ViPNet Coordinator HW 4

Настройка с помощью веб-интерфейса

infotecs

ФРКЕ.00130-03 90 05

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 ... **6**
О документе ... 7
Соглашения документа ... 8
Связанные документы ... 9
О программно-аппаратном комплексе ViPNet Coordinator HW ... 10
Обратная связь ... 11

Глава 1. Начало работы с веб-интерфейсом ViPNet Coordinator HW ... **12**
Назначение веб-интерфейса ... 13
Режимы пользователя и администратора ... 14
Ограничения при работе в режимах пользователя и администратора ... 15
Режим ограниченной функциональности ... 16
Подключение к веб-интерфейсу ... 17
Настройка даты и времени ... 20
Перезагрузка ViPNet Coordinator HW ... 22

Глава 2. Настройка подключения к сети ... **23**
Настройка сетевых интерфейсов Ethernet ... 24
Назначение дополнительных IP-адресов ... 27
Организация обработки трафика из нескольких VLAN ... 28
Подключение к беспроводной сети Wi-Fi ... 31
Подключение к мобильной сети 3G, 4G ... 34
Использование агрегированных сетевых интерфейсов ... 36
Создание агрегированного интерфейса ... 36
Режимы работы агрегированного интерфейса ... 39

Глава 3. Просмотр и изменение параметров VPN ... **42**
Просмотр информации о сетевых узлах ViPNet ... 43
Проверка соединения с сетевым узлом ViPNet ... 45
Просмотр и изменение списка туннелируемых узлов ... 46
Настройка защиты соединения по технологии L2OverIP ... 48
Общее описание технологии L2OverIP ... 48
Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI ... 51

Глава 4. Настройка сетевых фильтров ... **54**

Основные принципы фильтрации трафика 55
Общие сведения о сетевых фильтрах 59
Группы объектов 61
Системные группы объектов 62
Пользовательские группы объектов по умолчанию 63
Просмотр групп объектов 64
Создание и изменение группы объектов 65
Группа сетевых узлов ViPNet 66
Группа IP-адресов 68
Группа сетевых интерфейсов 69
Группа протоколов 71
Группа расписаний 72
Просмотр сетевых фильтров 75
Создание и изменение сетевого фильтра 76
Пример использования групп объектов и сетевых фильтров 79

Глава 5. Настройка правил трансляции адресов 82
Трансляция адресов в технологии ViPNet 83
Трансляция адреса назначения 84
Трансляция адреса источника 85
Просмотр правил трансляции адресов 87
Создание и изменение правила трансляции адресов 88

Глава 6. Настройка сетевых служб 90
Настройка параметров DHCP-сервера 91
Настройка DHCP-relay 94
Настройка параметров DNS-сервера 96
Настройка параметров NTP-сервера 98
Настройка параметров прокси-сервера 101
Настройка основных параметров прокси-сервера 103
Настройка фильтрации содержимого трафика 105
Настройка антивируса 107
Настройка параметров точки доступа к сети Wi-Fi 109

Глава 7. Настройка маршрутизации 112
Общие сведения о маршрутизации 113
Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW 114
Просмотр общей таблицы маршрутизации 117
Общие сведения для работы по протоколу OSPF 119

Настройка статической маршрутизации ... 121
Добавление статических маршрутов ... 121
Настройка балансировки IP-трафика ... 123
Настройка динамической маршрутизации ... 125
Настройка параметров динамических маршрутов от DHCP/PPP-протокола ... 125
Настройка административной дистанции для маршрутов DHCP-сервера ... 126
Настройка метрики для маршрутов DHCP-сервера ... 127
Настройка метрики для маршрутов PPP-протокола ... 128
Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола ... 129
Настройка параметров динамической маршрутизации по протоколу OSPF ... 130
Настройка протокола OSPF ... 131
Настройка перераспределения маршрутов ... 133

Глава 8. Мониторинг состояния ViPNet Coordinator HW и просмотр журнала IP-пакетов ... 135
Мониторинг состояния ViPNet Coordinator HW ... 136
Просмотр журнала регистрации IP-пакетов ... 138
Просмотр статистической информации об IP-пакетах ... 141
Просмотр системного журнала ... 142

Приложение A. Сетевые фильтры по умолчанию ... 143

Приложение B. Пользовательские группы протоколов по умолчанию ... 147

Приложение C. Типы событий в журнале регистрации IP-пакетов ... 150

Приложение D. Глоссарий ... 155

Приложение E. Указатель ... 161

Введение

О документе 7

Соглашения документа 8

Связанные документы 9

О программно-аппаратном комплексе ViPNet Coordinator HW 10

Обратная связь 11

О документе

В документе описана настройка ViPNet Coordinator HW с помощью веб-интерфейса. Документ предназначен для администраторов и пользователей, которые планируют работать с ViPNet Coordinator HW, используя веб-интерфейс.

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.

Связанные документы

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

Таблица 3. Связанные документы

Документ	Содержание
«ViPNet Coordinator HW. Общее описание»	Описание общей информации по ViPNet Coordinator HW, а также существующих исполнений и характеристик аппаратных платформ
«ViPNet Coordinator HW. Подготовка к работе»	Описание подготовки ViPNet Coordinator HW к использованию, развертывания виртуального образа ViPNet Coordinator HW, работы со справочниками и ключами узла, обновления ПО, резервного копирования и восстановления настроек
«ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»	Описание основных сценариев настройки ViPNet Coordinator HW с помощью командного интерпретатора, работы с журналами и мониторинга ViPNet Coordinator HW
«ViPNet Coordinator HW. Сценарии работы»	Описание практических сценариев использования ViPNet Coordinator HW, которые требуют комплексного применения различных команд и базовых схем настройки ViPNet Coordinator HW
«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
«ViPNet Coordinator HW. Лицензионные соглашения на компоненты сторонних производителей»	Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet Coordinator HW

О программно-аппаратном комплексе ViPNet Coordinator HW

Программно-аппаратный комплекс ViPNet Coordinator HW представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС GNU/Linux.

ViPNet Coordinator HW выступает в роли VPN-сервера и предназначен для использования в IP-сетях, защита которых организуется с применением комплекса программных продуктов ViPNet.

ViPNet Coordinator HW в сети ViPNet реализует функции координатора, а также ряд дополнительных функций.

Описание всех функций ViPNet Coordinator HW см. в документе «ViPNet Coordinator HW. Общее описание».

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

Начало работы с веб-интерфейсом ViPNet Coordinator HW

Назначение веб-интерфейса 13

Режимы пользователя и администратора 14

Режим ограниченной функциональности 16

Подключение к веб-интерфейсу 17

Настройка даты и времени 20

Перезагрузка ViPNet Coordinator HW 22

Назначение веб-интерфейса

Для просмотра и выполнения некоторых настроек ViPNet Coordinator HW вы можете использовать веб-интерфейс. Подключение к ViPNet Coordinator HW через веб-интерфейс 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. 156)).

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.

Режимы пользователя и администратора

Вы можете работать с веб-интерфейсом ViPNet Coordinator HW в режиме пользователя или в режиме администратора. Действия, которые вы можете выполнять, в этих режимах см. в таблице ниже.

Таблица 4. Работа в веб-интерфейсе в режимах пользователя и администратора

Действие	Режим пользователя	Режим администратора
Настройка подключения к сети (на стр. 23): • настройка сетевых интерфейсов Ethernet; • назначение дополнительных IP-адресов; • организация обработки трафика из нескольких VLAN; • подключение к сетям Wi-Fi и 3G; • использование агрегированных сетевых интерфейсов.	–	+
Просмотр сетевых фильтров (на стр. 75)	+	+
Создание и изменение сетевого фильтра (на стр. 76)	–	+
Просмотр правил трансляции адресов (на стр. 87)	+	+
Создание и изменение правила трансляции адресов (на стр. 88)	–	+
Просмотр групп объектов (на стр. 64)	+	+
Создание и изменение группы объектов (на стр. 65)	–	+
Изменение настроек сетевых служб (см. «Настройка сетевых служб» на стр. 90): • настройка DHCP, DNS, NTP и прокси-сервера; • настройка точки доступа к сети Wi-Fi; • настройка функциональности L2OverIP.	–	+
Просмотр общей таблицы маршрутизации (на стр. 117)	+	+
Изменение настроек маршрутизации (см. «Настройка маршрутизации» на стр. 112)	–	+
Просмотр информации о сетевых узлах ViPNet (на стр. 43)	+	+
Проверка соединения с сетевым узлом ViPNet (на стр. 45)	+	+

Действие	Режим пользователя	Режим администратора
Просмотр информации о туннелируемых узлах (см. «Просмотр и изменение списка туннелируемых узлов» на стр. 46)	+	+
Мониторинг состояния ViPNet Coordinator HW (на стр. 136)	+	+
• Получение журнала устранения неполадок	-	+
Просмотр журнала регистрации IP-пакетов (на стр. 138)	+	+
Просмотр статистической информации об IP-пакетах (на стр. 141)	+	+

Ограничения при работе в режимах пользователя и администратора

Одновременно с веб-интерфейсом могут работать не более 5 пользователей, причем только один из них — в режиме администратора. Переход в режим администратора можно выполнить только после аутентификации в режиме пользователя. При этом в момент перехода пользователя в режим администратора сеанс другого администратора как в веб-интерфейсе, так и в командном интерпретаторе (подробнее см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интепретатора») будет прерван (см. «Подключение к веб-интерфейсу» на стр. 17).

Режим ограниченной функциональности

При выключении одного или нескольких демонов (основных процессов) ViPNet Coordinator HW (iplircfg, failoverd) веб-интерфейс автоматически переходит в режим ограниченной функциональности. При этом появляется соответствующее сообщение с предложением выйти из веб-интерфейса либо продолжить работу с ограничением некоторых функций.

Примечание. Работа демонов может быть завершена как автоматически (в случае неполадок или на время выполнения некоторых операций), так и вручную администратором ViPNet Coordinator HW с помощью соответствующих команд.

В режиме ограниченной функциональности в зависимости от выключенного процесса ViPNet Coordinator HW могут быть недоступны следующие разделы веб-интерфейса:

- В случае завершения работы демона iplircfg целиком блокируются разделы **ViPNet VPN** и **Межсетевой экран**. При этом вы не сможете настраивать сетевые фильтры и правила трансляции адресов, работать со списком сетевых узлов ViPNet.
- В случае завершения работы демона failoverd в разделе **Мониторинг** не отображается информация о работе системы, выводится только информация об использовании памяти.

Также веб-интерфейс переходит в режим ограниченной функциональности при работе ViPNet Coordinator HW в режиме кластера горячего резервирования и при обновлении справочников и ключей, поступивших из программы ViPNet Центр управления сетью. В этом случае разделы **Системные настройки**, **Сетевые настройки** и **Прикладные сервисы** доступны только для просмотра, а раздел **Прикладные сервисы** > **DHCP** отсутствует.

В режиме ограниченной функциональности вы можете просмотреть информацию об остановленных процессах, недоступных настройках или ограниченных функциях, щелкнув значок в верхнем правом углу страницы.

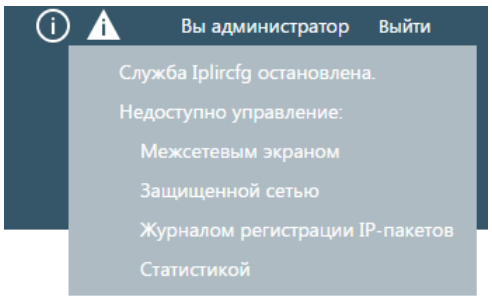


Рисунок 1. Просмотр информации об ограничениях функциональности

Подключение к веб-интерфейсу

Внимание! При подключении к веб-интерфейсу необходимо учитывать следующие особенности:

- В ViPNet Coordinator HW по умолчанию включен сетевой фильтр Allow ViPNet WebGUI, разрешающий передачу трафика по протоколу TCP через порт 8080 со всех узлов сети. Не удаляйте и не отключайте этот фильтр, иначе в противном случае вы не сможете подключиться.
- Подключение к веб-интерфейсу ViPNet Coordinator HW необходимо выполнять в отдельном браузере (но не в отдельных окне или вкладке браузера, который уже используется для просмотра других веб-ресурсов). В противном случае ViPNet Coordinator HW может быть уязвим для атаки типа «отказ в обслуживании».

Чтобы подключиться к веб-интерфейсу, выполните следующие действия:

1 В адресной строке веб-браузера введите `http://<IP-адрес>:8080`, указав текущий IP-адрес для доступа к узлу ViPNet Coordinator HW.

Текущий IP-адрес доступа к узлу ViPNet Coordinator HW вы можете посмотреть в ПО ViPNet, установленном на вашем узле.

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

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

2 В открывшемся окне аутентификации введите пароль пользователя сетевого узла ViPNet и нажмите кнопку **Войти**.

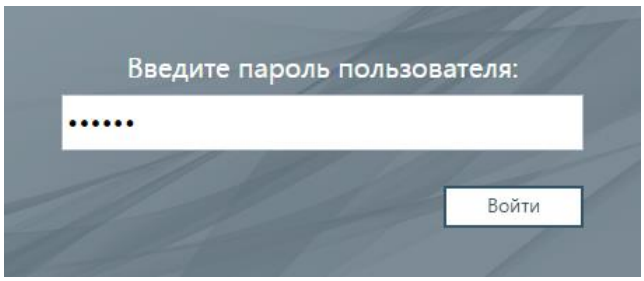


Рисунок 2. Аутентификация пользователя

Примечание. Если вы ввели неверный пароль, чтобы сделать очередную попытку ввода пароля подождите несколько секунд. Задержка реализована для предотвращения возможности подбора пароля методом перебора. С каждой новой неуспешной попыткой ввода пароля задержка увеличивается. Если вы ввели неверный пароль 10 раз подряд,

задержка составит 25 минут, но после нее вы также сможете повторить попытку ввода пароля. При успешной попытке ввода пароля счетчик, который фиксирует неуспешные попытки, обнуляется. Также счетчик обнуляется после десятой неуспешной попытки ввода пароля.

События обо всех неуспешных попытках ввода пароля фиксируются в журнале устранения неполадок.

После успешной аутентификации откроется начальная страница веб-интерфейса ViPNet Coordinator HW в режиме пользователя. В данном режиме вы можете только просматривать настройки ViPNet Coordinator HW. Чтобы изменять настройки, войдите в режим администратора (см. «Режимы пользователя и администратора» на стр. 14).

Рисунок 3. Начальная страница веб-интерфейса ViPNet Coordinator HW

Для входа в режим администратора выполните следующие действия:

1. В правом верхнем углу страницы щелкните ссылку **Войти как администратор**.
2. Введите пароль администратора данного сетевого узла или администратора группы сетевых узлов ViPNet.

Примечание. Если вы ввели неверный пароль, чтобы сделать очередную попытку ввода пароля подождите несколько секунд. Задержка реализована для предотвращения возможности подбора пароля методом перебора. С каждой новой неуспешной попыткой ввода пароля задержка увеличивается. Если вы ввели неверный пароль 10 раз подряд, задержка составит 25 минут, но после нее вы также сможете повторить попытку ввода пароля. При успешной попытке ввода пароля счетчик, который фиксирует неуспешные попытки, обнуляется. Также счетчик обнуляется после десятой неуспешной попытки ввода пароля.

События обо всех неуспешных попытках ввода пароля фиксируются в журнале устранения неполадок.

3 Чтобы прервать сеанс другого администратора, который возможно сейчас работает с узлом ViPNet Coordinator HW с помощью веб-интерфейса или командной строки с другого сетевого узла ViPNet, установите соответствующий флажок. Если вы не установите данный флажок, то сеанс другого администратора не будет прерван, а ваша попытка входа в режим администратора будет отклонена.

4 Нажмите кнопку **Войти**.

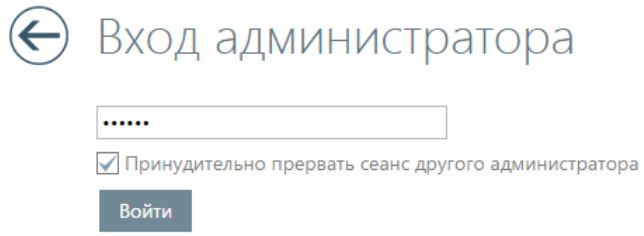


Рисунок 4. Вход в режим администратора

В результате вы будете работать в режиме администратора, сможете просматривать и изменять настройки ViPNet Coordinator HW с помощью веб-интерфейса.

Примечание. Если на ViPNet Coordinator HW истекают или уже истекли персональный ключ пользователя (см. глоссарий, стр. 159) или ключи защиты ключей обмена (см. глоссарий, стр. 158), то в веб-интерфейсе появится соответствующее сообщение. В этом случае требуется обновить ключи. О том, как обновить ключи, см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

Настройка даты и времени

Чтобы компьютер с программным обеспечением ViPNet Coordinator HW корректно взаимодействовал с другими защищенными узлами ViPNet, необходимо правильно настроить системные дату и время.

Внимание! Если системные дата и время заданы неверно, защищенные соединения с другими узлами ViPNet могут быть заблокированы.

Чтобы настроить системные дату и время, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Системные настройки** > **Дата и время**.

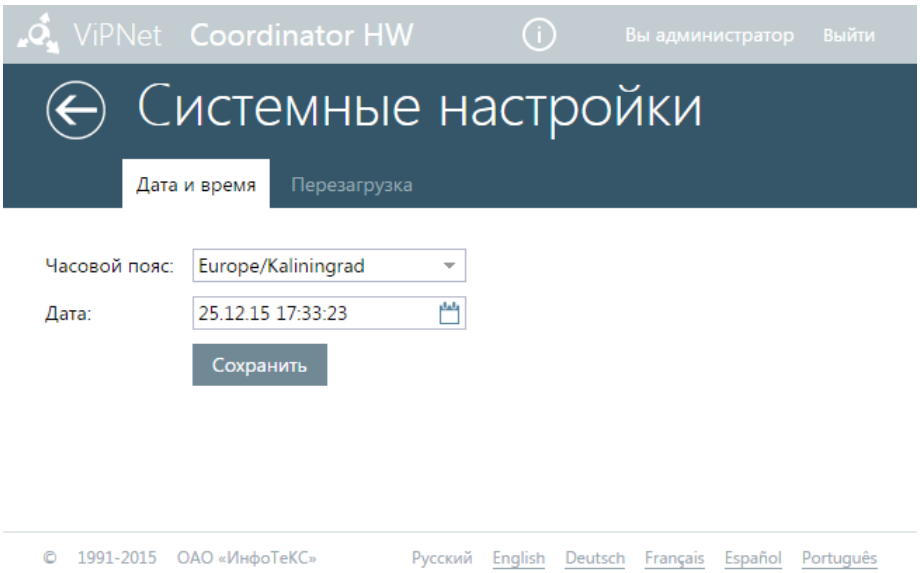


Рисунок 5. Настройка даты и времени

3 Если требуется изменить часовой пояс, в списке **Часовой пояс** выберите регион, где расположен сетевой узел с установленным программным обеспечением ViPNet Coordinator HW.

4 В поле **Дата** щелкните значок . Появится форма задания даты и времени.

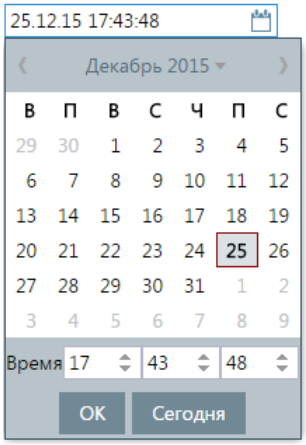


Рисунок 6. Задание даты и времени в соответствующей форме

5 В появившейся форме выполните следующие действия:

5.1 В календаре выберите необходимую дату.

5.2 Под календарем, в области **Время**, задайте необходимое время.

Примечание. Если вы хотите указать значения даты и времени, используемые в данный момент на компьютере, с помощью которого производится подключение к веб-интерфейсу, нажмите кнопку **Сегодня**.

5.3 Нажмите кнопку **OK**.

6 На странице **Дата и время** нажмите кнопку **Сохранить**.

Перезагрузка ViPNet Coordinator HW

В случае выявления каких-либо неполадок в работе ViPNet Coordinator HW, вы можете удаленно перезагрузить его с помощью веб-интерфейса. Для этого выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Системные настройки** > **Перезагрузка** и нажмите кнопку **Перезагрузить устройство**. При этом соединение с веб-интерфейсом будет разорвано, после перезагрузки повторно подключитесь к нему (см. «Подключение к веб-интерфейсу» на стр. 17).

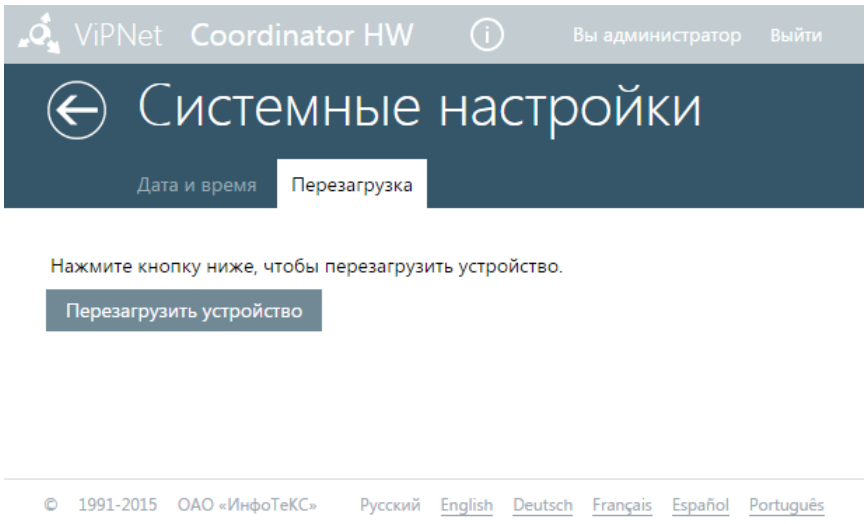


Рисунок 7. Перезагрузка ViPNet Coordinator HW

2

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet 24

Назначение дополнительных IP-адресов 27

Организация обработки трафика из нескольких VLAN 28

Подключение к беспроводной сети Wi-Fi 31

Подключение к мобильной сети 3G, 4G 34

Использование агрегированных сетевых интерфейсов 36

Настройка сетевых интерфейсов Ethernet

Чтобы настроить подключение к сети по протоколу Ethernet, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.

3 На левой панели выберите сетевой интерфейс Ethernet, который вы хотите настроить. Сетевым интерфейсам Ethernet, установленным в системе, присваиваются имена `eth0`, `eth1` и так далее (по количеству таких интерфейсов в системе).

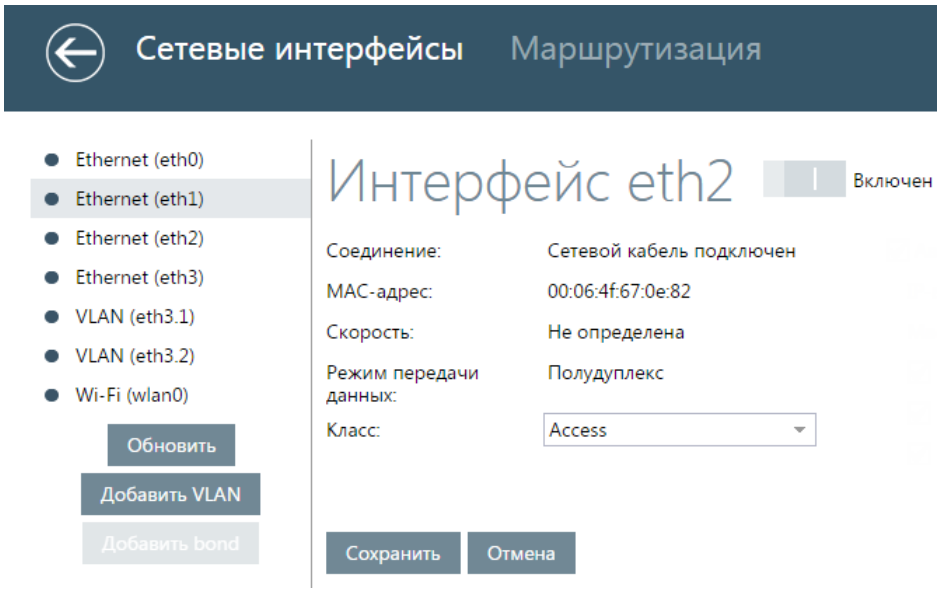


Рисунок 8. Выбор сетевого интерфейса Ethernet

4 По умолчанию сетевому интерфейсу назначен класс `Access` (см. глоссарий, стр. 157). При необходимости смените класс интерфейса в соответствующем списке:

- Если требуется, чтобы данный интерфейс Ethernet обрабатывал трафик из нескольких VLAN (см. «Организация обработки трафика из нескольких VLAN» на стр. 28), назначьте ему класс `trunk`.
- Если вы хотите объединить данный интерфейс Ethernet с другими в составе агрегированного интерфейса (см. «Использование агрегированных сетевых интерфейсов» на стр. 36), назначьте ему класс `slave`.

5 В правой части страницы выполните одно из действий:

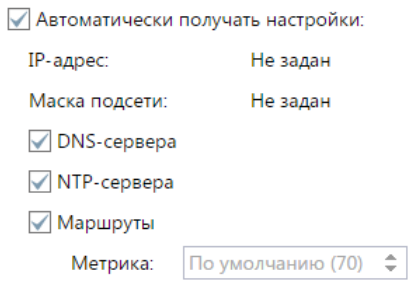


Рисунок 9. Настройка сетевого интерфейса

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Автоматически получать настройки.**

  Также для режима DHCP вы можете задать дополнительные параметры:

  - Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
  - Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
  - Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

    Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. Подробнее см. раздел Настройка параметров динамических маршрутов от DHCP/PPP-протокола (на стр. 125). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

    Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. «Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола» на стр. 129). Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера (на стр. 127).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите кнопку **Сохранить**.

6 Включите сетевой интерфейс. Для этого щелкните переключатель в верхней части страницы. Состояние сетевого интерфейса отображается рядом с переключателем.

Примечание. Сетевой интерфейс можно включить только после задания настроек подключения.

---

7 При необходимости выполните настройку маршрутизации (см. «Настройка маршрутизации» на стр. 112).

8 При необходимости задайте дополнительные IP-адреса для сетевого интерфейса (см. «Назначение дополнительных IP-адресов» на стр. 27).

Внимание! Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Назначение дополнительных IP-адресов

Назначение дополнительных IP-адресов (alias) для сетевых интерфейсов Ethernet ViPNet Coordinator HW удобно при развертывании сетей некоторых топологий. Например, с помощью дополнительных IP-адресов вы можете в рамках своей сети организовать логическую подсеть, узлам которой, в отличие от узлов остальной сети, будет разрешен доступ в Интернет.

Чтобы задать дополнительные IP-адреса на сетевом интерфейсе, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.
3. На левой панели выберите сетевой интерфейс, который вы хотите настроить.
4. Включите сетевой интерфейс. Для этого щелкните переключатель в верхней части страницы. Состояние сетевого интерфейса отображается рядом с переключателем.
5. На правой панели выполните следующие действия:
   - **5.1** Убедитесь, что сетевому интерфейсу назначен класс `access`.
   - **5.2** При задании дополнительного IP-адреса на сетевом интерфейсе должен быть установлен статический основной IP-адрес. Поэтому убедитесь, что снят флажок **Автоматически получать настройки**.
   - **5.3** В группе **Дополнительные IP-адреса** выполните одно из действий:
     - Чтобы добавить для сетевого интерфейса дополнительный IP-адрес, нажмите кнопку **Добавить** и появившейся строке задайте требуемый IP-адрес и маску подсети. Затем нажмите кнопку **Сохранить**.
     - Чтобы удалить дополнительный IP-адрес, в строке рядом с ним щелкните значок ✕. В окне сообщения нажмите кнопку **OK**.

Организация обработки трафика из нескольких VLAN

Вы можете использовать ViPNet Coordinator HW для обработки трафика в разветвленной сети, состоящей из нескольких независимых виртуальных локальных сетей VLAN (см. глоссарий, стр. 156). Это возможно благодаря поддержке виртуальных интерфейсов и тегированию (маркировке) трафика в соответствии со стандартом IEEE 802.1 Q.

Для организации обработки трафика из нескольких VLAN подключите один из сетевых интерфейсов ViPNet Coordinator HW (или компьютера, на котором развернут виртуальный образ ViPNet Coordinator HW) к коммутатору, объединяющему виртуальные сети, и выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы** (см. Рисунок 8 на стр. 24).
3. На левой панели выберите сетевой интерфейс Ethernet, к которому подключен коммутатор, и на правой панели в списке **Класс** выберите класс `trunk`. Нажмите кнопку **Сохранить**.
4. На левой панели нажмите кнопку **Добавить VLAN**. Появится окно **Создание VLAN**.

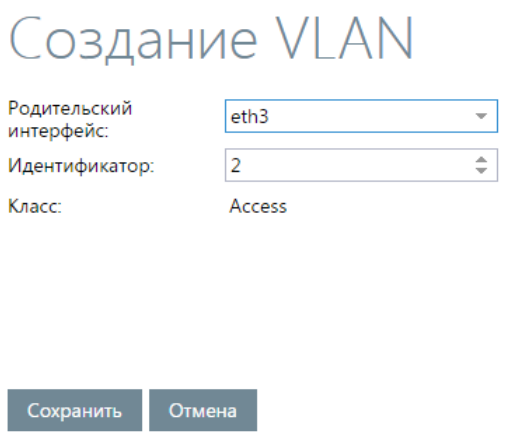


Рисунок 10. Создание виртуального интерфейса VLAN

5. В списке **Родительский интерфейс** отображаются интерфейсы Ethernet вашего ViPNet Coordinator HW, для которых указан класс `trunk`. Если таких интерфейсов несколько, выберите нужный вам.
6. В списке **Идентификатор** выберите номер создаваемого виртуального интерфейса. Создаваемому виртуальному интерфейсу будет присвоено имя в следующем формате:

   `<физический интерфейс>.<номер виртуального интерфейса>`
7. В правой части страницы укажите настройки для одной из сетей, находящихся за коммутатором:

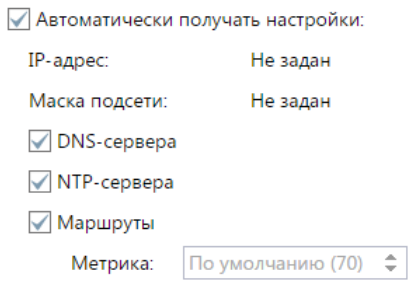


Рисунок 11. Настройка сетевого интерфейса

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Автоматически получать настройки.**

  Также для режима DHCP вы можете задать дополнительные параметры:

  - Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
  - Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
  - Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

    Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. Подробнее см. раздел Настройка параметров динамических маршрутов от DHCP/PPP-протокола (на стр. 125). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

    Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. «Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола» на стр. 129). Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера (на стр. 127).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите кнопку **Сохранить**.

8 В результате будет создан виртуальный интерфейс VLAN для одной из виртуальных сетей, находящихся за коммутатором. Он появится в списке сетевых интерфейсов на левой панели. Чтобы создать виртуальные интерфейсы для других сетей, повторите шаги 4–7.

9 Дальнейшие настройки необходимо производить в командном интерпретаторе (см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»):

9.1 Для редактирования файла конфигурации `iplir.conf` выполните команду:

```
hostname# iplir config
```

Примечание. Перед редактированием файла `iplir.conf` остановите демон iplir с помощью команды:

```
hotsname# iplir stop
```

После завершения редактирования файла `iplir.conf` запустите демон iplir с помощью команды:

```
hotsname# iplir start
```

9.2 Добавьте секции `[adapter]`, описывающие созданные виртуальные интерфейсы (см. документ «ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам», раздел «Секция [adapter]»). В каждой секции укажите следующие параметры:

```
name= <физический интерфейс>.<номер виртуального интерфейса>
type= internal
allowtraffic=on
```

9.3 В секции `[adapter]` с описанием интерфейса, к которому подключен коммутатор, присвойте параметру `allowtraffic` значение `off`:

9.4 Нажмите сочетание клавиш **Ctrl+O**, чтобы сохранить файл конфигурации, затем нажмите клавишу **Enter**.

9.5 Нажмите сочетание клавиш **Ctrl+X**, чтобы закрыть файл.

10 На левой панели выберите интерфейс, к которому подключен коммутатор, и включите его с помощью переключателя в верхней части страницы.

Созданные виртуальные интерфейсы VLAN включатся автоматически.

После произведенных настроек ViPNet Coordinator HW сможет обрабатывать трафик из виртуальных сетей на соответствующих виртуальных интерфейсах.

Пример организации обработки трафика из нескольких VLAN с помощью ViPNet Coordinator HW см. в документе «ViPNet Coordinator HW. Сценарии работы», раздел «Организация обработки трафика из нескольких VLAN».

Внимание! Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Подключение к беспроводной сети Wi-Fi

Внимание! Использование ViPNet Coordinator HW в качестве точки доступа Wi-Fi возможно только в исполнениях со встроенными адаптерами Wi-Fi: ViPNet Coordinator HW50 A, B на аппаратной платформе HW50 N2 и ViPNet Coordinator HW100 A, B на аппаратной платформе HW100 N2.

Чтобы настроить подключение к сети Wi-Fi, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.

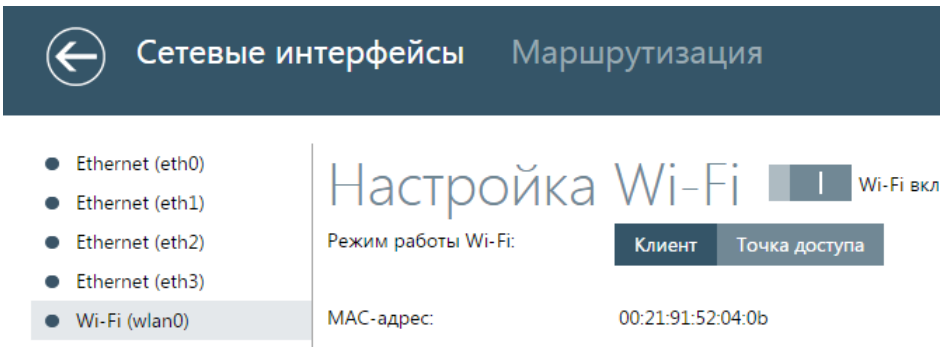


Рисунок 12. Выбор режима работы адаптера Wi-Fi

3 На левой панели выберите сетевой интерфейс Wi-Fi. Сетевому интерфейсу Wi-Fi, установленному в системе, присваивается имя `wlan0`.

4 Убедитесь, что выбранный интерфейс Wi-Fi включен. В противном случае щелкните переключатель в верхней части страницы. Состояние сетевого интерфейса отображается рядом с переключателем.

5 Сетевой интерфейс Wi-Fi всегда работает в режиме автоматического получения параметров от DHCP-сервера, при этом вы можете задать ряд дополнительных параметров. Для этого в правой части страницы выполните одно из приведенных ниже действий.

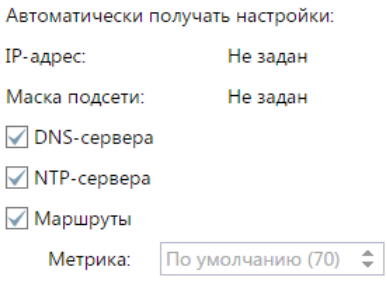


Рисунок 13. Настройка сетевого интерфейса Wi-Fi

- Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
- Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
- Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.
- Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. Подробнее см. раздел Настройка параметров динамических маршрутов от DHCP/PPP-протокола (на стр. 125). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. раздел Просмотр настроек DHCP в режиме клиента.

  Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. «Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола» на стр. 129). Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера (на стр. 127).

После задания необходимых настроек нажмите кнопку **Сохранить**.

6 Установите переключатель **Режим работы Wi-Fi** в положение **Клиент**.

7 Отобразится список доступных беспроводных сетей Wi-Fi.

Сети, защищенные паролем, отмечены значком . Сети с неподдерживаемыми типами аутентификации отмечены значком . Чтобы обновить список доступных сетей, нажмите кнопку **Обновить**.

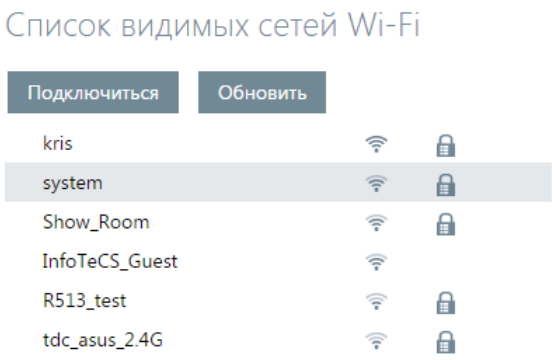


Рисунок 14. Выбор сети Wi-Fi для подключения

8 В списке доступных сетей Wi-Fi выберите сеть, к которой вы хотите подключиться, и нажмите кнопку **Подключиться**.

9 Если сеть защищена, в окне **Параметры подключения** в поле **Ключ безопасности** сети введите соответствующий пароль.

