ViPNet Coordinator HW 4

Общее описание

infotecs

ФРКЕ.00130-03 90 01

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, дом 1/23, строение 1

Тел: (495) 737-61-96 (горячая линия), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В документе описывается назначение и применение программно-аппаратного комплекса ViPNet Coordinator HW® (далее — ViPNet Coordinator HW) в составе защищенных сетей ViPNet, способы настройки и управления, приводится описание существующих исполнений ViPNet Coordinator HW, их аппаратных платформ и условий лицензирования.

Для кого предназначен документ

Документ предназначен для администраторов, отвечающих за настройку и эксплуатацию ViPNet Coordinator HW.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

При описании команд в данном документе используются следующие условные обозначения:

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

  ```
  hostname# команда
  ```

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

  ```
  hostname> команда
  ```

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

  ```
  команда <параметр>
  ```

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

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

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

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

Связанные документы

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

Таблица 3. Связанные документы

Документ	Содержание
«ViPNet Coordinator HW. Подготовка к работе»	Установка виртуального образа ViPNet Coordinator HW
	Установка, обновление и удаление справочников и ключей
	Обновление ПО ViPNet Coordinator HW, в том числе на кластере горячего резервирования
	Резервное копирование и восстановление настроек
«ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»	Настройка даты и времени
	Настройка подключения к сети (настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов, настройка подключения к сети 3G, 4G или Wi-Fi, использование динамических интерфейсов)
	Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, прокси-сервер, функциональность L2OverIP)
	Настройка подключения ViPNet Coordinator HW к внешней сети через межсетевой экран
	Настройка статической и динамической маршрутизации
	Настройка сетевых фильтров
	Настройка трансляции IP-адресов
	Настройка транспортного модуля MFTP
	Просмотр журнала конвертов MFTP
	Развертывание системы защиты от сбоев
	Настройка протоколирования событий и просмотр журналов (журналы устранения неполадок, журнал IP-пакетов)
«ViPNet Coordinator HW. Настройка с помощью веб-интерфейса»	Настройка даты и времени

Документ	Содержание
	Настройка подключения к сети (настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов, настройка подключения к сети 3G, 4G или Wi-Fi)
	Настройка динамической и статической маршрутизации
	Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, прокси-сервер, функциональность L2OverIP)
	Настройка сетевых фильтров
	Настройка трансляции IP-адресов
	Работа со списком защищенных узлов, связанных с ViPNet Coordinator HW
	Мониторинг состояния ViPNet Coordinator HW и просмотр журнала IP-пакетов
«ViPNet Coordinator HW. Сценарии работы»	Предоставление пользователям сети доступа в Интернет
	Организация демилитаризованной зоны (DMZ) в сети
	Настройка туннелей между удаленным клиентом и офисом, между двумя офисами
	Настройка ViPNet Coordinator HW для работы в качестве сервера открытого Интернета
	Развертывание типовых схем организации кластера горячего резервирования
	Организация обработки трафика из нескольких виртуальных локальных сетей (VLAN)
	Примеры настройки сервисных функций (DHCP-сервера, DHCP-relay агента, DNS- и NTP-сервера, центрального прокси-сервера)
	Настройка соединения между двумя удаленными сегментами сети с помощью технологии L2OverIP
	Организация обеспечения электропитания от UPS
«ViPNet Coordinator HW. Справочное руководство по командному интерпретатору»	Описание команд ViPNet Coordinator HW
«ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам»	Описание конфигурационных файлов управляющего демона и системы защиты от сбоев

Документ	Содержание
«ViPNet Coordinator HW. Лицензионные соглашения на компоненты сторонних производителей»	Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet Coordinator HW

Комплект поставки

В комплект поставки ViPNet Coordinator HW входят следующие компоненты:

- В зависимости от исполнения (см. «Описание исполнений ViPNet Coordinator HW» на стр. 38):
  - в случае исполнений ViPNet Coordinator HW — программно-аппаратный комплекс ViPNet Coordinator HW.
  - в случае исполнения ViPNet Coordinator HW VA — файл с образом виртуальной машины `va_vipnet_base_x86_64_4.x.x-xxxx.ova`.
- Файл обновления в формате LZH, необходимый для обновления ПО ViPNet Coordinator HW с более ранней версии на текущую.
- Документация в формате PDF:
  - «ViPNet Coordinator HW. Общее описание».
  - «ViPNet Coordinator HW. Подготовка к работе».
  - «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».
  - «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса».
  - «ViPNet Coordinator HW. Сценарии работы».
  - «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору».
  - «ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам».
  - «ViPNet Coordinator HW. Лицензионные соглашения на компоненты сторонних производителей».

Что нового в версии 4.2.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 4.2.1 по сравнению с версией 4.2. Информация об изменениях в предыдущих версиях содержится в приложении История версий (на стр. 71).

- **Поддержка новой аппаратной платформы ViPNet Coordinator HW**

  Реализована поддержка новой аппаратной платформы ViPNet Coordinator HW50 N4 на базе мини-компьютера Lanner NCA-1020C.

- **Фильтрация содержимого трафика, проходящего через прокси-сервер**

  Реализована фильтрация HTTP-трафика, проходящего через прокси-сервер, по его содержимому:

  - по MIME-типу файлов;
  - по методам протокола HTTP.

  Более подробную информацию см. в документах «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора» и «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса».

- **Антивирусная проверка трафика, проходящего через прокси-сервер**

  Реализована проверка трафика, проходящего через прокси-сервер, с помощью встроенного антивируса Kaspersky Anti-Virus. Более подробную информацию см. в документах «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса» и «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

- **Улучшенный поиск записей в журнале устранения неполадок**

  В новой версии ViPNet Coordinator HW появились следующие возможности работы с журналом устранения неполадок:

  - вывод результатов поиска в обратном хронологическом порядке;
  - просмотр записей, начиная с указанного момента времени;
  - просмотр записей только для указанной службы ViPNet или Linux;
  - поиск записей по части строки.

  Более подробную информацию см. в разделе «Просмотр журнала устранения неполадок» документа «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

- **Блокировка фрагментированных пакетов**

  В новой версии ViPNet Coordinator HW появилась настройка блокировки входящих фрагментированных IP-пакетов. Эта функция может быть полезна для защиты от DDoS-атак фрагментированными IP-пакетами. Более подробную информацию см. в разделе «Настройка дополнительных параметров межсетевого экрана» документа «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

- **Ограничение прав для просмотра журнала регистрации IP-пакетов**

В новой версии ViPNet Coordinator HW выполнение команды `iplir view` доступно только администратору. Подробнее см. раздел «Просмотр журнала регистрации IP-пакетов» документа «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

1

Общая информация

Защищенная сеть ViPNet

Программно-аппаратный комплекс ViPNet Coordinator HW предназначен для использования в защищенной сети ViPNet, построенной на основе комплекса программных продуктов ViPNet.

Сеть ViPNet представляет собой виртуальную защищенную сеть (см. глоссарий, стр. 88), которая может быть развернута поверх локальных или глобальных сетей любой структуры. В отличие от многих популярных VPN-решений, технология ViPNet обеспечивает защищенное взаимодействие между сетевыми узлами (см. глоссарий, стр. 90) по схеме «клиент-клиент».

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

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

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

Сетевые узлы ViPNet делятся на два типа:

- Клиент (ViPNet-клиент) (см. глоссарий, стр. 88) — рабочее место пользователя сети ViPNet.
- Координатор (ViPNet-координатор) (см. глоссарий, стр. 88) — сервер сети ViPNet. Сетевой узел ViPNet Coordinator HW является координатором.

Также сеть ViPNet может включать открытые узлы (компьютеры без программного обеспечения ViPNet), соединения которых через Интернет или другие публичные сети защищаются ViPNet-координаторами с помощью туннелирования на сетевом уровне (см. глоссарий, стр. 91).

Назначение ViPNet Coordinator HW

Программно-аппаратный комплекс ViPNet Coordinator HW распространяется в нескольких исполнениях. Каждое исполнение ViPNet Coordinator HW представляет собой интегрированное решение на базе специализированной аппаратной платформы, программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС GNU/Linux, а также роли, назначаемой сетевому узлу в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 87) и накладывающей определенные лицензионные ограничения (см. «Лицензирование ViPNet Coordinator HW» на стр. 28).

В качестве аппаратной платформы для исполнения ViPNet Coordinator HW может использоваться компактный компьютер или полноценный сервер, устанавливаемый в стандартные стойки. Существует также исполнение, не зависящее от аппаратной платформы, — ViPNet Coordinator HW VA, которое предназначено для развертывания на виртуальной машине. Характеристики всех поддерживаемых исполнений приведены в главе Описание исполнений ViPNet Coordinator HW (на стр. 38).

ViPNet Coordinator HW выступает в роли VPN-сервера и предназначен для использования в IP-сетях, защита которых организуется с применением комплекса программных продуктов ViPNet. Описание всех основных функций ViPNet Coordinator HW приведено в разделе Функции координатора в защищенной сети (на стр. 20).

ViPNet Coordinator HW также поддерживает следующие дополнительные возможности:

- Обработка прикладных протоколов FTP, DNS, H.323, SCCP, SIP для открытого трафика.
- Обработка трафика в виртуальных локальных сетях (поддержка VLAN IEEE 802.1 Q).
- Объединение нескольких физических сетевых интерфейсов в один логический — агрегированный интерфейс — для увеличения пропускной способности, повышения надежности, резервирования каналов связи.
- Выбор приоритетов для обрабатываемого IP-трафика в соответствии с протоколом DiffServ.
- Реализация функций DHCP-, DNS- и NTP-сервера.
- Реализация функций прокси-сервера с возможностью фильтрации HTTP-трафика по его содержимому и антивирусной проверки.
- Реализация функций клиента и точки доступа Wi-Fi.
- Реализация функций маршрутизатора IP-пакетов с возможностью настройки статической и динамической маршрутизации.
- Реализация функций кластера горячего резервирования.
- Взаимодействие с источником бесперебойного питания UPS (кроме исполнения ViPNet Coordinator HW VA).

- Совместимость с управляющим программным обеспечением ViPNet Administrator, ViPNet Policy Manager, ViPNet StateWatcher.

Функции координатора в защищенной сети

VPN-сервер в защищенной сети ViPNet называется координатором. Как правило, узел ViPNet Coordinator HW выполняет в сети одну или несколько функций в зависимости от задач, решаемых в рамках корпоративной сети, ее структуры, нагрузки на координатор и других факторов.

Координатор может выполнять в защищенной сети ViPNet следующие функции:

- Сервер IP-адресов (на стр. 20). Функция, которая позволяет обеспечить взаимодействие защищенных узлов ViPNet (см. глоссарий, стр. 91). Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.
- Маршрутизатор VPN-пакетов (на стр. 22). Функция, которая позволяет обеспечить маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы.
- Сервер соединений (на стр. 22). Функция, которая обеспечивает соединение клиентов и других координаторов друг с другом кратчайшим путем.
- VPN-шлюз (на стр. 23). Функция, которая позволяет организовать защищенные соединения между узлами локальных сетей (в том числе, на которых не установлено ПО ViPNet) и между сегментами сетей с помощью защищенных каналов (туннелей).
- Транспортный сервер (на стр. 25). Функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из программы ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 87), а также обмен прикладными транспортными конвертами (см. глоссарий, стр. 91) между узлами.
- Межсетевой экран (на стр. 26). Функция, которая позволяет обеспечить фильтрацию IP-трафика. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.
- Сервер открытого Интернета (на стр. 27). Функция, которая позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации.

Одновременно с этим ViPNet Coordinator HW поддерживает ряд дополнительных функций (см. «Назначение ViPNet Coordinator HW» на стр. 18).

Сервер IP-адресов

При подключении любого клиента с программой ViPNet Client (см. глоссарий, стр. 88) к сети или изменении его параметров подключения эти параметры сообщаются координатору, который играет роль сервера IP-адресов для данного клиента. В свою очередь, сервер IP-адресов

отправляет на клиент информацию о параметрах подключения и о состоянии всех узлов, с которыми у данного клиента имеется связь.

Таким образом, роль сервера IP-адресов заключается:

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

Рисунок 1. Сервер IP-адресов в сети ViPNet

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

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

Сервер IP-адресов работает по следующей логике:

- При появлении новой информации о своем клиенте (то есть о клиенте, который использует данный координатор в качестве сервера IP-адресов) координатор рассылает ее на другие свои клиенты и связанные координаторы.
- При появлении новой информации о клиентах других координаторов рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора.
- При отсутствии информации от своего клиента по истечении периода опроса координатор считает этот клиент недоступным и рассылает информацию об этом.
- В случае взаимодействия координатора с другой сетью ViPNet на шлюзовой координатор (см. глоссарий, стр. 91) другой сети высылается информация о состоянии всех узлов своей сети, связанных с узлами другой сети ViPNet. При получении такой информации из другой сети ViPNet координатор рассылает эту информации на все координаторы своей сети, а также на свои клиенты, связанные с узлами другой сети.

По умолчанию для клиента роль сервера IP-адресов выполняет его транспортный сервер (координатор, на котором клиент зарегистрирован в программе ViPNet Центр управления сетью). В

отличие от транспортного сервера, сервер IP-адресов можно сменить, выбрав любой другой координатор, с которым у данного клиента есть связь.

Маршрутизатор VPN-пакетов

Координатор осуществляет маршрутизацию транзитного защищенного трафика, который проходит через координатор на другие защищенные сетевые узлы. Маршрутизация осуществляется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями ViPNet.

Рисунок 2. Функция маршрутизации защищенного трафика в сети ViPNet

Маршрутизация защищенного трафика осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется трансляция сетевых адресов (NAT) (см. глоссарий, стр. 91). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора. Трансляция адресов для защищенного трафика выполняется автоматически в соответствии с параметрами, которые не могут быть изменены.

Сервер соединений

Координатор может выступать в качестве сервера соединений (см. глоссарий, стр. 90) и устанавливать соединения между клиентами и координаторами по кратчайшему пути, если они находятся в разных подсетях и не могут соединиться друг с другом напрямую. Для каждого клиента может быть назначен свой сервер соединений. По умолчанию сервером соединений для клиента выбран сервер IP-адресов. Для координаторов также при необходимости может быть выбран сервер соединений.

Рисунок 3. Организация соединений между сетевыми узлами ViPNet

На сервере соединений может быть настроен TCP-туннель, через который будет осуществляться соединение клиентов, находящихся во внешних сетях, с другими узлами сети ViPNet, в том случае, если интернет-провайдером блокируется протокол UDP.

