ViPNet Coordinator HW 4

Настройка с помощью веб-интерфейса

Версия продукта: 4.5.8

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

infotecs

ФРКЕ.00130-03 90 05

Версия продукта 4.5.8, документ обновлен 08.07.2025

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В документе описаны основные сценарии настройки ViPNet Coordinator HW с помощью веб-интерфейса, а также работа с журналами ViPNet Coordinator HW.

Настройка ViPNet Coordinator HW производится в режиме администратора. Просматривать настройки можно в режиме пользователя. В сценариях настройки опущен шаг аутентификации в режиме администратора. Подробнее см. в разделе Подключение к веб-интерфейсу.

Соглашения документа

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

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

Общие сведения о ViPNet Coordinator HW

ViPNet Coordinator HW — программно-аппаратный комплекс, который выполняет функции VPN-шлюза в сети ViPNet.

ViPNet Coordinator HW обеспечивает безопасную передачу данных между защищенными сегментами сети ViPNet, а также фильтрует IP-трафик. Он выполняет роль координатора в сети ViPNet. Роль назначается администратором сети.

Кроме аппаратных исполнений ViPNet Coordinator HW поставляется в виртуализированном исполнении ViPNet Coordinator VA, которое разворачивается на платформе виртуализации.

Описание всех функций и исполнений ViPNet Coordinator HW см. в документе «Подготовка к работе».

Обратная связь

Контактная информация

- Единый многоканальный телефон:

  +7 (495) 737-6192,

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

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телеграм-канал поддержки: t.me/vhd21

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

- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

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

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

1

Начало работы

Требования к рабочему месту

- Подключайтесь только с других защищенных узлов ViPNet, связанных с ViPNet Coordinator HW. Связи между узлами сети ViPNet задаются в ViPNet ЦУС или Prime.

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

- Браузер: Microsoft Edge, Google Chrome и Firefox последних версий.
- В настройках браузера разрешите Cookie и JavaScript, добавьте сайт в надежные расположения.
- Разрешение экрана 1360x768 пикселей или выше.
- Во избежание неполадок при подключении к веб-интерфейсу после обновления ПО ViPNet Coordinator HW очистите кеш браузера.

Внимание! 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 вы не сможете подключиться.

Режимы пользователя и администратора

Таблица 1. Доступные действия в режимах пользователя и администратора

Действие	Режим пользователя	Режим администратора
Настройка подключения к сети: • 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	+	+
Создание и изменение сетевых фильтров	–	+
Просмотр правил трансляции адресов	+	+
Создание и изменение правил трансляции адресов	–	+
Просмотр групп объектов	+	+
Создание и изменение групп объектов	–	+
Настройка сетевых служб: • настройка DHCP, DNS, NTP и прокси-сервера; • настройка точки доступа к сети Wi-Fi; • настройка функциональности L2OverIP.	–	+
Просмотр общей таблицы маршрутизации (см. Просмотр таблицы маршрутизации)	+	+
Настройка маршрутизации	–	+
Просмотр сведений о сетевых узлах ViPNet	+	+
Настройка видимости узлов	–	+
Просмотр и изменение списка туннелируемых узлов	+	+
Настройка туннелирования локальных адресов	–	+
Мониторинг состояния ViPNet Coordinator HW	+	+
Просмотр системного журнала	–	+
Экспорт диагностической информации	–	+

Действие	Режим пользователя	Режим администратора
Просмотр журнала транспортных конвертов (MFTP)	–	+
Просмотр журнала регистрации IP-пакетов	–	+
Просмотр статистической информации об IP-пакетах	+	+

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 будет прерван.

Подключение к веб-интерфейсу

Доступ к веб-интерфейсу ViPNet Coordinator HW выполняется по протоколу HTTPS. Подключение производится с использованием самоподписанного сертификата, который генерируется при инициализации ViPNet Coordinator HW. Вы можете настроить подключение по протоколу HTTPS, используя сертификат, выданный центром сертификации.

Чтобы подключиться к веб-интерфейсу:

1 В браузере введите `https://<IP-адрес>:<tcp-порт>`.

Примечание. IP-адрес узла ViPNet Coordinator HW можно посмотреть в списке защищенных узлов программы ViPNet Client, установленной на вашем узле.
TCP-порт по умолчанию — 8080, его можно изменить из командного интерпретатора.

2 В окне аутентификации введите пароль пользователя сетевого узла ViPNet Coordinator HW.

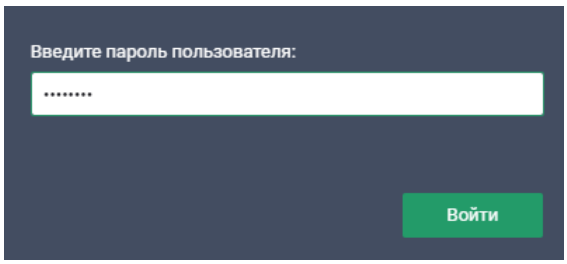

Рисунок 1. Аутентификация пользователя

Примечание. Для предотвращения подбора пароля методом перебора в ViPNet Coordinator HW реализована прогрессивная задержка ввода пароля. После трех неудачных попыток аутентификации возможность ввода пароля станет доступна через 3 секунды, а каждая последующая ошибка увеличит эту задержку. Счетчик ошибок сбрасывается при успешном вводе пароля, а также после десятой ошибки. Перезагрузка ViPNet Coordinator HW не сбрасывает счетчик ошибок.
Все неудачные попытки ввода пароля автоматически записываются в системный журнал.

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 изменить настройки, войдите в режим администратора:

1 В правом верхнем углу страницы в списке **Режим пользователя** выберите **Режим администратора**.

2 Введите пароль администратора данного сетевого узла или администратора группы сетевых узлов ViPNet.

В режиме администратора возможен только один сеанс работы с ViPNet Coordinator HW в веб-интерфейсе или командной строке. Чтобы принудительно прервать сеанс работы другого администратора, установите соответствующий флажок. Иначе ваш переход в режим администратора будет отклонен.

3 Нажмите **Войти**.

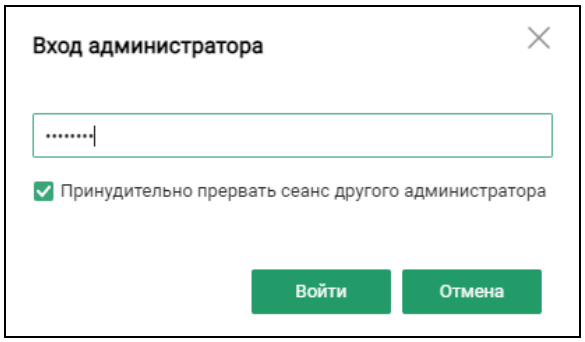

Рисунок 2. Вход в режим администратора

Примечание. Если на ViPNet Coordinator HW истекают или уже истекли сроки действия персонального ключа пользователя или ключа защиты ключей обмена, то в веб-интерфейсе появится соответствующее сообщение. В этом случае требуется обновить ключи. Подробнее см. в документе «Настройка с помощью командного интерпретатора», в разделе «Обновление ключей при истечении срока их действия».

На ViPNet Coordinator HW могут авторизоваться три типа администраторов:

- администратор сетевого узла ViPNet Coordinator HW;
- администратор группы сетевых узлов ViPNet;
- администратор сети ViPNet.

Внимание! По окончании работы всегда завершайте сеанс: нажмите **Режим пользователя** или **Режим администратора**, затем **Выйти**. Иначе, даже при закрытии вкладки или окна браузера сессия будет активна в течение 15 минут или пока ее не закроет другой пользователь.

Автоматическое завершение сеанса работы

Сеанс работы с веб-интерфейсом завершается автоматически в двух случаях:

- По истечении максимального времени бездействия (по умолчанию 15 минут).
- При обнаружении попытки межсайтовой подделки запроса.

Режим ограниченной функциональности

При выключении одной или нескольких служб ViPNet Coordinator HW веб-интерфейс автоматически переходит в режим ограниченной функциональности. При этом появляется соответствующее сообщение.

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

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

- В случае завершения работы службы `iplircfg` блокируются разделы **Журнал IP-пакетов**, **Статистика** (статистика IP-пакетов), **Управляющие соединения**, **Сетевые фильтры** , **Трансляция адресов (NAT)** и **Группы объектов**.
- В случае завершения работы службы `failoverd` в разделе **Журналы** > **Состояние системы** не отображается информация о работе системы.
- В случае завершения работы службы `mftpd` блокируется раздел **Журналы** > **Журнал MFTP**.

Также веб-интерфейс переходит в ограниченный режим:

- При работе ViPNet Coordinator HW в режиме кластера горячего резервирования. В этом случае раздел **Сетевые интерфейсы** доступен только для просмотра.
- В процессе обновления справочников и ключей, поступивших из ViPNet ЦУС или Prime.

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

2

Настройка системных параметров

Настройка даты и времени

Внимание! Настройте корректные дату и время, иначе защищенные соединения с другими узлами ViPNet могут блокироваться.

1 Выберите **Системные настройки** > **Общие** > **Дата и время**.

2 Укажите часовой пояс, дату и время.

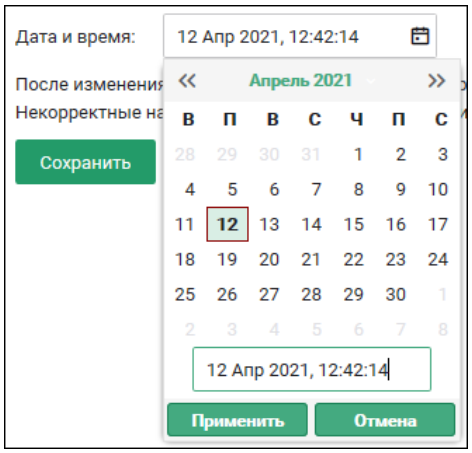

Рисунок 3. Задание даты и времени

3 Нажмите **Сохранить**.

Чтобы измененные настройки вступили в силу, завершите сеанс работы и подключитесь к веб-интерфейсу заново.

Установка серийного номера

Начиная с версии 4.5.6 ПО ViPNet Coordinator HW поддерживает серийные номера устройства для исполнений на аппаратных платформах. Для новых устройств номер устанавливается на производстве и не может быть изменен. Для устройств с ПО, обновленных пользователем, установите номер вручную в соответствии с указанным на этикетке устройства.

Примечание. Серийный номер указан на этикетке infotecs, которая находится на корпусе устройства, а также записан в формуляр. Если серийный номер был утерян обратитесь в службу поддержки ИнфоТеКС.

Серийный номер может быть длиной 8–9 символов и содержать арабские цифры: 0–9. Серийный номер имеет формат XXX-XXXXX(X), тире устанавливается автоматически.

Используйте серийный номер:

- При обращении в службу поддержки ИнфоТеКС.
- Для инвентаризации оборудования: серийный номер доступен по SNMP (OID .1.3.6.1.4.1.10812.1.10.1. в VIPNET-MIB).

Чтобы добавить серийный номер вручную:

1 В правой верхней части страницы нажмите .

Рисунок 4. Серийный номер не задан

2 Установите серийный номер:

2.1 Нажмите .

2.2 Укажите серийный номер.

2.3 Нажмите .

Внимание! Серийный номер можно редактировать, только если он не был установлен при производстве.

Перезагрузка ViPNet Coordinator HW

Вы можете удаленно перезагрузить ViPNet Coordinator HW, а также настроить перезагрузку по расписанию:

1 Выберите **Системные настройки** > **Сервисные функции** > **Управление устройством.**

2 Для перезагрузки нажмите **Перезагрузить**. В ответ на запрос подтверждения перезагрузки нажмите **OK**.

3 Для настройки перезагрузки по расписанию:

3.1 Включите **Перезагружать устройство по расписанию**.

3.2 Настройте расписание и нажмите **Сохранить**.

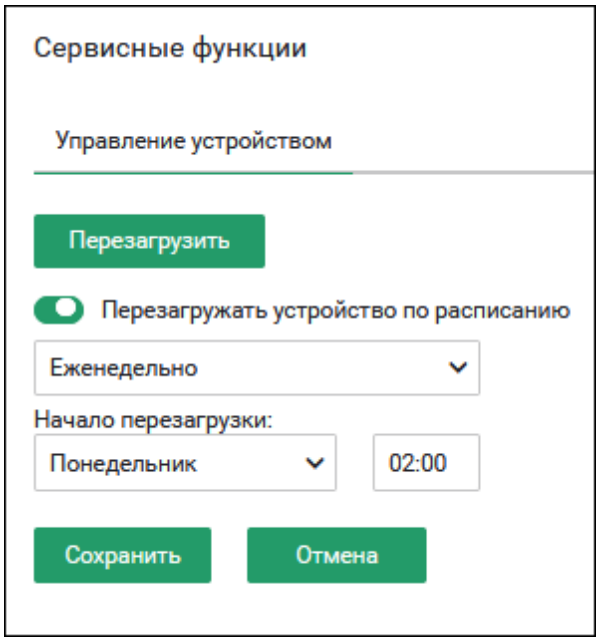

Рисунок 5. Перезагрузка ViPNet Coordinator HW

После перезагрузки соединение с ViPNet Coordinator HW через веб-интерфейс будет разорвано. Повторно подключитесь.

Настройка перезагрузки в кластере горячего резервирования

При работе ViPNet Coordinator HW в режиме кластера горячего резервирования расписание перезагрузки (дата и время) не синхронизируется между узлами кластера.

Настройку автоматической перезагрузки выполняйте в следующем порядке:

1 Настройте расписание перезагрузки на активном узле кластера.

2. Дождитесь, когда данные на активном и пассивном узле синхронизируются (по умолчанию — 60 секунд).
3. Подключитесь к командному интерпретатору пассивного узла кластера и проверьте настройки автоматической перезагрузки. Автоматическая перезагрузка должна быть включена. Если настройки не синхронизировались, проверьте настройки позже.
4. Настройте время и дату перезагрузки на пассивном узле. Чтобы не допустить одновременной перезагрузки обоих узлов кластера, устанавливайте время перезагрузки на узлах с разницей не менее 30 минут.

Подробнее см. документ «Настройка с помощью командного интерпретатора» раздел «Настройка расписания перезагрузки».

Управление ключами локального SSH-сервера

SSH-ключи используются для аутентификации при подключении к ViPNet Coordinator HW по протоколу SSH. SSH-ключи создаются при установке дистрибутива ключей.

В случае компрометации SSH-ключей или изменения политики безопасности, вы можете их перевыпустить:

1 Выберите **Системные настройки** > **Общие** > **SSH**.

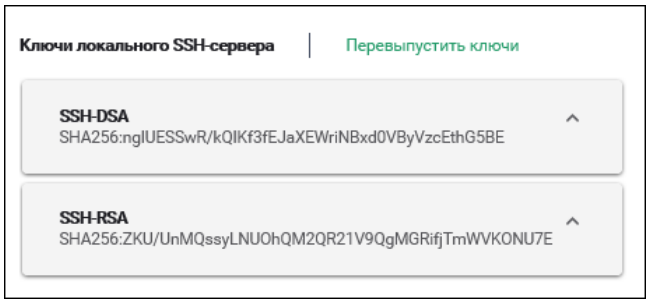

Рисунок 6. Ключи локального SSH-сервера

2 Нажмите **Перевыпустить ключи**.

3 Нажмите **Продолжить**.

Установка режима повышенной производительности

При обработке одного сетевого подключения можно настроить повышенную скорость обработки и передачи защищенного трафика.

По умолчанию ViPNet Coordinator HW работает в многопоточном режиме, который нацелен на быструю обработку нескольких сетевых соединений. Потоки шифрования в этом случае разбиты на несколько групп.

При включении режима повышенной производительности происходит перераспределение ресурсов ViPNet Coordinator HW: все аппаратные прерывания (IRQ) от сетевых адаптеров выполняются одним ядром процессора, а шифрование выполняется оставшимися ядрами.

Внимание! При включенном режиме в случае обработки большого количества подключений скорость обработки и передачи защищенного трафика будет снижена.

Режим повышенной производительности можно включить на следующих платформах:

- ViPNet Coordinator HW100 N1, N2, N3;
- ViPNet Coordinator HW1000 Q10;
- ViPNet Coordinator HW2000 Q4, Q5;
- ViPNet Coordinator HW5000 Q1, Q2.

Для включения режима повышенной производительности:

1 Выберите **Системные настройки > Общие > Профили производительности.**

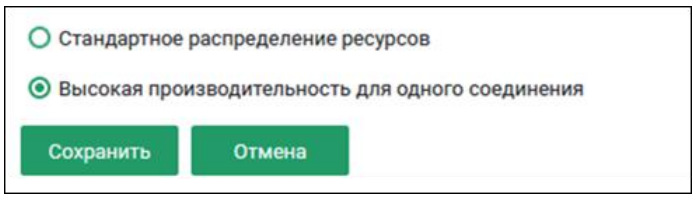

Рисунок 7. Выбор профиля производительности

2 Выберите **Высокая производительность для одного соединения.**

3 Нажмите **Сохранить**.

4 В окне **Применение профиля производительности** выберите **Перезагрузить сейчас** или **Применить при следующей перезагрузке**.

Нажмите **ОК**.

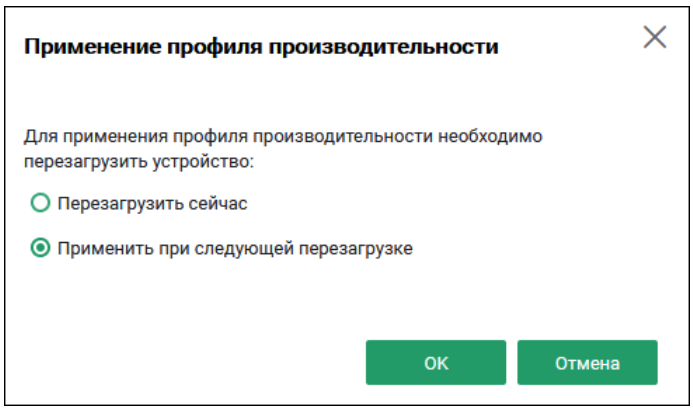

Рисунок 8. Применение профиля производительности

3

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet

Примечание. Вы не можете изменять параметры сетевых интерфейсов, которые задействованы в работе кластера, если служба `failoverd` запущена в режиме кластера горячего резервирования.

1 Выберите **Сетевые интерфейсы**.

2 Выберите интерфейс Ethernet, справа появится окно настроек. Сетевым интерфейсам Ethernet, установленным в системе, присваиваются имена `eth0`, `eth1` и так далее.

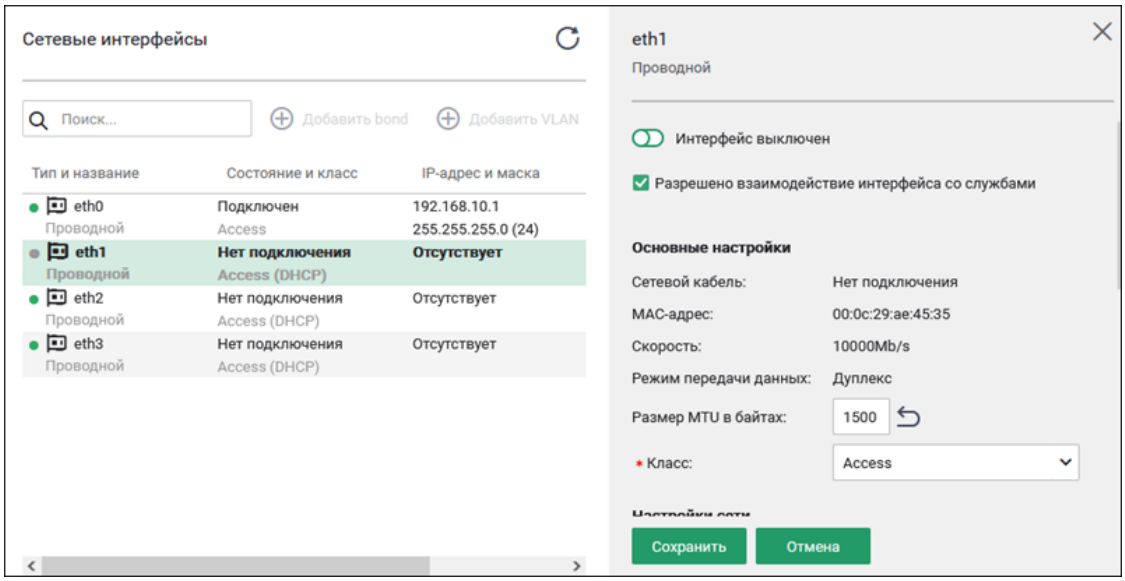

Рисунок 9. Настройка сетевого интерфейса Ethernet

3 По умолчанию для передачи данных через сетевой интерфейс используется размер MTU, равный 1500 байт. Чтобы оптимизировать передачу данных через интерфейс, измените размер MTU. Для этого в поле **Размер MTU в байтах** задайте значение от 1280 до 9000 байт. Чтобы вернуть значение по умолчанию, нажмите .

Внимание! Для исполнения ViPNet Coordinator VA накладываются ограничения:

- VMware Workstation, VMware vSphere — для изменения MTU необходимо предварительно настроить платформу виртуализации, разрешив использование Jumbo-кадров.
- Oracle VM VirtualBox — изменение MTU не поддерживается при использовании сетевых устройств AMD.

4 Задайте класс интерфейса (по умолчанию сетевому интерфейсу назначен класс `Access`.):

- Если требуется, чтобы данный интерфейс Ethernet обрабатывал трафик из нескольких VLAN, назначьте ему класс `trunk`.
- Если вы хотите объединить данный интерфейс Ethernet с другими в составе агрегированного интерфейса, назначьте ему класс `slave`.

Примечание. Исполнение HW10 не поддерживает агрегирование сетевых интерфейсов.

5 Выполните одно из действий:

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, выберите **Получать параметры автоматически.**

  Также для режима DHCP вы можете задать дополнительные параметры:

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

    Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка параметров маршрутов от DHCP/PPP-протокола). Чтобы просмотреть параметры, заданные для режима DHCP на всех сетевых интерфейсах, см. документ «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). 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.
- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

Внимание! При задании IP-адреса действуют ограничения:

- нельзя задать IP-адрес 0.*.*.*;
- нельзя задать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255;
- для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети или широковещательному каналу (broadcast).

6 Включите  сетевой интерфейс.

7 Нажмите **Сохранить**.

8 Если ни для одного включенного интерфейса Ethernet ViPNet Coordinator HW не было выбрано автоматическое получение маршрутов по DHCP, задайте статический маршрут по умолчанию.

Внимание! Если хотя бы на одном используемом интерфейсе Ethernet ViPNet Coordinator HW задано автоматическое получение маршрутов от DHCP-сервера, то в разделе **Маршрутизация** > **Маршрутизация** проверьте, что хотя бы один маршрут по умолчанию получен (см. Просмотр таблицы маршрутизации). Если такого маршрута нет, задайте статический маршрут по умолчанию.

9 Выполните дополнительные настройки:

- Задайте дополнительные IP-адреса для сетевого интерфейса.
- Настройте маршрутизацию.

Назначение дополнительных IP-адресов

С помощью дополнительных IP-адресов вы можете разделить сеть на логические подсети. Например, чтобы разрешить доступ в интернет только некоторым узлам, когда в остальной сети доступ закрыт.

Примечание. Максимальное количество сетевых интерфейсов в ViPNet Coordinator HW — 128 (как физических, так и виртуальных, включая loopback).

Чтобы задать дополнительные IP-адреса на сетевом интерфейсе:

1. Выберите **Сетевые интерфейсы**.
2. Нажмите на сетевой интерфейс Ethernet.
3. Убедитесь, что сетевому интерфейсу назначен класс **Access**.

   Если вы поменяли настройки нажмите **Сохранить**.
4. В поле **Настройка сети** > **Дополнительные IP-адреса** нажмите .

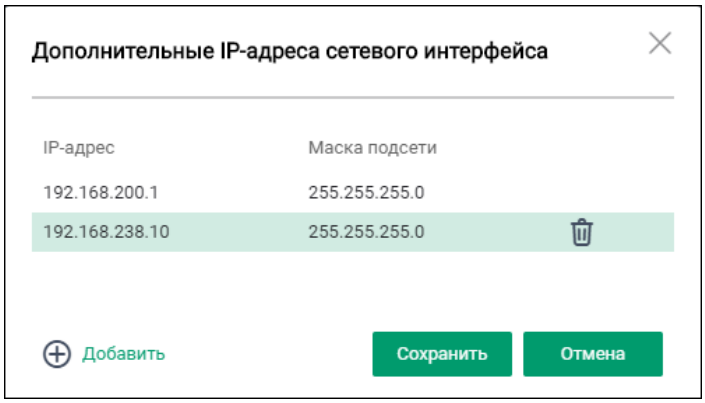

Рисунок 10. Назначение дополнительных IP-адресов

5. Нажмите **Добавить**.
6. Задайте IP-адрес и маску подсети. Сохраните изменения .
7. Нажмите **Сохранить**.

Организация обработки трафика из нескольких VLAN

Вы можете использовать ViPNet Coordinator HW для обработки трафика в физической локальной сети, разделенной на несколько независимых виртуальных локальных сетей — VLAN. Это возможно благодаря поддержке виртуальных сетевых интерфейсов и тегированию (маркировке) трафика в соответствии со стандартом IEEE 802.1Q. Каждой VLAN присваивается идентификатор из диапазона от 1 до 4094 (значения 0 и 4095 зарезервированы).

Для организации обработки трафика из нескольких VLAN:

1. Подключите один из сетевых интерфейсов ViPNet Coordinator HW к коммутатору, объединяющему виртуальные сети.
2. Выберите **Сетевые интерфейсы**.
3. Нажмите интерфейс Ethernet, к которому подключен коммутатор.
4. В правой части снимите флажок **Разрешено взаимодействие интерфейса со службами**.
5. В списке **Класс** выберите **Trunk** и нажмите **Сохранить**.

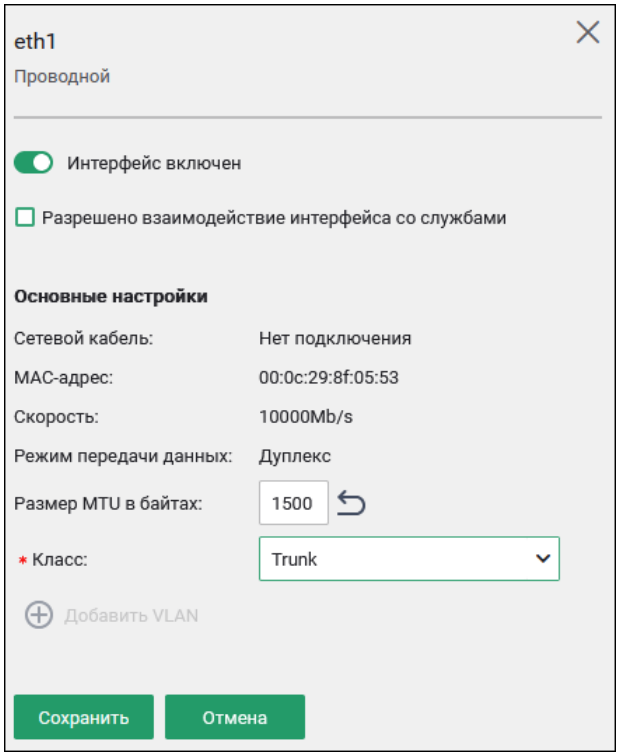

Рисунок 11. Настройка сетевого интерфейса для добавления VLAN

6. Нажмите **Добавить VLAN**.

6.1 В списке **Родительский интерфейс** отображаются интерфейсы Ethernet вашего ViPNet Coordinator HW, для которых указан класс `trunk`. Если таких интерфейсов несколько, выберите нужный вам.

6.2 В поле **Идентификатор** введите номер создаваемого виртуального интерфейса. Создаваемому виртуальному интерфейсу будет присвоено имя в следующем формате:

`<физический интерфейс>.<номер виртуального интерфейса>`

6.3 Нажмите **Сохранить**.

7 Выберите созданный виртуальный интерфейс и в правой части окна укажите настройки для одной из сетей, находящихся за коммутатором:

- Чтобы включить прохождение трафика через виртуальный интерфейс, установите флажок **Разрешено взаимодействие интерфейса со службами**.
- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, выберите Получать параметры автоматически.
  - Также для режима DHCP вы можете задать дополнительные параметры:
  - Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, выберите **DNS-сервера**.
  - Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, выберите **NTP-сервера**.
  - Чтобы включить автоматическое получение маршрутов от DHCP-сервера, выберите **Маршруты**.

    Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка параметров маршрутов от DHCP/PPP-протокола). Чтобы просмотреть параметры, заданные для режима DHCP на всех сетевых интерфейсах, см. документ «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). 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.
- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите **Сохранить**.

В результате будет создан виртуальный интерфейс VLAN для одной из виртуальных сетей, находящихся за коммутатором. Он появится в списке всех сетевых интерфейсов. Чтобы создать виртуальные интерфейсы для других сетей, повторите шаги 7–10.

8 Для передачи данных через виртуальный сетевой интерфейс используется размер MTU, унаследованный от родительского интерфейса. Чтобы оптимизировать передачу данных, вы можете изменить размер MTU родительского интерфейса. Для этого откройте окно настроек

интерфейса и в поле **Размер MTU в байтах** задайте новое значение из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию (1500 байт), нажмите ⮌.

Внимание! Значение MTU, заданное для интерфейса класса `trunk`, автоматически применяется ко всем виртуальным интерфейсам класса `vlan`, созданным на этом физическом интерфейсе.

Для исполнения ViPNet Coordinator VA накладываются ограничения:

- VMware Workstation, VMware vSphere — для изменения MTU необходимо предварительно настроить платформу виртуализации, разрешив использование Jumbo-кадров.
- Oracle VM VirtualBox — изменение MTU не поддерживается при использовании сетевых устройств AMD.

---

9 Включите интерфейс, к которому подключен коммутатор (родительский интерфейс).

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 «Настройка с помощью командного интерпретатора», раздел «Организация обработки трафика из нескольких VLAN».

Подключение к сети Wi-Fi

Примечание. Встроенный Wi-Fi-адаптер есть в аппаратных платформах HW50 N2 и HW100 N2. Внешние Wi-Fi-адаптеры не поддерживаются.

Если ViPNet Coordinator HW работает в режиме точки доступа, то он не сможет подключаться к другим сетям Wi-Fi.

1 Выберите **Сетевые интерфейсы**.

2 Выберите сетевой интерфейс Wi-Fi (`wlan0`). Справа появится окно настроек.

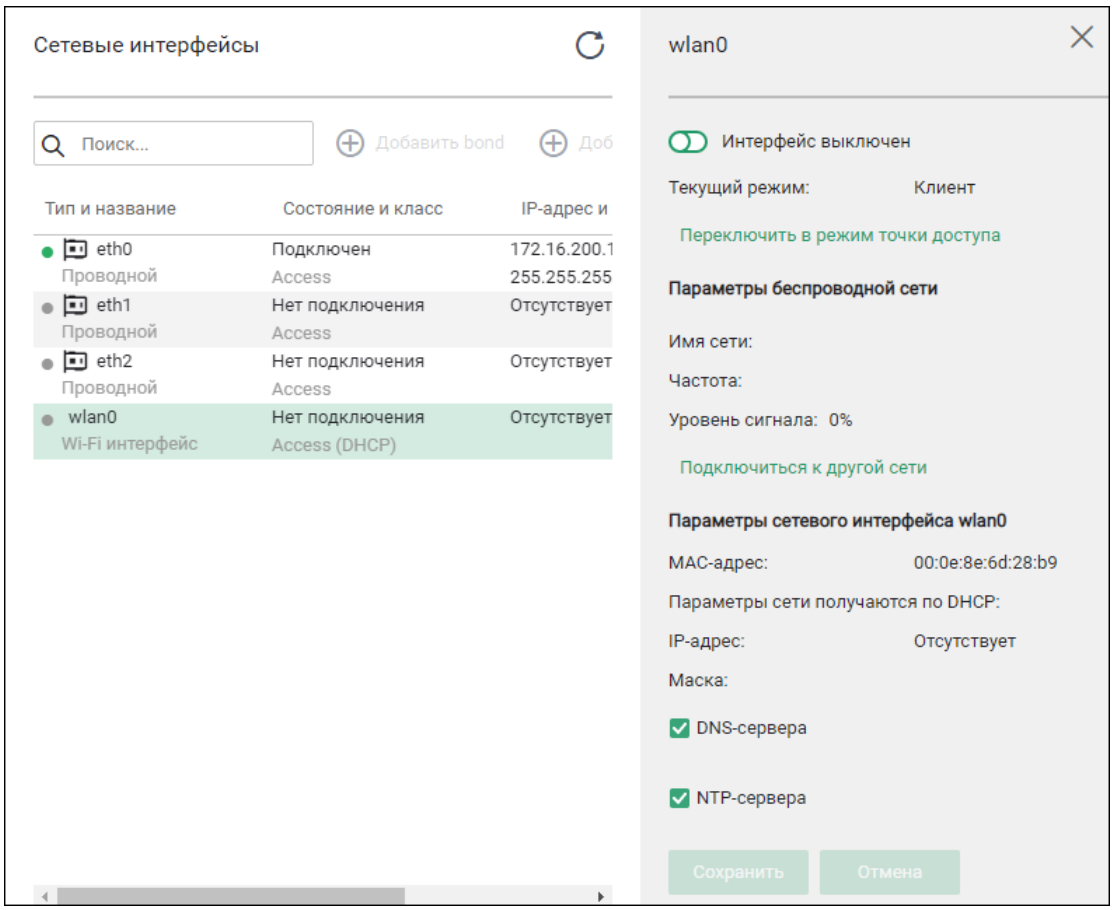

Рисунок 12. Настройка адаптера Wi-Fi

3 По умолчанию интерфейс Wi-Fi работает в режиме клиента. Если интерфейс Wi-Fi работает в режиме точки доступа, нажмите **Переключить в режим клиента**.

4 В группе **Параметры беспроводной сети** отображаются параметры подключения. Нажмите **Подключиться к другой сети**. Отобразится список доступных беспроводных сетей Wi-Fi.

Для сетей, защищенных паролем, указан используемый способ аутентификации. Чтобы обновить список доступных сетей, нажмите .

5 В списке доступных сетей Wi-Fi выберите сеть, к которой вы хотите подключиться.

- Если сеть защищена, в группе **Параметры подключения** укажите тип шифрования, введите пароль и нажмите **Подключиться**.

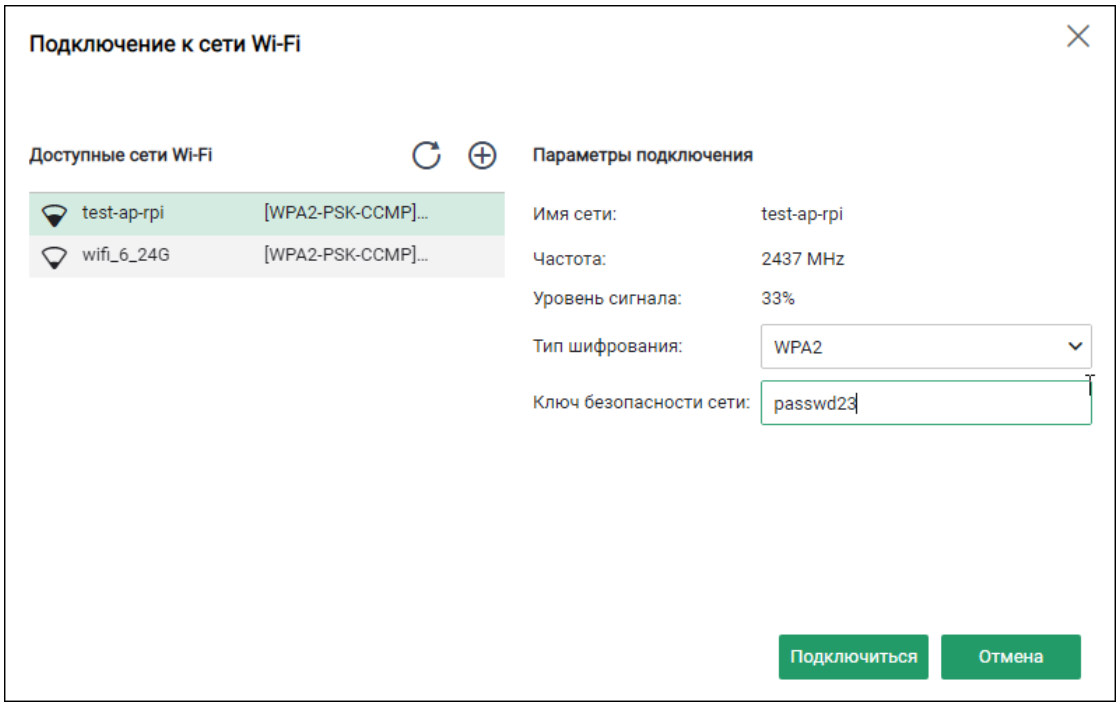

Рисунок 13. Подключение к защищенной сети Wi-Fi

- Если сеть Wi-Fi скрыта, но вы знаете ее имя и параметры доступа к ней, нажмите ⊕.

  В окне **Подключение к сети Wi-Fi** укажите имя, тип шифрования, пароль доступа к скрытой сети и нажмите **Подключиться**.

6 Сетевой интерфейс Wi-Fi всегда работает в режиме автоматического получения параметров от DHCP-сервера, при этом вы можете задать получение дополнительных параметров от DHCP-сервера:

- Адресов DNS-серверов.
- Адресов NTP-серверов.
- Маршрутов.

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. Подробнее см. раздел Настройка параметров динамических маршрутов от DHCP/PPP-протокола (см. Настройка параметров маршрутов от DHCP/PPP-протокола).

  Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию (см. Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола). 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.

7 Включите интерфейс Wi-Fi, если он выключен.

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

Подключение по PPPoE

Внимание!

- При настройке используйте доверенный PPPoE-сервер.
- Убедитесь, что у PPPoE-сервера, который вы используете, включена опция CHAP Rechallenge — периодическая аутентификация установленного соединения. Это защитит PPPoE-сервер от подмены координатора в сети.

Вы можете настроить PPPoE-соединение для подключения узлов к сети провайдера:

1 Выберите **Сетевые интерфейсы**.

2 Выберите Ethernet-интерфейс, через который будет установлено подключение к сети провайдера.

3 На панели справа в списке **Класс** выберите **Access** и нажмите **Сохранить**.

4 Нажмите **Добавить PPPoE**.

Вы можете добавить несколько PPPoE-интерфейсов на один Ethernet-интерфейс. Включенным может быть только один интерфейс, остальные интерфейсы — резервные. При потере соединения вы сможете переключиться на резервный PPPoE-интерфейс.

5 В окне **Добавление PPPoE**:

5.1 Укажите идентификатор интерфейса. Допустимые значения: 0–99.

5.2 В списке **Интерфейс** выберите Ethernet-интерфейс, через который ViPNet Coordinator HW соединен с сетью провайдера.

Отображаются только интерфейсы класса **Access**.

5.3 Выберите тип аутентификации.

5.4 Укажите имя пользователя и пароль, которые получили от провайдера.

5.5 Нажмите **Сохранить**.

PPPoE-интерфейс отобразится в списке интерфейсов:

- Рядом с указанным при создании Ethetnet-интерфейсом.
- В конце списка, если при создании Ethernet-интерфейс не был указан.

6 Настройте PPPoE-интерфейс:

6.1 В поле **Название** укажите дополнительную информацию, например, имя провайдера.