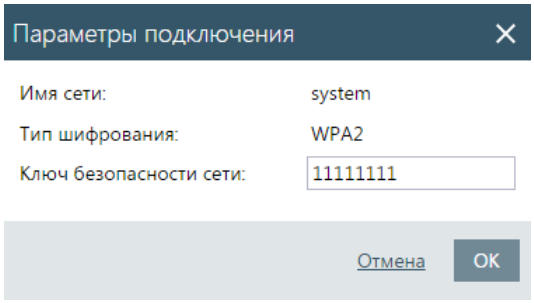


Рисунок 15. Подключение к защищенной сети Wi-Fi

10 Нажмите кнопку **Подключиться**.

В результате подключение к беспроводной сети Wi-Fi будет установлено.

Примечание. ViPNet Coordinator HW может также работать в качестве точки доступа к сети Wi-Fi (см. «Настройка параметров точки доступа к сети Wi-Fi» на стр. 109). Использование ViPNet Coordinator HW одновременно в качестве клиента и точки доступа Wi-Fi не поддерживается.

Подключение к мобильной сети 3G, 4G

Внимание! Подключение к мобильной сети возможно только в исполнениях ViPNet Coordinator HW со встроенными 3G-модемами: ViPNet ViPNet Coordinator HW50 A, B на аппаратной платформе HW50 N3 и ViPNet Coordinator HW100 A, B на аппаратной платформе HW100 N3.

Подключение к сети 3G, 4G выполняется по протоколу PPP. 3G-, 4G-модем представлен в операционной системе сетевым интерфейсом с именем `pppX`.

Для подключения к Интернету вы можете пользоваться услугами любого оператора мобильной связи. Для этого приобретите SIM-карту и установите ее в соответствующий слот ViPNet Coordinator HW. Если требуется, подключите необходимые услуги мобильного оператора. Подробную информацию об условиях подключения к Интернету можно получить у оператора мобильной связи.

Чтобы подключиться к мобильной сети, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.

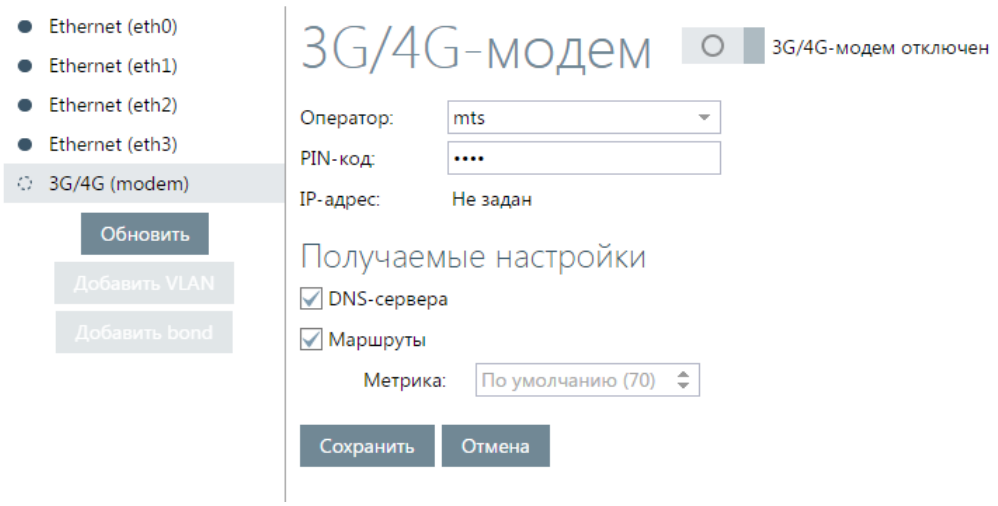


Рисунок 16. Настройка 3G-, 4G-модема

3. На левой панели выберите интерфейс модема, который вы хотите настроить.
4. В списке **Оператор** выберите название оператора, SIM-карту которого вы используете.
5. Если ваша SIM-карта защищена ПИН-кодом, в соответствующем поле введите этот ПИН-код.
6. При первом подключении модема к сети 3G, 4G на ViPNet Coordinator HW добавляется новый маршрут по умолчанию, в котором в качестве шлюза указан адрес узла сети вашего

мобильного оператора. Этот адрес 3G-, 4G-модем получает при подключении автоматически. Первоначально для нового маршрута задана метрика по умолчанию (см. «Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола» на стр. 129).

При необходимости выполните предварительные настройки ViPNet Coordinator HW в разделе **Получаемые настройки**:

- Если вы хотите задать для добавляемого маршрута другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов PPP-протокола (на стр. 128).
- Если вы не хотите добавлять маршрут по умолчанию, в котором используется шлюз, получаемый при первом подключении модема к сети 3G, 4G, снимите флажок **Маршруты**.
- При необходимости вы можете также отменить добавление адреса DNS-сервера, получаемого от вашего мобильного оператора при первом подключении 3G-, 4G-модема. Для этого снимите флажок **DNS-сервера**.

7 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

8 Включите интерфейс с помощью переключателя в верхней части страницы.

В результате подключение к мобильной сети 3G, 4G будет установлено. IP-адрес интерфейса появится в соответствующей строке.

Примечание. Если вы хотите изменить настройки 3G-, 4G-модема, сначала выключите его с помощью переключателя в верхней части страницы, затем установите необходимые параметры и снова включите модем.

Использование агрегированных сетевых интерфейсов

Если пропускной способности отдельных сетевых интерфейсов ViPNet Coordinator HW недостаточно для ваших задач или если требуется повысить надежность ваших каналов передачи данных, вы можете объединить несколько физических сетевых интерфейсов ViPNet Coordinator HW в один логический — агрегированный интерфейс (см. глоссарий, стр. 156). При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

Например, если вам нужен канал связи с пропускной способностью выше 1 Гбит/с, а на вашем исполнении ViPNet Coordinator HW есть только гигабитные интерфейсы, вы можете объединить два или три из них в один агрегированный. При этом даже если один из объединенных интерфейсов выйдет из строя, агрегированный канал продолжит работать.

Кроме того, вы можете использовать агрегированный интерфейс только для резервирования канала связи, без увеличения его пропускной способности. В этом случае весь трафик будет передаваться через один из подчиненных физических интерфейсов, остальные же начинают работать только при его сбое.

Агрегированные каналы целесообразно использовать в отказоустойчивых сетях, по каналам которых передаются большие объемы данных, например в сетях центров обработки данных.

Чтобы задать, как будет распределяться нагрузка по подчиненным физическим интерфейсам, необходимо выбрать один из режимов работы агрегированного интерфейса.

Создание агрегированного интерфейса

Чтобы добавить новый агрегированный сетевой интерфейс, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы** (см. Рисунок 8 на стр. 24).
3. На левой панели последовательно выберите сетевые интерфейсы Ethernet, которые вы хотите объединить, и на правой панели установите для них класс `slave`.
4. На левой панели нажмите кнопку **Добавить bond**. Откроется страница **Создание bond**.

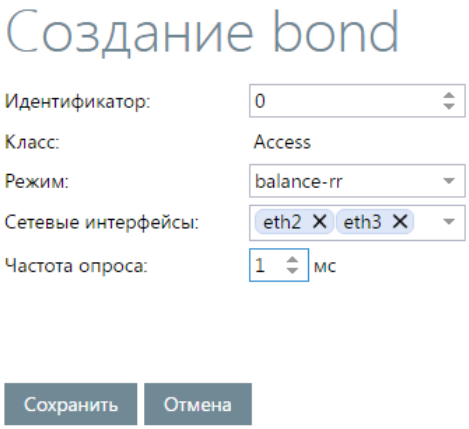


Рисунок 17. Создание агрегированного канала

5 На странице **Создание bond** задайте следующие параметры:

- В поле **Идентификатор** задайте номер создаваемого агрегированного интерфейса. Вы можете создать до трех агрегированных интерфейсов с номерами 0, 1 или 2. Созданный агрегированный интерфейс будет иметь имя `bond<номер>`.
- В списке **Режим** выберите режим работы агрегированного интерфейса.
- В списке **Сетевые интерфейсы** последовательно выберите физические интерфейсы класса `slave`, которые вы хотите объединить. Эти интерфейсы станут подчиненными для создаваемого агрегированного интерфейса. Вы можете выбрать до трех подчиненных интерфейсов. При создании агрегированного интерфейса необходимо выбрать не менее одного подчиненного интерфейса.

6 В поле **Частота опроса** задайте частоту проверки соединения на подчиненных физических интерфейсах в миллисекундах. Вы можете задать от 1 до 1000 миллисекунд.

7 Для режимов, в которых это требуется, задайте дополнительные параметры.

8 По умолчанию созданному интерфейсу назначается класс `access`. Если вы хотите, чтобы интерфейс обрабатывал трафик из нескольких VLAN (см. «Организация обработки трафика из нескольких VLAN» на стр. 28), назначьте ему класс `trunk`.

9 В правой части страницы выберите одно из действий:

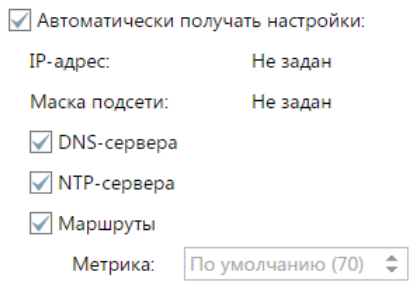


Рисунок 18. Настройка сетевого интерфейса

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Автоматически получать настройки.**

  Также для режима DHCP вы можете задать дополнительные параметры:

- Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
- Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
- Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. Подробнее см. раздел Настройка параметров динамических маршрутов от DHCP/PPP-протокола (на стр. 125). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

  Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. «Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола» на стр. 129). Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера (на стр. 127).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите кнопку **Сохранить**.

10 Дальнейшие настройки необходимо производить в командном интерпретаторе (см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»):

10.1 Для редактирования файла конфигурации `iplir.conf` выполните команду:

```
hostname# iplir config
```

Примечание. Перед редактированием файла `iplir.conf` остановите демон iplir с помощью команды:

```
hotsname# iplir stop
```

После завершения редактирования файла `iplir.conf` запустите демон iplir с помощью команды:

```
hotsname# iplir start
```

10.2 Добавьте секцию `[adapter]`, описывающую созданный агрегированный интерфейс (см. документ «ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам», раздел «Секция [adapter]»). В секции укажите следующие параметры:

```
name= bond<номер агрегированного интерфейса>
type= internal
allowtraffic= on
```

10.3 Нажмите сочетание клавиш **Ctrl+O**, чтобы сохранить файл конфигурации, затем нажмите клавишу **Enter**.

10.4 Нажмите сочетание клавиш **Ctrl+X**, чтобы закрыть файл.

11 Последовательно перейдите на страницы с настройками подчиненных физических интерфейсов и включите их с помощью соответствующих переключателей.

12 Вернитесь на страницу с агрегированным каналом и включите его с помощью переключателя в верхней части страницы.

В результате будет создан агрегированный канал с именем `bond<номер>`, работающий в заданном режиме и имеющий заданный класс. В дальнейшем вы можете работать с агрегированным интерфейсом так же, как и с обычным физическим.

Внимание! Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Режимы работы агрегированного интерфейса

При создании агрегированного интерфейса необходимо указать режим его работы, наиболее подходящий для решения ваших задач. В ViPNet Coordinator HW предусмотрено несколько режимов, позволяющих по-разному распределять нагрузку между подчиненными интерфейсами. Эти режимы и их параметры описаны в таблице ниже.

Таблица 5. Режимы работы агрегированного интерфейса

Режим	Описание
`balance-rr`	Режим, подходящий как для балансировки нагрузки на подчиненных интерфейсах, так и для защиты от сбоев. Может применяться в сетях с простой топологией. В этом режиме исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.
`balance-xor`	Режим, предназначенный для защиты от сбоев и распределения нагрузки таким образом, чтобы пакеты от одного и того же отправителя к одному и тому же получателю всегда отправлялись через один и тот же подчиненный интерфейс. В этом режиме для определения подчиненного физического интерфейса, через который отправляется пакет, используется специальная хэш-функция, алгоритм вычисления которой вы можете задать с помощью списка **Алгоритм хеширования** после создания агрегированного интерфейса. Вы можете задать один из следующих алгоритмов: • `layer2` — в алгоритме используются MAC-адреса отправителя и получателя пакета, таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами; • `layer2+3` — в алгоритме используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протокола

Режим	Описание
	IPv4), таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами и IP-адресами; • `layer3+4` — в алгоритме используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии), таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами, IP-адресами, а также портами TCP или UDP.
`balance-tlb`	Режим, предназначенный для балансировки нагрузки на подчиненных интерфейсах и рекомендуемый к использованию при передаче большого числа пакетов разного размера, когда более простые режимы не распределяют нагрузку равномерно. В этом режиме ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных физических интерфейсов, и на основе этого выполняется выбор интерфейса, через который будет передан пакет, попавший на агрегированный интерфейс. **Примечание.** Для работы агрегированного интерфейса в режиме `balance-tlb` необходимо, чтобы все подчиненные физические интерфейсы были подключены к сети через коммутатор.
`802.3ad`	Режим динамического агрегирования с использованием протокола LACP, предназначен для комплексной балансировки нагрузки. В этом режиме агрегированный интерфейс работает следующим образом: • Среди подчиненных физических интерфейсов формируются группы — «агрегаторы», скорость передачи данных на интерфейсах которых одинакова (например, группа гигабитных интерфейсов и группа 10-гигабитных интерфейсов). • Один из агрегаторов выбирается активным в соответствии с алгоритмом, задаваемым с помощью списка **Режим агрегатора** после создания агрегированного интерфейса. Вы можете выбрать один из приведенных ниже алгоритмов: `stable` — алгоритм, при котором первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора. `bandwidth` — режим, при котором первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора. `count` — режим, при котором первоначально выбирается агрегатор с наибольшим количеством подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора. • Внутри агрегатора подчиненный физический интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму

Режим	Описание
	`balance-xor`. • С другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью списка **Частота обмена пакетами** после создания агрегированного интерфейса. В случае выбора параметра `slow` обмен пакетами по протоколу LACP выполняется каждые 30 секунд, в случае выбора параметра `fast` — каждую секунду. Обмен пакетами позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую.
`active-backup`	Режим, предназначенный для защиты от сбоев, но не для балансировки нагрузки на подчиненных физических интерфейсах. В этом режиме один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью списка **Основной интерфейс** после создания агрегированного интерфейса), и все исходящие пакеты отправляются через него. При этом, в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
`broadcast`	Режим предоставляет наибольшую защиту от сбоев. В этом режиме пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно.

Примечание. Если в процессе функционирования агрегированного канала вы измените режим работы агрегированного интерфейса, возможно кратковременное пропадание соединения (до 1 секунды).

3

Просмотр и изменение параметров VPN

Просмотр информации о сетевых узлах ViPNet 43

Проверка соединения с сетевым узлом ViPNet 45

Просмотр и изменение списка туннелируемых узлов 46

Настройка защиты соединения по технологии L2OverIP 48

Просмотр информации о сетевых узлах ViPNet

Вы можете просмотреть сведения об узлах ViPNet, для которых администратор сети ViPNet в программе ViPNet Центр управления сетью (см. глоссарий, стр. 156) создал связь с вашим узлом ViPNet Coordinator HW (например, чтобы узнать IP-адреса доступа к узлам). Для этого выполните следующие действия:

1 На начальной странице веб-интерфейса щелкните плитку **VPN**.

2 На странице **Защищенная сеть** на вкладке **Узлы** просмотрите список имен и IP-адресов сетевых узлов ViPNet, с которыми у вашего узла есть связь, а также сведения о времени последней активности пользователей этих узлов. В этом списке:

- слева от имен узлов, являющихся клиентами ViPNet (см. глоссарий, стр. 157), отображается значок ;
- слева от имен узлов, являющихся координаторами ViPNet, отображается значок ;
- узлы, которые в текущий момент недоступны либо статус которых неизвестен, выделены серым цветом.

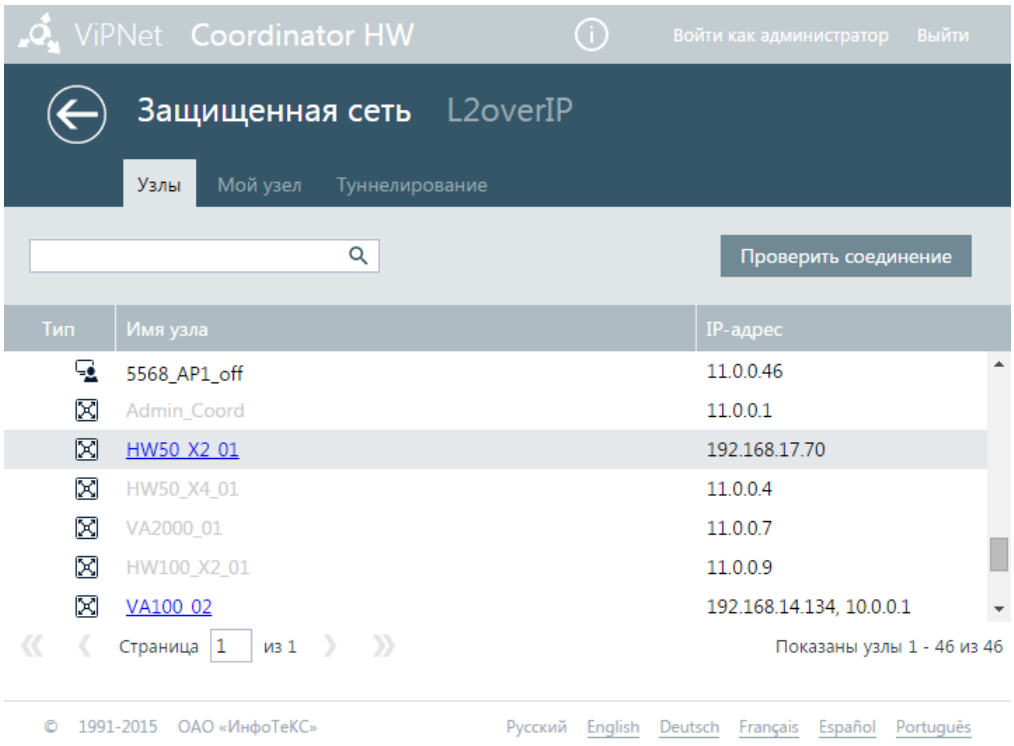


Рисунок 19. Просмотр списка защищенных узлов

3 Чтобы просмотреть подробные сведения о каком-либо узле, дважды щелкните его в списке. На открывшейся странице на панели навигации выберите соответствующий раздел, чтобы просмотреть следующую информацию:

- общая информация: имя узла, версия ПО ViPNet и операционной системы, установленных на узле, текущие IP-адреса видимости узла, порт доступа для TCP-туннеля;

> **Примечание.** Информация о версиях ПО ViPNet и операционной системы, установленных на узле, отображается только после проверки соединения с данным узлом (см. «Проверка соединения с сетевым узлом ViPNet» на стр. 45).

- IP-адреса доступа к узлу: реальные и виртуальные;
- настройки межсетевого экрана при подключении к внешней сети (для координаторов);
- настройки туннелирования (для координаторов).

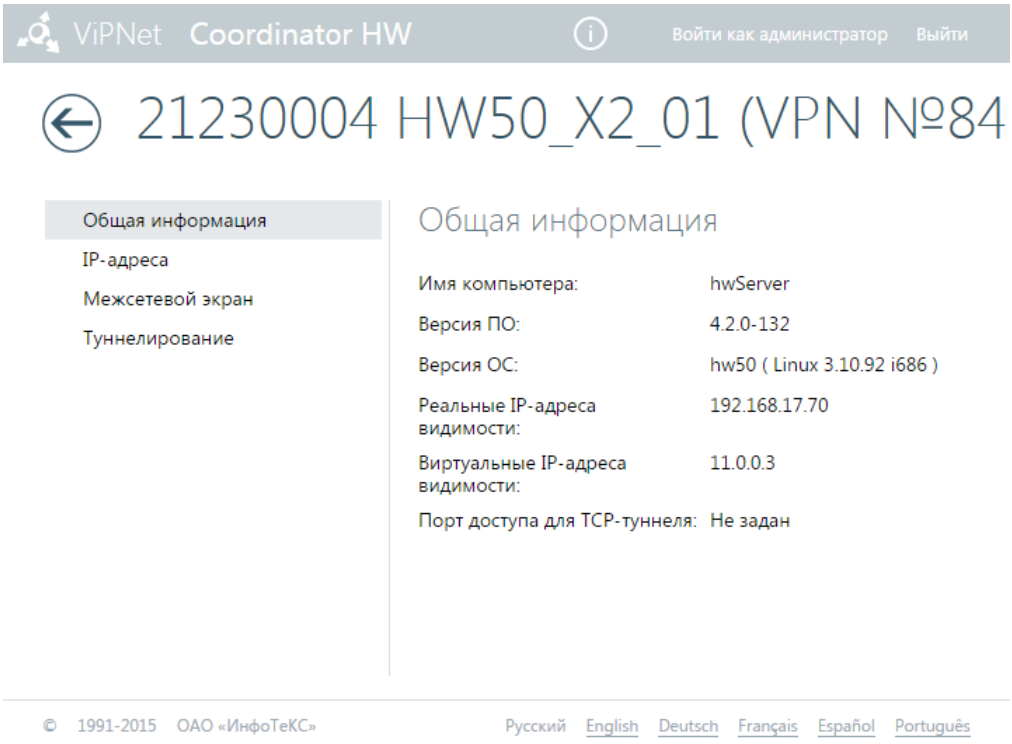


Рисунок 20. Просмотр информации об узле ViPNet

> **Примечание.** Чтобы просмотреть описанную выше информацию о собственном сетевом узле, на странице **VPN** > **Защищенная сеть** выберите вкладку **Мой узел**.

Проверка соединения с сетевым узлом ViPNet

Вы можете проверить соединение с сетевым узлом ViPNet (например, если работа с ресурсами этого узла была прервана, и вы хотите выяснить причину неполадки). Для этого выполните следующие действия:

1 Перейдите на страницу **VPN > Защищенная сеть**.

2 На вкладке **Узлы** (см. Рисунок 19 на стр. 43) в списке выберите узел, соединение с которым вы хотите проверить.

Совет. Чтобы быстро найти нужный узел в списке, воспользуйтесь полем поиска на панели инструментов.

3 На панели инструментов нажмите кнопку **Проверить соединение**. Если узел доступен, его имя будет выделено черным цветом. Для сетевых узлов под управлением ОС Windows также будет отображаться информация о времени последней активности пользователя этого узла.

Просмотр и изменение списка туннелируемых узлов

Технология туннелирования (см. глоссарий, стр. 160) позволяет защищать трафик открытых узлов корпоративной сети на потенциально опасном участке сети или включать открытые узлы в защищенную сеть без установки на эти узлы программного обеспечения ViPNet. Параметры туннелирования узлов задаются на координаторах сети ViPNet, которые будут выполнять туннелирование этих узлов.

Обычно параметры туннелирования рассылаются на узлы в составе справочников и ключей. Если туннелируемые адреса координатора заданы в программе ViPNet Центр управления сетью, то другие узлы получат информацию об этом автоматически. Если туннелируемые адреса заданы на координаторе вручную, эти адреса также необходимо указать вручную на каждом узле, который будет работать с этими туннелируемыми узлами посредством сети ViPNet.

В случае наличия лицензии на туннелирование хотя бы одного соединения вы можете просматривать информацию о количестве туннелируемых узлов, а также просматривать и добавлять IP-адреса сетевых узлов, туннелируемых вашим ViPNet Coordinator HW. Для этого выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **VPN** > **Защищенная сеть**.
3. Выберите вкладку **Туннелирование**. В результате отобразится информация о количестве туннелируемых узлов и их IP-адресах.

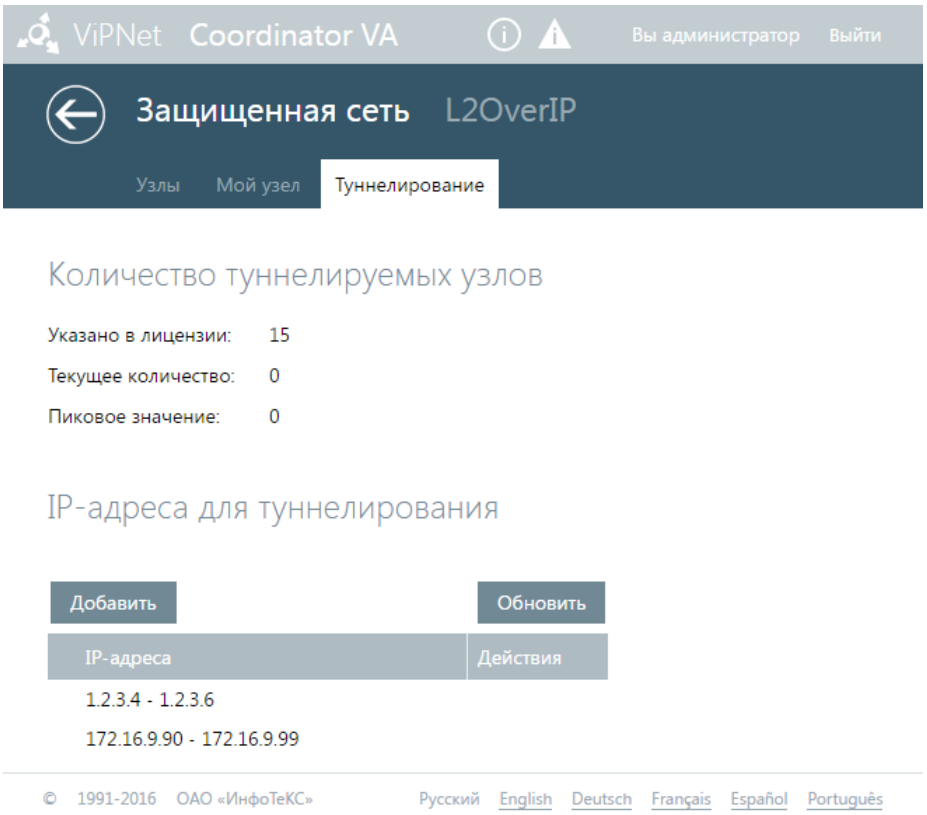


Рисунок 21. Просмотр и изменение списка туннелируемых узлов

4 Чтобы добавить IP-адрес туннелируемого узла в список, нажмите кнопку **Добавить** и задайте IP-адрес или диапазон IP-адресов узлов, туннелируемых вашим ViPNet Coordinator HW.

Внимание! На всех узлах, туннелируемых вашим ViPNet Coordinator HW, необходимо указать ViPNet Coordinator HW в качестве шлюза по умолчанию.

Настройка защиты соединения по технологии L2OverIP

Общее описание технологии L2OverIP

В ViPNet Coordinator HW реализована поддержка технологии L2OverIP (см. глоссарий, стр. 155), 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. Такая защита может потребоваться, например, для организации работы территориально распределенных ЦОДов (центров обработки данных), локальные сети которых объединены высокоскоростным каналом связи и представляют собой единый домен коллизий (см. глоссарий, стр. 157).

Внимание! Исполнения ViPNet Coordinator HW50 A, B и ViPNet Coordinator HW100 A, B не поддерживают функцию L2OverIP.

Функцию L2OverIP нельзя использовать для объединения сегментов, которые соединены какими-то другими каналами связи. Сегменты должны быть полностью разобщены. Иначе это может парализовать работу всей сети.

Для работы функции L2OverIP в исполнении ViPNet Coordinator HW VA необходимо в настройках среды виртуализации включить неразборчивый режим (Promiscuous Mode) для интерфейса, к которому привязан адаптер виртуальной машины. Подробнее см. руководство администратора платформы виртуализации, которую вы используете.

Технология L2OverIP предполагает взаимодействие между узлами нескольких удаленных сегментов сети через ViPNet Coordinator HW, которые установлены на границе этих сегментов. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой. Каждый ViPNet Coordinator HW осуществляет перехват Ethernet-кадров, отправленных из его сегмента сети в другой, их упаковку в IP-пакеты специального формата и передачу этих IP-пакетов другому ViPNet Coordinator HW по защищенному каналу. ViPNet Coordinator HW, получивший IP-пакеты специального формата, извлекает из них исходные кадры и передает получателям в своем сегменте.

Примечание. В большинстве практически важных случаев нужного результата можно достичь, объединяя не более 252 IP-адресов во всех объединяемых сегментах сети. Многократное превышение этого количества может привести к серьезному снижению производительности сети в объединяемых сегментах.

С увеличением числа IP-адресов в одном широковещательном сегменте сети значительно возрастает количество широковещательных служебных пакетов, что приводит к снижению пропускной способности сети и увеличению нагрузки на ViPNet Coordinator HW.

С помощью функции L2OverIP можно объединить несколько сегментов сети, в том числе сегменты, состоящие из виртуальных локальных сетей (VLAN). Возможны следующие варианты объединения:

- сегменты без VLAN, находящиеся за сетевыми интерфейсами класса `access`;
- виртуальная сеть VLAN из одного сегмента и виртуальная сеть VLAN из другого сегмента;
- все виртуальные сети VLAN из одного сегмента со всеми виртуальными сетями другого сегмента (для этого необходимо указать сетевые интерфейсы класса `trunk`, за которыми находятся виртуальные сети VLAN; кроме того, адреса виртуальных сетей VLAN должны совпадать);
- одна из виртуальных сетей VLAN сегмента и сегмент без VLAN, находящийся за сетевым интерфейсом класса `access`.

Примечание. Текущая версия ViPNet Coordinator HW позволяет объединить не более 31 сегмента сети.

Включение, выключение и настройка функции L2OverIP выполняется с помощью командного интерпретатора или веб-интерфейса (см. «Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI» на стр. 51).

Примечание. С помощью функции L2OverIP нельзя объединить между собой сети, находящиеся за ViPNet Coordinator HW разных версий (3.x и 4.x).

При использовании функции L2OverIP ViPNet Coordinator HW работает как виртуальный сетевой коммутатор, хранящий в памяти таблицу MAC-адресов сетевых узлов, от которых поступает сетевой трафик.

Каждому сегменту сети назначается свой номер порта, номера портов задаются в настройках L2OverIP. Порт, заданный для собственного сегмента сети, называется локальным. Порты, заданные на ViPNet Coordinator HW в других сегментах, называются удаленными. Трафик самого ViPNet Coordinator HW всегда относится к порту с номером 0.

Виртуальный коммутатор может по-разному обрабатывать одноадресные Ethernet-кадры с неизвестным MAC-адресом получателя: блокировать либо обрабатывать как многоадресные с рассылкой на все удаленные порты. Последняя возможность позволяет использовать функцию L2OverIP для схемы, когда два ViPNet Coordinator HW объединены с помощью агрегированного

канала и каждый из физических каналов работает через свою пару ViPNet Coordinator HW. В такой схеме (см. Рисунок 22 на стр. 50) кадры, которыми обмениваются два узла из разных сегментов, могут в одном направлении постоянно пересылаться через одну пару ViPNet Coordinator HW, а в другом направлении — через другую. В этом случае адрес получателя кадров будет определяться как неизвестный, и для обработки пакетов многоадресной рассылки следует использовать режим `smart-broadcast` (см. «Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI» на стр. 51).

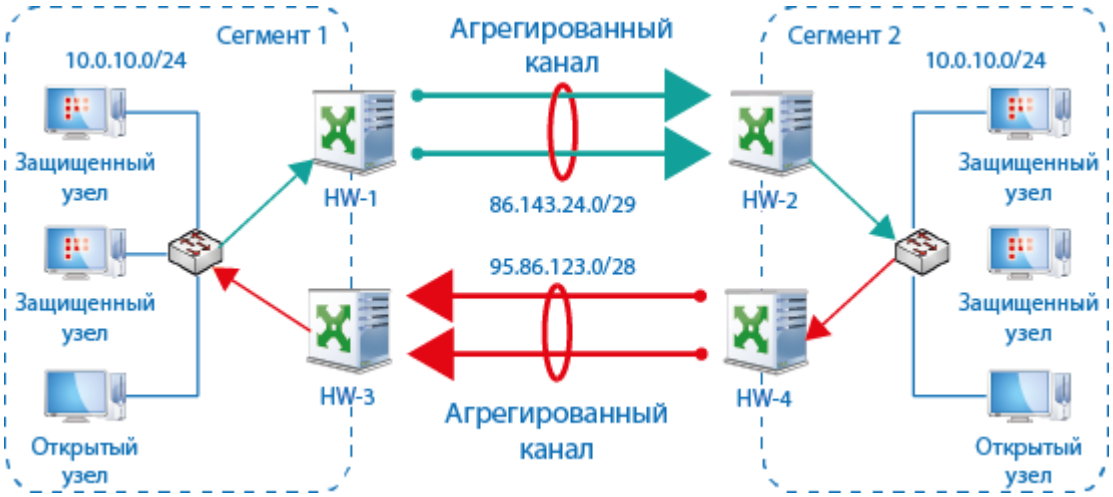


Рисунок 22. Схема работы сети с парами ViPNet Coordinator HW, объединенных с помощью агрегированных каналов

Рассылка Ethernet-кадров с неизвестным MAC-адресом получателя выполняется в соответствии с выбранным режимом обработки:

- кадры, принятые из локального порта, пересылаются на все удаленные порты и на порт с номером 0;
- кадры, принятые из удаленного порта, пересылаются на локальный порт и на порт с номером 0;
- кадры, принятые из порта с номером 0, в зависимости от выбранного режима либо блокируются, либо пересылаются на локальный порт и на все удаленные порты.

Функцию L2OverIP можно использовать в кластере горячего резервирования. В этом случае настройки функции L2OverIP достаточно выполнить на активном сервере, на пассивный сервер они передаются автоматически, если включено резервирование файлов конфигурации. При этом включить функциональность можно только на сервере, находящемся в активном режиме, на пассивном сервере он всегда выключен и будет включен только при переходе сервера в активный режим.

При работе в кластере горячего резервирования таблица MAC-адресов не передается пассивному серверу, и при переключении пассивного сервера в активный режим его таблица пуста. Это может привести к увеличению времени конвергенции сети после смены активного сервера — до тех пор, пока узлы из разных сегментов, взаимодействующие друг с другом, не отправят заново ARP-запросы.

Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI

При организации соединения между удаленными сегментами сети на канальном уровне каждый сегмент сети подключается к одному из интерфейсов ViPNet Coordinator HW, установленному на границе сегмента. Если сегмент сети состоит из нескольких VLAN (см. глоссарий, стр. 156), они должны быть объединены с помощью коммутатора в транковый порт, к которому подключается один из интерфейсов ViPNet Coordinator HW (см. «Организация обработки трафика из нескольких VLAN» на стр. 28).

Чтобы организовать защиту соединения сегментов, на каждом ViPNet Coordinator HW включите функцию L2OverIP и задайте ее параметры. Для этого выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **VPN** > **L2OveIP**.

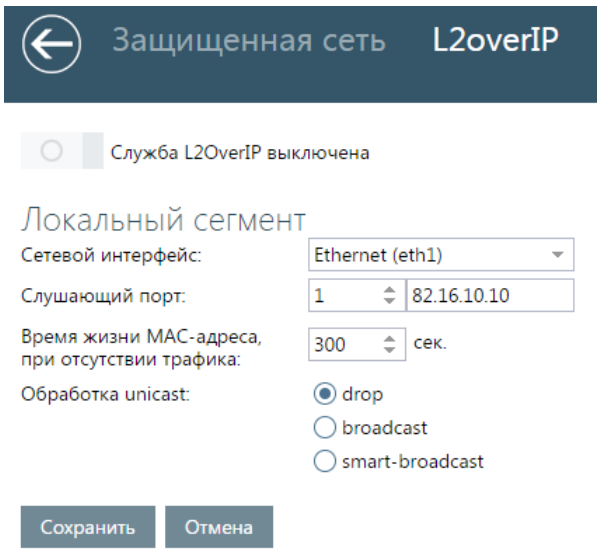


Рисунок 23. Настройка параметров соединения L2OverIP

3 В списке **Сетевой интерфейс** выберите сетевой интерфейс, сегмент сети которого будет объединяться с удаленным сегментом с помощью функции L2OverIP.

4 Задайте параметры локального сегмента сети, выбрав уникальный номер порта в списке **Слушающий порт** и IP-адрес внешнего интерфейса в поле **IP-адрес**.

5 При необходимости измените время жизни MAC-адреса в таблице MAC-адресов виртуального коммутатора (см. «Общее описание технологии L2OverIP» на стр. 48) при отсутствии трафика, поступающего от этого адреса, в соответствующем списке.

6 При необходимости измените режим обработки функцией L2OverIP одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя. Для этого установите переключатель **Обработка unicast** в одно из следующих положений:

- `drop` — блокировать.
- `broadcast` — обрабатывать как многоадресные с рассылкой на несколько портов:
  - кадры, принятые от локального порта, пересылаются на все удаленные порты и на порт с номером 0;
  - кадры, принятые от удаленного порта, пересылаются на локальный порт и на порт с номером 0;
  - кадры, принятые от порта с номером 0, пересылаются на локальный порт и на все удаленные порты.
- `smart-broadcast` — аналогично режиму `broadcast`, но без обработки кадров, принятых от порта с номером 0. В этом режиме кадры, принятые от порта с номером 0, блокируются.