Рисунок 4. Функция TCP-туннеля

Если удаленный клиент не может связаться с другими узлами по протоколу UDP, и на его сервере соединений (см. глоссарий, стр. 90) при этом настроен TCP-туннель, он автоматически начинает устанавливать с узлами соединение через TCP-туннель сервера соединений. На сервере соединений полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по протоколу UDP.

VPN-шлюз

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

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

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

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

Рисунок 5. Защита соединения на сетевом уровне модели OSI

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

Туннелирование на канальном уровне (или технология L2OverIP (см. глоссарий, стр. 86)) позволяет организовать защищенное соединение между узлами удаленных друг от друга сегментов сети, обеспечивая прямую связь между ними по протоколу Ethernet. С помощью этой технологии можно связывать различные сегменты в единую сеть вне зависимости от того, какие сетевые протоколы будут использоваться в этой сети (IP, IPX, MPLS, IEEE 802.2 и другие). При использовании протокола IP связанные через L2OverIP сегменты образуют единое адресное пространство в пределах одной IP-подсети.

Технология L2OverIP работает следующим образом:

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

Рисунок 6. Защита соединения на канальном уровне модели OSI

Функции туннелирования на канальном уровне не ограничиваются лицензией, при этом не поддерживаются исполнениями ViPNet Coordinator HW50 A, B и HW100 A, B. Для туннелирования требуется выполнить только ряд специальных настроек на координаторах, установленных на границе удаленных сегментов сети.

Транспортный сервер

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

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

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

Рисунок 7. Роль транспортного сервера в сети ViPNet

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

- Устанавливает соединение с сетевым узлом (по умолчанию такая логика действует при отправке конверта на другой транспортный сервер).
- Ожидает, когда соединение установит получатель конверта (по умолчанию эта логика действует при наличии конвертов для клиентов).

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

Межсетевой экран

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

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

Рисунок 8. Роль межсетевого экрана в сети ViPNet

Координатор также может осуществлять трансляцию сетевых адресов (NAT) для проходящего через него открытого трафика (см. глоссарий, стр. 91).

Примечание. Трансляция адресов для защищенного трафика осуществляется автоматически (см. «Маршрутизатор VPN-пакетов» на стр. 22).

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

- Для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов. Таким

образом, NAT позволяет компьютерам с локальными адресами получать доступ к Интернету от имени публичного адреса координатора.

Для решения этой задачи используется трансляция адреса источника.

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

  Для решения этой задачи используется трансляция адреса назначения.

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

Сервер открытого Интернета

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

Рисунок 9. Роль сервера открытого Интернета в сети ViPNet

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

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

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

Чтобы использовать на координаторе технологию «Открытый Интернет», в программе ViPNet Центр управления сетью для этого координатора следует включить функцию сервера открытого Интернета. Подробнее см. в документе «ViPNet Coordinator HW. Сценарии работы».

Лицензирование ViPNet Coordinator HW

Лицензирование ViPNet Coordinator HW осуществляется с помощью назначения сетевому узлу соответствующей роли в программе ViPNet Центр управления сетью (ЦУС). В таблице ниже приведены допустимые роли для различных исполнений ViPNet Coordinator HW. Соответствие исполнения назначенной роли проверяется при установке на ViPNet Coordinator HW справочников и ключей.

Таблица 4. Исполнения ViPNet Coordinator HW, их аппаратные платформы и соответствующие роли

Исполнение ViPNet Coordinator HW	Аппаратные платформы	Название роли
ViPNet Coordinator HW50 A	HW50 N1, N2, N3	Coordinator HW50 A
ViPNet Coordinator HW50 B	HW50 N1, N2, N3	Coordinator HW50 B
ViPNet Coordinator HW100 A	HW100 X1, X8	Coordinator HW100 A
ViPNet Coordinator HW100 B	HW100 X1, X8	Coordinator HW100 B
ViPNet Coordinator HW100 C	HW100 X2, X3, N1, N2, N3	Coordinator HW100 C
ViPNet Coordinator HW1000	HW1000 Q2,Q3, Q4	Coordinator HW1000
ViPNet Coordinator HW1000 C	HW1000 Q5	Coordinator HW1000 C
ViPNet Coordinator HW1000 D	HW1000 Q6	Coordinator HW1000 D
ViPNet Coordinator HW2000	HW2000 Q2, Q3, Q4	Coordinator HW2000
ViPNet Coordinator HW5000	HW5000 Q1	Coordinator HW5000
ViPNet Coordinator HW VA	HW VA	Coordinator HW-VA

Примечание. Исполнениям ViPNet Coordinator HW на аппаратных платформах HW50 N1, N2, N3 и HW100 X1, X8 могут быть назначены различные роли: Coordinator HW50 A, Coordinator HW50 B и Coordinator HW100 A, Coordinator HW100 B.

Роль может накладывать ограничения на поддержку функции транспортного сервера, на использование ViPNet Coordinator HW в кластере горячего резервирования, на функции туннелирования соединений на сетевом уровне. В таблице ниже приведены ограничения, накладываемые ролями.

Таблица 5. Лицензионные ограничения, накладываемые ролями

Название роли	Функции транспортного сервера	Использование в кластере горячего резервирования	Максимальное число туннелируемых соединений на сетевом уровне	Туннелирование на канальном уровне
Coordinator HW50 A	Нет	Да	2	Нет
Coordinator HW50 B	Нет	Да	5	Нет
Coordinator HW100 A	Нет	Да	2	Нет
Coordinator HW100 B	Нет	Да	5	Нет
Coordinator HW100 C	Да	Да	10	Да
Coordinator HW1000	Да	Да	Без ограничений	Да
Coordinator HW1000 C	Да	Да	Без ограничений	Да
Coordinator HW1000 D	Да	Да	Без ограничений	Да
Coordinator HW2000	Да	Да	Без ограничений	Да
Coordinator HW5000	Да	Да	Без ограничений	Да
Coordinator HW-VA	Да	Да	Задается в ЦУСе	Да

Внимание! Для организации кластера горячего резервирования на основе исполнений ViPNet Coordinator HW50 A, B или ViPNet Coordinator HW100 A, B, C необходимо дополнительно назначить сетевому узлу роль Failover100.

Для совместной работы в кластере вы можете использовать только одинаковые исполнения ViPNet Coordinator HW. Например, вы можете использовать в кластере исполнения ViPNet Coordinator HW1000 C на аппаратных платформах HW1000 Q2 и HW1000 Q3. Однако вы не можете использовать в кластере исполнения ViPNet Coordinator HW1000 C и ViPNet Coordinator HW1000 D.

Количество туннелируемых соединений на сетевом уровне, задаваемое в ЦУСе для исполнения ViPNet Coordinator HW VA, вычитается из общего числа туннелируемых соединений в лицензии на сеть ViPNet.

Внимание! В исполнениях ViPNet Coordinator HW50 A, B и ViPNet Coordinator HW100 A, B не поддерживаются функции шлюзового координатора (см. глоссарий, стр. 91) и транспортного сервера (см. глоссарий, стр. 91). Вследствие этого возникают следующие ограничения при формировании структуры сети ViPNet:

- Координатор, созданный для одного из этих исполнений, нельзя регистрировать в качестве шлюзового координатора в другие сети ViPNet. В противном случае работоспособность ViPNet Coordinator HW может быть нарушена.
- Клиенты ViPNet нельзя регистрировать за таким координатором. Координатор в данном случае может использоваться для туннелирования открытого IP-трафика (см. глоссарий, стр. 91).

Состав ПО ViPNet Coordinator HW

В состав ПО ViPNet Coordinator HW входят следующие основные функциональные модули:

- драйверы:
  - drviplir — основной драйвер ViPNet, взаимодействующий непосредственно с драйверами сетевых карт и контролирующий весь обмен трафиком данного компьютера с внешней сетью.
  - itcswd — watchdog-драйвер системы защиты от сбоев, контролирующий работоспособность демона failoverd.
  - itcscrpt — криптографический драйвер, осуществляющий шифрование данных по запросу драйвера drviplir.
  - l2overip — драйвер, который реализует технологию L2OverIP (туннелирование на канальном уровне).
- демоны:
  - iplircfg — осуществляет передачу необходимых параметров драйверу drviplir, рассылку и прием информации об IP-адресах клиентов, ведение журнала трафика и другие функции. Рекомендуется, чтобы этот демон всегда работал, но при завершении его работы драйвер drviplir продолжает работать и обмен трафиком не прерывается.
  - zebra — обеспечивает маршрутизацию IP-трафика.
  - failoverd — обеспечивает функционирование системы защиты от сбоев.
  - mftpd — обеспечивает прием и передачу транспортных конвертов между узлами сети ViPNet.
  - algd — осуществляет обработку прикладных протоколов.
  - snmpd — позволяет получать информацию о работе ViPNet Coordinator HW на удаленном узле по протоколу SNMP.
  - webgui-fcgi-server — обеспечивает функционирование сервера веб-интерфейса.

Режимы подключения ViPNet Coordinator HW к внешней сети

Для ViPNet Coordinator HW вы можете настроить один из следующих режимов подключения к внешней сети:

- Подключение через межсетевой экран с динамической трансляцией адресов (на стр. 33).
- Подключение без использования внешнего межсетевого экрана.

Подробное описание настройки каждого из режимов приведено в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

Подключение через координатор

Если необходимо защитить трафик отдельного сегмента внутри локальной сети, на границе которой уже установлен координатор, выполняющий функции межсетевого экрана для клиентов этой локальной сети, то на границу такого сегмента может быть установлен второй координатор.

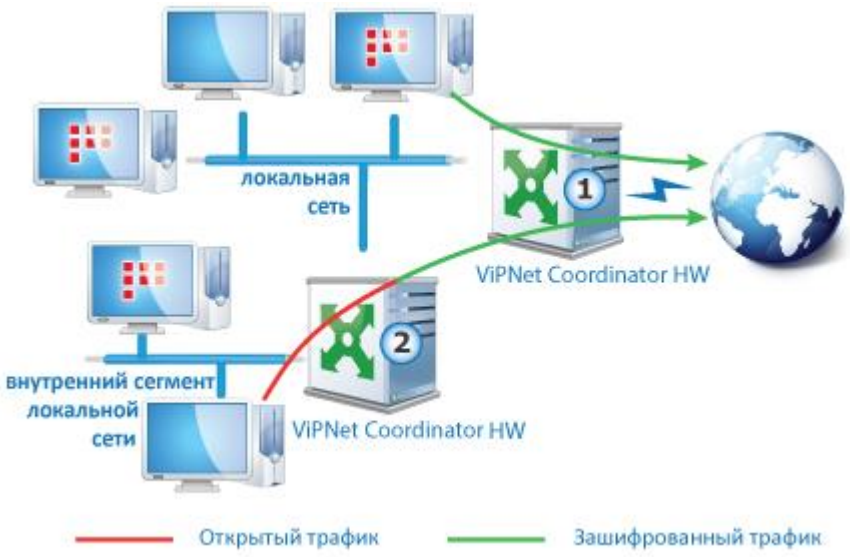

Рисунок 10. Подключение координатора через другой координатор

При этом координатор 1 (см. рисунок выше) должен быть выбран в качестве межсетевого экрана для координатора 2. Между двумя координаторами не должно быть никаких устройств, осуществляющих трансляцию адресов (NAT).

Такое включение координаторов называется каскадным включением. В результате для координаторов будет реализована автоматическая маршрутизация зашифрованного трафика из внутреннего сегмента сети как в локальную, так и в глобальную сеть.

Подключение через межсетевой экран со статической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT) и позволяющий настроить статические правила трансляции, между этим межсетевым экраном и узлами локальной сети следует установить координатор. На координаторе в этом случае должны быть настроены параметры подключения через межсетевой экран со статической трансляцией адресов. Для клиентов локальной сети данный координатор следует использовать в качестве сервера соединений.

Рисунок 11. Подключение координатора через межсетевой экран со статической трансляцией адресов

Подключение через межсетевой экран с динамической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT), и на нем затруднительно настроить статические правила трансляции, то для защиты IP-трафика локальной сети, в том числе и при инициативных соединениях снаружи, на координаторе можно настроить подключение через межсетевой экран с динамической трансляцией адресов.

Для координатора с данным типом подключения должен существовать постоянно доступный ViPNet-координатор, расположенный во внешней сети, который будет являться сервером соединений (см. глоссарий, стр. 90).

Рисунок 12. Подключение координатора через межсетевой экран с динамической трансляцией адресов

Сервер соединений должен быть доступен из внешней сети по публичному IP-адресу. Через него будет устанавливаться соединение между координатором локальной сети и удаленными узлами до тех пор, пока не будет установлено соединение напрямую.

Подключение без использования межсетевого экрана

Подключение без использования межсетевого экрана следует настраивать на координаторе в том случае, если ни один из его сетевых интерфейсов не находится за устройством NAT, то есть когда координатор доступен из маршрутизируемой сети. Если координатор должен быть доступен для других узлов, находящихся во внешних сетях, то один из его интерфейсов должен иметь публичный IP-адрес.

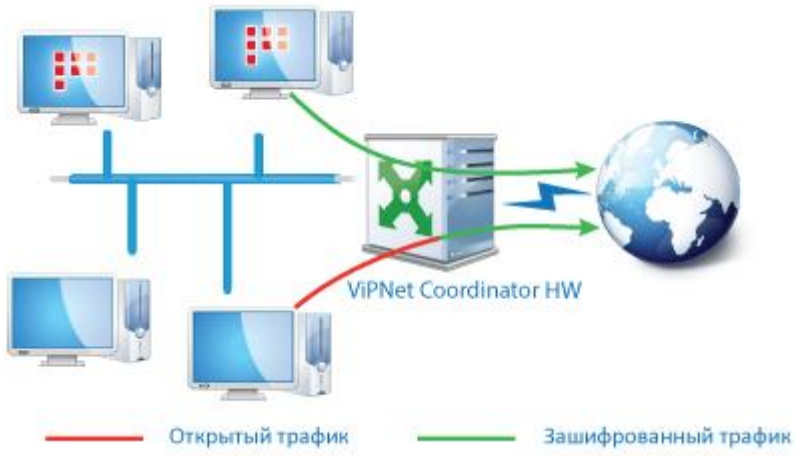

Рисунок 13. Подключение координатора без использования межсетевого экрана

Обработка сетевого трафика в соответствии с его приоритетом

В ViPNet Coordinator HW реализована поддержка протокола классификации сетевого трафика DiffServ (см. глоссарий, стр. 86). Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена DSCP-метка (см. глоссарий, стр. 86), задающая приоритет обработки пакета.

