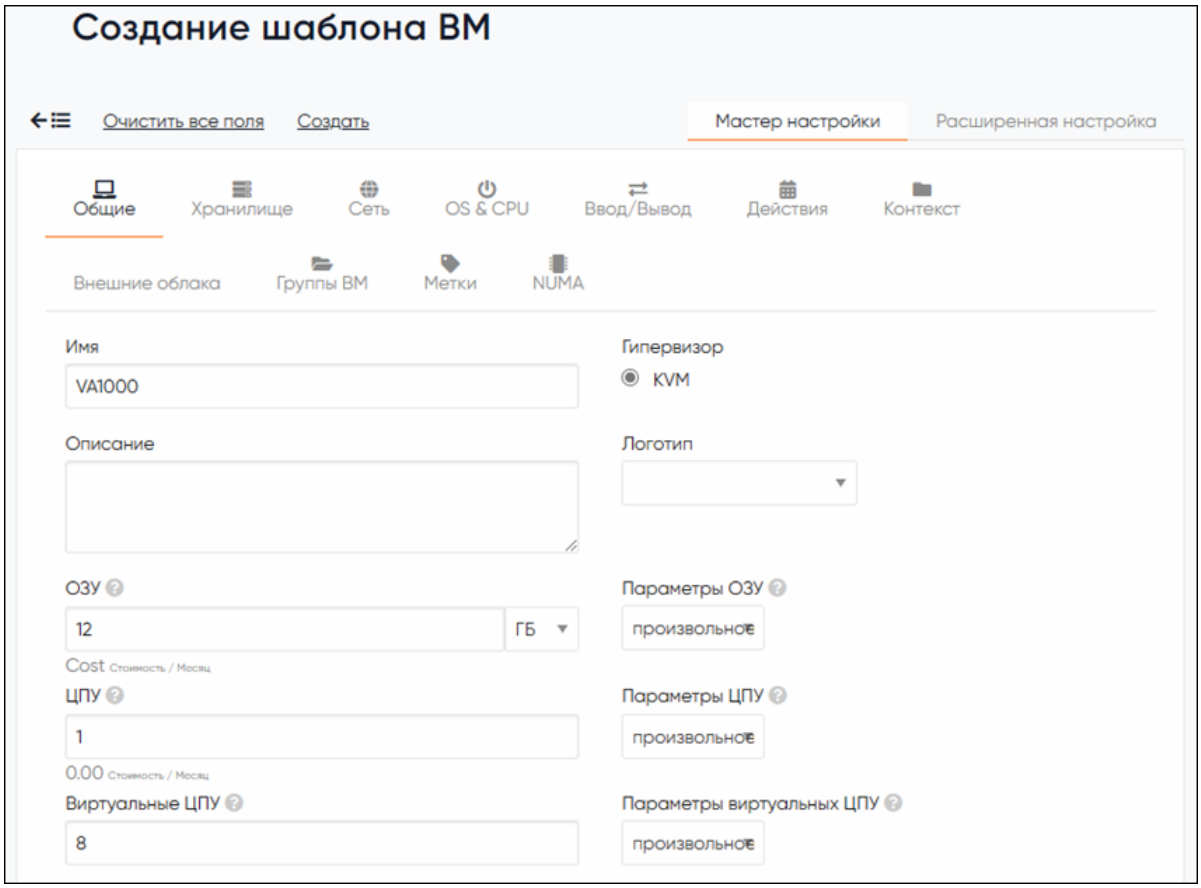

Рисунок 43. Создание шаблона виртуальной машины

7.2 На вкладке **Хранилище**:

7.2.1 Для **ДИСК 0** выберите **Образ**, затем из списка ниже выберите файл образа диска с меткой `disk1`, например va_disk1.

7.2.2 Нажмите ⊕ и для **ДИСК 1** выберите **Образ**, затем из списка ниже выберите файл образа диска с меткой `disk2`, например va_disk2.

7.3 На вкладке **Сеть**:

7.3.1 Для **Сетевой интерфейс 0** выберите из списка ниже сеть, к которой он будет подключен.

7.3.2 Добавьте сетевой интерфейс: нажмите ⊕ и выберите из списка ниже сеть, к которой он будет подключен.

7.3.3 Повторите шаг 3.2, чтобы общее количество сетевых интерфейсов виртуальной машины стало 4.

7.4 На вкладке **OS & CPU** в разделе **Порядок загрузки** проверьте, что **disk0** — первое загрузочное устройство.

7.5 На вкладке **NUMA** установите флажок **NUMA Topology** и задайте параметры:

7.5.1 **Pin Policy** — **none**.

7.5.2 **Sockets** — 1.

7.5.3 **Cores** — 4.

7.5.4 **Threads** — 2.