6.2 В разделе **Основные настройки** укажите **MTU в байтах**. По умолчанию — 1492.

6.3 В разделе **Сетевые настройки** выберите:

- **Получать параметры автоматически** — чтобы при подключении к сети провайдера получить от DHCP-сервера IP-адрес и маску подсети.

По умолчанию PPPoE-интерфейс получает динамический IP-адрес от PPPoE-сервера. Если провайдер передал вам IP-адрес, назначьте его статически.

- **Получать маршрут по умолчанию** — чтобы при подключении к сети провайдера получить маршрут по умолчанию, в котором в качестве шлюза указан адрес сети провайдера.
- **Получать адрес DNS-сервера от провайдера** — чтобы при подключении к сети провайдера получить IP-адрес DNS-сервера.

6.4 Нажмите **Сохранить**.

7 Включите PPPoE-интерфейс.

Включить PPPoE-интерфейс можно, только если указаны основные настройки: интерфейс, имя и пароль пользователя, тип аутентификации.

После включения PPPoE-интерфейса установится соединение с PPPoE-сервером.

При потере соединения ViPNet Coordinator HW будет автоматически пытаться подключиться к PPPoE-серверу, пока соединение не будет восстановлено. Это может занять длительное время. Для подключения к другому PPPoE-серверу добавьте на Ethernet-интерфейс резервный PPPoE-интерфейс и включите резервный интерфейс. Резервный интерфейс станет активным, подключение к PPPoE-серверу будет выполняться через него.

Особенности при работе в кластере

- PPPoE-соединение в кластере не резервируется: при потере соединения активный узел пытается подключиться к PPPoE-серверу до восстановления соединения. Узлы кластера не переключатся, даже если PPPoE-соединение не будет восстановлено.
- На пассивном узле кластера доступен только просмотр PPPoE-интерфейсов и их настроек.
- При переключении узлов кластера PPPoE-соединение восстанавливается автоматически.

Настройка подключения к мобильной сети

Настройки для подключения к мобильной сети зависят от оператора связи. При включении модема ViPNet Coordinator HW запрашивает коды MCC и MNC, комбинация которых используется для идентификации оператора в списке мобильных операторов. Если нужная комбинация найдена, устанавливаются настройки подключения к мобильной сети соответствующего оператора.

Настроить подключение к мобильной сети можно только на исполнениях на аппаратных платформах.

Для настройки подключения:

1. Выберите **Сетевые интерфейсы**.
2. Выберите сетевой интерфейс модема.
3. Отключите интерфейс, если он включен.
4. Если на вашей SIM-карте установлен ПИН, задайте его в группе **Информация об устройстве** в поле **PIN-код**.

Предварительные настройки

Предварительные настройки ViPNet Coordinator HW выполняются в группе **Получаемые настройки.** Перед подключением к мобильной сети вы можете:

- Отказаться от получения маршрута по умолчанию

  При первом подключении модема к мобильной сети на ViPNet Coordinator HW добавляется новый маршрут по умолчанию, в котором в качестве шлюза указан адрес узла сети вашего мобильного оператора. Чтобы отказаться от получения маршрута снимите флажок **Маршруты**.

- Изменить метрику маршрута по умолчанию

  Первоначально для нового маршрута задана метрика по умолчанию. Чтобы 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.

- Отказаться от добавления адреса DNS-сервера

  При первом подключении модема оператор добавляет адрес DNS-сервера. Чтобы отказаться от добавления снимите флажок **DNS-серверы**.

Автоматическое определение оператора

1 Включите  интерфейс модема.

2 В группе **Параметры подключения** проверьте отобразились ли параметры подключения к мобильной сети. Если параметры не отображаются:

   2.1 Отключите  интерфейс модема.

   2.2 В группе **Информация об устройстве**:

   - В поле **SIM-карта** проверьте состояние SIM-карты.
   - В поле **PIN-код** проверьте правильность ПИНа.

   Исправьте ошибки, если они есть (поменяйте SIM-карту, введите верный ПИН).

   2.3 Включите  интерфейс модема.

Если параметры все еще не отображаются выберите оператора вручную или добавьте нового.

Настройка модема вручную

Выбор оператора вручную

1 Отключите  интерфейс модема.

2 Нажмите **Операторы**.

3 Выберите страну.

4 В списке найдите вашего оператора и проверьте параметры подключения. Если параметры верные нажмите **Выбрать**.

5 Включите  интерфейс модема.

Если вашего оператора с необходимыми параметрами подключения нет в списке, добавьте нового.

Добавление нового оператора

1 Отключите  интерфейс модема.

2 Нажмите **Операторы**.

3 Нажмите **Добавить оператора**. Заполните параметры:

   3.1 Выберите страну.

   3.2 Введите название оператора.

   3.3 Нажмите **Сохранить**.

4 В списке найдите созданного оператора и заполните параметры подключения.

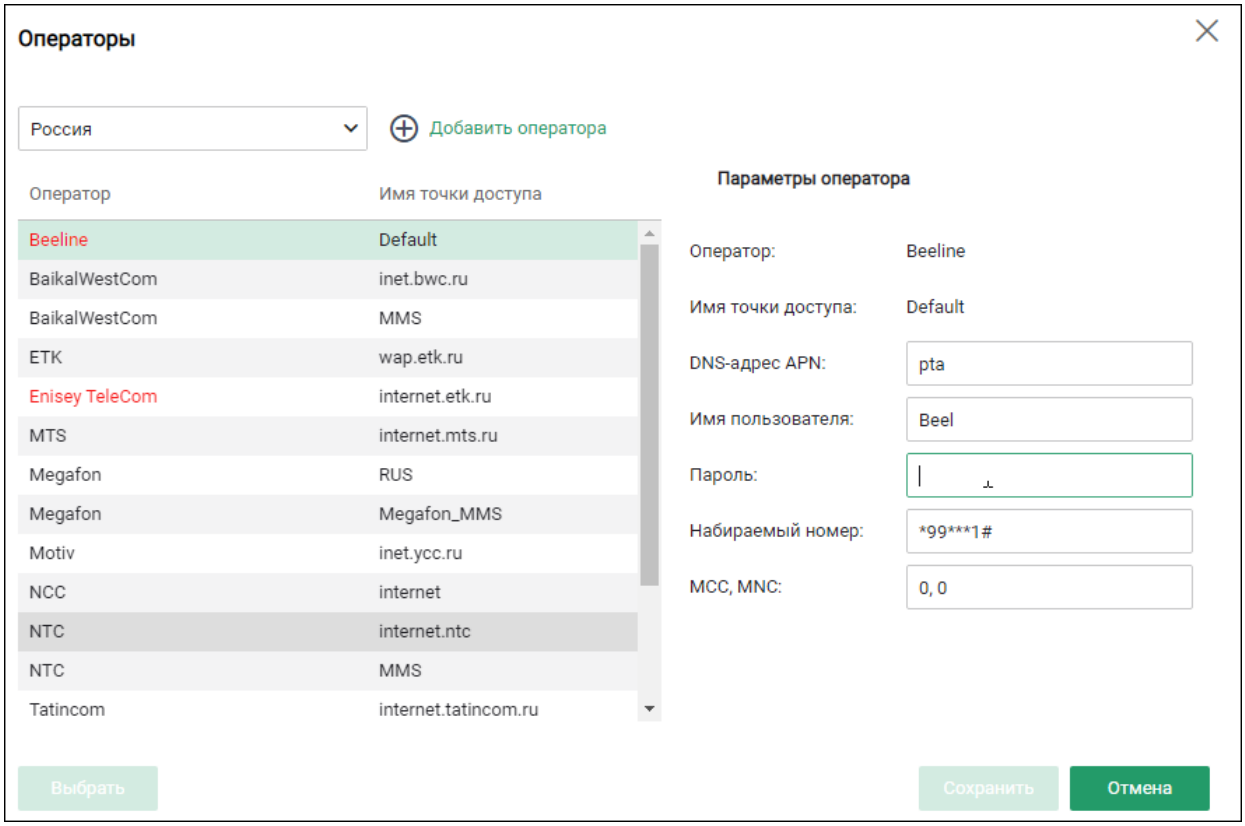

Рисунок 14. Добавление нового оператора

5 Нажмите **Сохранить**.

6 Нажмите **Выбрать**, чтобы выбрать созданного оператора в качестве текущего для подключения.

7 Включите интерфейс модема.

Примечание. Чтобы удалить всех созданных вами операторов из списка нажмите **Сбросить параметры подключения**.

Настройка учета мобильного трафика

ViPNet Coordinator HW позволяет отслеживать количество используемого мобильного трафика и отправлять уведомления о превышении установленного ограничения. Эта функция может быть полезна, когда ViPNet Coordinator HW выходит в интернет через мобильную сеть, а оператор мобильной связи ограничивает объем потребляемого трафика. Превышение допустимого объема трафика может привести к ненужным расходам или потере связи между ViPNet Coordinator HW и управляющим ПО.

Чтобы этого не произошло, вы можете настроить учет используемого трафика и уведомления о превышении разрешенного объема.

Настроить учет мобильного трафика можно только на исполнениях на аппаратных платформах.

Настройка учета используемого трафика

1. Выберите **Сетевые интерфейсы**.
2. Выберите сетевой интерфейс модема.
3. В поле **Дата начала учета** укажите день месяца, с которого начинается учет трафика.
4. В поле **Установить лимит трафика (МБ)** установите флажок и введите объем мобильного трафика, при котором устройство отправляет уведомление.

Настройка оповещения

1. Выберите **Системные настройки** > **Оповещения**.
2. Отключите оповещения, если они включены.
3. Укажите параметры подключения к SMTP-серверу:
   - адрес или доменное имя;
   - протокол защиты;

     Примечание. Порт подключения к серверу устанавливается в зависимости от выбора протокола защиты. Если вы хотите, чтобы ViPNet Coordinator HW подключался к SMTP-серверу через порт, отличный от порта по умолчанию, измените его.

   - имя пользователя и пароль для подключения
   - адрес электронной почты, с которого будут приходить оповещения.

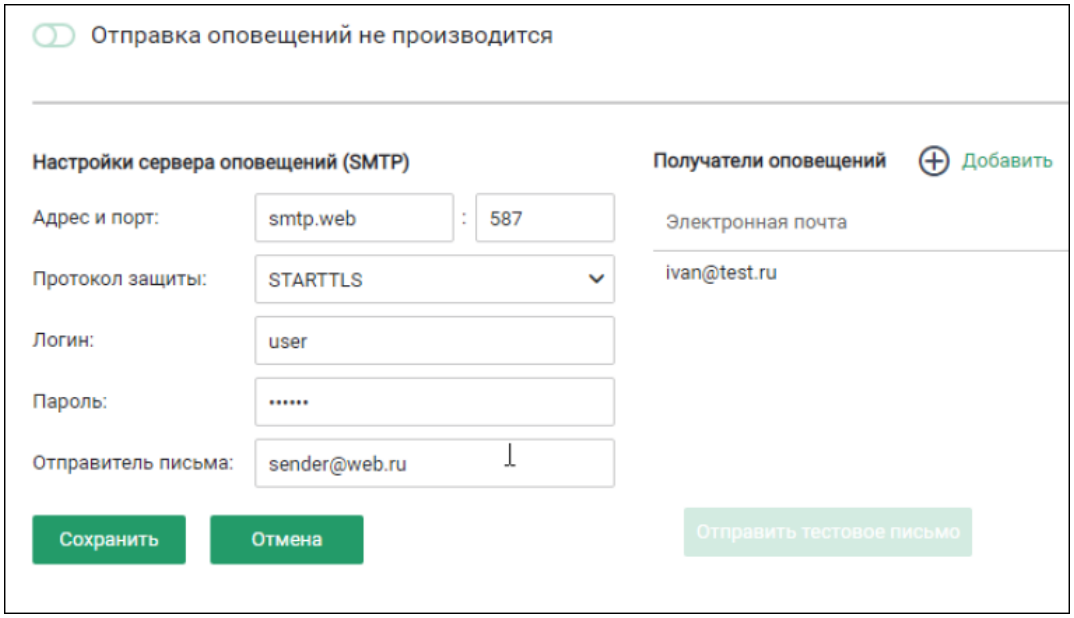

Рисунок 15. Настройка оповещений

4 Укажите адреса электронной почты, на которые будут приходить оповещения:

4.1 В поле **Получатель** нажмите **Добавить**.

4.2 Введите адрес электронной почты.

4.3 Нажмите .

Примечание. Чтобы отредактировать существующий адрес, выберите его в списке и нажмите .
Чтобы удалить получателя выберите его в списке и нажмите .

5 Включите оповещения.

6 Нажмите **Отправить тестовое письмо**, чтобы проверить работу SMTP-сервера.

Если появится сообщение об ошибке проверьте:

- настройки SMTP-сервера;
- настройки электронной почты;
- интерфейс модема (должен быть включен).

Примечание. После включения SMTP-оповещений автоматически создастся разрешающий сетевой фильтр.

Оповещения отправляются, как только потребляемый трафик достигает 75%, 85% и 95% от указанного ограничения трафика.

Использование агрегированных сетевых интерфейсов

Примечание. Исполнение HW10 не поддерживает агрегирование сетевых интерфейсов.

Агрегирование сетевых интерфейсов — объединение нескольких физических сетевых интерфейсов в один логический. При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

Агрегированные сетевые интерфейсы можно использовать:

- Чтобы увеличить пропускную способность сетевых интерфейсов ViPNet Coordinator HW. Например, если вам нужен канал связи с пропускной способностью выше 1 Гбит/с, а на вашем исполнении ViPNet Coordinator HW есть только гигабитные сетевые интерфейсы, вы можете объединить два или три из них в один агрегированный.
- Чтобы повысить надежность канала связи. Если один из объединенных интерфейсов выйдет из строя, агрегированный канал связи продолжит работать.
- Для резервирования канала связи, без увеличения его пропускной способности. Весь трафик будет передаваться через один из подчиненных физических интерфейсов, остальные же начинают работать только при его сбое.

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

Чтобы задать распределение нагрузки по подчиненным физическим интерфейсам, выберите один из режимов работы агрегированного интерфейса.

Внимание! Работоспособность агрегированных интерфейсов в ViPNet Coordinator VA не гарантируется. Если вам необходимо использовать агрегированный канал для ViPNet Coordinator VA, настройте его на платформе виртуализации.

Режимы работы агрегированного интерфейса

При создании агрегированного интерфейса указывайте режим его работы, наиболее подходящий для решения ваших задач. В ViPNet Coordinator HW предусмотрено несколько режимов, позволяющих по-разному распределять нагрузку между подчиненными физическими интерфейсами.

balance-rr

Подходит как для балансировки нагрузки на подчиненных интерфейсах, так и для защиты от сбоев. Может применяться в сетях с простой топологией.

Исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные поочередно: первый пакет отправляется через один подчиненный интерфейс, второй — через следующий и так далее.

balance-xor

Предназначен 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.

Для определения подчиненного физического интерфейса, через который отправляется пакет, используется специальная хэш-функция, алгоритм вычисления которой вы можете задать с помощью списка **Алгоритм хэширования** после создания агрегированного интерфейса:

- **layer2** — используются MAC-адреса отправителя и получателя пакета. Одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами;
- **layer2+3** — используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протокола IPv4). Одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами и IP-адресами;
- **layer3+4** — используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии). Одинаковыми считаются сетевые узлы с одинаковыми IP-адресами, а также портами TCP или UDP.

balance-tlb

Подходит для балансировки нагрузки на подчиненных интерфейсах. Используется при передаче большого числа пакетов разного размера, когда более простые режимы не распределяют нагрузку равномерно.

Учитывается размер 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 в режиме balance-tlb необходимо, чтобы все подчиненные интерфейсы были подключены к сети через коммутатор.

802.3ad

Режим динамического агрегирования с использованием протокола LACP для комплексной балансировки нагрузки. В этом режиме агрегированный интерфейс работает следующим образом:

- Среди подчиненных интерфейсов формируются группы — «агрегаторы», с одинаковой скоростью передачи данных (например, группа гигабитных интерфейсов). Параметры `mtu`, `duplex`, `autoneg` для физических интерфейсов, объединяемых в группу, должны совпадать.
- Один из агрегаторов выбирается активным в соответствии с режимом выбора, задаваемым с помощью списка **Режим агрегатора** после создания агрегированного интерфейса. Вы можете задать один из режимов:
  - **stable** — первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора.
  - **bandwidth** — первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных интерфейсов, в агрегаторах производится перегруппировка подчиненных интерфейсов и выполняется выбор нового агрегатора.
  - **count** — первоначально выбирается агрегатор с наибольшим количеством подчиненных интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных интерфейсов, в агрегаторах производится перегруппировка подчиненных интерфейсов и выполняется выбор нового агрегатора.
- Внутри агрегатора подчиненный интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму **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.

Примечание. Механизм MC-LAG (MLAG) не поддерживается. Поэтому физические порты разных ViPNet Coordinator HW нельзя использовать в одном агрегированном интерфейсе.

---

active-backup

Предназначен для защиты от сбоев, но не для балансировки нагрузки на подчиненных интерфейсах.

Один из подчиненных интерфейсов назначается основным, и все исходящие пакеты отправляются через него. При этом в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.

broadcast

Предоставляет наибольшую защиту от сбоев. Пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные интерфейсы одновременно.

Примечание. Режим broadcast требует специальной настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов данных.

Если агрегированный канал связи работает в режиме **broadcast**, организовать на этом канале защиту соединения по технологии L2OverIP невозможно.

Создание агрегированного интерфейса

1 Выберите **Сетевые интерфейсы**.

2 Для всех сетевых интерфейсов Ethernet, которые вы хотите объединить, установите класс `slave`.

3 Нажмите **Добавить bond**.

4 В открывшемся окне задайте параметры:

- В поле **Идентификатор** задайте номер создаваемого агрегированного интерфейса. Вы можете создать до восьми агрегированных интерфейсов с номерами 0-7. 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. Количество подчиненных интерфейсов ограничено только общим количеством интерфейсов на ViPNet Coordinator HW. При создании агрегированного интерфейса необходимо выбрать не менее одного подчиненного интерфейса.

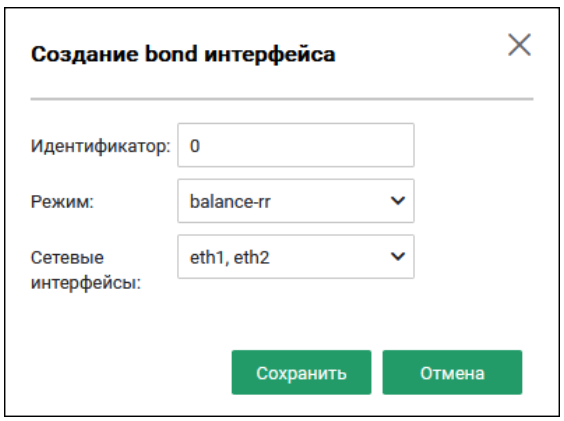

Рисунок 16. Создание агрегированного интерфейса

5 Настройте параметры агрегированного интерфейса:

5.1 Выберите созданный агрегированный интерфейс.

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

5.3 Чтобы интерфейс обрабатывал трафик из нескольких VLAN, назначьте ему класс `trunk`. По умолчанию созданному интерфейсу назначается класс `access`.

5.4 Чтобы включить на интерфейсе режим автоматического получения параметров от DHCP-сервера, выберите **Получать параметры автоматически.**

Также для режима DHCP вы можете задать дополнительные параметры:

- Включить автоматическое получение адресов DNS-серверов (установите флажок **DNS-сервера**).
- Включить автоматическое получение адресов NTP-серверов (установите флажок **NTP-сервера**).
- Включить автоматическое получение маршрутов (установите флажок **Маршруты**).

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка параметров маршрутов от DHCP/PPP-протокола). Чтобы просмотреть параметры, заданные для режима DHCP на всех сетевых интерфейсах, см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».
- Задать специфичную метрику для маршрутов, полученных от DHCP-сервера (укажите ее в поле **Метрика**).

  Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера.

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

5.6 Чтобы включить прохождение трафика через созданный агрегированный интерфейс, установите флажок **Разрешено взаимодействие интерфейса со службами**.

5.7 Чтобы оптимизировать передачу данных через интерфейс, вы можете изменить размер MTU (по умолчанию используется размер MTU, равный 1500 байт). Для этого в поле **Размер MTU в байтах** задайте новое значение MTU из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию (1500 байт), нажмите ⮌.

Внимание! Значение MTU, заданное для интерфейса класса `bond`, будет использоваться на всех подчиненных физических интерфейсах класса `slave`.

Для исполнения ViPNet Coordinator VA накладываются ограничения:

- VMware Workstation, VMware vSphere — для изменения MTU необходимо предварительно настроить платформу виртуализации, разрешив использование Jumbo-кадров.
- Oracle VM VirtualBox — изменение MTU не поддерживается при использовании сетевых устройств AMD.

5.8 Нажмите **Сохранить**.

6 Последовательно включите подчиненные физические интерфейсы.

7 Включите агрегированный интерфейс.

Причины сбоя подчиненного интерфейса

Причинами сбоев в работе подчиненного интерфейса могут быть:

- Неисправность сетевого оборудования (сетевой карты).
- Несогласованность дуплексных скоростных режимов работы сетевого интерфейса.
- Неисправность физического тракта (медного, оптического соединения).

Чтобы выяснить причины сбоя в работе подчиненного интерфейса:

1 Проверьте работоспособность интерфейса:

1.1 Выберите **Сетевые интерфейсы**.

1.2 Посмотрите информацию об интерфейсе в таблице. Если интерфейс включен, но в столбце **Состояние и класс** отображается **Нет подключения**, интерфейс не работоспособный.

2 Проверьте режим работы смежного устройства, с которым устанавливается связь по агрегированному интерфейсу. Режимы работы должны совпадать на обоих устройствах.

Просмотр ARP-таблицы

Чтобы просмотреть ARP-таблицу с записями о преобразованиях IP-адресов в MAC-адреса:

1 Выберите **Маршрутизация** > **ARP-таблица**.

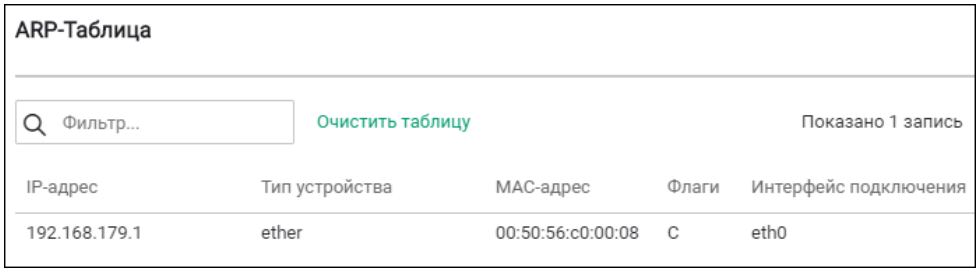

Рисунок 17. Просмотр ARP-таблицы

2 В поле **Фильтр** вы можете ввести как полные, так и частичные значения параметров:

- имя сетевого интерфейса;
- имя интерфейса VLAN;
- MAC-адрес;
- IP-адрес.

3 В случае сетевых сбоев вы можете очистить ARP-таблицу (только в режиме администратора).

4

Просмотр и изменение параметров VPN

Просмотр сведений о сетевых узлах ViPNet

Вы можете просмотреть сведения об узлах ViPNet, для которых установлены связи с вашим узлом: например, чтобы узнать IP-адреса узлов, с которых разрешена настройка и управление.

1 Выберите **Защищенная сеть (VPN)** > **Управляющие соединения** > **Узлы ViPNet**.

Страница **Узлы ViPNet** содержит список сетевых узлов, с которыми у вашего узла есть связь, а также сведения о времени последней активности пользователей этих узлов.

Примечание. Активность определяется временем, когда между координатором и узлом организуется соединение (например, обмен межузловой информацией или проверка связи). Данные сохраняются в памяти ViPNet Coordinator HW, обновляются при каждом новом соединении и хранятся до перезапуска службы `iplircfg`.

Таким образом, даже если узел выключен, сведения о времени последней активности будут отображаться, пока на ViPNet Coordinator HW не перезапустится служба `iplircfg`.

В этом списке:

- — клиенты ViPNet;
- — координаторы ViPNet;

Узлы, которые в текущий момент недоступны либо статус которых неизвестен, отображаются серым цветом.

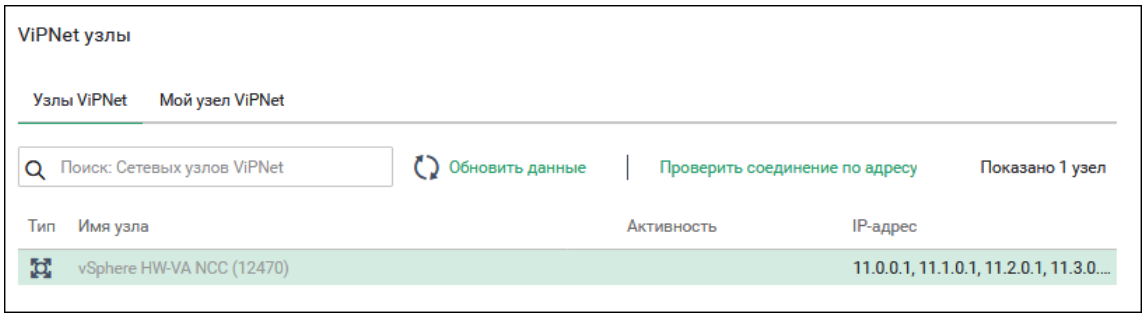

Рисунок 18. Просмотр списка узлов сети ViPNet

2 Чтобы просмотреть подробные сведения о каком-либо узле, щелкните его в списке. Информация об узле содержит разделы:

- общая информация: имя узла, версия операционной системы (отображается после проверки соединения), статус соединения, используемый тип шифрования;
- IP-адреса доступа к узлу: реальные и виртуальные;
- настройки межсетевого экрана при подключении к внешней сети (для координаторов сети ViPNet);

- настройки туннелирования (для координаторов сети ViPNet);
- доменные имена сетевого узла.

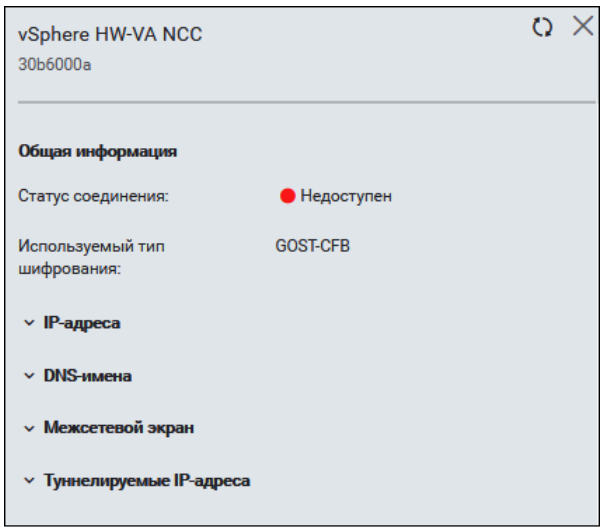

Рисунок 19. Просмотр информации о сетевом узле ViPNet

Вы можете проверить соединение с сетевым узлом ViPNet: например, если сеанс управления с этого узла был прерван, и вы хотите выяснить причину неполадки.

1 На странице **Узлы ViPNet** выберите узел, соединение с которым вы хотите проверить.

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

---

2 Нажмите **Обновить данные**. Если узел доступен, его имя отображается черным цветом и в столбце **Активность** отображается время последней активности.

Чтобы проверить соединение с узлом по его IP-адресу или доменному имени:

1 На странице **Узлы ViPNet** нажмите **Проверить соединение по адресу**.

2 Введите IP-адрес или доменное имя узла, с которым хотите проверить соединение.

3 Нажмите **Проверить**.

Вы можете просмотреть сведения о собственном сетевом узле ViPNet. Для этого откройте **Управляющие соединения > Мой узел ViPNet**.

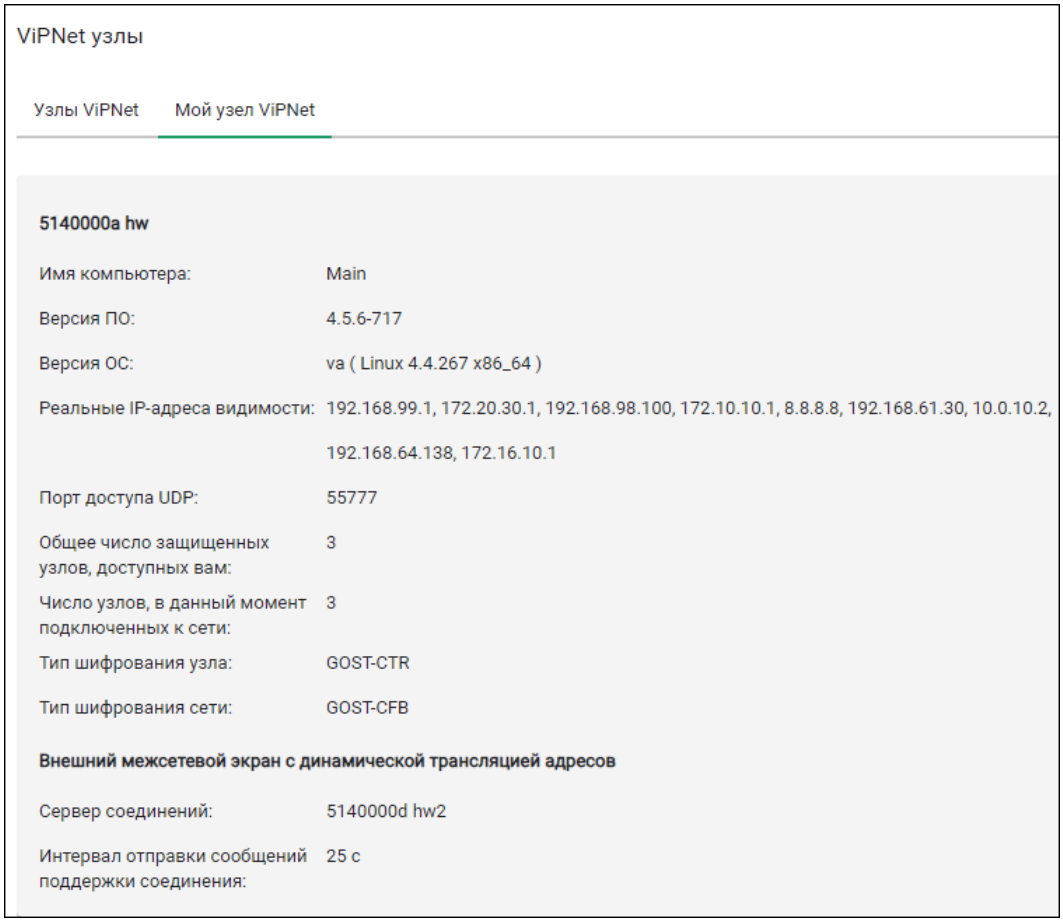

Рисунок 20. Просмотр сведений о собственном сетевом узле ViPNet

Настройка видимости узлов

При подключении удаленных пользователей к ресурсам локальной сети, а также при организации взаимодействия локальных сетей с использованием технологии VPN может возникать проблема пересечения IP-адресов. Например, два сетевых узла, находящихся в разных сетях, которые взаимодействуют с помощью VPN, могут иметь одинаковые частные IP-адреса, и в случае обращения по такому адресу возникнет неоднозначность. Технология виртуальных IP-адресов позволяет решить эту проблему без изменения текущей адресной структуры сетей.

Каждый узел сети ViPNet при получении справочников автоматически формирует виртуальные IP-адреса для доступа ко всем защищенным узлам, с которыми у него имеется связь. Если среди них есть координаторы, виртуальные IP-адреса формируются также для всех узлов, которые эти координаторы туннелируют. Каждому реальному IP-адресу узла ставится в соответствие виртуальный IP-адрес. В результате каждый защищенный узел имеет собственный список виртуальных IP-адресов для доступа к узлам сети ViPNet.

По умолчанию на ViPNet Coordinator HW используются следующие настройки видимости:

- защищенные узлы, находящиеся в одном и том же широковещательном сегменте, доступны по реальным IP-адресам;
- туннелируемые узлы (узлы, туннелируемые другими координаторами) доступны по реальным IP-адресам;
- остальные узлы сети ViPNet доступны по виртуальным IP-адресам.

Веб-интерфейс позволяет настроить видимость для отдельных узлов. Чтобы настроить видимость для всех узлов сети ViPNet, отредактируйте файл iplir.conf. Подробнее см. в документе «Настройка с помощью командного интерпретатора» в разделе «Настройка видимости узлов».

Чтобы настроить видимость защищенных узлов:

1. Выберите **Защищенная сеть (VPN) > Управляющие соединения > Узлы ViPNet**.
2. В списке выберите узел, для которого надо настроить видимость.
3. В разделе **IP-адреса** в поле **IP-адреса видимости** выберите тип видимости узла: **Реальные** или **Виртуальные**.

Чтобы настроить видимость туннелируемых IP-адресов:

1. Выберите **Защищенная сеть (VPN) > Управляющие соединения > Узлы ViPNet**.
2. В списке выберите туннелирующий координатор, для которого надо настроить видимость туннелируемых IP-адресов.
3. В разделе **Туннелируемые IP-адреса** в поле **IP-адреса видимости** выберите тип видимости узла: **Реальные** или **Виртуальные**.

Примечание. При переключении типа видимости на **Реальные**, диапазоны с пересекающимися адресами исключаются из списка туннелируемых IP-адресов без предупреждения.

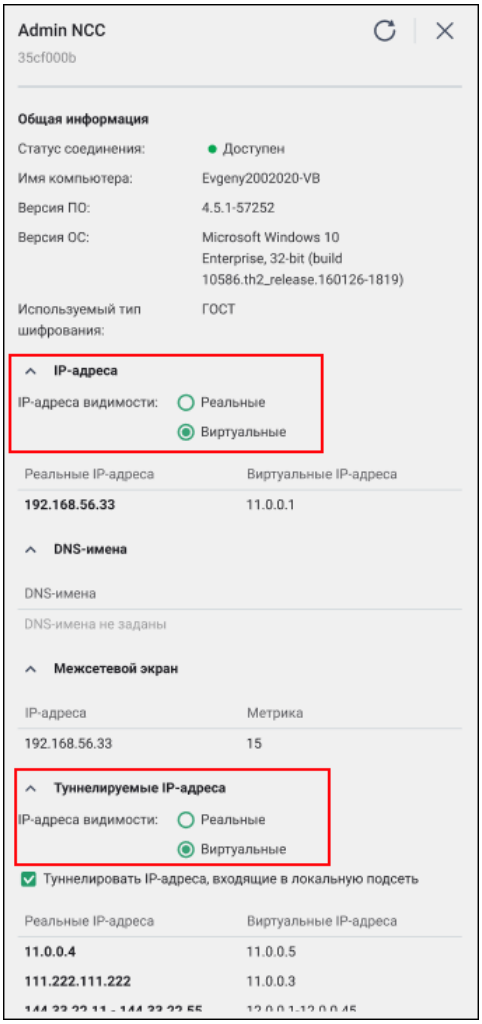

Рисунок 21. Настройка видимости

Просмотр и изменение списка туннелируемых узлов

Туннелирование позволяет защищать трафик открытых узлов корпоративной сети на потенциально опасном участке сети или включать открытые узлы в защищенную сеть без установки на эти узлы ПО ViPNet. Настройки туннелирования открытых узлов, которые задает администратор сети ViPNet, хранятся на координаторах сети ViPNet, выполняющих туннелирование этих узлов.

Если туннелируемые координатором узлы заданы в ViPNet ЦУС или Prime, то другие узлы получат информацию об этом автоматически в составе справочников. Если туннелируемые IP-адреса заданы на координаторе вручную, эти адреса также необходимо указать вручную на каждом узле, который будет подключаться к этим туннелируемым узлам посредством сети ViPNet.

При наличии 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.

Внимание! На всех туннелируемых узлах сети настройте статические маршруты для защищаемого трафика через ViPNet Coordinator HW или укажите ViPNet Coordinator HW в качестве шлюза по умолчанию.

Чтобы добавить туннелируемый IP-адрес или диапазон туннелируемых IP-адресов:

1 Выберите **Защищенная сеть (VPN) > Туннелирование**.

В результате отобразится информация о количестве туннелируемых узлов и их IP-адресах.

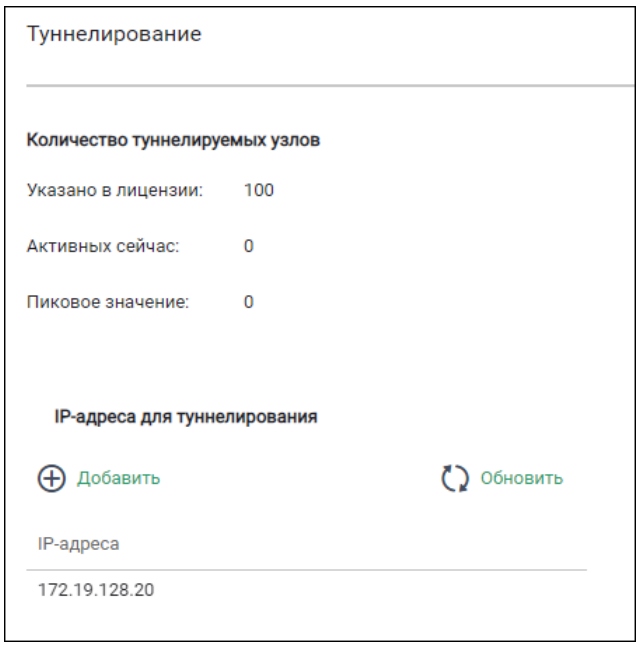

Рисунок 22. Просмотр информации о туннелируемых узлах

2 Нажмите ⊕ **Добавить** и задайте IP-адрес или диапазон IP-адресов узлов, туннелируемых вашим ViPNet Coordinator HW.

Внимание! При добавлении туннелируемых IP-адресов происходит проверка конфликта адресов. Если у связанных координаторов тип видимости туннелируемых IP-адресов **Реальные**, то при конфликте адресов сохранить настройки невозможно.

Настройка туннелирования локальных адресов

Технология туннелирования предполагает направление трафика узла не напрямую на другой узел, а через туннелирующий координатор, где трафик фильтруется и защищается криптографическими методами.

В локальной сети вы можете направлять трафик напрямую на туннелируемый узел, минуя туннелирующий координатор.

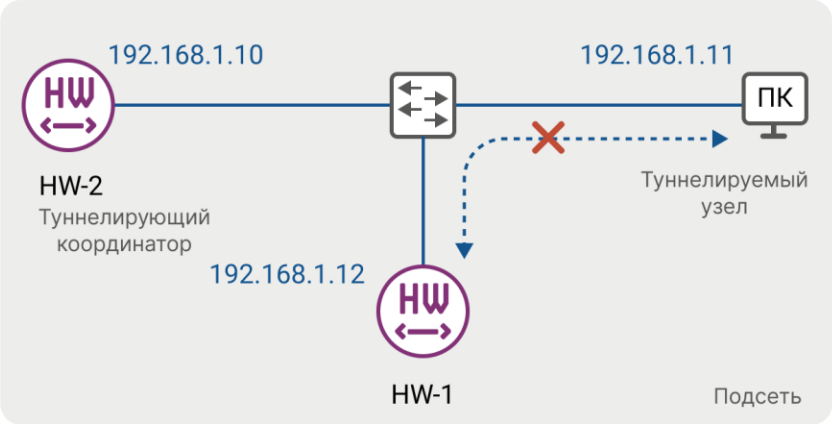

Рисунок 23. Трафик между ПК и HW-1 заблокирован

Примечание. Отключайте туннелирование если затруднен доступ к туннелируемым узлам в локальной подсети.