7 Задайте параметры удаленного сегмента сети, указав его номер порта и актуальный адрес видимости удаленного ViPNet Coordinator HW. Для этого выполните следующие действия:

7.1 В области **Удаленные сегменты** нажмите кнопку **Добавить сегмент**.

7.2 В соответствующих полях укажите IP-адрес и порт уделенного сегмента сети.

7.3 Нажмите кнопку **Сохранить**.

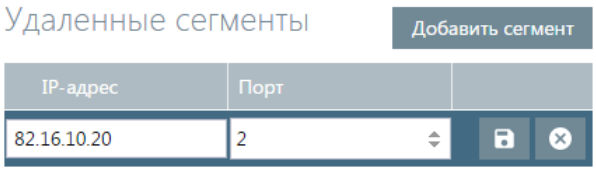


Рисунок 24. Добавление удаленного сегмента сети при создании соединения L2OverIP

8 Добавьте сетевой фильтр защищенной сети, разрешающий любые соединения по протоколу 97 (см. «Создание и изменение сетевого фильтра» на стр. 76).

9 Включите функцию L2OverIP. Для этого щелкните переключатель в верхней части страницы.

После настройки и включения функции L2OverIP на всех ViPNet Coordinator HW взаимодействие между узлами удаленных сегментов сети будет защищено на канальном уровне модели OSI.

Внимание! На двух ViPNet Coordinator HW, между которыми организовано соединение L2OverIP, IP-адреса локального и удаленного сегментов должны быть настроены симметричным образом. То есть на каждом ViPNet Coordinator HW в качестве IP-адреса удаленного сегмента должен быть указан IP-адрес видимости сетевого интерфейса, который задан на втором ViPNet Coordinator HW в качестве внешнего интерфейса локального сегмента.

Примеры организации защищенного соединения между удаленными сегментами сети с использованием технологии L2OverIP см. в документе «ViPNet Coordinator HW. Сценарии работы», раздел «Защита соединения между удаленными сегментами сети на канальном уровне модели OSI».

4

Настройка сетевых фильтров

Основные принципы фильтрации трафика 55

Общие сведения о сетевых фильтрах 59

Группы объектов 61

Просмотр групп объектов 64

Создание и изменение группы объектов 65

Просмотр сетевых фильтров 75

Создание и изменение сетевого фильтра 76

Пример использования групп объектов и сетевых фильтров 79

Основные принципы фильтрации трафика

Фильтрации подвергается весь трафик, который проходит через сетевой узел:

- открытый (нешифрованный) трафик;
- защищенный (зашифрованный) трафик;
- туннелируемый трафик.

Рисунок 25. Виды IP-трафика

Наибольшую опасность представляет трафик из открытой сети, поскольку в случае атаки достаточно сложно обнаружить ее источник и принять оперативные меры по ее пресечению.

И открытый, и защищенный трафик может быть локальным или широковещательным. Под локальным трафиком понимается входящий или исходящий трафик конкретного узла (то есть когда сетевой узел является отправителем или получателем IP-пакетов). Под широковещательным трафиком имеется в виду передача узлом IP-пакетов, у которых IP-адрес или MAC-адрес назначения является широковещательным адресом (то есть когда пакеты передаются всем узлам определенного сегмента сети).

Кроме этого, через координатор может проходить транзитный трафик. Координатор логически не является ни отправителем, ни получателем транзитных IP-пакетов, такие пакеты следуют через него на другие узлы.

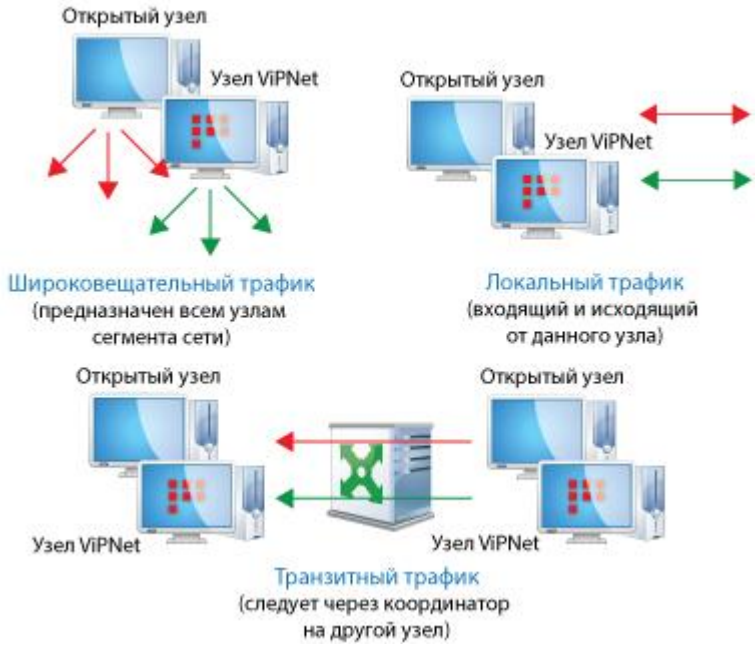


Рисунок 26. Виды защищенного и открытого трафика

Для того чтобы правильно настроить сетевые фильтры (см. глоссарий, стр. 159), необходимо понимать основные принципы фильтрации трафика:

- Все открытые IP-пакеты, в том числе те, которые передаются между координаторами и туннелируемыми ресурсами, проверяются в соответствии с правилами антиспуфинга, если они настроены.

  Если IP-пакет имеет адрес отправителя, разрешенный правилом антиспуфинга, он пропускается, в противном случае — блокируется.

- Все входящие и исходящие открытые и зашифрованные IP-пакеты проверяются в соответствии с условиями сетевых фильтров в порядке убывания приоритета этих фильтров (см. «Общие сведения о сетевых фильтрах» на стр. 59).

- Если IP-пакет соответствует условию одного из фильтров, то он пропускается или блокируется этим фильтром.

- Если IP-пакет был пропущен или заблокирован одним из фильтров, то фильтры с более низким приоритетом никак на него не влияют.

- Если IP-пакет был пропущен одним из фильтров, то ответные IP-пакеты в рамках текущего соединения будут пропускаться автоматически.

- Если IP-пакет не был обработан ни одним фильтром, то он блокируется фильтром по умолчанию.

- Вновь созданные фильтры влияют как на новые, так и на уже существующие соединения. То есть, если фильтр, блокирующий трафик какого-либо соединения, добавлен после установления этого соединения, то соединение будет разорвано.

Для того чтобы правильно настроить фильтры открытой сети (см. «Общие сведения о сетевых фильтрах» на стр. 59), необходимо понимать схему фильтрации открытого трафика в ViPNet Coordinator HW (см. Рисунок 27 на стр. 58):

1. Все входящие IP-пакеты проверяются на предмет фрагментации, если включена соответствующая настройка межсетевого экрана (см. раздел «Настройка дополнительных параметров межсетевого экрана» документа «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»).
2. Если IP-пакет фрагментирован, то он блокируется. Если IP-пакет не фрагментирован, то для него выполняется трансляция адреса назначения (Destination NAT) (см. «Трансляция адреса назначения» на стр. 84), если создано соответствующее правило трансляции адресов.
3. После трансляции адреса назначения IP-пакет проходит проверку встроенным средством антиспуфинга, если оно включено (см. раздел «Настройка антиспуфинга» документа «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»).
4. В случае успешной проверки встроенным средством антиспуфинга для IP-пакета возможны следующие варианты дальнейшего пути:
   - Если IP-пакет относится к протоколу HTTP (транспортный протокол TCP, порт 80) и прокси-сервер включен:
     - IP-пакет проходит проверку на уровне фильтрации содержимого трафика (см. «Настройка фильтрации содержимого трафика» на стр. 105).
     - В случае успешной проверки IP-пакет проходит антивирусную проверку, если она включена (см. «Настройка антивируса» на стр. 107).
     - В случае успешной антивирусной проверки IP-пакет пропускается.
   - Если IP-пакет не относится к протоколу HTTP или прокси-сервер выключен:
     - IP-пакет проходит проверку сетевыми фильтрами (см. «Общие сведения о сетевых фильтрах» на стр. 59).
     - В случае успешной проверки сетевыми фильтрами для IP-пакета выполняется трансляция адреса источника (Source NAT), если создано соответствующее правило трансляции адресов (см. «Трансляция адреса источника» на стр. 85).
     - Затем IP-пакет пропускается.

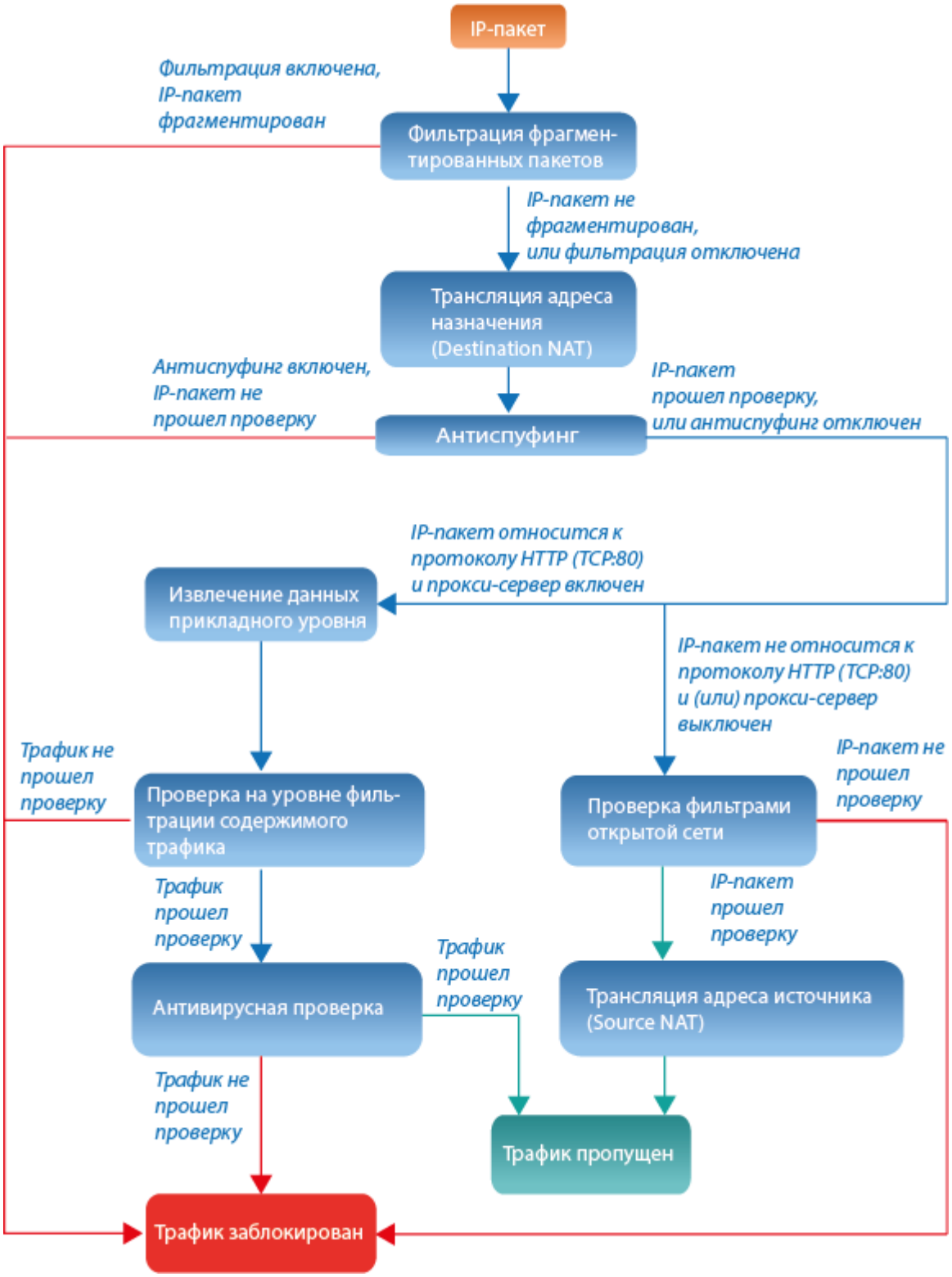


Рисунок 27. Схема фильтрации открытого трафика ViPNet Coordinator HW

Общие сведения о сетевых фильтрах

Различаются сетевые фильтры (см. глоссарий, стр. 159) для защищенного трафика, для открытого трафика (локального и транзитного) и для туннелируемого трафика. Они выполняют следующие функции:

- Фильтры открытой сети могут разрешать либо блокировать обмен IP-трафиком с открытыми узлами.

Примечание. Открытыми узлами называются узлы, на которых не установлено программное обеспечение ViPNet с функцией шифрования трафика. К ним относятся также компьютеры с программным обеспечением ViPNet CryptoService и ViPNet Registration Point.

- Фильтры защищенной сети могут разрешать или блокировать обмен IP-трафиком с защищенными узлами ViPNet (см. глоссарий, стр. 160), с которыми данный узел имеет связь.
- Фильтры для туннелируемого трафика могут разрешать или блокировать IP-пакеты, передаваемые между туннелируемыми узлами и узлами сети ViPNet, с которыми данный координатор имеет связь.

Внимание! Работа с фильтрами туннелируемых узлов возможна только при наличии лицензии на туннелирование хотя бы одного соединения.

Различаются следующие сетевые фильтры:

- Служебные фильтры, включающие:
  - Фильтры, разрешающие входящий и исходящий IP-трафик для служб ViPNet.
  - Фильтры, разрешающие открытый IP-трафик, который используется для проверки работоспособности сетевых интерфейсов в режиме кластера горячего резервирования (см. глоссарий, стр. 157).
- Фильтры, поступившие в составе политик безопасности. Политика безопасности представляет собой набор параметров, регулирующих безопасность сетевого узла. Она формируется администратором сети ViPNet в программе ViPNet Policy Manager (см. глоссарий, стр. 156), может включать сетевые фильтры и правила трансляции адресов и рассылается на узлы с помощью транспортного модуля MFTP. При получении политики безопасности из программы ViPNet Policy Manager она немедленно применяется на узле.
- Предустановленные фильтры и фильтры, заданные пользователем. Предустановленные фильтры разрешают только некоторые типы IP-пакетов (см. «Сетевые фильтры по умолчанию» на стр. 142). Для работы с какими-либо дополнительными сервисами пользователю необходимо создать соответствующие фильтры.

- Блокирующий фильтр по умолчанию.

Примечание. Если ViPNet Coordinator HW версии 4.x обновлялся с версии 3.x, вместо предустановленных фильтров на узле будут присутствовать фильтры, которые использовались до обновления в сконвертированном формате (подробнее см. в документе «ViPNet Coordinator HW. Подготовка к работе»).

Служебные фильтры создаются в ViPNet Coordinator HW автоматически, имеют самый высокий приоритет, то есть применяются в первую очередь, и недоступны для редактирования. После служебных фильтров применяются фильтры, поступившие в составе политик безопасности из программы ViPNet Policy Manager. Эти фильтры также недоступны для редактирования. Затем применяются предустановленные фильтры и фильтры, заданные пользователем. Их можно изменять и удалять. Наименьший приоритет имеет блокирующий фильтр по умолчанию, который нельзя ни изменить, ни удалить.

Последовательность применения сетевых фильтров в порядке убывания приоритета представлена ниже.

Рисунок 28. Последовательность применения сетевых фильтров

Сетевые фильтры могут включать в себя следующие параметры:

- условие — адрес отправителя и получателя IP-пакетов, на которые действует фильтр, и протоколы, используемые для передачи этих IP-пакетов (например, TCP, UDP, ICMP);
- расписание применения фильтра — ежедневно, еженедельно или по календарю;
- действие, применяемое к IP-пакетам — пропускать или блокировать IP-пакеты, соответствующие условию фильтра.

О том, как просмотреть фильтры, заданные на узле, создать или изменить фильтры на узле см. в соответствующем разделе ниже.

Группы объектов

Группы объектов позволяют упростить процессы создания и изменения сетевых фильтров и правил трансляции сетевых адресов (см. глоссарий, стр. 160) в ViPNet Coordinator HW. Каждая группа объединяет несколько объектов одного типа (например, IP-адреса или сетевые интерфейсы). Группы можно указывать при задании параметров фильтра или правила трансляции вместо перечисления отдельных объектов.

В зависимости от типа объединяемых объектов различаются следующие группы:

- Группа сетевых узлов ViPNet — содержит любую комбинацию узлов ViPNet, используется в фильтрах защищенной сети и фильтрах туннелируемых узлов.
- Группа IP-адресов — содержит любую комбинацию IP-адресов, диапазонов IP-адресов и DNS-имен, используется в фильтрах открытой сети, фильтрах туннелируемых узлов и правилах трансляции адресов.
- Группа сетевых интерфейсов — содержит любую комбинацию сетевых интерфейсов, используется в фильтрах открытой сети и фильтрах туннелируемых узлов.
- Группа протоколов — содержит любую комбинацию сетевых протоколов и портов, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов и правилах трансляции адресов.
- Группа расписания — содержит любую комбинацию параметров, определяющих время действия фильтра, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов и правилах трансляции адресов.

Каждая группа объектов относится к одному из следующих видов:

- Системные группы объектов — настроенные по умолчанию группы с фиксированными именами, которые могут использоваться для задания адресов отправителей и получателей IP-пакетов в фильтрах (см. «Создание и изменение сетевого фильтра» на стр. 76) и правилах трансляции адресов, а также при создании пользовательских групп объектов. Такие группы объектов не отображаются в списках групп (см. «Просмотр групп объектов» на стр. 64), их нельзя ни изменить, ни удалить.
- Группы объектов из программы ViPNet Policy Manager (см. глоссарий, стр. 156) — группы, получаемые в составе политик безопасности, и используемые в соответствующих фильтрах (см. «Общие сведения о сетевых фильтрах» на стр. 59). Такие группы нельзя ни удалять, ни изменять, ни использовать для задания параметров пользовательских фильтров и групп объектов.
- Пользовательские группы объектов — группы, создаваемые пользователем на узле, а также несколько групп, настроенных по умолчанию (см. «Пользовательские группы объектов по умолчанию» на стр. 63). Такие группы можно использовать для задания параметров фильтров (см. «Создание и изменение сетевого фильтра» на стр. 76) и правил трансляции, а также при создании других пользовательских групп объектов. При необходимости их можно удалить.

Системные группы объектов

В таблице ниже описаны доступные системные группы объектов.

Таблица 6. Системные группы объектов

Имя группы объектов в веб-интерфейсе (в командном интерпретаторе ViPNet)	**Описание**
Все клиенты (`allclients`)	Все клиенты (см. глоссарий, стр. 157), с которыми у узла есть связь. Можно использовать в фильтрах защищенной сети и фильтрах туннелируемых узлов для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла.
Все координаторы (`allcoordinators`)	Все координаторы, с которыми у узла есть связь. Можно использовать в фильтрах защищенной сети и фильтрах туннелируемых узлов для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла.
Широковещательные адреса (`broadcast`)	Все широковещательные адреса. Можно использовать в фильтрах защищенной сети и локальных фильтрах открытой сети для идентификации широковещательных адресов получателей. Использование других адресов совместно с этой группой недопустимо.
Мой узел (`local`)	Собственный узел. Можно использовать в фильтрах защищенной сети и локальных фильтрах открытой сети для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла. Использование других адресов совместно с этой группой недопустимо.
Другие узлы (`remote`)	Другие узлы ViPNet (любые, кроме собственного). Можно использовать в фильтрах защищенной и открытой сетей для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла.
Туннелируемые IP-адреса (`tunneledip`)	Все IP-адреса, туннелируемые координатором. Можно использовать в фильтрах туннелируемых узлов для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла.

Имя группы объектов в веб-интерфейсе (в командном интерпретаторе ViPNet)	Описание
Групповые адреса (`multicast`)	Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255). Можно использовать в локальных фильтрах открытой сети для задания назначения исходящих IP-пакетов узла. Использование других адресов совместно с этой группой недопустимо.
Все объекты (`any`)	Все объекты группы конкретного типа. Можно использовать только при создании других групп объектов.

Пользовательские группы объектов по умолчанию

По умолчанию в ViPNet Coordinator HW настроены следующие пользовательские группы объектов:

- Группы IP-адресов:
  - PrivateNetworkIP (частные IP-адреса) — включает IP-адреса локальных сетей: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16.
  - InternetIP (публичные IP-адреса) — включает все IP-адреса, за исключением частных IP-адресов.
- Группы протоколов, которые наиболее часто используются при создании сетевых фильтров. Они перечислены в приложении (см. «Пользовательские группы протоколов по умолчанию» на стр. 147).
- Группы расписаний:
  - Workdays (рабочие дни) — включает рабочие дни недели (с понедельника по пятницу).
  - Weekends (выходные дни) — включает выходные дни недели (субботу и воскресенье).

Примечание. О том, как просмотреть пользовательские группы объектов, созданные на узле, см. в разделе Просмотр групп объектов (на стр. 64).

Просмотр групп объектов

Чтобы просмотреть пользовательские группы объектов и группы объектов, полученные из программы ViPNet Policy Manager, выполните следующие действия:

1 На начальной странице веб-интерфейса щелкните плитку **Межсетевой экран** и перейдите в раздел **Группы объектов**.

2 На странице **Группы объектов** выберите вкладку групп объектов нужного типа. В результате отобразится список, содержащий имена групп объектов и информацию об объектах, входящих и не входящих в группу.

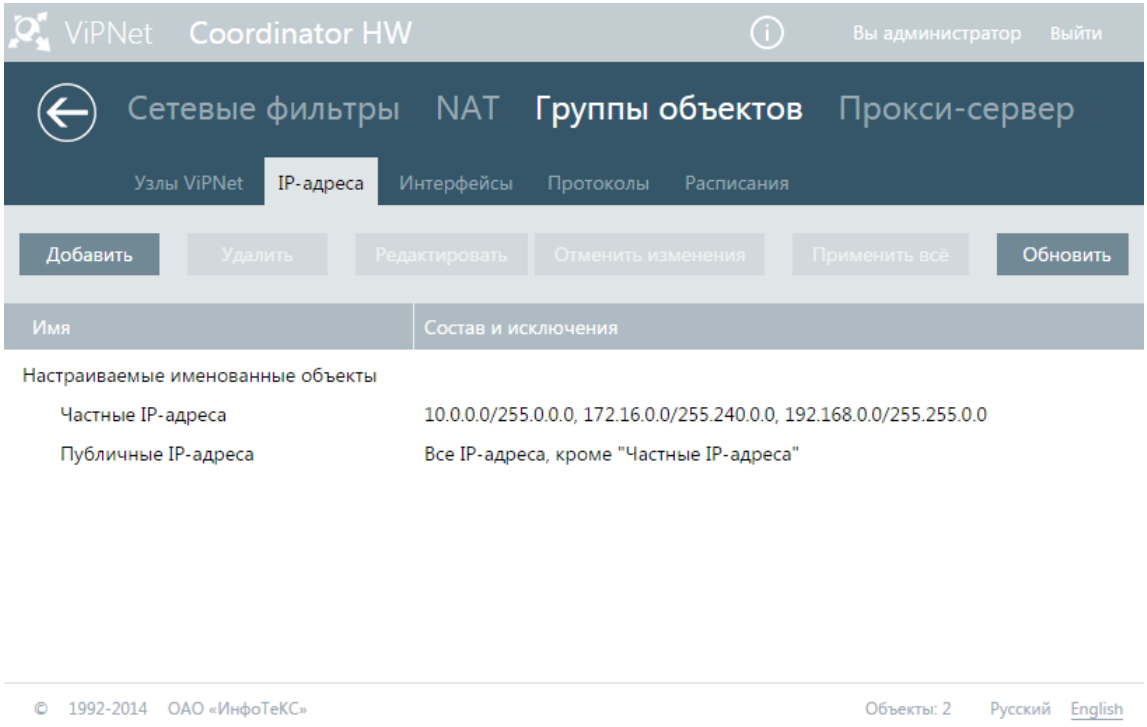


Рисунок 29. Просмотр групп IP-адресов

3 Для просмотра подробной информации об использовании группы объектов дважды щелкните ее в списке и на открывшейся странице нажмите кнопку **Просмотр**.

Создание и изменение группы объектов

Чтобы создать или изменить группу объектов, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 На странице **Межсетевой экран** > **Группы объектов** выберите вкладку групп объектов нужного типа.

3 Выполните одно из действий:

- Чтобы создать группу объектов, на панели инструментов нажмите кнопку **Добавить**.
- Чтобы изменить группу объектов, дважды щелкните ее в списке групп.

Примечание. Чтобы просмотреть, в каких сетевых фильтрах, правилах трансляции адресов и группах объектов используется группа, которую вы хотите изменить, нажмите кнопку **Показать**.

---

4 На странице создания или изменения группы задайте следующие параметры:

4.1 В соответствующем поле задайте имя группы.

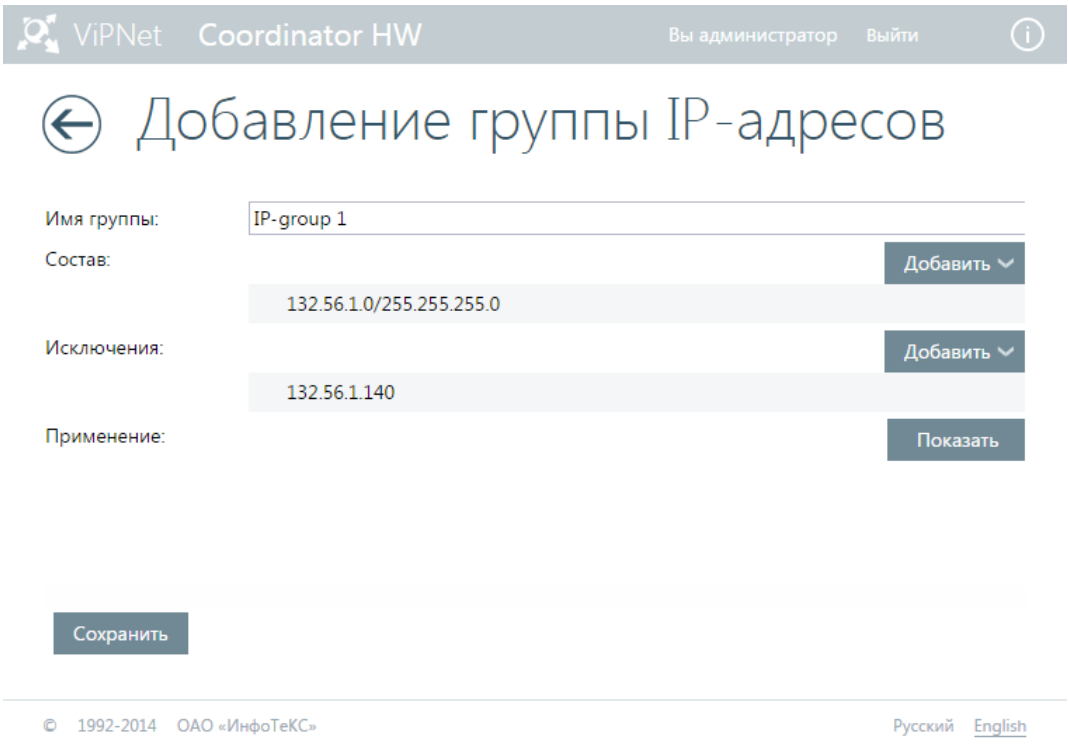


Рисунок 30. Создание группы IP-адресов

4.2 В разделах **Состав** и **Исключения** укажите объекты, входящие и не входящие в группу соответственно. Для этого в зависимости от типа объектов воспользуйтесь рекомендациями соответствующего раздела:

- Группа сетевых узлов ViPNet (на стр. 66).
- Группа IP-адресов (на стр. 68).
- Группа сетевых интерфейсов (на стр. 69).
- Группа протоколов (на стр. 71).
- Группа расписаний (на стр. 72).

4.3 Нажмите кнопку **Сохранить**.

Примечание. Чтобы изменить или удалить объект, который вы ранее добавили в группу или исключили из нее, в строке этого объекта нажмите кнопку или  соответственно.

---

5 Чтобы изменения вступили в силу, на странице **Группы объектов** нажмите кнопку **Применить все**.

Группа сетевых узлов ViPNet

При создании или изменении группы сетевых узлов ViPNet вы можете добавить или исключить следующие объекты:

- сетевые узлы ViPNet, с которыми связан узел ViPNet Coordinator HW;
- сеть ViPNet, с которой связана ваша сеть ViPNet;
- ранее созданную группу сетевых узлов ViPNet;
- системные группы объектов: **Все координаторы**, **Все клиенты**, **Все объекты**.

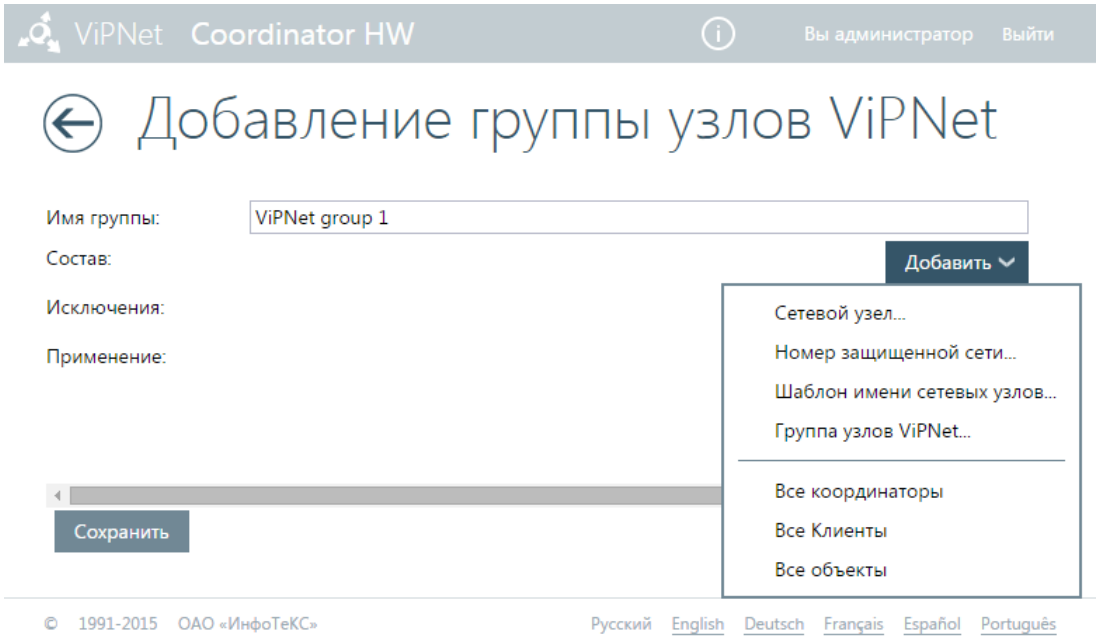


Рисунок 31. Добавление сетевого узла ViPNet в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) один или несколько сетевых узлов, выберите пункт **Сетевой узел** и установите флажки рядом с нужными узлами. Первым в этом списке отображается собственный узел.
- Если вы хотите добавить (исключить) несколько сетевых узлов с незначительно отличающимися именами, выберите пункт **Шаблон имени сетевых узлов** и укажите маску имен узлов, используя символ «?» для замены одного символа, и символ «*» для замены нескольких символов.
- Если вы хотите добавить (исключить) все узлы определенной сети ViPNet, выберите пункт **Номер защищенной сети** и укажите номер этой сети.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп сетевых узлов ViPNet, выберите пункт **Группа узлов ViPNet** и установите флажки рядом с нужными группами.
- Если вы хотите добавить (исключить) системную группу объектов, выберите соответствующую группу.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров защищенной сети и фильтров туннелируемых узлов (см. «Создание и изменение сетевого фильтра» на стр. 76).

Группа IP-адресов

При создании или изменении группы IP-адресов вы можете добавить или исключить следующие объекты:

- IP-адреса или диапазоны IP-адресов;
- DNS-имена;
- ранее созданные группы IP-адресов;
- системные группы: **Мой узел**, **Другие узлы**, **Все объекты**.

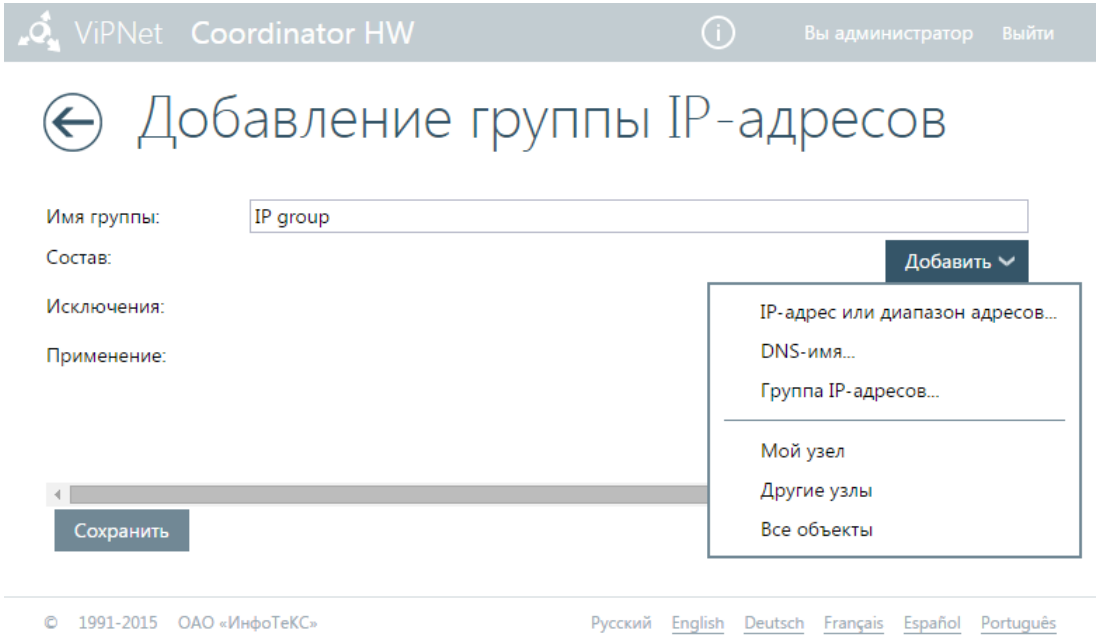


Рисунок 32. Добавление IP-адресов в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) один или несколько IP-адресов либо диапазонов IP-адресов, выберите пункт **IP-адрес или диапазон адресов** и выполните одно из действий:
  - для задания одного IP-адреса в списке выберите соответствующий тип адреса и укажите этот IP-адрес;
  - для задания IP-адресов подсети в списке выберите соответствующий тип адреса и укажите адрес и маску этой подсети (по умолчанию — `255.255.255.0/24`);
  - для задания диапазона IP-адресов в списке выберите соответствующий тип адреса и укажите начальный и конечный IP-адреса этого диапазона.

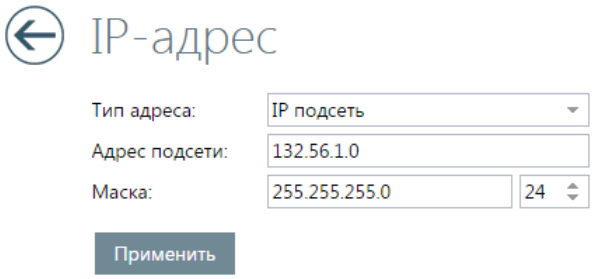


Рисунок 33. Добавление IP-адреса подсети

- Если вы хотите добавить (исключить) DNS-имя, выберите пункт **DNS-имя** и укажите DNS-имя.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп IP-адресов, выберите пункт **Группы IP-адресов** и установите флажки рядом с нужными группами.
- Если вы хотите добавить (исключить) системную группу объектов, выберите соответствующую группу.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров открытой сети, фильтров туннелируемых узлов (см. «Создание и изменение сетевого фильтра» на стр. 76) и правил трансляции адресов (см. «Создание и изменение правила трансляции адресов» на стр. 88).

Группа сетевых интерфейсов

При создании или изменении группы сетевых интерфейсов вы можете добавить или исключить следующие объекты:

- сетевые интерфейсы собственного узла;
- IP-адрес или диапазон IP-адресов сетевых интерфейсов узлов;
- ранее созданную группу сетевых интерфейсов;
- системную группу объектов **Все объекты**.