> **Примечание.** Задайте значения параметров так, чтобы Sockets * Cores * Threads = Виртуальные ЦПУ

7.6 На панели инструментов нажмите **Создать**.

8 Щелкните шаблон виртуальной машины в списке и на панели инструментов нажмите **Развернуть**.

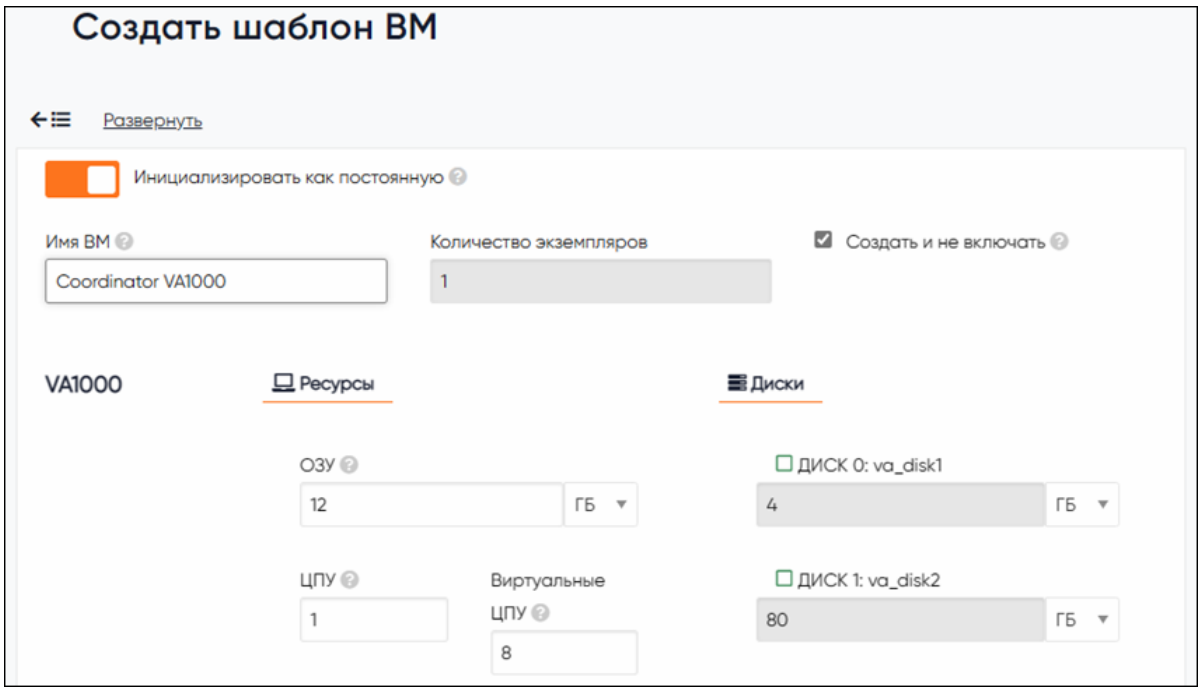

Рисунок 44. Создание виртуальной машины на основе шаблона

8.1 Включите **Инициализировать как постоянную**.

8.2 Укажите имя виртуальной машины.

8.3 Установите флажок **Создать и не включать**.

8.4 На панели инструментов нажмите **Развернуть**.

Виртуальная машина ViPNet Coordinator VA готова к использованию.

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 45. 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.

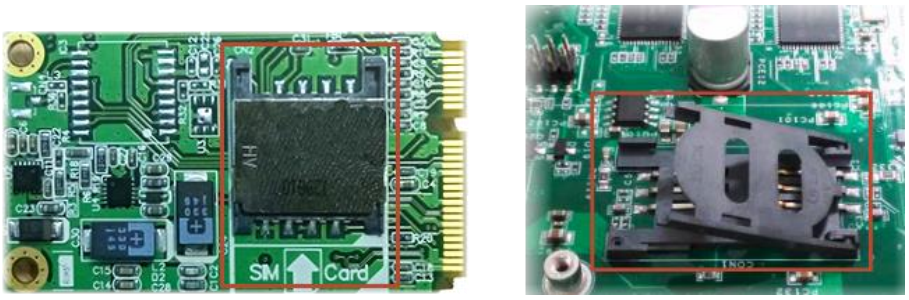

Рисунок 46. Разъемы для SIM-карты

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

6 Соберите корпус ViPNet Coordinator HW.