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

ViPNet Coordinator HW поддерживает следующие политики обработки трафика с учетом приоритета в соответствии с RFC 2474 https://tools.ietf.org/html/rfc2474 и RFC 2475 https://tools.ietf.org/html/rfc2475:

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

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

Назначение и принципы работы системы защиты от сбоев

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNet Coordinator HW и создания отказоустойчивого решения на базе узлов ViPNet Coordinator HW. Данная система может работать в одиночном режиме (см. «Работа системы защиты от сбоев в одиночном режиме» на стр. 36) или в режиме кластера горячего резервирования (см. «Работа системы защиты от сбоев в режиме кластера горячего резервирования» на стр. 36).

Настройка системы защиты от сбоев выполняется путем редактирования конфигурационного файла `failover.ini`. Подробнее о параметрах, содержащихся в этом файле см. в документе «ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам».

Работа системы защиты от сбоев в одиночном режиме

По умолчанию в ViPNet Coordinator HW система защиты от сбоев работает в одиночном режиме. При этом данная система обеспечивает постоянную работоспособность программы, выполняя следующие функции:

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

Работа системы защиты от сбоев в режиме кластера горячего резервирования

Помимо контроля работоспособности программы ViPNet Coordinator HW (см. «Работа системы защиты от сбоев в одиночном режиме» на стр. 36), в режиме кластера горячего резервирования система защиты от сбоев позволяет передавать функции вышедшего из строя сервера другому (резервному) серверу. Кластер горячего резервирования состоит из двух взаимосвязанных серверов ViPNet Coordinator HW:

- активного сервера — который работает в активном режиме и выполняет функции координатора ViPNet;
- пассивного сервера — который работает в пассивном режиме, то есть в режиме ожидания.

В случае сбоев, критичных для работоспособности ViPNet Coordinator HW на активном сервере, пассивный сервер переключается в активный режим и выполняет функции сбойного сервера, который после перезагрузки переходит в пассивный режим.

При работе в режиме кластера горячего резервирования некоторые функции ViPNet Coordinator HW недоступны (см. «Функции ViPNet Coordinator HW, недоступные в режиме кластера горячего резервирования» на стр. 37).

Функции ViPNet Coordinator HW, недоступные в режиме кластера горячего резервирования

В режиме кластера недоступны следующие сетевые службы ViPNet Coordinator HW:

- DHCP-сервер.
- Служба DHCP-relay.
- Модули Wi-Fi и 3G/4G.

Перед переключением в режим кластера горячего резервирования необходимо отключить перечисленные функции.

2

Описание исполнений ViPNet Coordinator HW

Исполнения ViPNet Coordinator HW50

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

Аппаратные платформы, на которых распространяются исполнения ViPNet Coordinator HW50, приведены в таблице ниже.

Примечание. Оба исполнения распространяются на одних и тех же аппаратных платформах, но имеют различные ограничения на максимальное число туннелируемых соединений на сетевом уровне (см. «Лицензирование ViPNet Coordinator HW» на стр. 28).

Таблица 6. Аппаратные платформы для исполнений ViPNet Coordinator HW50

Исполнение	Аппаратные платформы	Максимальное число туннелируемых соединений на сетевом уровне
ViPNet Coordinator HW50 A	HW50 N1, N2, N3, N4	2
ViPNet Coordinator HW50 B	HW50 N1, N2, N3, N4	5

Аппаратные платформы HW50 N1, N2, N3 представляют собой мини-компьютеры NCA-1010A с низким уровнем тепловыделения и энергопотребления, производимые компанией Lanner Electronics Incorporated, и различаются наличием дополнительных расширений:

- HW50 N1 — компьютер NCA-1010A без расширений.
- HW50 N2 — компьютер NCA-1010A с Wi-Fi-адаптером.
- HW50 N3 — компьютер NCA-1010A с 3G-модемом.

Аппаратные платформы HW50 N1, N2, N3 имеют следующие технические характеристики:

Таблица 7. Характеристики HW50 N1, N2, N3

Характеристика	Описание
Форм-фактор	Компьютер Lanner NCA-1010A
Размеры (ШхВхГ)	124,3x19,4x119,7 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В

Характеристика	Описание
Потребляемая мощность	До 36 Вт
Источник постоянного тока	12 В, 3 А
Процессор	Intel Atom E3815
Оперативная память	2 Гбайт
Накопители	SSD 2 Гбайт
Сетевые порты	3 порта Ethernet RJ45 10/100/1000 Мбит/с
3G-модем	Только в аппаратной платформе HW50 N3
Адаптер Wi-Fi	Только в аппаратной платформе HW50 N2
Порты ввода-вывода	1 порт HDMI 1 служебный порт RJ45 1 порт USB 2.0 1 порт USB 3.0

Аппаратная платформа HW50 N4 представляет собой мини-компьютер NCA-1020C с низким уровнем тепловыделения и энергопотребления, производимый компанией Lanner Electronics Incorporated, и поставляется без дополнительных расширений.

Аппаратная платформа HW50 N4 имеет следующие технические характеристики:

Таблица 8. Характеристики HW50 N4

Характеристика	Описание
Форм-фактор	Компьютер Lanner NCA-1020C
Размеры (ШхВхГ)	136,76x35,5x119,66 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Потребляемая мощность	До 36 Вт
Источник постоянного тока	12 В, 3 А
Процессор	Intel Celeron N3010 (2 ядра)
Оперативная память	2 Гбайт
Накопители	SSD 2 Гбайт
Сетевые порты	3 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	1 порт HDMI 1 служебный порт RJ45 1 порт USB 2.0 1 порт USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

На передней панели аппаратных платформ HW50 N1, N2, N3, N4 расположен разъем USB 2.0, порт HDMI, а также служебный разъем RJ45, предназначенный для подключения компьютера (ноутбука) при установке справочников и ключей.

Рисунок 14. Передняя панель ViPNet Coordinator HW50

Остальные коммуникационные разъемы находятся на задней панели:

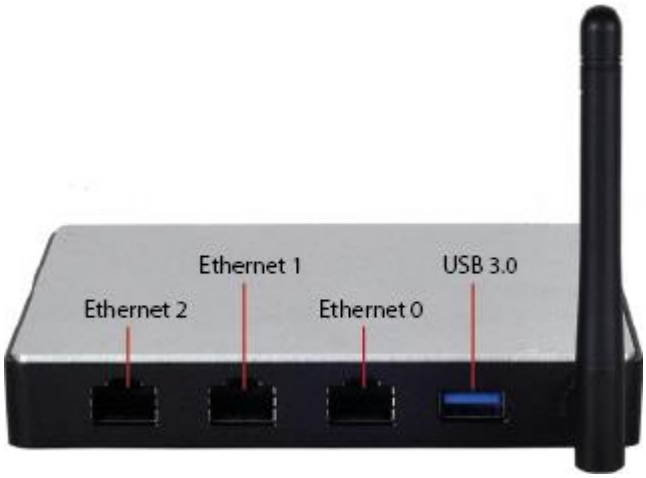

Рисунок 15. Задняя панель ViPNet Coordinator HW50

Примечание. Чтобы вставить SIM-карту оператора связи во встроенный 3G-модем аппаратной платформы HW50 N3, необходимо разобрать корпус мини-компьютера (см. раздел «Установка SIM-карты в HW50 N3 и HW100 N3» в документе «ViPNet Coordinator HW. Подготовка к работе»).

Исполнения ViPNet Coordinator HW100

Исполнения ViPNet Coordinator HW100 имеют компактные габаритные размеры и небольшой вес, поэтому их использование особенно оправдано в местах, где физическое пространство ограничено. Исполнения могут быть использованы для защиты филиалов компаний и небольших удаленных офисов.

Аппаратные платформы, на которых распространяются исполнения ViPNet Coordinator HW100, приведены в таблице ниже.

Примечание. Исполнения ViPNet Coordinator HW100 A и ViPNet Coordinator HW100 B распространяются на одних и тех же аппаратных платформах, но имеют различные ограничения на максимальное число туннелируемых соединений на сетевом уровне (см. «Лицензирование ViPNet Coordinator HW» на стр. 28).

Таблица 9. Аппаратные платформы для исполнений ViPNet Coordinator HW100

Исполнение	Аппаратные платформы	Максимальное число туннелируемых соединений на сетевом уровне
ViPNet Coordinator HW100 A	HW100 X1, X8	2
ViPNet Coordinator HW100 B	HW100 X1, X8	5
ViPNet Coordinator HW100 C	HW100 X2, X3, N1, N2, N3	10

Аппаратные платформы для исполнений ViPNet Coordinator HW100 представляют собой мини-компьютеры с пассивным охлаждением (без вентилятора охлаждения), производимые компаниями Lex Computech и Lanner с низким уровнем тепловыделения и энергопотребления.

Технические характеристики аппаратных платформ для исполнений ViPNet Coordinator HW100 приведены в следующих разделах:

- Аппаратные платформы HW100 X1, X2, X3, X8 (на стр. 42).
- Аппаратные платформы HW100 N1, N2, N3 (на стр. 44).

Аппаратные платформы HW100 X1, X2, X3, X8

Аппаратные платформы HW100 X1, X2, X3, X8 имеют следующие технические характеристики:

Таблица 10. Характеристики HW100 X1, X2, X3, X8

Характеристика	Описание
Форм-фактор	Компьютер BK3741S-00C серии BRIK (HW100 X1, X2) Компьютер BK3791S-00C серии BRIK (HW100 X3, X8)
Размеры (ШхВхГ)	187x130x52 мм
Масса	1 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Потребляемая мощность	До 25 Вт
Источник постоянного тока	12 В, 5 А
Процессор	Intel Atom N270 (HW100 X1, X2) Intel Atom N2600 (HW100 X3, X8)
Оперативная память	От 1 Гбайт (HW100 X1, X2) От 2 Гбайт (HW100 X3, X8)
Накопители	SSD от 1 Гбайт (HW100 X1, X2) SSD от 2 Гбайт (HW100 X3, X8) HDD от 80 Гбайт (HW100 X2, X3)
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	VGA 2 порта USB 2.0 COM-порт RS-232 (только в аппаратных платформах HW100 X3, X8)

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

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

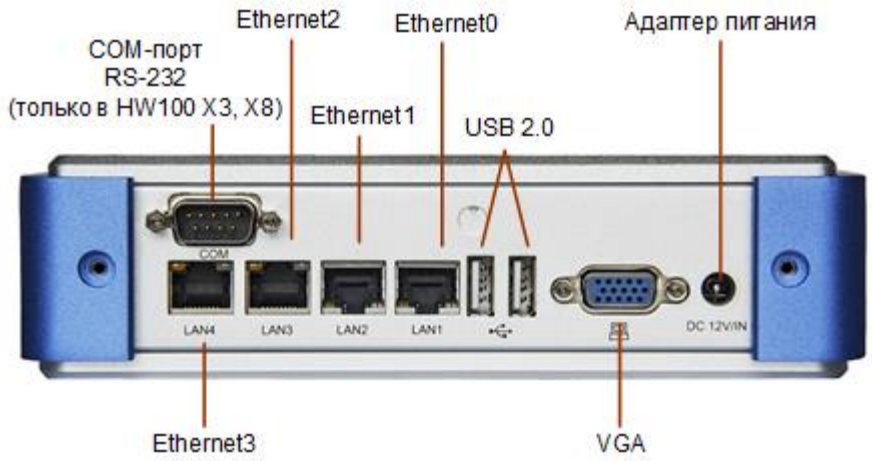

Рисунок 16. Задняя панель HW100 X1, X2, X3, X8

Аппаратные платформы HW100 N1, N2, N3

Аппаратные платформы HW100 N1, N2, N3 различаются наличием дополнительных расширений:

- HW100 N1 — компьютер Lanner LEC-6032-IT2 без расширений.
- HW100 N2 — компьютер Lanner LEC-6032-IT2 с Wi-Fi-адаптером.
- HW100 N3 — компьютер Lanner LEC-6032-IT2 с 3G-модемом.

Аппаратные платформы HW100 N1, N2, N3 имеют следующие технические характеристики:

Таблица 11. Характеристики HW100 N1, N2, N3

Характеристика	Описание
Форм-фактор	Компьютер Lanner LEC-6032-IT2
Размеры (ШхВхГ)	170x138x41,5
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Источник постоянного тока	24 В, 2,5 А
Процессор	Intel Celeron N2807
Оперативная память	От 2 Гбайт
Накопители	SSD от 2 Гбайт HDD от 80 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 1 порт Ethernet SFP 1 Гбит/с
3G-модем	Только в аппаратной платформе HW100 N3
Адаптер Wi-Fi	Только в аппаратной платформе HW100 N2

Характеристика	Описание
Порты ввода-вывода	1 порт VGA 1 служебный порт RJ45 1 порт USB 2.0 1 порт USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

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

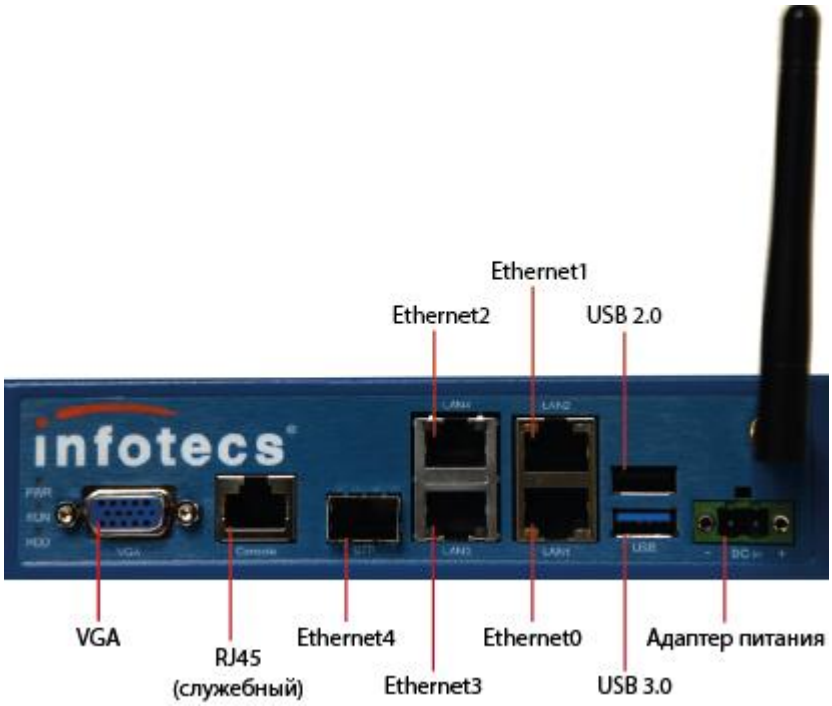

Рисунок 17. Задняя панель HW100 N1, N2, N3

Примечание. Чтобы вставить SIM-карту оператора связи во встроенный 3G-модем аппаратной платформы HW100 N3, необходимо разобрать корпус мини-компьютера (см. раздел «Установка SIM-карты в HW 50 N3 и HW100 N3» в документе «ViPNet Coordinator HW. Подготовка к работе»).