Чтобы отключить туннелирование локальных адресов:

1. Выберите **Защищенная сеть (VPN) > Управляющие соединения > Узлы ViPNet**.
2. В списке узлов выберите туннелирующий координатор.
3. На панели справа в разделе **Туннелируемые IP-адреса** включите **Туннелировать IP-адреса, входящие в локальную подсеть**.

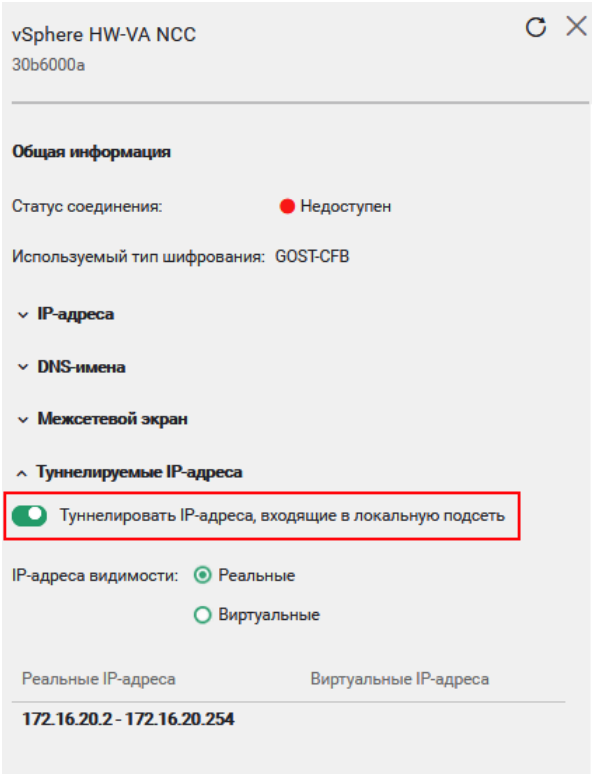

Рисунок 24. Настройка туннелирования локальных адресов

Настройка туннелирования на канальном уровне по технологии L2OverIP

Общее описание технологии L2OverIP

ViPNet Coordinator HW поддерживает технологию L2OverIP, которая позволяет организовать защиту удалённых сегментов сети, использующих одно адресное пространство, на канальном уровне модели OSI. В результате сетевые 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 распределённых ЦОДов (центров обработки данных), локальные сети которых объединены высокоскоростным каналом связи и представляют собой единый широковещательный домен.

Технология L2OverIP предполагает взаимодействие между узлами нескольких удалённых сегментов сети через ViPNet Coordinator HW, которые установлены на границах этих сегментов. ViPNet Coordinator HW перехватывает Ethernet-кадры, отправленные из его сегмента сети в другой, упаковывает их в IP-пакеты специального формата и передаёт эти IP-пакеты другому ViPNet Coordinator HW по защищённому каналу. ViPNet Coordinator HW, получивший IP-пакеты специального формата, извлекает из них исходные кадры и передаёт получателям в своем сегменте.

Сетевой интерфейс ViPNet Coordinator HW, к которому подключаются узлы сегмента сети, должен иметь класс:

- `access` со статическим IP-адресом для физических интерфейсов `eth`, виртуальных интерфейсов `vlan` или агрегированных интерфейсов `bond`;
- `trunk` для физических интерфейсов `eth` или агрегированных интерфейсов `bond`.

С помощью L2OverIP можно объединить несколько сегментов сети, в том числе VLAN:

- 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`.

При использовании 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, который задается 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 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. 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).

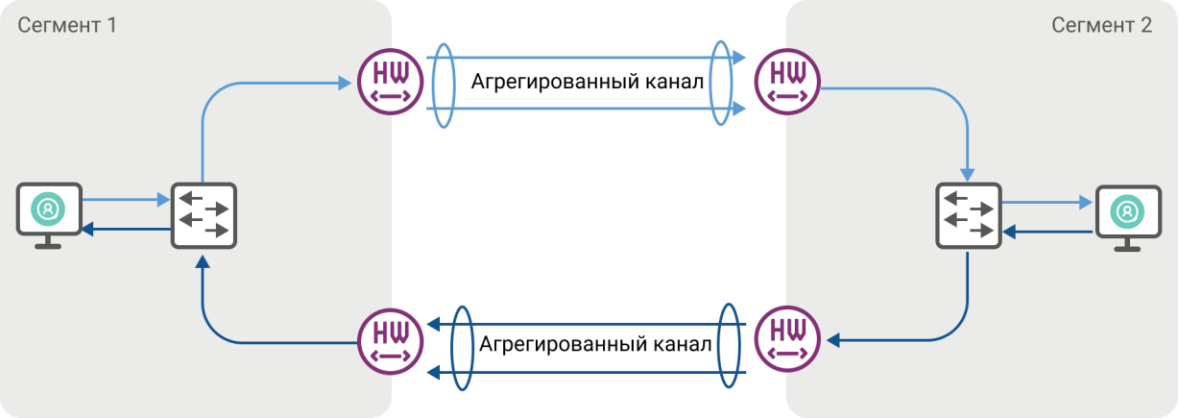

Рисунок 25. Схема работы сети с парами ViPNet Coordinator HW, объединенных с помощью агрегированных каналов

Рассылка Ethernet-кадров с неизвестным MAC-адресом получателя выполняется в соответствии с 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.

L2OverIP можно использовать в кластере горячего резервирования. Настройка L2OverIP выполняется на активном узле. Таблица MAC-адресов не передается пассивному узлу, и при переключении пассивного узла в активный режим его таблица пуста. Это приводит к увеличению

времени конвергенции сети после смены активного узла — до тех пор, пока узлы из разных сегментов, взаимодействующие друг с другом, не отправят заново ARP-запросы.

Особенности реализации L2OverIP

- L2OverIP не поддерживается в исполнениях HW10 и HW50.
- Сегменты сети, объединяемые по L2OverIP, должны быть изолированы друг от друга. Сетевое взаимодействие между ними должно осуществляться только по каналам связи между ViPNet Coordinator HW, установленными на границах объединяемых сегментов.
- Использование беспроводных интерфейсов в L2OverIP не поддерживается.
- Текущая версия ViPNet Coordinator HW позволяет объединять не более 31 сегмента сети.
- Используйте не более 252 IP-адресов во всех объединяемых сегментах сети. Превышение этого количества может привести к снижению пропускной способности сети в связи с возрастанием служебного трафика в широковещательном домене.
- Для исполнения ViPNet Coordinator VA в настройках платформы виртуализации включите неразборчивый режим (Promiscuous Mode) на интерфейсе, к которому привязан адаптер виртуальной машины.
- Поиск IP-пакетов, переданных по L2OverIP, в журнале IP-пакетов необходимо выполнять по признакам исходных IP-пакетов: IP-адрес источника и получателя, номер TCP- и UDP-порта, интерфейс.

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 сетевых интерфейсов ViPNet Coordinator HW, установленному на границе сегмента. Если сегмент сети состоит из нескольких VLAN, они должны быть объединены с помощью коммутатора в транковый порт, к которому подключается один из сетевых интерфейсов ViPNet Coordinator HW.

Чтобы организовать защиту соединения сегментов, на каждом ViPNet Coordinator HW включите функцию L2OverIP и задайте ее параметры:

1 Задайте статический IP-адрес сетевого интерфейса, через который по L2OverIP будут объединяться сегменты. Задайте этот IP-адрес шлюзом по умолчанию для узлов сегмента.

2 Выберите **Защищенная сеть (VPN)** > **L2OverIP**.

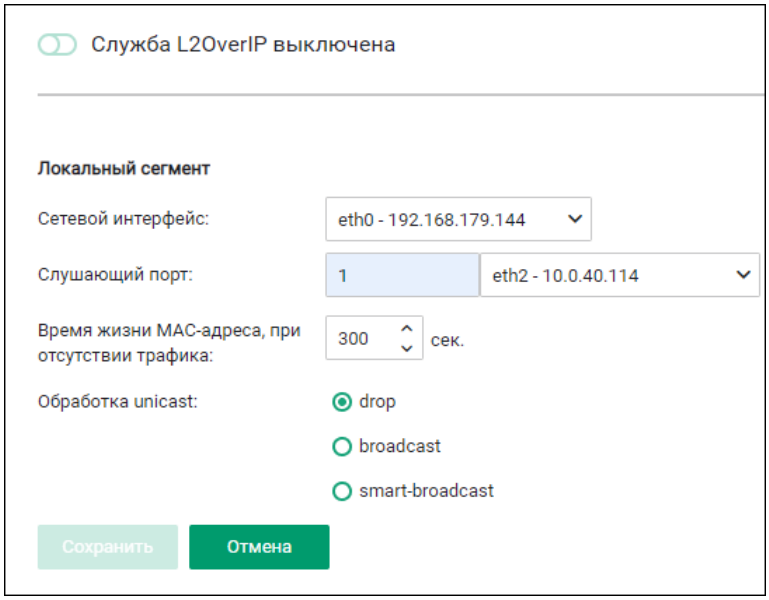

Рисунок 26. Настройка параметров соединения L2OverIP

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, задав уникальный номер порта в поле **Слушающий порт** и выберите IP-адрес внешнего интерфейса в списке рядом.

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

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.

Для этого в области **Удаленные сегменты** нажмите ⊕ **Добавить сегмент**, укажите IP-адрес и порт удаленного сегмента сети, нажмите 💾.

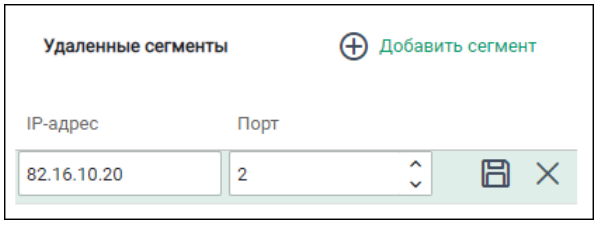

Рисунок 27. Добавление удаленного сегмента сети при создании соединения L2OverIP

8 Добавьте сетевые фильтры защищенной сети, разрешающий любые соединения по протоколу 97, со следующими параметрами:

- Действие: Пропускать трафик.
- Источники: Мой узел ViPNet.
- Протокол: IP: 97.

- Действие: Пропускать трафик.
- Назначение: Мой узел ViPNet.
- Протокол: IP: 97.

9 Нажмите **Сохранить**.

10 Включите службу L2OverIP.

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.

Настройка TCP-туннеля

При удаленном подключении клиентов к сетям ViPNet может возникать проблема с передачей IP-пакетов по протоколу UDP из-за того, что данный протокол блокируется некоторыми интернет-провайдерами. Но в этих случаях обычно разрешен доступ по протоколу TCP через порты 80 (HTTP) и 443 (HTTPS).

Для решения проблемы доступа можно организовать взаимодействие клиентов с другими узлами сети ViPNet через TCP-туннель, настроенный на сервере соединений этих клиентов.

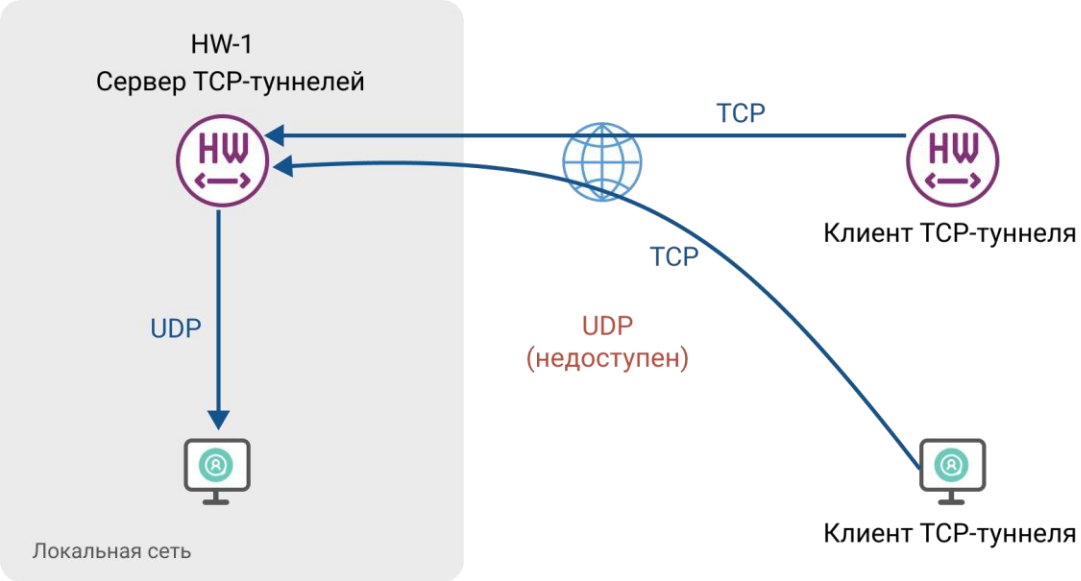

Рисунок 28. Настройка TCP-туннеля

В данном сценарии:

- Клиент TCP-туннеля — удаленный узел, подключенный через TCP-туннель. Клиентом может быть ViPNet-клиент или координатор.
- Сервер TCP-туннелей — координатор, выполняющий функцию сервера соединений, через который происходит подключение TCP-клиентов.

Если клиент TCP-туннеля не может связаться со своим сервером соединений (сервером TCP-туннелей) по протоколу UDP, он автоматически начинает устанавливать с ним соединение через TCP-туннель. Сервер соединений (сервер TCP-туннелей) передает полученные от клиента IP-пакеты дальше на узлы назначения по протоколу UDP.

ViPNet Coordinator HW может работать в режиме сервера TCP-туннелей или клиента TCP-туннеля, подключаясь к своему серверу соединений. Исполнения HW10 и HW50 не поддерживают режим сервера TCP-туннелей.

Настройка сервера TCP-туннелей

Для работы координатора в роли сервера TCP-туннелей:

- На ViPNet Coordinator HW в файле `iplir.conf` в списке адресов доступа (параметр `accessiplist` в собственной секции `[id]`) должен быть задан хотя бы один публичный адрес, поскольку для установления TCP-соединения клиент использует именно публичный IP-адрес доступа сервера соединений. Подробнее см. документ «Справочник команд и конфигурационных файлов».
- На ViPNet Coordinator HW включите функцию сервера TCP-туннелей и настройте порт для входящих TCP-соединений (см. описание ниже).
- На клиентах должен быть задан номер порта, который используется на ViPNet Coordinator HW для TCP-соединений.

  Номер порта должен поступать клиенту от сервера соединений в составе служебной информации. Если служебная информация не поступила, то порт на клиенте можно задать вручную.
- В случае подключения координатора через межсетевой экран настройте правило, разрешающее соединения через TCP-туннель.

Примечание. ViPNet Coordinator HW может поддерживать не более 100 соединений через TCP-туннель.

При соединении через TCP-туннель клиентам не будут приходить уведомления в случае рассинхронизации времени.

Чтобы настроить сервер TCP-туннелей:

1. Выберите **Защищенная сеть (VPN)** > **Управляющие соединения** > **Мой узел ViPNet**.
2. Включите **TCP-туннель**.
3. Нажмите .
4. Выберите роль координатора **Сервер**.
5. Укажите **TCP-порт координатора** для TCP-соединений.

   После изменения номера порта на все сетевые узлы, для которых данный координатор является сервером соединений, будет отправлена служебная информация с новым номером порта для TCP-соединений.
6. Нажмите **Сохранить**.

Примечание. В случае если протокол UDP перестал блокироваться, соединение по данному протоколу восстановится при следующих условиях:

- по истечении тайм-аута отправки служебных IP-пакетов с клиента на сервер соединений (по умолчанию тайм-аут равен 5 минутам);
- после проверки соединения этого узла с другим;
- после смены IP-адреса узла (например, при изменении точки доступа к интернету).

Настройка TCP-клиента

Чтобы ViPNet Coordinator HW мог работать как TCP-клиент, он должен быть подключен к сети в режиме «С динамической трансляцией адресов». Подробнее см. документ «Настройка с помощью командного интерпретатора».

Чтобы настроить TCP-клиент:

1. Выберите **Защищенная сеть (VPN) > Управляющие соединения > Мой узел ViPNet**.
2. Включите **TCP-туннель**.
3. Нажмите .
4. Выберите роль координатора **Клиент**.
5. Выберите один из режимов подключения:
   - **Подключаться при отсутствии связи по UDP**.
   - **Подключаться всегда**.
6. Укажите **Порт сервера TCP-туннелей**.
7. Нажмите **Сохранить**.

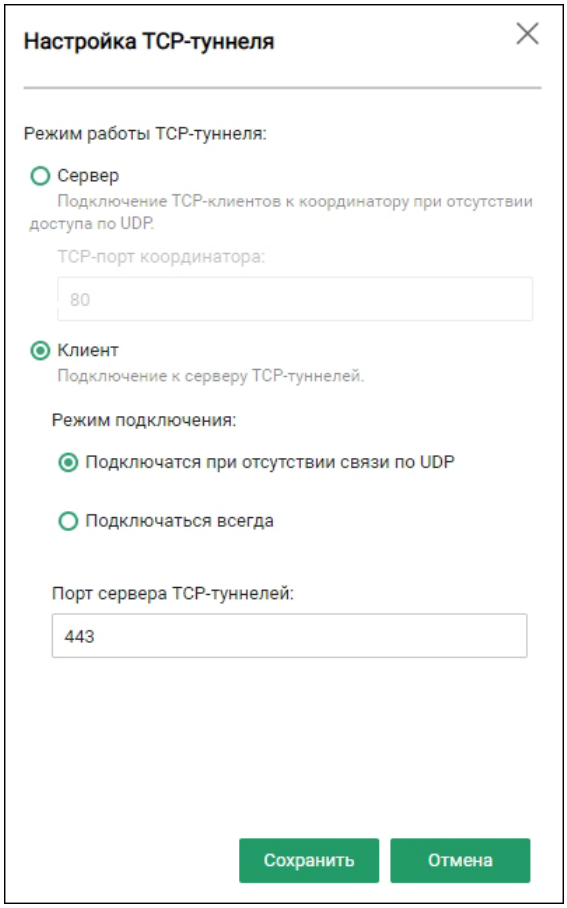

Рисунок 29. Настройка TCP-клиента

5

Настройка сетевых фильтров

Основные принципы фильтрации трафика

Виды трафика

Фильтрации подвергается весь трафик, который проходит через ViPNet Coordinator HW:

- → — незашифрованный (открытый) трафик между открытыми (или открытым и защищенным) узлами;
- → — зашифрованный (защищенный) трафик между узлами сети ViPNet.

Трафик может быть локальным или транзитным:

- локальный трафик — трафик, в котором ViPNet Coordinator HW является получателем или отправителем IP-пакетов;
- транзитный трафик — трафик, в котором ViPNet Coordinator HW не является ни получателем, ни отправителем IP-пакетов.

ViPNet Coordinator HW обрабатывает трафик, разделяя его на следующие виды:

- локальный незашифрованный трафик — между открытым узлом и ViPNet Coordinator HW. Обрабатывается локальными фильтрами открытой сети;
- локальный зашифрованный трафик — трафик между узлами сети ViPNet, при этом ViPNet Coordinator HW является получателем или отправителем IP-пакетов. Обрабатывается фильтрами защищенной сети;
- туннелируемый трафик — трафик между двумя открытыми (или открытым и защищенным) узлами, зашифрованный в пределах сети ViPNet. Обрабатывается фильтрами туннелируемых узлов;

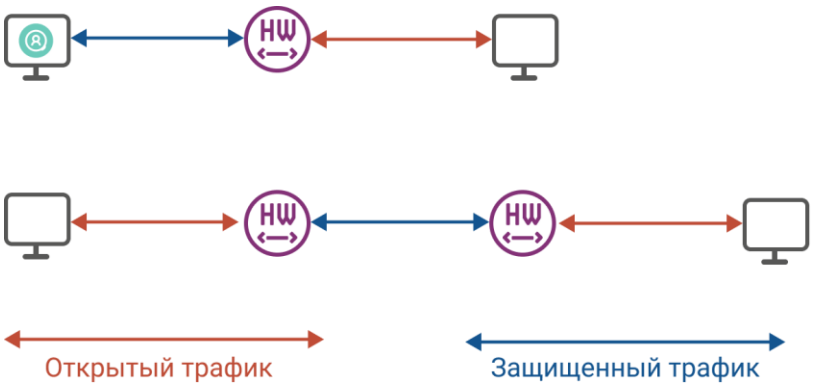

Рисунок 30. Туннелируемый трафик

- транзитный трафик — зашифрованный или незашифрованный трафик между узлами, проходящий через координатор, который не является ни отправителем, ни получателем IP-пакетов. Обрабатывается транзитными фильтрами открытой сети.

Принципы фильтрации

Принципы фильтрации трафика:

- Все входящие и исходящие открытые и защищенные IP-пакеты обрабатываются сетевыми фильтрами в порядке убывания приоритета этих фильтров.
- Если IP-пакет соответствует условию одного из фильтров, он пропускается или блокируется этим фильтром. При этом фильтры с более низким приоритетом не применяются.
- Если IP-пакет был пропущен одним из фильтров, ответные IP-пакеты (включая служебные ICMP-пакеты) в рамках текущего соединения будут пропускаться автоматически.
- Если IP-пакет не был обработан ни одним из фильтров, он блокируется фильтром по умолчанию.

ViPNet Coordinator HW обрабатывает входящий трафик следующим образом:

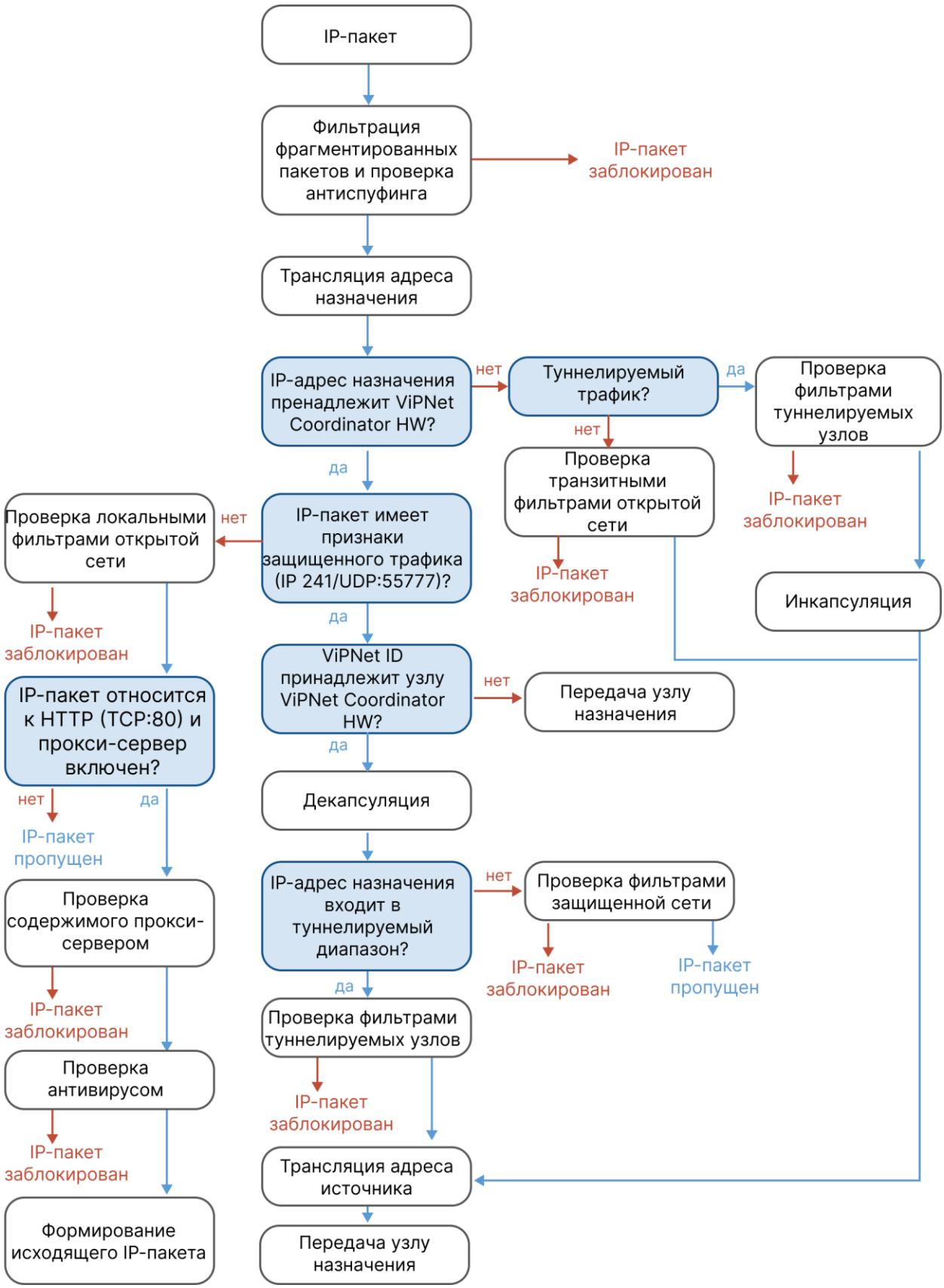

Рисунок 31. Схема фильтрации трафика

IP-пакет, поступивший на сетевой интерфейс ViPNet Coordinator HW, последовательно проходит ряд проверок:

1. IP-пакет проверяется на фрагментацию, если эта проверка включена (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка дополнительных параметров межсетевого экрана»). Если IP-пакет фрагментирован, он блокируется, иначе — передается на следующий шаг проверки.
2. IP-пакет обрабатывается правилами антиспуфинга, если он включен (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка антиспуфинга»). В результате IP-пакет блокируется или передается на следующий шаг проверки.
3. В случаях, указанных ниже, выполняется трансляция IP-адреса назначения (см. Трансляция адреса назначения):
   - IP-пакет удовлетворяет условиям правила трансляции адресов (см. Создание и изменение правил трансляции адресов).
   - Включена трансляция прикладного протокола, к которому относится IP-пакет (см. Настройка обработки прикладных протоколов).
   - IP-пакет соответствует протоколу HTTP (TCP: 80) и прокси-сервер работает в «прозрачном» режиме (см. Настройка параметров прокси-сервера). В этом случае с помощью трансляции адреса назначения транзитный трафик перенаправляется на ViPNet Coordinator HW и обрабатывается как локальный трафик открытой сети.
4. Если IP-пакет адресован ViPNet Coordinator HW и имеет признаки защищенного трафика (протокол IP/241 или протокол UDP и порт 55777 или другой порт, настроенный администратором), то в IP-пакете проверяется идентификатор узла ViPNet (ViPNet ID):
   - Если ViPNet ID не принадлежит ViPNet Coordinator HW, в IP-пакете преобразуются IP-адреса и порты в соответствии с имеющейся информацией о ближайшей к узлу назначения точке доступа. Затем IP-пакет отправляется в сеть для передачи узлу назначения.
   - Если ViPNet ID принадлежит ViPNet Coordinator HW, выполняется расшифровка и декапсуляция IP-пакета. Полученный IP-пакет (исходный IP-пакет) проверяется на принадлежность туннелируемому трафику:
     - Если IP-адрес назначения в исходном IP-пакете входит в туннелируемый диапазон ViPNet Coordinator HW, IP-пакет проверяется фильтрами туннелируемых узлов. В результате IP-пакет блокируется или отправляется на туннелируемый узел после трансляции адреса источника (см. Трансляция адреса источника).
     - Если IP-адрес назначения в исходном IP-пакете не входит в туннелируемый диапазон ViPNet Coordinator HW, IP-пакет проверяется фильтрами защищенной сети, после чего блокируется или пропускается.
5. Если IP-пакет адресован ViPNet Coordinator HW и не имеет признаков защищенного трафика, IP-пакет проверяется локальными фильтрами открытой сети. В результате IP-пакет блокируется или проходит следующие проверки:

   5.1 Если IP-пакет относится к протоколу HTTP (TCP: 80), он проверяется прокси-сервером на прикладном уровне. Если прокси-сервер выключен, IP-пакет пропускается.

5.2 После проверки прокси-сервером выполняется антивирусная проверка IP-пакета, если она включена (см. Настройка антивирусной проверки). В результате IP-пакет блокируется или формируется новый исходящий IP-пакет.

6 Если IP-пакет адресован не ViPNet Coordinator HW, а другому узлу, проверяется принадлежность IP-пакета туннелируемому трафику:

- Если IP-адрес отправителя входит в туннелируемый диапазон ViPNet Coordinator HW, а IP-адрес получателя входит в туннелируемый диапазон другого координатора или принадлежит защищенному узлу, IP-пакет проверяется фильтрами туннелируемых узлов. В результате IP-пакет блокируется или отправляется получателю после процедур инкапсуляции и трансляции адреса источника.
- Если IP-адрес отправителя входит в туннелируемый диапазон ViPNet Coordinator HW, но при этом принадлежит защищённому узлу, то трафик не является туннелируемым и проверяется транзитными фильтрами открытой сети.
- Если IP-пакет не принадлежит туннелируемому трафику, он проверяется транзитными фильтрами открытой сети. В результате IP-пакет блокируется или отправляется получателю после трансляции адреса источника.

Особенности при настройке фильтрации трафика на ViPNet Coordinator HW:

- TCP-порт 2047 и UDP-порт 2046 являются служебными портами ViPNet Coordinator HW, поэтому входящий открытый трафик, поступающий на эти порты, блокируется без возможности настройки.
- Изменения в конфигурации межсетевого экрана, влияющие на открытый транзитный трафик, начинают действовать сразу, в том числе для уже установленных ранее соединений.

  Изменения в конфигурации межсетевого экрана, влияющие на другие виды трафика, будут действовать только для новых соединений. К уже установленным соединениям изменения не будут применены до истечения времени жизни соединения. Чтобы принудительно применить изменения ко всем соединениям, в командном интерпретаторе поочередно выполните команды:

  ```
  hostname# vpn stop
  hostname# vpn start
  ```

Общие сведения о сетевых фильтрах

Различаются сетевые фильтры 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.** К открытым узлам также относятся компьютеры с ПО ViPNet Registration Point.

- Фильтры защищенной сети могут разрешать или блокировать обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел ViPNet Coordinator HW 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. Создаются в ViPNet Coordinator HW автоматически. Имеют самый высокий приоритет и недоступны для редактирования.
- Фильтры, поступившие в составе политик безопасности (фильтры из управляющего приложения). Политика безопасности представляет собой набор параметров, регулирующих безопасность сетевого узла. Она формируется администратором сети ViPNet в ViPNet Policy Manager или Policy Management (модуль ViPNet Prime), может включать сетевые фильтры и правила трансляции сетевых адресов и рассылается на сетевые узлы ViPNet с помощью транспортного сервера MFTP. При получении политики безопасности из ViPNet Policy Manager или Policy Management (модуль ViPNet Prime) она немедленно применяется на узле.

  Фильтры, поступившие в составе политик безопасности, применяются после служебных фильтров. Недоступны для редактирования.
- Предустановленные фильтры и фильтры, заданные пользователем. Предустановленные фильтры разрешают только некоторые типы IP-пакетов. Для работы с какими-либо дополнительными сервисами пользователю необходимо создать свои фильтры.

  Применяются после фильтров, поступивших в составе политик безопасности. Доступны для редактирования.
- Блокирующий фильтр по умолчанию.

Применяется после всех фильтров. Недоступен для редактирования.

Последовательность применения сетевых фильтров в порядке убывания приоритета представлена ниже.

Рисунок 32. 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.

Группы объектов

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

В зависимости от типа объединяемых объектов различаются следующие группы:

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

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 сетевых фильтрах и правилах трансляции адресов (см. Создание и изменение правил трансляции адресов), а также при создании пользовательских групп объектов. Такие группы объектов не отображаются в списках групп (см. Просмотр групп объектов), их нельзя ни изменить, ни удалить.
- Группы объектов из ViPNet Policy Manager или Policy Management (модуль ViPNet Prime) — группы, получаемые в составе политик безопасности, и используемые в соответствующих фильтрах (см. Общие сведения о сетевых фильтрах). 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. Такие группы можно использовать для задания параметров сетевых фильтров и правил трансляции адресов (см. Создание и изменение правил трансляции адресов), а также при создании других пользовательских групп объектов.

Системные группы объектов

Таблица 2. Системные группы объектов

Имя группы в веб-интерфейсе (в командном интерпретаторе)	Описание
Все клиенты (allclients)	Все клиенты, 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 ViPNet Coordinator HW. 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.
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 адреса получателя. 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

- Группы IP-адресов:
  - `PrivateNetworkIP` (частные IP-адреса) — IP-адреса локальных сетей: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16.
  - `InternetIP` (публичные IP-адреса) — IP-адреса за исключением частных IP-адресов.
  - `HttpProxyUsers` — IP-адреса локальных сетей, которым разрешен доступ к прокси-серверу. Группа создается автоматически при первом запуске прокси-сервера.
- Группы протоколов (см. Пользовательские группы протоколов по умолчанию).
- Группы расписаний:
  - `Workdays` — рабочие дни недели (с понедельника по пятницу).
  - `Weekends` — выходные дни недели (суббота и воскресенье).

Просмотр групп объектов

Чтобы просмотреть пользовательские группы объектов и группы объектов, полученные из ViPNet Policy Manager или Policy Management (модуль ViPNet Prime):

1 Выберите **Межсетевой экран** > **Группы объектов**.

2 Выберите вкладку группы объектов: **Узлы ViPNet**, **IP-адреса**, **Интерфейсы**, **Протоколы** или **Расписания**.

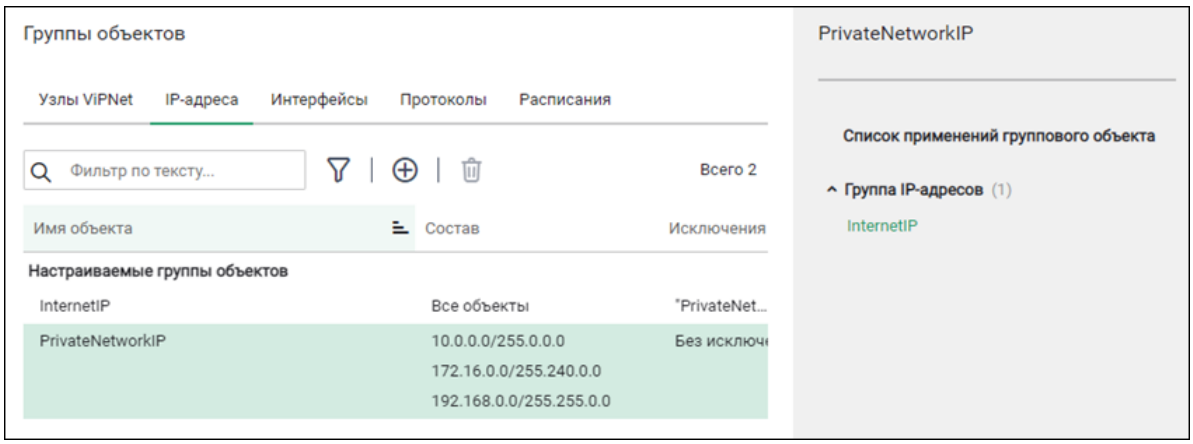

Рисунок 33. Просмотр групп IP-адресов

3 Чтобы просмотреть применение группы объектов, щелкните ее в списке.

Создание и изменение групп объектов

1 Выберите **Межсетевой экран** > **Группы объектов**.

2 Выберите вкладку группы объектов.

3 Чтобы создать группу объектов, нажмите **Добавить**.

4 Чтобы изменить группу объектов, наведите указатель на группу объектов и нажмите .

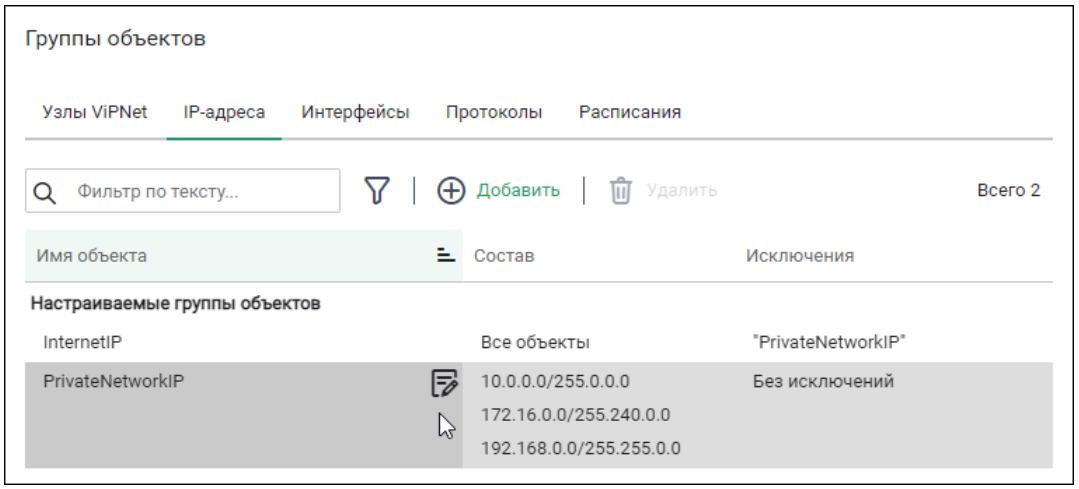

Рисунок 34. Изменение группы объектов

5 Задайте параметры:

5.1 Задайте имя группы.

Внимание! Если имя группы объектов начинается с символа @, или содержит символы " и пробел, то эту группу можно использовать только в настройке ViPNet Coordinator HW с помощью веб-интерфейса; в настройке с помощью командного интерпретатора группа будет недоступна.

Группы объектов из разных категорий не могут иметь одинаковые имена.

5.2 В списках **Состав** и **Исключения** укажите объекты. В зависимости от их типа воспользуйтесь рекомендациями разделов:

- Группа сетевых узлов ViPNet.
- Группа IP-адресов.
- Группа интерфейсов.
- Группа протоколов.
- Группа расписаний.

Чтобы быстро изменить значение в составе (исключениях) группы объектов, наведите курсор на строку и нажмите  .

Внимание! Количество объектов, входящих в группу, не должно превышать 1000.

5.3 Нажмите **Сохранить**.

6 Чтобы изменения вступили в силу, нажмите **Применить все**.

Группа сетевых узлов ViPNet

Чтобы добавить (исключить) объект:

1 Раскройте один из списков: **Состав** (чтобы добавить объект) или **Исключения** (чтобы исключить объект).

2 Выберите объект:

- **Сетевой узел ViPNet**, с которыми связан узел ViPNet Coordinator HW (первым в этом списке отображается собственный узел).
- **Номер защищенной сети ViPNet**, с которой связана ваша сеть ViPNet — укажите номер этой сети (добавляются или исключаются все узлы сети).
- **Шаблон имени сетевых узлов ViPNet** — укажите шаблон имени узлов, используя ? для замены одного символа, и * для замены нескольких символов.
- **Группа узлов ViPNet** — выберите созданную ранее группу узлов.
- Чтобы добавить (исключить) системную группу объектов, выберите эту группу в списке. Группу **Все объекты** можно только добавить.

3 Нажмите **Сохранить**.