Способы установки дистрибутива ключей

В ходе инициализации ViPNet Coordinator HW и ViPNet Coordinator VA необходимо установить дистрибутив ключей. Существует два способа установки дистрибутива ключей, использование которых определяется исполнением и способом подключения:

- С помощью внешнего устройства — USB-носителя или CD-диска:
  - ViPNet Coordinator HW. Для подключения используются монитор и клавиатура (через порты VGA и PS/2) или компьютер (через консольный порт); файл дистрибутива ключей располагается на USB-носителе или CD-диске, USB-носитель или CD-привод подключены к ViPNet Coordinator HW.
  - ViPNet Coordinator VA. Для подключения используется консоль платформы виртуализации; файл дистрибутива ключей располагается на USB-носителе или CD-диске, USB-носитель или CD-привод подключены к ViPNet Coordinator VA средствами платформы виртуализации.
- С помощью компьютера по протоколу TFTP:
  - ViPNet Coordinator HW. Компьютер подключается к сетевому интерфейсу `eth1` ViPNet Coordinator HW напрямую, с помощью сетевого кабеля RJ45 Cat. 5; файл дистрибутива ключей располагается в папке на компьютере.
  - ViPNet Coordinator VA. Компьютер подключается к сетевому интерфейсу `eth1` ViPNet Coordinator VA средствами платформы виртуализации; файл дистрибутива ключей располагается в папке на компьютере.

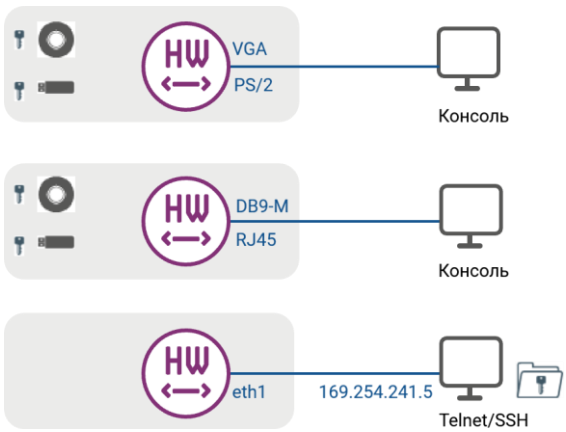

Рисунок 47. Способы подключения к ViPNet Coordinator HW и установки дистрибутива ключей

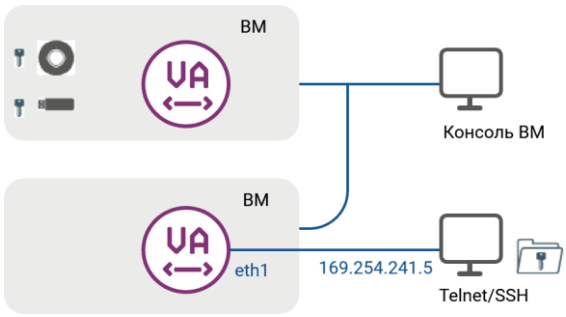

Рисунок 48. Способы подключения к ViPNet Coordinator VA и установки дистрибутива ключей

Установка с внешнего устройства

ViPNet Coordinator HW:

1. Запишите файл дистрибутива ключей:
   - На USB-носитель с файловой системой FAT32, ext2, ext3 или ext4.
   - На CD-диск.
2. Подключите USB-носитель или CD-привод к ViPNet Coordinator HW; вставьте CD-диск в привод.
3. Подключитесь к ViPNet Coordinator HW:
   - С помощью монитора и клавиатуры к портам VGA и PS/2.
   - С помощью компьютера к консольному порту ViPNet Coordinator HW, используя кабель с разъемами DB9 или RJ45, и задайте параметры подключения клиента удаленного доступа (приведены настройки PuTTY):
     - Terminal — VT100+.
     - Remote character set — KOI8-R.
     - Connection type — Serial:
       - Speed — 38400.
       - Data — 8.
       - Parity — None.
       - Stopbits — 1.
       - Flow Control — None.

ViPNet Coordinator VA:

1. Запишите файл дистрибутива ключей:
   - На USB-носитель с файловой системой FAT32, ext2, ext3 или ext4.
   - На CD-диск.
2. Подключите USB-носитель или CD-привод к ViPNet Coordinator VA средствами платформы виртуализации; вставьте CD-диск в привод.

3 Подключитесь к виртуальной машине ViPNet Coordinator VA с помощью консоли платформы виртуализации.

Установка по TFTP

Для установки дистрибутива ключей вам понадобятся:

- Компьютер с сетевой картой Ethernet и Windows или Linux любых версий.
- Сетевой кабель RJ45 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, и 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 Установите на сетевом интерфейсе компьютера IP-адрес `169.254.241.5`.

3 Подключите сетевой интерфейс компьютера:

- К порту `eth1` ViPNet Coordinator HW с помощью сетевого кабеля.
- К порту `eth1` ViPNet Coordinator VA средствами платформы виртуализации.

4 Подключитесь к ViPNet Coordinator HW или ViPNet Coordinator VA с помощью клиента удаленного доступа 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**).