Аппаратные платформы HW100 N1, N2, N3 имеют однопортовый сетевой адаптер SFP (порт Ethernet 4), с которым совместим SFP-трансивер модели AFBR 5710PZ производства Avago Technologies.

Исполнения ViPNet Coordinator HW1000

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

Аппаратные платформы, на которых распространяются исполнения ViPNet Coordinator HW1000, приведены в таблице ниже.

Таблица 12. Аппаратные платформы для исполнений ViPNet Coordinator HW1000

Исполнение	Аппаратные платформы
ViPNet Coordinator HW1000	HW1000 Q2, Q3, Q4
ViPNet Coordinator HW1000 C	HW1000 Q5
ViPNet Coordinator HW1000 D	HW1000 Q6

Аппаратные платформы для исполнений ViPNet Coordinator HW1000 представляют собой серверы AquaServer серии T40 производства ГК «Аквариус».

Технические характеристики аппаратных платформ для исполнений ViPNet Coordinator HW1000 приведены в следующих разделах:

- Аппаратные платформы HW1000 Q2, Q3 (на стр. 46).
- Аппаратные платформы HW1000 Q4, Q5, Q6 (на стр. 47).

Аппаратные платформы HW1000 Q2, Q3

Аппаратные платформы HW1000 Q2 и Q3 имеют следующие технические характеристики:

Таблица 13. Характеристики HW1000 Q2, Q3

Характеристика	Описание
Форм-фактор	Сервер AquaServer T40 S44 19" Rack 1U
Размеры (ШхВхГ)	432x43,6x375 мм
Масса	6,5 кг
Питание	Встроенный блок питания мощностью 220 Вт, 110–220 В
Потребляемая мощность	До 155 Вт
Источник постоянного тока	Отсутствует

Характеристика	Описание
Процессор	Intel Core i3-530 (HW1000 Q2) Intel Core i5-750 (HW1000 Q3)
Оперативная память	От 2 Гбайт
Накопители	SSD от 2 Гбайт HDD от 240 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	VGA PS/2-совместимая клавиатура, PS/2-совместимая мышь COM-порт RS-232 4 порта USB 2.0 1 порт IPMI

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

На передней панели HW1000 Q2, Q3 расположены 2 разъема USB 2.0, остальные коммуникационные разъемы находятся на задней панели.

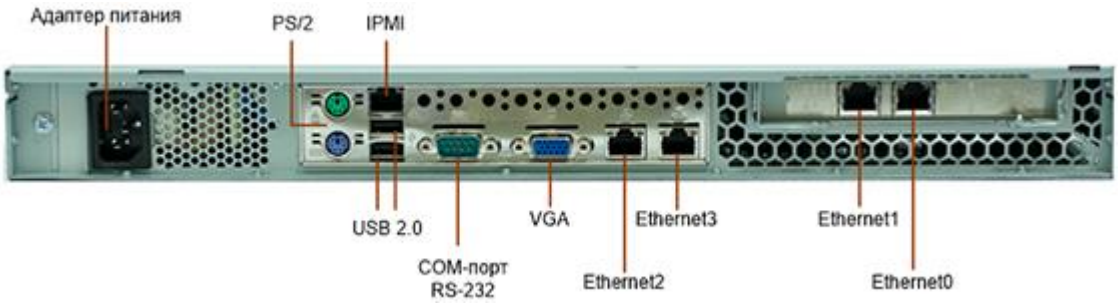

Рисунок 18. Задняя панель ViPNet Coordinator HW1000 Q2/Q3

Аппаратные платформы HW1000 Q4, Q5, Q6

Аппаратные платформы HW1000 Q4, Q5, Q6 имеют следующие технические характеристики:

Таблица 14. Характеристики HW1000 Q4, Q5, Q6

Характеристика	Описание
Форм-фактор	Сервер AquaServer T41 S24 19” Rack 1U
Размеры (ШхВхГ)	430x43,4x380 мм
Масса	7,2 кг
Питание	Встроенный блок питания мощностью 250 Вт, 100–240 В

Характеристика	Описание
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Процессор	HW1000 Q4: Intel Celeron G1820 HW1000 Q5, Q6: Intel Core i3-4360
Оперативная память	От 2 Гбайт
Накопители	SSD от 2 Гбайт HDD от 500 Гбайт
Сетевые порты	HW1000 Q4: 4 порта Ethernet RJ45 10/100/1000 Мбит/с HW1000 Q5: 6 портов Ethernet RJ45 10/100/1000 Мбит/с HW1000 Q6: 4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP 1 Гбит/с
Порты ввода-вывода	2 порта VGA PS/2-совместимая клавиатура, PS/2-совместимая мышь COM-порт RS-232 4 порта USB 2.0 2 порта USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

На передней панели HW1000 Q4, Q5, Q6 расположены COM-порт, 2 разъема USB 2.0 и порт VGA.

Рисунок 19. Передняя панель HW1000 Q4, Q5, Q6

Остальные коммуникационные разъемы находятся на задней панели.

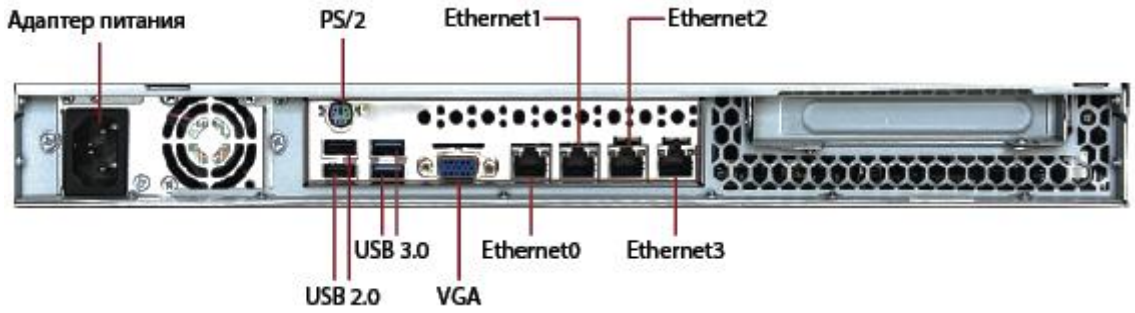

Рисунок 20. Задняя панель HW1000 Q4

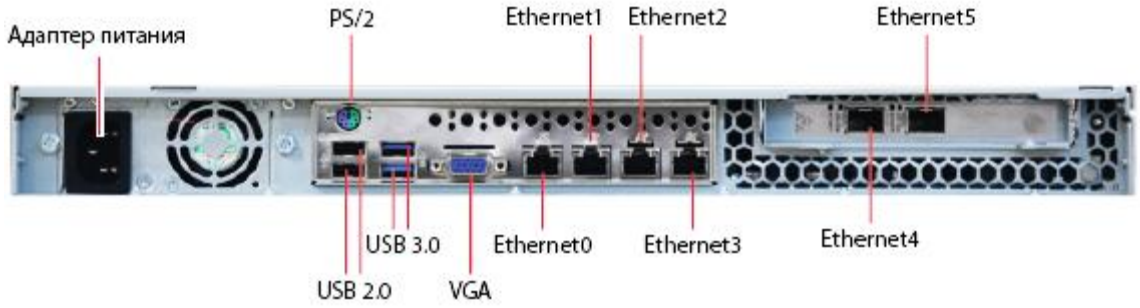

Рисунок 21. Задняя панель HW1000 Q5, Q6

Аппаратная платформа HW1000 Q6 имеет двухпортовый сетевой адаптер (порты Ethernet 4 и Ethernet 5), с которым совместим SFP-трансивер модели Avago AFBR 5710PZ (один трансивер этой модели входит в комплект поставки).

Исполнение ViPNet Coordinator HW2000

Исполнение ViPNet Coordinator HW2000 устанавливается в телекоммуникационную стойку 19". Благодаря использованию серверов с процессорами Intel Xeon и высокоскоростных сетевых интерфейсов, исполнение ViPNet Coordinator HW2000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа в ЦОДы (центры обработки данных) и к ресурсам облачных вычислений.

Примечание. Исполнение ViPNet Coordinator HW2000 на аппаратной платформе HW2000 Q4 имеет укороченный корпус.

Исполнение ViPNet Coordinator HW2000 распространяется на аппаратных платформах HW2000 Q2, HW2000 Q3 и HW2000 Q4.

Аппаратные платформы для исполнений ViPNet Coordinator HW2000 представляют собой серверы AquaServer серии T50 производства ГК «Аквариус».

Технические характеристики аппаратных платформ для исполнения ViPNet Coordinator HW2000 приведены в следующих разделах:

- Аппаратная платформа HW2000 Q2 (на стр. 50).
- Аппаратная платформа HW2000 Q3 (на стр. 52).
- Аппаратная платформа HW2000 Q4 (на стр. 53).

Все аппаратные платформы для исполнения ViPNet Coordinator HW2000 имеют двухпортовые сетевые адаптеры Intel Ethernet SPF+. С адаптерами этой серии совместимы только следующие модели SFP-трансиверов:

- AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies;
- E10GSFPSR производства Intel Corporation;
- E10GSFPLR производства Intel Corporation.

Аппаратная платформа HW2000 Q2

Аппаратная платформа HW2000 Q2 имеет следующие технические характеристики:

Таблица 15. Характеристики HW2000 Q2

Характеристика	Описание
Форм-фактор	Сервер AquaServer T50 D57 19" Rack 1U
Размеры (ШхВхГ)	444x43x685 мм
Масса	15 кг
Питание	Встроенный блок питания мощностью 600 Вт, 100–240 В
Потребляемая мощность	470 Вт
Источник постоянного тока	Отсутствует
Процессор	2xIntel Xeon E5645
Оперативная память	От 4 Гбайт
Накопители	SSD от 2 Гбайт HDD от 480 Гбайт
Сетевые порты	2 порта Ethernet RJ45 10/100/1000 Мбит/с 4 порта Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-совместимая клавиатура, PS/2-совместимая мышь COM-порт RS-232 4 порта USB 2.0 1 порт IPMI

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

На передней панели HW2000 Q2 расположены 2 разъема USB:

Рисунок 22. Передняя панель ViPNet Coordinator HW2000 Q2, Q3

Остальные коммуникационные разъемы находятся на задней панели:

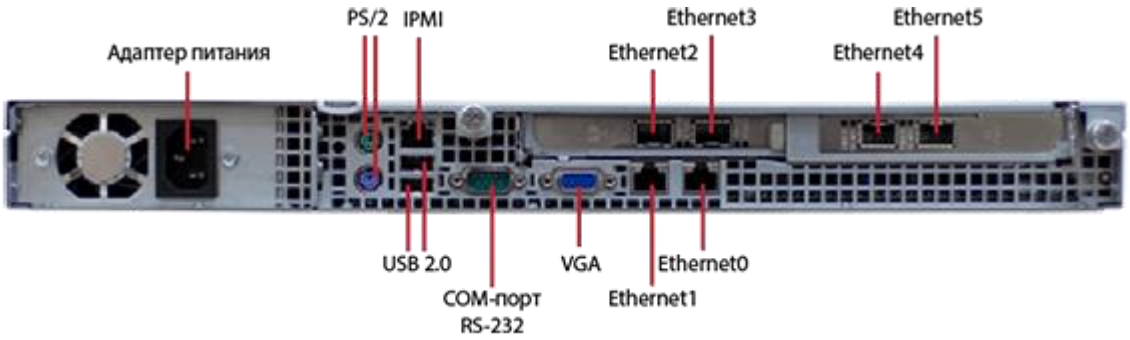

Рисунок 23. Задняя панель ViPNet Coordinator HW2000 Q2

Аппаратная платформа HW2000 Q3

Аппаратная платформа HW2000 Q3 имеет следующие технические характеристики:

Таблица 16. Характеристики HW2000 Q3

Характеристика	Описание
Форм-фактор	Сервер AquaServer T50 D14 19” Rack 1U
Размеры (ШхВхГ)	444x43,4x615 мм
Масса	15 кг
Питание	Встроенный блок питания мощностью 600 Вт, 100–240 В
Потребляемая мощность	До 440 Вт
Источник постоянного тока	Отсутствует
Процессор	2xIntel Xeon E5-2620 v2
Оперативная память	От 8 Гбайт
Накопители	SSD от 2 Гбайт HDD от 1000 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 4 порта Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-совместимая клавиатура, PS/2-совместимая мышь COM-порт RS-232 4 порта USB 2.0 1 порт IPMI

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

Аналогично аппаратной платформе HW2000 Q2 (см. рисунок на стр. 51), на передней панели HW2000 Q3 расположены 2 разъема USB.

Остальные коммуникационные разъемы находятся на задней панели:

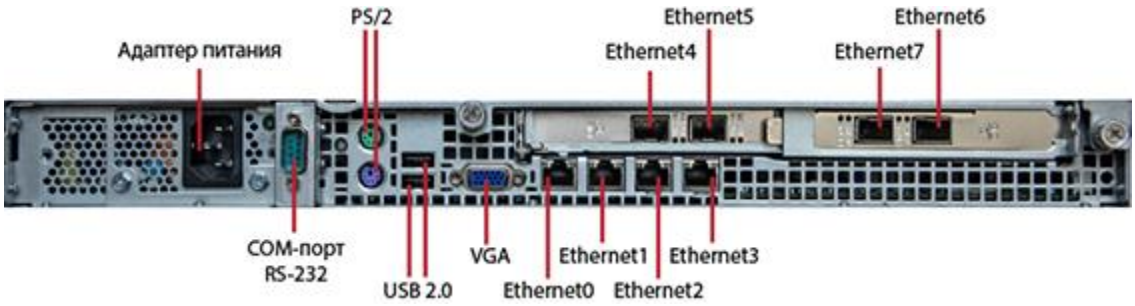

Рисунок 24. Задняя панель ViPNet Coordinator HW2000 Q3

Аппаратная платформа HW2000 Q4

Аппаратная платформа HW2000 Q4 имеет следующие технические характеристики:

Таблица 17. Характеристики HW2000 Q4

Характеристика	Описание
Форм-фактор	Сервер AquaServer T51 D14 — 1U в укороченном корпусе
Размеры (ШхВхГ)	444x44x383 мм
Масса	13 кг
Питание	Встроенный блок питания мощностью 500 Вт, 100-127 В/200-240 В
Потребляемая мощность	310 Вт
Источник постоянного тока	Отсутствует
Процессор	2xIntel Xeon E5-2609v3
Оперативная память	От 4 Гбайт
Накопители	SSD от 2 Гбайт HDD от 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP+ 10 Гбит/с 2 порта Broadcom Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши COM-порт RS-232 2 порта USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

На передней панели HW2000 Q4 расположен COM-порт RS-232.