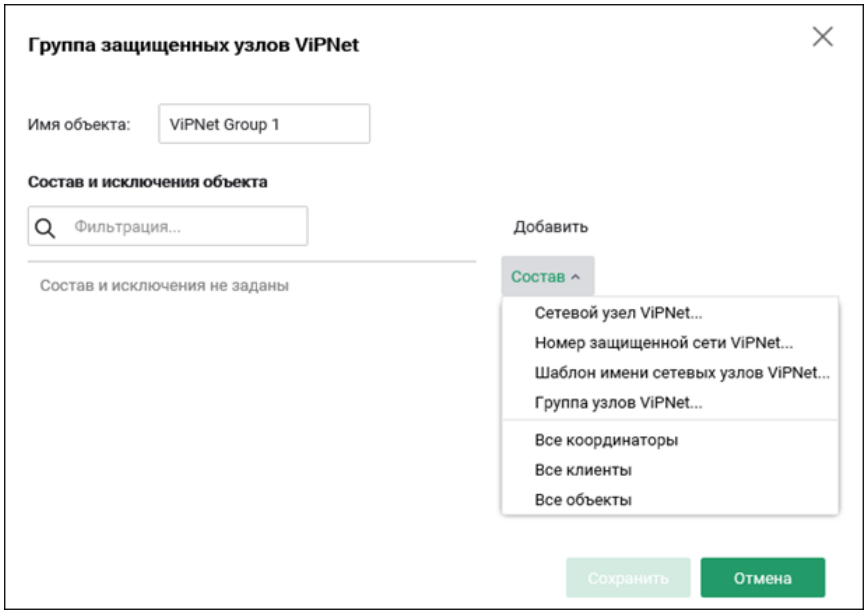

Рисунок 35. Добавление сетевого узла ViPNet в группу

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.

Группа IP-адресов

1 Раскройте один из списков: **Состав** (чтобы добавить объект) или **Исключения** (чтобы исключить из группы).

2 Выберите объект:

- **IP-адрес или диапазон адресов** — выберите тип адреса, затем введите параметры;

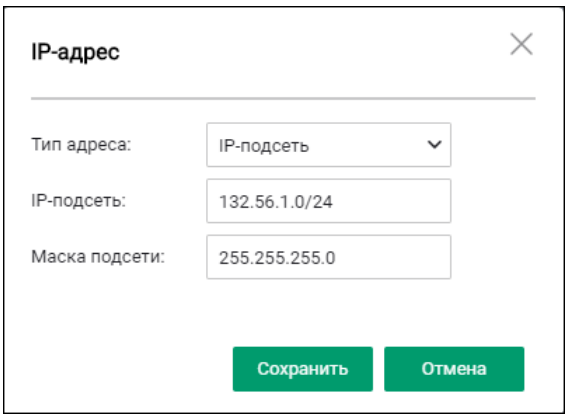

Рисунок 36. Добавление IP-адреса подсети

- **DNS-имя**;
- **Группы IP-адресов**;

- **Все объекты** (можно только добавить).

Нажмите **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 и правил трансляции адресов (см. Создание и изменение правил трансляции адресов)

Группа интерфейсов

Чтобы добавить (исключить) объект:

1 Раскройте один из списков: **Состав** или **Исключения**.

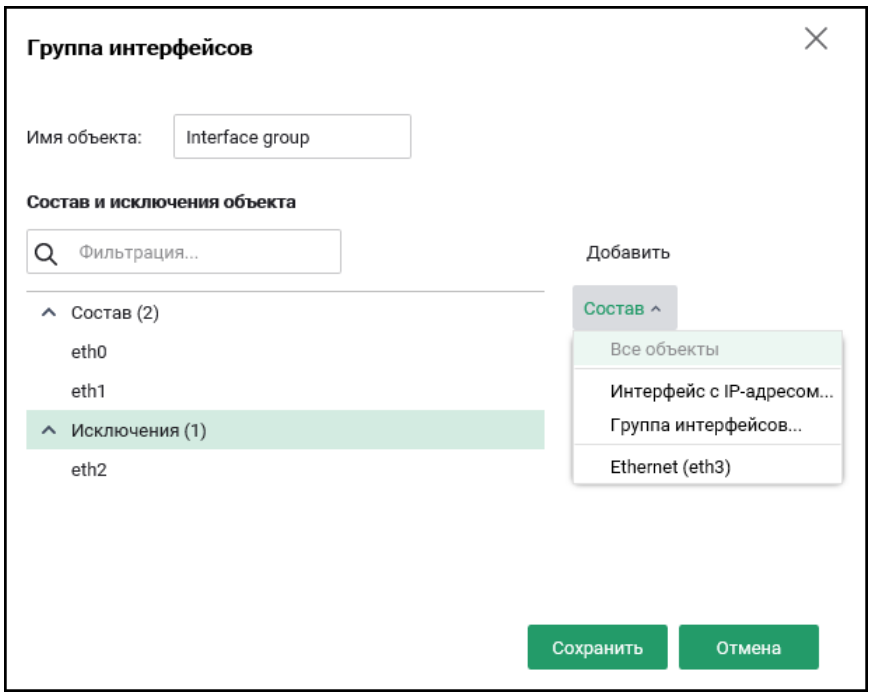

Рисунок 37. Добавление сетевых интерфейсов в группу

2 Выберите объект:

- Чтобы добавить (исключить) один или несколько интерфейсов собственного узла, выберите имя этого интерфейса (**Ethernet (eth0)**, **Ethernet (eth1)** и т.д.).
- Чтобы 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.

- Чтобы добавить (исключить) одну или несколько групп сетевых интерфейсов, выберите **Группа интерфейсов** и установите флажки рядом с нужными группами.
- Чтобы добавить в группу все сетевые интерфейсы и группы интерфейсов, выберите **Все объекты**.

3 Нажмите **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать сетевые интерфейсы при создании и изменении фильтров открытой сети и правил трансляции адресов (см. Создание и изменение правил трансляции адресов).

Группа протоколов

Чтобы добавить (исключить) объект:

1 Раскройте один из списков **Состав** или **Исключения**.

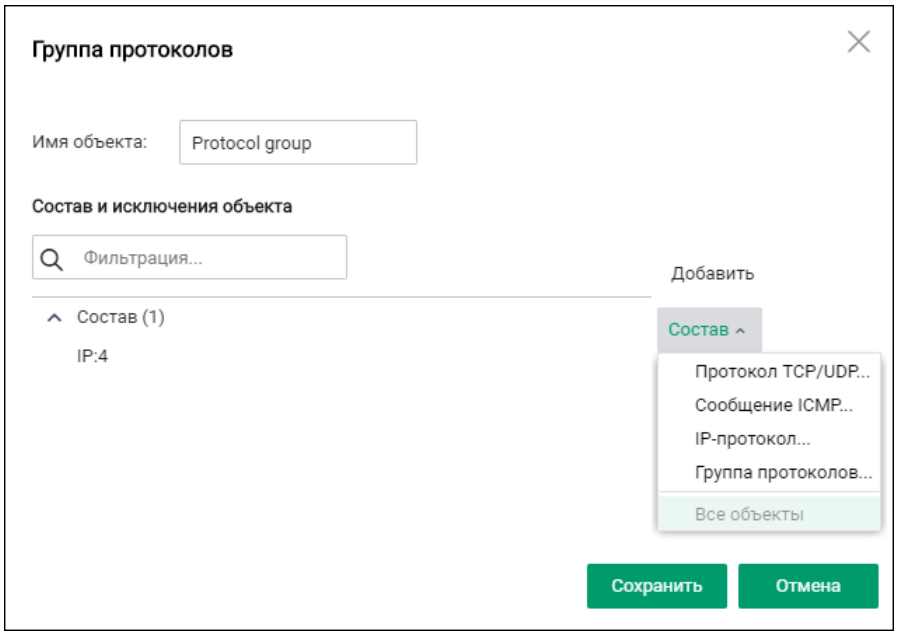

Рисунок 38. Добавление группы протоколов

2 Выберите объект:

- 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 **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 **Диапазон портов** и укажите начальный и конечный номера портов в диапазоне от 0 до 65535.

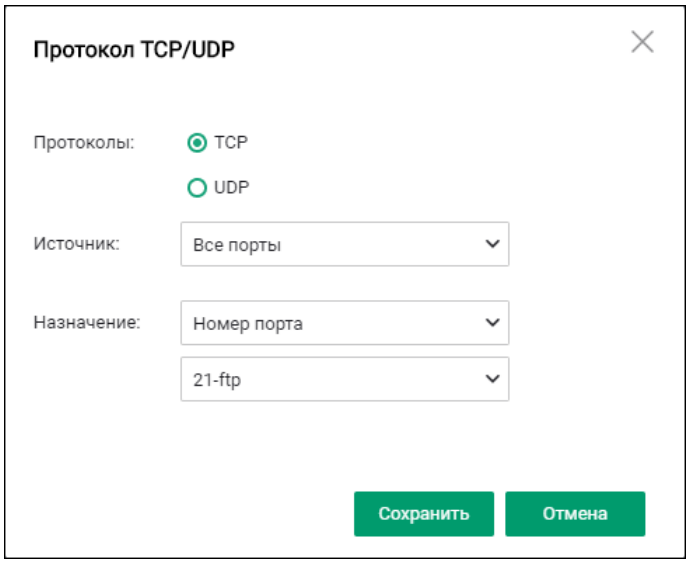

Рисунок 39. Добавление протокола в группу

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

3 Нажмите **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать протоколы при создании и изменении сетевых фильтров и правил трансляции адресов (см. Создание и изменение правил трансляции адресов).

Группа расписаний

Чтобы добавить объект в группу расписаний или исключить его:

1 Раскройте один из списков: **Состав** или **Исключения**.

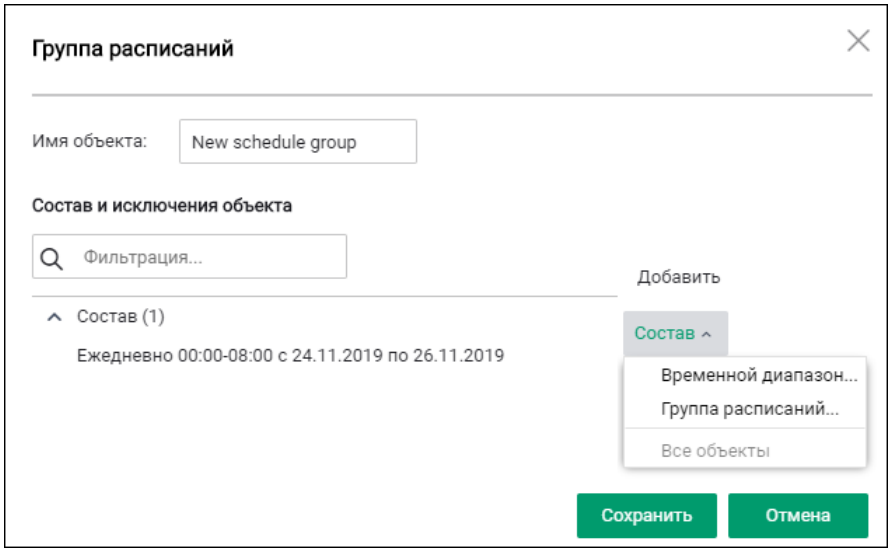

Рисунок 40. Добавление группы расписаний

2 Выберите объект:

- Чтобы указать интервал времени и периодичность, когда фильтр или правило трансляции сетевых адресов будет применяться (не применяться), выберите **Временной диапазон** и выполните:
  - в разделе **Время выполнения фильтра** укажите интервал времени;
  - в разделе **Период выполнения фильтра** выберите:
    - **Ежедневно** — чтобы фильтр или правило трансляции применялось (не применялось) каждый день. Чтобы задать другой период, выберите **в период** и укажите интервал дат, в который фильтр или правило трансляции будет применяться (не применяться) ежедневно;
    - **Еженедельно** — чтобы фильтр или правило трансляции применялось (не применялось) в определенные дни недели. Выберите дни недели.

Примечание. Чтобы создать круглосуточное расписание, установите время выполнения фильтра с 00:00 по 00:00. Если период выполнения фильтра задается явным указанием дат, то в расписание не входит дата окончания периода.

Например, чтобы фильтр работал круглосуточно в период с 01.03 по 08.03 включительно, установите время выполнения фильтра с 00:00 по 00:00, а период выполнения фильтра с 01.03 по 09.03.

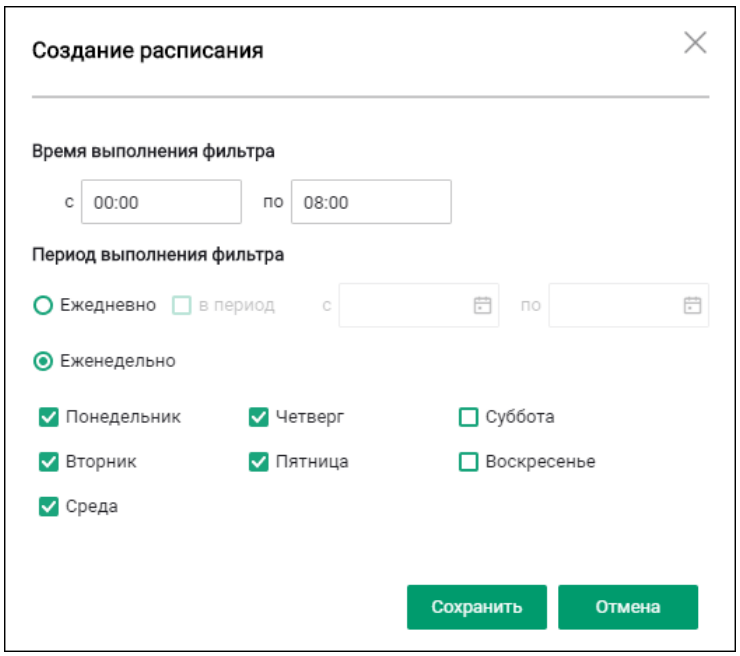

Рисунок 41. Добавление расписания в группу

- Чтобы добавить (исключить) одну или несколько групп расписаний, выберите **Группа расписаний** и выберите группы.
- Чтобы добавить в группу все временные диапазоны и группы расписаний, выберите **Все объекты**.

3 Нажмите **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать расписания при создании и изменении сетевых фильтров.

Просмотр сетевых фильтров

1 Выберите **Межсетевой экран** > **Сетевые фильтры**.

2 Выберите вкладку сетевых фильтров нужного типа, чтобы посмотреть список фильтров и информацию о них.

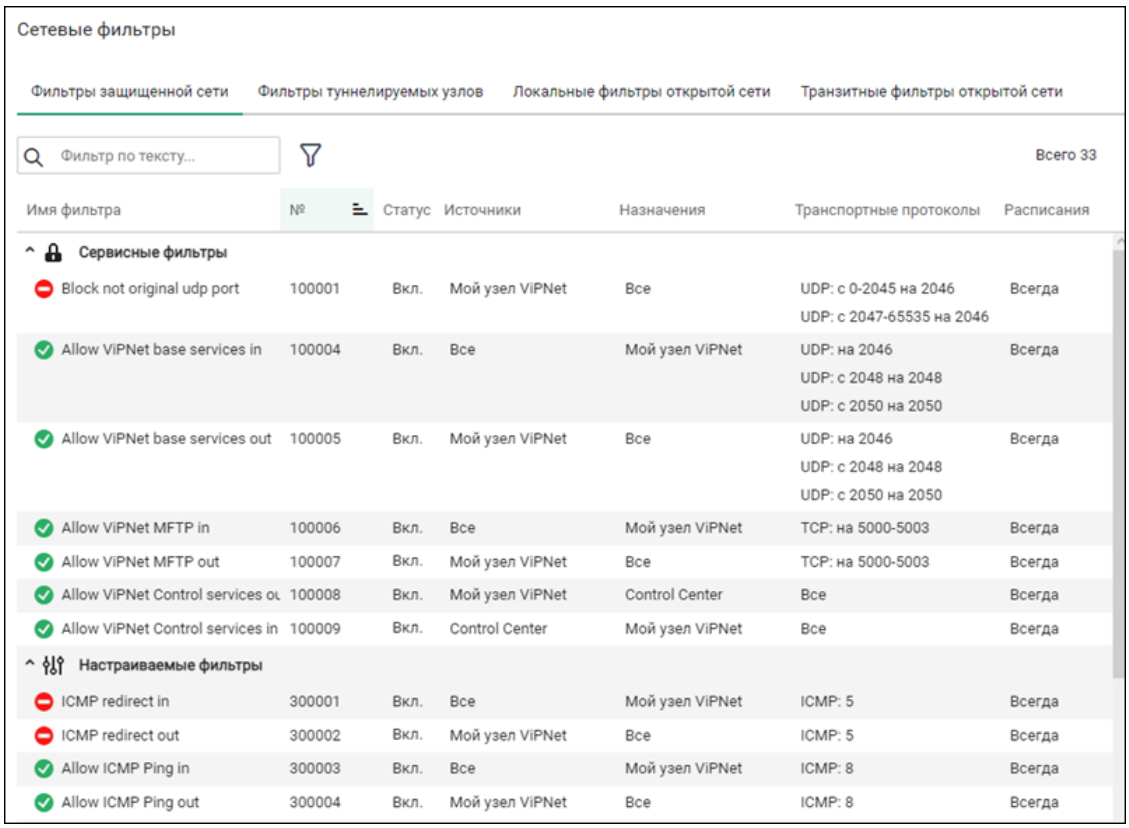

Рисунок 42. Просмотр сетевых фильтров

Создание и изменение сетевых фильтров

1 Выберите **Межсетевой экран** > **Сетевые фильтры**.

2 Выберите вкладку сетевых фильтров нужного типа:

- **Фильтры защищенной сети;**
- **Фильтры туннелируемых узлов;**
- **Локальные фильтры открытой сети**;
- **Транзитные фильтры открытой сети.**

3 Выполните одно из действий:

- Чтобы создать фильтр, нажмите **Добавить**;
- Чтобы изменить фильтр, наведите курсор на название фильтра и нажмите ;
- Чтобы изменить значение одного параметра фильтра, наведите курсор на это значение и нажмите .

4 В окне **Параметры сетевого фильтра** укажите: действие (блокировать или пропускать трафик), протоколы, источники, назначения, расписания.

Примечание. Не используйте в названии фильтра кириллицу.

При срабатывании фильтра в системном журнале зафиксируется событие. События, в описании которых есть символы на кириллице, не отображаются при поиске по тексту сообщений.

В разделе **Признаки трафика, по группам** будут сформированы значения признаков трафика по группам протоколов, источников, назначений и расписаний в соответствии с типом фильтра. Вы можете изменить или удалить ранее введенные настройки с помощью кнопок и .

Если признаки трафика не указаны, правило применяется ко всем протоколам, источникам и назначениям, круглосуточно.

Примечание. При задании источника для фильтров защищенной сети:

- Нельзя использовать другие источники совместно с **Мой узел ViPNet** и **Другие узлы**.
- Фильтры защищенной сети используются только для локального защищенного трафика, поэтому в качестве источника или назначения должен быть задан **Мой узел ViPNet**. Вместо собственного узла назначением также могут быть **Широковещательные адреса**.

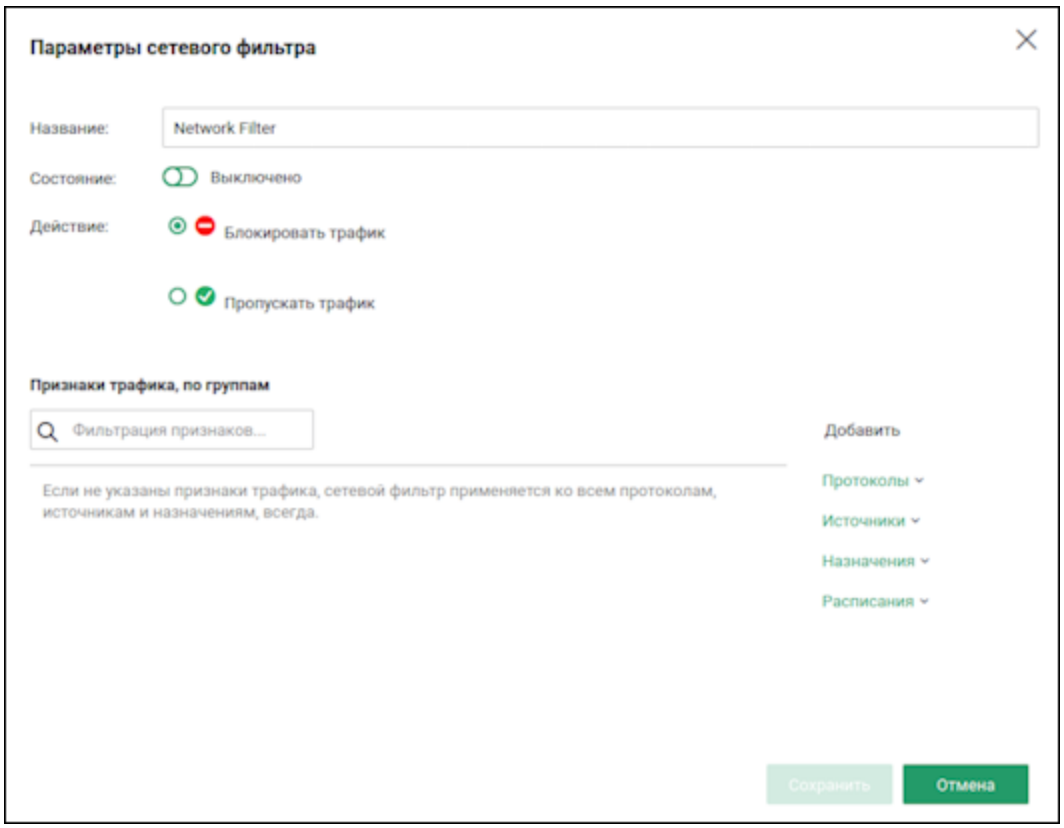

Рисунок 43. Изменение признаков трафика по группам

5 Нажмите **Сохранить**.

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

Чтобы изменить приоритет фильтра, перетащите его на нужную строку с помощью значка ⠿.

Чтобы изменения вступили в силу, нажмите **Применить все**.

Пример использования групп объектов и сетевых фильтров

Допустим, в компании координатор ViPNet Coordinator HW туннелирует почтовый сервер. 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 выполняется по протоколам SMTP, POP3 и IMAP. Поэтому надо 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).

Чтобы создать группу почтовых протоколов SMTP, POP3 и IMAP:

1 Выберите **Межсетевой экран** > **Группы объектов**.

2 Выберите вкладку **Протоколы** и нажмите **Добавить:**

2.1 В поле **Имя объекта** укажите имя группы.

2.2 Чтобы добавьте протокол SMTP, в списке **Состав** выберите **Протокол TCP/UDP**:

2.2.1 Протоколы — TCP.

2.2.2 Источник — Все порты.

2.2.3 Назначение — Номер порта и укажите номер **25-smtp**.

2.2.4 Нажмите **Сохранить**.

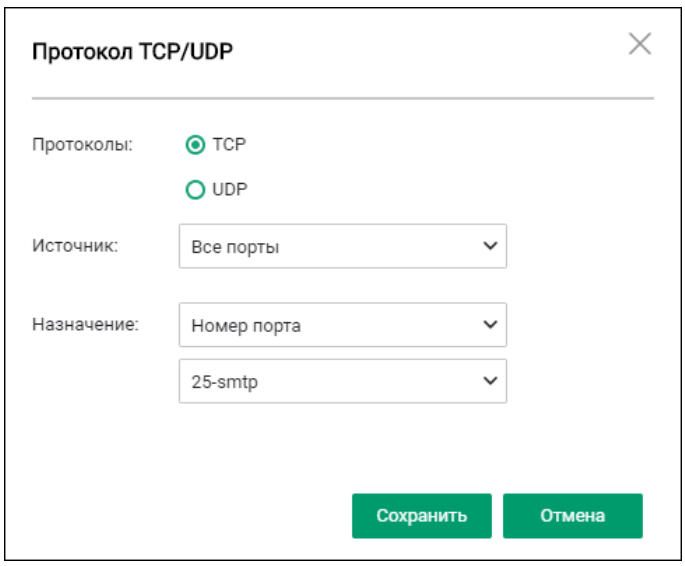

Рисунок 44. Добавление протокола SMTP в группу

2.3 Аналогичным образом добавьте протоколы POP3 (порт — 110) и IMAP (порт — 143).

3 Нажмите **Сохранить**.

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

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

1 Выберите **Межсетевой экран** > **Сетевые фильтры**.

2 Выберите вкладку **Локальные фильтры открытой сети** и нажмите **Добавить**:

2.1 Укажите имя сетевого фильтра.

2.2 Включите фильтр в поле **Состояние**.

2.3 Переключатель **Действие** установите в положение **Пропускать трафик**.

2.4 В списке **Протоколы** выберите **Группа протоколов:**

2.4.1 Выберите ранее созданную группу почтовых протоколов.

2.4.2 Нажмите **Сохранить**.

2.5 Нажмите **Сохранить**.

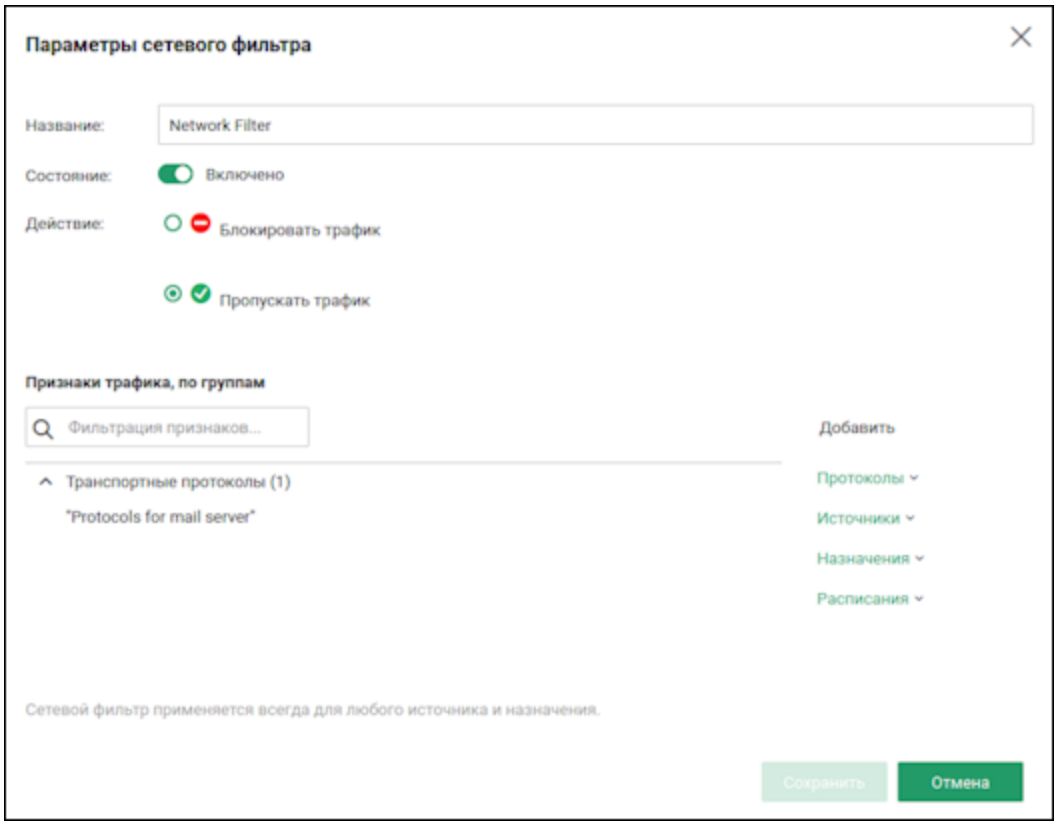

Рисунок 45. Создание локального фильтра открытой сети на почтовом сервере

3 Чтобы изменения вступили в силу, на странице **Сетевые фильтры** нажмите **Применить все**.

Обработка фрагментированных пакетов

Сетевые протоколы содержат механизмы управления размером IP-пакетов. ViPNet Coordinator HW при шифровании трафика добавляет к каждому IP-пакету служебный заголовок (выполняет инкапсуляцию), вследствие чего размер сформированного ViPNet-пакета может получиться больше заданного в MTU и потребует фрагментации. В свою очередь, некоторые сервисы не позволяют фрагментировать свои пакеты (например, видео-трафик), используя флаг Don't fragment (DF). В любом случае, обработка фрагментированных пакетов снижает пропускную способность сети (так как два пакета вместо одного суммарно длиннее, и их обработка требует больше ресурсов), поэтому в ViPNet Coordinator HW предусмотрены средства решения этой проблемы.

Установка TCP-соединения

На этапе установки соединения по протоколу TCP сервер и клиент обмениваются значениями MSS (максимальная длина сегмента), которые основаны на MTU их сетевых интерфейсов, и в итоге принимается минимальное из двух значений. В результате инкапсуляции IP-пакета ViPNet Coordinator HW учитывает размер, на который был увеличен IP-пакет после инкапсуляции, и уменьшает значение MSS с учетом этих данных.

Также вы можете настроить дополнительное уменьшение размера MSS с помощью параметра `mssdecrease` конфигурационного файла `iplir.conf` (подробнее см. в документе «Справочник команд и конфигурационных файлов», раздел «Файл iplir.conf»).

Обработка IP-пакетов с флагом Don't fragment (DF)

Рассмотрим случай, когда ViPNet Coordinator HW туннелирует сетевые узлы, которые отправляют через него IP-пакеты с размером, не превышающим размер MTU, заданный на внешнем сетевом интерфейсе ViPNet Coordinator HW. При шифровании трафика размер IP-пакета может превысить MTU, и в этом случае IP-пакет будет фрагментирован.

Если же такой IP-пакет имеет флаг DF, запрещающий фрагментацию, то, в зависимости от его размера, будет выполнен один из сценариев:

- Если размер IP-пакета после инкапсуляции не превышает MTU, то ViPNet Coordinator HW его пропустит и сбросит флаг DF (который не восстановится при последующей декапсуляции).
- Если размер IP-пакета после инкапсуляции превышает MTU, то ViPNet Coordinator HW его отбросит (при этом в журнале IP-пакетов появится запись о блокировке с кодом события 97) и отправит ICMP-сообщение о необходимости фрагментации IP-пакета (ICMP type 3, code 4) его отправителю. В зависимости от настройки отправителя IP-пакетов необходимо выполнить одно из действий:
    - Если отправитель IP-пакетов с флагом DF не получает (не обрабатывает) такие ICMP-сообщения, то ему необходимо самостоятельно уменьшить размер IP-пакетов.

- Если отправитель IP-пакетов с флагом DF принимает и корректно обрабатывает ICMP-сообщения ICMP type 3, code 4 (в соответствии с RFC 4459), то такой трафик будет пропущен.

Блокировка входящих фрагментированных пакетов

Фрагментированные IP-пакеты используются как средство сетевой атаки «отказ в обслуживании» (DDoS). В качестве меры защиты от такой атаки используется опция межсетевого экрана `block-fragmented-packets`, которая блокирует все входящие фрагментированные IP-пакеты на всех сетевых интерфейсах. Подробнее см. в документе «Настройка с помощью командного интерпретатора», раздел «Настройка дополнительных параметров межсетевого экрана».

6

Настройка правил трансляции адресов

Трансляция сетевых адресов (NAT)

Трансляция сетевых адресов (NAT) — механизм преобразования IP-адресов одной сети в IP-адреса другой сети. Технология трансляции сетевых адресов описана в RFC 2663 (IP Network Address Translator Terminology and Considerations).

ViPNet Coordinator HW может выполнять:

- Трансляцию адреса источника (маскарадинг (masquerading) или динамическую трансляцию).

  В этом случае при прохождении через координатор IP-пакетов от отправителей с частными IP-адресами в них заменяется адрес отправителя на внешний (реальный) адрес координатора. При получении ответных пакетов в них подменяется IP-адрес получателя обратно на частный IP-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. В результате локальные сети, использующие частные IP-адреса, получают доступ к ресурсам интернета.

- Трансляцию адреса назначения (перенаправление портов (port forwarding) или статическую трансляцию).

  В этом случае IP-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 узла 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.

- Одновременную трансляцию сетевых адресов источника и назначения.

  Используется в сложных схемах маршрутизации трафика.

Трансляция сетевых адресов выполняется координатором, только если настроены соответствующие правила (см. Создание и изменение правил трансляции адресов). Координатор должен иметь как минимум два сетевых интерфейса:

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

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

Трансляция адреса назначения

Трансляция адреса узла назначения применяется 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 сетевых узлов публичный IP-адрес координатора. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.

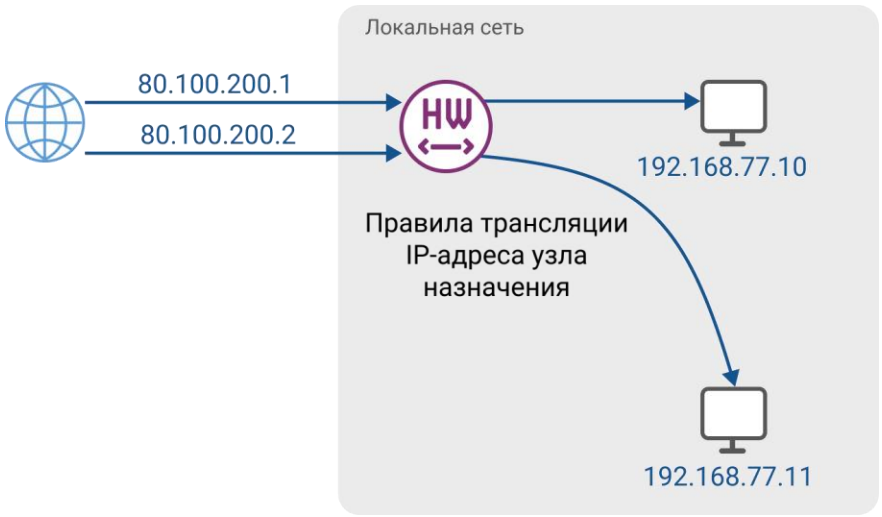

Рисунок 46. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

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

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) локальным IP-адресом в соответствии с правилом. Затем пакет передается через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.
- При прохождении ответных IP-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 узлу в интернете.

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

Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний сетевой узел. Чтобы локальный сетевой 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).

Трансляция адреса источника

Трансляция адреса источника предназначена для организации доступа узлов локальной сети в интернет. Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных сетевых узлов публичный IP-адрес координатора. Таким образом, узлы локальной сети могут устанавливать соединения с узлами в интернете от имени публичного IP-адреса координатора.

Рисунок 47. 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, будут преобразованы:

- В момент передачи IP-пакета из локальной сети в интернет координатор преобразует IP-адрес (или IP-адрес и порт) отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. При этом частный IP-адрес отправителя заменяется на публичный IP-адрес внешнего сетевого интерфейса координатора, обеспечивающего доступ во внешнюю 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 IP-пакетов ViPNet Coordinator HW производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета координатор заменяет в нем IP-адрес получателя на частный IP-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 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 список правил трансляции адресов, выберите **Межсетевой экран** > **Трансляция адресов (NAT)**.

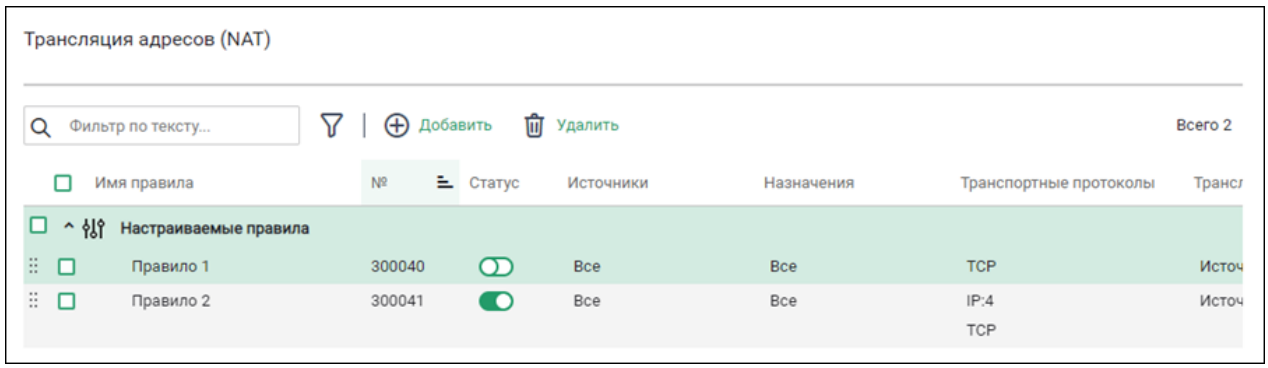

Рисунок 48. Просмотр правил трансляции адресов

Чтобы просмотреть определенные правила, нажмите и укажите критерии поиска.

Для поиска правил по тексту начните вводить его в поле **Фильтр по тексту**.

Создание и изменение правил трансляции адресов

Примечание. Если вы создаете правила трансляции адресов для транзитного трафика, то дополнительно к правилу трансляции необходимо создать соответствующие транзитные фильтры.

1 Выберите **Межсетевой экран** > **Трансляция адресов (NAT)**.

2 Выполните одно из действий:

- Чтобы создать правило трансляции, нажмите **Добавить**.
- Чтобы изменить правило трансляции, в поле **Имя правила** или **Трансляция** нажмите .

3 Задайте имя правила трансляции.

4 Включите правило, чтобы оно начало действовать после создания.

5 Если требуется трансляция адреса источника для исходящих IP-пакетов, выберите **Заменять адрес источника на** и выполните одно из действий:

- Чтобы IP-адрес отправителя заменялся на адрес внешнего сетевого интерфейса ViPNet Coordinator HW, выберите **Адрес исходящего интерфейса (определяется автоматически).**
- Чтобы указать другой IP-адрес для замены IP-адреса отправителя, выберите **Другой адрес** и задайте его (IP-адрес должен быть назначен интерфейсу ViPNet Coordinator HW).

Внимание! Если вы зададите IP-адрес, не назначенный ни одному из интерфейсов ViPNet Coordinator HW, то после трансляции IP-адреса он не будет входить в подсеть исходящего трафика. Чтобы трансляция адреса отправителя работала по такой схеме, настройте маршрутизацию в вашей сети так, чтобы обратный трафик направлялся на тот же сетевой интерфейс ViPNet Coordinator HW, на котором выполнялась трансляция адрес отправителя.

6 Если требуется трансляция адреса назначения для входящих IP-пакетов:

6.1 Выберите **Заменять адрес назначения на** и укажите IP-адрес.

6.2 Если кроме трансляции адреса назначения требуется трансляция порта назначения, выберите **Заменять порт назначения на** и укажите порт.

7 По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам. Чтобы фильтр применялся к IP-пакетам, передаваемым по определенным протоколам, в списке **Протоколы** укажите протокол, сообщение ICMP или группы протоколов.

8 В разделе **Источники** по умолчанию указаны все отправители IP-пакетов (**Все**). Чтобы выбрать определенных отправителей IP-пакетов, в разделе **Добавить** раскройте список **Источники** и укажите IP-адреса, диапазоны IP-адресов, доменные имена или группы IP-адресов.

9 В разделе **Назначения** по умолчанию указаны все получатели IP-пакетов (**Все**). Чтобы выбрать определенных получателей IP-пакетов, в разделе **Добавить** раскройте список **Назначения** и укажите IP-адреса, диапазоны IP-адресов, доменные имена или группы IP-адресов.

10 Нажмите **Сохранить**.