Инициализация в консольном режиме

1. Включите ViPNet Coordinator HW (виртуальную машину ViPNet Coordinator VA).
2. В строке приглашения введите имя пользователя `user` и пароль `user`.
3. Выберите консольный режим работы мастера установки дистрибутива ключей — введите `1`.
4. Примите условия соглашения. Если текст отображается некорректно, проверьте кодировку в параметрах подключения к ViPNet Coordinator HW.
5. Начните установку — в строке `Now you need to install keys or restore configuration from backup. Do you want to begin? [Yes/No]` введите `y` и нажмите **Enter**.
6. Введите номер континента или UTC из списка и нажмите **Enter**.
7. Введите номер страны из списка и нажмите **Enter**.

   Список содержит страны, расположенные на выбранном континенте.
8. Введите номер часового пояса из списка и нажмите **Enter**.

   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**.
10. Если требуется изменить текущую дату и время, введите дату и время в формате `YYYY-MM-DD hh:mm:ss` и нажмите **Enter**.
11. Выберите способ установки файла дистрибутива ключей — в строке `Would you like to install appliance initialization file from TFTP, USB or CD storage device? [t/u/c]` введите:
    - `t` — для установки с компьютера по протоколу TFTP.
    - `u` — для установки с USB-носителя.
    - `c` — для установки с CD-диска.
12. Для установки с компьютера по протоколу TFTP:

    12.1 На компьютере выполните команду:

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

    12.2 В мастере установки подтвердите установку файла дистрибутива ключей — нажмите **Next**.
13. Для установки с USB-носителя или CD-диска:

    13.1 Подключите USB-носитель или CD-привод; вставьте CD-диск в привод.

    13.2 Чтобы найти файлы `ds5`, в мастере установки, нажмите **Enter**.

- Если на USB-носителе или CD-диске обнаружен только один файл `ds5`, он будет выбран для установки.
- Если обнаружено несколько файлов `ds5`, введите номер файла из списка `Found several application initialization files` и нажмите **Enter**.

Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы `ds5`.

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

- Если файлов `ds5` не обнаружено, мастер предложит выбрать способ переноса дистрибутива ключей заново (шаг 11).

14 Введите пароль к файлу дистрибутива ключей — в строке `Enter password` введите пароль и нажмите **Enter**.

15 Выберите ручной способ настройки — в строке `Select the setup method` введите `1` и нажмите **Enter**.

16 Задайте пароль локального администратора `admin` — в строке `Enter new admin password` введите и подтвердите пароль, затем нажмите **Enter**.

17 Если задан способ аутентификации пользователей по сертификату — в строке `Have you got token authentication mode [Yes/No]` введите `y` и нажмите **Enter**.

17.1 Подключите USB-токен и инициализируйте его (будет издан сертификат и сгенерирован закрытый ключ локального администратора `admin`) — в строке `Do you want to initialize token? [Yes/No]` введите `y` и нажмите **Enter**.

17.2 В строке `Enter admin-token PIN` введите ПИН администратора USB-токена и нажмите **Enter**.

17.3 Задайте ПИН пользователя USB-токена локального администратора `admin` — в строке `Enter new user-token PIN` введите и подтвердите ПИН, затем нажмите **Enter**.

18 Последовательно настройте сетевые интерфейсы, начиная с `eth0`:

- Чтобы настроить интерфейс, включите его — в строке `Configure interface eth<номер>? [Yes/No]` введите `y` и нажмите **Enter**.
- Чтобы пропустить настройку интерфейса и перейти к следующему, введите `n` и нажмите **Enter**.

В случае отказа от настройки последнего сетевого интерфейса, мастер перейдет к настройке DNS-сервера (шаг 22).

19 Установите для интерфейса режим:

- Режим DHCP — в строке `Use dhcp on the interface eth<номер>? [Yes/No]` введите `y` и нажмите **Enter**.
- Режим статической адресации — введите `n` и нажмите **Enter**.

20 Если был выбран режим статической адресации:

- Введите последовательно IP-адрес и маску интерфейса и нажмите **Enter**.

Внимание! Ограничения при задании IP-адреса:

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

- Если интерфейс не последний, мастер перейдет к настройке следующего интерфейса (шаг 18).

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

22 Установите режим запуска DNS-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в строке `Do you want to enable DNS server? [Yes/No]` введите `y` и нажмите **Enter**.
- Если запускать не нужно, введите `n` и нажмите **Enter**. Мастер перейдет к настройке NTP-сервера (шаг 24).

23 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**.
- Если DNS-сервер добавлять не нужно, введите `n` и нажмите **Enter**.

24 Установите режим запуска NTP-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в строке `Do you want to enable NTP server? [Yes/No]` введите `y` и нажмите **Enter**.
- Если NTP-сервер запускать не нужно, введите `n` и нажмите **Enter**. Мастер перейдет к настройке имени компьютера (шаг 26).