Остальные коммуникационные разъемы находятся на задней панели:

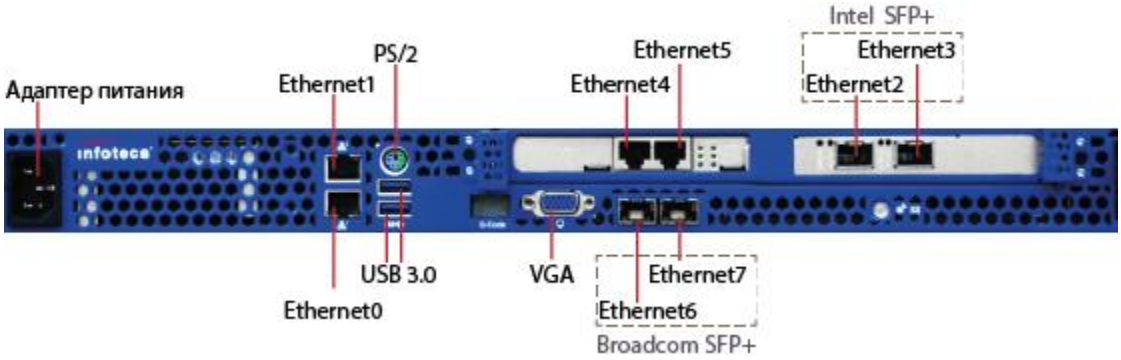

Рисунок 25. Задняя панель ViPNet Coordinator HW2000 Q4

Помимо двухпортового сетевого адаптера Intel Ethernet SFP+ аппаратная платформа ViPNet Coordinator HW2000 Q4 имеет двухпортовый сетевой адаптер Broadcom Ethernet SFP+. С этим адаптером совместимы только следующие модели SFP-трансиверов:

- AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies;
- E10GSFPLR производства Intel Corporation.

Исполнение ViPNet Coordinator HW5000

Исполнение ViPNet Coordinator HW5000 устанавливается в телекоммуникационную стойку 19″ и имеет укороченный корпус. Благодаря использованию сервера с процессором Intel Xeon последнего поколения и высокоскоростных сетевых интерфейсов, а также благодаря компактному форм-фактору, исполнение ViPNet Coordinator HW5000 является идеальным решением для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных (ЦОДы) и к ресурсам облачных вычислений в ограниченном пространстве телекоммуникационных стоек.

Исполнение ViPNet Coordinator HW5000 распространяется на аппаратной платформе HW5000 Q1.

Аппаратная платформа HW5000 Q1 представляет собой сервер сверхвысокой производительности AquaServer T51 D14 производства ГК «Аквариус».

Аппаратная платформа HW5000 Q1 имеет следующие технические характеристики:

Таблица 18. Характеристики HW5000 Q1

Характеристика	Описание
Форм-фактор	Сервер AquaServer T51 D14 — 1U в укороченном корпусе
Размеры (ШхВхГ)	444x44x383 мм
Масса	13 кг
Питание	Встроенный блок питания мощностью 500 Вт, 100-127 В/200-240 В
Потребляемая мощность	310 Вт
Источник постоянного тока	Отсутствует
Процессор	2xIntel Xeon E5-2620v3
Оперативная память	8 Гбайт
Накопители	SSD 2 Гбайт HDD 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP+ 10 Гбит/с 2 порта Broadcom Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши COM-порт RS-232 2 порта USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet, функционирующее под управлением адаптированной ОС GNU/Linux.

На передней панели HW5000 Q1 расположен COM-порт RS-232.

Остальные коммуникационные разъемы находятся на задней панели:

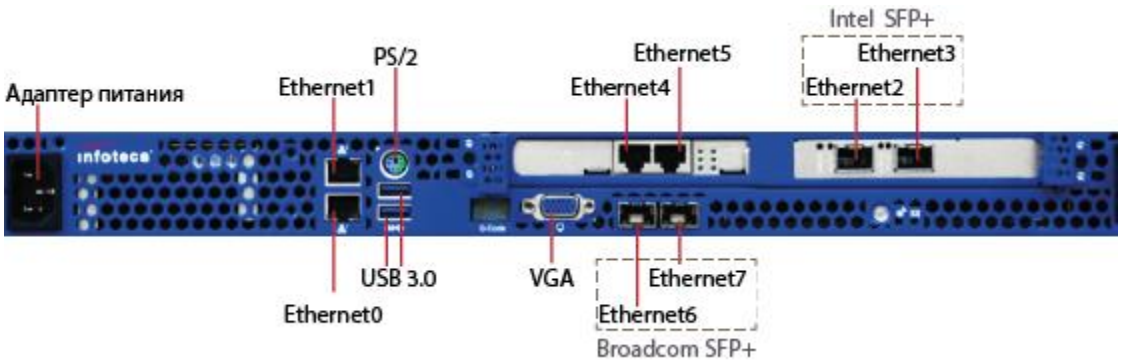

Рисунок 26. Задняя панель ViPNet Coordinator HW5000 Q1

Аппаратная платформа HW5000 Q1 имеет двухпортовый сетевой адаптер Intel Ethernet SFP+. С адаптерами этой серии совместимы только следующие модели SFP-трансиверов:

- AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies;
- E10GSFPSR производства Intel Corporation;
- E10GSFPLR производства Intel Corporation.

Аппаратная платформа HW5000 Q1 имеет двухпортовый сетевой адаптер Broadcom Ethernet SFP+. С этим адаптером совместимы только следующие модели SFP-трансиверов:

- AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies;
- E10GSFPLR производства Intel Corporation.

Исполнение ViPNet Coordinator HW VA

Исполнение ViPNet Coordinator HW VA представляет собой программное обеспечение, которое функционирует под управлением адаптированной ОС GNU/Linux. Поддерживаемые платформы виртуализации: VMware Workstation, VMware vSphere и Oracle VM VirtualBox. Работа на других платформах виртуализации не гарантируется.

Внимание! В исполнении ViPNet Coordinator HW VA установлено следующее ограничение: для шифрования трафика вы можете использовать не более двух процессоров.

Коммутация 10-гигабитных сетевых портов в ViPNet Coordinator HW2000 и HW5000

Аппаратные платформы HW2000 Q2 и HW2000 Q3 имеют несколько двухпортовых 10-гигабитных сетевых адаптеров Intel Ethernet серии X520.

Аппаратные платформы HW2000 Q4 и HW5000 Q1 имеют по одному двухпортовому 10-гигабитному сетевому адаптеру Intel Ethernet SFP+ и по одному двухпортовому 10-гигабитному сетевому адаптеру Broadcom Ethernet SFP+.

Для подключения всех перечисленных адаптеров к сети можно использовать как SFP-трансиверы, так и кабели, напрямую подключаемые к адаптерам. Подключаемый кабель должен удовлетворять следующим требованиям:

- Любой SFP+ пассивный медный кабель, соответствующий требованиям спецификаций SFF-8431 v4.1 и SFF-8472 v10.4.
- Идентификатор по спецификации SFF-8472 должен иметь значение 03h (SFP или SFP Plus). Вы можете проверить это значение у изготовителя кабеля.
- Максимальная длина кабеля — 7 метров.

Примечание. Нельзя использовать кабель прямого подключения для соединения с гигабитным коммутатором, к которому можно подключать SFP-модули. При таком подключении 10-гигабитные сетевые адаптеры поддерживают только скорость, равную 1 Гбит.

Корпорация Intel производит пассивные медные кабели прямого подключения различной длины, которые полностью совместимы с 10-гигабитными сетевыми адаптерами, используемыми в исполнениях ViPNet Coordinator HW2000 и ViPNet Coordinator HW5000. В таблице ниже приведена информация, которая поможет вам приобрести нужный кабель.

Таблица 19. Коды продукции для заказа кабелей прямого подключения

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

3

Возможности управления ViPNet Coordinator HW

Способы управления ViPNet Coordinator HW

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

- Административное программное обеспечение ViPNet — программы ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 87) и ViPNet Policy Manager (см. глоссарий, стр. 87).

  Выполнение настроек в ЦУСе облегчает управление ViPNet Coordinator HW и позволяет оповестить об изменении параметров сетевые узлы ViPNet, связанные с ViPNet Coordinator HW, путем отправки на эти узлы справочников и ключей. Программа Policy Manager позволяет централизованно управлять встроенными сетевыми экранами узлов, в том числе координаторов ViPNet Coordinator HW (см. «Управление с помощью административного ПО ViPNet» на стр. 66).

- Веб-интерфейс.

  Наглядный и интуитивно понятный веб-интерфейс позволяет упростить и сделать более удобными просмотр и выполнение некоторых настроек ViPNet Coordinator HW (см. «Управление с помощью веб-интерфейса» на стр. 67).

- Командный интерпретатор ViPNet Coordinator HW.

  Вы можете использовать командную оболочку ViPNet локально или удаленно через протокол SSH. Командный интерпретатор предоставляет наиболее полные возможности по администрированию ViPNet Coordinator HW (см. «Назначение командного интерпретатора» на стр. 68).

Кроме того, для удаленного просмотра журнала и очереди конвертов MFTP на ViPNet Coordinator HW вы можете использовать апплет SGA (см. «Удаленный мониторинг журнала и очереди конвертов MFTP с помощью апплета SGA» на стр. 70).

Полномочия при различных способах управления

Таблица 20. Основные действия, доступные при различных способах управления ViPNet Coordinator HW

	Режимы подключения		
	Пользователь узла	**Администратор узла**	**Администратор сети**
		Доступ	
Интерфейс для управления ViPNet Coordinator HW	веб-интерфейс (удаленное управление) командный интерпретатор (локальное или удаленное управление)		программа ViPNet Центр управления сетью или ViPNet Policy Manager (удаленное управление)
Способ аутентификации	пароль пользователя	пароль пользователя, пароль администратора узла ViPNet	пароль администратора ViPNet Центр управления сетью или ViPNet Policy Manager
		Установка	
Локальное обновление ПО ViPNet	–	+	–
Удаленное обновление ПО ViPNet	–	–	+
		Обслуживание	
Настройка системных параметров	–	+	–
Настройка параметров сетевых интерфейсов	–	+	+
Настройка подключения к внешнему межсетевому экрану	–	+	+
Настройка IP-адресов координатора и туннелируемых им IP-адресов	–	+	+
Настройка встроенного межсетевого экрана	–	+	+

	Режимы подключения		
	Пользователь узла	**Администратор узла**	**Администратор сети**
Запуск и завершение работы демонов и драйверов	+ (только для командного интерпретатора)	+	–
Настройка системных служб	–	+	–
Просмотр журналов и настроек	–	+	–

Режимы работы в командном интерпретаторе и веб-интерфейсе

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

- Режим пользователя. Данный режим становится активным по умолчанию после аутентификации на ViPNet Coordinator HW (см. «Способы аутентификации пользователя» на стр. 65). При работе с командным интерпретатором или веб-интерфейсом в данном режиме пользователю недоступно изменение настроек ViPNet Coordinator HW. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ `>`.
- Режим администратора. В данном режиме в командном интерпретаторе и веб-интерфейсе доступны все настройки. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ `#`. Чтобы перейти в режим администратора, в командном интерпретаторе или веб-интерфейсе требуется авторизоваться с использованием пароля администратора сетевого узла.

Способы аутентификации пользователя

Прежде чем начать работу с ViPNet Coordinator HW, требуется пройти аутентификацию. Возможно два способа аутентификации:

- «Пароль». При аутентификации требуется ввести имя учетной записи и пароль пользователя. Каждый раз при вводе пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу (см. глоссарий, стр. 89).
- «Устройство». При аутентификации требуется ввести имя учетной записи, подключить устройство, на котором сохранен персональный ключ, и ввести ПИН-код доступа к устройству.

Внимание! В текущей версии ViPNet Coordinator HW для аутентификации могут использоваться только внешние устройства Rutoken lite производства компании «Актив-софт».

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

При локальном подключении к ViPNet Coordinator HW аутентификация производится в командном интерпретаторе (см. «Назначение командного интерпретатора» на стр. 68).

При подключении через веб-интерфейс (см. «Управление с помощью веб-интерфейса» на стр. 67) или удаленном подключении по протоколу SSH (см. «Удаленное подключение с помощью протокола SSH» на стр. 69) аутентификация состоит из двух этапов:

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

Управление с помощью административного ПО ViPNet

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

- ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 87).

  Данная программа, входящая в состав программного комплекса ViPNet Administrator (см. глоссарий, стр. 87), предназначена для формирования структуры сети ViPNet, задания основных параметров сетевых узлов, централизованной отправки справочников, ключей и программного обеспечения на сетевые узлы ViPNet (подробнее см. в документе «ViPNet Центр управления сетью. Руководство администратора»).

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

- ViPNet Policy Manager (см. глоссарий, стр. 87).

  Данная программа предназначена для формирования администратором безопасности корпоративных политик безопасности (см. глоссарий, стр. 90) и их рассылки на узлы по сети ViPNet (подробнее см. в документе «ViPNet Policy Manager. Руководство администратора»). Политики безопасности могут включать в себя сетевые фильтры и правила трансляции IP-адресов. Фильтры и правила трансляции, полученные из программы ViPNet Policy Manager, недоступны для редактирования на узлах.

Управление с помощью веб-интерфейса

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

- Настройка подключения ViPNet Coordinator HW к сети: настройка сетевых интерфейсов, параметров подключения к сетям 3G, 4G, Wi-Fi.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера.
- Настройка защиты соединения по технологии L2OverIP.
- Настройка статической и динамической маршрутизации.
- Работа со списком сетевых узлов ViPNet.
- Мониторинг состояния ViPNet Coordinator HW и просмотр журнала IP-пакетов.