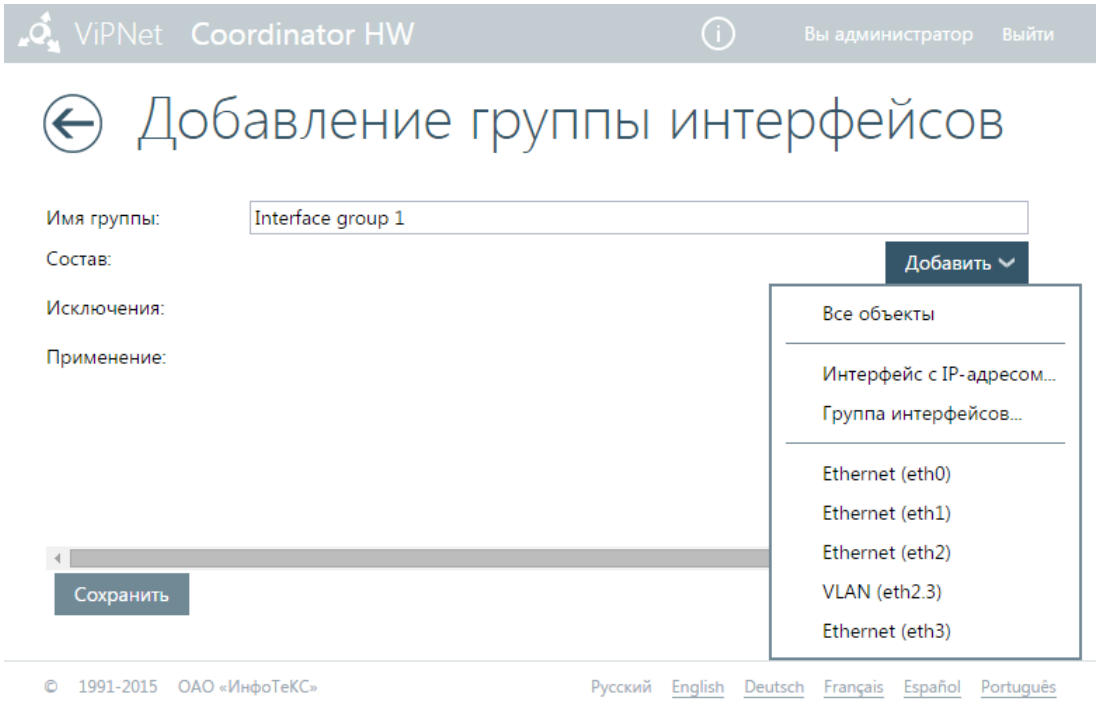


Рисунок 34. Добавление сетевых интерфейсов в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) один или несколько интерфейсов собственного узла, выберите имя этого интерфейса (`Ethernet (eth0)`, `Ethernet (eth1)` и так далее).
- Если вы хотите добавить (исключить) IP-адрес или диапазон IP-адресов интерфейсов, выберите пункт **Интерфейс с IP-адресом** и выполните одно из действий:
  - для задания одного IP-адреса в списке выберите соответствующий тип адреса и укажите этот IP-адрес.
  - для задания IP-адресов подсети в списке выберите соответствующий тип адреса и укажите адрес и маску этой подсети (по умолчанию — `255.255.255.0/24`).
  - для задания диапазона IP-адресов в списке выберите соответствующий тип адреса и укажите начальный и конечный IP-адреса этого диапазона.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп сетевых интерфейсов, выберите пункт **Группа интерфейсов** и установите флажки рядом с нужными группами.
- Если вы хотите добавить (исключить) системную группу объектов **Все объекты**, выберите ее.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать сетевые интерфейсы при создании и изменении фильтров открытой сети и фильтров туннелируемых узлов (см. «Создание и изменение сетевого фильтра» на стр. 76).

Группа протоколов

При создании и изменении группы протоколов вы можете добавить или исключить следующие объекты:

- протокол TCP, UDP, ICMP или другой протокол;
- ранее созданную группу протоколов;
- системную группу **Все объекты**.

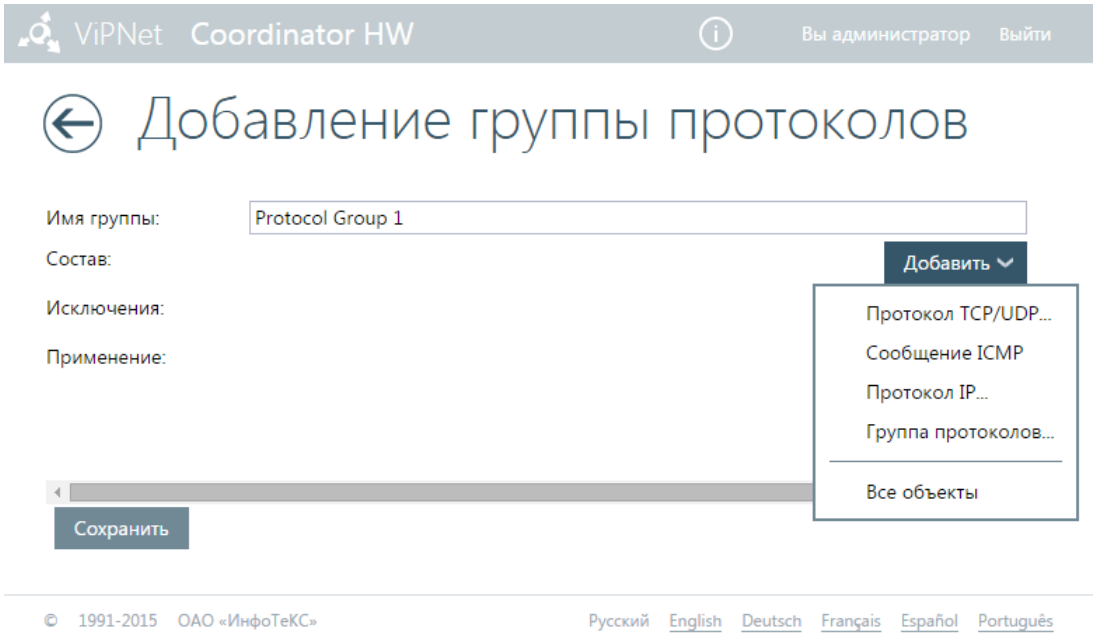


Рисунок 35. Добавление протоколов в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) протокол TCP или UDP, выберите пункт **Протокол TCP/UDP** и установите переключатель **Протоколы** в нужное положение. По умолчанию для протокола выбраны все порты источника и назначения (**Все порты**). Для задания одного или нескольких портов источника или назначения выполните одно из действий:
  - для задания номера одного порта в соответствующем списке выберите пункт **Номер порта**, затем выберите один из стандартных номеров портов в списке или укажите произвольный номер порта в диапазоне от 0 до 65535;
  - для задания диапазона портов в соответствующем списке выберите пункт **Диапазон портов** и укажите начальный и конечный номера портов в диапазоне от 0 до 65535.

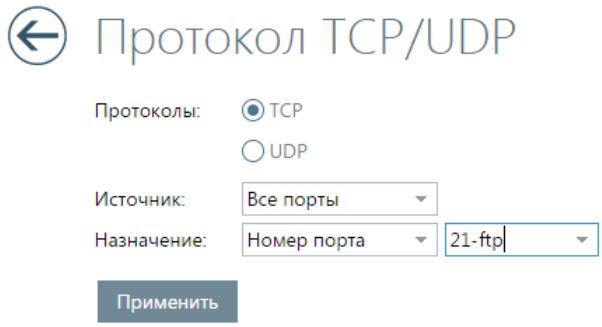


Рисунок 36. Добавление TCP-протокола

- Если вы хотите добавить (исключить) протокол ICMP, выберите пункт **Сообщение ICMP**, затем выберите нужный тип ICMP-сообщений в списке и при необходимости их код.
- Если вы хотите добавить (исключить) другой протокол, выберите пункт **Протокол IP**, затем выберите один из протоколов в списке либо введите его номер.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп проколов, выберите пункт **Группа протоколов** и установите флажки рядом с нужными группами.
- Если вы хотите добавить (исключить) системную группу **Все объекты**, выберите ее.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать протоколы при создании и изменении сетевых фильтров (см. «Создание и изменение сетевого фильтра» на стр. 76) и правил трансляции адресов (см. «Создание и изменение правила трансляции адресов» на стр. 88).

Группа расписаний

При создании или изменении группы расписаний вы можете добавить или исключить следующие объекты:

- временной диапазон;
- ранее созданную группу расписаний;
- системную группу объектов **Все объекты**.

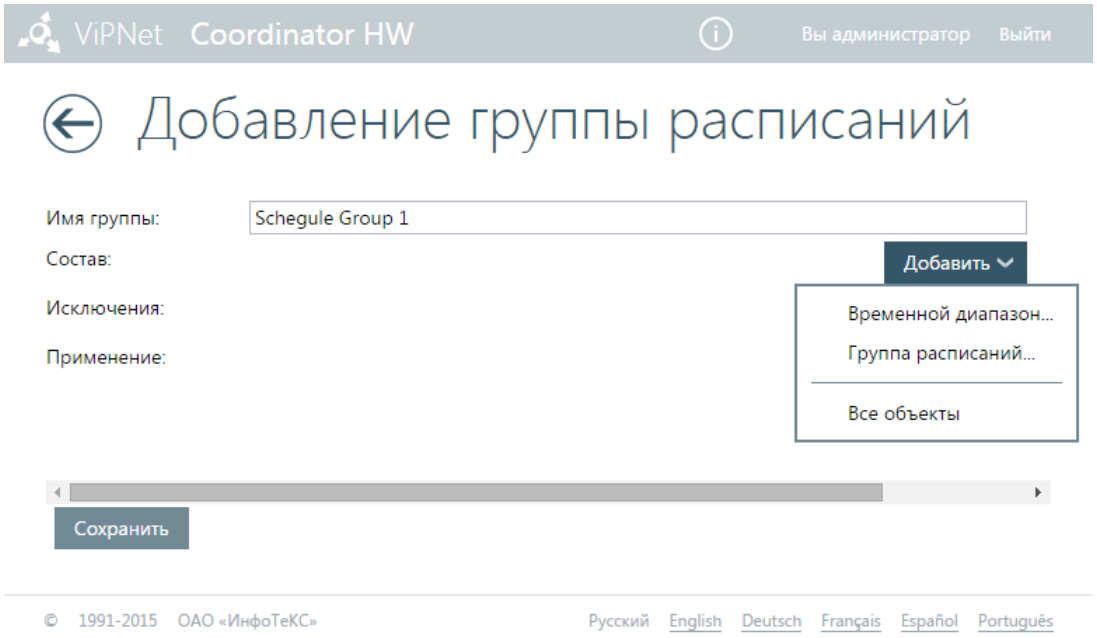


Рисунок 37. Добавление расписания в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите указать интервал времени и периодичность, когда фильтр или правило трансляции будет применяться (не будет применяться), выберите пункт **Временной диапазон** и выполните следующие действия:
  - в разделе **Время выполнения фильтра** укажите интервал времени;
  - в разделе **Период выполнения фильтра** выберите один из вариантов:
    - **Ежедневно —** чтобы фильтр или правило трансляции применялось (не применялось) каждый день. При необходимости установите флажок **в период** и укажите интервал дат, в который фильтр или правило трансляции будет применяться (не будет применяться) ежедневно;
    - **Еженедельно** — чтобы фильтр или правило трансляции применялось (не применялось) в определенные дни недели. Установите флажки рядом с нужными днями недели.

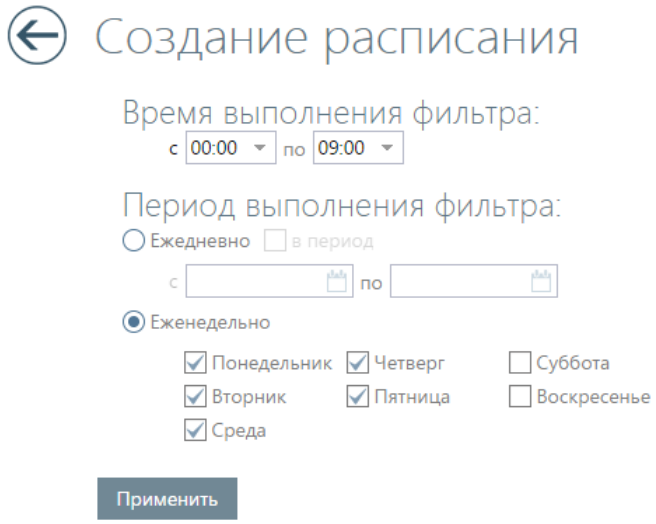


Рисунок 38. Добавление расписания

- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп расписаний, выберите пункт **Группа расписаний** и установите флажки рядом с нужными группами.
- Если вы хотите добавить (исключить) системную группу **Все объекты**, выберите ее.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать расписания при создании и изменении сетевых фильтров (см. «Создание и изменение сетевого фильтра» на стр. 76) и правил трансляции адресов (см. «Создание и изменение правила трансляции адресов» на стр. 88).

Просмотр сетевых фильтров

Чтобы просмотреть сетевые фильтры, заданные на узле ViPNet Coordinator HW, выполните следующие действия:

1 На начальной странице веб-интерфейса щелкните плитку **Межсетевой экран**.

2 На странице **Сетевые фильтры** выберите вкладку сетевых фильтров нужного типа. В результате отобразится список таких фильтров в порядке убывания их приоритета.

Примечание. Вкладка **Фильтры туннелируемых узлов** присутствует только в случае наличия лицензии на туннелирование (см. глоссарий, стр. 160) для хотя бы одного соединения.

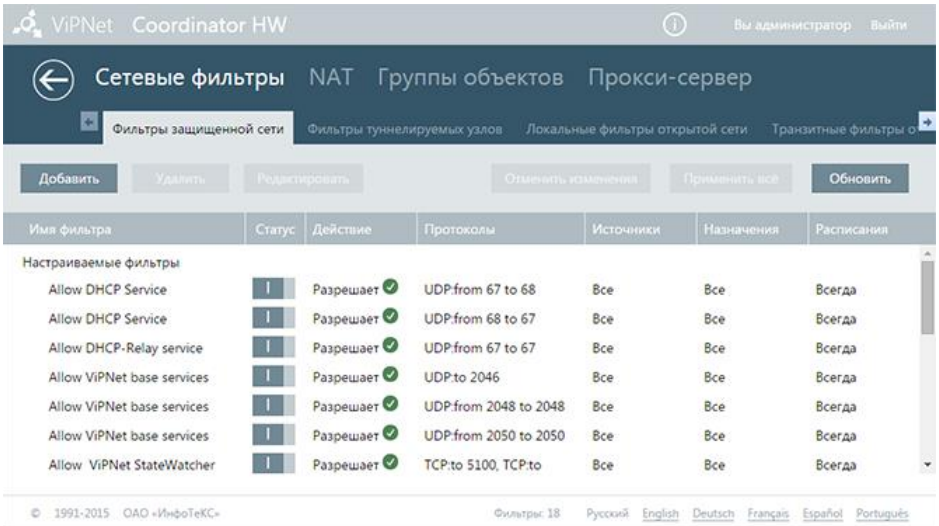


Рисунок 39. Просмотр фильтров защищенной сети

3 Для просмотра подробной информации о фильтре дважды щелкните его в списке.

Создание и изменение сетевого фильтра

Чтобы создать или изменить сетевой фильтр на узле ViPNet Coordinator HW, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. На странице **Межсетевой экран** > **Сетевые фильтры** выберите вкладку сетевых фильтров нужного типа.
3. Выполните одно из действий:
   - Чтобы создать фильтр, на панели инструментов нажмите кнопку **Добавить**.
   - Чтобы изменить фильтр, дважды щелкните его в списке.
4. На открывшейся странице выполните следующие действия:
   - В соответствующем поле укажите имя фильтра.
   - Чтобы фильтр начал действовать после создания, установите флажок **Фильтр включен**.
   - С помощью соответствующего переключателя выберите действие сетевого фильтра: **Блокировать трафик** или **Пропускать трафик**.
   - В разделе **Источники** по умолчанию указаны все отправители IP-пакетов (**Все**). Чтобы выбрать определенных отправителей IP-пакетов, нажмите кнопку **Добавить** и укажите:
     - для фильтров защищенной сети: сетевые узлы ViPNet, группы сетевых узлов ViPNet, системные группы **Мой узел**, **Другие узлы**, **Все координаторы**, **Все клиенты** (см. «Группа сетевых узлов ViPNet» на стр. 66).
     - для фильтров туннелируемых узлов: IP-адреса или диапазоны IP-адресов, DNS-имена, туннелируемые IP-адреса (см. «Группа IP-адресов» на стр. 68), сетевые узлы ViPNet, группы сетевых узлов ViPNet, системные группы **Все координаторы**, **Все клиенты** (см. «Группа сетевых узлов ViPNet» на стр. 66).
     - для локальных фильтров открытой сети: IP-адреса или диапазоны IP-адресов, DNS-имена, группы IP-адресов, системные группы **Мой узел**, **Другие узлы** (см. «Группа IP-адресов» на стр. 68).
     - для транзитных фильтров открытой сети: IP-адреса или диапазоны IP-адресов, DNS-имена, группы IP-адресов (см. «Группа IP-адресов» на стр. 68).

     При необходимости в разделе **Источники** для фильтров туннелируемых узлов и транзитных фильтров открытой сети установите флажок **Сетевой интерфейс** и укажите сетевой интерфейс, с которого будут отправляться IP-пакеты (см. «Группа сетевых интерфейсов» на стр. 69).

- В разделе **Назначения** по умолчанию указаны все получатели IP-пакетов (**Все**). Чтобы выбрать определенных получателей IP-пакетов, нажмите кнопку **Добавить** и укажите:
  - для фильтров защищенной сети: сетевые узлы ViPNet, группы сетевых узлов ViPNet, системные группы **Мой узел**, **Другие узлы**, **Все координаторы**, **Все клиенты**, **Широковещательные адреса** (см. «Группа сетевых узлов ViPNet» на стр. 66).
  - для фильтров туннелируемых узлов: IP-адреса или диапазоны IP-адресов, DNS-имена, туннелируемые IP-адреса (см. «Группа IP-адресов» на стр. 68), сетевые узлы ViPNet, группы сетевых узлов ViPNet, системные группы **Все координаторы**, **Все клиенты** (см. «Группа сетевых узлов ViPNet» на стр. 66).
  - для локальных фильтров открытой сети: IP-адреса или диапазоны IP-адресов, DNS-имена, группы IP-адресов, системные группы **Мой узел**, **Другие узлы**, **Широковещательные адреса**, **Групповые адреса** (см. «Группа IP-адресов» на стр. 68).
  - для транзитных фильтров открытой сети: IP-адреса или диапазоны IP-адресов, DNS-имена, группы IP-адресов (см. «Группа IP-адресов» на стр. 68).

  При необходимости в разделе **Назначения** для фильтров туннелируемых узлов, локальных и транзитных фильтрах открытой сети установите флажок **Сетевой интерфейс** и укажите сетевой интерфейс, на котором будут приниматься IP-пакеты (см. «Группа сетевых интерфейсов» на стр. 69).
- По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам. Чтобы фильтр применялся к IP-пакетам, передаваемым по определенным протоколам, в соответствующем разделе укажите протоколы (см. «Группа протоколов» на стр. 71).
- По умолчанию фильтр применяется постоянно. Чтобы фильтр применялся периодически в определенное время, в соответствующем разделе укажите расписания (см. «Группа расписаний» на стр. 72).

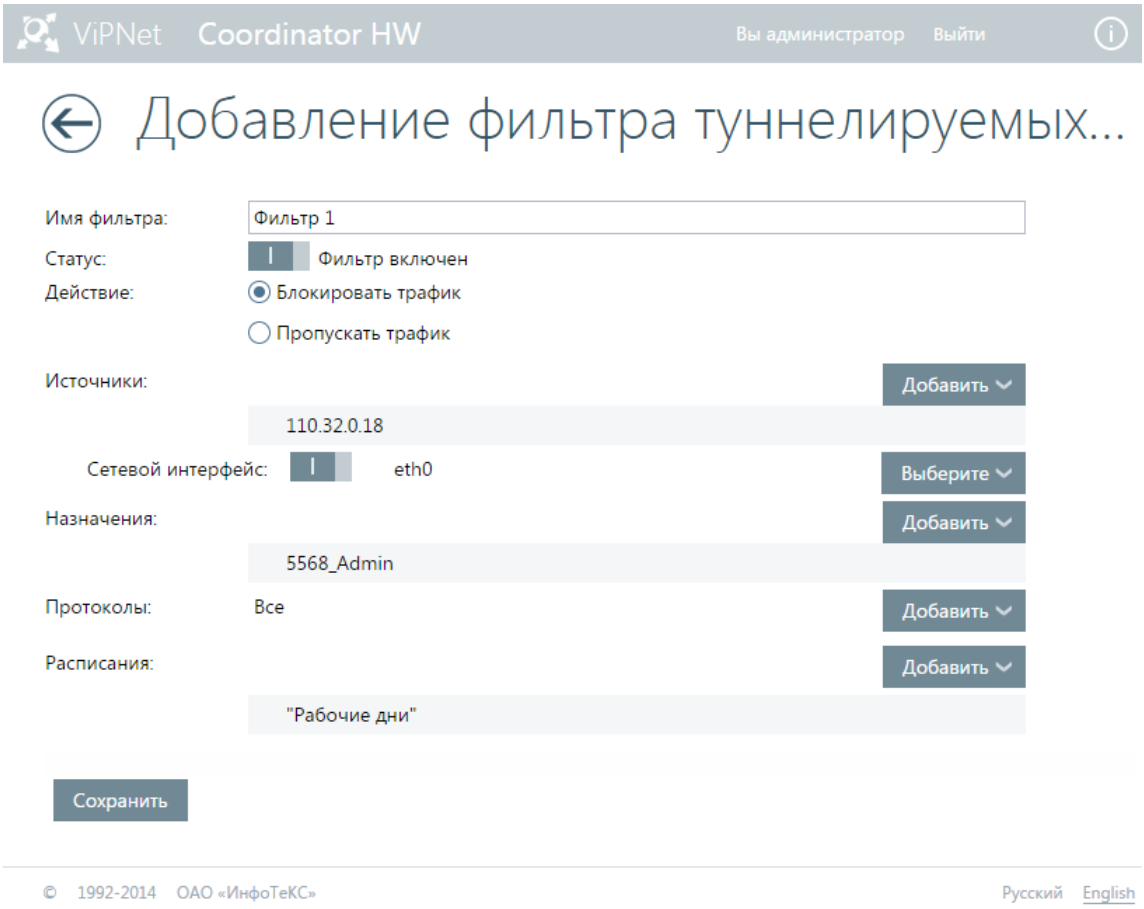


Рисунок 40. Создание сетевого фильтра

- Нажмите кнопку **Сохранить**.

В результате созданный фильтр отобразится в списке на соответствующей вкладке страницы **Сетевые фильтры**.

5 Чтобы изменить приоритет фильтра, перетащите его на нужную строку списка.

6 Чтобы фильтр вступил в действие, нажмите кнопку **Применить все**.

Пример использования групп объектов и сетевых фильтров

Рассмотрим пример применения групп объектов и сетевых фильтров. Допустим, в компании координатор ViPNet Coordinator HW выполняет функции защищенного почтового сервера, и требуется организовать обмен электронными письмами с удаленными пользователями, использующими внешние почтовые серверы, и доступ таких пользователей к электронным письмам на защищенном почтовом сервере.

Обмен электронными письмами с внешними почтовыми серверами осуществляется по протоколам SMTP, POP3 и IMAP. Поэтому для организации такого обмена на защищенном почтовом сервере ViPNet Coordinator HW необходимо создать сетевой фильтр, разрешающий прием и передачу IP-пакетов по 25-му порту протокола TCP (для протокола SMTP), а также по 110-му и 143-му портам (для протоколов POP3 и IMAP соответственно).

Примечание. В примере указаны номера портов для протоколов SMTP, POP3 и IMAP используемые по умолчанию. В вашей сети номера портов для этих протоколов зависят от настроек почтового сервера.

Вы можете создать группу протоколов, в которую будут входить все указанные выше протоколы, и затем использовать ее при создании сетевого фильтра. При необходимости вы можете также использовать данную группу при создании других фильтров на почтовом сервере.

Чтобы создать группу почтовых протоколов, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. На странице **Межсетевой экран** > **Группы объектов** выберите вкладку **Протоколы** и на панели инструментов нажмите кнопку **Добавить**.
3. На странице **Добавление группы протоколов** выполните следующие действия:
   - Укажите имя группы.
   - В разделе **Состав** добавьте протокол SMTP. Для этого нажмите кнопку **Добавить**, выберите пункт **Протокол TCP/UDP** (см. Рисунок 34 на стр. 71) и в открывшемся окне выберите:
     - в разделе **Протокол** — пункт **TCP**;
     - в разделе **Источники** — пункт **Все порты**;
     - в разделе **Назначение** — пункт **Номер порта**, и укажите номер **25-smtp**.

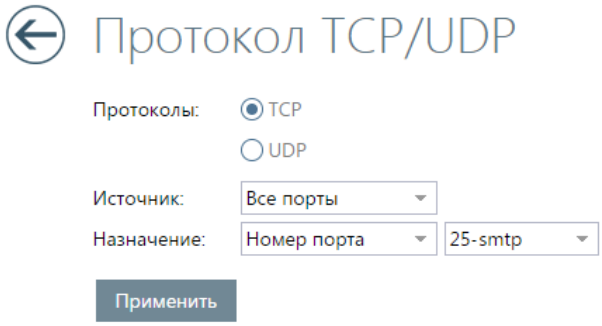


Рисунок 41. Добавление протокола SMTP

Затем нажмите кнопку **Применить**.

- Аналогичным образом в разделе **Состав** добавьте протоколы POP3 (порт — 110) и IMAP (порт — 143).
- Нажмите кнопку **Сохранить**. В результате созданная группа протоколов появится в списке.

4 Чтобы изменения вступили в силу, на странице **Группы объектов** нажмите кнопку **Применить все**.

Чтобы создать сетевой фильтр для обмена электронными письмами с внешними почтовыми серверами с любыми IP-адресами, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 На странице **Межсетевой экран** > **Сетевые фильтры** выберите вкладку **Локальные фильтры открытой сети** и на панели инструментов нажмите кнопку **Добавить**.

3 На странице **Добавление локального фильтра открытой сети** выполните следующие действия:

- Укажите имя сетевого фильтра.
- Установите флажок **Фильтр включен**.
- Переключатель **Действие** установите в положение **Пропускать трафик**.
- В разделе **Протоколы** нажмите кнопку **Добавить** и выберите пункт **Группа протоколов** (см. Рисунок 34 на стр. 71). В открывшемся окне выберите ранее созданную группу почтовых протоколов и нажмите кнопку **Применить**.
- Нажмите кнопку **Сохранить**.

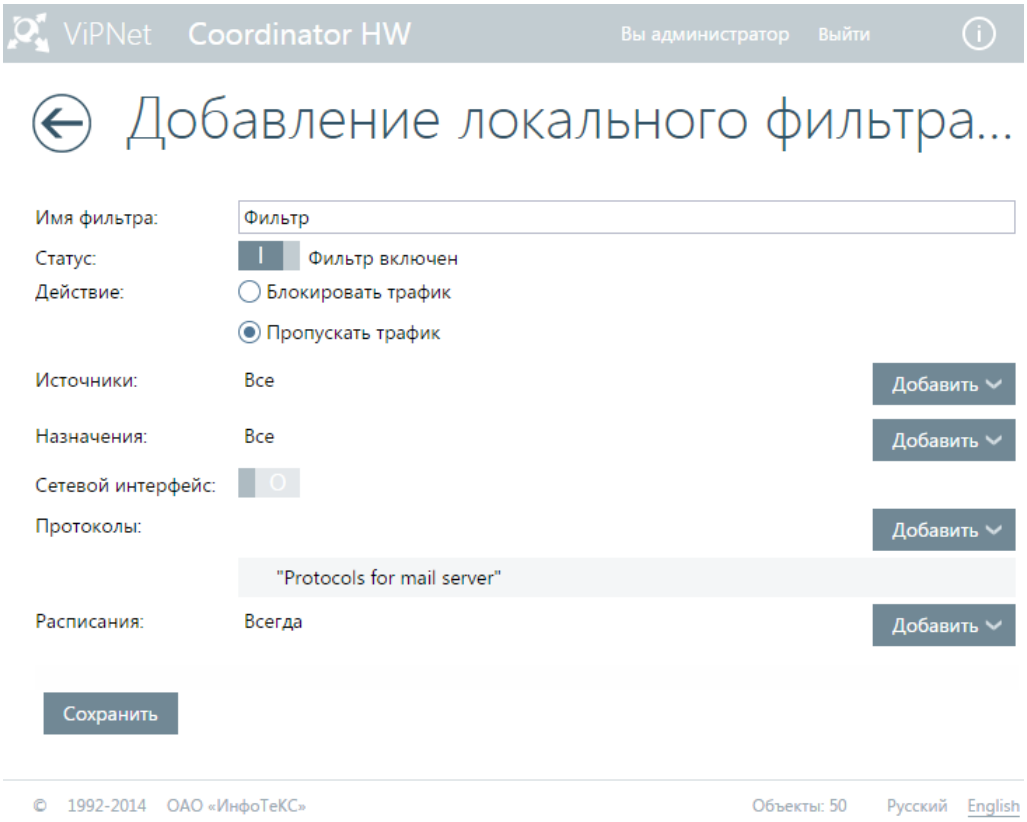


Рисунок 42. Добавление фильтра для почтового сервера

В результате созданный сетевой фильтр появится в соответствующем списке, и на защищенном почтовом сервере будет разрешен обмен электронными письмами с удаленными пользователями и доступ таких пользователей к электронным письмам на защищенном почтовом сервере.

5

Настройка правил трансляции адресов

Трансляция адресов в технологии ViPNet 83

Просмотр правил трансляции адресов 87

Создание и изменение правила трансляции адресов 88

Трансляция адресов в технологии ViPNet

Трансляция сетевых адресов (NAT) — это механизм преобразования IP-адресов одной сети в IP-адреса другой сети. Технология трансляции адресов описана в RFC 2663 (http://tools.ietf.org/html/rfc2663).

ViPNet Coordinator HW может выполнять трансляцию адресов следующих типов:

- Трансляция адреса источника (на стр. 85), называемая также маскарадингом (masquerading) или динамической трансляцией.

  В этом случае при прохождении через координатор пакетов от отправителей с частными адресами в них заменяется адрес отправителя на внешний (реальный) адрес координатора. При получении ответных пакетов в них подменяется адрес получателя обратно на частный адрес, и в таком виде пакет доставляется в частную сеть.

  Используется для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов (см. глоссарий, стр. 159). В результате локальные сети, использующие частные адреса (см. глоссарий, стр. 160), получают доступ к ресурсам Интернета.

- Трансляция адреса назначения (на стр. 84), называемая также форвардингом портов (port forwarding) или статической трансляцией.

  В этом случае пакеты, приходящие из Интернета на определенный порт внешнего адреса координатора, перенаправляются на указанный адрес внутренней сети путем подмены в них адреса получателя, а у ответных пакетов от компьютера внутренней сети подменяется адрес отправителя.

  Используется для организации доступа к ресурсам локальной сети из Интернета. В результате локальные сети, использующие частные адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

- Одновременная трансляция адресов источника и назначения. Может использоваться в сложных схемах маршрутизации трафика.

Трансляция сетевых адресов выполняется координатором, только если настроены соответствующие правила. Координатор должен иметь как минимум два сетевых интерфейса (см. глоссарий, стр. 159):

- внешний интерфейс — имеет публичный IP-адрес и обеспечивает доступ в Интернет;
- внутренний интерфейс — имеет частный IP-адрес.

Внимание! Правила трансляции, описанные в данном разделе, относятся только к открытому трафику. Для защищенного трафика действуют автоматические механизмы трансляции адресов, параметры которых не могут быть изменены.

Трансляция адреса назначения

Трансляция адреса узла назначения предназначена для организации доступа из Интернета к серверам локальной сети, не имеющим публичного IP-адреса. Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных узлов публичный IP-адрес координатора. В соответствии с правилом, в заголовках IP-пакетов публичный IP-адрес (или IP-адрес и порт) назначения заменяется частным адресом локальной сети. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.

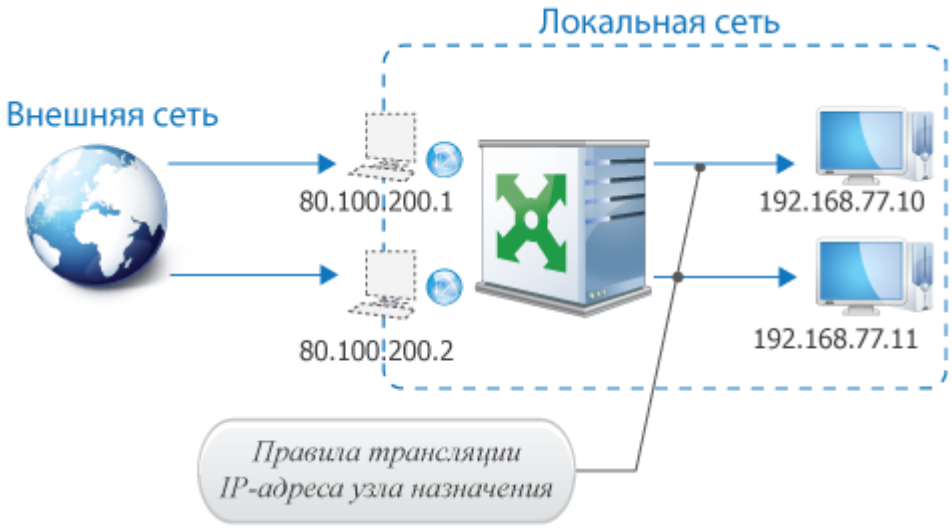


Рисунок 43. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

Если для внешнего IP-адреса координатора задано правило трансляции адреса назначения, то при обращении к этому адресу из Интернета будут выполняться следующие преобразования:

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) локальным адресом в соответствии с описанным правилом. Затем пакет передается через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.
- При прохождении ответных пакетов (в рамках уже созданной сессии) координатор производит обратную замену IP-адресов. Адрес отправителя (IP-адрес локального узла) подменяется публичным IP-адресом внешнего сетевого интерфейса координатора. Затем ответный пакет отправляется по назначению (узлу в Интернете).

  Таким образом, при передаче в Интернете пакет выглядит так, будто отправитель и получатель этого пакета имеют публичные IP-адреса.

Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний узел. Чтобы локальный узел мог также иметь доступ в Интернет (двусторонний NAT), необходимо в дополнение к правилу трансляции адреса узла назначения задать также правило трансляции адреса источника (см. «Трансляция адреса источника» на стр. 85).

Трансляция адреса источника

Трансляция адреса источника предназначена для организации доступа локальных компьютеров в Интернет. Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных узлов публичный IP-адрес координатора. В соответствии с правилом, в заголовках IP-пакетов частные IP-адреса источника заменяются на публичный IP-адрес. Таким образом, узлы локальной сети могут устанавливать соединения с узлами в Интернете от имени публичного IP-адреса координатора.

Рисунок 44. Организация доступа в Интернет при помощи правила трансляции IP-адреса источника

Если на координаторе настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через координатор из локальной сети в Интернет (или другие глобальные сети), будут преобразованы следующим образом:

- В момент передачи IP-пакета из локальной сети в Интернет координатор преобразует адрес и (или) порт отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. В процессе преобразования частный адрес отправителя пакета заменяется на публичный адрес внешнего сетевого интерфейса координатора, обеспечивающего доступ в глобальную сеть. При дальнейшей передаче в Интернете пакет имеет публичный IP-адрес отправителя. Номера портов отправителя (для протоколов TCP и UDP) и запоминаемые параметры (для протокола ICMP) пакетов имеют уникальные значения для всех исходящих IP-соединений внешнего сетевого интерфейса координатора. После преобразования пакет отправляется адресату в Интернете.
- При прохождении ответных пакетов координатор производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета координатор заменяет в нем адрес получателя на частный адрес узла локальной сети, которому адресован ответный пакет. Преобразование происходит на основании уникальных номеров портов, присвоенных исходящим пакетам (для протоколов TCP и UDP), и запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также

преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.

Примечание. Для всех протоколов, кроме TCP, UDP и ICMP, преобразуются только IP-адреса. Для протоколов с частичным преобразованием трансляция IP-адреса источника не будет работать, если несколько узлов локальной сети одновременно инициируют соединение с одним и тем же IP-адресом публичной сети.

Просмотр правил трансляции адресов

Чтобы просмотреть правила трансляции адресов (см. глоссарий, стр. 160), заданные на узле ViPNet Coordinator HW, выполните следующие действия:

1 На начальной странице веб-интерфейса щелкните плитку **Межсетевой экран**.

2 Перейдите на страницу **NAT**. В результате отобразится список правил трансляции адресов в порядке убывания приоритета.