25 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**.
- Если NTP-сервер добавлять не нужно, введите `n` и нажмите **Enter**.

26 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**.
- Если имя изменять не нужно, нажмите **Enter**.

27 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**.

- Если диапазон виртуальных адресов изменять не нужно, введите `n` и нажмите **Enter**.

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».

---

28 Если был настроен хотя бы один сетевой интерфейс:

- Настройте проверку связи 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**.
- Если проверять связь не нужно, введите `n` и нажмите **Enter**. Мастер перейдет к запуску драйверов и служб (шаг 39).

29 Задайте режим подключения ViPNet Coordinator HW к внешней сети:

- В строке `Do you want to configure firewall mode? [Yes/No]` введите символ `y` и нажмите **Enter**.
- Если вы хотите использовать настройки подключения из дистрибутива ключей, введите `n` и нажмите **Enter**. Мастер перейдет к выбору узла сети ViPNet для проверки связи (шаг 33).

30 Выберите режим подключения ViPNet Coordinator HW к внешней сети:

- **Со статической трансляцией адресов** — введите `1` и нажмите **Enter**.
- **С динамической трансляцией адресов** — введите `2` и нажмите **Enter**.

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

31 Если был выбран режим **Со статической трансляцией адресов**:

31.1 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**.

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

31.2 Выберите внешний сетевой интерфейс — в строке `Please choose the network interface which will be used as external` введите номер интерфейса в списке и нажмите **Enter**.

Мастер перейдет к проверке связи с другим узлом сети ViPNet (шаг 33).

32 Если был выбран режим **С динамической трансляцией адресов**:

32.1 Выберите координатор, через который ViPNet Coordinator HW будет подключаться к сети:

32.1.1 В строке `Please choose the ViPNet Coordinator` введите номер координатора в списке и нажмите **Enter**. В списке выводятся только те координаторы, с которыми у ViPNet Coordinator HW заданы связи в справочниках устанавливаемого дистрибутива ключей.

32.1.2 Если для выбранного координатора не указан IP-адрес, 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**.

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

32.2 Выберите внешний сетевой интерфейс, как на шаге 31.2.

33 Выберите из списка сетевых узлов ViPNet, с которыми ViPNet Coordinator HW имеет связи, узел для проверки — в строке `Please choose the ViPNet host by number [<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**.

34 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**.

35 Запустите проверку связи с узлом сети ViPNet — в строке `Now the special temporary network settings will be applied and ViPNet will be launched in order to probe the VPN connection [Yes/No]` введите `y` и нажмите **Enter**.

Проверка может занять несколько минут.

36 Если связь с узлом сети ViPNet была установлена, все настройки, выполненные до проверки, сохраняются в конфигурационном файле `iplir.conf` ViPNet Coordinator HW. Нажмите **Enter**, чтобы перейти к запуску драйверов и служб (шаг 39).

37 Если связь с узлом сети ViPNet установить не удалось, то для выяснения причины просмотрите журнал IP-пакетов:

37.1 В строке `Do you want to view IP packet log in order to investigate the issue? [Yes/No]` введите `y` и нажмите **Enter**.

37.2 Просмотрите журнал и выясните причину. Подробнее о работе с журналом см. документ «Настройка с помощью командного интерпретатора».

37.3 Нажмите **Exit**, чтобы завершить просмотр журнала.

38 В зависимости от причины, по которой не удалось установить связь узлом сети ViPNet:

- Нажмите **Ctrl**+**C**, чтобы заново настроить проверку связи ViPNet Coordinator HW с узлом сети ViPNet (шаг 28).
- Нажмите **Enter**, чтобы продолжить работу мастера.

39 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**.

40 Завершите инициализацию ViPNet Coordinator HW — в строке `ViPNet Coordinator HW successfully deployed! Press Enter to proceed to authentication form` нажмите **Enter**.

Инициализация в полноэкранном режиме

1 Включите ViPNet Coordinator HW (виртуальную машину ViPNet Coordinator VA).

2 В строке приглашения введите имя пользователя `user` и пароль `user`.

3 Выберите полноэкранный режим работы мастера установки дистрибутива ключей — введите `2`.

4 Примите условия соглашения. Если текст отображается некорректно, проверьте кодировку в параметрах подключения к ViPNet Coordinator HW.

5 Начните установку — в окне **You must install keys or restore saved configuration. Would you like to start installing keys or restoring configuration?** нажмите **Next**.

6 Выберите континент или время UTC из списка и нажмите **Next**.

7 Выберите страну из списка и нажмите **Next**.

Список содержит страны, расположенные на выбранном континенте.

8 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 окне **Is the above information is OK?** нажмите **Yes**.