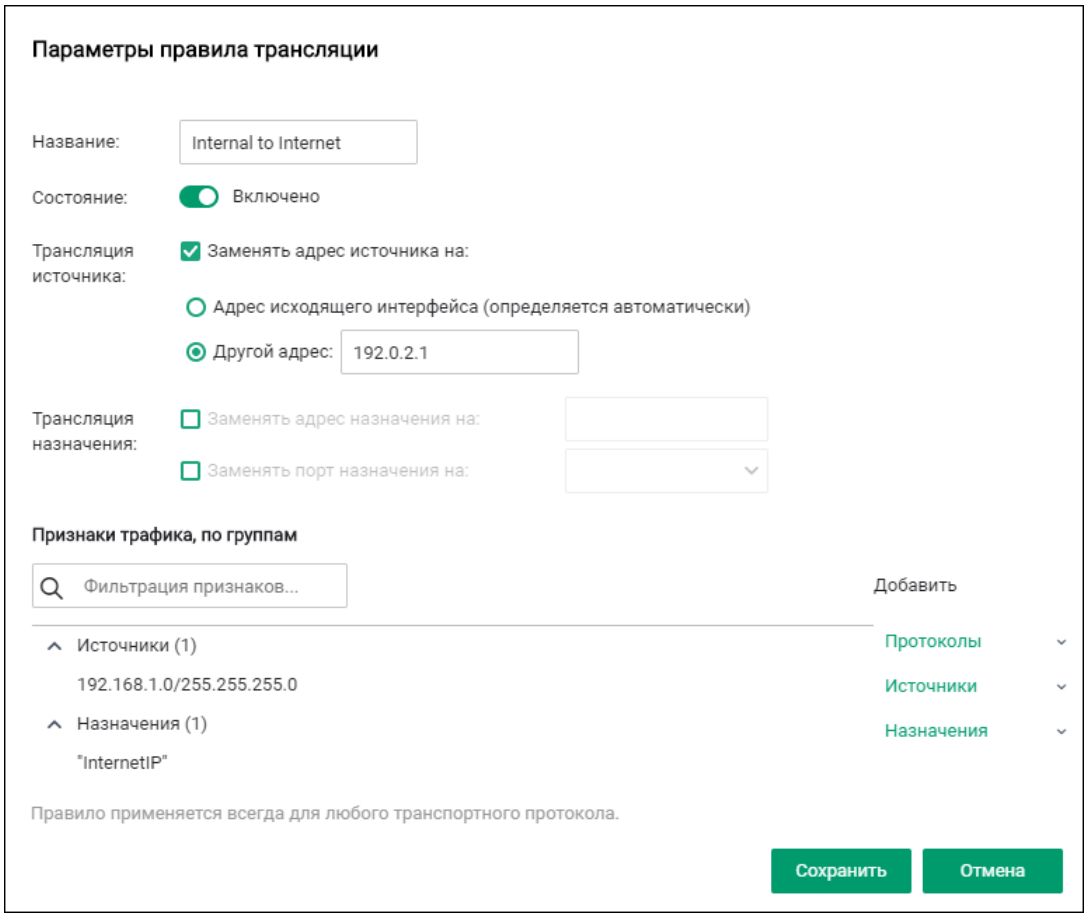

Рисунок 49. Создание правила трансляции адресов

11 Чтобы изменить приоритет правила трансляции, перетащите его на нужную строку списка за значок ⠿.

12 Чтобы правило вступило в действие, нажмите **Применить все**.

Примечание. Примененное правило трансляции адресов будет работать для вновь устанавливаемых соединений. Для уже установленных соединений правило будет работать после истечения времени жизни соединения.

7

Настройка обработки прикладных протоколов

О прикладных протоколах

Прикладные протоколы обеспечивают работу пользовательских сетевых сервисов, например, IP-телефонии, DNS, FTP. При использовании данных служб IP-адреса часто передаются в теле сообщения прикладного протокола. Эта особенность может повлиять на доступность сервисов в защищенной сети с виртуальной адресацией или трансляцией сетевых адресов. Кроме того, некоторые прикладные протоколы, помимо управляющего соединения, открывают для передачи данных дополнительные соединения. Поскольку параметры таких соединений заранее неизвестны, невозможно создать сетевой фильтр, разрешающий только необходимый трафик.

ViPNet Coordinator HW может выполнять роль шлюза прикладного уровня, что позволяет решить перечисленные проблемы, обеспечивая:

- Подмену IP-адресов в теле сообщения прикладного протокола на виртуальные IP-адреса.
- Подмену IP-адреса в теле сообщения протокола FTP при трансляции адреса источника или назначения в транзитном FTP-трафике.
- Создание временных сетевых фильтров, пропускающих IP-пакеты дополнительных соединений, которые используются прикладным протоколом.

Примечание. Для разрешения управляющего соединения между узлами создайте сетевой фильтр вручную.

Вы можете настроить обработку прикладных протоколов для открытого и туннелируемого трафика. Список поддерживаемых прикладных протоколов см. ниже.

Поддерживаемые прикладные протоколы

В ViPNet Coordinator HW можно настроить обработку следующих прикладных протоколов:

- DNS — для доступа к сетевым узлам по доменным именам.
- FTP — для передачи файлов между FTP-клиентом и FTP-сервером.

  Команды FTP-протокола EPRT и EPSV, используемые некоторыми FTP-клиентами, не поддерживаются ViPNet Coordinator HW.
- SIP — для установления соединений, включающих обмен мультимедийными данными между клиентами.

  Не поддерживаются SIP-клиенты и телекоммуникационные серверы, использующие при подключении протокол TLS, «компактные поля» (compact headers) или сжатие данных в сообщениях SIP.

  Для некоторых SIP-клиентов могут не обрабатываться такие дополнительные данные, как телефонные справочники, информация о доступности абонента и другие.
- H.323 — для передачи мультимедийных данных в IP-сетях (IP-телефония, видео- и аудиоконференции).

  При использовании IP-телефонов Yate не поддерживается виртуальная видимость IP-адресов. RTCP-трафик между IP-телефонами Polycom может работать некорректно при виртуальной видимости IP-адресов.
- SCCP — для передачи сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты (Cisco Unity Connection и Cisco Unified Communication Manager (CallManager)).

  Передача мультимедийных данных с использованием протокола SCCP возможна, если сервер голосовой почты туннелируется координатором ViPNet Coordinator HW.

Примечание. ViPNet Coordinator HW также поддерживает обработку прикладного протокола Cisco NetMeeting для организация видеоконференций, но только при использовании видимости по реальным IP-адресам между клиентским ПО Cisco Meeting App в сети ViPNet и туннелируемым сервером Cisco Meeting Server.

Список поддерживаемых прикладных протоколов изменить нельзя.

Настройка параметров обработки прикладных протоколов

Для просмотра текущих настроек обработки прикладных протоколов выберите **Межсетевой экран > Обработка прикладных протоколов**.

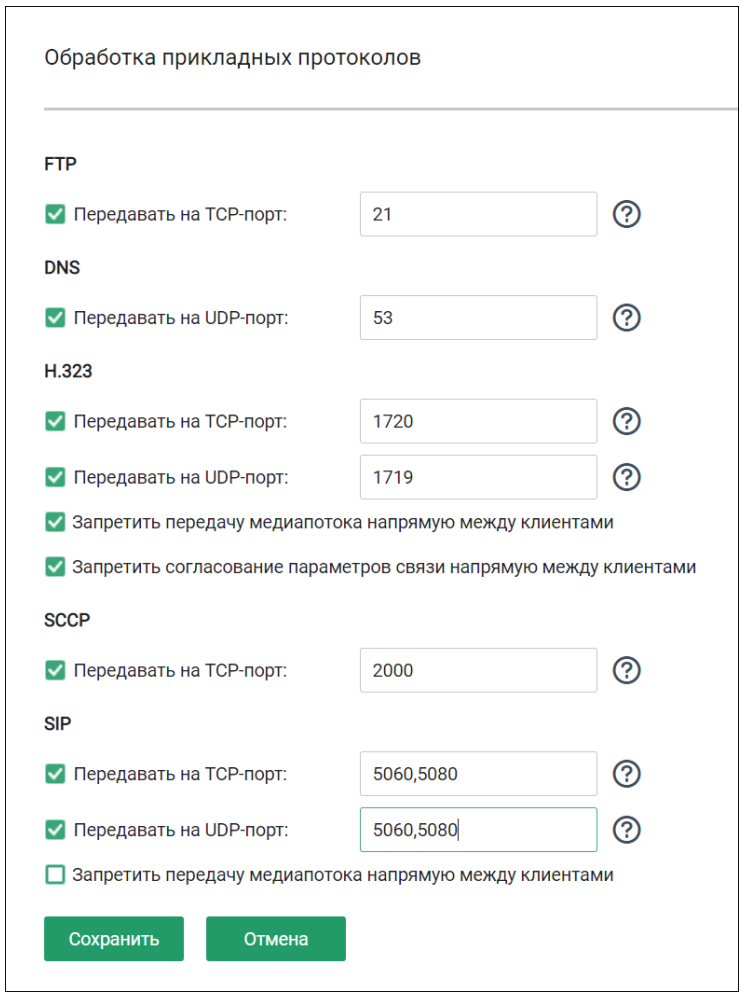

Рисунок 50. Обработка прикладных протоколов

Внимание! При выключении обработки прикладного протокола работа соответствующих сетевых служб на защищенном узле будет невозможна.

После настройки обработки прикладных протоколов (включить или выключить обработку, изменить порт) необходимо перезапустить приложение (например, DNS-, FTP-, SIP-клиент) или устройство (например, SIP-телефон).

Чтобы настроить параметры обработки прикладных протоколов:

1 Выберите **Межсетевой экран > Обработка прикладных протоколов**.

2 Чтобы включить использование прикладного протокола установите флажок.

3 В строке прикладного протокола, который необходимо настроить введите порт, диапазон портов или список портов, разделенных запятой для сетевого протокола.

4 Настройте режим подключения для протоколов SIP и H323:

Медиа-потоки могут передаваться напрямую (т.н. режим Direct Call или Peer-to-Peer RTP), либо через сервер телефонии. По умолчанию ViPNet Coordinator HW блокирует медиа-потоки между абонентами, которые соединяются напрямую (минуя сервер телефонии).

Если в вашей сети используется IP-телефония или видеосвязь, и на сервере телефонии, за которым находятся абоненты, настроен режим Direct Call (Peer-to-Peer RTP), разрешите прямое подключение, сняв соответствующие флажки:

- **Запретить передачу медиапотока напрямую между клиентами**.
- **Запретить согласование параметров связи напрямую между клиентами** (для протокола H323).

Внимание! Использование режима прямого соединения создает временные разрешающие правила межсетевого экрана, что снижает защищённость, если ViPNet Coordinator HW расположен на границе защищаемой сети. Если вы планируете использовать режим прямого соединения для абонентов, то разместите ViPNet Coordinator HW внутри защищенного периметра.

5 Нажмите **Сохранить**.

Примечание. Выбранные параметры обработки прикладных протоколов должны соответствовать параметрам, указанным в настройках соответствующих приложений (FTP-клиент, DNS-клиент, SIP-клиент и так далее).

8

Настройка сетевых служб

Настройка DHCP-сервера

В состав ViPNet Coordinator HW входит DHCP-сервер. Он динамически назначает IP-адреса сетевым узлам (DHCP-клиентам). Также DHCP-сервер может передать дополнительные параметры — IP-адреса шлюза по умолчанию, DNS-, NTP-сервера и другие.

DHCP-сервер может обслуживать DHCP-клиентов, которые находятся:

- в одной сети с DHCP-сервером, в том числе в сегментах сети, объединенных по L2OverIP;
- в удаленных подсетях с помощью агента DHCP-relay.

Чтобы запустить DHCP-сервер на одном из сетевых интерфейсов Ethernet:

1 Выберите **Прикладные сервисы** > **DHCP-сервер**.

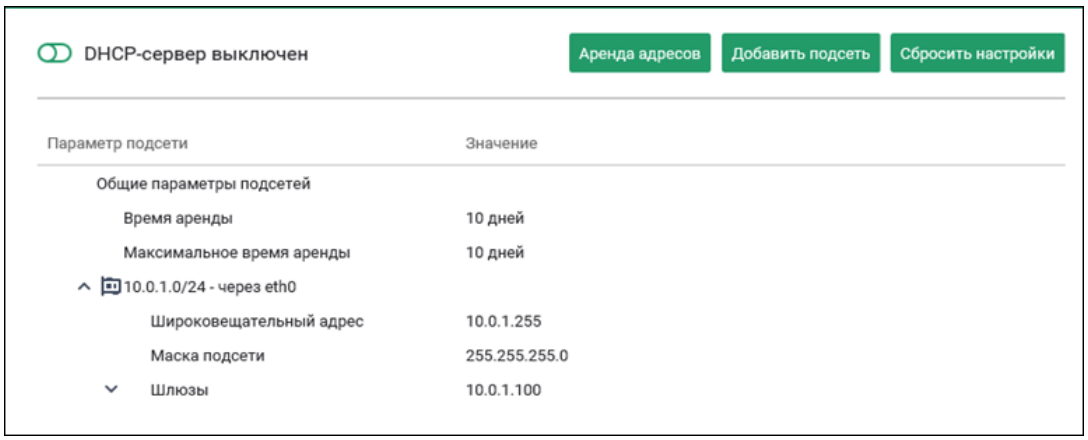

Рисунок 51. Настройка параметров DHCP-сервера

2 Выключите DHCP-сервер.

3 Нажмите **Добавить подсеть**, клиентов которой будет обслуживать DHCP-сервер.

4 Выберите тип подсети — **Локальная** или **Удаленная**.

5 Выберите сетевой интерфейс ViPNet Coordinator HW, а также (для удаленной подсети) IP-адрес и маску подсети.

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

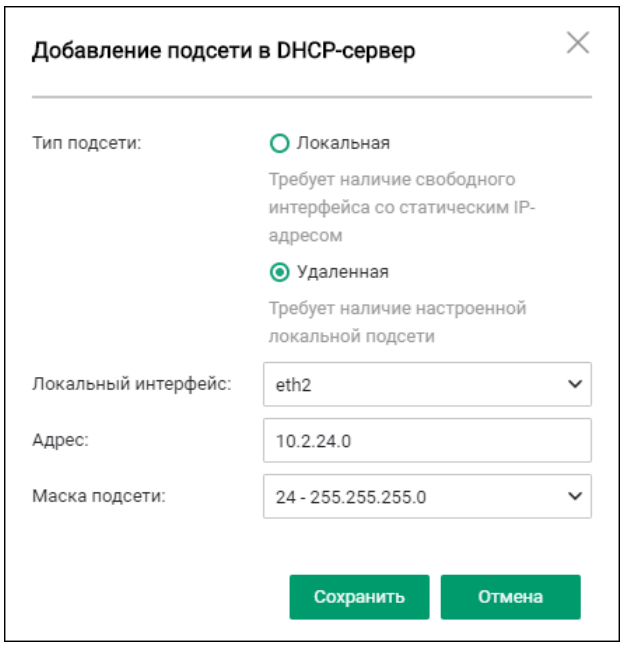

Рисунок 52. Добавление подсети для DHCP-сервера

6 Нажмите **Сохранить**.

7 Чтобы задать параметры, передаваемые DHCP-сервером своим клиентам, нажмите ⊕ в строке **Общие параметры подсетей** или в строке добавленной подсети.

7.1 Выберите нужный параметр и задайте его значения.

Например, для добавленной подсети задайте интервал IP-адресов, которые должны присваиваться клиентам DHCP. Диапазон IP-адресов должен принадлежать сети интерфейса и не должен включать адрес самого интерфейса.

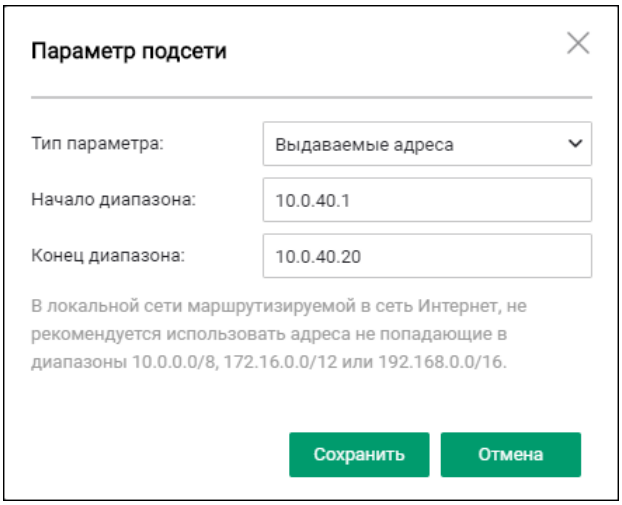

Рисунок 53. Добавление диапазона IP-адресов для DHCP-клиентов

Примечание. DHCP-сервер может выделять клиентам любые диапазоны IP-адресов. Однако в локальной сети, маршрутизируемой в 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.

В общих параметрах подсетей вы можете изменить, например, время аренды IP-адресов, выделяемых DHCP-сервером своим клиентам. При этом параметр **Максимальное время аренды** задаёт ограничение для клиентов, которые сами запрашивают определённое время аренды у DHCP-сервера.

7.2 Нажмите **Сохранить**.

8 Чтобы изменить значение какого-либо параметра DHCP-сервера, нажмите .

9 Включите DHCP-сервер.

Чтобы просмотреть список клиентов DHCP-сервера, нажмите **Аренда адресов**.

Если несколько клиентов получили одинаковые IP-адреса, возможно, у них совпадает идентификатор DHCP-клиента (UID). Чтобы избежать этого, в сетевых настройках клиентов задайте MAC-адрес в качестве идентификатора DHCP.

Настройка DHCP-relay

ViPNet Coordinator HW можно использовать в качестве агента DHCP-relay. Он принимает от узлов DHCP-запросы и передает их DHCP-серверу. Ответы, полученные от DHCP-сервера, агент DHCP-relay перенаправляет сетевым узлам.

Внимание! Для приема и перенаправления DHCP-запросов через DHCP-relay необходимо, чтобы DHCP-сервер поддерживал Option 82 Suboption 5.

Агент DHCP-relay используется, когда сетевые узлы не могут обращаться напрямую к DHCP-серверу. Например, в разветвленной сети из нескольких подсетей, в которых нет своего DHCP-сервера.

Агент DHCP-relay может работать с несколькими локальными сетями. Это могут быть как сети, подключенные к разным физическим сетевым интерфейсам ViPNet Coordinator HW, так и виртуальные локальные сети, подключенные к одному физическому интерфейсу.

Вы можете настроить несколько копий DHCP-relay, которые будут иметь различные слушающие, внешние интерфейсы и IP-адреса DHCP-серверов.

Узлы, которые будут обращаться к DHCP-серверу через ViPNet Coordinator HW, могут быть защищенными и открытыми. DHCP-сервер может быть защищенным, открытым или туннелируемым узлом.

Если агент DHCP-relay перенаправляет запросы на DHCP-сервер, который туннелируется другим координатором, настройте между координаторами видимость по реальным IP-адресам. Если между ними настроена видимость по виртуальным адресам, ответы от DHCP-сервера будут отправляться на реальный адрес ViPNet Coordinator HW, выступающего в качестве агента DHCP-relay, и не будут доставлены.

Чтобы запустить DHCP-relay:

1 Выберите **Прикладные сервисы** > **DHCP-relay**.

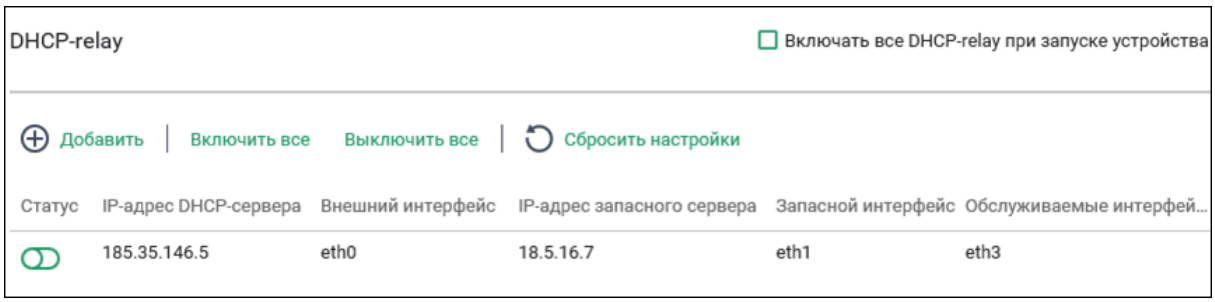

Рисунок 54. Настройка параметров DHCP-relay

2 Нажмите **Добавить**.

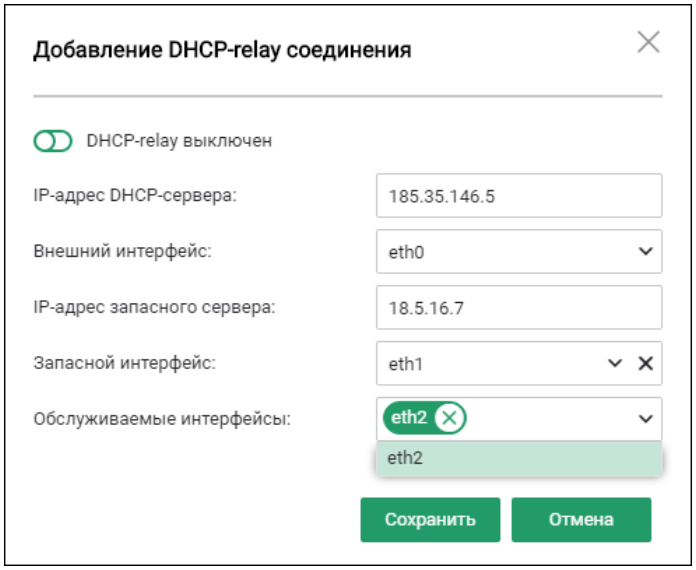

Рисунок 55. Добавление соединения DHCP-relay

3 Задайте **IP-адрес DHCP-сервера** вашей сети.

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

5 Если в вашей сети есть запасной DHCP-сервер, то вы также можете указать сетевой интерфейс ViPNet Coordinator HW, который должен использоваться для доступа к запасному серверу, и IP-адрес запасного DHCP-сервера.

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

7 Нажмите **Сохранить**.

8 Включите созданную копию DHCP-relay.

9 Чтобы все копии DHCP-relay автоматически запускались при загрузке ViPNet Coordinator HW, выберите **Включать все DHCP-relay при запуске устройства**.

Настройка DNS-сервера

В состав ViPNet Coordinator HW входит локальный DNS-сервер, который преобразует доменные имена 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 преобразует доменные имена с использованием корневых DNS-серверов из домена `root-servers.net`. Этот список можно дополнить DNS-серверами пересылки (forwarders).

Внимание! В качестве DNS-серверов пересылки используйте доверенные DNS-серверы из сети ViPNet. Ответы на запросы DNS-клиентов, приходящие не от доверенных DNS-серверов, могут быть скомпрометированы.

Список дополнительных DNS-серверов:

- Можно получить от внешнего DHCP-сервера.

  На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера, а DHCP-сервер должен отправлять информацию о DNS-серверах.

  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.

  Настройте получение информации о DNS-серверах только на одном интерфейсе. Данные об адресах DNS-серверов поступают автоматически, откажитесь от их получения.

- Задать вручную.

Внимание! Если DNS-серверы пересылки недоступны, но при этом доступны корневые DNS-серверы, DNS-клиенты будут получать ответы на свои запросы с задержкой.

Чтобы настроить параметры локального DNS-сервера:

1 Выберите **Прикладные сервисы** > **DNS-сервер**.

  Список DNS-серверов включает в себя IP-адреса серверов, заданные пользователем вручную или полученные автоматически от DHCP-сервера.

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

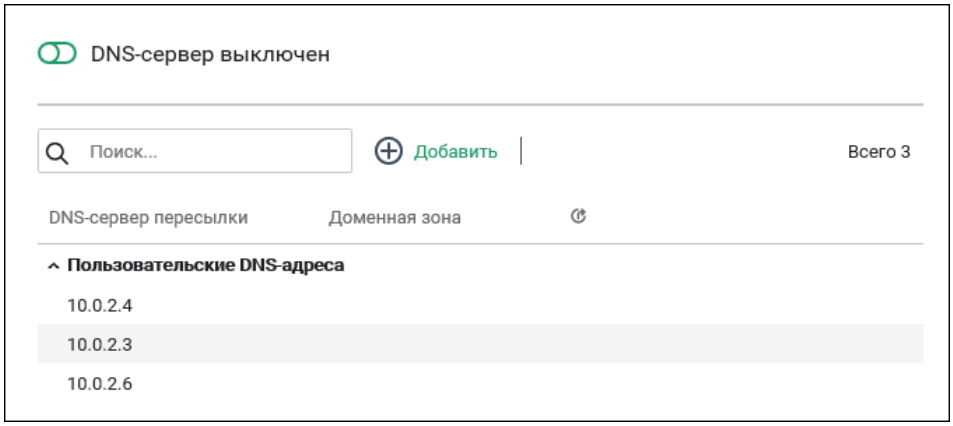

Рисунок 56. Настройка параметров DNS-сервера

2 Чтобы добавить IP-адрес нового DNS-сервера в список, нажмите **Добавить:**

- Укажите IP-адрес DNS-сервера пересылки.

  По умолчанию DNS-запросы перенаправляются на корневые DNS-серверы из домена root-servers.net.

- Если необходимо перенаправлять DNS-запросы для определенных зон, то добавьте для каждой такой зоны IP-адрес DNS-сервера пересылки в поле **Доменная зона**.

Примечание. При добавлении двух и более DNS-серверов пересылки, серверы, добавленные без указания имени зоны, имеют приоритет и будут использоваться для перенаправления всех DNS-запросов вне зависимости от наличия серверов пересылки для отдельных зон.

- Нажмите **Сохранить**.

3 Чтобы включить перенаправление запросов на DNS-серверы, указанные в списке, включите DNS-сервер.

Настройка NTP-сервера

Примечание. При настройке исполнения ViPNet Coordinator VA, не устанавливайте одновременно синхронизацию времени на виртуальной платформе и ViPNet Coordinator VA.

В состав ViPNet Coordinator HW входит локальный NTP-сервер. Он используется для синхронизации времени на ViPNet Coordinator HW и на других сетевых узлах (NTP-клиентах).

По умолчанию локальный NTP-сервер синхронизирует время с публичными NTP-серверами из кластера `vniiftri.ru` при подключении к интернету.

Этот кластер серверов можно дополнить другими NTP-серверами (публичными или корпоративными). Это удобно, когда нет интернета или есть более предпочтительный NTP-сервер.

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

Описание секции и параметра см. в документе «Справочник команд и конфигурационных файлов», в разделе «Файл iplir.conf».

Список дополнительных NTP-серверов:

- Можно получить от внешнего DHCP-сервера.

  На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера и DHCP-сервер должен отправлять информацию о NTP-серверах.

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

  Настройте получение адресов NTP-серверов только на одном интерфейсе. Данные об адресах NTP-серверов поступают автоматически, вы можете отказаться от их получения.

- Сформировать вручную.

Чтобы настроить параметры NTP-сервера:

1 Выберите **Прикладные сервисы** > **NTP-серверы**:

   - На вкладке **Список серверов** указаны серверы:
     - заданные по умолчанию;
     - полученные автоматически от DHCP-сервера.

- заданные вручную;

- На вкладке **Мониторинг** указана информация о включенных серверах, которые заданы по умолчанию или вручную:
  - IP-адрес или доменное имя.
  - Тип соединения — тип передачи данных, например unicast или manycast.
  - Уровень иерархии — уровень внешних NTP-серверов, относительно которого ViPNet Coordinator HW может перейти в изолированный режим, если не удается установить соединение со всеми внешними NTP-серверами меньше указанного уровня (при настроенном переходе в изолированный режим).
  - Вышестоящий сервер — тип вышестоящего NTP-сервера для синхронизации времени.
  - Последняя синхронизация — время получения последнего ответа от NTP-сервера.
  - Частота опроса — период опроса NTP-сервера.
  - Ожидание ответа — время в миллисекундах между отправкой и получением ответа.
  - Разница с сервером — смещение в миллисекундах между ViPNet Coordinator HW и NTP-сервером.
  - Джиттер — абсолютное значение среднеквадратичного отклонения смещения относительно ViPNet Coordinator HW.

2 Чтобы добавить внешний NTP-сервер:

2.1 На вкладке **Список серверов** нажмите **Добавить**.

2.2 Укажите IP-адрес или доменное имя NTP-сервера.

2.3 Выберите тип:

- **Сервер** — если NTP-сервер только рассылает данные о времени.
- **Пир** — если NTP-сервер рассылает и получает данные о времени.

2.4 Нажмите **Сохранить**.

3 Чтобы изменить внешний NTP-сервер, наведите на него в столбце **IP-адрес или доменное имя** и нажмите .

Вы можете изменять и удалять только серверы, добавленные вручную.

4 Чтобы настроить локальный NTP-сервер, нажмите **Настройки**:

4.1 Чтобы исключить из процесса синхронизации времени NTP-серверы, заданные по умолчанию, снимите флажок **Использовать серверы, заданные по умолчанию**.

Примечание. Перед отключением использования NTP-серверов по умолчанию добавьте не менее четырех дополнительных NTP-серверов. Иначе, если один из серверов выйдет из строя, у ViPNet Coordinator HW не будет достаточно информации, чтобы определить, какой из оставшихся серверов предоставляет правильное время.

4.2 Чтобы локальный NTP-сервер при потере соединения с внешними NTP-серверами переходил в изолированный режим, выберите **Переходить в изолированный режим** и укажите уровень иерархии.

Если со всеми внешними NTP-серверами меньше указанного уровня не удается установить соединение в течение 5 минут, локальный NTP-сервер переходит в изолированный режим.

Внимание!

- Разрешите переход локального NTP-сервера в изолированный режим, если ViPNet Coordinator HW используется в качестве NTP-сервера для внутренней сети. Иначе клиенты ViPNet Coordinator HW не будут получать информацию о точном времени при потере соединения ViPNet Coordinator HW с внешними NTP-серверами, так как в этом случае локальный NTP-сервер будет считаться недостоверным.
- Если время на вышестоящем NTP-сервере будет изменено более чем на один час вперед или назад, то это может привести к аварийному завершению работы NTP-сервера ViPNet Coordinator HW. В этом случае повторно запустите NTP-сервер.

4.3 Нажмите **Сохранить**.

5 Включите NTP-сервер.

Внимание! NTP-серверы, указанные по доменному имени, будут доступны, только если запущен DNS-сервер (см. Настройка DNS-сервера).

Информация о попытках подключения к NTP-серверам записывается в системный журнал. Если ViPNet Coordinator HW не удалось подключиться ни к одному из NTP-серверов, локальный NTP-сервер запускается с тем временем, которое было задано при первоначальной настройке. Для таких случаев вы можете добавить в список NTP-серверов выбранный NTP-сервер локальной сети, с которым ViPNet Coordinator HW сможет синхронизировать время в случае невозможности подключения к внешним NTP-серверам.

Настройка параметров прокси-сервера

Прокси-сервер ViPNet Coordinator HW обладает следующими возможностями:

- Кеширование данных для ускорения доступа пользователей к часто запрашиваемым ресурсам.
- «Прозрачный» режим работы, для которого не требуется дополнительная настройка приложений на рабочих местах пользователей.
- Контент-фильтрация HTTP-трафика.
- Проверка трафика с помощью внешнего антивируса.

Рисунок 57. Схема работы прокси-сервера ViPNet Coordinator HW

Порядок обработки запроса при обращении к интернет-ресурсу:

1 Запрос от клиента прокси-сервера поступает на ViPNet Coordinator HW:
   - Обрабатывается сетевыми фильтрами:
     - если сработал запрещающий сетевой фильтр, то передача IP-пакетов блокируется, в журнал IP-пакетов добавляется запись об этом событии (см. Типы событий в журнале регистрации IP-пакетов);
     - если запрос не попал под действие ни одного из запрещающих сетевых фильтров, он передается на прокси-сервер.
   - Если включена контент-фильтрация трафика, то запрос обрабатывается ее правилами:
     - если ни одно правило не сработало, то применяется правило по умолчанию (блокирующее или разрешающее);
     - если сработало запрещающее правило по HTTP-методу или MIME-типу, то передача HTTP-трафика блокируется.
   - Если 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 контент-фильтрации трафика или при проверке антивирусом, он передается на интернет-ресурс.
3 Ответ от интернет-ресурса поступает на ViPNet Coordinator HW:

- Обрабатывается сетевыми фильтрами аналогично шагу 1.
- Если включена функция фильтрации содержимого трафика, то ответ обрабатывается ее правилами аналогично шагу 1.
- Если 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 сообщение от антивируса и попытка загрузки файла будет заблокирована. Запись об этом событии будет создана в системном журнале.

В случае успешного прохождения всех проверок HTTP-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. Вы также можете включить антивирусную проверку и контент-фильтрацию трафика.

Режимы работы прокси-сервера:

- Обычный режим — в пользовательских приложениях, например в браузере, требуется настроить подключение: указать IP-адрес и порт прокси-сервера и исключить использование прокси-сервера для локальных адресов, в том числе адресов ViPNet Coordinator HW.
- «Прозрачный» режим — 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 ViPNet Coordinator HW, на котором запущен прокси-сервер.

Настройка основных параметров прокси-сервера

Чтобы использовать встроенный прокси-сервер для защиты вашей локальной сети, настройте основные параметры прокси-сервера.

Вы также можете включить фильтрацию содержимого (см. Настройка правил контент-фильтрации трафика) и антивирусную проверку трафика (см. Настройка антивирусной проверки).

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.

На стороне пользователя в качестве шлюза по умолчанию задайте IP-адрес интерфейса, на который прокси-сервер ViPNet Coordinator HW принимает запросы от этого пользователя.

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

Чтобы настроить прокси-сервер:

1 Выберите **Межсетевой экран** > **Прокси-сервер** > **Общие настройки**.

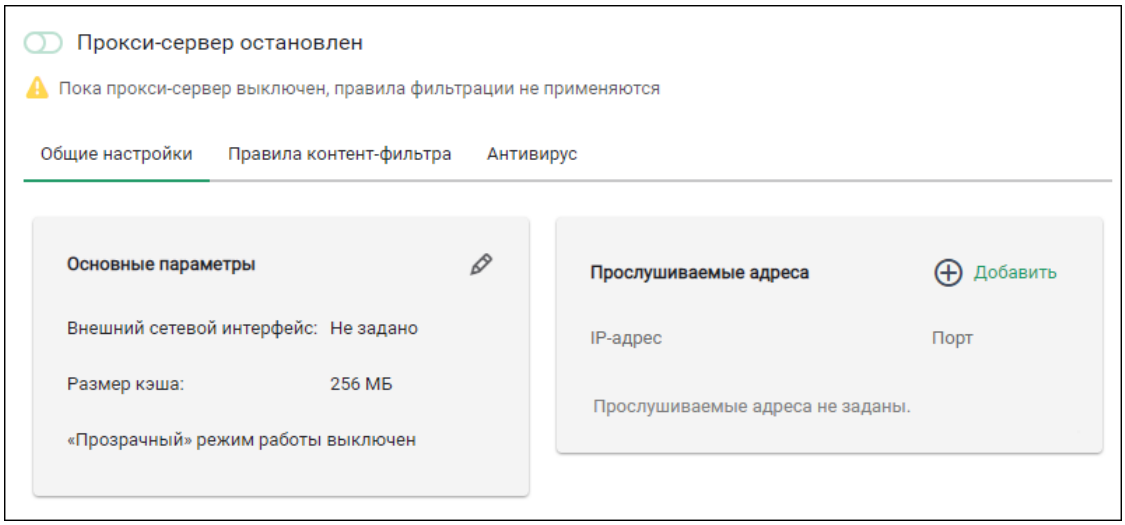

Рисунок 58. Общие настройки прокси-сервера

2 В разделе **Основные параметры** нажмите .

2.1 В списке **Внешний сетевой интерфейс** выберите сетевой интерфейс, подключенный к интернету.

2.2 В поле **Размер кеша** укажите размер кеша прокси-сервера. Кеш используется для хранения копии данных, к которым часто обращаются пользователи.

2.3 Чтобы не настраивать ПО на рабочих местах пользователей, которые подключаются к интернету через прокси-сервер, выберите **«Прозрачный» режим работы** прокси-сервера.

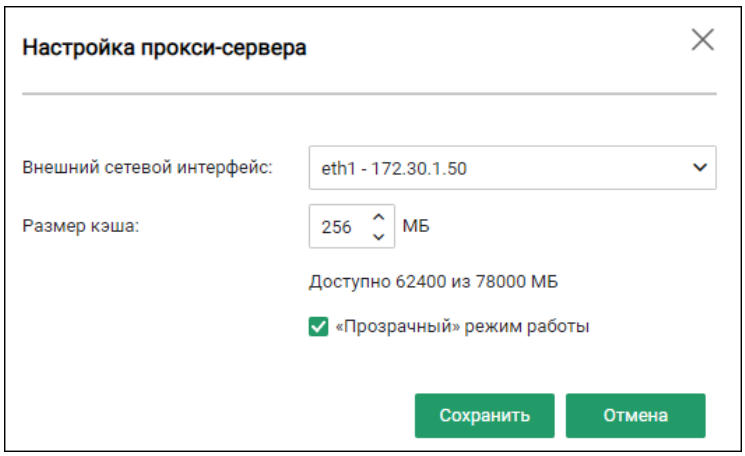

Рисунок 59. Настройка основных параметров прокси-сервера

2.4 Нажмите **Сохранить**.

3 В разделе **Прослушиваемые адреса** нажмите **Добавить**.

4 Задайте IP-адрес и порт, которые прокси-сервер должен использовать, чтобы принимать запросы пользователей.

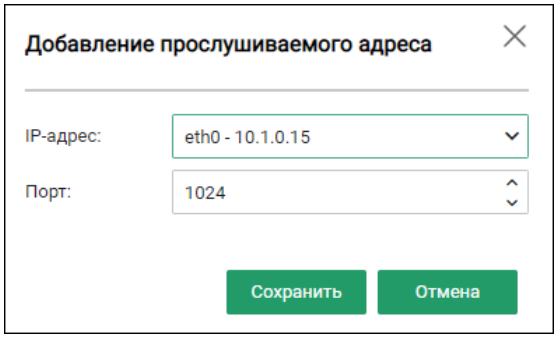

Рисунок 60. Добавление прослушиваемого адреса прокси-сервера

Внимание! Задавайте для прослушивания сетевые интерфейсы со статическими IP-адресами. После изменения IP-адресов сетевых интерфейсов завершите работу прокси-сервера, задайте текущие IP-адреса интерфейсов, использующихся для организации соединения, а затем снова запустите прокси-сервер. Задавайте номер порта, который не используется другими сервисами.

5 Нажмите **Сохранить**.

6 Включите прокси-сервер.

Внимание! Перед запуском прокси-сервера задайте IP-адрес для прослушивания и порт, 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.

После первого запуска использование прокси-сервера будет разрешено для IP-адресов локальных сетей, входящих в пользовательскую группу объектов `HttpProxyUsers`. По умолчанию в эту группу входят те же IP-адреса, что и в пользовательскую группу объектов `PrivateNetworkIP` (10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16).

Внимание! Пользовательская группа объектов `HttpProxyUsers` автоматически создается при первом запуске прокси-сервера.

Чтобы добавить или удалить IP-адреса из списка локальных сетей, которым разрешено использовать прокси-сервер, остановите сервер, затем измените группу объектов `HttpProxyUsers` (см. Создание и изменение групп объектов) и вновь запустите прокси-сервер.