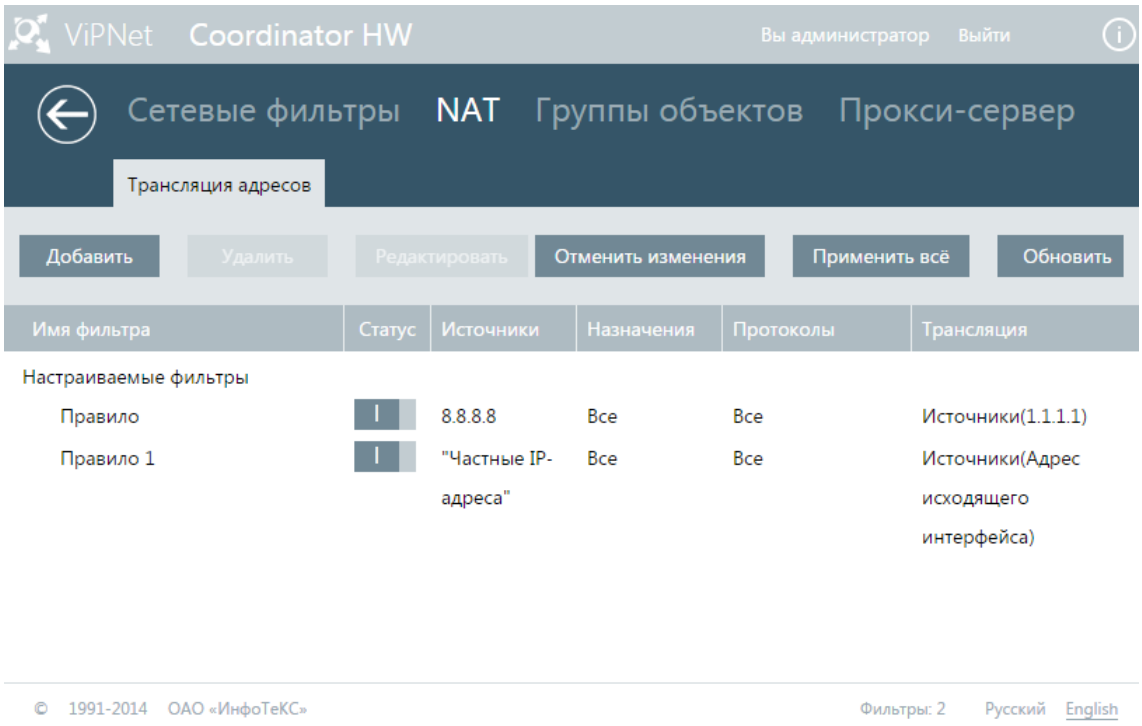


Рисунок 45. Просмотр правил трансляции IP-адресов

3 Для просмотра подробной информации о правиле трансляции дважды щелкните его в списке.

Создание и изменение правила трансляции адресов

Чтобы создать или изменить правило трансляции адресов, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Межсетевой экран** > **NAT**.
3. Выполните одно из действий:
   - Чтобы создать правило трансляции, на панели инструментов нажмите кнопку **Добавить**.
   - Чтобы изменить правило трансляции, дважды щелкните его в списке или нажмите кнопку **Редактировать**.
4. На открывшейся странице выполните следующие действия:
   - В соответствующем поле укажите имя правила трансляции.
   - Чтобы правило трансляции начало действовать после создания, установите флажок **Правило включено**.
   - Если требуется трансляция адреса источника для исходящих IP-пакетов, в разделе **Трансляция источника** установите флажок **Заменять адрес источника на** и выполните одно из действий:
     - чтобы IP-адрес отправителя заменялся на адрес внешнего сетевого интерфейса ViPNet Coordinator HW, установите переключатель в положение **адрес исходящего интерфейса (определяется автоматически)**;
     - чтобы указать другой IP-адрес для замены IP-адреса отправителя, установите переключатель в положение **другой IP-адрес** и укажите нужный IP-адрес.
   - Если требуется трансляция адреса назначения для входящих IP-пакетов, в разделе **Трансляция назначения** установите флажок **Заменять адрес назначения на** и при необходимости флажок **Заменять порт назначения на** и укажите IP-адрес и порт, которые будут иметь IP-пакеты, переданные ViPNet Coordinator HW в локальную сеть.
   - В разделе **Источники** по умолчанию указаны все отправители IP-пакетов (**Все**). Чтобы выбрать определенных получателей IP-пакетов, нажмите кнопку **Добавить** и укажите IP-адреса, диапазоны IP-адресов или группы IP-адресов (см. «Группа IP-адресов» на стр. 68).
   - В разделе **Назначения** по умолчанию указаны все получатели IP-пакетов (**Все**). Чтобы выбрать определенных получателей IP-пакетов, нажмите кнопку **Добавить** и укажите IP-адреса, диапазоны IP-адресов или группы IP-адресов (см. «Группа IP-адресов» на стр. 68).
   - По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам. Чтобы фильтр применялся к IP-пакетам, передаваемым по определенным протоколам, в соответствующем разделе укажите протоколы (см. «Группа протоколов» на стр. 71).

- Нажмите кнопку **Сохранить**. В результате созданное правило трансляции отобразится в списке на странице **Межсетевой экран** > **NAT**.

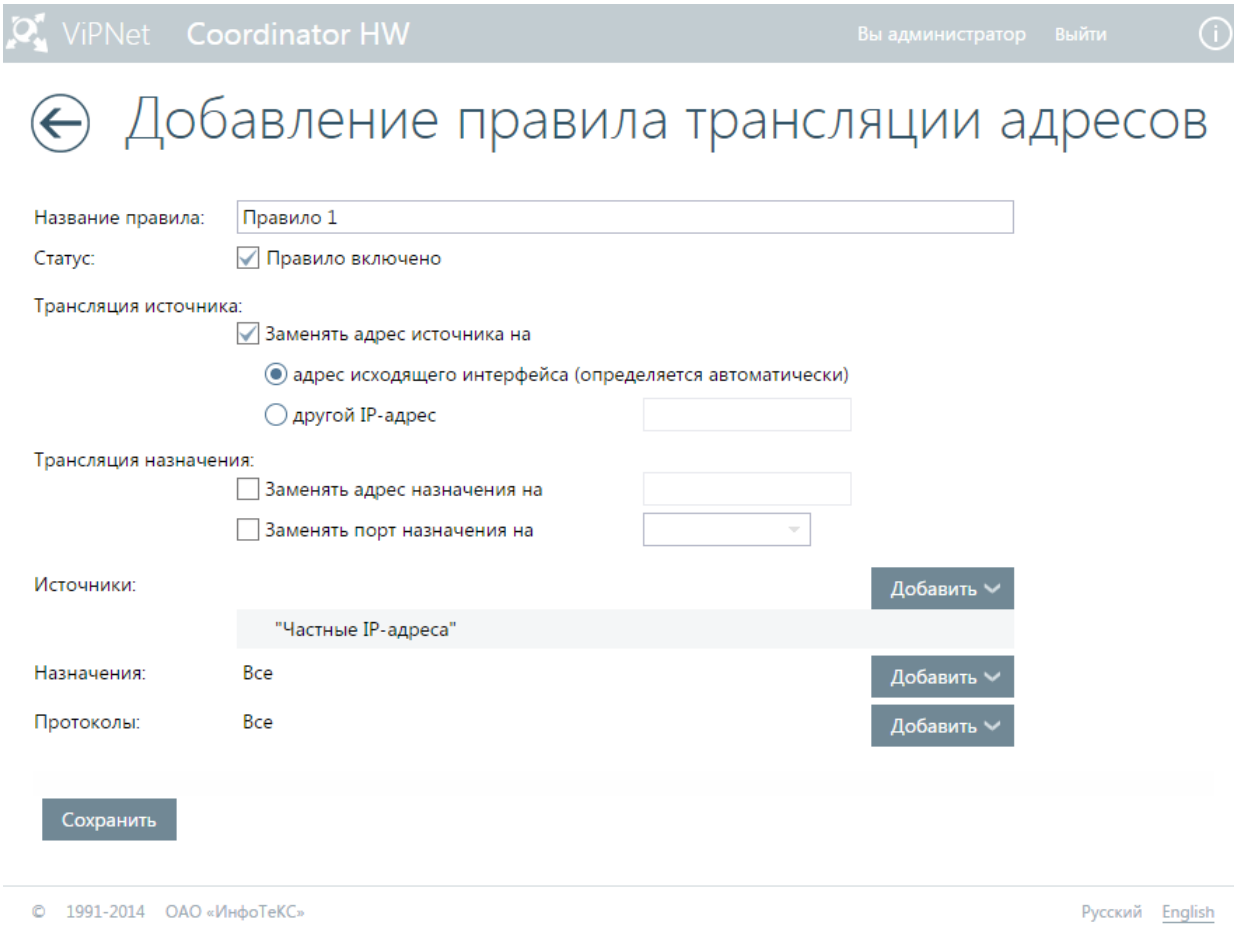


Рисунок 46. Создание правила трансляции адресов

5 Чтобы изменить приоритет правила трансляции, перетащите его на нужную строку списка.

6 Чтобы правило вступило в действие, нажмите кнопку **Применить все**.

6

Настройка сетевых служб

Настройка параметров DHCP-сервера 91

Настройка DHCP-relay 94

Настройка параметров DNS-сервера 96

Настройка параметров NTP-сервера 98

Настройка параметров прокси-сервера 101

Настройка параметров точки доступа к сети Wi-Fi 109

Настройка параметров DHCP-сервера

В состав ПО ViPNet Coordinator HW входит DHCP-сервер, который может использоваться для динамического назначения IP-адресов сетевым узлам (DHCP-клиентам). Одновременно с выделением IP-адресов DHCP-сервер может назначать дополнительные параметры настройки клиентов, например, IP-адреса шлюза по умолчанию и WINS-серверов.

В качестве адресов DNS-сервера и NTP-сервера DHCP-сервер всегда предоставляет клиентам адрес интерфейса, с которым он работает. Клиенты, получившие от ViPNet Coordinator HW вместе с IP-адресом адреса DNS- и NTP-серверов, будут осуществлять запросы на разрешение имен и синхронизацию времени через соответствующие серверы, запущенные на ViPNet Coordinator HW. Если на ViPNet Coordinator HW эти серверы не запущены, то клиенты не смогут работать с DNS-именами и синхронизировать свое время.

Внимание! Использование ViPNet Coordinator HW в качестве DHCP-сервера возможно только при работе в одиночном режиме. Работа DHCP-сервера в режиме кластера горячего резервирования не поддерживается.

Чтобы запустить DHCP-сервер на одном из сетевых интерфейсов Ethernet, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Прикладные сервисы** > **DHCP**.

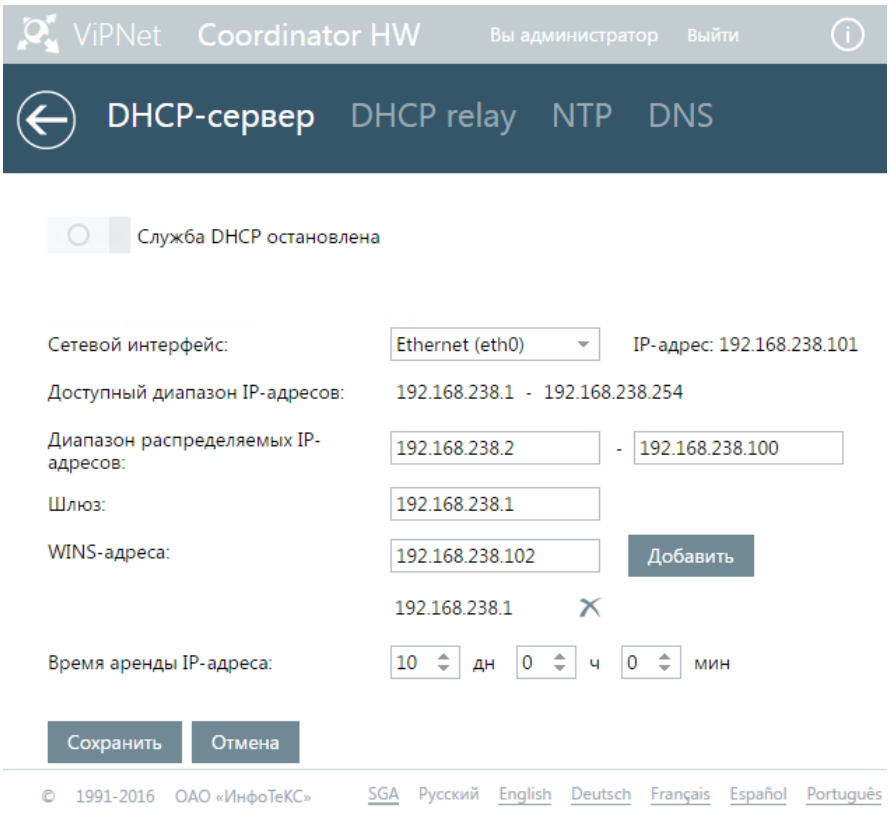


Рисунок 47. Настройка параметров DHCP-сервера

3 В списке **Сетевой интерфейс** выберите сетевой интерфейс, на котором должен быть запущен DHCP-сервер.

Примечание. Сетевой интерфейс для DHCP-сервера не должен быть дополнительным, а также должен быть включен и иметь статический IP-адрес.

---

4 В полях **Диапазон распределяемых IP-адресов** задайте интервал IP-адресов, которые должны присваиваться клиентам DHCP. Диапазон IP-адресов должен принадлежать сети интерфейса и не должен включать адрес самого интерфейса.

Примечание. DHCP-сервер может выделять клиентам любые диапазоны IP-адресов. Однако в локальной сети, маршрутизируемой в сеть Интернет, рекомендуется выделять IP-адреса только из диапазонов, установленных стандартом для частных сетей: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`.

---

5 В поле **Шлюз** введите IP-адрес шлюза по умолчанию, который должны получать клиенты от DHCP-сервера. IP-адрес шлюза должен принадлежать сети интерфейса.

6 При необходимости добавьте адрес WINS-сервера (или нескольких серверов), для этого укажите адрес в поле **WINS-адреса** и нажмите кнопку **Добавить**.

7 Задайте время аренды IP-адреса в соответствующих полях.

8 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

9 Чтобы запустить DHCP-сервер или завершить его работу, щелкните переключатель в верхней части страницы. Состояние DHCP-сервера отображается напротив переключателя.

Настройка DHCP-relay

В состав ПО ViPNet Coordinator HW входит служба DHCP-relay, которая позволяет использовать ViPNet Coordinator HW в качестве агента DHCP-relay. Такая необходимость может возникнуть в случае, если сетевые узлы должны получать IP-адреса от удаленного DHCP-сервера, к которому они не могут обращаться напрямую. Агент DHCP-relay обеспечивает взаимодействие таких сетевых узлов с DHCP-сервером: он принимает от узлов DHCP-запросы и передает их DHCP-серверу. Ответы, полученные от DHCP-сервера, агент перенаправляет сетевым узлам.

С помощью агента DHCP-relay также можно организовать выделение IP-адресов узлам разветвленной сети, включающей несколько подсетей. В этом случае не нужно устанавливать в каждой подсети свой DHCP-сервер, а достаточно использовать только один DHCP-сервер.

ViPNet Coordinator HW может обслуживать в качестве агента DHCP-relay несколько локальных сетей. Это могут быть как сети, подключенные к разным физическим интерфейсам ViPNet Coordinator HW, так и виртуальные локальные сети, подключенные к одному физическому интерфейсу.

Чтобы включить службу DHCP-relay, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Прикладные сервисы** > **DHCP relay.**

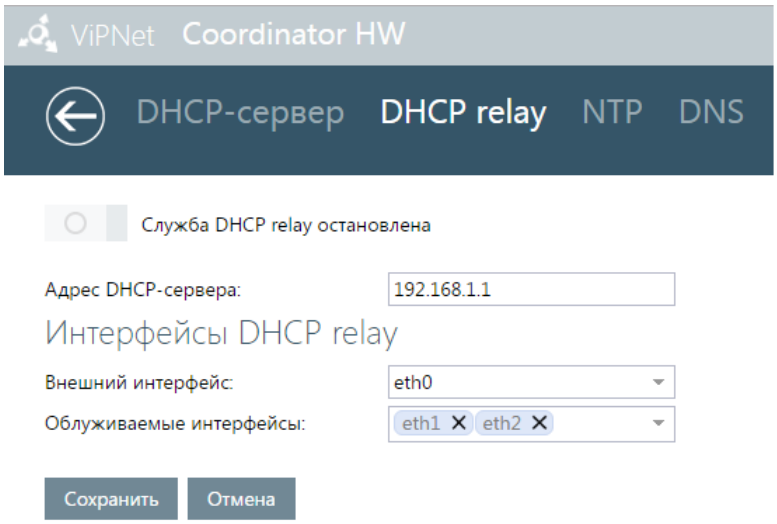


Рисунок 48. Настройка параметров DHCP-ретранслятора

3 В поле **Адрес DHCP-сервера** задайте адрес DHCP-сервера вашей сети.

4 В списке **Внешний интерфейс** выберите сетевой интерфейс, который должен получать данные от DHCP-сервера.

5 В списке **Обслуживаемые интерфейсы** выберите сетевые интерфейсы, с помощью которых должны распределяться IP-адреса DHCP-клиентам.

6 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

Настройка параметров DNS-сервера

В состав ПО ViPNet Coordinator HW входит DNS-сервер (далее — локальный DNS-сервер), который может использоваться для разрешения (преобразования) символьных имен в IP-адреса в ответ на собственные запросы и на запросы других сетевых узлов (DNS-клиентов).

Локальный DNS-сервер перенаправляет поступающие к нему DNS-запросы на вышестоящие DNS-серверы и передает полученные ответы DNS-клиентам. По умолчанию локальный DNS-сервер настроен таким образом, что он может выполнять разрешение имен с использованием корневых DNS-серверов. Для этого требуется наличие подключения к Интернету. При отсутствии доступа к Интернету для разрешения имен следует использовать другие доступные (не корневые) DNS-серверы. В этом случае необходимо добавить адреса доступных серверов в настройки локального DNS-сервера.

Все DNS-серверы, отличные от корневых, добавляются в качестве DNS-серверов пересылки (forwarder). Если адрес доступного DNS-сервера известен заранее, то его можно задать в процессе первоначальной установки справочников и ключей (подробнее см. в документе «ViPNet Coordinator HW. Подготовка к работе»).

Внимание! В ситуации, когда DNS-серверы пересылки, заданные в настройках локального DNS-сервера, недоступны, но при этом доступны корневые DNS-серверы, DNS-клиенты будут получать ответы на свои запросы с задержкой.

Список DNS-серверов пересылки можно сформировать вручную. Также можно получить адреса DNS-серверов от внешнего DHCP-сервера, если на одном из интерфейсов ViPNet Coordinator HW установлен режим DHCP (см. «Настройка параметров DHCP-сервера» на стр. 91). В полученный от DHCP-сервера список можно добавлять адреса вручную. После перезагрузки ViPNet Coordinator HW или установки на интерфейсе статического IP-адреса список, полученный от внешнего DHCP-сервера, удаляется из настроек локального DNS-сервера. В этом случае для разрешения имен будут использоваться корневые DNS-серверы.

Примечание. Если режим DHCP установлен на нескольких интерфейсах ViPNet Coordinator HW, то результат обработки собственных DNS-запросов и запросов DNS-клиентов не определен, так как неизвестно, какой интерфейс будет включен первым и какой список DNS-серверов пересылки получит ViPNet Coordinator HW.

Чтобы настроить параметры DNS-сервера, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Прикладные сервисы** > **DNS**.

На странице **DNS** содержится список DNS-серверов, который может включать в себя как IP-адреса, заданные пользователем, так и IP-адреса, полученные автоматически от DHCP-сервера. Тип каждого DNS-сервера показан в столбце **Тип**.

Напротив переключателя вверху страницы отображается состояние DNS-серверов.

Изменить или удалить IP-адреса серверов, полученные автоматически, невозможно.

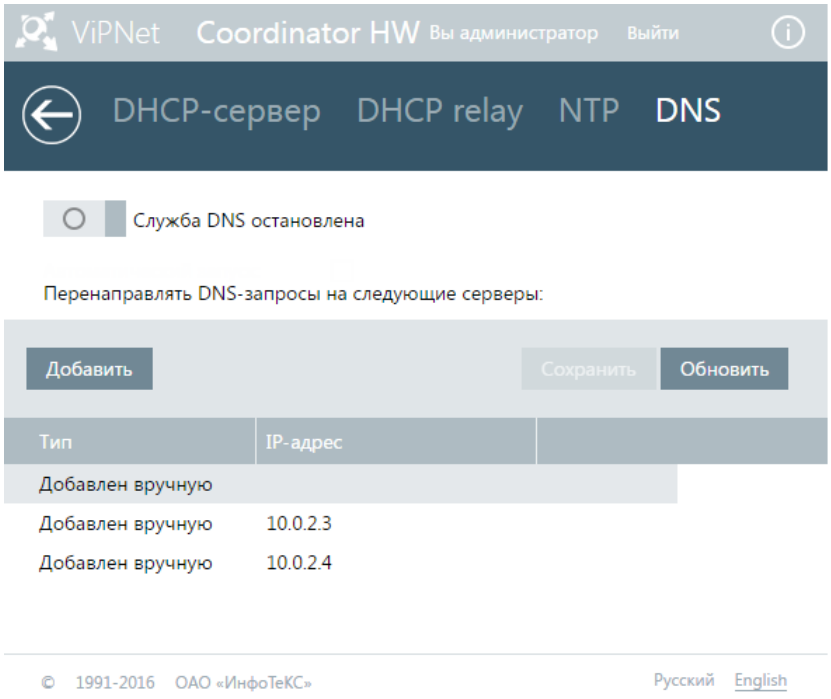


Рисунок 49. Настройка параметров DNS-сервера

3 Чтобы добавить IP-адрес нового DNS-сервера в список, нажмите кнопку **Добавить** и задайте IP-адрес DNS-сервера.

Для изменения IP-адреса DNS-сервера дважды щелкните строку с ним и внесите необходимые изменения. Для удаления IP-адреса DNS-сервера из списка в строке рядом с ним щелкните значок , и в появившемся сообщении нажмите кнопку **ОК**.

4 Чтобы запустить все заданные в списке DNS-серверы или завершить их работу, щелкните переключатель в верхней части страницы.

5 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

Настройка параметров NTP-сервера

В состав ПО ViPNet Coordinator HW входит NTP-сервер (далее — локальный NTP-сервер), который может использоваться для синхронизации времени на самом ViPNet Coordinator HW и на других сетевых узлах (NTP-клиентах).

По умолчанию локальный NTP-сервер настроен таким образом, что при наличии подключения к Интернету он может осуществлять синхронизацию времени с использованием публичных NTP-серверов из кластера `pool.ntp.org`. Этот кластер серверов можно дополнить другими NTP-серверами (публичными или корпоративными).

Внимание! Для синхронизации времени рекомендуется использоваться только доверенные NTP-серверы из защищенной сети.

Такая необходимость может возникнуть в случае отсутствия доступа к Интернету или при наличии более близкого и менее нагруженного NTP-сервера (например, корпоративного). Если адрес дополнительного NTP-сервера известен заранее, то его можно задать в процессе первоначальной установки справочников и ключей (подробнее см. в документе «ViPNet Coordinator HW. Подготовка к работе»).

Примечание. Если в качестве дополнительного NTP-сервера используется защищенный узел, видимый по реальному адресу, то для успешной синхронизации времени с таким сервером при загрузке системы рекомендуется с помощью командного интерпретатора в файле `iplir.conf` в секции `[id]` для этого защищенного узла установить параметр `visibility` в значение `real`.

Описание команды, с помощью которого вы можете редактировать файл `iplir.conf` см. в документе «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору».

Описание секции и параметра см. в документе «ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам», в разделе «Файл iplir.conf».

Список дополнительных NTP-серверов можно сформировать вручную или получить их адреса от внешнего DHCP-сервера. При этом в полученный от DHCP-сервера список можно добавлять адреса вручную. После перезагрузки ViPNet Coordinator HW или установки на интерфейсе статического IP-адреса список, полученный от внешнего DHCP-сервера, удаляется из настроек локального NTP-сервера.

Примечание. Если режим DHCP установлен на нескольких интерфейсах ViPNet Coordinator HW, то результат синхронизации времени на самом ViPNet Coordinator HW и на NTP-клиентах не определен, так как неизвестно, какой интерфейс будет включен первым и какой список дополнительных NTP-серверов получит ViPNet Coordinator HW.

Чтобы настроить параметры NTP-сервера, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Прикладные сервисы** > **NTP**.

На странице **NTP** содержится список NTP-серверов, который может включать в себя как серверы, заданные пользователем, так и серверы, полученные автоматически от DHCP-сервера. Тип каждого NTP-сервера показан в столбце **Тип**. Изменить или удалить серверы, полученные автоматически, невозможно.

Примечание. Сервер `pool.ntp.org`, использующийся по умолчанию, не отображается в списке.

Напротив переключателя вверху страницы отображается состояние NTP-серверов.

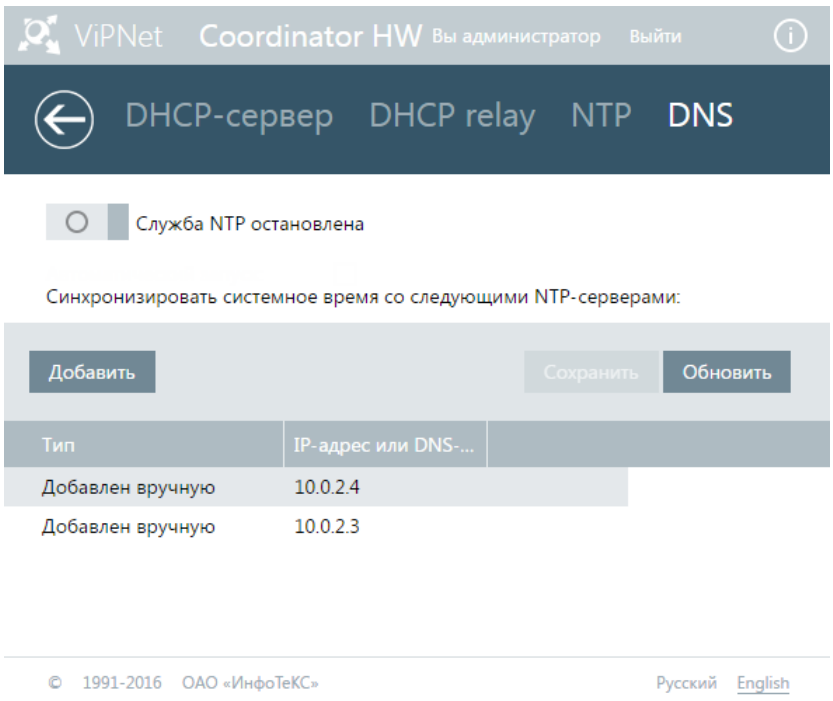


Рисунок 50. Настройка параметров NTP-сервера

3 Чтобы добавить IP-адрес нового NTP-сервера в список, нажмите кнопку **Добавить** и задайте IP-адрес или DNS-имя NTP-сервера.

Для изменения IP-адреса или DNS-имени NTP-сервера дважды щелкните строку с ним и внесите необходимые изменения. Для удаления IP-адреса или DNS-имени NTP-сервера из

списка в строке рядом с ним щелкните значок  , и в появившемся сообщении нажмите кнопку **OK**.

4 Чтобы запустить все заданные в списке NTP-серверы или завершить их работу, щелкните переключатель в верхней части страницы.

Внимание! NTP-серверы, указанные по DNS-имени, будут доступны, только если запущен DNS-сервер (см. «Настройка параметров DNS-сервера» на стр. 96).

Если ViPNet Coordinator HW не удалось подключиться ни к одному из NTP-серверов, локальный NTP-сервер не запускается. Информация о попытках подключения к NTP-серверам записывается в журнал событий.

1 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

Настройка параметров прокси-сервера

Прокси-сервер, входящий в состав программного обеспечения ViPNet Coordinator HW, обладает следующими возможностями:

- Кэширование данных для ускорения доступа пользователей к часто запрашиваемым ресурсам.
- Работа в «прозрачном» режиме, для которого не требуется дополнительная настройка приложений на рабочих местах пользователей.
- Фильтрация содержимого трафика.
- Проверка трафика с помощью антивируса.

Схема работы прокси-сервера при обработке запроса пользователя представлена на следующем рисунке.

Рисунок 51: Схема работы прокси-сервера ViPNet Coordinator HW

При обращении пользователя к какому-либо интернет-ресурсу запрос обрабатывается следующим образом:

1 Запрос от клиента прокси-сервера поступает на ViPNet Coordinator HW:
   - Запрос обрабатывается сетевыми фильтрами:
     - если для запроса сработал запрещающий сетевой фильтр, то передача IP-пакетов блокируется, в журнал регистрации IP-пакетов добавляется запись об этом событии (см. «Типы событий в журнале регистрации IP-пакетов» на стр. 150);

- если запрос не попал ни под один из запрещающих сетевых фильтров, он передается на прокси-сервер.

  - Если на прокси-сервере включена функция фильтрации содержимого трафика, то запрос обрабатывается ее правилами:
    - если ни одно правило не сработало для данного типа содержимого HTTP-трафика, то применяется правило по умолчанию (блокирующее или разрешающее);
    - если для данного типа содержимого трафика сработало запрещающее правило, то передача данных этого типа содержимого блокируется.
  - Если на прокси-сервере включена антивирусная проверка трафика, данные проверяются на наличие вирусов. Если пользователь попытается отправить файл, в котором был обнаружен вирус, он увидит соответствующее сообщение от антивируса и попытка отправки файла будет заблокирована. Запись об этом событии будет создана в системном журнале.

2. Если запрос не был заблокирован при фильтрации содержимого трафика или при проверке антивирусом, он передается на интернет-ресурс.
3. Ответ от интернет-ресурса поступает на ViPNet Coordinator HW:
   - Ответ обрабатывается сетевыми фильтрами аналогично п. 1.
   - Если на прокси-сервере включена функция фильтрации содержимого трафика, то ответ обрабатывается ее правилами аналогично п. 1.
   - Если на прокси-сервере включена антивирусная проверка трафика, данные проверяются на наличие вирусов. Если пользователь попытается загрузить файл (в том числе открыть HTML-страницу), в котором был обнаружен вирус, он увидит соответствующее сообщение от антивируса и попытка загрузки файла будет заблокирована. Запись об этом событии будет создана в системном журнале.
4. В случае успешного прохождения всех проверок трафик от прокси-сервера передается пользователю.

Если вы хотите использовать встроенный прокси-сервер для защиты интернет-соединения пользователей вашей локальной сети, настройте основные параметры прокси-сервера (см. «Настройка основных параметров прокси-сервера» на стр. 103). Вы также можете включить антивирусную проверку (см. «Настройка антивируса» на стр. 107) и фильтрацию содержимого трафика (см. «Настройка фильтрации содержимого трафика» на стр. 105).

Настройка основных параметров предполагает выбор внешнего сетевого интерфейса сервера, задание IP-адресов, на которых прокси-сервер будет принимать запросы от пользователей, и IP-адресов локальных сетей, которым разрешено использовать прокси-сервер. Вы также можете включить «прозрачный» режим работы прокси-сервера. Если прокси-сервер работает в обычном режиме («прозрачный» режим выключен), в пользовательских приложениях, например в веб-браузере, требуется указать IP-адрес и порт прокси-сервера.

Если прокси-сервер работает в «прозрачном» режиме, дополнительная настройка приложений не требуется. При этом пользователи не имеют возможности отказаться от использования прокси-сервера. На компьютерах пользователей задайте IP-адрес прокси-сервера (узла с ПО ViPNet Coordinator HW) в качестве шлюза по умолчанию.

Настройка основных параметров прокси-сервера

Если вы хотите использовать встроенный прокси-сервер для защиты интернет-соединения пользователей вашей локальной сети, настройте основные параметры прокси-сервера. Вы также можете включить фильтрацию содержимого и антивирусную проверку трафика. Для получения более подробной информации см. разделы Настройка фильтрации содержимого трафика (на стр. 105) и Настройка антивируса (на стр. 107).

Настройка основных параметров предполагает выбор внешнего сетевого интерфейса сервера, задание IP-адресов, на которых прокси-сервер будет принимать запросы от пользователей (прослушивать их), и IP-адресов локальных сетей, которым разрешено использовать прокси-сервер. Вы также можете включить «прозрачный» режим работы прокси-сервера.

Если прокси-сервер работает в обычном режиме («прозрачный» режим выключен), в пользовательских приложениях, например в веб-браузере, требуется указать IP-адрес и порт прокси-сервера.

Если прокси-сервер работает в «прозрачном» режиме (см. глоссарий, стр. 159), дополнительная настройка приложений не требуется. При этом пользователи не имеют возможности отказаться от использования прокси-сервера. На компьютерах пользователей в качестве шлюза по умолчанию необходимо указать IP-адрес компьютера с программным обеспечением ViPNet Coordinator HW, который играет роль прокси-сервера.

Примечание. При настройке параметров прокси-сервера в файле конфигурации межсетевого экрана автоматически создаются необходимые сетевые фильтры и правила трансляции адресов.

Чтобы настроить основные параметры прокси-сервера, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. На начальной странице щелкните плитку **Межсетевой экран**.
3. Перейдите на страницу **Прокси-сервер** > **Общие настройки**.
4. В группе **Основные настройки Прокси-сервера** выполните следующие действия:
   - В списке **Внешний сетевой интерфейс** выберите сетевой интерфейс, подключенный к Интернету.
   - В поле **Размер кэша** укажите размер кэша прокси-сервера. Напротив этого поля указан объем свободного места на диске. Кэш используется для хранения копии данных, к которым часто обращаются пользователи.

- Если вы хотите включить «прозрачный» режим работы прокси-сервера, установите флажок **«Прозрачный» режим работы**.
- Нажмите кнопку **Сохранить**.

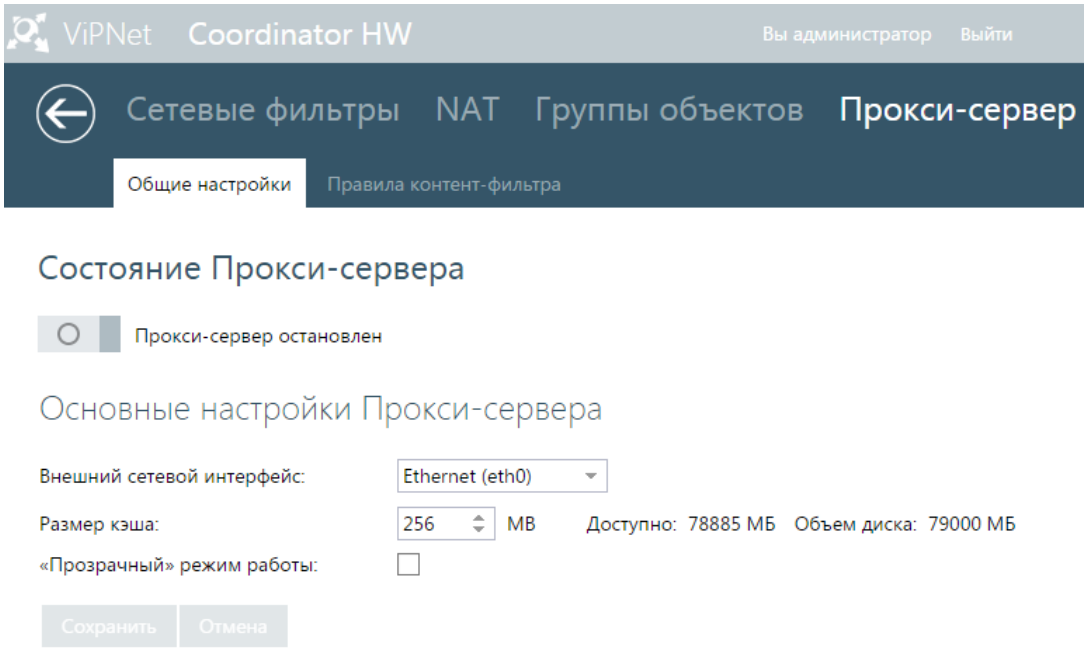


Рисунок 52. Настройка основных параметров прокси-сервера

5 В группе **Прослушиваемые адреса** задайте IP-адреса и порты, которые прокси-сервер должен использовать, чтобы принимать запросы пользователей. Для этого нажмите кнопку **Добавить** и в появившемся списке выберите IP-адрес, а также укажите номер порта для прослушивания. Затем нажмите кнопку **Сохранить**.

Рисунок 53. Задание прослушиваемых IP-адресов

Внимание! Мы рекомендуем задавать для прослушивания сетевые интерфейсы со статическими IP-адресами. После изменения IP-адресов сетевых интерфейсов необходимо завершить работу прокси-сервера, задать текущие IP-адреса интерфейсов, использующихся для организации соединения, а затем снова запустить прокси-сервер.

6 В группе **Обслуживаемые сети** задайте список локальных сетей, которым разрешено использовать прокси-сервер. Для этого нажмите кнопку **Добавить** и в появившемся поле задайте IP-адрес сети в нотации CIDR. Например, 192.168.1.0/24. Затем нажмите кнопку **Сохранить**.

Рисунок 54. Задание сетей, которым разрешено использовать прокси-сервер

7 Чтобы запустить прокси-сервер, щелкните переключатель в верхней части страницы. Состояние прокси-сервера отображается напротив переключателя.

Внимание! Перед запуском прокси-сервера необходимо задать IP-адрес и порт для прослушивания, а также внешний сетевой интерфейс ViPNet Coordinator HW.

При запуске прокси-сервера будут автоматически сформированы сетевые фильтры и правила трансляции адресов, необходимые для доступа в Интернет через прокси-сервер для узлов защищенной и открытой сети. При завершении работы прокси-сервера правила автоматически удаляются, при повторном запуске правила формируются заново.