10 Если требуется изменить текущую дату и время — установите их в календаре и нажмите **Next**.

11 Выберите способ установки дистрибутива ключей — в окне **Would you like to start installing appliance initialization file from TFTP, USB or CD storage device?** выберите способ 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_дистрибутива_ключей>
```

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

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

13.1 Подключите USB-носитель или CD-привод; вставьте CD-диск в привод.

13.2 Чтобы найти файлы `ds5`, в мастере установки, нажмите **Next**.

- Если на USB-носителе или CD-диске обнаружен только один файл `ds5`, он будет выбран для установки.
- Если обнаружено несколько файлов `ds5`, в окне **Found several application initialization files. Please choose one appliance initialization files** выберите файл в списке и нажмите **Next**.

Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы `ds5`.

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 `ds5` не обнаружено, мастер предложит выбрать способ переноса дистрибутива ключей заново (шаг 11).

14 Введите пароль к файлу дистрибутива ключей — в окне **Enter password for selected appliance initialization file** введите пароль и нажмите **Next**.

15 Выберите ручной способ настройки — в окне **Please select further setup method** выберите **Configure manually** и нажмите **Next**.

16 Задайте пароль локального администратора `admin` — в окне **To access the device, set the administrator password** введите и подтвердите пароль, затем нажмите **Next**.

17 Если задан способ аутентификации пользователей по сертификату — в окне **Have you got token authentication mode?** нажмите **Yes**.

17.1 Подключите USB-токен и инициализируйте его (будет издан сертификат и сгенерирован закрытый ключ локального администратора admin) — в окне **Do you want to initialize token?** нажмите **Yes**.

17.2 В окне **Enter admin-token PIN** введите ПИН администратора USB-токена и нажмите **Next**.

17.3 Задайте ПИН пользователя USB-токена — в окне **To access token device set user-token PIN** введите и подтвердите ПИН, затем нажмите **Next**.

18 Последовательно настройте сетевые интерфейсы, начиная с `eth0`.

- Чтобы настроить интерфейс, включите его — в окне **UP/DOWN settings for interface eth<номер>** выберите **UP** и нажмите **Next**.
- Чтобы пропустить настройку интерфейса и перейти к следующему — выберите **DOWN** и нажмите **Next**.

В случае отказа от настройки последнего сетевого интерфейса, мастер перейдет к настройке DNS-сервера (шаг 22).

19 Установите режим интерфейса:

- Режим DHCP — в окне **Setting for interface eth<номер>** выберите **DHCP** и нажмите **Next**.
- Режим статической адресации — выберите **StaticIP** и нажмите **Next**.

20 Если был выбран режим статической адресации:

- Задайте IP-адрес — в окне **Static IP-address setting for eth<номер>** введите IP-адрес и маску интерфейса и нажмите **Next**.

Внимание! Ограничения при задании IP-адреса:

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

- Если интерфейс не последний, мастер перейдет к настройке следующего интерфейса (шаг 18).

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

22 Установите режим запуска DNS-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в окне **Enable/Disable DNS server mode** выберите **ON (Enable starting the DNS server at boot)** и нажмите **Next**.
- Если запускать не нужно, выберите **OFF (Disable starting the DNS server at boot)** и нажмите **Next**. Мастер перейдет к настройке NTP-сервера (шаг 24).

23 При подключении к интернету в качестве DNS-серверов по умолчанию используются корневые DNS-серверы:

- Чтобы добавить DNS-сервер, в окне **Do you want to add custom DNS server?** выберите **Yes (Add custom DNS server)** и нажмите **Next**. Введите IP-адрес DNS-сервера и нажмите **Next**.
- Если DNS-сервер добавлять не нужно, выберите **No (Leave the default setting)** и нажмите **Next**.

24 Установите режим запуска NTP-сервера при загрузке ViPNet Coordinator HW:

- Чтобы включить автоматический запуск, в окне **Enable/Disable NTP server mode** выберите **ON (Enable starting the NTP server at boot)** и нажмите **Next**.
- Если NTP-сервер запускать не нужно, выберите **OFF (Disable starting the NTP server at boot)** и нажмите **Next**. Мастер перейдет к настройке имени компьютера (шаг 26).

25 Для синхронизации системного времени по умолчанию используются публичные NTP-серверы:

- Чтобы добавить NTP-сервер, в окне **Do you want to add custom NTP server?** выберите **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, выберите **No (Leave the default setting)** и нажмите **Next**.

26 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 **Next**.
- Если имя изменять не нужно, нажмите **Next**.

27 Текущий диапазон виртуальных адресов может пересекаться с диапазоном IP-адресов, который используется для адресации в вашей сети:

- Чтобы изменить диапазон виртуальных адресов, в окне **Do you want to specify custom virtual IP address range?** выберите:
  - **Ranges (Set custom virtual IP range)** и нажмите **Next**. Введите начальный и конечный адреса нового диапазона виртуальных адресов и нажмите **Next**.
  - **CIDR (Set custom virtual IP range in the CIDR notation)** и нажмите **Next**. Введите начальный адрес в нотации CIDR нового диапазона виртуальных адресов и нажмите **Next**.
- Если диапазон виртуальных адресов изменять не нужно, выберите **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».

---

28 Если был настроен хотя бы один сетевой интерфейс:

- Настройте проверку связи ViPNet Coordinator HW с узлом сети ViPNet — в окне **Do you want to probe VPN-connection with some host in order to verify the configuration you've just made?** нажмите **Yes**.
- Если проверять связь не нужно, нажмите **No**. Мастер перейдет к запуску драйверов и служб (шаг 38).

29 Задайте режим подключения ViPNet Coordinator HW к внешней сети:

- В окне **Do you want to configure firewall mode?** нажмите **Yes**.
- Если вы хотите использовать настройки подключения из дистрибутива ключей, нажмите **No**. Мастер перейдет к выбору узла сети ViPNet для проверки связи (шаг 33).

30 Выберите режим подключения ViPNet Coordinator HW к внешней сети:

- **Со статической трансляцией адресов** — выберите **1 Static NAT** и нажмите **Next**.
- **С динамической трансляцией адресов** — выберите **2 Dynamic NAT** и нажмите **Next**.

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

31 Если был выбран режим **Со статической трансляцией адресов**:

31.1 По умолчанию для отправки и получения UDP-пакетов используется порт 55777. Чтобы изменить номер порта, в окне **Do you want to specify custom UDP port?** 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.

31.2 Выберите внешний сетевой интерфейс — в окне **Please choose the network interface which will be used as external** выберите сетевой интерфейс в списке и нажмите **Next**.

Мастер перейдет к проверке связи с другим узлом сети ViPNet (шаг 33).

32 Если был выбран режим **С динамической трансляцией адресов**:

32.1 Выберите координатор, через который ViPNet Coordinator HW будет подключаться к сети:

32.1.1 В окне **Please choose the ViPNet Coordinator** выберите координатор из списка и нажмите **Next**. В списке выводятся только те координаторы, с которыми у ViPNet Coordinator HW заданы связи в справочниках устанавливаемого дистрибутива ключей.

32.1.2 Если для выбранного координатора не указан IP-адрес, задайте его вручную — в окне **The IP address of the ViPNet host has not been found. Do you want to specify one?** нажмите **Yes**. Введите IP-адрес и нажмите **Next**.

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

32.2 Выберите внешний сетевой интерфейс, как на шаге 31.2.

33 Выберите из списка сетевых узлов ViPNet, с которыми ViPNet Coordinator HW имеет связи, узел для проверки — в окне **Choose the ViPNet host, which you are going to use for testing the VPN connection** выберите сетевой узел и нажмите **Next**.

34 Если в справочниках устанавливаемого дистрибутива ключей не указан IP-адрес выбранного узла сети ViPNet, задайте его вручную — в окне **The IP address of the VPN host has not been found. Do you want to specify one?** нажмите **Yes**. Введите IP-адрес и нажмите **Next**.

35 Запустите проверку связи с узлом сети ViPNet — в окне **Now the special temporary network settings will be applied and ViPNet will be launched in order to probe the VPN connection** нажмите **Start**.

Проверка может занять несколько минут. Дождитесь сообщения о результатах проверки:

36 Если связь с узлом сети ViPNet была установлена, все настройки, выполненные до проверки, сохраняются в конфигурационном файле `iplir.conf` ViPNet Coordinator HW. Нажмите **OK**, чтобы перейти к запуску драйверов и служб (шаг 38).

37 Если связь с узлом сети ViPNet установить не удалось, то для выяснения причины просмотрите журнал IP-пакетов:

37.1 В окне **Error: VPN probing has FAILED! Do you want to view IP packet log in order to investigate the issue?** нажмите **Yes**.

37.2 Просмотрите журнал и выясните причину. Подробнее о работе с журналом см. документ «Настройка с помощью командного интерпретатора».

37.3 Нажмите **Exit**, чтобы завершить просмотр журнала и заново настроить проверку связи ViPNet Coordinator HW с узлом сети ViPNet (шаг 28).

38 Запустите драйверы и службы ViPNet Coordinator HW перед завершением работы мастера — в окне **Do you want to start VPN services before leaving the installation wizard?** нажмите **Yes**.

39 Завершите инициализацию ViPNet Coordinator HW — в окне **Setup wizard is successfully completed** нажмите **Finish**.

После инициализации

1. Подключитесь к ViPNet Coordinator HW (ViPNet Coordinator VA) с помощью командного интерпретатора.