Подключение к веб-интерфейсу ViPNet Coordinator HW следует осуществлять только с выделенных рабочих мест по каналу, защищенному средствами ПО ViPNet. Вы можете подключаться к ViPNet Coordinator HW с других защищенных узлов ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 87)).

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

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

Примечание. Для подключения к веб-интерфейсу ViPNet Coordinator HW используйте следующие веб-браузеры:

- Internet Explorer 10, 11.
- Google Chrome и Mozilla Firefox последней версии.

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

Назначение командного интерпретатора

Командный интерпретатор обеспечивает наиболее полные возможности администрирования ViPNet Coordinator HW по сравнению с веб-интерфейсом. С помощью командного интерпретатора ViPNet вы можете выполнять следующие действия:

- Настройка системных функций ViPNet Coordinator HW: настройка даты и времени, создание копий конфигурации и другое.
- Настройка подключения ViPNet Coordinator HW к сети (настройка сетевых интерфейсов, параметров подключения к сетям 3G, 4G, Wi-Fi.
- Настройка режимов подключения ViPNet Coordinator HW к сети через межсетевой экран.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов.
- Управление обработкой прикладных протоколов.
- Настройка VPN: настройка видимости узлов, туннелирования адресов и другие.
- Настройка защиты соединения по технологии L2OverIP.
- Настройка транспортного модуля: выбор канала передачи конвертов между узлами, настройка протоколирования событий транспортного модуля и другое.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера.
- Настройка статической и динамической маршрутизации.
- Настройка системы защиты от сбоев.
- Резервирование справочников, ключей и настроек ViPNet Coordinator HW, обновление ViPNet Coordinator HW.
- Настройка параметров протоколирования событий, просмотр журналов регистрации IP-пакетов, транспортных конвертов, устранения неполадок.
- Настройка параметров удаленного мониторинга по протоколу SNMP и другое.

Командный интерпретатор запускается автоматически после аутентификации пользователя ViPNet Coordinator HW. При этом он может быть запущен как локально с помощью COM-консоли (см. глоссарий, стр. 86) или обычной консоли (см. глоссарий, стр. 89), так и удаленно при подключении с других узлов сети ViPNet, связанных с ViPNet Coordinator HW, по протоколу SSH (см. «Удаленное подключение с помощью протокола SSH» на стр. 69).

Подробнее об установке, обновлении, удалении ПО на ViPNet Coordinator HW с помощью командного интерпретатора см. в документе «ViPNet Coordinator HW. Подготовка к работе». Подробнее об остальных операциях в командном интерпретаторе см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

Удаленное подключение с помощью протокола SSH

Настройку и управление ViPNet Coordinator HW с помощью командного интерпретатора можно производить не только через локальную консоль, но также с помощью удаленного подключения по протоколу SSH. Удаленное подключение к ViPNet Coordinator HW следует осуществлять только с выделенных рабочих мест по каналу, защищенному средствами ПО ViPNet. Вы можете подключаться к ViPNet Coordinator HW с других защищенных узлов ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 87)).

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

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких узлов.

Примечание. При этом одновременно может быть запущено ограниченное количество удаленных сессий. Ограничения зависят от исполнения ViPNet Coordinator HW:

- 5 удаленных сессий — для всех исполнений ViPNet Coordinator HW50 и HW100.
- 30 удаленных сессий — для остальных исполнений ViPNet Coordinator HW.

Только в одной удаленной сессии можно работать в режиме администратора (независимо от исполнения).

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

Удаленный мониторинг журнала и очереди конвертов MFTP с помощью апплета SGA

Для удаленного просмотра журнала и очереди конвертов MFTP на ViPNet Coordinator HW вы можете использовать апплет SGA.

Совет. Для всех функций мониторинга работы ViPNet Coordinator HW, кроме просмотра журнала и очереди конвертов MFTP, рекомендуется использовать веб-интерфейс ViPNet Coordinator HW (см. «Управление с помощью веб-интерфейса» на стр. 67).

Чтобы подключиться к апплету SGA, на удаленном узле ViPNet выполните следующие действия:

1 В адресной строке веб-браузера введите адрес `http://<IP-адрес координатора>:8080`

Примечание. Апплет SGA недоступен, если ViPNet Coordinator HW выполняет функцию сервера открытого Интернета (см. «Сервер открытого Интернета» на стр. 27).

2 На открывшейся странице введите пароль пользователя ViPNet Coordinator HW и нажмите кнопку **Войти**.

3 В правом нижнем углу страницы щелкните ссылку **SGA**.

Внимание! Для корректной работы апплета SGA с часовыми поясами на вашем компьютере должно быть установлено ПО Java SE Runtime Environment 7 версии 7u79 (32-разрядная версия).

Подробнее о работе с апплетом SGA см. в документе «Апплет мониторинга и управления ViPNet-координатором. Руководство пользователя».

A

История версий

Что нового в версии 4.2.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 4.2.0 по сравнению с версией 4.1.3.

- **Поддержка новых аппаратных платформ ViPNet Coordinator HW**

  Реализована поддержка новых аппаратных платформ ViPNet Coordinator HW (см. «Описание исполнений ViPNet Coordinator HW» на стр. 38):

  - HW50 N1, N2, N3 — на базе мини-компьютера Lanner NCA-1010A. Аппаратная платформа N2 оснащена Wi-Fi-адаптером, а аппаратная платформа N3 — 3G-модемом.
  - HW100 N1, N2, N3 — на базе мини-компьютера Lanner LEC-6032-IT2. Аппаратная платформа N2 оснащена Wi-Fi-адаптером, а аппаратная платформа N3 — 3G-модемом.
  - HW1000 Q4, Q5, Q6 — на базе телеком-серверов AquaServer серии Telecom.
  - HW2000 Q4 — на базе телеком-сервера AquaServer серии Telecom.

- **Новый способ аутентификации пользователя**

  Реализован новый способ аутентификации пользователя «Устройство». При его назначении пользователю в процессе аутентификации требуется подключить внешнее устройство, на котором хранится его персональный ключ. В предыдущих версиях аутентификацию пользователь мог пройти только по паролю.

  Новый способ аутентификации обеспечивает дополнительную безопасность при эксплуатации ViPNet Coordinator HW и должен использоваться тогда, когда этого требует политика безопасности организации, в которой используется ViPNet Coordinator HW.

- **Механизм создания временных задержек при неуспешном вводе пароля**

В новой версии ViPNet Coordinator HW если пользователь или администратор вводит неверный пароль, то перед следующей попыткой ввода пароля ему нужно подождать несколько секунд. Задержка реализована для предотвращения возможности подбора пароля методом перебора. С каждой новой неуспешной попыткой ввода пароля задержка увеличивается. Если был введен неверный пароль 10 раз подряд, задержка составит 25 минут, но после нее можно повторить очередную попытку ввода пароля. При успешном вводе пароля счетчик, который фиксирует неуспешные попытки, обнуляется. Также счетчик обнуляется после десятой неуспешной попытки ввода пароля.

Кроме этого, теперь информация обо всех неуспешных попытках ввода пароля фиксируются в журнале устранения неполадок.

- **Подключение ViPNet Coordinator HW к сети через встроенный 3G-модем или адаптер Wi-Fi**

  Новые аппаратные платформы HW50 и HW100 могут подключаться к сети с помощью встроенного 3G-модема (аппаратные платформы HW50 N3 и HW100 N3) или встроенного Wi-Fi-адаптера (аппаратные платформы HW50 N2 и HW100 N2). Кроме того, теперь можно использовать HW50 N2 или HW100 N2 в качестве точки доступа Wi-Fi.

- **Новые функции маршрутизации IP-трафика**

  В предыдущих версиях ViPNet Coordinator HW функции маршрутизации были реализованы в базовом варианте. ViPNet Coordinator HW мог осуществлять только статическую маршрутизацию IP-трафика с использованием маршрутов, заданных администратором на основе адреса получателя IP-пакета. Таким образом, настройка параметров маршрутизации на ViPNet Coordinator HW, работающего в сетях со сложной разветвленной структурой, могла быть довольно трудоемкой.

  В новой версии ViPNet Coordinator HW функции маршрутизации были доработаны следующим образом:

  - Реализованы функции динамической маршрутизации IP-трафика с использованием протокола OSPF (см. глоссарий, стр. 87). Данный протокол позволяет маршрутизаторам обмениваться друг с другом информацией о доступных им сетях, автоматически строить доступные маршруты в каждую сеть и выбирать из них наилучшие.
  - Расширены функции маршрутизации по протоколу DHCP (см. глоссарий, стр. 86). Теперь ViPNet Coordinator HW может получать от DHCP-сервера не только маршрут по умолчанию, но и другие сформированные маршруты.
  - Добавлена возможность создания статического маршрута с несколькими шлюзами и настройки распределения нагрузки передаваемого IP-трафика между ними.
  - Добавлена возможность настраивать приоритеты маршрутов, формируемых по различным протоколам, с помощью метрик (см. глоссарий, стр. 89) и административных дистанций (см. глоссарий, стр. 88). Теперь это необходимо, так как может быть несколько источников маршрутов.

  Подробную информацию о настройке маршрутизации см. в документах «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса», «ViPNet Coordinator HW. Сценарии работы».

- **Возможность создания агрегированных интерфейсов**

В новой версии ViPNet Coordinator HW появилась возможность объединять несколько физических сетевых интерфейсов ViPNet Coordinator HW в один агрегированный. Эта функция может понадобиться, если пропускной способности отдельных сетевых интерфейсов недостаточно для решения ваших задач. Также вы можете использовать агрегированные интерфейсы для повышения надежности и резервирования каналов связи. При соответствующей настройке агрегированного интерфейса передача данных будет продолжаться, даже если какой-либо входящий в него физический интерфейс выйдет из строя.

Подробную информацию о работе с агрегированными интерфейсами см. в документах «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса».

- **Использование динамических интерфейсов**

  В новой версии ViPNet Coordinator HW динамические интерфейсы (см. глоссарий, стр. 88), которые добавляются при подключении координатора к сети 3G, 4G или Wi-Fi, автоматически становятся активными и начинают пропускать IP-трафик. В предыдущих версиях, чтобы новый динамический интерфейс стал активным и пропускал IP-трафик в соответствии с настроенными сетевыми фильтрами, его требовалось описать в файле `iplir.conf` с помощью секции `[adapter]` и разрешить прохождение IP-пакетов через него с помощью параметра `allowtraffic`.

- **Автоматический и ручной режимы назначения виртуальных адресов туннелируемых узлов**

  В новой версии появилась возможность выбора автоматического или ручного режима назначения виртуальных адресов туннелируемых узлов (параметр `tunnel_virt_assignment` секции `[misc]` файла `iplir.conf`). По умолчанию в новой версии ViPNet Coordinator HW виртуальные адреса для туннелируемых узлов задаются в автоматическом режиме. В случае обновления ViPNet Coordinator HW до текущей версии происходит проверка файла `iplir.conf` на наличие заданных вручную виртуальных адресов для туннелируемых узлов. Если такие адреса заданы в файле `iplir.conf`, устанавливается ручной режим назначения виртуальных адресов туннелируемых узлов и настройки сохраняются.

- **Настройка видимости туннелируемых узлов**

  В предыдущих версиях ViPNet Coordinator HW адреса видимости туннелируемых узлов определялись только вручную, и в результате обновления программного обеспечения на узле, на котором были вручную настроены виртуальные адреса туннелируемых узлов, такие узлы могли стать недоступны.

  Теперь вы можете настроить для ViPNet Coordinator HW видимость всех туннелируемых им узлов по реальным или виртуальным адресам с помощью параметра `tunnelvisibility` секции `[id]` файла `iplir.conf`.

  Подробную информацию о параметрах для настройки туннелирования см. в документе «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору и конфигурационным файлам».

- **Отсутствие принудительного переназначения виртуальных адресов**

  В предыдущей версии ViPNet Coordinator HW можно было принудительно запустить автоматическое переназначение виртуальных адресов всех защищенных узлов с помощью

параметра `startvirtualiphash` в секции `[virtualip]` файла `iplir.conf`. В результате такого переназначения некоторые узлы могли стать недоступны, поэтому больше данный параметр не используется.

- **Проверка связи с координаторами**

  Теперь в случае использования альтернативных каналов доступа для взаимодействия ViPNet Coordinator HW с каким-либо другим координатором вы можете настроить периодическую отправку сообщений на этот координатор с целью оперативного определения его недоступности по текущему адресу доступа и попытки подключения к нему по другому адресу доступа. Период отправки таких сообщений можно указать в параметре `checkconnection_interval` в секции `[id]` этого координатора в файле `iplir.conf`. Подробнее см. в документе «ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам».

- **Возможность настройки TCP-туннеля**

  При удаленном подключении клиента к сети ViPNet может возникать проблема с передачей IP-пакетов по протоколу UDP из-за блокирования этого протокола некоторыми интернет-провайдерами. Теперь, если передача IP-пакетов по протоколу UDP невозможна, клиент может связываться с другими узлами сети ViPNet по протоколу TCP через свой сервер соединений (см. глоссарий, стр. 90). Поэтому в новой версии ViPNet Coordinator HW, который функционирует в качестве сервера соединений для таких клиентов, можно настроить TCP-туннель (см. глоссарий, стр. 87, см. глоссарий, стр. 22), с помощью которого клиенты смогут связываться с другими узлами при блокировании UDP-протокола. Подробную информацию об этом см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

- **Возможность добавления файла с резервным набором персональных ключей (РНПК)**

  В предыдущих версиях РНПК (см. глоссарий, стр. 90) на ViPNet Coordinator HW можно было добавить только с помощью дистрибутива ключей, что было крайне неудобно, потому что в этом случае на координаторе приходилось разворачивать с нуля справочники и ключи. При этом без РНПК на ViPNet Coordinator HW нельзя удаленно обновить справочники и ключи после компрометации (см. глоссарий, стр. 88) или смены мастер-ключей в сети. Поступившие ключи, зашифрованные на новом персональном ключе, без РНПК невозможно расшифровать и использовать.

  В новой версии появилась возможность добавить на ViPNet Coordinator HW файл с РНПК отдельно от дистрибутива ключей, если он отсутствует. Подробнее об этом см. в документе «ViPNet Coordinator HW. Подготовка к работе».

- **Возможность просмотра информации об установленных ключах**

  В новой версии у администратора ViPNet Coordinator HW появилась возможность просмотреть информацию об установленных ключах. По данной информации администратор может узнать, например, присутствует ли на узле РНПК. а также даты обновления ключей и ряд других сведений. Кроме этого, информация будет полезна сотрудникам технического сопровождения «ИнфоТеКС» для устранения неполадок в работоспособности ViPNet Coordinator HW, если такие произошли после обновления ключей на узле.