Внимание! Если для подключения к Интернету ViPNet Coordinator HW использует маршрут с несколькими шлюзами (multi-hop route), для корректной работы прокси-сервера на ViPNet Coordinator HW создайте фильтр открытой сети со следующими параметрами:

- Действие: **Пропускать трафик**.
- Источники: **Мой узел**.
- Назначения: **Группа IP-адресов** > **InternetIP**, флажок **Все объекты, кроме "PivateNetworkIP"**.
- Протоколы: TCP: 21, TCP: 80, TCP: 443.

Подробнее о создании сетевых фильтров см. в разделе Создание и изменение сетевого фильтра (на стр. 76).

Настройка фильтрации содержимого трафика

Прокси-сервер ViPNet Coordinator HW имеет функцию проверки HTTP-трафика по его содержимому. С помощью правил фильтрации содержимого трафика вы можете настроить блокировку трафика по MIME-типу (см. глоссарий, стр. 155) файла или приложения, а также по типу HTTP-метода запроса к удаленному ресурсу.

Фильтрация содержимого трафика включается автоматически при запуске прокси-сервера. Для настройки параметров этой функции выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 На начальной странице щелкните плитку **Межсетевой экран**.

3 Перейдите на страницу **Прокси-сервер** > **Правила контент-фильтра**.

На этой странице отображается список правил фильтрации содержимого трафика.

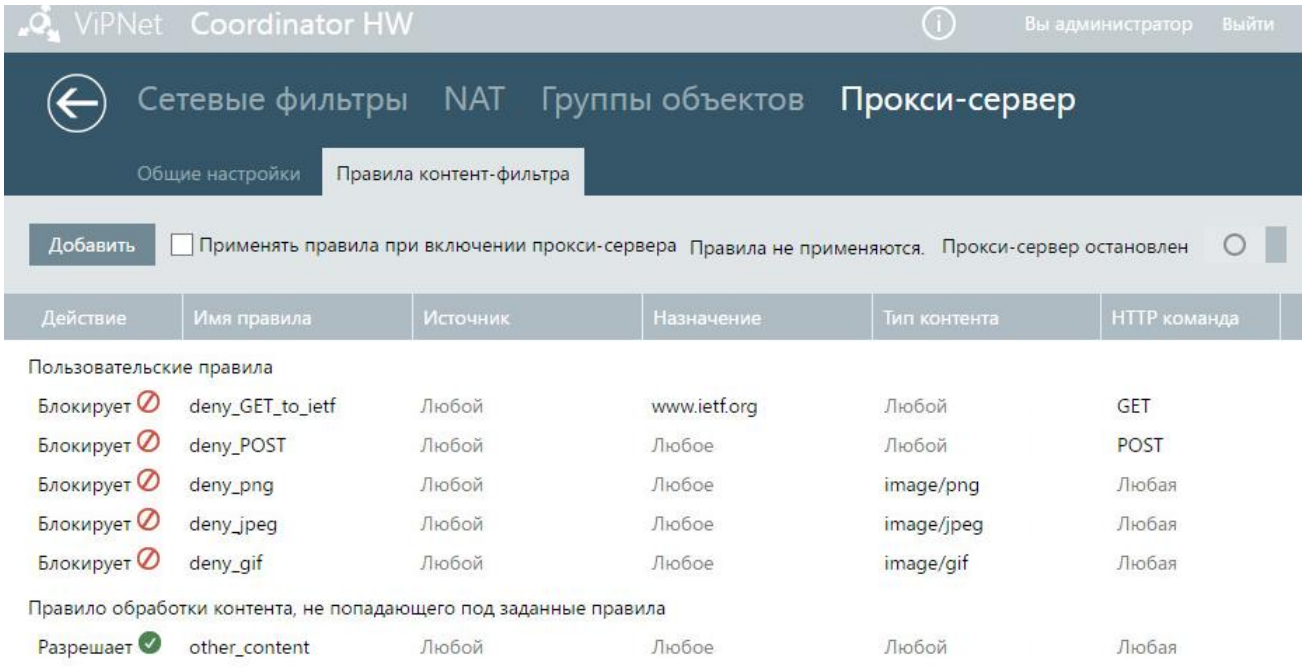


Рисунок 55. Настройка фильтрации содержимого трафика

4 Чтобы добавить новое правило фильтрации содержимого, нажмите кнопку **Добавить** и выполните следующие действия:

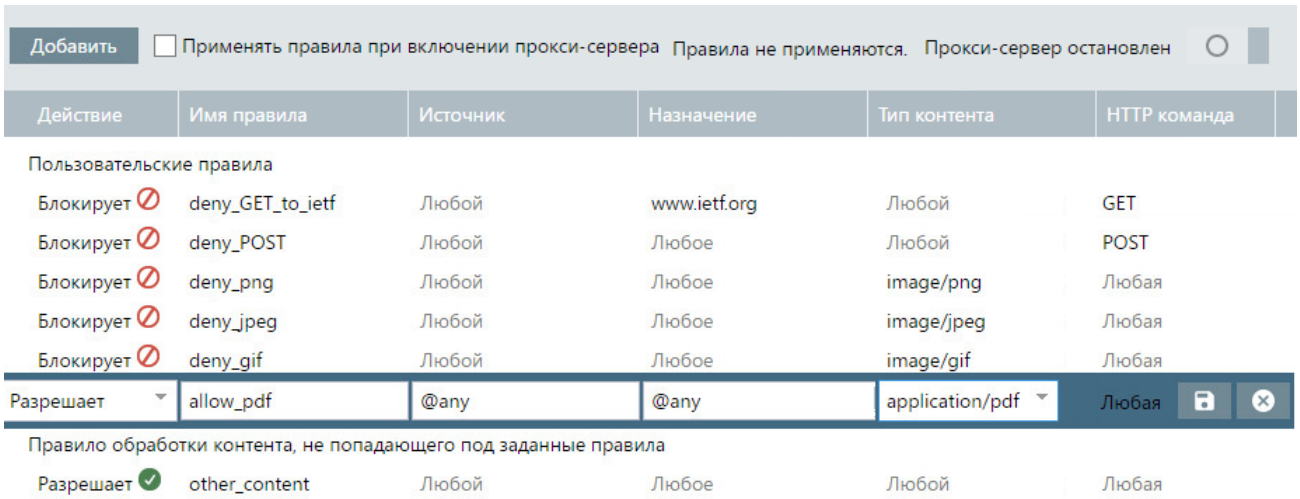


Рисунок 56. Добавление правила фильтрации содержимого трафика

4.1 В столбце **Действие** выберите тип правила — разрешающее или блокирующее.

4.2 В соответствующем столбце задайте имя правила.

4.3 В соответствующих столбцах задайте IP-адрес источника и назначения, для которых будет действовать правило. Чтобы задать любой узел в качестве источника или назначения, введите `@any`. Для указания назначения вы также можете использовать доменное имя.

Примечание. В качестве источника необходимо указать клиента прокси-сервера, в качестве назначения — удаленный HTTP-сервер.

4.4 В соответствующем столбце выберите тип контента (см. глоссарий, стр. 155).

Примечание. MIME-тип файла может зависеть от настроек удаленного HTTP-сервера, с которого этот файл был загружен. То есть, файл будет иметь тот MIME-тип, который был назначен ему HTTP-сервером.

4.5 Если вы выбрали тип контента **Любой,** в столбце **HTTP команда** выберите метод протокола HTTP.

4.6 Чтобы сохранить созданное правило, нажмите кнопку  . Чтобы отменить создание правила, нажмите кнопку  .

После создания правила и запуска прокси-сервера созданные правила будут блокировать ненужный трафик.

5 Чтобы применить созданные правила при следующем запуске прокси-сервера, установите флажок **Применять правила при включении прокси-сервера**.

Настройка антивируса

Если ViPNet Coordinator HW используется в качестве прокси-сервера, вы можете настроить антивирусную проверку данных, передаваемых через прокси-сервер по протоколу HTTP в обоих направлениях: из Интернета к пользователю и от пользователя в Интернет (например, загрузка файла на файлообменный ресурс).

Внимание! Если при загрузке зараженного файла на файлообменные ресурсы используется метод множественной загрузки (multipart upload), то антивирусная проверка не сможет обнаружить вирус в этом файле.

Для антивирусной проверки содержимого трафика в прокси-сервер встроено антивирусное решение, разрабатываемое компанией «Лаборатория Касперского».

Для настройки параметров антивируса выполните следующие действия:

1 Через веб-интерфейс войдите в ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 На начальной странице щелкните плитку **Межсетевой экран**.

3 Перейдите на страницу **Прокси-сервер** > **Антивирус**.

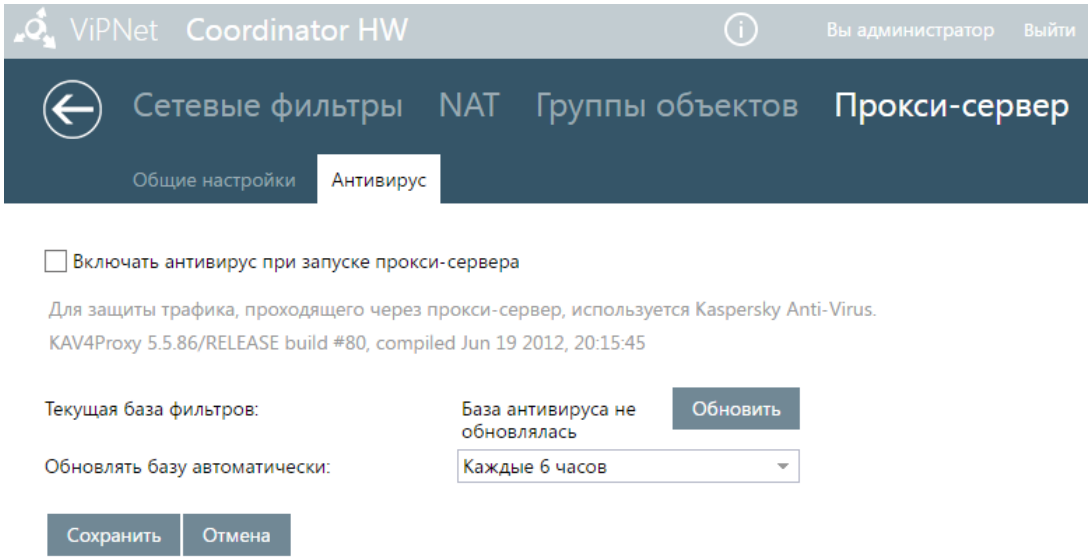


Рисунок 57. Настройка антивируса

4 Чтобы обновить антивирусную базу, нажмите кнопку **Обновить**. Обновление базы начнется в фоновом режиме.

Внимание! Обновление антивирусных баз возможно только при наличии действующей лицензии. Если вы не установили лицензионный ключ или срок действия ключа истек, установите лицензионный ключ с помощью командного интерпретатора (см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»).

---

5 Чтобы антивирусная база обновлялась автоматически, выберите нужный период обновления из списка **Обновлять базу автоматически**.

6 Чтобы запустить антивирус, установите соответствующий флажок в верхней части страницы.

7 Нажмите кнопку **Сохранить**.

Настройка параметров точки доступа к сети Wi-Fi

Внимание! Использование ViPNet Coordinator HW в качестве точки доступа Wi-Fi возможно только в исполнениях со встроенными адаптерами Wi-Fi: ViPNet Coordinator HW50 A, B на аппаратной платформе HW50 N2 и ViPNet Coordinator HW100 A, B на аппаратной платформе HW100 N2.

Если включена точка доступа Wi-Fi, сетевому интерфейсу `wlan0` автоматически присваивается IP-адрес 192.168.20.1 и на этом интерфейсе запускается DHCP-сервер. DHCP-сервер имеет собственные параметры, которые не могут быть просмотрены или изменены пользователем:

- Диапазон распределяемых IP-адресов: 192.168.20.2–192.168.20.20.
- Адреса DNS- и NTP-сервера: 192.168.20.1 (адрес сетевого интерфейса `wlan0`).

Примечание. Если требуется обеспечить возможность соединений между устройствами, которые подключены к сети Wi-Fi, и устройствами, подключенными к сети Ethernet, на узле ViPNet Coordinator HW создайте транзитные фильтры открытой сети, разрешающие пропускание IP-пакетов между этими сетями (см. «Создание и изменение сетевого фильтра» на стр. 76).

Чтобы настроить ViPNet Coordinator HW для работы в качестве точки доступа Wi-Fi, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.

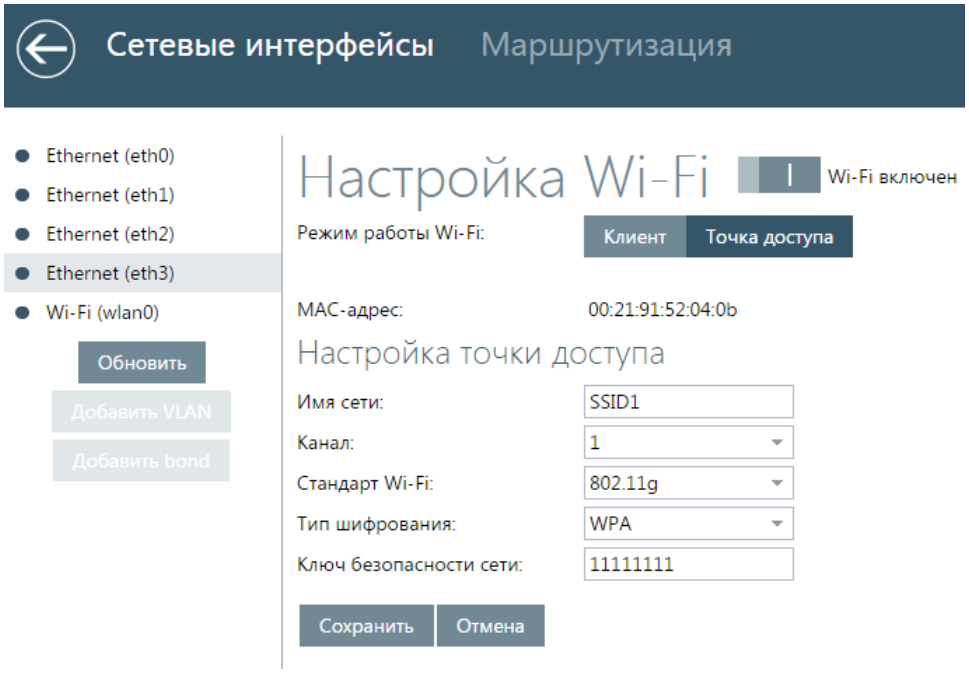


Рисунок 58. Настройка параметров точки доступа Wi-Fi

3 На левой панели выберите сетевой интерфейс Wi-Fi. Сетевому интерфейсу Wi-Fi, установленному в системе, присваивается имя `wlan0`.

4 Установите переключатель **Режим работы Wi-Fi** в положение **Точка доступа**.

5 В поле **Имя сети** задайте имя вашей сети Wi-Fi.

6 В списке **Канал** выберите номер канала Wi-Fi, который вы хотите использовать для точки доступа.

7 В списке **Стандарт Wi-Fi** выберите стандарт беспроводной связи для вашей сети Wi-Fi. Поддерживаются следующие стандарты:

- 802.11b — 2,4 ГГц, скорость соединения до 11 Мбит/с.
- 802.11g — 2,4 ГГц, скорость соединения до 54 Мбит/с.

8 В списке **Тип шифрования** выберите тип шифрования для аутентификации пользователей:

- При выборе типа **Без шифрования** пользователи смогут подключаться к сети без ввода пароля.
- При выборе типов **WPA** или **WPA2** в поле **Ключ безопасности сети** введите пароль для аутентификации пользователей. Заданный пароль нужно будет сообщить пользователям для подключения к вашей сети Wi-Fi.

9 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

10 Для обеспечения соединения между устройствами в сети Wi-Fi и компьютерами в вашей сети Ethernet на сетевом узле ViPNet Coordinator HW задайте в файле конфигурации межсетевого экрана правила, разрешающие обмен IP-пакетами между этими сетями

11 Включите сетевой интерфейс Wi-Fi. Для этого щелкните переключатель в верхней части страницы. Состояние сетевого интерфейса отображается рядом с переключателем.

В результате ваш ViPNet Coordinator HW будет функционировать в качестве точки доступа Wi-Fi.

Примечание. ViPNet Coordinator HW может также работать в качестве клиента сети Wi-Fi (см. «Подключение к беспроводной сети Wi-Fi» на стр. 31). Использование ViPNet Coordinator HW одновременно в качестве клиента и точки доступа Wi-Fi не поддерживается.

7

Настройка маршрутизации

Общие сведения о маршрутизации 113

Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW 114

Просмотр общей таблицы маршрутизации 117

Общие сведения для работы по протоколу OSPF 119

Настройка статической маршрутизации 121

Настройка динамической маршрутизации 125

Общие сведения о маршрутизации

ViPNet Coordinator HW поддерживает функции маршрутизации IP-трафика в сетях со сложной структурой.

Под маршрутизацией понимается процесс выбора маршрута следования IP-пакета (см. глоссарий, стр. 158), передаваемого в сети от одного узла другому. Маршрут следования выбирается из подмножества маршрутов, заданных на маршрутизаторе и хранящихся в таблице маршрутизации.

В таблицу маршрутизации маршруты могут попадать в явном виде (статические маршруты) либо с помощью алгоритмов маршрутизации на основе информации о топологии и состоянии сети, предоставляемой протоколами маршрутизации (динамические маршруты). В первом случае не требуется никаких дополнительных условий. Но стоит заметить, что в сетях со сложной структурой процесс настройки статических маршрутов может стать весьма трудоемким из-за большого числа маршрутов, которые требуется создать. Во втором случае на всех маршрутизаторах в сети должно быть настроено использование определенного протокола динамической маршрутизации, по которому маршрутизаторы будут обмениваться друг с другом информацией о доступных им сетях, автоматически строить доступные маршруты в каждую сеть и выбирать из них наилучшие.

Статическую маршрутизацию удобно использовать в небольших сетях либо в крупных сетях в частных случаях. В сетях с разветвленной и неоднородной топологией рекомендуется использовать динамическую маршрутизацию. Кроме автоматического формирования таблиц маршрутизации, динамическая маршрутизация позволяет:

- Автоматически выбирать по определенным критериям наилучший маршрут из нескольких доступных.
- Организовать защиту от сбоев. В случае сбоя какого-либо маршрутизатора автоматически выбирается другой наилучший маршрут и загружается в таблицу маршрутизации.
- Организовать динамическую балансировку нагрузки передаваемого IP-трафика.

ViPNet Coordinator HW может выполнять маршрутизацию IP-трафика с использованием следующих видов маршрутов:

- статических маршрутов, в том числе на основе маршрутов с несколькими шлюзами;
- динамических маршрутов, формируемых по протоколу DHCP и PPP;
- динамических маршрутов, формируемых протоколом OSPF (см. глоссарий, стр. 156).

Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW

В ViPNet Coordinator HW для хранения маршрутов используются две таблицы маршрутизации:

- Routing Information Base (далее — RIB) — полная таблица маршрутизации, которая содержит все статические маршруты, созданные администратором, и все динамические маршруты, полученные по протоколам DHCP, PPP и OSPF.
- Forwarding Information Base (далее — FIB) — таблица маршрутизации, которая содержит только наилучшие статические и динамические маршруты в каждую сеть, выбранные из RIB; загружается в ядро системы и используется при маршрутизации IP-трафика.

Все новые маршруты, независимо от способа их создания, попадают в RIB. Каждый маршрут имеет следующие характеристики:

- Источник получения маршрута — определяет, каким образом был сформирован маршрут: с использованием статического правила или по протоколу динамической маршрутизации.
- Административная дистанция — определяет приоритет маршрута от каждого источника. Используется тогда, когда в таблице маршрутизации задано несколько маршрутов в одну и ту же сеть. Чем меньше административная дистанция, тем более приоритетным считается маршрут.

  Административная дистанция задается для каждого статического маршрута. В случае динамических маршрутов административная дистанция задается не для конкретного маршрута, а для всего протокола сразу. Поэтому все динамические маршруты, добавленные в RIB этим протоколом, имеют одинаковую дистанцию.

  Административная дистанция для протокола PPP отдельно не задается и равна дистанции для протокола DHCP. Административная дистанция для протоколов DHCP/PPP и OSPF не может быть одинаковой, чтобы маршруты этих протоколов не перемешивались. Также административная дистанция статических правил маршрутизации не может совпадать с дистанцией, заданной для какого-либо протокола динамической маршрутизации.

Примечание. В ViPNet Coordinator HW для каждого типа маршрутов задается по умолчанию следующая административная дистанция:

- для статических маршрутов — 10;
- для маршрутов DHCP/PPP-сервера — 70;
- для маршрутов протокола OSPF — 110.

Для первых двух типов маршрутов вы можете менять значение административной дистанции, для маршрутов последнего типа менять это значение нельзя.

Для маршрутов DHCP/PPP-сервера задается общая административная дистанция.

- Метрика — определяет приоритет внутри списка динамических маршрутов, сформированных и добавленных в RIB определенным протоколом динамической маршрутизации. Чем меньше метрика, тем выше приоритет маршрута.

  Для DHCP-протокола метрики указываются вручную, причем на каждом сетевом интерфейсе, на котором включен режим DHCP и настроен параметр получения маршрутов от DHCP-сервера. Таким образом, если на разные сетевые интерфейсы будут получены одинаковые DHCP-маршруты в одну и ту же сеть, то будет выбран маршрут с наименьшей метрикой. Для PPP-протокола также может быть задана метрика вручную в том случае, если ViPNet Coordinator HW подключен к нескольким сетям, одной из которых является сеть 3G или 4G, а в другой развернут DHCP-сервер. Если метрики для DHCP/PPP-протоколов не были заданы, то используется метрика по умолчанию.

- Для динамических маршрутов, формируемых протоколом OSPF, метрики формируются самим протоколом, поэтому их задавать не требуется.

- Вес — определяет долю IP-трафика, который будет проходить по маршруту через указанный шлюз. Используется только в статических маршрутах и задается для шлюза. Позволяет настроить балансировку передаваемого IP-трафика между несколькими шлюзами, когда часть IP-пакетов направляется на один шлюз, а часть — на другой. Поэтому вес задается тогда, когда создается несколько статических маршрутов с одинаковым IP-адресом назначения и разными шлюзами.

Таблица FIB формируется на основе содержания таблицы RIB и включает в себя только наилучшие маршруты в каждую сеть. Если в результате заполнения таблицы RIB в ней оказывается несколько маршрутов в одну сеть, то наилучший маршрут определяется по следующим правилам:

- Если в RIB присутствуют статические маршруты с разной дистанцией, то в FIB загружается маршрут с наименьшей дистанцией. Например, имеется два маршрута в сеть 10.0.5.0 с маской 255.255.255.0. Для первого маршрута задана административная дистанция — 10, для второго — 30. В результате в FIB попадет первый маршрут.

- Если в RIB присутствуют статические маршруты с одинаковой дистанцией, то в FIB загружаются все маршруты.

- Если в RIB присутствуют динамические маршруты, то в FIB загружается маршрут с наибольшим приоритетом (то есть наименьшей метрикой, заданной протоколом динамической маршрутизации). Если приоритеты равны, то в FIB попадают все маршруты.

Маршруты от одного источника (Static, DHCP, OSPF) в одну и ту же сеть с одинаковыми метриками (или административными дистанциями в случае статических маршрутов) при маршрутизации суммируются — объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре такие маршруты отображаются в виде одного маршрута с несколькими шлюзами:

```
10.100.2.0/24 [30/23] (weight 1) via 10.1.30.202, eth1
                      (weight 1) via 10.1.31.201, eth2
```

Внимание! Если хотя бы один из шлюзов объединенного маршрута multi-hop route выйдет из строя, работоспособность маршрута не может быть гарантирована.

Если маршрут был удален из RIB, то он также удаляется из FIB. При этом по вышеописанным правилам выбирается новый наилучший маршрут в ту же сеть из имеющихся в RIB и немедленно загружается в FIB.

Просмотр общей таблицы маршрутизации

Чтобы просмотреть список всех существующих маршрутов (содержимое таблицы RIB (см. «Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW» на стр. 114)) перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **Сводная таблица**.

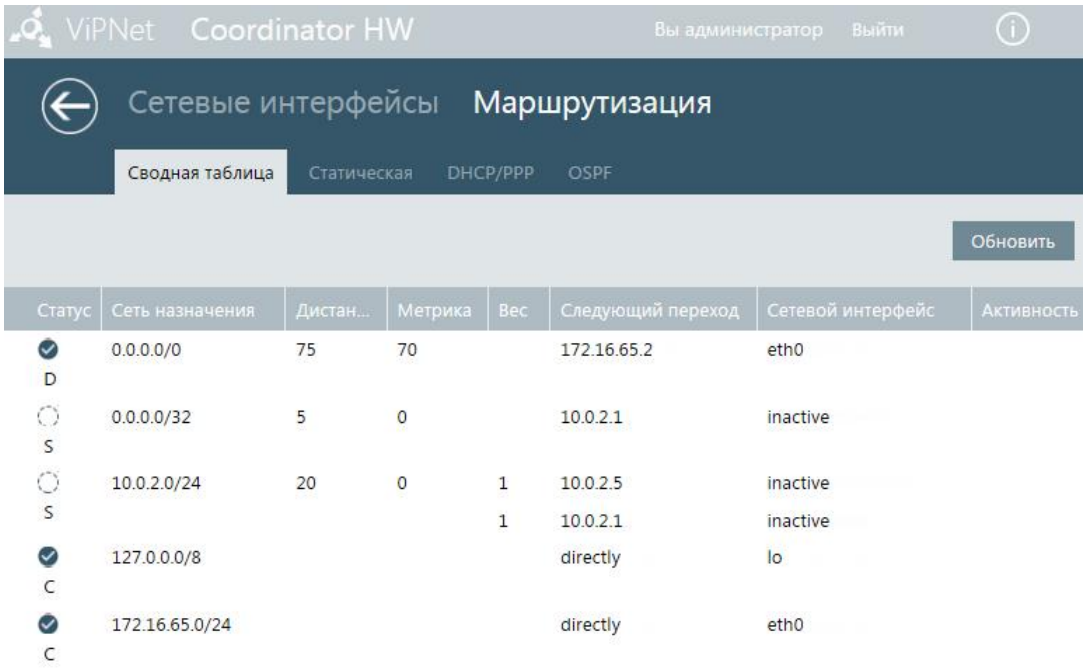


Рисунок 59. Просмотр общей таблицы маршрутизации

Совет. Чтобы обновить содержимое списка маршрутов, нажмите кнопку **Обновить**.

В списке для каждого маршрута отображается статус. Список всех возможных статусов приведен в таблице ниже.

Таблица 7. Статусы маршрутов

Статус	Пояснение
	Наилучший маршрут, который загружен в FIB и используется в процессе маршрутизации.
C	Маршрут в подсеть, к которой подключен один из интерфейсов ViPNet Coordinator HW.
D	Маршрут, предоставленный DHCP/PPP-сервером. В текущей версии ViPNet Coordinator HW нельзя настроить взаимодействие с PPP-сервером. Поэтому маршруты, имеющие атрибут D, — это маршруты исключительно DHCP-сервера.
O	Маршрут протокола динамической маршрутизации OSPF.
S	Статический маршрут.

Списки маршрутов от конкретного источника вы можете посмотреть в разделе **Маршруты** на отдельных вкладках **Статическая**, **DHCP/PPP**, **OSPF**.

Общие сведения для работы по протоколу OSPF

Протокол OSPF является внутренним шлюзовым протоколом (Interior Gateway Protocol, IGP) и используется для распространения данных маршрутизации внутри одной автономной системы (см. глоссарий, стр. 156).

Работа по данному протоколу устроена следующим образом. OSPF-маршрутизаторы сначала посредством широковещательной рассылки (multicast) устанавливают связь друг с другом. Затем посредством однонаправленной рассылки (unicast) начинают обмениваться друг с другом сообщениями типа Link State Advertise (LSA), в которых передают информацию о состоянии каналов связи. На маршрутизаторе при получении LSA-сообщения информация из него заносится в базу данных (link state database). Если LSA-сообщение содержит новую информацию о канале связи по сравнению с той, которая содержится в базе данных, то оно передается соседним маршрутизаторам (см. глоссарий, стр. 158). После заполнения базы данных на каждом маршрутизаторе по алгоритму Дейкстры вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость (см. глоссарий, стр. 159). Таким образом, каждый OSPF-маршрутизатор имеет собственное представление о состоянии каналов связи и топологии сети, но при этом все маршрутизаторы используют одну базу данных состояний каналов связи для вычисления кратчайших маршрутов.

Межсетевая среда, в которой находятся OSPF-маршрутизаторы, представляется как совокупность областей (см. глоссарий, стр. 158), соединенных друг с другом через некоторую базовую область. В зависимости от этого выделяют несколько типов областей и несколько типов маршрутизаторов.

Выделяют следующие типы областей маршрутизации:

- Область 0 или базовая область (backbone area) — область, с которой должны быть соединены все остальные области автономной системы.
- Стандартная область — область, способная граничить как с другими областями, так и с другими автономными системами.
- Стандартная тупиковая область (stub area) — область, граничащая только с другими областями.
- Полностью тупиковая область (totally stubby area) — область, граничащая только с одной областью.
- Не полностью тупиковая область (not-so-stubby area) — стандартная тупиковая область, имеющая возможность взаимодействовать с другими автономными системами с помощью пограничных маршрутизаторов (ABR).

Каждый OSPF-маршрутизатор входит в определенную область маршрутизации и обменивается информацией только с маршрутизаторами, входящими в эту же область. При этом обмен производится не напрямую, а через посредника — маршрутизатор, выбранный главным в этой области. Информация между разными областями передается через маршрутизатор, который

располагается на границе этих областей. Если автономная система взаимодействует с другой автономной системой, то информация передается через маршрутизатор, который располагается на границе систем. Такой подход позволяет уменьшить объем рассылаемых LSA-сообщений, тем самым уменьшить нагрузку на маршрутизаторы и повысить скорость построения таблиц маршрутизации.

Таким образом, выделяют следующие типы маршрутизаторов:

- Внутренний маршрутизатор (internal router, IR) — маршрутизатор, все сетевые интерфейсы которого находятся в одной области.
- Назначенный маршрутизатор (designated router, DR) — маршрутизатор, выбранный главным среди всех внутренних маршрутизаторов в одной области.
- Резервный назначенный маршрутизатор (backup designated router, BDR) — маршрутизатор, берущий на себя функции главного в случае, если он вышел из строя.
- Межобластной граничный маршрутизатор (area border router, ABR) — маршрутизатор, соединяющий несколько областей OSPF одной автономной системы.
- Граничный маршрутизатор автономной системы (autonomous system boundary router, ASBR) — маршрутизатор, граничащий с другой автономной системой, работающей по другому протоколу динамической маршрутизации (IGRP, EIGRP, IS-IS, RIP, BGP, Static).

Настройка статической маршрутизации

Если ViPNet Coordinator HW функционирует в сети, конфигурация которой никогда не меняется или в которой используется минимальное количество путей для доставки IP-пакетов, то вы можете настроить маршрутизацию на ViPNet Coordinator HW вручную с помощью статических маршрутов. Кроме этого, настройка маршрутизации вручную также может потребоваться, когда нет возможности использовать в сети маршрутизаторы, работающие по протоколам динамической маршрутизации, или в следующих случаях:

- Чтобы направлять часть IP-трафика всегда по конкретным маршрутам (например, есть требование направлять IP-трафик по самому надежному каналу), или направлять IP-трафик пользователей в Интернет через конкретный шлюз.
- Если нужен статический маршрут по умолчанию на случай, когда работа по протоколам динамической маршрутизации будет невозможна.
- Чтобы распределять передачу IP-трафика по нескольким маршрутам.

Добавление статических маршрутов

Чтобы добавить новый статический маршрут, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **Статическая**.
3. Нажмите кнопку **Добавить**.
4. Задайте следующие параметры маршрута:
   - IP-адрес назначения маршрута и маску подсети. Маска подсети должна быть указана в битовом формате через слэш после IP-адреса (0.0.0.0/0).
   - IP-адрес шлюза для доступа к IP-адресу назначения.
   - Административная дистанция (см. глоссарий, стр. 157). Если вы не укажете значение административной дистанции, то оно будет задано автоматически и равно 10. Если вы укажете административную дистанцию, и ее значение будет совпадать со значением административной дистанции, заданной протоколам динамической маршрутизации (см. «Настройка административной дистанции для маршрутов DHCP-сервера» на стр. 126), маршрут не сможет быть добавлен. В этом случае создайте маршрут с другим значением административной дистанции.

- Вес (см. глоссарий, стр. 157). Укажите его в том случае, если вы создаете несколько маршрутов в одну сеть с разными шлюзами, между которыми требуется производить балансировку нагрузки. Подробнее см. раздел Настройка балансировки IP-трафика.

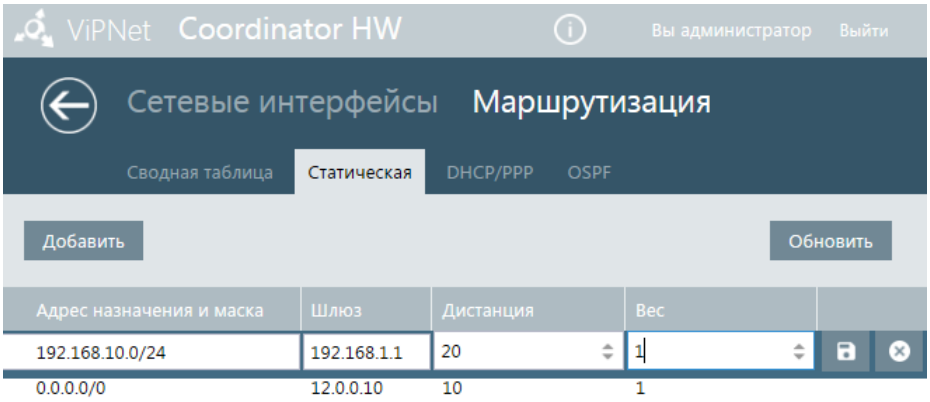


Рисунок 60. Добавление статического маршрута

5 Нажмите кнопку **Сохранить**.

В результате маршрут появится в списке статических маршрутов. Кроме этого, он будет добавлен в таблицу RIB (см. «Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW» на стр. 114) и появится на вкладке **Сводная таблица**. Если маршрут будет выбран наилучшим (см. «Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW» на стр. 114), то он будет загружен в таблицу FIB и начнет использоваться при маршрутизации IP-трафика. В этом случае в списке маршрутов на вкладке **Сводная таблица** он будет иметь значок .

Совет. Если вам требуется получить один статический маршрут с несколькими шлюзами, создайте несколько статических маршрутов в одну и ту же сеть с одинаковой административной дистанцией, указав в каждом по одному шлюзу. В результате эти маршруты будут просуммированы и объединены в один с несколькими шлюзами. Как правило, такие маршруты требуются для балансировки нагрузки, поэтому в маршрутах также должен быть задан вес шлюзам (см. «Настройка балансировки IP-трафика» на стр. 123).

Если в списках не появился новый маршрут, обновите ее содержимое. Для этого нажмите кнопку **Обновить**.

При необходимости вы можете отредактировать значение административной дистанции и веса в маршруте. Для этого дважды щелкните строку маршрута, внесите необходимые изменения и нажмите кнопку **Сохранить**. Если вам нужно изменить IP-адрес назначения или шлюза, удалите маршрут и создайте новый с нужными параметрами. Чтобы удалить маршрут, в строке рядом с ним щелкните значок , после чего в появившемся окне сообщения нажмите кнопку **ОК**.

Настройка балансировки IP-трафика

Если вы хотите ускорить процесс отправки IP-пакетов в сеть назначения, то вы можете создать несколько статических маршрутов в данную сеть через разные шлюзы и настроить балансировку IP-трафика между этими маршрутами. Это позволит в процессе разных TCP-соединений отправлять часть IP-пакетов по одному маршруту, часть — по другому, что повысит скорость передачи IP-пакетов в сеть назначения. Балансировка IP-трафика настраивается с помощью одного из параметров маршрутов — веса (см. глоссарий, стр. 157) (`weight`). При этом все маршруты, которые будут участвовать в балансировке IP-трафика, должны иметь одинаковую административную дистанцию, то есть иметь одинаковый приоритет.

Примечание. При маршрутизации маршруты в одну сеть назначения и с одинаковой дистанцией объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре общей таблицы маршрутизации они отображаются как один маршрут с несколькими шлюзами (см. «Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW» на стр. 114).

Для настройки балансировки IP-трафика выполните следующие действия:

1. Создайте нужное количество маршрутов (см. «Добавление статических маршрутов» на стр. 121) с одинаковым адресом назначения и с разными шлюзами.
2. Задайте каждому маршруту одинаковую административную дистанцию.
3. Задайте в каждом маршруте вес шлюзу. IP-трафик будет распределяться между шлюзами в соответствии с соотношением их весов. Например:
   - если вы создаете 2 маршрута и в каждом маршруте вес шлюза равен 1, то IP-трафик будет разделен между этими маршрутами поровну, то есть 50% IP-трафика будет передаваться по одному маршруту, 50% — по второму;
   - если вы создаете 3 маршрута, и в первом маршруте вес шлюза равен 1, во втором — вес шлюза равен 2, в третьем — вес шлюза равен 3, то по второму маршруту будет передаваться в два раза больше IP-трафика, чем по первому, по третьему — в три раза больше, чем по первому.