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 "PrivateNetworkIP"**.
- Протоколы: TCP: 21, TCP: 80, TCP: 443, TCP: 9443.

Подробнее о создании сетевых фильтров см. в разделе Создание и изменение сетевых фильтров.

Настройка правил контент-фильтрации трафика

1 Выберите **Межсетевой экран** > **Прокси-сервер** > **Правила контент-фильтра**.

2 Остановите прокси-сервер.

3 Нажмите **Добавить** и задайте параметры нового правила:

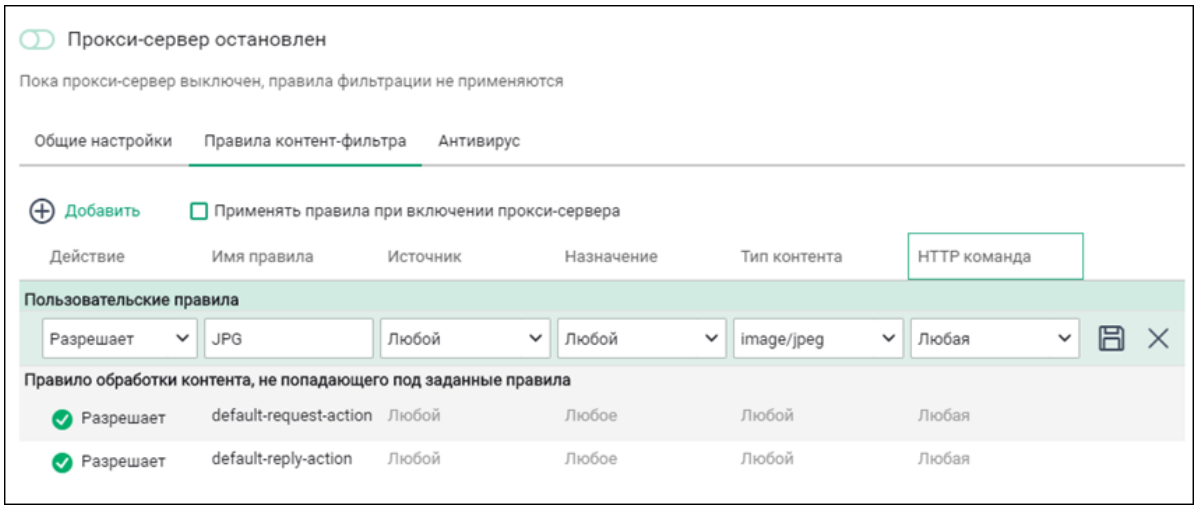

Рисунок 61. Добавление правила фильтрации

3.1 В списке **Действие** выберите тип правила — разрешающее или блокирующее.

3.2 Задайте имя правила.

3.3 Выберите IP-адрес источника и назначения, для которых будет действовать правило.

Чтобы задать любой узел в качестве источника или назначения выберите в списке значение **Любой**. Для задания адреса назначения вы также можете использовать доменное имя (в том числе с использованием национальных символов, например, кириллицы).

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

3.4 Выберите тип контента.

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.

3.5 Если в списке **Тип контента** на шаге 4 вы выбрали тип **Любой**, то в списке **HTTP команда** необходимо выбрать один из методов HTTP. Например, чтобы разрешить или запретить доступ к сайту, укажите HTTP-метод GET.

3.6 Нажмите .

4 Выберите **Применять правила при включении прокси-сервера**.

5 Запустите прокси-сервер.

Настройка антивирусной проверки

1 Выберите **Межсетевой экран** > **Прокси-сервер** > **Антивирус**.

2 Остановите прокси-сервер.

3 Нажмите в группе параметров **Внешний антивирус**.

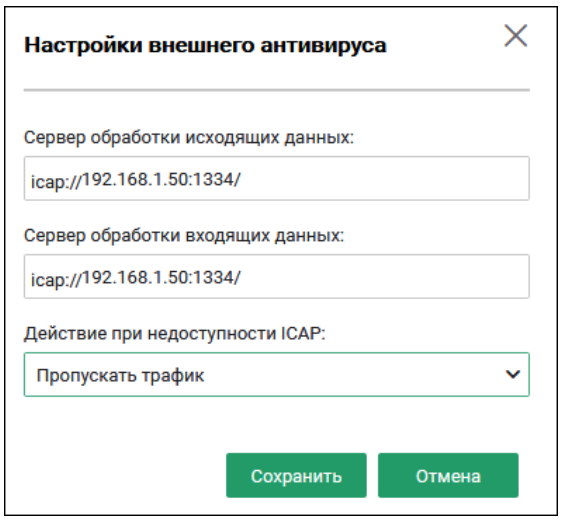

Рисунок 62. Настройки внешнего антивируса

4 Задайте путь к серверам обработки исходящих и входящих данных в формате `icap://адрес[:порт]/`.

Внимание! В конце адреса ICAP-сервера необходимо указать символ «/». Если не указано значение параметра `порт`, то будет использоваться значение по умолчанию 1344.

5 Выберите **Действие при недоступности ICAP**:

- **Пропускать трафик.**
- **Блокировать трафик**.

6 Нажмите **Сохранить**.

7 В поле **Инспекция** выберите **Проводится**.

Внимание! Время на ICAP-сервере должно быть синхронизировано с ViPNet Coordinator HW.

8 Запустите прокси-сервер и дождитесь его запуска.

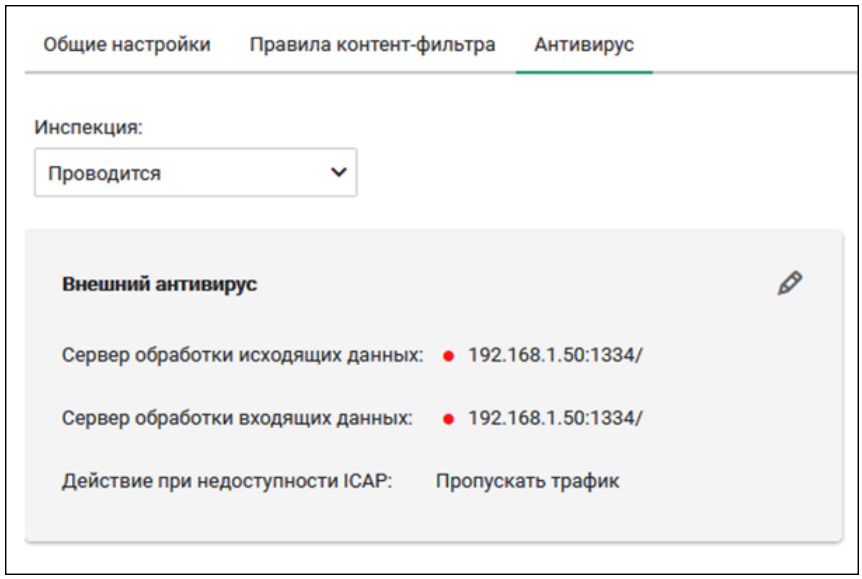

Рисунок 63. Пример настройки внешнего антивируса

В результате выполненной настройки антивирусная проверка будет выполняться на ICAP- сервере с IP-адресом 192.168.1.50 и портом по умолчанию 1344. При недоступности ICAP-сервера трафик будет пропускаться прокси-сервером без антивирусной фильтрации.

Настройка параметров точки доступа к сети Wi-Fi

Примечание. Встроенный Wi-Fi-адаптер есть в аппаратных платформах HW50 N2 и HW100 N2.

Внешние Wi-Fi-адаптеры не поддерживаются.

Если ViPNet Coordinator HW работает в режиме клиента, то он не сможет работать в режиме точки доступа.

1 Выберите **Сетевые интерфейсы**.

2 Выберите сетевой интерфейс Wi-Fi (`wlan0`), справа появится окно настроек.

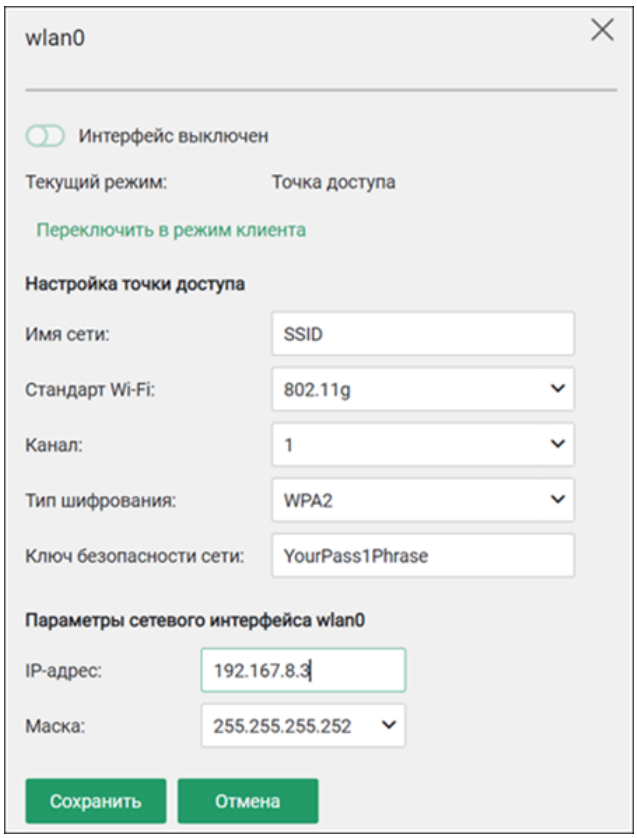

Рисунок 64. Настройка параметров точки доступа Wi-Fi

3 По умолчанию интерфейс Wi-Fi работает в режиме клиента. Чтобы переключить интерфейс Wi-Fi в режим точки доступа, нажмите **Переключить в режим точки доступа**.

Примечание. Кнопка **Переключить в режим точки доступа** активна только при выключенном интерфейсе wlan0.

4 В соответствующих полях задайте статический IP-адрес и маску подсети.

5 Задайте **Имя сети** Wi-Fi.

6 Выберите **Стандарт Wi-Fi** для вашей сети:

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

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

8 Выберите **Тип шифрования** для аутентификации пользователей:

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

9 Настройте параметры DHCP-сервера для интерфейса wlan0 (см. Настройка DHCP-сервера).

10 Включите  интерфейс.

11 Нажмите **Сохранить**.

12 Если требуется обеспечить возможность соединений между устройствами, которые подключены к сети Wi-Fi, и устройствами, подключенными к сети Ethernet, создайте транзитные фильтры открытой сети, разрешающие пропускание IP-пакетов между этими сетями.

9

Настройка маршрутизации

Общие сведения о маршрутизации

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

Маршрутизация — процесс выбора маршрута следования IP-пакета, передаваемого в сети от одного узла другому. Он выбирается из подмножества маршрутов, заданных на ViPNet Coordinator HW в таблице маршрутизации.

Маршруты могут быть:

- Статические — добавляются в таблицу маршрутизации вручную. Удобно использовать в небольших сетях.
- Динамические — попадают в таблицу маршрутизации с помощью алгоритмов на основе информации о топологии и состоянии сети, предоставляемой протоколами маршрутизации. Удобно использовать в сетях с разветвлённой и неоднородной топологией. Все маршрутизаторы в сети должны использовать определённый протокол динамической маршрутизации, по которому они будут обмениваться информацией о доступных им сетях, автоматически строить доступные маршруты в каждую сеть и выбирать из них наилучшие.

Динамическая маршрутизация кроме автоматического формирования таблиц маршрутизации позволяет:

- Автоматически выбирать по определенным критериям лучший маршрут из нескольких доступных. В том числе, в случае сбоев других маршрутизаторов в сети.
- Организовать динамическую балансировку нагрузки передаваемого IP-трафика.

ViPNet Coordinator HW может маршрутизировать IP-трафик с использованием следующих видов маршрутов:

- статических, в том числе на основе маршрутов с несколькими шлюзами;
- полученных по протоколу DHCP и PPP;
- формируемых протоколом OSPF.

Принципы маршрутизации

В ViPNet Coordinator HW для хранения маршрутов используются:

- Таблица маршрутизации по умолчанию (Main) — содержит:
  - статические маршруты, заданные вручную (Static);
  - маршруты в подсети, к которым подключены сетевые интерфейсы (Connected);
  - маршруты, полученные по протоколам DHCP, PPP, OSPF.
- Пользовательские таблицы маршрутизации — могут содержать только статические маршруты, заданные вручную, и использоваться для создания политик маршрутизации.

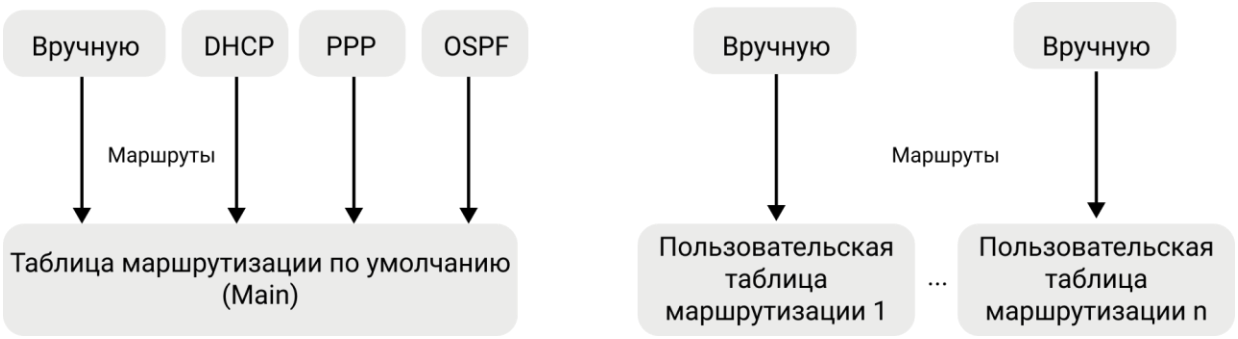

Рисунок 65. Формирование таблиц маршрутизации

В маршрутизации трафика участвуют не все маршруты, содержащиеся в таблице маршрутизации, а только лучшие маршруты в каждую сеть (подробнее см. «Формирование списка лучших маршрутов» ниже).

Характеристики маршрутов

- Источник получения маршрута (Connected, Static, PPP, DHCP, OSPF) — определяет, каким образом был получен маршрут.
- Административная дистанция — определяет приоритет маршрута от каждого источника. Учитывается, когда в таблице маршрутизации есть несколько маршрутов в одну и ту же сеть:
  - Чем меньше административная дистанция, тем более приоритетным считается маршрут.
  - Административная дистанция задаётся для каждого статического маршрута.
  - Для протокола PPP административная дистанция отдельно не задаётся и равна дистанции для протокола DHCP.
  - Административная дистанция статических маршрутов не может совпадать с дистанцией, заданной для маршрутов протокола OSPF.

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

- для статических маршрутов — 10;
- для маршрутов протоколов DHCP и PPP — 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.

- Метрика — определяет приоритет маршрутов протоколов DHCP, PPP и OSPF. Чем меньше метрика, тем выше приоритет маршрута.
  - Для маршрутов протокола DHCP 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 маршрутов протокола PPP метрика может быть задана вручную в том случае, если ViPNet Coordinator HW подключен к нескольким сетям, одной из которых является сеть 3G/4G, а в другой установлен DHCP-сервер. Если метрики для протоколов DHCP и PPP не были заданы, то используется метрика по умолчанию.

  Для маршрутов протокола OSPF метрика (стоимость) формируются автоматически.
- Вес — определяет долю IP-трафика, который будет проходить по маршруту через указанный шлюз. Используется только в статических маршрутах и задаётся для шлюза. Позволяет настроить балансировку передаваемого IP-трафика между несколькими шлюзами, когда часть IP-пакетов направляется на один шлюз, а часть — на другой (см. Настройка балансировки IP-трафика). Поэтому вес задаётся при создании нескольких статических маршрутов с одинаковым IP-адресом назначения и разными шлюзами.

Политики маршрутизации

Выбор, по какой таблице маршрутизировать трафик, определяется активной политикой маршрутизации. В качестве активной политики вы можете выбрать:

- Политику маршрутизации по умолчанию — выбрана автоматически после инициализации ViPNet Coordinator HW. Политика использует маршруты из таблицы маршрутизации по умолчанию (Main). Настройка политики недоступна.
- Одну из пользовательских политик маршрутизации — создаются пользователем. С помощью таких политик вы можете разделить IP-трафик по признакам и маршрутизировать его по разным таблицам маршрутизации (см. Настройка функции MultiWAN).

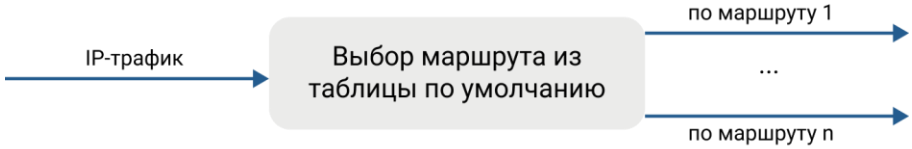

Рисунок 66. Маршрутизация при политике по умолчанию

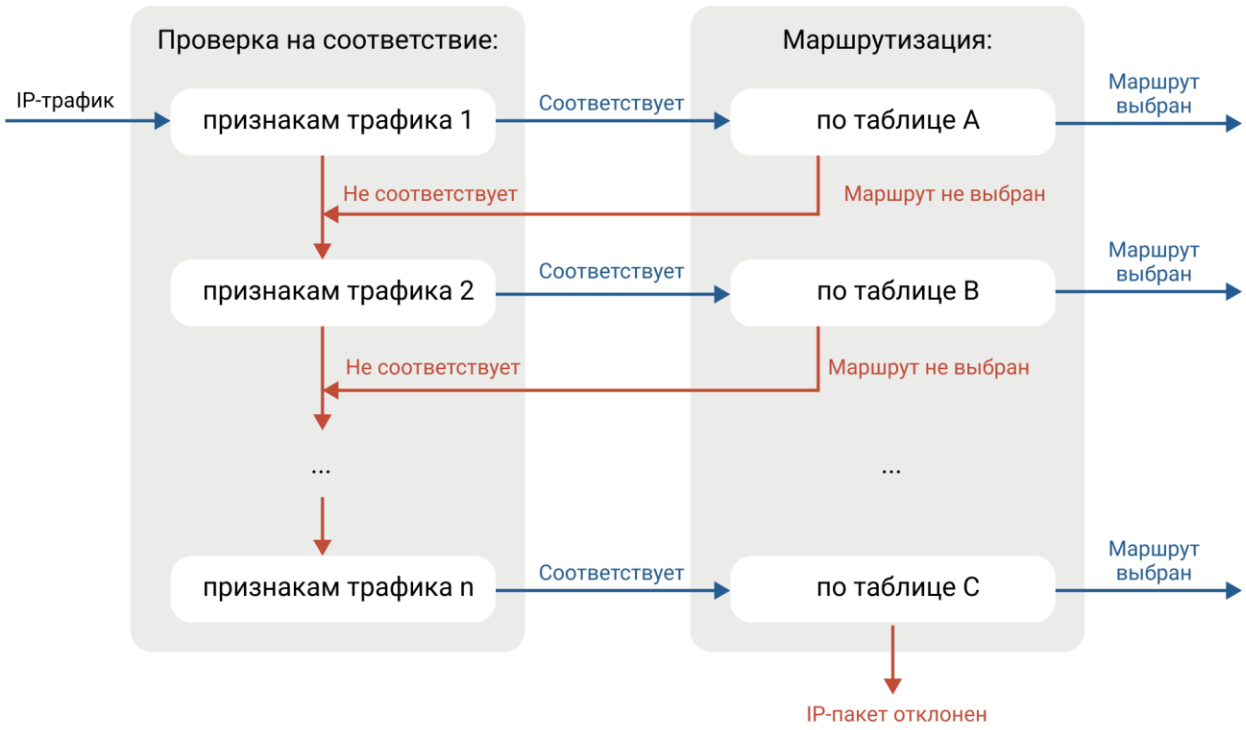

Рисунок 67. Маршрутизация при пользовательской политике

Пользовательская политика маршрутизации состоит из правил маршрутизации. Для каждого правила задаются:

- Приоритет — определяет в каком порядке правила будут применяться к трафику.
- Признаки трафика — задают условия, которым должен соответствовать трафик. Если признаки не указаны, правило распространяется на весь трафик.
- Таблица маршрутизации, по которой должен обрабатываться трафик, соответствующий заданным признакам трафика. Можно указать пользовательскую таблицу или таблицу по умолчанию.

Принципы маршрутизации при использовании пользовательской политики:

- IP-пакет последовательно проходит проверку правилами маршрутизации в соответствии с их приоритетом.
- Если IP-пакет соответствует всем признакам, заданным в правиле, он будет обработан по указанной таблице маршрутизации.
- Если IP-пакет не соответствует хотя бы одному из признаков правила, он передаётся на проверку следующему по приоритету правилу маршрутизации.

Формирование списка лучших маршрутов

В маршрутизации участвуют только лучшие статические и динамические маршруты в каждую сеть. Остальные маршруты в таблице игнорируются. Лучшие маршруты определяются в каждой таблице маршрутизации по следующим правилам:

- Из нескольких маршрутов в одну сеть лучшим признаётся маршрут с меньшей административной дистанцией, даже если маршруты получены из разных источников (Static, DHCP или OSPF). 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 маршрутизации будет участвовать первый маршрут. Если дистанции маршрутов, полученных из одного источника, равны, будут участвовать оба маршрута.
- Из нескольких маршрутов с разными префиксами (например, 10.0.0.0/8 и 10.0.0.0/16) лучшими признаются все маршруты.

Выбор маршрута из списка лучших

В процессе маршрутизации для каждого IP-пакета выбирается маршрут из списка лучших маршрутов. При наличии нескольких маршрутов в нужную сеть выполняются правила:

- Из нескольких лучших динамических маршрутов в одну сеть будет выбран маршрут с наименьшей метрикой, заданной протоколом динамической маршрутизации. Если метрики равны, будет выбран один из маршрутов в соответствии со стратегией маршрутизации ECMP (Equal-cost multi-path routing).
- Из нескольких лучших маршрутов в одну сеть с разным префиксом (маской подсети), будет выбран маршрут с наиболее длинным префиксом.
- 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 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 объединённого маршрута multi-hop route выйдет из строя, работоспособность маршрута не гарантируется.

Просмотр таблицы маршрутизации

Чтобы просмотреть список всех существующих маршрутов в таблице маршрутизации по умолчанию (Main):

Выберите **Маршрутизация** > **Маршрутизация** > **Сводная таблица.**

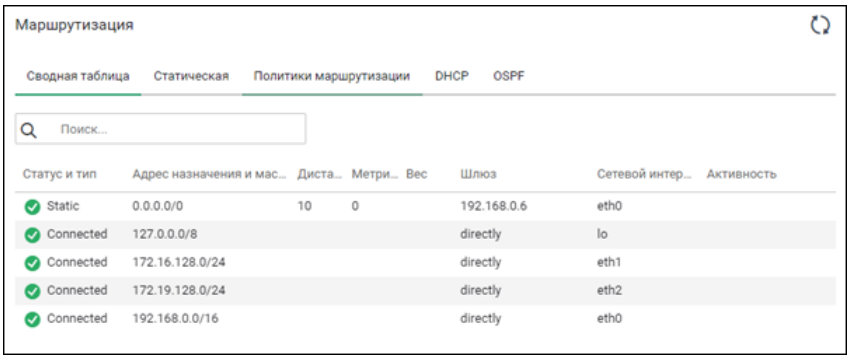

Рисунок 68. Просмотр общей таблицы маршрутизации

В списке для каждого маршрута отображается статус и тип. Если маршрут признан лучшим, он будет иметь статус . Такой маршрут будет участвовать в маршрутизации IP-трафика.

Для просмотра списка маршрутов от конкретного источника откройте вкладку **Статическая**, **DHCP** или **OSPF**.

Настройка статической маршрутизации

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

- Чтобы направлять часть IP-трафика по конкретным маршрутам (например, есть требование направлять IP-трафик по самому надежному каналу связи) или через конкретный шлюз.
- Нужен статический маршрут по умолчанию, если работа по протоколам динамической маршрутизации невозможна.
- Чтобы распределять передачу IP-трафика по нескольким маршрутам.

Внимание! В текущей версии ViPNet Coordinator HW не поддерживается асимметричная маршрутизация. Убедитесь, что пакеты проходят от источника до пункта назначения и обратно через координатор. При необходимости добавьте необходимые маршруты до узла или сети назначения или настройте динамическую трансляцию адресов.

Добавление статических маршрутов

Вы можете добавить статические маршруты в таблицу маршрутизации по умолчанию или создать пользовательские таблицы маршрутизации. Пользовательские таблицы маршрутизации используются для создания политик маршрутизации (см. Настройка политик маршрутизации).

Чтобы добавить статический маршрут:

1 Выберите **Маршрутизация** > **Маршрутизация** > **Статическая**.

2 Нажмите **Добавить маршрут**. Если у вас уже есть созданные таблицы маршрутизации, наведите курсор на нужную таблицу и нажмите .

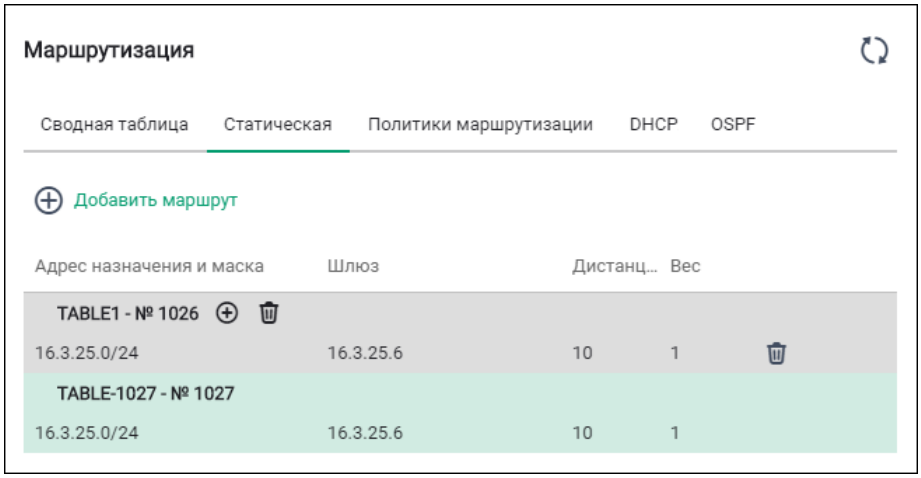

Рисунок 69. Список статических маршрутов

3 Задайте параметры маршрута:

- Таблица маршрутизации — выберите существующую таблицу или **Создать таблицу**.

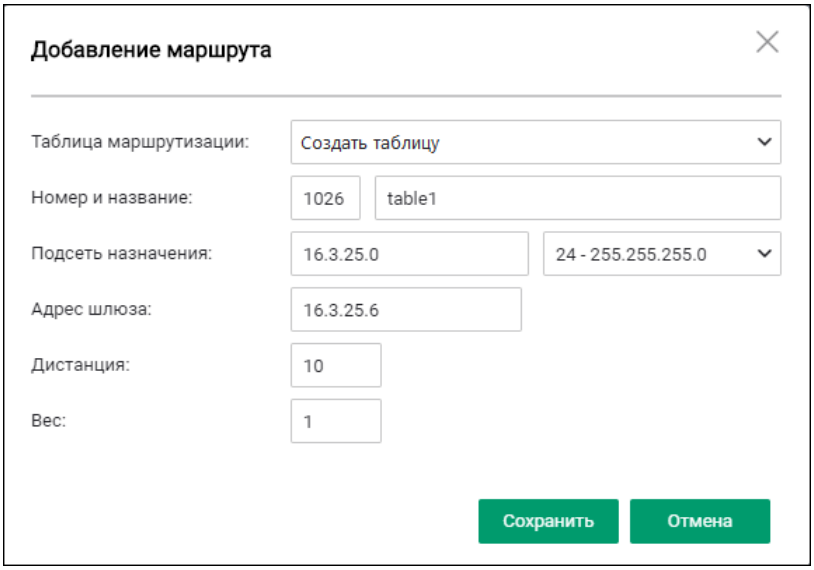

Рисунок 70. Добавление статического маршрута

- Номер и название создаваемой таблицы маршрутизации (если вы создаёте новую таблицу).

Примечание. В названии таблицы можно использовать до 63 символов:

- буквы латинского алфавита (A–z);
- цифры (0–9);
- знак «минус» (-).

Кроме того, нельзя создать таблицу с именем «main».

- IP-адрес назначения маршрута и маска подсети.
- IP-адрес шлюза для доступа к IP-адресу назначения.

- Административная дистанция. Если вы не укажете значение, автоматически будет задано значение 10. Если вы укажете административную дистанцию, и её значение будет совпадать со значением административной дистанции, заданной протоколам динамической маршрутизации, маршрут не будет добавлен. В этом случае создайте маршрут с другим значением административной дистанции.
- Вес. 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.

4 Нажмите **Сохранить**.

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).

Если в списках не появился новый маршрут, обновите списки  .

Маршрут, добавленный в таблицу маршрутизации по умолчанию, будет отображаться на вкладке **Сводная таблица**.

Для использования пользовательских таблиц маршрутизации создайте политику маршрутизации и активируйте её (см. Настройка политик маршрутизации).

Если нужно изменить параметры маршрута, удалите маршрут и создайте новый с нужными параметрами. Чтобы удалить маршрут или таблицу маршрутизации, нажмите  .

Настройка балансировки IP-трафика

Чтобы ускорить процесс отправки IP-пакетов в сеть назначения, создайте несколько статических маршрутов в данную сеть через разные шлюзы и настройте балансировку IP-трафика между ними. Это позволит для разных TCP-соединений отправлять IP-пакеты по разным маршрутам, что повысит скорость передачи IP-пакетов в сеть назначения. Балансировка трафика настраивается с помощью одного из параметров маршрутов — веса (`weight`). При этом все маршруты, которые будут участвовать в балансировке трафика, должны иметь одинаковую административную дистанцию, то есть иметь одинаковый приоритет.

Примечание. Маршруты в одну сеть назначения и с одинаковой дистанцией объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре таблицы маршрутизации на вкладке **Сводная таблица** они отображаются как один маршрут с несколькими шлюзами (см. Принципы маршрутизации).

Для настройки балансировки трафика:

1. Создайте маршруты с одинаковым IP-адресом назначения и с разными шлюзами.
2. Задайте каждому маршруту одинаковую административную дистанцию.
3. Задайте в каждом маршруте вес шлюзу. Трафик будет распределяться между шлюзами в соответствии с соотношением их весов. Например:
   - если вы создаёте два маршрута и в каждом маршруте вес шлюза равен 1, то трафик будет разделён между этими маршрутами поровну, то есть 50% трафика будет передаваться по одному маршруту, 50% — по второму;
   - если вы создаёте три 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 трафика, чем по первому, по третьему — в три раза больше, чем по первому.

Пример создания статических маршрутов с весом шлюзов равным 1:

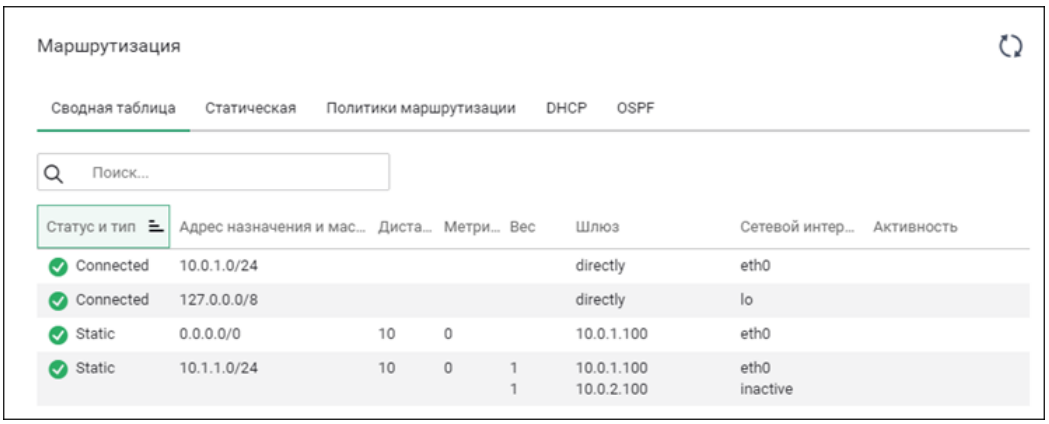

Рисунок 71. Распределение нагрузки между статическими маршрутами в одну сеть

Примечание. Если при создании маршрута вы не укажете вес шлюза, то автоматически шлюзу будет назначен вес равный 1. Нельзя задать вес равный 0 или более 256.

Балансировка IP-трафика будет осуществляться только если созданные маршруты признаны лучшими (см. Принципы маршрутизации).

Настройка параметров маршрутов от DHCP/PPP-протокола

Если на каком-либо сетевом интерфейсе ViPNet Coordinator HW включен режим DHCP и настроено автоматическое получение маршрутов, то в процессе маршрутизации будут использоваться эти маршруты. В этом случае настройте дополнительные параметры:

1. Настройте административную дистанцию для протокола DHCP. Это позволит определить приоритет маршрутов DHCP-сервера среди всех маршрутов в таблице маршрутизации по умолчанию (статических маршрутов, маршрутов протокола OSPF, если такие есть).
2. Если режим DHCP включен на нескольких сетевых интерфейсах, настройте метрики протокола DHCP на каждом сетевом интерфейсе, на котором включен этот режим. Это позволит определить приоритет среди маршрутов DHCP-сервера в одну и ту же сеть, полученных с разных сетевых интерфейсов.

Если ViPNet Coordinator HW подключен, например, к сети 3G и получает информацию для маршрута по умолчанию от PPP-сервера провайдера, 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 маршруты, а также настроена статическая маршрутизация (см. Настройка статической маршрутизации) или динамическая маршрутизация, то задайте административную дистанцию для маршрутов протокола DHCP. 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, 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:

1. Выберите **Маршрутизация** > **Маршрутизация** > **DHCP**.

2 Введите значение административной дистанции в поле **Дистанция по умолчанию** и нажмите **Сохранить**. По умолчанию указана административная дистанция 70.

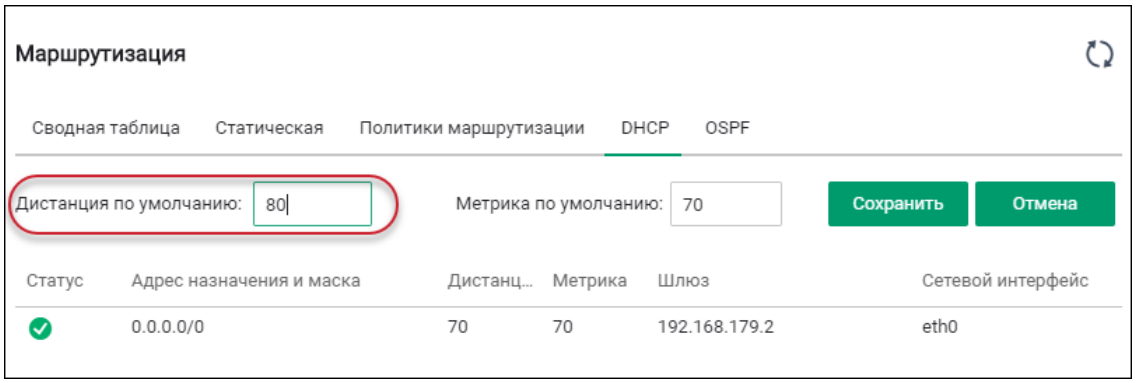

Рисунок 72. Задание административной дистанции маршрутам DHCP-сервера

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 разные маршруты от DHCP-сервера в одну и ту же сеть. В этом случае требуется определить, какой маршрут является лучшим, чтобы использовать его при маршрутизации трафика. Параметром, позволяющим выбрать наилучший маршрут, выступает метрика маршрута. Её можно задать на каждом сетевом интерфейсе, на котором включен режим DHCP, чтобы определить приоритет маршрутов DHCP-сервера на разных сетевых интерфейсах. Чем меньше значение метрики, тем выше приоритет маршрута. Если на разных сетевых 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 неё используется метрика по умолчанию.

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

- Ethernet.
- VLAN.
- Wi-Fi (wlan) — нет в исполнении ViPNet Coordinator VA.
- Агрегированный интерфейс.

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:

1 Выберите **Сетевые интерфейсы**.

2 Выберите интерфейс, справа появится окно настроек.

3 Убедитесь, что установлены флажки **Получать параметры автоматически** (включен режим DHCP) и **Маршруты** (автоматическое получение маршрутов).

4 Введите значение в поле **Метрика** и нажмите **Сохранить**. Если поле оставить пустым, будет использоваться метрика по умолчанию.

Настройка метрики для маршрутов PPP-протокола

Если ViPNet Coordinator HW подключен к мобильной сети 3G, 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.

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

Если кроме подключения к сети 3G 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 приоритет выше, 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). В этом случае маршруты по умолчанию PPP- и DHCP-протокола будут иметь одинаковый приоритет.

Метрику для PPP-протокола вы можете настроить в параметрах интерфейса модема и только в том случае, если разрешено добавление маршрута по умолчанию от PPP-сервера провайдера. Чтобы настроить метрику:

1. Выберите **Сетевые интерфейсы**.
2. Выберите интерфейс модема, справа появится окно настроек.
3. Убедитесь, что установлен флажок **Маршруты** (разрешено добавление маршрута по умолчанию).
4. Введите значение в поле **Метрика** и нажмите **Сохранить**. Если поле оставить пустым, будет использоваться метрика по умолчанию.

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

Если для маршрутов протоколов DHCP и PPP не задавались специфичные метрики, то для определения приоритета маршрутов будет использоваться метрика по умолчанию (первоначально — 70).

Чтобы изменить метрику:

1. Выберите **Маршрутизация** > **Маршрутизация** > **DHCP**.
2. Введите новое значение в поле **Метрика** и нажмите **Сохранить**. Метрика по умолчанию — 70.

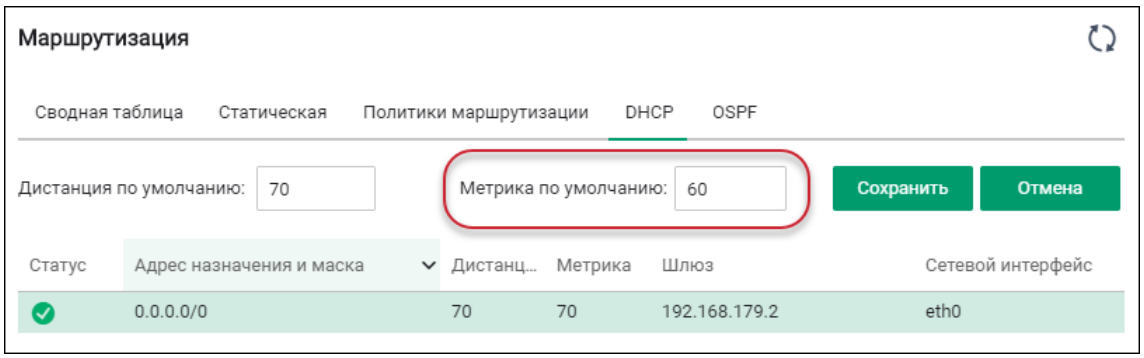

Рисунок 73. Задание метрики по умолчанию

Настройка динамической маршрутизации

Внимание! Исполнение HW10 не поддерживает динамическую маршрутизацию.