- **Просмотр журнала регистрации IP-пакетов с помощью веб-интерфейса**

В предыдущих версиях ViPNet Coordinator HW для просмотра журнала регистрации IP-пакетов, а также статистической информации о количестве IP-пакетов, блокированных или пропущенных ViPNet Coordinator HW, использовался командный интерпретатор или апплет SGA. В новой версии ViPNet Coordinator HW эта функция стала доступна и в веб-интерфейсе.

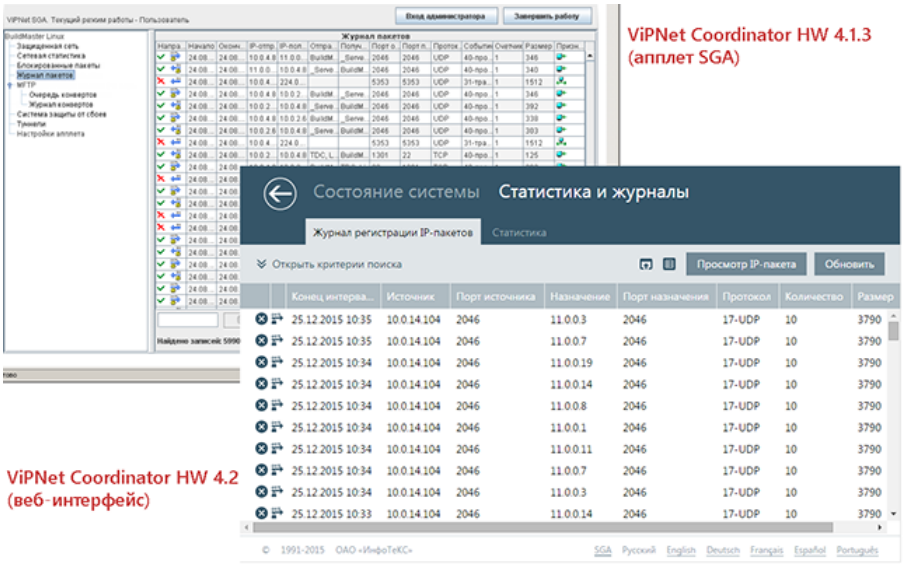

Рисунок 27. Просмотр журнала регистрации IP-пакетов в ViPNet Coordinator HW 4.1.3 и 4.2

- **Поддержка протокола классификации сетевого трафика DiffServ**

  Предыдущие версии ViPNet Coordinator HW для поддержки механизма обеспечения качества обслуживания (QoS) копировали в заголовки зашифрованных IP-пакетов ToS-биты или DSCP-метки (см. глоссарий, стр. 86), содержащиеся в заголовках исходных IP-пакетов. В новой версии ViPNet Coordinator HW помимо маркирования зашифрованных IP-пакетов также выполняется анализ значений DSCP-меток, и пакеты с более высоким приоритетом обрабатываются в первую очередь. Это позволяет предотвратить потерю приоритетного трафика в случае перегрузки ViPNet Coordinator HW.

- **Обновление встроенного SNMP-агента**

  Для взаимодействия с последними версиями программного обеспечения сетевого менеджмента (NMS) в ViPNet Coordinator HW версии 4.2 добавлена поддержка новых параметров баз управляющей информации SNMP.

  В предыдущих версиях SNMP-агент автоматически запускался при загрузке ViPNet Coordinator HW. В новой версии добавлен набор команд, позволяющих запускать SNMP-агент, завершать и изменять параметры его работы.

- **Изменение команд для запуска и остановки демона algd**

  В предыдущих версиях запуск демона algd, обрабатывающего прикладные протоколы, выполнялся с помощью команды `alg start`, а завершение работы демона — с помощью команды `alg stop`. Так как остановка только демона algd может привести к некорректной обработке прикладных протоколов, в новой версии ViPNet Coordinator HW указанные команды удалены. Вместо них добавлена команда для перезагрузки демона — `alg restart`.

- **Изменение терминологии**

Термин «конфигурация ПО ViPNet Coordinator HW» заменен на термин «копия конфигурации VPN». Новый термин более точно описывает данную сущность.

Что нового в версии 4.1.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 4.1.3 по сравнению с версией 4.1.1.

- **Поддержка новой аппаратной платформы HW5000 Q1**

  Реализована поддержка новой аппаратной платформы HW5000 Q1. В данной аппаратной платформе в качестве основы используется сервер AquaServer T51 D15 с укороченным корпусом и двумя процессорами Intel Xeon E5-2620v3.

- **Резервирование критически важных файлов в аппаратных платформах ViPNet Coordinator HW с двумя накопителями**

  Теперь в аппаратных платформах ViPNet Coordinator HW с двумя накопителями выполняется регулярное резервирование образов модулей адаптированной ОС GNU/Linux и ПО ViPNet Coordinator HW, используемых при загрузке ViPNet Coordinator HW, а также конфигурационных файлов. Эти образы и файлы будут автоматически восстановлены во время проверки их целостности при выявлении искажения.

- **Исправление ошибок**

  В версии 4.1.3 исправлены ошибки, выявленные в процессе эксплуатации версии 4.1.1.

Что нового в версии 4.1.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 4.1.1 по сравнению с версией 4.1.0.

- **Дополнительные настройки туннелирования**

  В настройки координаторов, связанных с ViPNet Coordinator HW (секции `[id]`), добавлены новые параметры туннелирования — `exclude_from_tunnels` и `usetunnel`. Теперь в случае необходимости вы можете исключить один или несколько адресов из диапазона туннелирования, а также выключить туннелирование незащищенных компьютеров координатором. Эти настройки задаются только локально.

  Кроме того, раньше соединение с туннелируемыми узлами, находящимися в одной подсети с собственным узлом, всегда осуществлялось через координатор, который туннелирует данные узлы. По этой причине доступ к таким узлам мог быть затруднен. Теперь по умолчанию соединение с туннелируемыми узлами, находящимися в локальной подсети, осуществляется напрямую (минуя координатор). Настройку по умолчанию можно изменить с помощью параметра `tunnel_local_network`, который содержится в секции `[misc]` файла конфигурации `iplir.conf`.

- **Настройка прямой маршрутизации между сетями ViPNet**

Появилась возможность настроить прямую маршрутизацию транспортных конвертов между двумя сетями ViPNet. Для настройки служит новый параметр `transit`, содержащийся в секции `[channel]` файла конфигурации транспортного модуля MFTP. С помощью этого параметра можно указать, на каком координаторе вместо шлюзового будут обрабатываться конверты при их передаче из одной сети в другую. Прямая маршрутизация позволяет снизить нагрузку на шлюзовые координаторы.

- **Исправление ошибок**

  В версии 4.1.1 исправлены ошибки, выявленные в процессе эксплуатации версии 4.1.0.

Что нового в версии 4.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 4.1.0 по сравнению с версией 4.0.0.

- **Новые аппаратные платформы HW100 X3, HW100 X4**

  Реализована поддержка двух новых аппаратных платформ семейства HW100 — HW100 X3 и HW100 X4. Аппаратные платформы основаны на компьютере BK3741S-00C с процессором Intel Atom N2600, аппаратная платформа HW100 X4 дополнительно имеет встроенный аппаратный криптоускоритель. Криптоускоритель позволяет увеличить скорость выполнения криптографических операций. Работа с криптоускорителем осуществляется с помощью специальных команд (подробнее см. в документе «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору и конфигурационным файлам»).

- **Поддержка новой технологии осуществления соединений**

  Реализована поддержка новой технологии осуществления соединений в сети ViPNet. При использовании данной технологии клиенты автоматически устанавливают взаимодействие с другими узлами по кратчайшему возможному маршруту независимо от используемого способа подключения к сети. Если же узлам не удается установить взаимодействие напрямую, то они используют серверы соединений (по умолчанию серверами соединения узлов являются их серверы IP-адресов).

- **Поддержка множественных адресов доступа к узлам**

  Раньше в файле `iplir.conf` для ViPNet Coordinator HW и связанных с ним узлов ViPNet указывался один IP-адрес доступа, а при необходимости использования множественных IP-адресов настраивался доступ к узлу через один из фиксированных альтернативных каналов связи, переключение каналов осуществлялось вручную. Теперь для каждого узла можно задать несколько IP-адресов доступа, а также указать для них приоритет. При этом система будет автоматически определять наиболее предпочтительный из доступных каналов и устанавливать связь через него. Функциональность фиксированных альтернативных каналов связи больше не поддерживается.

- **Увеличена производительность встроенного межсетевого экрана**

  Встроенный межсетевой экран в аппаратных платформах HW1000 и HW2000 теперь может обрабатывать большее количество одновременных соединений. Максимальное значение одновременно обрабатываемых соединений (параметр `max-connections`) зависит от объема

оперативной памяти каждой аппаратной платформы. Подробнее см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Настройка дополнительных параметров межсетевого экрана».

- **Веб-интерфейс для настройки ViPNet Coordinator HW**

  Раньше настройка межсетевого экрана и сервисов DNS, NTP и DHCP осуществлялась только с помощью командной консоли, теперь появилась возможность выполнять данные настройки с помощью удобного веб-интерфейса. Работа с веб-интерфейсом возможна с любого узла сети ViPNet, связанного с координатором.

- **Поддержка расписаний**

  Появилась возможность привязывать действие сетевых фильтров к определенным временным интервалам — применять фильтры по расписанию. Например, вы можете создать сетевой фильтр, который будет блокировать доступ к некоторым веб-ресурсам в рабочее время в будние дни.

- **Работа с группами объектов**

  Теперь вы можете объединять однотипные объекты в именованные группы. Группы объектов облегчают ввод условий при создании сетевых фильтров и правил трансляции, если в них требуется указать целый ряд объектов одного типа. Например, если требуется создать несколько сетевых фильтров, в которых нужно указать IP-адреса сегмента сети, вы можете предварительно создать группу этих IP-адресов и далее добавлять ее в условия фильтров.

- **Встроенный HTTP-прокси-сервер**

  Теперь при работе ViPNet Coordinator HW вы можете настроить встроенный HTTP-прокси-сервер, который будет осуществлять контроль доступа пользователей корпоративной сети к различным интернет-ресурсам.

- **Изменения в функционале L2OverIP**

  Теперь с помощью функции L2OverIP можно объединить на канальном уровне модели OSI до 31 сегмента сети, в том числе сегменты, разделенные на виртуальные локальные сети. При этом настройка функции стала более простой — не требуется задавать отдельный IP-адрес для каждого сегмента и настраивать туннелирование этого адреса. Кроме того, теперь функция L2OverIP может обрабатывать интенсивный многоадресный трафик благодаря использованию многопоточной обработки.

- **Изменения в мастере установки ключей**

  В мастере установки ключей появилась возможность настроить подключение ViPNet Coordinator HW к внешней сети через межсетевой экран и выполнить проверку связи с другим узлом сети ViPNet.

- **Изменение имени пользователя для аутентификации**

  Раньше для аутентификации пользователя использовалось имя `vipnet`. Теперь вместо этого имени используется имя `user`.

Что нового в версии 4.0.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 4.0.0 по сравнению с версией 3.5.0.

- **Поддержка совместной работы с ПО ViPNet Policy Manager версии 4.x**

  Теперь ViPNet Coordinator HW может принимать и обрабатывать политики безопасности, присланные из программы ViPNet Policy Manager версии 4.x.

- **Новый формат сетевых фильтров и правил трансляции IP-адресов**

  В ViPNet Coordinator HW 4.0 используется новый формат сетевых фильтров и правил трансляции IP-адресов, который является единым для ПО ViPNet (как под управлением ОС Windows, так и ОС GNU/Linux), а также позволяет применять политики безопасности, созданные в программе ViPNet Policy Manager 4.x. При обновлении ViPNet Coordinator HW с версии 3.x правила защищенной и открытой сети конвертируются в соответствующие сетевые фильтры и правила трансляции.

  Также был изменен механизм управления сетевыми фильтрами и правилами трансляции. Ранее все настройки правил открытой сети и все параметры фильтрации трафика защищенной сети производились в конфигурационных файлах `firewall.conf` и `iplir.conf` соответственно. Теперь работа с сетевыми фильтрами и правилами трансляции осуществляется с помощью командного интерпретатора.

- **Добавлена возможность использования системных групп объектов в сетевых фильтрах и правилах трансляции IP-адресов**

  Ранее все параметры в условии правила необходимо было задавать вручную. Теперь для сетевых фильтров и правил трансляции адресов появилась возможность использовать встроенные системные группы объектов с фиксированными именами, которые заменяют ряд часто используемых параметров.

- **Отказ от режимов безопасности**

  В версии 4.0 режимы безопасности не используются. Необходимый уровень безопасности можно настроить, создав соответствующие сетевые фильтры.

- **Антиспуфинг**

  Для обеспечения высокого уровня безопасности сети в ViPNet Coordinator HW используется функция антиспуфинга. В версии 3.2.x настройка антиспуфинга выполнялась администратором вручную. В версии 4.0 настройка антиспуфинга выполняется автоматически. При этом соответствующие фильтры формируются автоматически на основе таблицы маршрутизации данного сетевого узла.

- **Обработка прикладных протоколов**

  В новой версии ViPNet Coordinator HW реализована функция обработки следующих прикладных протоколов: FTP, DNS, H.323, SCCP, SIP. Данная функция позволяет использовать указанные прикладные протоколы на защищенных узлах, которым назначены виртуальные IP-адреса или для которых выполняется трансляция адресов.

- **Отказ от некоторых аппаратных платформ ViPNet Coordinator HW**

В новой версии ПАК больше не поддерживаются следующие аппаратные платформы: HW100 E1, HW100 E2, HW100 K1, HW1000 Q1, HW-MCM и все аппаратные платформы HW10.

- **Поддержка исполнения HW VA**

  Реализована поддержка исполнения ViPNet Coordinator HW VA, не зависящего от аппаратной платформы. Данное исполнение представляет собой виртуализированное решение, предназначенное для разворачивания на виртуальной машине.

- **Мониторинг неактивных удаленных сессий**

  Раньше при работе с ПАК количество удаленных сессий по протоколу SSH было неограниченно, что могло привести к сбоям в работе ПАК при одновременном подключении большого количества пользователей. Для предотвращения возникновения таких ситуаций было введено ограничение на количество одновременных удаленных сессий пользователей, а также был реализован механизм мониторинга неактивных сессий. Теперь максимальное количество удаленных сессий в зависимости от используемой аппаратной платформы равно 5 (для аппаратных платформ HW100 X1, X2) или 30 (для остальных аппаратных платформ). Если какая-либо сессия пользователя была неактивна в течение заданного времени (по умолчанию — 30 минут), то сессия будет принудительно завершена.