2. Пройдите аутентификацию с учетной записью локального администратора `admin`.
3. Перейдите в режим настройки:

   ```
   hostname> enable
   ```

4. Выясните IP-адрес доступа к ViPNet Prime:

   ```
   hostname# iplir node <ViPNet ID ViPNet Prime> show
   ```

5. Добавьте в файл `hosts` запись о соответствии IP-адреса доступа к ViPNet Prime и доменного имени ViPNet Prime:

   ```
   hostname# machine hosts add <IP-адрес доступа к ViPNet Prime> <доменное имя ViPNet Prime>
   ```

6. В таблице маршрутизации проверьте маршрут по умолчанию:

   ```
   hostname# inet show routing
   ```

   Если маршрут по умолчанию отсутствует, задайте статический маршрут по умолчанию (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка маршрутизации»). Убедитесь, что маршрут валиден.

7. По умолчанию доступ к ViPNet Coordinator HW (ViPNet Coordinator VA) по SSH заблокирован. Чтобы разрешить доступ, создайте фильтр защищённой сети:

   ```
   hostname# firewall vpn add rule "Allow SSH server" src <ViPNet ID узла | группа ViPNet ID узлов> dst @local service @ssh pass
   ```

   Удаленное подключение по SSH следует выполнять только с защищенных узлов ViPNet, связанных с ViPNet Coordinator HW (ViPNet Coordinator VA).

8. По умолчанию доступ к ViPNet Coordinator HW (ViPNet Coordinator VA) с помощью веб-интерфейса заблокирован. Чтобы разрешить доступ, создайте фильтр защищённой сети:

   ```
   hostname# firewall vpn add rule "Allow ViPNet WebGUI" src <ViPNet ID узла | группа ViPNet ID узлов> dst @local tcp dport 8080 pass
   ```

   Удаленное подключение с помощью веб-интерфейса следует выполнять только с защищенных узлов ViPNet, связанных с ViPNet Coordinator HW (ViPNet Coordinator VA).

9. Если вы предполагаете использовать локальную учетную запись `user` для аудита ViPNet Coordinator HW (ViPNet Coordinator VA), разблокируйте ее:

   ```
   hostname# user passwd
   Type the new user password:
   Confirm new user password:
   The new password has been successfully set.
   ```

10. Если в сети ViPNet используются ViPNet Coordinator HW (ViPNet Coordinator VA) любой из версий ниже, чем 4.5.1, настройте транспортные серверы MFTP (см. документ «Настройка с

помощью командного интерпретатора», раздел «Настройка транзитного режима транспортного сервера MFTP»).

A

Термины и сокращения

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 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 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 TIAS

Threat Intelligence Analytics System. Программно-аппаратный комплекс анализа событии информационной безопасности, поступающих от различных источников: ViPNet IDS NS, ViPNet IDS HS, ViPNet xFirewall, ViPNet Coordinator HW 5 и ViPNet EPP; автоматически выявляет инциденты информационной безопасности на основании потока этих событий.

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.

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

Набор симметричных ключей обмена с защищенными узлами сети ViPNet. Формируется в ViPNet Prime на основе заданных связей между узлами.

В ViPNet Coordinator HW версии 5.0 и выше используется дистрибутив ключей `ds5`. Содержит справочники, ключи и лицензии, необходимые для инициализации и работы ViPNet Coordinator HW.

В ViPNet Coordinator HW версий 4.4.x, ViPNet xFirewall и ViPNet Client используется дистрибутив ключей `dst`.

Защищенный интернет-шлюз (открытый интернет)

Технология, реализованная в программном обеспечении ViPNet. При подключении к интернету узлы локальной сети изолируются от защищенной сети, а при работе в защищенной сети — 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.

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.

Открытый узел

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

Политики безопасности

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

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.

Сообщение UT

Файл, передаваемый из ViPNet Prime в ViPNet Coordinator HW версии 5.x. Сообщение содержит один из компонентов:

- Политики безопасности.
- Обновление справочников и ключей ViPNet Coordinator HW.

Транспортный клиент UT

Клиентская часть транспортного компонента UT ViPNet Prime. Обеспечивает прием сообщений UT от транспортного сервера UT ViPNet Prime в ViPNet Coordinator HW версии 5.x, поддерживающего работу с дистрибутивом ключей `ds5`.

Транспортный конверт

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

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами сети ViPNet.

Транспортный сервер UT

Серверная часть транспортного компонента UT ViPNet Prime. Обеспечивает передачу сообщений UT от ViPNet Prime к транспортному клиенту UT ViPNet Coordinator HW версии 5.x, поддерживающего работу с дистрибутивом ключей `ds5`.

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 Prime каждой сети при организации взаимодействия между двумя различными сетями ViPNet.