Пример создания статических маршрутов с весом шлюзов равным 1:

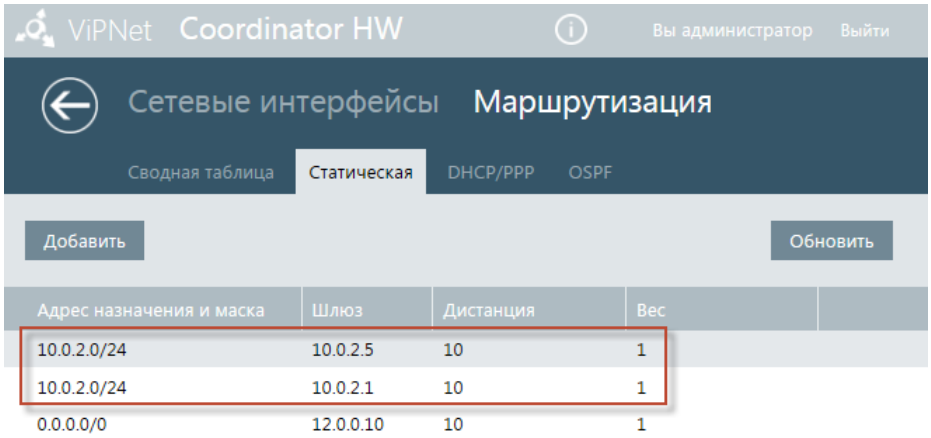


Рисунок 61. Распределение нагрузки между статическими маршрутами в одну сеть

Примечание. Если в процессе создания маршрута вы не укажете вес шлюза, то автоматически шлюзу будет назначен вес равный 1. Вы не можете задать вес равный 0.

Балансировка IP-трафика будет осуществляться, только если созданные маршруты признаны наилучшими и присутствуют в таблице FIB (см. «Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW» на стр. 114).

Настройка динамической маршрутизации

Если в вашей сети поддерживается работа по протоколу DHCP, PPP или OSPF (см. глоссарий, стр. 156), то вы можете настроить на ViPNet Coordinator HW динамическую маршрутизацию. Данные настройки позволят автоматически создавать таблицы маршрутизации на основе маршрутов, формируемых по данным протоколам, и распространять их между другими маршрутизаторами в рамках одной сети.

Внимание! Исполнения ViPNet Coordinator HW50 A, B и Coordinator HW100 A, B не поддерживают динамическую маршрутизацию.

Настройку динамической маршрутизации должен выполнять опытный администратор, понимающий принципы работы протоколов динамической маршрутизации, в том числе протокола OSPF. Приведенная в руководстве информация носит справочный характер.

Настройка параметров динамических маршрутов от DHCP/PPP-протокола

Если на каком-либо сетевом интерфейсе ViPNet Coordinator HW включен режим DHCP и настроено автоматическое получение маршрутов от DHCP-сервера (см. «Настройка сетевых интерфейсов Ethernet» на стр. 24), то в процессе маршрутизации будут использоваться эти маршруты. В этом случае выполните следующие дополнительные настройки:

1. Настройте административную дистанцию для протокола DHCP (см. «Настройка административной дистанции для маршрутов DHCP-сервера» на стр. 126). Это позволит определить приоритет маршрутов DHCP-сервера среди всех маршрутов, имеющихся в таблице RIB (статических маршрутов, маршрутов протокола OSPF, если такие есть).
2. Если режим DHCP включен на нескольких сетевых интерфейсах, настройте метрики DHCP-протокола на каждом сетевом интерфейсе, на котором включен этот режим (см. «Настройка метрики для маршрутов DHCP-сервера» на стр. 127). Это позволит определить приоритет среди маршрутов DHCP-сервера в одну и ту же сеть, полученных с разных сетевых интерфейсов.

Если ViPNet Coordinator HW подключен к сети 3G или 4G и получает информацию для маршрута по умолчанию от PPP-сервера провайдера (см. «Подключение к мобильной сети 3G, 4G» на стр. 34), и при этом он также подключен к другой сети и получает в ней маршрутную информацию от DHCP-сервера, то в этом случае задайте метрику для PPP-протокола. Это позволит определить, какой маршрут по умолчанию (сформированный на основе шлюза по умолчанию от PPP-сервера или предоставленный DHCP-сервером) является приоритетным. Административная дистанция для этого протокола не задается и равна дистанции для протокола DHCP.

Настройка административной дистанции для маршрутов DHCP-сервера

Если на ViPNet Coordinator HW настроено взаимодействие с DHCP-сервером, от которого поступают динамические маршруты для маршрутизации IP-трафика, а также настроена статическая маршрутизация (см. «Настройка статической маршрутизации» на стр. 121) или динамическая маршрутизация по протоколу OSPF (см. «Настройка параметров динамической маршрутизации по протоколу OSPF» на стр. 130), то требуется задать административную дистанцию для маршрутов DHCP-протокола. Административная дистанция определит приоритет данных маршрутов среди всех остальных, и в случае, если будет обнаружено несколько маршрутов в одну и ту же сеть из разных источников, будет выбран тот маршрут, у которого выше приоритет. Чем меньше значение административной дистанции (см. глоссарий, стр. 157), тем выше приоритет маршрута.

Примечание. Административная дистанция определяет приоритет всех маршрутов DHCP-сервера, независимо от того, на какой сетевой интерфейс они поступили.

Чтобы задать административную дистанцию для маршрутов, поступающих от DHCP-сервера, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **DHCP/PPP**.
3. Введите значение административной дистанции в поле **Дистанция** и нажмите кнопку **Сохранить**. По умолчанию указана административная дистанция 70.

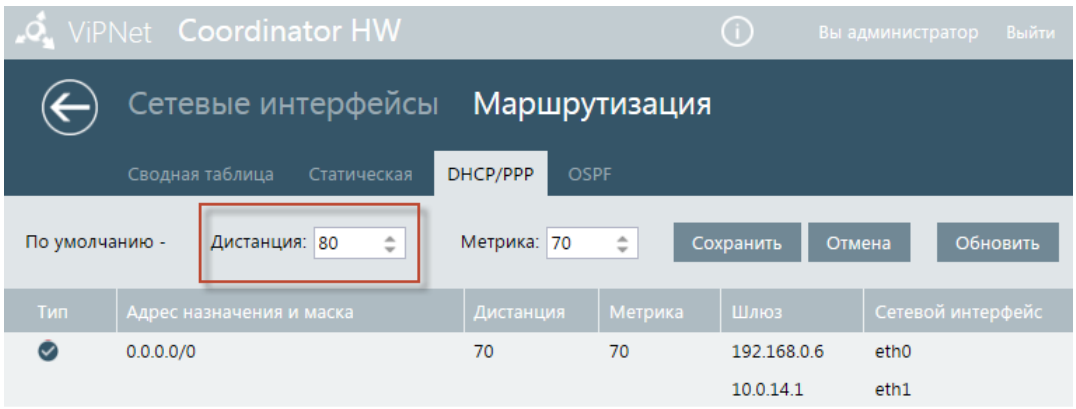


Рисунок 62. Задание административной дистанции маршрутам DHCP-сервера

Примечание. В командном интерпретаторе ViPNet Coordinator HW вы также можете задать административную дистанцию для маршрутов по умолчанию. В текущей версии веб-интерфейса такая возможность отсутствует.

Настройка метрики для маршрутов DHCP-сервера

Если на ViPNet Coordinator HW режим DHCP включен на нескольких сетевых интерфейсах, то может сложиться ситуация, когда с этих интерфейсов поступят одинаковые маршруты от DHCP-сервера в одну и ту же сеть. В этом случае требуется определить, какой маршрут является наилучшим, чтобы добавить его в FIB (см. «Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW» на стр. 114) и использовать при маршрутизации. Параметром, позволяющим выбрать наилучший маршрут, выступает метрика (см. глоссарий, стр. 158). Ее можно задать на каждом сетевом интерфейсе, на котором включен режим DHCP, чтобы определить приоритет маршрутов DHCP-сервера на разных интерфейсах. Чем меньше значение метрики, тем выше приоритет маршрута. Если на интерфейсах заданы одинаковые метрики, то поступившие маршруты в одну и ту же сеть будут объединены в один маршрут с несколькими шлюзами.

В ViPNet Coordinator HW вы можете задать или удалить метрику для маршрутов DHCP-сервера на конкретном сетевом интерфейсе (далее — специфичная метрика). Если специфичная метрика не задана, то вместо нее используется метрика по умолчанию.

Примечание. Задать специфичную метрику для протокола DHCP вы можете на сетевых интерфейсах следующих типов:

- Ethernet (см. «Настройка сетевых интерфейсов Ethernet» на стр. 24).
- VLAN (см. «Организация обработки трафика из нескольких VLAN» на стр. 28).
- Wi-Fi (wlan) (см. «Подключение к беспроводной сети Wi-Fi» на стр. 31).
- Агрегированный интерфейс (см. «Использование агрегированных сетевых интерфейсов» на стр. 36).

При этом должны выполняться следующие условия:

- на нескольких сетевых интерфейсах включен режим DHCP;
- на этих интерфейсах настроен параметр автоматического получения маршрутов от DHCP-сервера.

Если режим DHCP включен только на одном сетевом интерфейсе, то настройка специфичной метрики не требуется, поскольку для группы маршрутов в рамках одного сетевого интерфейса она всегда будет одинаковой.

Чтобы настроить метрику для маршрутов, поступающих от DHCP-сервера, на сетевом интерфейсе одного из указанных типов, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.
3. На левой панели выберите интерфейс, на котором требуется задать метрику.
4. Убедитесь, что на данном интерфейсе включен режим DHCP (установлен флажок **Автоматически получать настройки**) и настроено автоматическое получение маршрутов от него (установлен флажок **Маршруты**).

5 Введите значение метрики в поле **Метрика** и нажмите кнопку **Сохранить**.

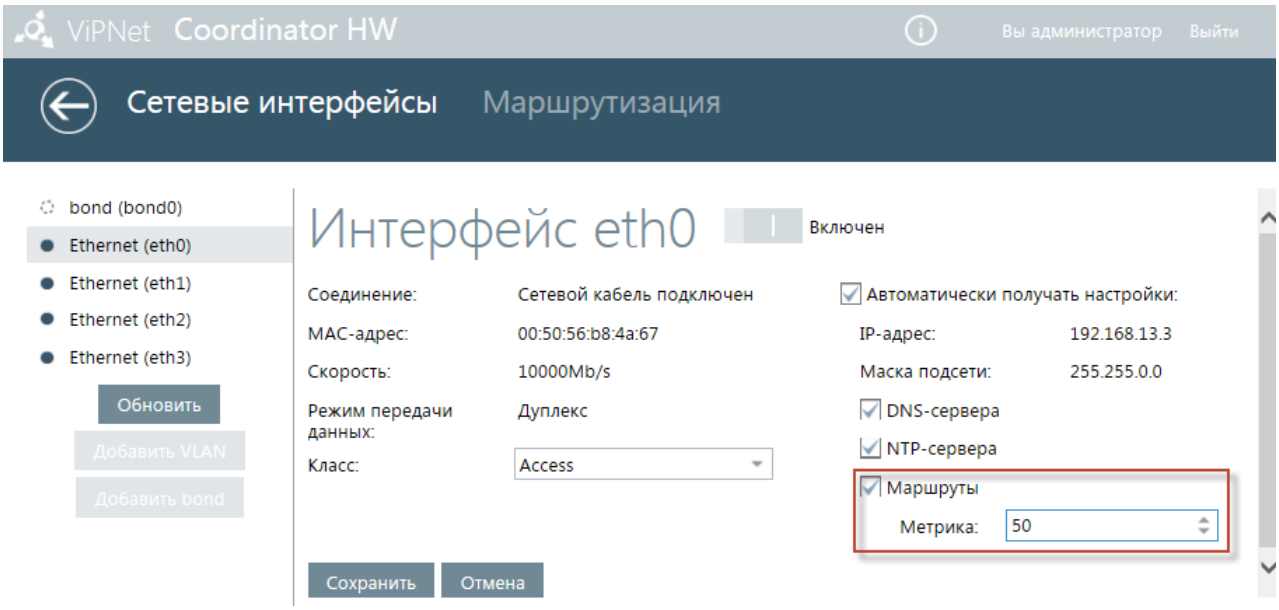


Рисунок 63. Задание метрики для протокола DHCP на конкретном сетевом интерфейсе

6 Если требуется удалить метрику на сетевом интерфейсе, удалите ее значение в указанном поле. После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

Настройка метрики для маршрутов PPP-протокола

Если ViPNet Coordinator HW подключен к мобильной сети 3G или 4G (см. «Подключение к мобильной сети 3G, 4G» на стр. 34), то при первом соединении с сервером провайдера он может получить от него по протоколу PPP IP-адрес шлюза по умолчанию, на основе которого будет добавлен маршрут по умолчанию (см. глоссарий, стр. 158).

Примечание. Шлюз по умолчанию поступает на ViPNet Coordinator HW от PPP-сервера только, если в свойствах интерфейса модема установлен флажок **Маршруты**.

Если кроме подключения к сети 3G, 4G, ViPNet Coordinator HW также подключен к другим сетям, в которых информация об адресах и маршрутах распространяется DHCP-сервером, то он также будет получать маршруты по умолчанию по протоколу DHCP. Если требуется, чтобы маршрут по умолчанию PPP-протокола имел выше приоритет, чем маршруты по умолчанию DHCP-протокола, и использовался в процессе маршрутизации, требуется задать метрику для протокола PPP (далее – специфичную метрику). Причем она должна быть меньше метрики DHCP-протокола на каждом сетевом интерфейсе, на которых они заданы. Если специфичная метрика не будет задана, то вместо нее будет использоваться метрика по умолчанию (см. «Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола» на стр. 129). В этом случае маршруты по умолчанию PPP- и DHCP-протокола будут иметь одинаковый приоритет.

Метрику для PPP-протокола вы можете настроить в свойствах интерфейса модема и только в том случае, если разрешено добавление маршрута по умолчанию от PPP-сервера провайдера. Для этого выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.

3 На левой панели выберите интерфейс модема.

4 Убедитесь, что на данном интерфейсе разрешено добавление маршрута по умолчанию (установлен флажок **Маршруты**).

5 Введите значение метрики в поле **Метрика** и нажмите кнопку **Сохранить**.

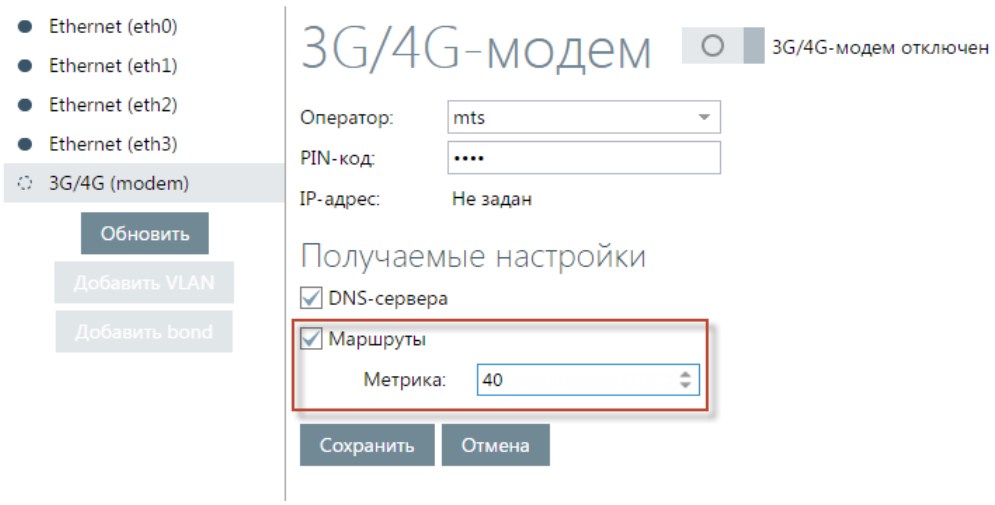


Рисунок 64. Задание метрики для протокола PPP на сетевом интерфейсе модема

6 Если требуется удалить метрику на сетевом интерфейсе, удалите ее значение в указанном поле. После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола

Если для маршрутов DHCP/PPP-протокола не задавались специфичные метрики, то для определения приоритета маршрутов этих протоколов будет использоваться метрика по умолчанию. Первоначально метрика по умолчанию равна 70. При необходимости вы можете изменить это значение. Для этого выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **DHCP/PPP**.

3 Введите новое значение метрики в поле **Метрика** и нажмите кнопку **Сохранить**. Первоначально метрика по умолчанию равна 70.

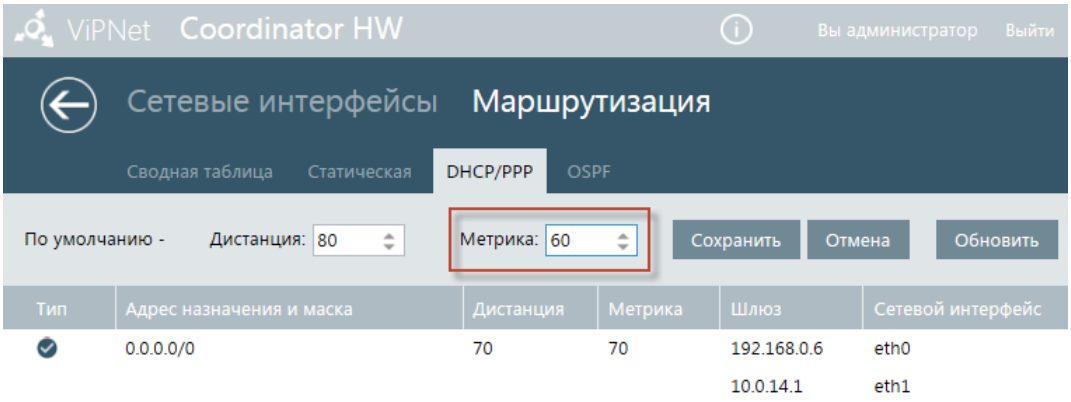


Рисунок 65. Задание метрики по умолчанию

Настройка параметров динамической маршрутизации по протоколу OSPF

Совет. Настройка динамической маршрутизации по протоколу OSPF имеет смысл в том случае, если в сети, в которой установлен ViPNet Coordinator HW, одновременно выполняются следующие условия:

- используются другие OSPF-маршрутизаторы и они напрямую связаны с ViPNet Coordinator HW;
- поддерживается многоадресное вещание (multicast);
- по требованиям безопасности вашей организации разрешена передача IP-трафика по протоколу OSPF между сетевыми узлами.

В процессе настройки маршрутизации по протоколу OSPF вам потребуется:

- включить использование протокола OSPF;
- указать сети, к которым подключен ViPNet Coordinator HW и которые будут участвовать в маршрутизации по протоколу OSPF, и области маршрутизации (см. глоссарий, стр. 158);
- создать ряд сетевых фильтров.

При настройке динамической маршрутизации по протоколу OSPF следует учитывать следующие рекомендации и ограничения:

- В случае сбоя на одном из маршрутов для переключения на альтернативный маршрут может потребоваться до 15 минут. Чтобы уменьшить время переключения, рекомендуется в файле `iplir.conf` в секциях `[id]`, соответствующих связанным координаторам ViPNet, задать более короткий период опроса, изменив значение параметра `checkconnection_interval` (подробнее см. в документе «ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам»). Например, можно задать для параметра значение 30 секунд. При этом необходимо учитывать, что сокращение периода опроса приведет к увеличению количества служебного трафика между координаторами, в результате чего может снизиться производительность координаторов.

- Если ваш ViPNet Coordinator HW непосредственно связан с другими координаторами ViPNet, рекомендуется в файле `iplir.conf` в секциях `[id]`, соответствующих этим координаторам, указать в параметре `accessiplist` метрику `1`. В этом случае при наличии нескольких альтернативных маршрутов защищенный трафик всегда будет передаваться по кратчайшему маршруту — через соседний координатор ViPNet.

При необходимости вы также можете настроить перераспределение маршрутов (см. глоссарий, стр. 158) по протоколу OSPF.

Настройка протокола OSPF

Для настройки протокола OSPF выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **OSPF**.

3 В разделе **Настройки** включите использование протокола, установив переключатель в верхней части страницы в положение **Включена**.

4 Укажите подсеть, в которой должна осуществляться маршрутизация по протоколу OSPF. Для этого нажмите кнопку **Добавить** и укажите следующие параметры:

   - IP-адрес подсети и маску подсети в нотации CIDR (например, 0.0.0.0/0).
   - Область маршрутизации (см. глоссарий, стр. 158), в которую входит указанная подсеть.

   Нажмите кнопку **Сохранить**.

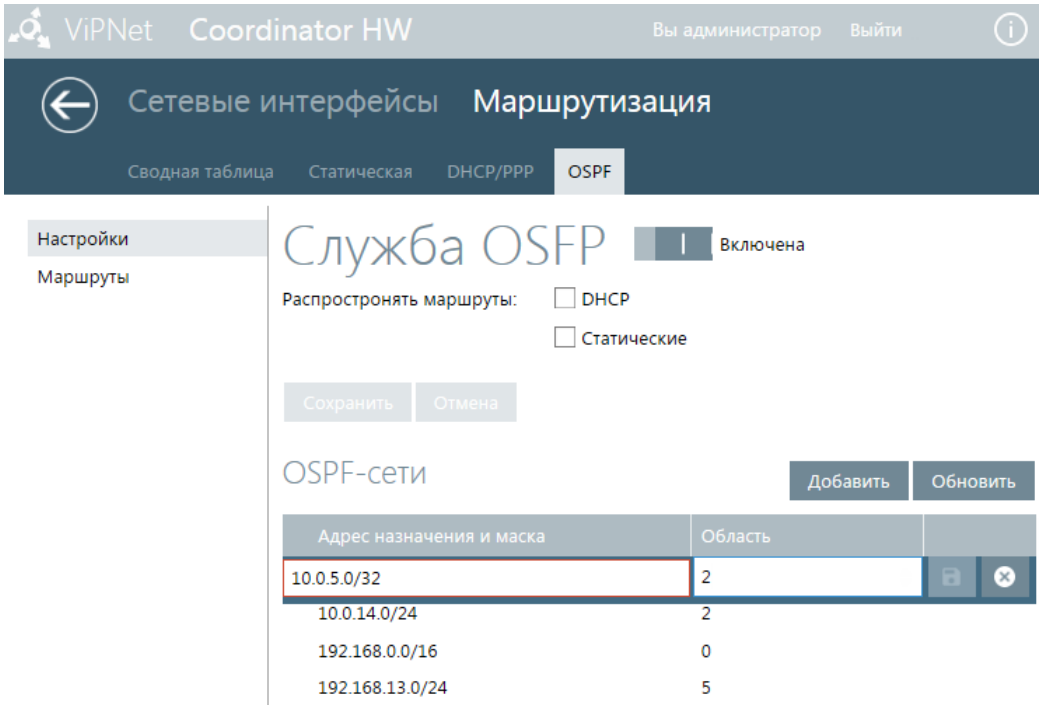


Рисунок 66. Настройка OSPF-протокола

5 Создайте следующие сетевые фильтры открытой сети:

- Фильтры, разрешающие входящий однонаправленный IP-трафик (unicast) и широковещательный (multicast) IP-трафик по протоколу OSPF от всех соседних OSPF-маршрутизаторов, с которыми взаимодействует ViPNet Coordinator HW:

Таблица 8. Фильтры для входящего OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Rule 1	<IP-адрес OSPF-маршрутизатора>	@local	IP:89	pass
Rule 2	<IP-адрес OSPF-маршрутизатора>	@multicast	IP:89	pass

Фильтры должны быть созданы для каждого соседнего OSPF-маршрутизатора в области, в которой находится ViPNet Coordinator HW.

Примечание. Если вы обновили ViPNet Coordinator HW с версии 4.1 и ниже, то системный объект `@OSPF` вам требуется создать вручную (см. «Группа протоколов» на стр. 71). В фильтрах вместо `@OSPF` вы также можете указать `proto 89`.

- Фильтр, разрешающий исходящий IP-трафик ViPNet Coordinator HW по протоколу OSPF от любого IP-адреса источника:

Таблица 9. Фильтры для исходящего OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Rule 3	@local	@any	IP:89	pass

Подробнее о создании сетевых фильтров см. в разделе Создание и изменение сетевого фильтра (на стр. 76).

Внимание! Если вы не настроите указанные фильтры, то ViPNet Coordinator HW не сможет работать по протоколу OSPF (см. «Общие сведения для работы по протоколу OSPF» на стр. 119).

Если впоследствии потребуется отказаться от использования протокола OSPF для маршрутизации, установите переключатель в положение **Отключена**.

Если в подсети прекращено использование протокола OSPF, удалите ее. Чтобы удалить подсеть, в строке рядом с ней щелкните значок  , после чего в появившемся окне сообщения нажмите кнопку **OK**.

Настройка перераспределения маршрутов

Протокол OSPF позволяет осуществлять перераспределение (redistribute) маршрутов (см. глоссарий, стр. 158). В каких случаях это может требоваться?

В одной разветвленной сети может быть образовано нескольких автономных систем (см. глоссарий, стр. 156) по причине использования в разных подсетях разных протоколов маршрутизации. Например, в одной подсети может использоваться статическая маршрутизация, в другой — динамическая маршрутизация по протоколу OSPF. В результате это образует две автономные системы. Чтобы системы могли взаимодействовать друг с другом, на маршрутизаторе, который установлен на границе этих систем, требуется настроить перераспределение маршрутов. В результате произойдет обмен маршрутной информацией, получаемой из этих систем, и они будут иметь связь друг с другом.

На рисунке ниже показана схема взаимодействия нескольких автономных систем.

Рисунок 67. Пример топологии сети с настроенным перераспределением маршрутов

В приведенном примере рассматривается 4 взаимодействующих подсети, 2 из которых входят в одну автономную систему, поскольку они работают по одному протоколу OSPF, остальные — в две другие автономные системы, поскольку они работают по протоколам Static и DHCP соответственно. При этом маршрутизатор 1 является граничным маршрутизатором (см. «Общие сведения для работы по протоколу OSPF» на стр. 119), поскольку он расположен на границе трех автономных систем. Чтобы маршрутизаторы 2 и 3 могли получить информацию о маршрутах, используемых на маршрутизаторах 4 и 5, и, соответственно, чтобы узлы сети филиала и сетей партнеров могли обмениваться IP-трафиком друг с другом, требуется настроить перераспределение маршрутов на маршрутизаторе 1. После настройки маршруты, полученные из сетей партнеров (от маршрутизаторов 4 и 5) на маршрутизаторе 1, будут передаваться на маршрутизатор 2, а с

маршрутизатора 2 — на маршрутизатор 3. В результате маршрутизатор 3 будет знать статические маршруты, прописанные в сети партнера 1, и маршруты, выдаваемые DHCP-сервером, в сети партнера 2.

Чтобы настроить параметры перераспределения маршрутов, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).

2 Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **OSPF**.

3 В разделе **Настройки** установите флажок в группе **Распространять маршруты**:

- **DHCP**, чтобы включить перераспределение маршрутов DHCP-сервера.
- **Статические**, чтобы включить перераспределение статических маршрутов.

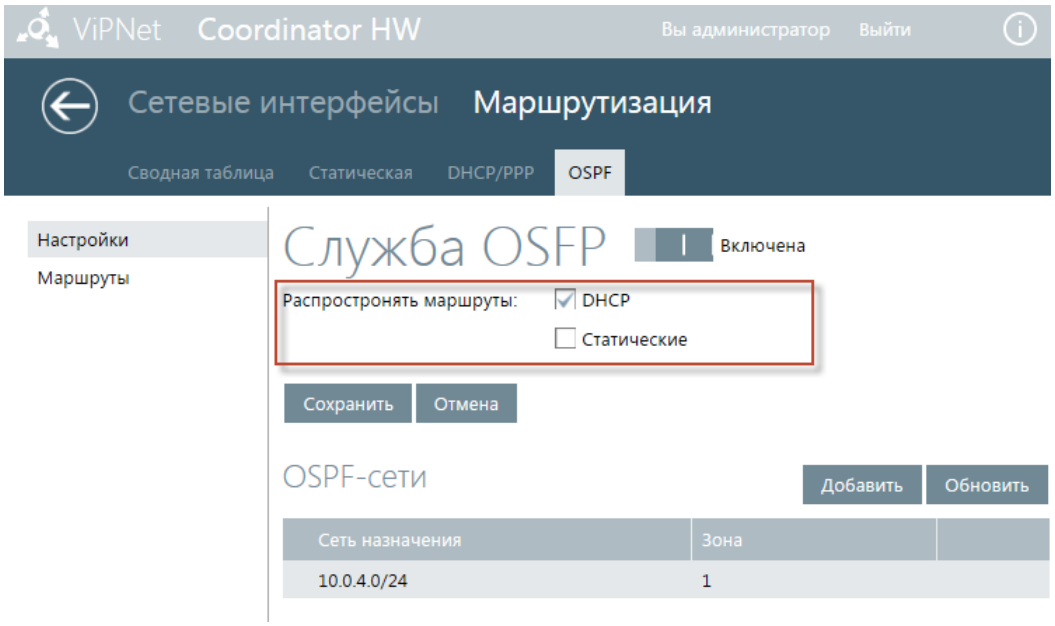


Рисунок 68. Включение перераспределения маршрутов DHCP-сервера

4 Чтобы выключить перераспределение маршрутов, снимите соответствующие флажки.

5 Нажмите кнопку **Сохранить**.

8

Мониторинг состояния ViPNet Coordinator HW и просмотр журнала IP-пакетов

Мониторинг состояния ViPNet Coordinator HW 136

Просмотр журнала регистрации IP-пакетов 138

Просмотр статистической информации об IP-пакетах 141

Мониторинг состояния ViPNet Coordinator HW

Вы можете следить за состоянием узла ViPNet Coordinator HW в режиме реального времени, просматривая графики загрузки процессора и оперативной памяти, время непрерывной работы, а также текущее состояние демонов и драйверов ViPNet Coordinator HW.

Примечание. Для демона системы защиты от сбоев failover на странице **Состояние системы** также отображается режим работы (одиночный режим или режим кластера горячего резервирования).

При работе в режиме кластера горячего резервирования графики загрузки процессора и оперативной памяти отображаются только для активного сервера кластера.

Чтобы просмотреть информацию о текущем состоянии ViPNet Coordinator HW, выполните следующие действия:

1. На начальной странице веб-интерфейса щелкните плитку **Мониторинг**.
2. На странице **Состояние системы** будет отображена информация о ViPNet Coordinator HW. На данной странице вы можете следить за изменением отображенных параметров.

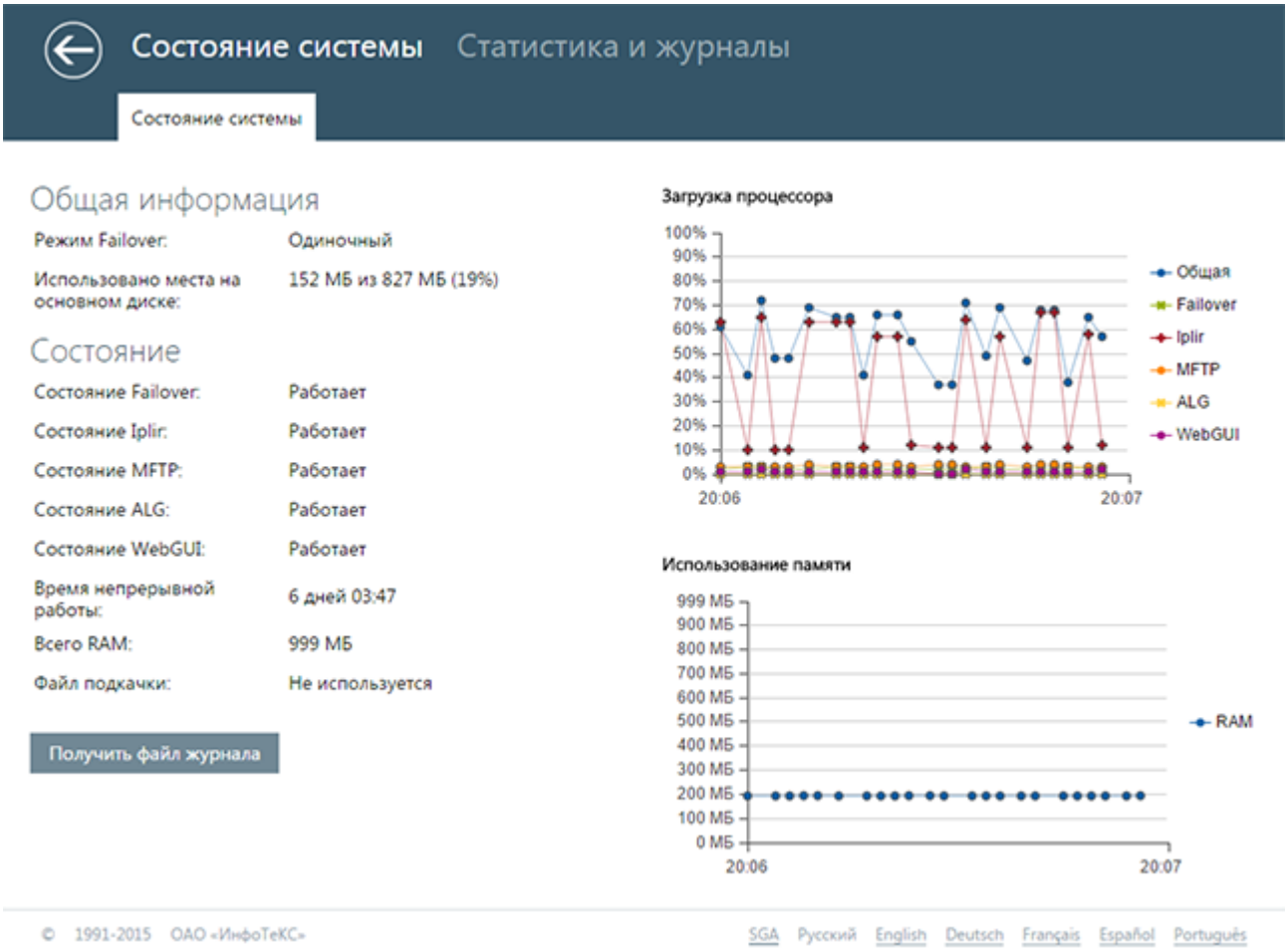


Рисунок 69. Мониторинг состояния ViPNet Coordinator HW

3 События, связанные с демонами, входящими в состав ViPNet Coordinator HW, записываются в журнал устранения неполадок ПО ViPNet. Этот журнал позволяет диагностировать правильность функционирования ПО. Он содержит большое количество деталей о процессах, происходящих внутри служб ViPNet Coordinator HW, и предназначен для разработчиков.

Чтобы загрузить архив с расширением `*.zip`, содержащий текстовый файл журнала устранения неполадок ПО ViPNet, нажмите кнопку **Получить файл журнала**.

Внимание! Загрузка архива журнала устранения неполадок доступна только в режиме администратора (см. «Режимы пользователя и администратора» на стр. 14).

Просмотр журнала регистрации IP-пакетов

Управляющий демон ViPNet Coordinator HW ведет журнал регистрации IP-пакетов, в который заносится информация обо всех IP-пакетах, проходящих через сетевые интерфейсы узла.

Чтобы просмотреть этот журнал, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet Coordinator HW в режиме администратора (см. «Подключение к веб-интерфейсу» на стр. 17).
2. На начальной странице веб-интерфейса щелкните плитку **Мониторинг** и перейдите на страницу **Статистика и журналы**. На вкладке **Журнал регистрации IP-пакетов** по умолчанию заданы параметры для просмотра записей обо всех IP-пакетов, прошедших через сетевые интерфейсы собственного узла за последний час (по умолчанию не более 100 записей). Чтобы просмотреть такие записи, нажмите кнопку **Найти**.
3. Чтобы выбрать записи из журнала регистрации IP-пакетов для просмотра, укажите следующие критерии поиска IP-пакетов:
   - В разделе **Признаки IP-пакетов** в соответствующих списках выберите:
     - сетевой интерфейс, через который проходят IP-пакеты (eth0, eth1 и так далее);
     - тип трафика, к которому относятся IP-пакеты (туннелируемый, транзитный защищенный, транзитный открытый, локальный защищенный или локальный открытый);
     - тип адреса IP-пакетов (одноадресный, широковещательный или групповой);
     - признак трансляции IP-пакетов (транслированные, не транслированные);
     - событие, к которому относятся IP-пакеты (блокированный, пропущенный или служебный);
     - протокол, с использованием которого передаются IP-пакеты (TCP, UDP, ICMP или другой).