Что нового в версии 3.5.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 3.5.0 по сравнению с версией 3.3.0.

- **Поддержка новых аппаратных платформ HW100 X3/X8/Y1 и HW1000 Q4**

  Реализована поддержка новых аппаратных платформ HW100 X3/X8/Y1 и HW1000 Q4.

  В аппаратных платформах HW100 X3/X8 в качестве основы используется компьютер BK3741S-00C с процессором Intel Atom N2600.

  В аппаратной платформе HW100 Y1 (ПАК Symanitron ViPNet 100) в качестве основы используется компьютер Symanitron Brain-F810.

  В аппаратной платформе HW1000 Q4 в качестве основы используется сервер AquaServer T41 S24 с процессором Intel Celeron G1820.

- **Исправление ошибок**

  В версии 3.5.0 исправлены ошибки, выявленные в процессе эксплуатации версии 3.3.0.

Что нового в версии 3.3.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 3.3.0 по сравнению с версией 3.2.0.

- **Поддержка новой аппаратной платформы HW1000 S1**

Реализована поддержка новой аппаратной платформы HW1000 S1. В данной аппаратной платформе в качестве основы используется сервер ASUS RS300-E7/PS4 с процессором Intel Xeon.

- **Отказ от некоторых аппаратных платформ ViPNet Coordinator HW**

  В новой версии больше не поддерживаются следующие аппаратные платформы: HW100 K1, HW-MCM и все аппаратные платформы HW10.

- **Изменение списка временных зон для России**

  Изменился список временных зон для России в связи с переходом на зимнее время с 26 октября 2014 года. Теперь в России 11 временных зон, а московское время соответствует третьему часовому поясу в национальной шкале времени UTC+3.

- **Исправление ошибок в программном обеспечении**

  Исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 3.2.0.

Что нового в версии 3.2.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 3.2.0 по сравнению с версией 3.1.0.

- **Поддержка новой аппаратной платформы HW2000 Q3**

  Реализована поддержка новой аппаратной платформы ViPNet Coordinator HW2000 Q3.

  В аппаратной платформе HW2000 Q3 в качестве основы используется сервер AquaServer T50 D14 с процессорами E5-2620 v2 (см. «Аппаратная платформа HW2000 Q3» на стр. 52) и высокоскоростными сетевыми интерфейсами.

  Все аппаратные платформы HW2000 можно использовать для организации кластера горячего резервирования.

- **Изменение команд для настройки DNS-сервера, установленного на ViPNet Coordinator HW**

  Добавлены команды для задания IP-адресов сетевых узлов и подсетей, узлам которых разрешены DNS-запросы к локальному DNS-серверу: `inet dns clients list`, `inet dns clients add`, `inet dns clients delete`.

  Были переименованы следующие команды:

  Таблица 21. Команды, переименованные в версии 3.2

Команда в прошлых версиях ViPNet Coordinator HW	Команда в версии 3.2.0
`inet dns list`	`inet dns forwarders list`
`inet dns add`	`inet dns forwarders add`
`inet dns delete`	`inet dns forwarders delete`

- **Изменение состава файлов экспорта**

Для оптимизации работы с файлами экспорта из их состава исключены следующие данные:

- журнал регистрации IP-пакетов;
- журнал транспортных конвертов MFTP;
- очередь транспортных конвертов.

Что нового в версии 3.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 3.1.0 по сравнению с версией 3.0.0.

- **Синхронизация системной таблицы маршрутизации при работе в режиме кластера горячего резервирования**

  Реализована передача системной таблицы маршрутизации с активного сервера, входящего в состав кластера горячего резервирования, на пассивный сервер. Теперь файл, содержащий таблицу маршрутизации, передается вместе с другими файлами конфигурации. Если полученная таблица маршрутизации отличается от текущей таблицы пассивного сервера, то происходит немедленная загрузка и применение новых маршрутов. Это избавляет от необходимости изменять маршруты вручную.

- **Возможность объединения удаленных сегментов сети с помощью технологии L2OverIP**

  Реализована функция L2OverIP, которая позволяет объединить на канальном уровне два удаленных сегмента сети, использующих одно и то же адресное пространство. В результате объединения узлы из разных сегментов будут взаимодействовать друг с другом так, как будто они находятся в одной локальной сети. Включение и настройка функции производится с помощью командного интерпретатора.

- **Расширение условий, задаваемых в правилах трансляции IP-адресов**

  Расширен список допустимых выражений для задания в условии правил трансляции IP-адресов. Теперь в лексеме `to` для правил трансляции адреса отправителя и в лексеме `from` для правил трансляции адреса получателя можно указать не только значение `anyip`, но также адрес, диапазон и список адресов, маску адресов, порт и диапазон портов.

- **Возможность указания любого протокола в правилах трансляции IP-адресов**

  Сняты ограничения на протокол, задаваемый в правилах трансляции IP-адресов. Теперь в лексеме `proto` можно указать любой протокол, в том числе протокол GRE. Поддержка протокола GRE в правилах трансляции позволяет обеспечить доступ удаленных клиентов к серверу по технологии PPTP VPN, которая использует протокол GRE для передачи пакетов.

- **Изменение состава отображаемой информации о продукте**

  Изменен состав информации о ViPNet Coordinator HW, которая отображается локально по команде `version` и удаленно на узлах, связанных с ПАК. Теперь основная информация содержит версию продукта, наименование аппаратной платформы и версию ПО ViPNet в составе ПАК. Для получения полной информации о продукте, включая версии его компонентов, в команду `version` добавлен параметр `full`.

Что нового в версии 3.0.0

В этом разделе представлен краткий обзор изменений и новых возможностей ПАК ViPNet Coordinator HW версии 3.0.0.

- **Прекращение поддержки аппаратной платформы HW-VPNM**

  Аппаратная платформа HW-VPNM более не поддерживается в составе ПАК ViPNet Coordinator HW.

- **Включение в состав аппаратных платформ ПАК ViPNet Coordinator HW продукта ПАК «NME-RVPN ViPNet»**

  В состав аппаратных платформ ПАК ViPNet Coordinator HW включен ПАК «NME-RVPN ViPNet», который ранее выпускался как отдельный продукт. Теперь ПАК «NME-RVPN ViPNet» поддерживается как аппаратная платформа HW-MCM C2.

- **Изменение наименований аппаратных платформ ПАК ViPNet Coordinator HW**

  Произведена замена наименований аппаратных платформ ПАК ViPNet Coordinator HW. В таблице ниже приведено соответствие новых наименований старым.

Новое наименование	Старое наименование
HW100 E1	HW100 G1 базовой конфигурации (без жесткого диска)
HW100 E2	HW100 G1 расширенной конфигурации (с жестким диском)
HW100 X1	HW100 G2 базовой конфигурации (без жесткого диска)
HW100 X2	HW100 G2 расширенной конфигурации (с жестким диском)
HW1000 Q1	HW1000 G1
HW1000 Q2	HW1000 G2
HW-MCM C2	NME-RVPN ViPNet

- **Пополнение списка поддерживаемых аппаратных платформ новыми аппаратными платформами — HW10 A1, A2, A3, A4, HW100 K1, HW1000 Q3 и HW2000 Q2**

  Реализована поддержка новых аппаратных платформ — HW10 A1, A2, A3, A4, ПАК ViPNet Coordinator HW100 K1, HW1000 Q3 и HW2000 Q2.

  В аппаратных платформах HW10 A1, A2, A3, A4 в качестве основы используется Plug-компьютер IP-Plug.

  В аппаратной платформе HW100 K1 в качестве основы используется компьютер Kraftway Credo VV20.

  В аппаратной платформе HW1000 Q3 в качестве основы используется сервер AquaServer T40 S44 с процессором Intel Core i5-750.

В аппаратной платформе HW2000 Q2 в качестве основы используется сервер AquaServer T50 D57 с процессорами Intel Xeon последнего поколения и высокоскоростными сетевыми интерфейсами (см. «Исполнение ViPNet Coordinator HW2000» на стр. 50).

Все аппаратные платформы HW1000 и HW2000 можно использовать для организации кластера горячего резервирования.

- **Возможность использования ПАК ViPNet Coordinator HW для организации кластера без дополнительной регистрации**

  Отменена регистрация ПАК ViPNet Coordinator HW в прикладной задаче «ViPNet Failover». Теперь аппаратные платформы, поддерживающие режим кластера горячего резервирования, можно использовать по своему усмотрению — в качестве отдельных сетевых узлов или в составе кластера.

- **Переход на более производительный драйвер сетевой защиты**

  Драйвер сетевой защиты, входящий в состав ПО ПАК ViPNet Coordinator HW, заменен на новый производительный драйвер, который эффективно использует многоядерную архитектуру современных процессоров. Это позволяет шифровать потоки трафика со скоростью до 3 Гбит/с (аппаратная платформа HW2000 Q2).

- **Отказ от использования 5-го режима безопасности**

  Режим безопасности 5, который можно было установить на отдельных сетевых интерфейсах для выключения сетевой защиты, более не поддерживается. Теперь сетевую защиту можно включить или выключить только одновременно на всех интерфейсах ПАК с помощью команд группы vipnet.

- **Поддержка функции агента DHCP-relay**

  В состав ПАК ViPNet Coordinator HW включена служба DHCP-relay, которая позволяет использовать ПАК в качестве агента DHCP-relay. Настройка и управление службой производится с помощью командного интерпретатора.

- **Поддержка технологии VLAN**

  Реализована поддержка технологии виртуальных локальных сетей (VLAN) в соответствии со стандартом IEEE 802.1 Q. Теперь можно использовать ПАК в разветвленной сети, состоящей из нескольких виртуальных (логических) сетей, с помощью создания нескольких виртуальных интерфейсов на базе одного физического интерфейса. Как следствие, произошло разделение интерфейсов ПАК на два класса — класс интерфейсов, используемых обычным образом, и класс интерфейсов, используемых для работы с VLAN. В командный интерпретатор добавлены команды, необходимые для изменения класса интерфейса и для настройки и управления виртуальными интерфейсами.

- **Возможность экспорта журнала регистрации IP-пакетов на USB-носитель**

  Реализован экспорт журнала регистрации IP-пакетов на USB-носитель. Теперь при просмотре журнала можно сохранить выбранные записи в файле и затем перенести файл на USB-носитель с помощью команды `admin export packetdb usb`.

- **Поддержка SSH-клиента**

Реализована поддержка SSH-клиента для возможности подключения к удаленному компьютеру. Запуск SSH-клиента осуществляется с помощью команды `inet ssh`.

- **Возможность задания имени компьютера**

  Реализована возможность задания произвольного имени компьютера вместо установленного по умолчанию. Имя задается с помощью команды `machine set hostname`.

- **Возможность просмотра статистики работы межсетевого экрана**

  Реализована команда `iplir show firewall status`, с помощью которой можно просмотреть текущие параметры работы межсетевого экрана.

- **Поддержка режима шифрования CTR (Counter mode)**

  Реализован режим шифрования CTR (в дополнение к используемому режиму CFB — Cipher Feedback mode), который позволяет получить выигрыш в скорости до 20%. Теперь можно установить нужный режим с помощью команды `iplir set cipher-mode`.

- **Возможность гибкой настройки видимости сетевых узлов**

  Изменен принцип настройки видимости сетевых узлов. Раньше видимость узлов (по реальному или виртуальному IP-адресу) определялась автоматически, и только для отдельных узлов можно было задать принудительную видимость по реальному IP-адресу. Теперь реализована возможность групповой настройки видимости, которая позволяет задать видимость сразу для всех узлов некоторых сетей ViPNet, а также установить видимость, используемую по умолчанию. Новые настройки видимости задаются в секции `[visibility]` файла `iplir.conf`.

- **Изменение правил фильтрации открытых IP-пакетов, установленных по умолчанию**

  Из настроек межсетевого экрана исключены правила по умолчанию, разрешающие входящий трафик по портам 53 и 123 для открытых узлов, которые необходимы для использования ПАК в качестве DNS- и NTP-серверов. Это сделано с целью повышения безопасности ПАК и его защиты от атак. Теперь для использования ПАК в качестве DNS- и NTP-серверов для открытых узлов требуется вручную добавить необходимые правила для узлов доверенных сетей. Также из настроек исключены закомментированные правила по умолчанию.

- **Изменение терминологии**

  Термин «справочно-ключевая информация» заменен на термин «справочники и ключи». Изменение связано с модернизацией терминологии, используемой в технологии ViPNet.

B

Глоссарий

COM-консоль

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

DHCP (Dynamic Host Configuration Protocol)

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

DiffServ (Differentiated Service)

Протокол, обеспечивающий классификацию сетевого трафика при помощи DSCP-меток (см. глоссарий, стр. 86), добавляемых в заголовки IP-пакетов.

DSCP-метка

Информация о приоритете обработки IP-пакета, указанная в заголовке IP-пакета.

L2OverIP

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

MIME-тип

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

OSPF (Open Shortest Path First)

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

PPP (Point-to-Point Protocol)

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

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг Интернета.

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

ViPNet Administrator

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

ViPNet Policy Manager

Программа, которая входит в состав программного комплекса ViPNet. Предназначена для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Центр управления сетью (ЦУС)

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

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

Административная дистанция

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

Администратор сети ViPNet

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

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

Динамический сетевой интерфейс

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

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

Существуют следующие группы динамических интерфейсов:

- `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
- `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

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.

Компрометация ключей

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

Координатор (ViPNet-координатор)

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

сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Межсетевой экран

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

Метрика маршрута

Предназначена для задания приоритета маршрута передачи IP-трафика.

Обычная консоль

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

Открытый Интернет

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

Открытый узел

Узел, с которым обмен информацией происходит в незашифрованном виде.

Персональный ключ пользователя

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

ПК ViPNet StateWatcher

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

Политика безопасности

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

Резервный набор персональных ключей (РНПК)

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

Роль

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

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

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

Сервер IP-адресов

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

Сервер соединений

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

Сетевой узел ViPNet

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

Сеть ViPNet

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

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

Статический сетевой интерфейс

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

Трансляция сетевых адресов (NAT)

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

Транспортный конверт

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

Транспортный модуль (MFTP)

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

Транспортный сервер

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

Туннелирование

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

Узел сети ViPNet

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

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие.

Шлюзовые координаторы назначаются в ЦУСе каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

Указатель