Если в вашей сети поддерживается работа по протоколу OSPF, то вы можете настроить на ViPNet Coordinator HW динамическую маршрутизацию. Данные настройки позволят автоматически создавать таблицы маршрутизации на основе маршрутов, формируемых по данному протоколу, и распространять их между другими маршрутизаторами в рамках одной сети.

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

- используются другие OSPF-маршрутизаторы, и они напрямую связаны с ViPNet Coordinator HW;
- используется протокол OSPF версии 2;
- поддерживается многоадресное вещание (multicast);
- по требованиям безопасности вашей организации разрешена передача IP-трафика по протоколу OSPF между сетевыми узлами.

Внимание! 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.

Общие сведения о протоколе OSPF

Протокол OSPF — внутренний шлюзовой протокол (Interior Gateway Protocol, IGP), используется для распространения данных маршрутизации внутри одной автономной системы.

Реализация протокола OSPF в ViPNet Coordinator HW имеет ограничения: из RFC 2328 не поддерживаются:

- изменение пропускной способности reference-bandwidth — cost, auto-cost;
- настройка метрик маршрутов;
- перераспределение (redistribute) маршрутов, кроме заданных статически и полученных по DHCP;

- настройка параметров взаимодействия соседних маршрутизаторов — HelloInterval и DeadInterval;
- другие типы областей (area type), кроме backbone и standard;
- настройка типа сети (network types), — задан тип Broadcast;
- фильтрация по политике импорта и экспорта маршрутов;
- виртуальные каналы (Virtual Links).

OSPF-маршрутизация работает следующим образом:

1. OSPF-маршрутизаторы устанавливают связь друг с другом посредством многоадресной (multicast) рассылки.
2. OSPF-маршрутизаторы начинают обмениваться сообщениями типа LSA (Link State Advertisements), в которых передают информацию о состоянии каналов связи с помощью однонаправленной (unicast) рассылки.
3. 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 передаётся маршрутизаторам-соседям.
4. На каждом маршрутизаторе по алгоритму Дейкстры (SPF algorithm) вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость. 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 маршрутизации, соединённых друг с другом через некоторую базовую область.

Выделяют следующие типы областей маршрутизации:

- Базовая или область 0 (backbone area) — с ней должны быть соединены все остальные области автономной системы.
- Стандартная (standard area) — граничит как с другими областями, так и с другими автономными системами.
- Стандартная тупиковая (stub area) — граничит только с другими областями.
- Полностью тупиковая (totally stubby area) — граничит только с одной областью.
- Не полностью тупиковая (not-so-stubby area) — стандартная тупиковая область, которая может взаимодействовать с другими автономными системами с помощью пограничных маршрутизаторов (ABR).

Каждый OSPF-маршрутизатор входит в определённую область маршрутизации и обменивается информацией только с маршрутизаторами, входящими в эту же область. При этом обмен идет не напрямую, а через посредника — маршрутизатор, выбранный главным в этой области. Информация между разными областями передаётся через маршрутизатор, который располагается на границе этих областей. Если автономная система взаимодействует с другой автономной системой, то информация передаётся через маршрутизатор, который располагается на границе

систем. Такой подход позволяет уменьшить объём рассылаемых LSA-сообщений, тем самым уменьшить нагрузку на маршрутизаторы и повысить скорость построения таблиц маршрутизации.

Выделяют следующие типы маршрутизаторов:

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

Примечание. Для проверки подлинности маршрутов, полученных с других устройств по протоколу OSPF, мы рекомендуем настроить аутентификацию на маршрутизаторах.

Протокол OSPF поддерживает два способа аутентификации:

- простая аутентификация на пароле (simple password authentication). Одинаковый пароль настраивается на интерфейсах, через которые передаётся информация по протоколу OSPF. Пароль передаётся в открытом виде.
- криптографическая аутентификация (cryptographic authentication). Общий секретный ключ и идентификатор ключа настраиваются на интерфейсах, через которые передаётся информация по протоколу OSPF. Ключ передаётся в зашифрованном виде (используется алгоритм хэширования md5).

Аутентификация настраивается для соседних маршрутизаторов. По умолчанию протокол OSPF не использует аутентификацию.

Настройка параметров динамической маршрутизации по протоколу OSPF

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;
- создать ряд сетевых фильтров.

При настройке динамической маршрутизации по протоколу OSPF учитывайте:

- В случае сбоя на одном из маршрутов для переключения на альтернативный маршрут может потребоваться около 10 секунд после того, как будет обнаружено отсутствие ответного трафика на исходящий трафик от координатора, который потерял связь с удаленным координатором.
- 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.

Вы также можете настроить перераспределение маршрутов по протоколу OSPF.

Настройка протокола OSPF

1 Выберите **Маршрутизация** > **Маршрутизация** > **OSPF**.

2 Включите **Служба OSPF**.

3 Для настройки области маршрутизации выберите вкладку **Области**.

3.1 Нажмите **Добавить** и укажите параметры:

3.1.1 Идентификатор области маршрутизации.

Указать область маршрутизации можно:

- в десятичном формате 0-4294967295;
- в формате A.B.C.D, где A, B, C, D — целое число от 0 до 255. Данный способ можно использовать, чтобы в качестве идентификатора указать адрес сети, в которой будет осуществляться обмен информацией.

В интерфейсе будут отображены оба представления.

3.1.2 Способ аутентификации:

- **Нет** — без аутентификации;
- **Пароль** — простая аутентификация на пароле (simple password authentication);
- **MD5** — криптографическая аутентификация (cryptographic authentication).

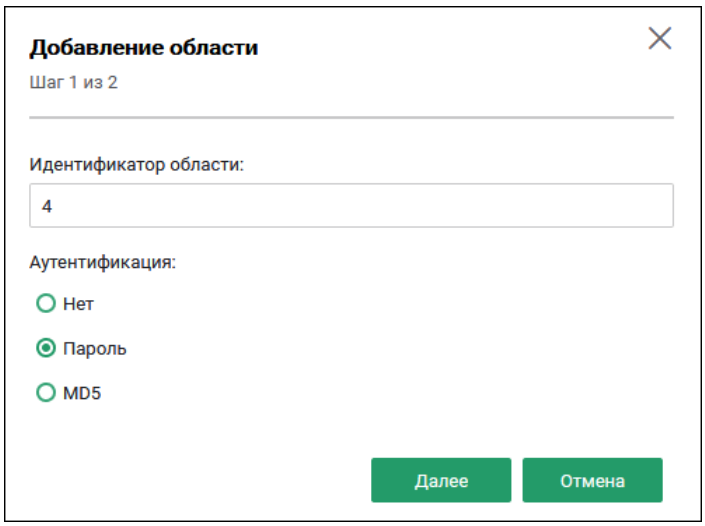

Рисунок 74. Добавление области

3.2 Нажмите **Далее.**

3.3 Нажмите **Добавить** и задайте сети, входящие в область маршрутизации:

3.3.1 Введите IP-адрес и маску сети в нотации CIDR, например 10.0.0.0/16.

3.3.2 Нажмите .

Вы можете указать не более 128 сетей.

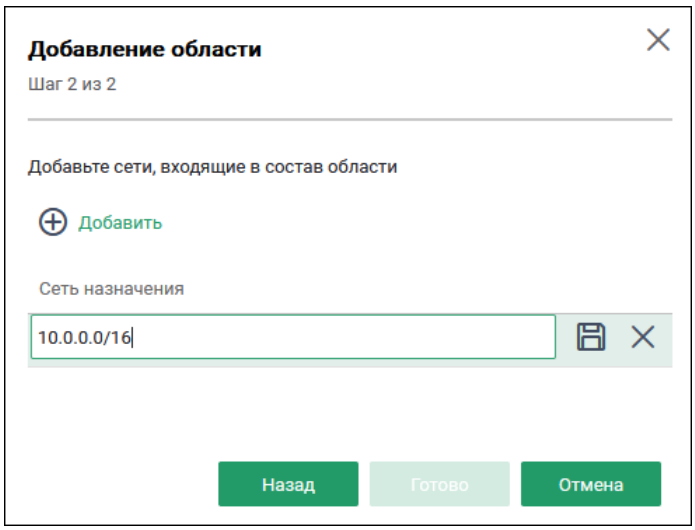

Рисунок 75. Добавление подсети

3.4 Нажмите **Готово.**

4 Для настройки интерфейса, за которым находится область маршрутизации, выберите вкладку **Интерфейсы.**

4.1 В строке интерфейса нажмите .

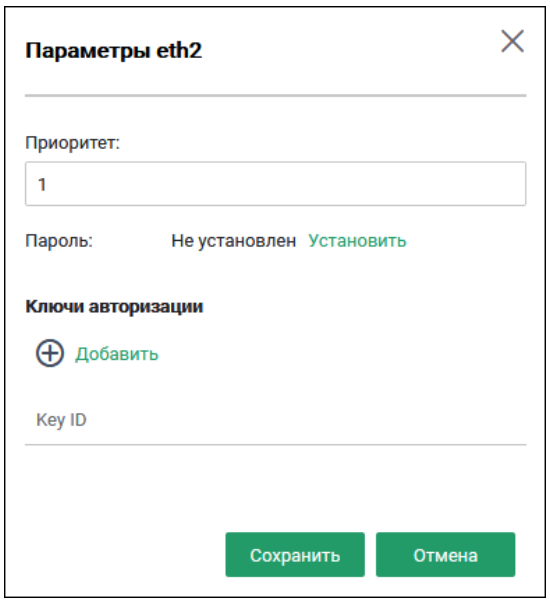

Рисунок 76. Настройка параметров интерфейса

4.2 При аутентификации на пароле задайте его:

4.2.1 В поле **Пароль** нажмите **Установить.**

4.2.2 Введите пароль и его подтверждение.

4.2.3 Нажмите **Сохранить.**

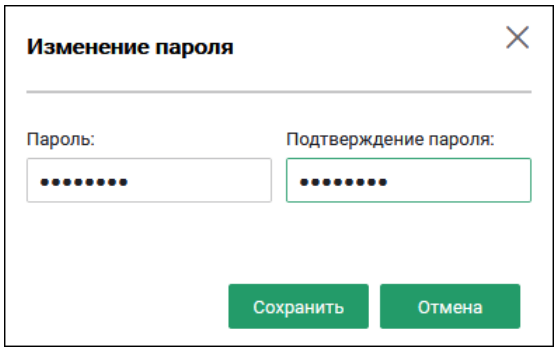

Рисунок 77. Установка пароля

4.3 При криптографической аутентификации добавьте ключ:

4.3.1 В группе **Ключи авторизации**, нажмите **Добавить**.

4.3.2 Задайте идентификатор ключа.

4.3.3 Задайте ключ и его подтверждение.

4.3.4 Нажмите **Сохранить**.

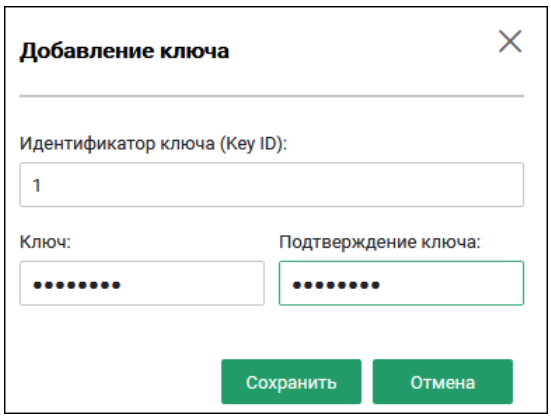

Рисунок 78. Добавление ключа

Примечание. На каждом интерфейсе вы можете создать не более 255 ключей с уникальным идентификатором ключа и только один пароль.

5 Создайте сетевые фильтры открытой сети:

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

Таблица 3. Фильтры для входящего открытого OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Allow OSPF unicast	<IP-адрес OSPF-маршрутизатора>	@local	IP:89	pass
Allow OSPF multicast	<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). В фильтрах вместо `@OSPF` вы также можете указать `proto 89`.

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

Таблица 4. Фильтры для исходящего открытого OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Allow OSPF outcoming	@local	@any	IP:89	pass

6 Если между координаторами сети ViPNet установлены связи на уровне пользователей (в том числе между координатором и ViPNet xFirewall), создайте фильтры защищённой сети:

Таблица 5. Фильтры для OSPF-трафика в защищённой сети

Название	Источник	Назначение	Протокол	Действие
Allow OSPF outcoming	@local	@any	IP:89	pass
Allow OSPF incoming	@any	@local	IP:89	pass

Настройка перераспределения маршрутов

Протокол OSPF может перераспределять маршруты, заданные статически или полученные по протоколу DHCP. Это может понадобиться, если в подсетях разветвленной сети используются разные виды маршрутов.

Рассмотрим пример:

- Главный офис и филиал входят в одну автономную систему. Используют маршрутизацию по протоколу OSPF.
- Сеть партнера является другой автономной системой. Использует статическую маршрутизацию (Static). На маршрутизаторе настроены статические маршруты для сетей главного офиса и филиала.
- HW-1 расположен на границе автономных областей и является граничным маршрутизатором.
- На HW-1 настроены статические маршруты в сеть партнера.

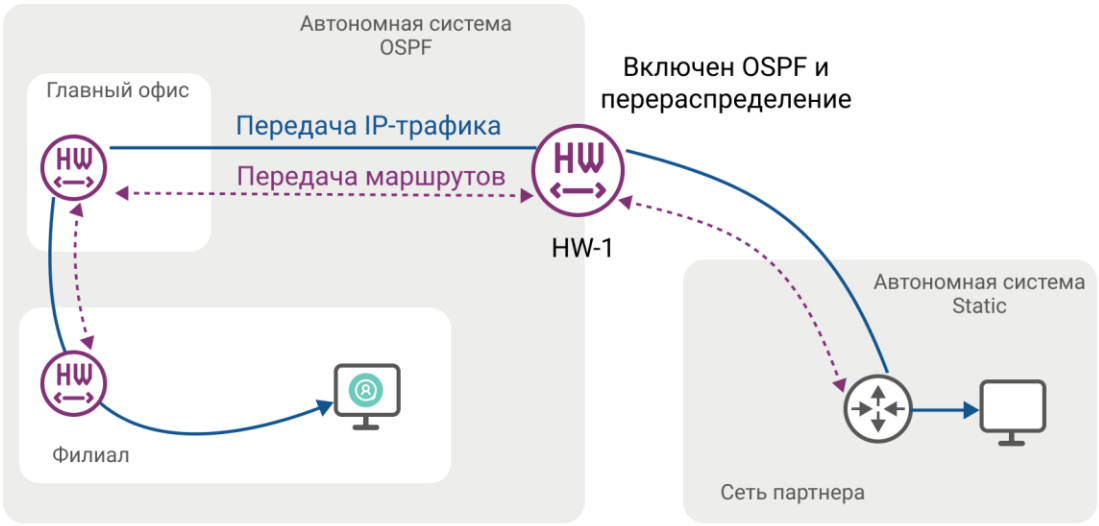

Рисунок 79. Перераспределение маршрутов

Чтобы узлы сети филиала могли обмениваться IP-трафиком с узлами сети партнера, вместо настройки статических маршрутов на оборудовании сетей главного офиса и филиала включите перераспределение статических маршрутов на координаторе HW_1:

1 Выберите **Маршрутизация** > **Маршрутизация** > **OSPF**.

2 Включите маршрутизацию по протоколу OSPF.

3 Перейдите в **Настройки службы**.

4 Установите флажок **Статические** в группе **Типы распространяемых маршрутов.**

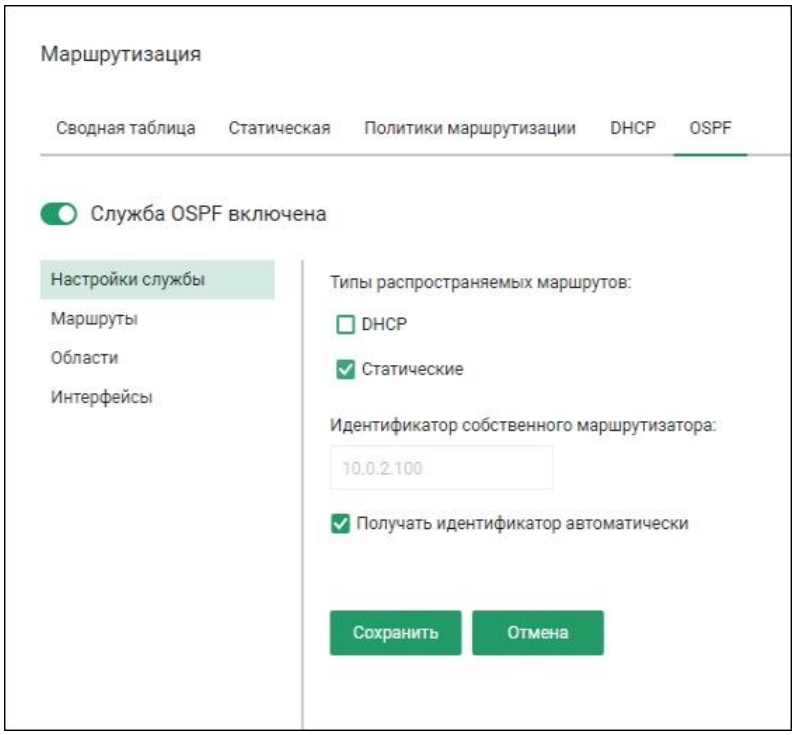

Рисунок 80. Включение перераспределения маршрутов DHCP-сервера

5 Нажмите **Сохранить**.

Координатор HW-1 передаст статические маршруты в автономную сеть офиса и узлы сети филиала смогут обмениваться IP-трафиком с узлами сети партнера.

Примечание.

- Статический маршрут по умолчанию не перераспределяется.
- Если в сети партнера используются динамические маршруты от DHCP-сервера, установите флажок **DHCP** в группе **Типы распространяемых маршрутов**. Также на граничном маршрутизаторе должно быть настроено получение маршрутов от DHCP-сервера сети партнера.

Настройка функции MultiWAN

Если для доступа ViPNet Coordinator HW в интернет используется несколько шлюзов (провайдеров), то вы можете настроить политики маршрутизации для различных случаев. Например, для распределения нагрузки между каналами связи или для резервирования каналов при использовании нескольких интернет-провайдеров на случай отказа одного из них (чтобы избежать потерь трафика).

Для этих целей в ViPNet Coordinator HW реализована технология MultiWAN, позволяющая настроить поведение ViPNet Coordinator HW в случае недоступности одного из интернет-шлюзов. Эта технология представлена в ViPNet Coordinator HW следующими функциями:

- Пользовательские таблицы маршрутизации (см. Добавление статических маршрутов). С их помощью вы можете задать различные маршруты для различных ситуаций. Например, основную таблицу маршрутизации и дополнительную таблицу маршрутизации на случай, если шлюз основного провайдера станет недоступен и потребуется перенаправить трафик через шлюз альтернативного провайдера.
- Политики маршрутизации (см. Настройка политик маршрутизации). С их помощью вы можете задать условия, при которых трафик будет перенаправляться по заданным таблицам маршрутизации.
- Проверка состояния шлюзов (Dead Gateway Detection, DGD) (см. Настройка проверки состояния шлюзов (DGD)). С помощью этой функции вы можете задавать выполнение политики маршрутизации в зависимости от доступности или недоступности шлюза.

Особенности настройки функции MultiWAN

- Не добавляйте в пользовательские таблицы маршрутизации маршруты, противоречащие маршрутам в таблице по умолчанию.
- Не используйте динамические маршруты, получаемые по протоколам DHCP и OSPF при настройке маршрутизации для резервирования канала доступа в интернет (при использовании DHCP отключите автоматическое получение маршрутов. Динамические маршруты записываются в таблицу по умолчанию и будут задействованы с соответствующим приоритетом. Не используйте канал с динамическими маршрутами в качестве резервного канала.
- Добавляйте маршруты только в пользовательские таблицы маршрутизации, а таблицу по умолчанию изменяйте лишь в крайнем случае.
- Перед активацией политики маршрутизации убедитесь, что она настроена корректно и не нарушит связь ViPNet Coordinator HW с узлом, с которого вы настраиваете ViPNet Coordinator HW.

  К нарушению связи может привести:

- отсутствие в политике правила, разрешающего обрабатывать весь трафик через таблицу маршрутизации по умолчанию;
- наличие в политике правила, обрабатывающего весь трафик, с приоритетом выше, чем у правила обрабатывающего весь трафик по таблице маршрутизации по умолчанию;
- удаление правила, содержащего таблицу маршрутизации по умолчанию или удаление из правила таблицы маршрутизации по умолчанию.

- Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере горячего резервирования — это может привести к циклической перезагрузке обоих узлов кластера.
- После добавления проверки шлюза DGD по протоколу TCP и портам 80 и 443 необходимо создать соответствующий разрешающий сетевой фильтр: источник — **Мой узел ViPNet**, назначение — IP-адрес шлюза, порты назначения 80 и 443.

Настройка политик маршрутизации

Примечание. Принципы использования политик маршрутизации см. в разделе Принципы маршрутизации.

Для применения пользовательской политики маршрутизации необходимо добавить в неё правила маршрутизации и выбрать её в качестве активной.

Каждое правило состоит из условий, которые применяются к трафику (признаки трафика), и действия, которое выполняется, если трафик соответствует условиям.

1 Выберите **Маршрутизация** > **Маршрутизация** > **Политики маршрутизации**.

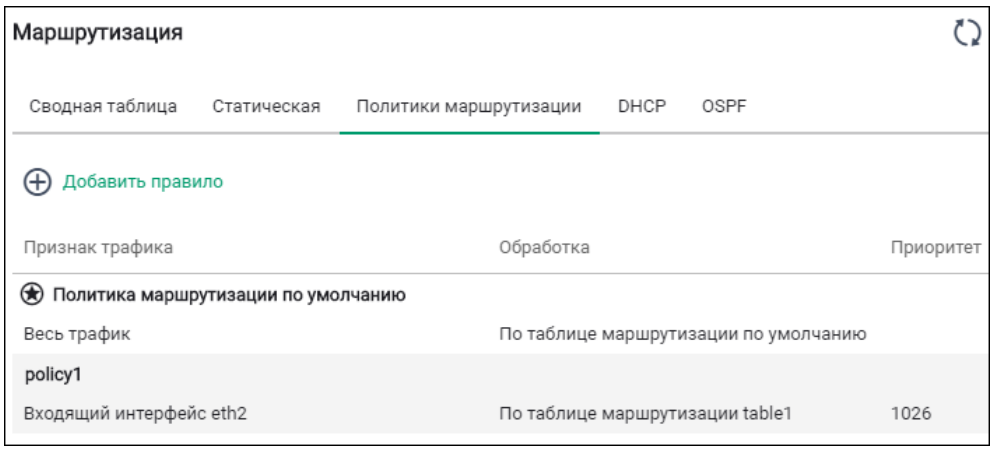

Рисунок 81. Настройка политик маршрутизации

2 Нажмите **Добавить правило** или наведите курсор на нужную политику и нажмите .

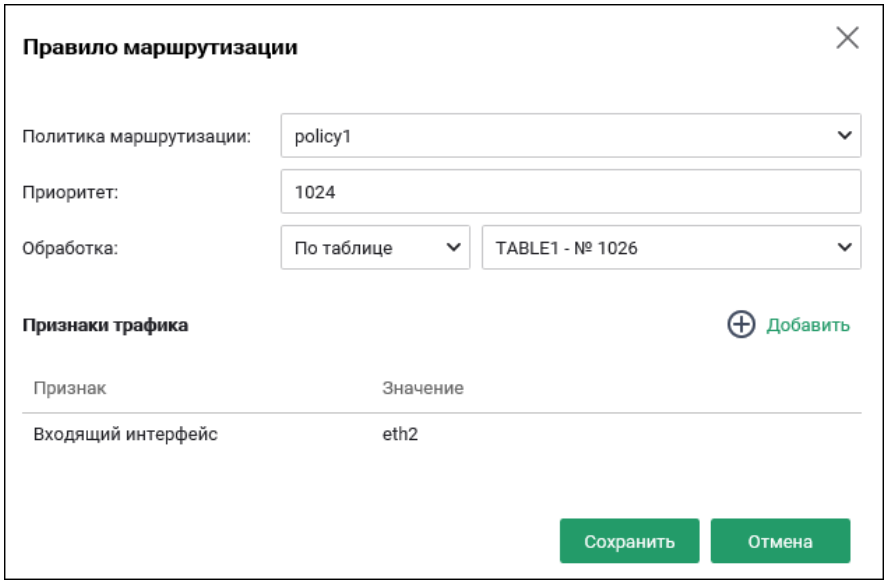

Рисунок 82. Добавление правила маршрутизации

3 Задайте имя политики (если вы хотите добавить правило в новую политику маршрутизации) или выберите существующую политику.

4 Задайте приоритет правила от 1024 до 2048. Чем меньше значение, тем выше приоритет правила.

Примечание. Приоритет у правил по таблице по умолчанию должен быть выше, чем у общих правил маршрутизации, применяющихся для всего трафика.

---

5 Выберите метод обработки IP-пакетов для правила маршрутизации:

- Чтобы IP-пакеты, попадающие под правило маршрутизации, обрабатывались по созданной ранее таблице маршрутизации (см. Добавление статических маршрутов), выберите **По таблице** и в появившемся списке выберите таблицу маршрутизации.
- Чтобы блокировать IP-пакеты, попадающие под политику маршрутизации, выберите **Блокировать**.

6 Задайте параметры IP-пакетов, по которым будет выполняться правило маршрутизации:

6.1 Нажмите ⊕ **Добавить**.

6.2 В списке **Признак** выберите один из параметров IP-пакетов, по которым будет выполняться правило маршрутизации.

6.3 В поле (или списке) **Значение** задайте (или выберите) значение выбранного параметра.

6.4 Нажмите **Сохранить**.

Внимание! Чтобы не нарушить прохождение IP-трафика между локальными сетями (сетевыми интерфейсами ViPNet Coordinator HW), в каждую пользовательскую политику маршрутизации добавьте правило для всего трафика (без признаков) с таблицей маршрутизации по умолчанию. Только эта таблица содержит маршруты в локальную сеть (`connected`). При этом мы рекомендуем присвоить такому правилу наивысший приоритет в политике и очистить таблицу по умолчанию от статических и динамических маршрутов.

7 Чтобы сохранить созданное правило маршрутизации, нажмите **Сохранить**.

8 Чтобы активировать политику маршрутизации, в строке рядом с ней нажмите и подтвердите свои действия.

Внимание! После смены активной политики вы можете потерять доступ к ViPNet Coordinator HW через веб-интерфейс.

Настройка проверки состояния шлюзов (DGD)

1 Выберите **Маршрутизация > Проверка шлюзов (DGD)**.

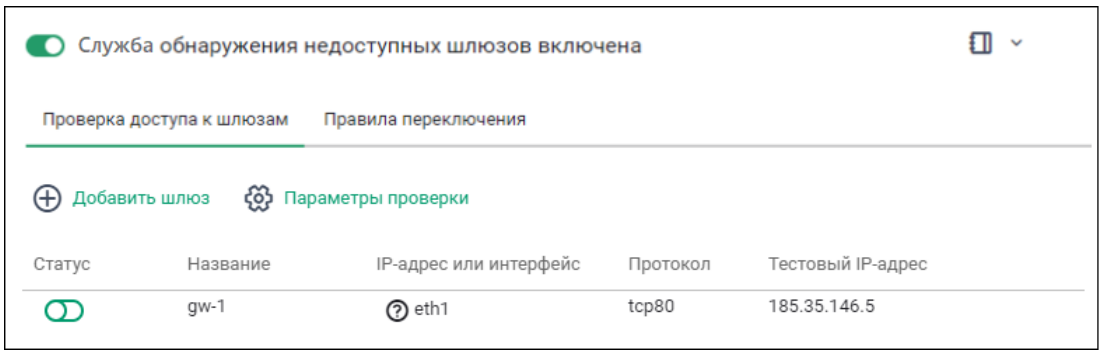

Рисунок 83. Настройка проверки состояния шлюзов

2 Включите **Служба обнаружения недоступных шлюзов**.

3 Нажмите **Добавить шлюз** и задайте параметры:

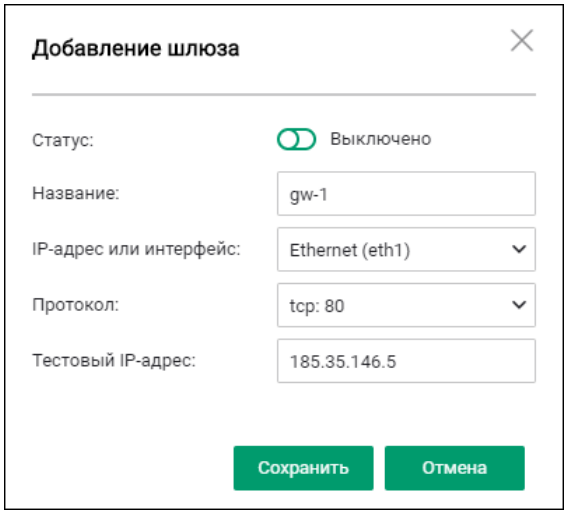

Рисунок 84. Добавление проверки доступности шлюза

- произвольное название шлюза;
- IP-адрес шлюза или сетевой интерфейс ViPNet Coordinator HW;

> **Примечание.** Сетевой интерфейс можно выбрать, если он получает IP-адрес по протоколу DHCP. Также, в качестве сетевого интерфейса, вы можете выбрать динамический ppp-интерфейс.

- метод проверки (протокол и порт);
- тестовый IP-адрес шлюза — IP-адрес сетевого узла, по которому будет проверяться доступность шлюза. Несколько шлюзов могут иметь один и тот же тестовый IP-адрес.

4 Если вы задали проверку шлюза с использованием TCP-соединения и порта 80 или 443, создайте разрешающий сетевой фильтр со следующими параметрами:

- Действие: Пропускать трафик.
- Источники: Мой узел ViPNet.
- Назначения: тестовый IP-адрес шлюза.
- Протоколы: TCP: 80, TCP: 443.

Подробнее о создании сетевых фильтров см. в разделе Создание и изменение сетевых фильтров.

5 Чтобы включить проверку состояния шлюза, щелкните переключатель в столбце **Статус**.

6 Чтобы добавить действие, выполняемое при доступности (недоступности) шлюза:

6.1 Выберите вкладку **Правила переключения**.

6.2 Нажмите **Добавить правило**.

6.3 Задайте параметры:

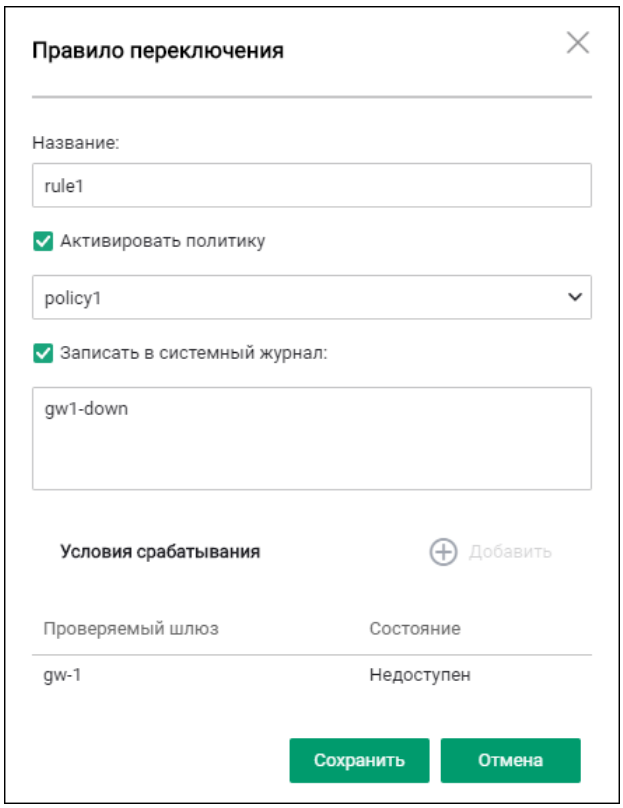

Рисунок 85. Добавление правила проверки состояния шлюза

- Чтобы при обнаружении доступности (недоступности) шлюза выполнялась политика маршрутизации, выберите **Активировать политику** и выберите политику маршрутизации из списка.
- Чтобы при обнаружении доступности (недоступности) шлюза создавалась запись в системном журнале, выберите **Записать в системный журнал** и введите текст, который будет записываться в журнал.
- Чтобы добавить условие срабатывания проверки шлюза (доступность или недоступность), нажмите **Добавить**.
- Выберите из списка шлюз и условие его проверки.

6.4 Нажмите **Сохранить**.

7 Чтобы сбросить параметры проверки доступности к значениям по умолчанию:

7.1 Выберите вкладку **Проверка доступа к шлюзам**.

7.2 Нажмите **Параметры проверки**.

7.3 Нажмите **Сброс настроек**.

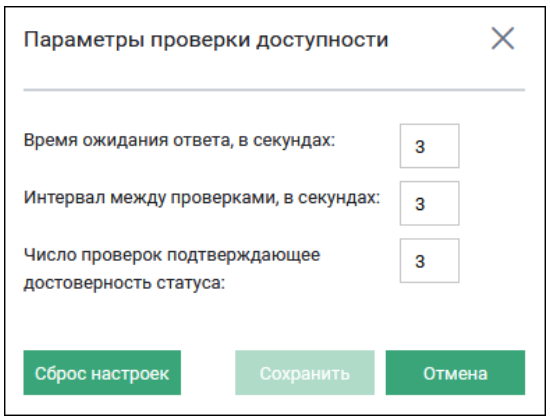

Рисунок 86. Окно настроек проверки доступности шлюза

10

Работа с сертификатами

Общие сведения

В веб-интерфейсе вы можете:

- создать запрос на выпуск сертификата;
- импортировать серверный сертификат, списки отозванных сертификатов;
- перевыпустить самоподписанный сертификат.

Для настройки подключения с помощью сертификата, выданного центром сертификации:

1 Создайте запрос на выпуск серверного сертификата (см. Создание запроса на выпуск сертификата).

2 Экспортируйте созданный запрос.

3 Перешлите запрос на выпуск серверного сертификата в аккредитованный удостоверяющий центр (например, GlobalSign, VeriSign и др.).

Примечание. При выпуске сертификатов учитывайте:

- Сертификаты должны быть подписаны с использованием алгоритма RSA.
- Поддерживается импорт сертификатов в кодировке DER и Base64.
- УЦ должен использовать алгоритм подписи SHA-2.

---

4 Импортируйте серверный сертификат в локальное хранилище ViPNet Coordinator HW.

5 Установите импортированный сертификат для доступа по протоколу HTTPS через командный интерпретатор (подробнее в документе «Настройка с помощью командного интерпретатора»).

Создание запроса на выпуск сертификата

1 Выберите **Системные настройки** > **Сертификаты** > **Установленные сертификаты.**

2 Создайте запрос на выпуск серверного сертификата.

- Нажмите **Создать запрос на сертификат** и заполните параметры запроса.

  Обязательные параметры:

  - **Имя файла** — имя запроса на создание сертификата;
  - **Размер ключа RSA** — размер создаваемого RSA-ключа в битах: 2048, 3072, 4096;
  - **Хэш-функция** — алгоритм хэширования: sha256, sha384, sha512.
  - **IP-адреса ресурса или доменные имена**.

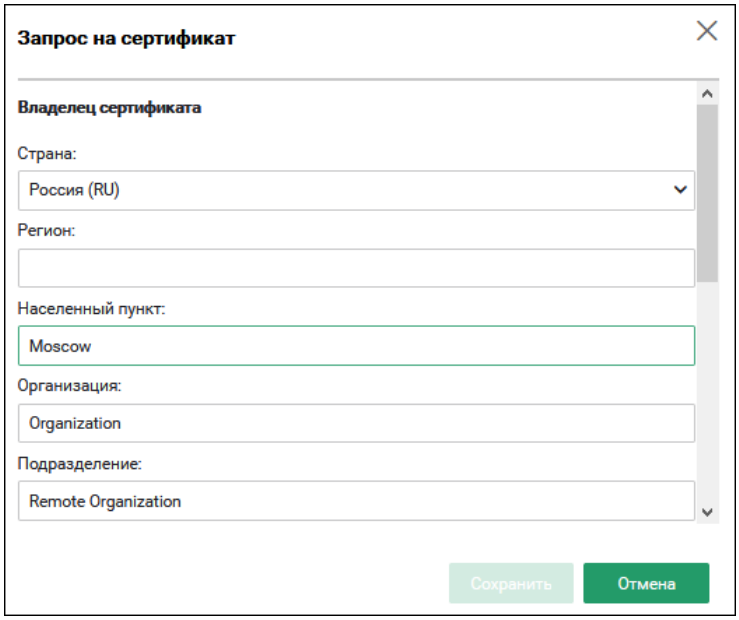

Рисунок 87. Параметры запроса

- Нажмите **Сохранить**. Созданный запрос отобразится на странице со знаком .

  Будет создан файл запроса и файл с закрытым ключом.

3 Скачайте запрос на сертификат. В соответствующей строке нажмите .

Для удаления запроса на сертификат в соответствующей строке нажмите .

Импорт сертификата

1 Выберите **Системные настройки** > **Сертификаты** > **Установленные сертификаты.**

2 Нажмите **Импортировать.**

3 Вставьте текст сертификата (или списка отозванных сертификатов) или нажмите **Загрузить файл** и выберите сертификат (список отозванных сертификатов).

4 После проверки сертификата нажмите **Импортировать**.

Загруженный сертификат отобразится на странице **Установленные сертификаты**:

- — корневой сертификат;
- — локальный сертификат;
- — отозванный сертификат.

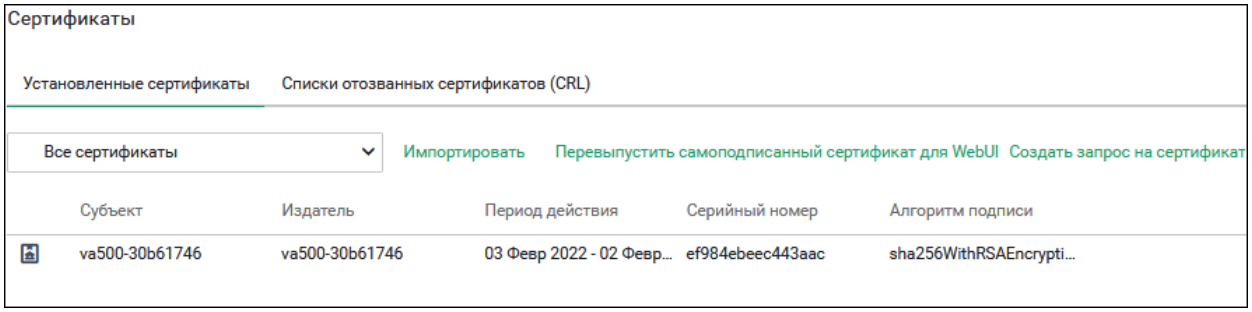

Рисунок 88. Установленные сертификаты

Список отозванных сертификатов отобразится на странице **Списки отозванных сертификатов (CRL)**.

Для удаления сертификата в соответствующей строке нажмите .

Также вы можете перевыпустить самоподписанный сертификат. Для этого нажмите **Перевыпустить самоподписанный сертификат для WebUI**, в появившемся окне заполните необходимую информацию и нажмите **Создать**. После перевыпуска самоподписанного сертификата пройдите авторизацию.

11

Мониторинг состояния ViPNet Coordinator HW и просмотр журналов

Мониторинг состояния ViPNet Coordinator HW

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

Примечание. Для службы системы защиты от сбоев Failover на странице **Состояние системы** также отображается режим работы (режим кластера горячего резервирования).