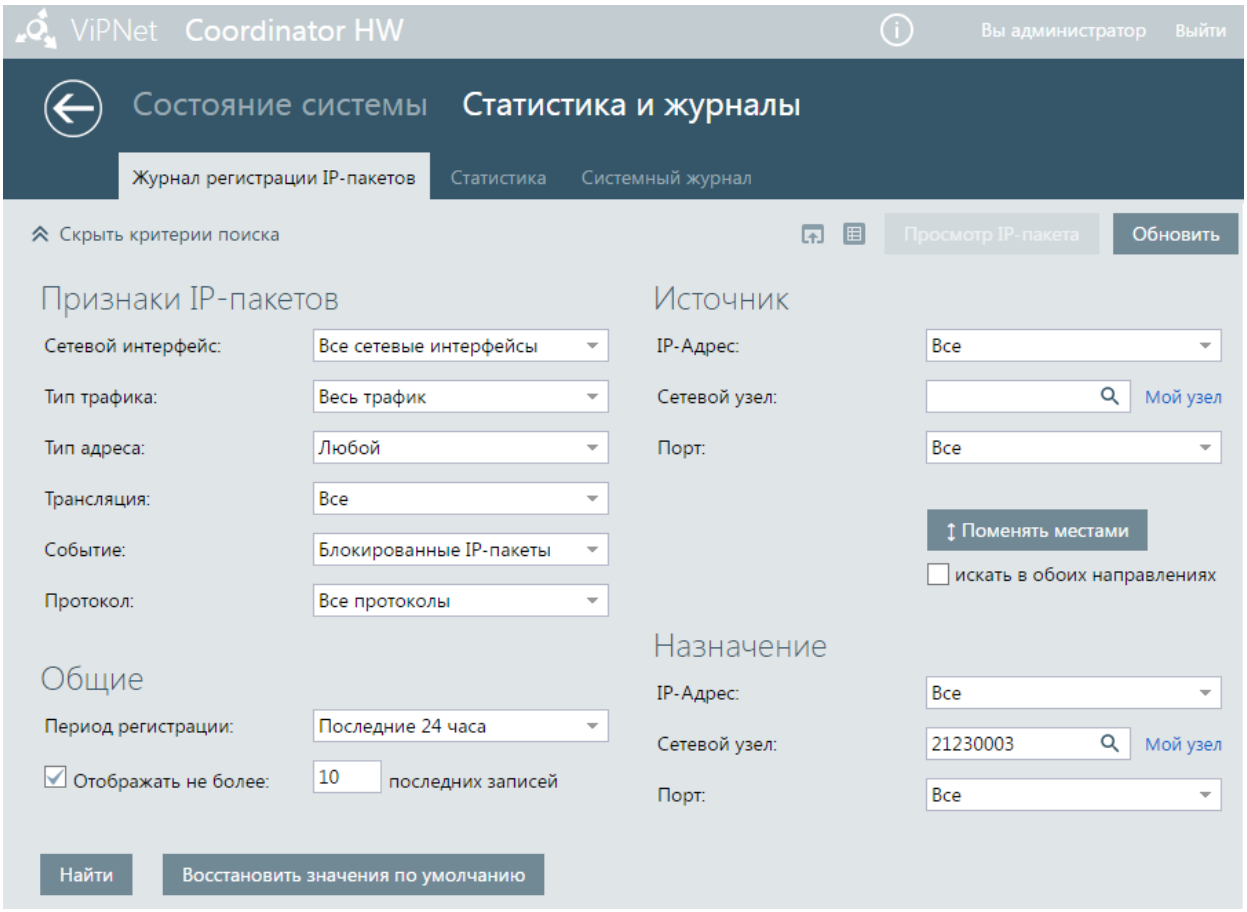


Рисунок 70. Задание критериев поиска IP-пакетов в журнале

- В разделе **Источник** (**Назначение**) в соответствующих полях укажите:
  - IP-адрес отправителя (получателя) или диапазон IP-адресов отправителей (получателей);
  - идентификатор сетевого узла;
  - номер порта отправителя (получателя).

Совет. В разделах **Источник** и **Назначение**:

- Чтобы указать идентификатор сетевого узла нажмите кнопку , в открывшемся окне выберите нужный узел в списке и нажмите кнопку **Далее**. Первым в этом списке отображается собственный узел.
- Чтобы поменять местами IP-адреса, сетевые узлы и порты отправителей и получателей, нажмите соответствующую кнопку.
- Чтобы одновременно просмотреть не только записи об IP-пакетах, переданных отправителем получателю, но и об IP-пакетах, переданных в обратном направлении, установите флажок **искать в обоих направлениях**.

- В разделе **Общие**:

- в поле **Период регистрации** укажите диапазон времени, за который вы хотите просмотреть информацию об IP-пакетах;
- чтобы ограничить число записей об IP-пакетах, отображаемое в результате поиска, установите соответствующий флажок и укажите это число.

Затем нажмите кнопку **Найти**. В результате на вкладке **Журнал регистрации IP-пакетов** отобразится список записей об IP-пакетах, отвечающих заданным критериям поиска.

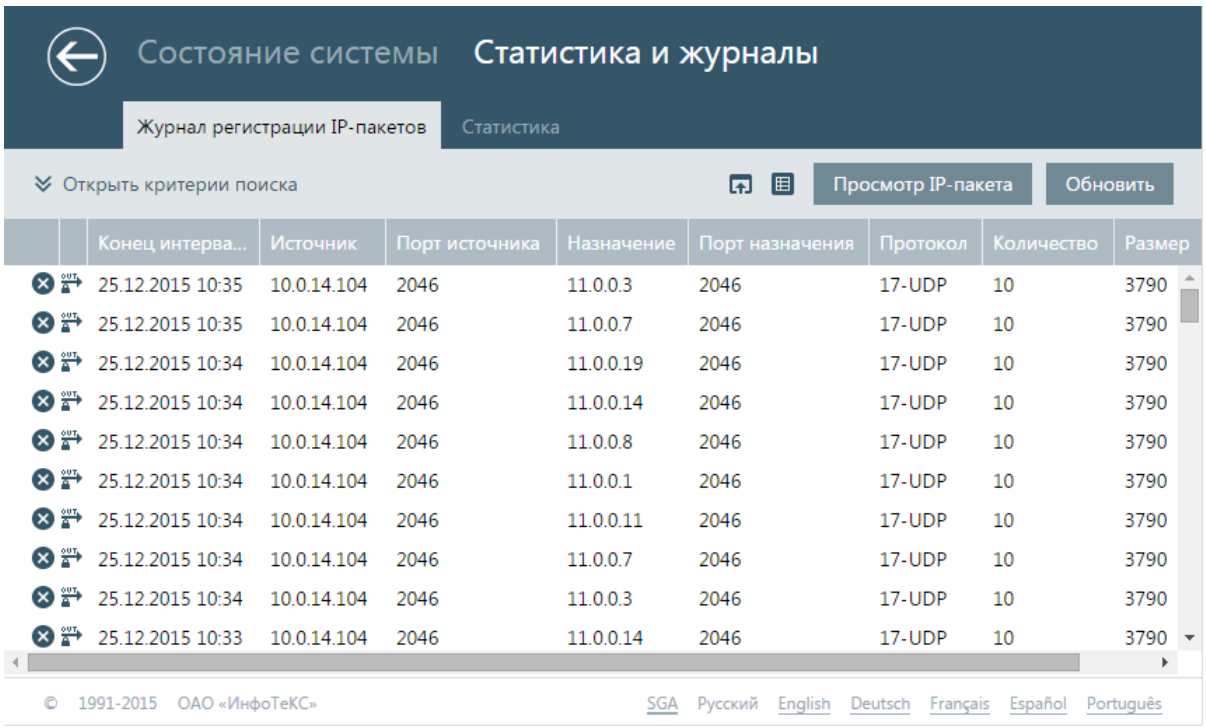
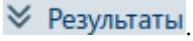


Рисунок 71. Просмотр записей в журнале регистрации IP-пакетов

4 Выполните одно из действий:

- Для просмотра подробной информации об IP-пакете дважды щелкните соответствующую запись в списке.
- Для экспорта списка найденных записей об IP-пакетах в файл формата XLS (например, для последующего анализа) на панели инструментов нажмите кнопку  .
- Для завершения просмотра списка найденных записей об IP-пакетах или изменения параметров поиска IP-пакетов в журнале на панели инструментов нажмите ссылку 

.

Просмотр статистической информации об IP-пакетах

Чтобы просмотреть статистическую информацию о количестве IP-пакетов, блокированных или пропущенных на узле, выполните следующие действия:

1 Перейдите на страницу **Мониторинг** > **Статистика и журналы** и выберите вкладку **Статистика**. В результате отобразится информация о количестве открытых, зашифрованных, широковещательных открытых и широковещательных зашифрованных IP-пакетах, прошедших через все сетевые интерфейсы узла.

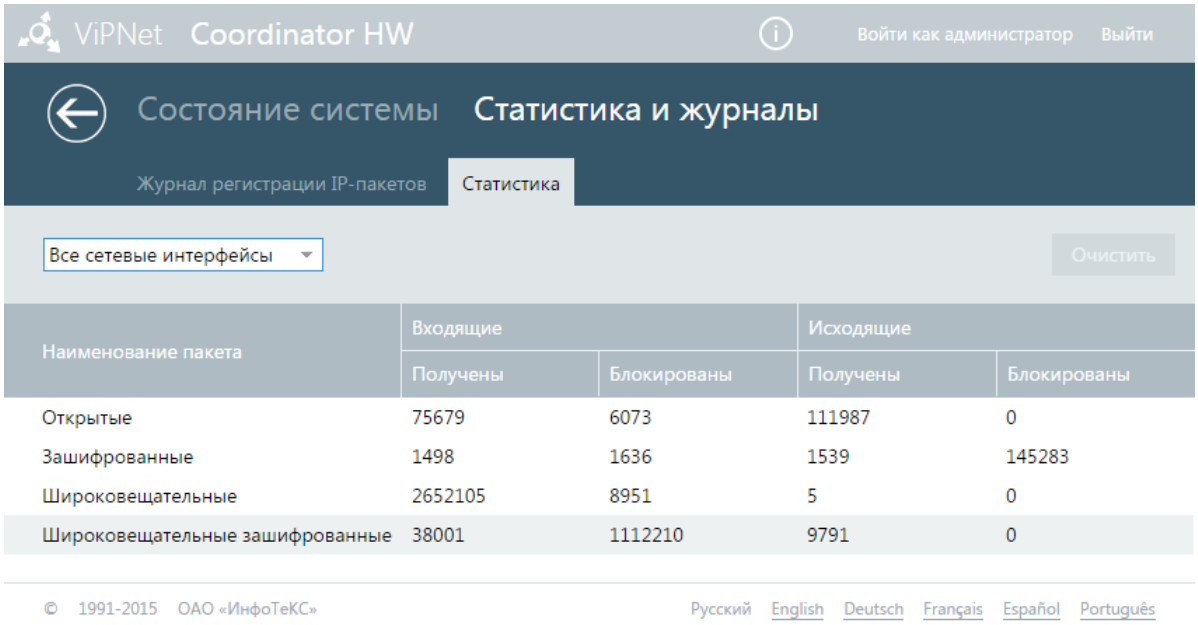


Рисунок 72. Просмотр информации о количестве IP-пакетов, прошедших через все сетевые интерфейсы ViPNet Coordinator HW

2 Чтобы просмотреть информацию о количестве IP-пакетов, прошедших через определенный сетевой интерфейс ViPNet Coordinator HW, выберите этот интерфейс в списке на панели инструментов.

Просмотр системного журнала

Чтобы просмотреть системный журнал ViPNet Coordinator HW, выполните следующие действия:

1. На начальной странице веб-интерфейса щелкните плитку **Мониторинг** и перейдите на страницу **Статистика и журналы**. На вкладке **Системный журнал** по умолчанию заданы параметры для просмотра записей о всех службах за все время работы ViPNet Coordinator HW.
2. Чтобы выбрать записи из системного журнала для просмотра, укажите следующие критерии поиска записей:
   - В разделе **Фильтр событий** выберите службу в соответствующем списке и введите текстовую строку для поиска. Нажмите кнопку **Применить фильтр**.
   - В разделе **Переход к времени** задайте дату и время, чтобы просмотреть записи журнала с указанного момента времени. Нажмите кнопку **Перейти**.

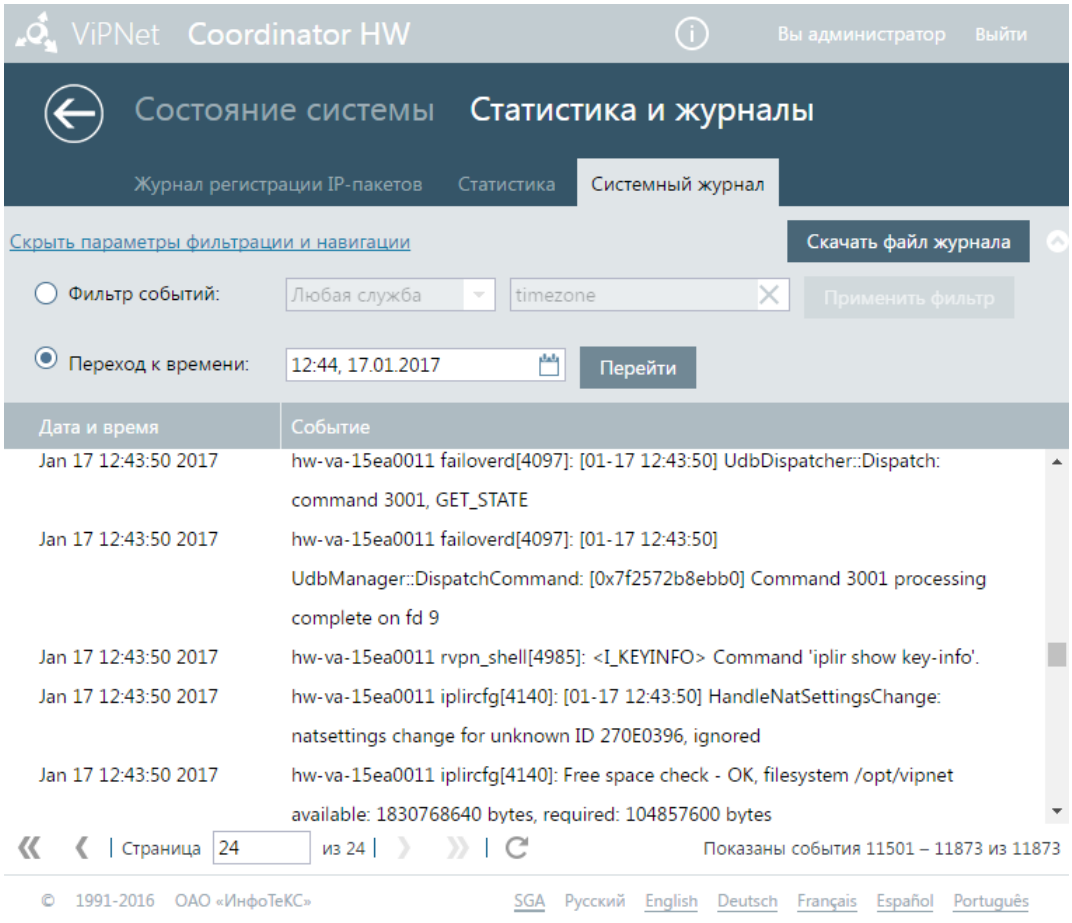


Рисунок 73. Просмотр записей в системном журнале

Сетевые фильтры по умолчанию

Сетевые фильтры, в том числе фильтры системы защиты от сбоев, создаваемые в ViPNet Coordinator HW по умолчанию, перечислены в таблицах ниже.

Таблица 10. Фильтры защищенной сети (vpn)

Название	Источник	Назначение	Протокол	Действие
В активном режиме кластера (нередактируемый)				
ViPNet Service	@any	@any	udp: from 2060 to 2060	pass
В пассивном режиме кластера (нередактируемый)				
Block all vpn traffic	@any	@any	@any	drop
Общие фильтры				
Allow DHCP service	@any	@any	udp: from 67 to 68, from 68 to 67	pass
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Allow ViPNet base services	@any	@any	udp: to 2046, from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet DBViewer	@any	@any	tcp: to 2047	pass
Allow ViPNet StateWatcher	@any	@local	tcp: to 5100, 10092	pass
Allow ViPNet MFTP	@any	@any	tcp: to 5000-5003	pass
Allow ViPNet WebGUI	@any	@local	tcp: to 8080	pass
Allow ViPNet SGA	@any	@local	tcp: to 10095, tcp: to 5103, tcp: to 10093	pass
Allow ICMP Ping	@any	@any	icmp8	pass
Allow SSH	@any	@any	tcp: to 22	pass
Allow DNS	@any	@any	udp: to 53	pass
Allow NTP	@any	@any	udp: to 123	pass

Название	Источник	Назначение	Протокол	Действие
Allow UPS service **Примечание.** В исполнении ViPNet Coordinator HW VA данный фильтр отсутствует.	@any	@any	tcp: to 3493	pass
Allow syslog outgoing	@local	@any	udp: to 514	pass
Allow SNMP	@any	@local	udp: to 161	pass
Allow SNMP traps	@local	@any	udp: to 162	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 11. Локальные фильтры открытой сети (`local`)

Название	Источник	Назначение	Протокол	Действие
В одиночном режиме системы защиты от сбоев, в активном и пассивном режимах кластера (нередактируемые)				
ViPNet Service CommonIn	@any	@local	tcp/udp: to 2046, 2047, 10095, 10096, 5100, 5103, 10092, 10093	drop
ViPNet Service CommonOut	@local	@any	tcp/udp: from 2046	drop
В активном режиме кластера (нередактируемые)				
Failover test IP	@local	<список значений параметров `testip` из `failover.ini`>	icmp	pass
Failover Channel	@local	iface <значение параметра `device` из `failover.ini`>	@any	pass
Failover Channel	<значение параметра `activeip` второго сервера из `failover.ini`>	iface <значение параметра `device` из `failover.ini`>	@any	pass
В пассивном режиме кластера (нередактируемые)				

Название	Источник	Назначение	Протокол	Действие
Failover Channel	@local	iface <значение параметра `device` из `failover.ini`>	@any	pass
Failover Channel	<значение параметра `activeip` второго сервера из `failover.ini`>	iface <значение параметра `device` из `failover.ini`>	@any	pass
ARP requests to active	@local	<список значений параметров `activeip` из `failover.ini`>	udp: to <значение `connect_port` из `failover.ini`>	pass
Block all local traffic	@any	@any	@any	drop
Общие фильтры				
Allow DHCP service	@any	@any	udp: from 67 to 68, from 68 to 67	pass
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Allow ICMP Ping	@local	@any	icmp8	pass
Allow DNS	@local	@any	udp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 12. Транзитные фильтры открытой сети (`forward`)

Название	Источник	Назначение	Протокол	Действие
В пассивном режиме кластера				
Block all forward traffic	@any	@any	@any	drop
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 13. Фильтры туннелируемых узлов (`tunnel`)

Название	Источник	Назначение	Протокол	Действие
В пассивном режиме кластера (нередактируемый)				
Block all tunnel traffic	@any	@any	@any	drop
Общий фильтр				
To all tunnel nodes	@any	@tunneledip	@any	pass
From all tunnel nodes	@tunneledip	@any	@any	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

A

Пользовательские группы протоколов по умолчанию

По умолчанию в ViPNet Coordinator HW настроены пользовательские группы протоколов, перечисленные в таблице ниже.

Таблица 14. Пользовательские группы протоколов, настроенные по умолчанию

Имя группы протоколов	Состав группы протоколов
DHCP	UDP:from 67-68 to 67-68
CITRIX	TCP:to 1494
DNS	UDP:to 53
FTP	TCP:to 21
GRE	IP:47
H323	TCP:to 1720
HTTP	TCP:to 80, TCP:to 8080
HTTP-Proxy	TCP:to 3128
HTTPS	TCP:to 443
IGMP	IP:2
IKE	UDP:to 500
IMAP	TCP:to 143
IPSecESP	IP:50

Имя группы протоколов	Состав группы протоколов
Kerberos	TCP:to 88, TCP:to 749, UDP:to 88, UDP:to 749
L2TP	UDP:to 1701
LDAP	TCP:to 389, UDP:to 389
LotusNotes	TCP:to 1352
MS-SQL	TCP:to 1433-1434, UDP:to 1433-1434
MySQL	TCP:to 3306
NetBIOS-DGM	UDP:from 138 to 138
NetBIOS-NC	UDP:from 137 to 137
NetMeeting	TCP:to 1503
NTP	UDP:to 123
PING	ICMP:8
POP3	TCP:to 110
Postgres	TCP:to 5432
PPTP	TCP:to 1723
RADIUS	UDP:to 1812-1813
RDP	TCP:to 3389
RTSP	TCP:to 554
SCCP	TCP:to 2000
SIP	TCP:to 5060, UDP:to 5060
SMTP	TCP:to 25
SNMP	UDP:to 161
SNMP-Traps	UDP:to 162
SSH	TCP:to 22
Syslog	UDP:to 514
Telnet	TCP:to 23
TFTP	UDP:to 69
UPnP	TCP:to 1900, TCP:to 2869, UDP:to 1900, UDP:to 2869
MFTP	TCP:to 5000-5003
StateWatcher	TCP:to 2047, TCP:to 5100, TCP:to 10092
ViPNetBase	UDP:to 2046, UDP:from 2048 to 2048, UDP:from 2050 to 2050
Cluster	UDP:from 2060 to 2060

Имя группы протоколов	Состав группы протоколов
ClusterMonitoring	UDP:from 2060 to 2065, UDP:from 2065 to 2060
SGA	TCP:to 5103, TCP:to 10093, TCP:to 10095
WindowsMobileDevices	TCP:to 990, TCP:to 999, TCP:to 5678, TCP:to 5721, TCP:to 26675
WindowsMobileDevices2	UDP:to 5679
VNC	TCP:to 5900
OSPF	IP:89

B

Типы событий в журнале регистрации IP-пакетов

Типы событий, регистрируемых в журнале IP-пакетов ViPNet Coordinator HW, можно поделить на следующие группы и подгруппы:

Рисунок 74. Классификация событий в журнале IP-пакетов

Описание типов событий каждой подгруппы приведено в таблицах.

*Таблица 15. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные сетевыми фильтрами защищенной сети***

Номер события	Описание события
1	Не найден ключ для передачи пакета сетевому узлу с идентификатором, указанным в пакете
2	Неверное значение имитозащитной вставки пакета. Защищенные данные или открытая информация в пакете были изменены при передаче
3	Входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет заблокирован фильтром защищенной сети
4	Слишком большой тайм-аут пакета, то есть время его отправки отличается от времени его получения на величину, большую указанной в соответствующей настройке
5	Входящий пакет отправлен сетевым узлом с версией драйвера ViPNet, не совместимой с версией драйвера ViPNet на сетевом узле получателя
7	Метод шифрования, код которого указан во входящем пакете, не поддерживается
8	Недопустимые параметры в расшифрованном пакете
9	IP-пакет блокирован главным фильтром защищенной сети
10	Неизвестен идентификатор сетевого узла отправителя пакета
13	Превышено максимальное время пребывания пакета в сети
14	Неверный адрес получателя пакета
15	Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов
16	Исчерпана лицензия на количество туннелируемых узлов
17	Неверный IP-адрес получателя
18	Неизвестный IP-адрес получателя
19	Подмена узла отправителя
70	Транзитный IP-пакет заблокирован фильтром защищенной сети

*Таблица 16. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные сетевыми фильтрами открытой сети***

Номер события	Описание события
20	Заблокирован открытый пакет
21	Идентификатор отправителя пакета неизвестен
22	От защищенного узла получен открытый пакет
23	От защищенного узла получен открытый широковещательный пакет

Номер события	Описание события
24	На порт, используемый одним из демонов ViPNet, получен открытый пакет
30	Локальный пакет заблокирован фильтром открытой сети
31	Транзитный пакет заблокирован фильтром открытой сети
32	Широковещательный пакет заблокирован фильтром открытой сети
33	Пакет заблокирован фильтром антиспуфинга
37	Пакет заблокирован фильтром туннелируемых ресурсов
39	Пакет заблокирован фильтром по умолчанию при загрузке компьютера

*Таблица 17. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные по другим причинам***

Номер события	Описание события
80	Размер заголовка IP-пакета меньше допустимого
81	Недопустимая версия протокола IP (поддерживается только IPv4)
82	Длина заголовка IP-пакет меньше допустимой
83	Длина IP-пакета меньше указанной в IP-заголовке
84	Значение контрольной суммы в заголовке IP-пакета отличается от ее значения в IP-пакете
85	Размер TCP-заголовка меньше допустимого
86	Размер UDP-заголовка меньше допустимого
87	Обработаны не все фрагменты IP-пакета
88	Широковещательный адрес отправителя в IP-пакете
89	Перекрытие фрагментов IP-пакета. Наиболее устаревший из перекрываемых фрагментов IP-пакета отброшен
90	IP-пакет не был обработан, так как для его обработки недостаточно вычислительных ресурсов
91	IP-пакет получен во время инициализации драйвера ViPNet
92	Размер IP-пакета превышает 48 Кбайт
93	По истечении допустимого времени получены не все фрагменты IP-пакета
95	Получены два IP-пакета от узлов с разными IP-адресами и одинаковыми идентификаторами
99	Заблокирован фрагментированный IP-пакет

Номер события	Описание события
101	Транзитный IP-пакет не может быть маршрутизирован
102	Прикладной пакет не обработан, так как не загружен модуль обработки на прикладном уровне
103	Количество установленных соединений превышает допустимое значение, заданное в соответствующих настройках
104	Соединение заблокировано, так как параметры исходящих пакетов (socketpair) для этого соединения совпадают с такими параметрами для ранее установленного соединения
105	Не удалось выделить динамический порт для правила трансляции адресов (в пуле нет свободных портов)
111	Не найден ключ обмена
112	Неверное значение имитозащитной вставки в незашифрованном пакете версии 4.2
113	Неизвестный идентификатор сетевого узла отправителя
115	Не удалось найти маршрут для IP-пакета в таблице маршрутизации
116	Не найден сетевой адаптер
117	Не удалось определить MAC-адрес получателя пакета по его IP-адресу
118	Ошибка при шифровании исходящего IP-пакета для защищенного узла
119	Получен зашифрованный IP-пакет неизвестного формата, который не может быть расшифрован
120	Ошибка при отправке IP-пакета защищенному узлу из-за проблем с доступом к этому узлу
121	Ошибка в работе кластера горячего резервирования
122	Получен IP-пакет неизвестного протокола канального уровня
130	Отсутствуют свободные динамические порты, необходимые для создания соединения
131	Ошибка обработки прикладных протоколов: не удалось построить маршрут
132	Ошибка обработки прикладных протоколов: отсутствуют свободные динамические порты UDP
133	Ошибка обработки прикладных протоколов: порты источника и назначения IP-пакета принадлежат разным прикладным сервисам
134	Ошибка обработки прикладных протоколов: ошибка в таблице соответствия между прикладными сервисами и сетевыми протоколами, портами
137	Шифрование исходящего IP-пакета с использованием данного алгоритма запрещено (тесты алгоритма не прошли)

*Таблица 18. События группы **Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные зашифрованные IP-пакеты***

Номер события	Описание события
40	Пропущен зашифрованный IP-пакет
41	Пропущен зашифрованный широковещательный IP-пакет
44	Маршрутизация зашифрованного транзитного IP-пакета с подменой адреса получателя
45	Пакет пропущен на туннелирующем координаторе, так как он поступил от туннелируемого узла или предназначен для такого узла

*Таблица 19. События группы **Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные незашифрованные IP-пакеты***

Номер события	Описание события
60	Пропущен незашифрованный IP-пакет
61	Пропущен незашифрованный широковещательный IP-пакет
62	Пропущен незашифрованный транзитный IP-пакет
63	IP-пакет пропущен фильтром для туннелируемых ресурсов
64	IP-пакет пропущен при запуске операционной системы
65	Пропущен зашифрованный IP-пакет для незарегистрированного узла ViPNet

*Таблица 20. События группы **Все IP-пакеты/Служебные события***

Номер события	Описание события
42	Изменился IP-адрес сетевого узла
46	Изменились параметры доступа к сетевому узлу
47	Истек интервал отправки IP-пакетов, передаваемых сетевым узлом своему серверу соединений. Событие может возникать только для тех узлов, которые работают через межсетевой экран с динамической трансляцией адресов
48	Узел доступен по широковещательному адресу
49	Изменился IP-адрес собственного сетевого узла
110	Новый IP-адрес сетевого узла зарегистрирован на DNS-сервере
114	DNS-имя узла не зарегистрировано на DNS-сервере

Глоссарий

DHCP-сервер

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

DNS-сервер

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

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

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.

NTP-сервер

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

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

OSPF (Open Shortest Path First)

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

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.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу узлов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет узлам группироваться вместе, даже если они не находятся в одной физической сети.

Автономная система

Один или несколько сегментов сети, в которых осуществляется маршрутизация по одному протоколу (OSPF, IGRP, EIGRP, IS-IS, RIP, BGP, Static). Также может трактоваться как домен маршрутизации — группа маршрутизаторов сети, работающих по одинаковым протоколам маршрутизации.

Агрегированный сетевой интерфейс

Логический сетевой интерфейс (см. глоссарий, стр. 159), образованный из нескольких физических интерфейсов Ethernet, объединенных на канальном уровне сетевой модели OSI.

Административная дистанция

Характеристика маршрута (см. глоссарий, стр. 158). Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

Вес

Параметр, который задается для шлюза в статическом маршруте (см. глоссарий, стр. 158) в виде целого числа в диапазоне от 1 до 255. Позволяет настроить балансировку IP-трафика между шлюзами в одинаковый адрес назначения. Определяет долю IP-трафика, который должен передаваться по маршруту на указанный шлюз.

Домен коллизий

Часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети.

Сеть Ethernet, построенная на повторителях, всегда образует один домен коллизий. Мосты, коммутаторы и маршрутизаторы делят сеть Ethernet на несколько доменов коллизий.

Защищенный IP-трафик

Поток IP-пакетов, зашифрованных с помощью программного обеспечения ViPNet.

Класс сетевого интерфейса

Признак, определяющий назначение сетевого интерфейса. В ViPNet Coordinator HW интерфейсам можно назначить следующие классы: `access`, `trunk`, `slave`.

По умолчанию сетевому интерфейсу назначен класс `access`. Если требуется, чтобы интерфейс Ethernet или агрегированный интерфейс обрабатывал трафик из нескольких VLAN, ему необходимо назначить класс `trunk`. Чтобы объединить несколько интерфейсов Ethernet в агрегированный интерфейс, каждому из таких интерфейсов необходимо предварительно назначить класс `slave`.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных серверов ViPNet Coordinator HW, один из которых (активный) выполняет функции координатора сети ViPNet, а другой сервер (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet на активном сервере, пассивный сервер переключается в активный режим для выполнения функций сбойного сервера. При этом сбойный сервер перезагружается и становится пассивным.

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.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Маршрут

Путь следования IP-трафика при передаче в сети от одного узла другому.

Маршрут по умолчанию

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

Маршрутизатор-сосед

OSPF-маршрутизатор, находящиеся в одной области маршрутизации с другими маршрутизаторами этого типа.

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.

Область маршрутизации

Одна или несколько IP-сетей, в которых осуществляется обмен информацией по определенному протоколу, в частности, по протоколу OSPF (см. глоссарий, стр. 156).

Протокол OSPF рассматривает межсетевую среду как множество областей, соединенных друг с другом через некоторую базовую область (backbone area). Для идентификации областей каждой из них выделяется специальный идентификатор (area ID), представляющий собой 32-разрядное число, которое записывается так же, как и IP-адрес — в десятично-точечном формате (в виде четырех однобайтовых чисел, разделенных точками).

Открытый трафик

Поток незашифрованных IP-пакетов.

Перераспределение маршрутов

Обмен маршрутной информацией между двумя различными маршрутизирующими протоколами.

Персональный ключ пользователя

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

Прозрачный режим работы прокси-сервера

Режим работы, при котором не требуется выполнять настройку программного обеспечения на рабочих местах пользователей, подключающихся к Интернету через прокси-сервер.

Прокси-сервер

Программа, транслирующая соединения по некоторым протоколам из внутренней сети во внешнюю и выступающая при этом как посредник между клиентами и сервером.

Публичный адрес

IP-адрес, который может применяться в Интернете.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN (см. глоссарий, стр. 156).

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

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).

Стоимость маршрута

Количество издержек, которые возникнут при отправке IP-пакета в сеть назначения через тот или иной шлюз. Стоимость маршрута обратно пропорциональна его пропускной способности канала связи.

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных в сети.

Трансляция сетевых адресов (NAT)

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

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.

Частный адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к Интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в Интернете. Чтобы выйти в Интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

Шлюз

Устройство, предназначенное для соединения двух сетей с разными канальными протоколами. Перед передачей данных из одной сети в другую шлюз их преобразует, обеспечивая совместимость протоколов.

Указатель

L

L2OverIP - 48

M

MIME-тип - 105, 107

O

OSPF (Open Shortest Path First) - 113, 125, 158

V

ViPNet Policy Manager - 59, 61
ViPNet Центр управления сетью (ЦУС) - 13, 43
VLAN - 28, 51, 133, 159

A

Автономная система - 119
Агрегированный сетевой интерфейс - 36
Административная дистанция - 121, 126

B

Вес - 122, 123

Г

Группа IP-адресов - 66, 76, 77, 88
Группа протоколов - 66, 77, 88, 132
Группа расписаний - 66, 77
Группа сетевых интерфейсов - 66, 76, 77
Группа сетевых узлов ViPNet - 66, 76, 77

Д

Добавление статических маршрутов - 123
Домен коллизий - 48

И

Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола - 25, 29, 32, 35, 38, 128
Использование агрегированных сетевых интерфейсов - 24, 127

К

Класс сетевого интерфейса - 24
Кластер горячего резервирования - 59
Клиент (ViPNet-клиент) - 43, 62
Ключ защиты - 19

М

Маршрут - 113, 157
Маршрут по умолчанию - 128
Машрутизатор-сосед - 119
Метрика маршрута - 127

Мониторинг состояния ViPNet Coordinator HW - 15

Н

Назначение дополнительных IP-адресов - 26
Настройка административной дистанции для маршрутов DHCP-сервера - 121, 125
Настройка антивируса - 102, 103
Настройка балансировки IP-трафика - 122
Настройка маршрутизации - 14, 25
Настройка метрики для маршрутов DHCP-сервера - 25, 29, 32, 38, 125
Настройка метрики для маршрутов PPP-протокола - 35
Настройка основных параметров прокси-сервера - 102
Настройка параметров DHCP-сервера - 96
Настройка параметров DNS-сервера - 100
Настройка параметров динамических маршрутов от DHCP/PPP-протокола - 25, 29, 32, 38
Настройка параметров динамической маршрутизации по протоколу OSPF - 126
Настройка параметров точки доступа к сети Wi-Fi - 33
Настройка подключения к сети - 14
Настройка сетевых интерфейсов Ethernet - 125, 127
Настройка сетевых служб - 14
Настройка статической маршрутизации - 126
Настройка фильтрации содержимого трафика - 102, 103

О

Область маршрутизации - 119, 130, 131
Общее описание технологии L2OverIP - 51
Общие сведения для работы по протоколу OSPF - 132, 133
Общие сведения о сетевых фильтрах - 56, 61
Организация защиты соединения между удаленными сегментами сети на канальном уровне модели OSI - 49
Организация обработки трафика из нескольких VLAN - 24, 37, 51, 127

П

Перераспределение маршрутов - 131, 133
Персональный ключ пользователя - 19
Подключение к беспроводной сети Wi-Fi - 111, 127
Подключение к веб-интерфейсу - 15, 20, 22, 24, 27, 28, 31, 34, 36, 46, 51, 65, 76, 79, 80, 88, 91, 94, 96, 99, 103, 106, 108, 109, 121, 126, 127, 129, 131, 134, 138
Подключение к мобильной сети 3G, 4G - 125, 128
Пользовательские группы объектов по умолчанию - 61
Пользовательские группы протоколов по умолчанию - 63
Принципы формирования таблиц маршрутизации в ViPNet Coordinator HW - 117, 122, 123, 124, 127
Проверка соединения с сетевым узлом ViPNet - 14, 44
Прозрачный режим работы прокси-сервера - 103
Просмотр групп объектов - 14, 61, 63
Просмотр журнала регистрации IP-пакетов - 15
Просмотр и изменение списка туннелируемых узлов - 15
Просмотр информации о сетевых узлах ViPNet - 14
Просмотр общей таблицы маршрутизации - 14
Просмотр правил трансляции адресов - 14
Просмотр сетевых фильтров - 14
Просмотр статистической информации об IP-пакетах - 15
Публичный адрес - 83

Р

Режимы пользователя и администратора - 18, 137

С

Сетевой интерфейс - 83, 156
Сетевой фильтр - 56, 59
Сетевые фильтры по умолчанию - 59
Создание и изменение группы объектов - 14
Создание и изменение правила трансляции адресов - 14, 69, 72, 74
Создание и изменение сетевого фильтра - 14, 52, 61, 67, 69, 70, 72, 74, 105, 109, 132

Стоимость маршрута - 119

Т

Типы событий в журнале регистрации IP-пакетов - 101
Трансляция адреса источника - 83, 84
Трансляция адреса назначения - 83
Трансляция сетевых адресов (NAT) - 61, 87
Туннелирование - 46, 75

У

Узел сети ViPNet - 59

Ч

Частный адрес - 83