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

Чтобы просмотреть информацию о текущем состоянии ViPNet Coordinator HW:

1 Выберите **Журналы** > **Состояние системы**.

2 На странице **Состояние системы** будет отображена информация о ViPNet Coordinator HW. На данной странице вы можете следить за изменением отображенных параметров.

Внимание! При остановленной службе системы защиты от сбоев (Failover) информация о состоянии системы не отображается.

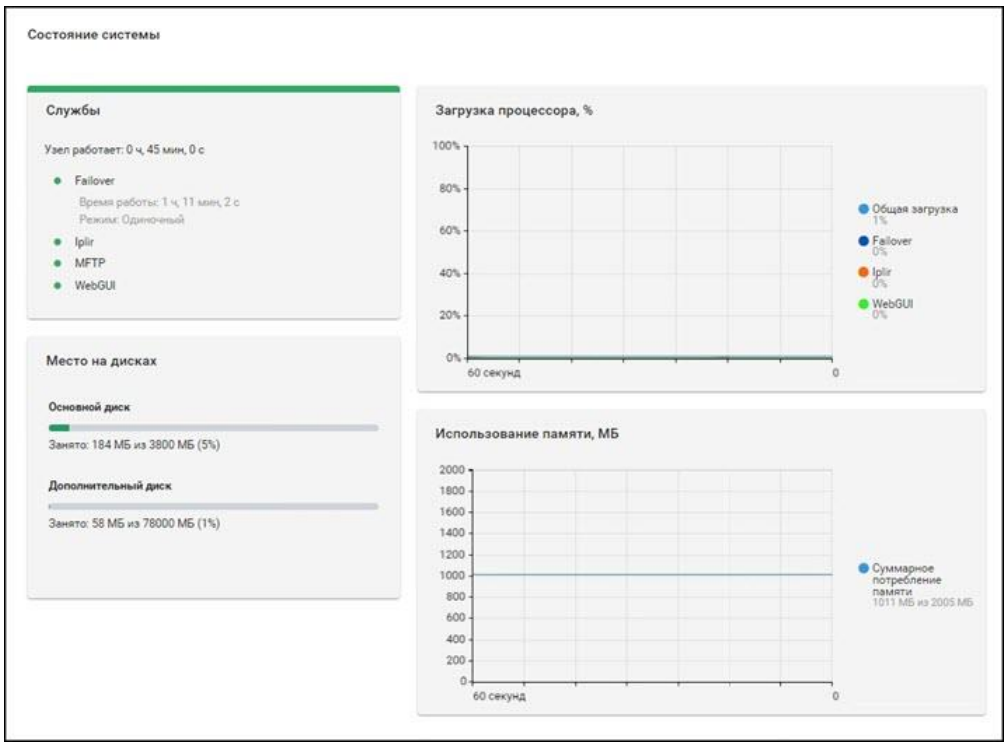

Рисунок 89. Мониторинг состояния ViPNet Coordinator HW

3 События, связанные со службами, входящими в состав ViPNet Coordinator HW, записываются в системный журнал. Этот журнал позволяет проверить работоспособность ПО. Он содержит большое количество деталей о процессах, происходящих внутри служб ViPNet Coordinator HW, и предназначен для разработчиков.

Мониторинг по SNMP

С помощью SNMP-агента, входящего в состав ПО ViPNet Coordinator HW, вы можете удаленно получать информацию о работе ViPNet Coordinator HW, а также настраивать автоматическое оповещение о важных событиях.

Информация, доступная по протоколу SNMP, представлена в виде набора SNMP-параметров. Каждый параметр имеет уникальный идентификатор (OID). Список доступных SNMP-параметров ViPNet Coordinator HW вы можете просмотреть в приложении Базы управляющей информации (MIB) для протокола SNMP. Все SNMP-параметры доступны только для чтения.

Для получения информации о состоянии ViPNet Coordinator HW вы можете использовать любую программу, предназначенную для получения информации по протоколу SNMP (SNMP-менеджер), например:

- ViPNet StateWatcher. Данный программный комплекс собирает информацию о состоянии установленных на узлах компонентов ПО ViPNet, о текущей загруженности аппаратного обеспечения узлов, о состоянии сетевых интерфейсов и о статусе связей между узлами.
- ViPNet NVS. Система мониторинга для сбора информации о состоянии и составе устройств в сети ViPNet. ViPNet NVS — функциональный модуль системы управления ViPNet Prime.
- Утилита snmpwalk (пакет net-snmp).
- Система мониторинга Zabbix.

Сетевой узел, собирающий информацию по протоколу SNMP (с установленным SNMP-менеджером), называется сервером мониторинга.

В качестве сервера мониторинга мы рекомендуем использовать защищенный или туннелируемый узел. Если вы будете использовать открытый узел, добавьте сетевые фильтры, разрешающие локальный SNMP-трафик:

- с IP-адреса сервера мониторинга на ViPNet Coordinator HW на UDP-порт 161;
- с ViPNet Coordinator HW на IP-адрес сервера мониторинга на UDP-порт 162.

Протокол SNMP поддерживает следующие способы получения информации:

- Передача параметров по запросу — сервер мониторинга посылает SNMP-запрос на ViPNet Coordinator HW и получает в ответ значения необходимых параметров.
- Передача оповещений — SNMP-агент ViPNet Coordinator HW автоматически отправляет SNMP-оповещения на сервер мониторинга при наступлении определенного события.

Примечание. Чтобы SNMP-запросы обрабатывались корректно, настройте их отправку на IP-адрес ViPNet Coordinator HW, который доступен с системы мониторинга по кратчайшему маршруту.

Если вы импортируете в сервер мониторинга MIB-файлы, поддерживаемые ViPNet Coordinator HW, вы сможете:

- использовать в SNMP-запросах текстовые обозначения параметров вместо числовых (например, `infVipNetHostName` вместо `.1.3.6.1.4.1.10812.1.1.7`);
- получать текстовые обозначения некоторых числовых параметров в ответах на SNMP-запросы (например, при запросе состояния интерфейса вместо значения `1` или `2` вы получите значение `up` или `down`);
- получать оповещения от ViPNet Coordinator HW в виде текстовых обозначений параметров вместо числовых (например, `infvpnWebStart` вместо `.1.3.6.1.4.1.10812.1.0.10`).

Чтобы скачать MIB-файлы см. Настройка SNMP-агента.

SNMP-агент ViPNet Coordinator HW поддерживает одновременную работу по протоколам SNMPv1, SNMPv2c и SNMPv3.

Для ограничения доступа к SNMP-параметрам используются следующие подходы в разных версиях протокола SNMP:

- В SNMPv1 и SNMPv2c в качестве идентификатора и пароля для доступа к SNMP-параметрам используется параметр community string. ViPNet Coordinator HW ответит на SNMP-запрос, если community string в запросе совпадает с любым из community string, заданных на ViPNet Coordinator HW.

  Для получения SNMP-оповещений сервером мониторинга в настройках его SNMP-менеджера задайте параметр community-trap string. Чтобы сервер мониторинга смог принять адресованные ему оповещения, community-trap string должен быть указан и в настройках отправки оповещений на ViPNet Coordinator HW.
- В SNMPv3 создаются учетные записи пользователей SNMP. ViPNet Coordinator HW ответит на SNMP-запрос, если данные пользователя в запросе совпадают с данными любого из пользователей, заданных на ViPNet Coordinator HW:
  - имя пользователя;
  - пароль пользователя и алгоритм хэширования пароля;
  - способ аутентификации;
  - ключ и алгоритм шифрования (если заданы).

  Для получения SNMP-оповещений сервером мониторинга в настройках его SNMP-менеджера укажите данные одного из пользователей SNMP, заданных на ViPNet Coordinator HW. При использовании оповещений типа TRAP, в настройках SNMP-менеджера дополнительно к учетным данным пользователя укажите параметр `engineID` (OID .1.3.6.1.6.3.10.2.1.1.0).

Настройка SNMP-агента

Чтобы настроить SNMP-агент для мониторинга ViPNet Coordinator HW:

1 Выберите **Системные настройки** > **Общие** > **SNMP**.

На странице отображаются текущие настройки SNMP-агента.

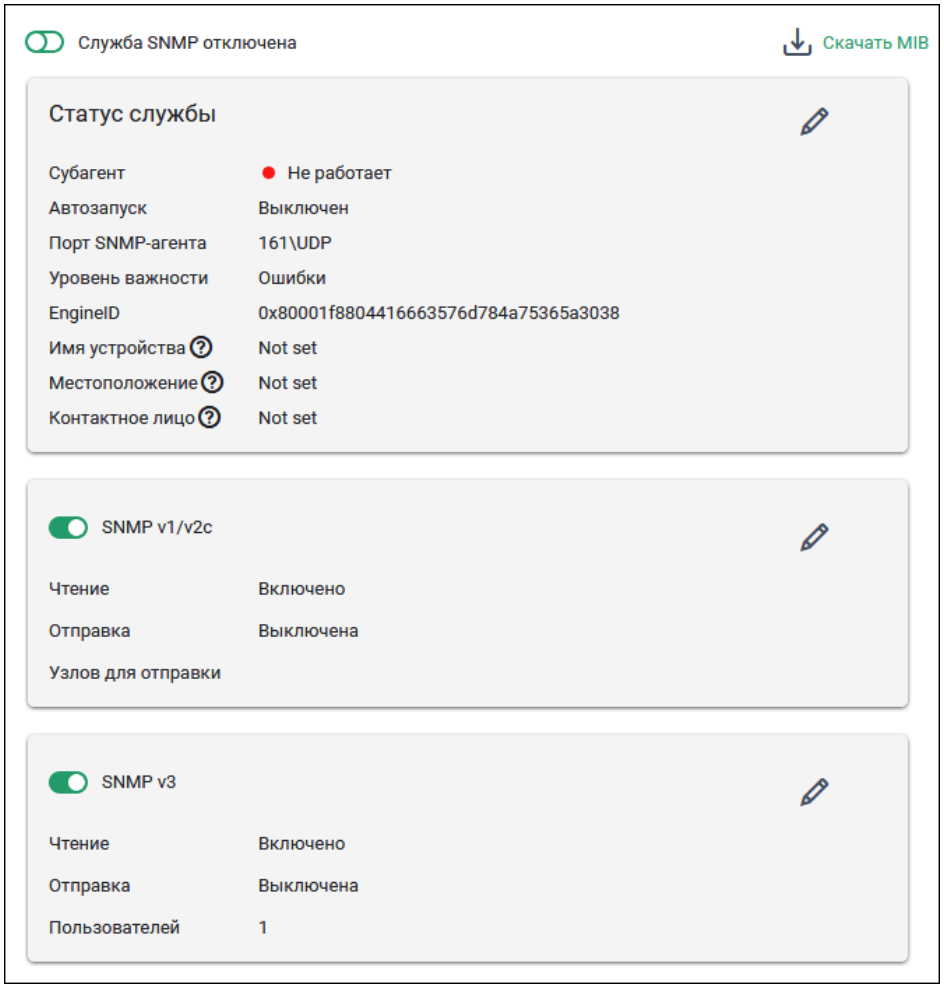

Рисунок 90. Настройка мониторинга по протоколу SNMP

2 Включите службу SNMP-агента.

3 Включите использование протокола **SNMP v1/v2c** и (или) **SNMP v3**.

Примечание. Использование протоколов недоступно, если не заданы Community string (для SNMPv1/v2c) или пользователи (для SNMPv3).

---

4 Чтобы изменить основные параметры SNMP-агента, нажмите в разделе **Статус службы**.

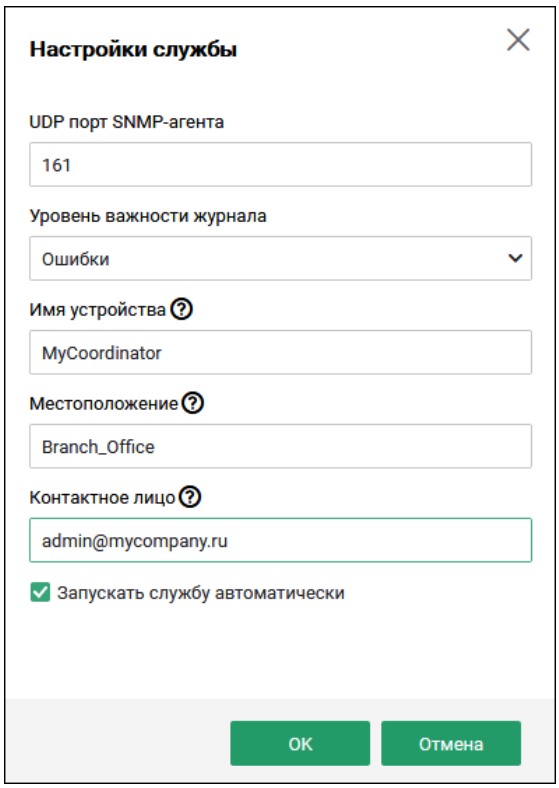

Рисунок 91. Настройка службы SNMP

4.1 Вы можете изменить UDP-порт, на котором SNMP-агент принимает запросы (по умолчанию 161).

4.2 Вы можете изменить уровень важности событий SNMP-агента, которые будут регистрироваться в системном журнале:

- **Критический** — записываются критические ошибки, после которых SNMP-агент не может продолжить работу;
- **Ошибки** — (по умолчанию) записываются ошибки, после которых SNMP-агент может продолжать работу;
- **Информационный** — записывается только информация, касающаяся инициализации SNMP-агента;
- **Отладочный** — записывается служебная информация, используемая при отладке;
- **Выключено** — регистрация событий выключена.

4.3 Задайте информацию о вашем ViPNet Coordinator HW, которая будет доступна по SNMP при чтении SNMP-параметров:

- **Имя устройства** (OID .1.3.6.1.2.1.1.5.0);
- **Местоположение** (OID .1.3.6.1.2.1.1.6.0);
- **Контактное лицо** (OID .1.3.6.1.2.1.1.4.0).

Примечание. При работе ViPNet Coordinator HW в режиме кластера горячего резервирования параметры **Имя устройства** и **Местоположение** не синхронизируются между узлами кластера. Если кластер уже развернут, чтобы изменить их на пассивном узле кластера, подключитесь к нему с помощью консоли и выполните необходимые команды (подробнее см. в документе «Настройка с помощью командного интерпретатора», в разделе «Настройка SNMP-агента»).

4.4 Чтобы SNMP-агент запускался при загрузке ViPNet Coordinator HW, выберите **Запускать службу автоматически**.

5 Для настройки параметров протоколов SNMPv1 и SNMPv2c нажмите в разделе **SNMP v1/v2c**.

5.1 Выберите вкладку **Чтение** для настройки чтения SNMP-параметров.

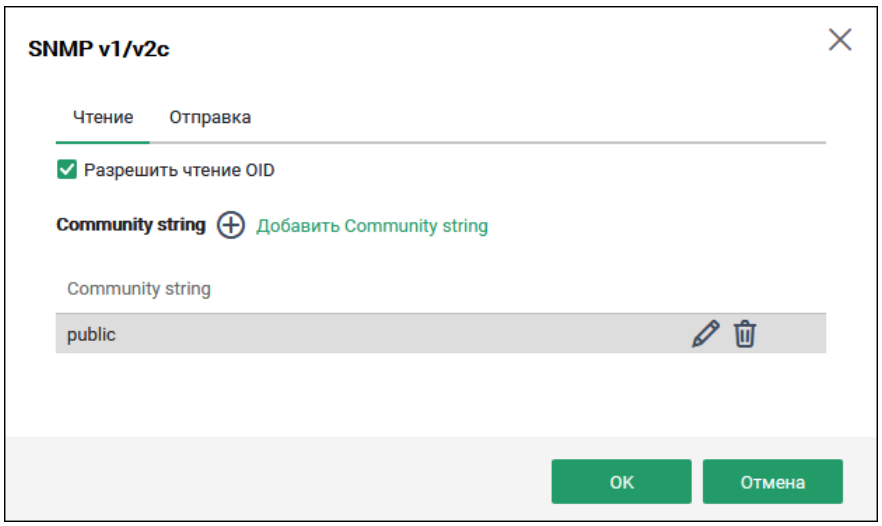

Рисунок 92. Настройка чтения SNMP-параметров

5.2 Чтобы разрешить чтение SNMP-параметров, выберите **Разрешить чтение OID**.

5.3 Выполните одно из действий:

- Чтобы добавить community string (пароль) для чтения SNMP-параметров ViPNet Coordinator HW, нажмите **Добавить**.

  Максимальное количество community string для чтения — 16.

- Чтобы изменить community string, наведите на него курсор и нажмите .
- Чтобы удалить community string, наведите на него курсор и нажмите .

5.4 Выберите вкладку **Отправка** для настройки отправки SNMP-оповещений.

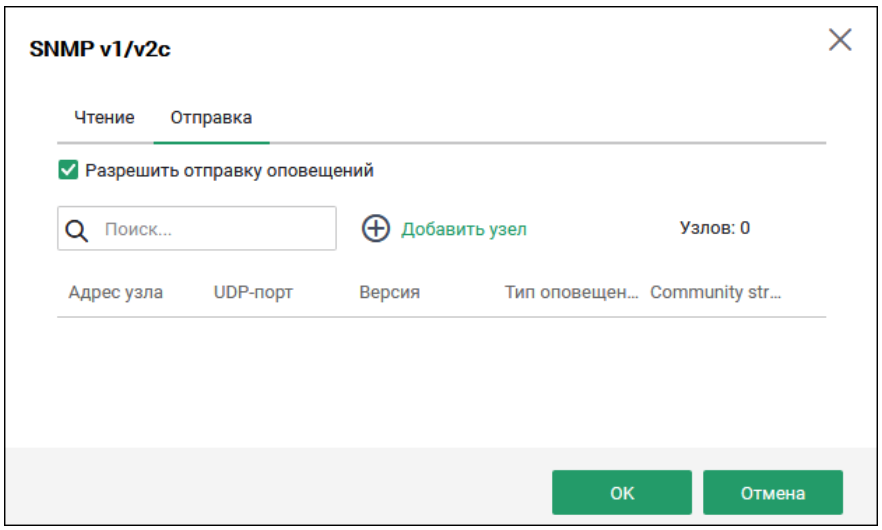

Рисунок 93. Настройка отправки SNMP-оповещений

5.5 Чтобы разрешить отправку SNMP-оповещений, выберите **Разрешить отправку оповещений**.

5.6 Чтобы добавить сетевой узел для отправки SNMP-оповещений, нажмите ⊕ **Добавить узел**.

Максимальное количество сетевых узлов — 16.

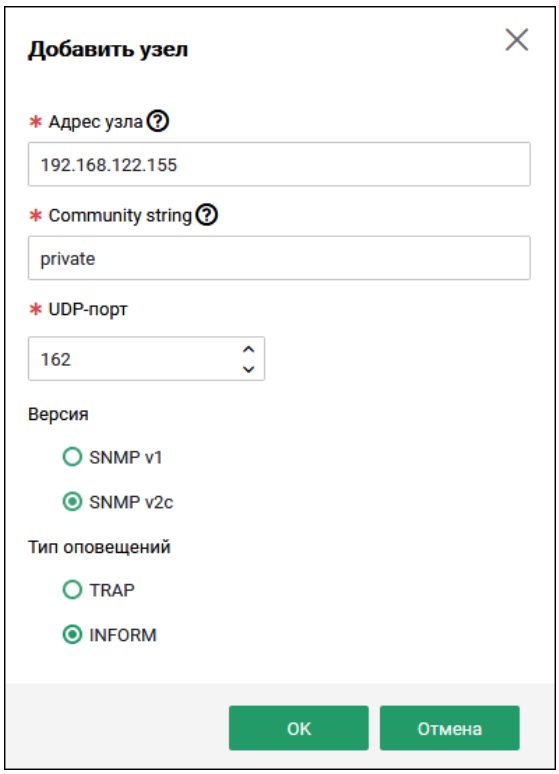

Рисунок 94. Добавление узла для отправки оповещений в SNMP v1 и v2c

5.7 Задайте параметры:

- Адрес сервера мониторинга в поле **Адрес узла**.

- Community string, которое задано на сервере мониторинга (community-trap string).
- Порт, на который будут отправляться SNMP-оповещения (по умолчанию UDP 162).

> **Внимание!** Если задан порт, отличный от UDP 162, добавьте сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт.

- Версию протокола SNMP, по которому будут отправляться SNMP-оповещения.
- Тип SNMP-оповещений.

6 Для настройки параметров протокола SNMPv3 нажмите в разделе **SNMPv3**.

6.1 Чтобы разрешить чтение SNMP-параметров, выберите **Разрешить чтение OID** на вкладке **Разрешения**.

6.2 Чтобы разрешить отправку SNMP-оповещений, выберите **Разрешить отправку оповещений**.

6.3 Перейдите на вкладку **Пользователи** и выполните одно из действий:

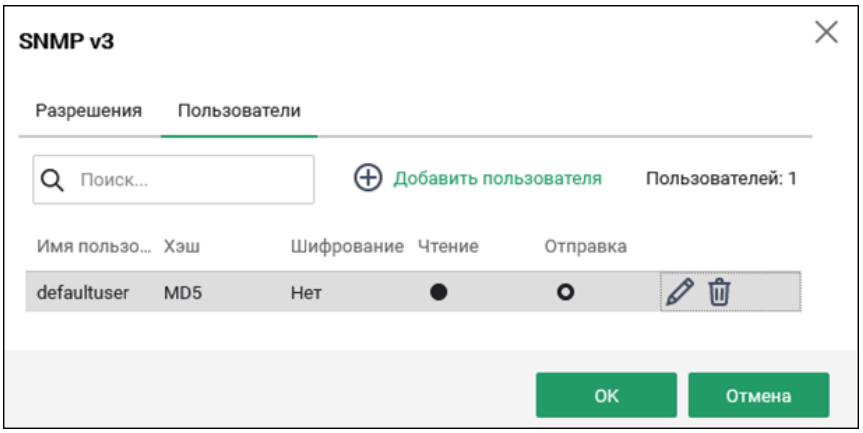

Рисунок 95. Настройка протокола SNMPv3

- Чтобы добавить пользователя для чтения SNMP-параметров ViPNet Coordinator HW, нажмите **Добавить пользователя**.

  Максимальное количество пользователей — 32.
- Чтобы изменить пользователя, наведите на него курсор и нажмите .
- Чтобы удалить пользователя, наведите на него курсор и нажмите .

6.4 В окне **Добавить пользователя** задайте параметры:

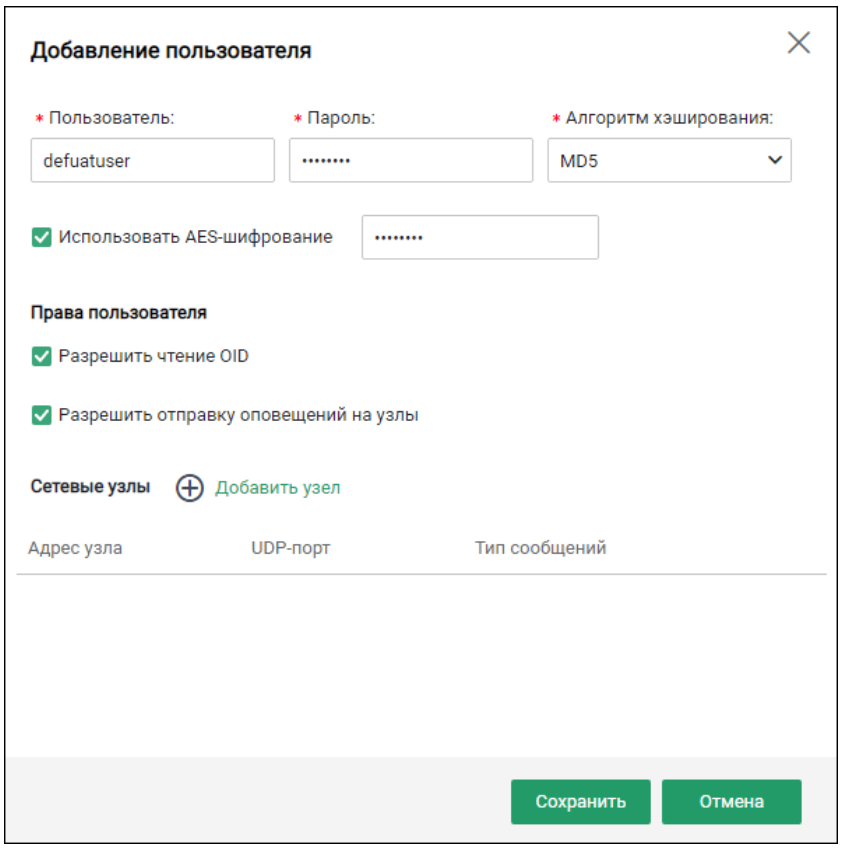

Рисунок 96. Добавление пользователя для чтения SNMP-параметров

- Имя пользователя и пароль.

> **Внимание!** Не используйте повторяющиеся последовательности символов в пароле. Иначе его хэш может совпасть с хэшем другого пароля. Например, пароли `AbcdAbcd` и `AbcdAbcdAbcd` будут иметь одинаковые хэши. Подробнее см. RFC 3414.

- Алгоритм хэширования пароля (по умолчанию MD5).
- Чтобы разрешить чтение SNMP-параметров для пользователя, выберите **Разрешить чтение OID.**
- Чтобы разрешить отправку SNMP-оповещений для пользователя, выберите **Разрешить отправку оповещений**.
- Чтобы шифровать трафик между сервером мониторинга и ViPNet Coordinator HW, выберите **Использовать AES-шифрование** и задайте ключ шифрования.

> **Внимание!** Не используйте повторяющиеся последовательности символов в ключе шифрования. Иначе его хэш может совпасть с хэшем другого ключа. Например, ключи `AbcdAbcd` и `AbcdAbcdAbcd` будут иметь одинаковые хэши. Подробнее см. RFC 3414.

- Чтобы добавить сетевой узел для отправки SNMP-оповещений, нажмите ⊕ **Добавить узел**.

6.5 В окне **Добавить узел** задайте параметры:

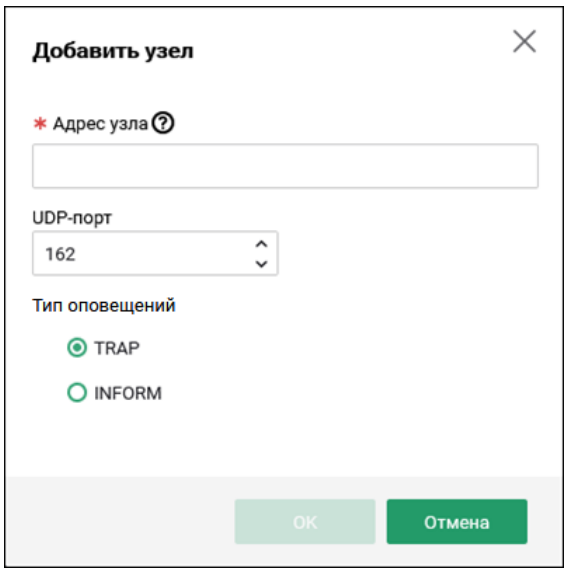

Рисунок 97. Добавление узла для отправки оповещений в SNMP3

- Адрес сервера мониторинга в поле **Адрес узла**.
- Порт, на который будут отправляться оповещения (по умолчанию UDP 162).

> **Внимание!** Если задан порт, отличный от UDP 162, необходимо добавить сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт.

- Тип оповещений.

Чтобы скачать MIB-файлы, поддерживаемые ViPNet Coordinator HW, нажмите **Скачать MIB**.

Мониторинг кластера

Вы можете следить за состоянием обоих узлов кластера по протоколу SNMP. При этом только активный узел кластера принимает SNMP-запросы и отправляет SNMP-оповещения. Для мониторинга пассивного узла кластера активный узел перенаправляет полученные SNMP-запросы на пассивный через интерфейс синхронизации и возвращает ответы отправителю.

Поскольку узлы кластера могут переключаться, SNMP-запрос должен указывать, какой из узлов должен на него ответить. Для этого используются следующие параметры SNMP-агента:

- При использовании SNMPv1 и SNMPv2c для каждого ViPNet Coordinator HW кластера создается community string для режима кластера. SNMP-запрос с таким community string будет адресован конкретному ViPNet Coordinator HW независимо от его текущего режима работы в кластере (активный или пассивный). При переключении системы защиты от сбоев в одиночный режим, community string для режима кластера автоматически удаляется.

- При использовании SNMPv3 каждому узлу кластера назначается свой контекст (строка, идентифицирующая ViPNet Coordinator HW в кластере). Контексты создаются автоматически на активном узле в формате `Node<порядковый номер>`, где `<порядковый номер>` — число от 1, которое выбирается по возрастанию в соответствии с IP-адресом интерфейса синхронизации.

Для мониторинга кластера по протоколу SNMP:

1 Настройте SNMP-агент на активном узле кластера (см. Настройка SNMP-агента).

Настройки будут переданы на пассивный узел при последующей синхронизации.

Примечание. Если на момент развертывания кластера SNMP-агент уже настроен на одном из ViPNet Coordinator HW, запускайте `failover` в режиме кластера сначала на ViPNet Coordinator HW с настроенным SNMP-агентом. Тогда другой узел кластера получит актуальную конфигурацию SNMP-агента от активного узла. Исходная конфигурация агента на пассивном узле при этом удаляется.

---

2 Чтобы настроить чтение SNMP-параметров узлов кластера по протоколам SNMPv1 и SNMPv2c, нажмите  в разделе **SNMPv1/v2c**.

2.1 Выберите вкладку **Community string кластера**.

2.2 Чтобы разрешить чтение SNMP-параметров в кластере, выберите **Мониторинг узлов кластера по протоколам SNMPv1/v2c**.

2.3 Чтобы задать community string для чтения SNMP-параметров узла кластера, наведите курсор на узел кластера и нажмите  .

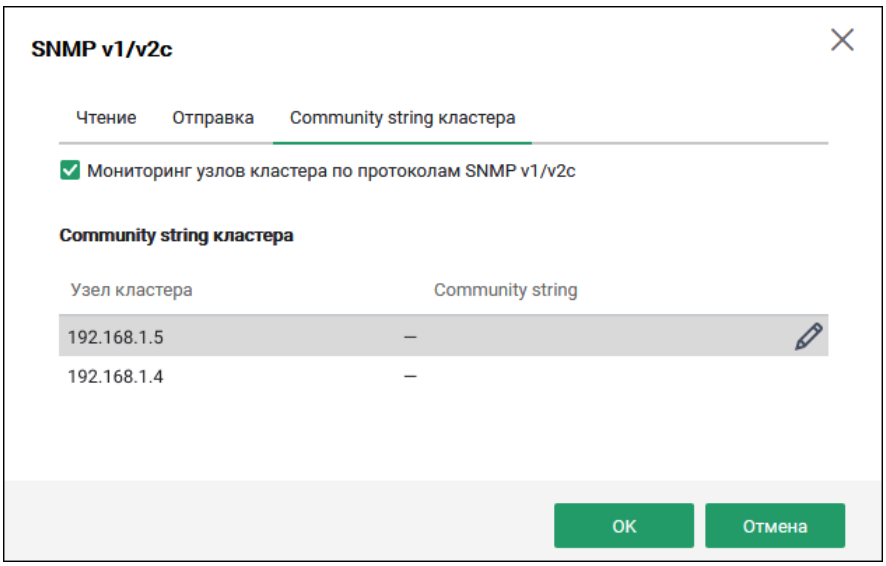

Рисунок 98. Настройка чтения SNMP-параметров в кластере

2.4 Введите community string, отличное от других.

Допустимая длина — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

3 Чтобы просмотреть контексты, присвоенные узлам кластера при использовании протокола SNMPv3, нажмите в разделе **SNMPv3**.

3.1 Выберите вкладку **Контексты кластера**.

3.2 Если требуется изменить контексты узлов кластера, наведите указатель мыши на узел кластера и нажмите . Задайте новый контекст в поле **Контекст узла**.

Допустимая длина — от 1 до 32 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита и цифры.

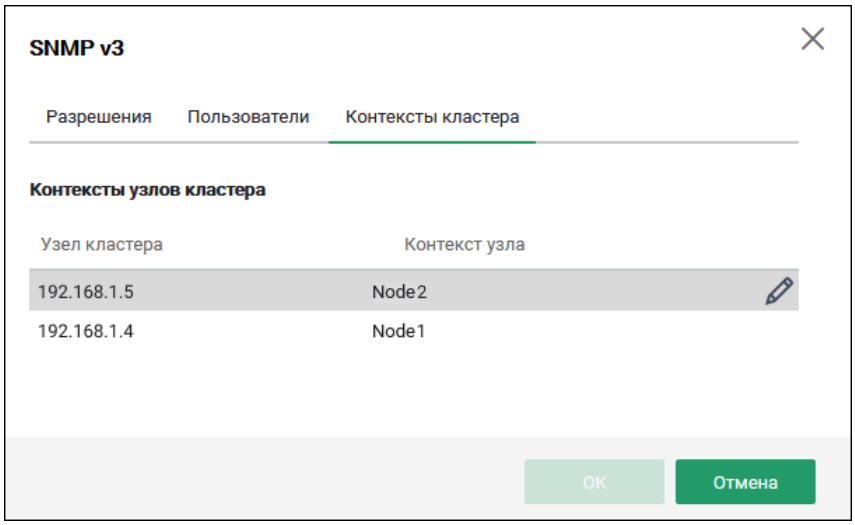

Рисунок 99. Просмотр контекстов для узлов кластера

4 В зависимости от версии протокола SNMP используйте созданные community string или контексты в SNMP-запросах для получения информации о состоянии конкретного узла кластера (см. руководство по настройке используемого SNMP-менеджера):

- При использовании протоколов SNMPv1 и SNMPv2c отправляйте SNMP-запрос с community string соответствующего узла кластера.
- При использовании протокола SNMPv3 отправляйте SNMP-запрос с учетными данными пользователя, созданного при настройке SNMP-агента (см. Настройка SNMP-агента), и контекстом соответствующего узла. Если запрос не содержит контекст, ответ будет получен от активного узла кластера.

Пример настройки системы мониторинга

Рассмотрим пример: необходимо узнать кто из ViPNet-клиентов, работающих в определенный промежуток времени подключался с известного IP-адреса к сети через ViPNet Coordinator HW.

По протоколу SNMP можно получить информацию о подключенных ViPNet-клиентах, для которых координатор является сервером IP-адресов (подробнее см. VIPNET-MIB):

- идентификатор узла;
- имя узла;

- IP-адрес точки доступа к узлу;
- порт точки доступа к узлу.

Используя эти данные настроим систему мониторинга так, чтобы в ней можно было посмотреть историю изменений IP-адреса ViPNet-клиента:

Примечание. Ниже представлен сценарий с особенностями настройки для системы мониторинга Zabbix 6.4. Подробные настройки системы читайте в документах на систему мониторинга.

Перед настройкой системы мониторинга настройте SNMP-агент ViPNet Coordinator HW (см. Настройка SNMP-агента).

---

1 Создайте шаблон для узлов мониторинга с именем ViPNet.

2 Создайте правило обнаружения. Система мониторинга будет автоматически создавать данные о ViPNet-клиентах в виде элементов данных узла мониторинга (координатора).

Заполните обязательные поля следующим образом:

- **Name**: vipnet.client.ip
- **Type**: SNMP agent
- **Key**: vipnet.client.ip
- **SNMP OID**: discovery[{#CLIENTID},1.3.6.1.4.1.10812.1.4.1.1.1, {#CLIENTNAME},1.3.6.1.4.1.10812.1.4.1.1.2]
- **Update interval**: время обнаружения новых клиентов на координаторе (по умолчанию 1m)
- **Keep lost resources period**: время, по истечению которого будут удалены данные пользователей, которые больше не зарегистрированы на координаторе.

Совет. В системе мониторинга идентификатор узла сети ViPNet будет отображаться через пробел: 00 5D 20 21 Client-01. Вы можете настроить отображение без пробелов (005D2021 Client-01):

1 Перейдите на вкладку **Preprocessing**.

2 В поле **Name** выберите **JavaScript**.

3 В поле **Parameters** введите: return (value.replace(/(..)\s(..)\s(..)\s(..)/g, '$1$2$3$4')).

---

3 Создайте прототип элемента данных. Заполните обязательные поля следующим образом:

- **Name**: {#CLIENTID} {#CLIENTNAME}
- **Type**: SNMP agent
- **Key**: vipnet.client.ip[{#CLIENTID}]
- **Type of information**: Text
- **SNMP OID**: 1.3.6.1.4.1.10812.1.4.1.1.3.{#SNMPINDEX}

- **Update interval**: время опроса координатора (по умолчанию 1m)
- **History storage period**: Storage period. Также укажите время хранения данных о ViPNet-клиентах (по умолчанию 90 дней)

4 Создайте прототип триггера для оповещений. Заполните обязательные поля следующим образом:

- **Name**: Client IP address changed
- **Event name**: Client {#CLIENTID} : IP address changed to {ITEM.LASTVALUE1}
- **Severity**: важность триггера
- **Expression**: last(/ViPNet/vipnet.client.ip[{#CLIENTID}], #1)<>last(/ViPNet/vipnet.client.ip[{#CLIENTID}], #2) and length(last(/ViPNet/vipnet.client.ip[{#CLIENTID}]))>0
- **OK event generation**: None
- Установите флажок **Allow manual close**

5 Добавьте координатор в систему мониторинга, используя созданный шаблон. **SNMP Community** должно быть таким же, какое вы устанавливали на координаторе.

6 Создайте экран мониторинга.

7 Создайте виджет, в котором будет отображаться информация о ViPNet-клиентах и их IP-адресах подключения.

8 Создайте виджет, в котором будут отображаться события со сменой IP-адресов ViPNet-клиентов. Для просмотра истории IP-адресов подключения ViPNet-клиента нажмите на IP-адрес клиента в созданном ранее виджете и выберите **Latest values**. Отобразится история изменения IP-адреса ViPNet-клиента с возможностью фильтрации по временному диапазону.

Также вы можете настроить систему мониторинга так, чтобы она отображала историю подключения или отключения ViPNet-клиентов. Для этого в предыдущем сценарии на 4 шаге создайте прототипы триггеров:

- **Name**: {#CLIENTID} {#CLIENTNAME} connected
- **Event name**: {#CLIENTID} {#CLIENTNAME} connected
- **Severity**: важность триггера
- **Expression**: nodata(/ViPNet/vipnet.client.ip[{#CLIENTID}],1m)=0
- **OK event generation**: None
- Установите флажок **Allow manual close**

- **Name**: {#CLIENTID} {#CLIENTNAME} disconnected
- **Event name**: {#CLIENTID} {#CLIENTNAME} disconnected
- **Severity**: Важность триггера
- **Expression**: nodata(/ViPNet/vipnet.client.ip[{#CLIENTID}],1m)=1

- **OK event generation**: None
- Установите флажок **Allow manual close**

История подключения или отключения ViPNet-клиентов будет доступна в разделе Zabbix: **Monitoring -> Problems**. Для удобства просмотра вы можете отфильтровать записи по имени координатора или ViPNet-клиента.

Просмотр журнала регистрации IP-пакетов

В журнал регистрации IP-пакетов заносится информация об IP-пакетах (зашифрованных и открытых), проходящих через сетевые интерфейсы ViPNet Coordinator HW.

В этот журнал вносится информация не о соединениях, а об IP-пакетах, которые проходят через сетевые интерфейсы, поэтому:

- каждый пропущенный и заблокированный локальный IP-пакет отображается в журнале один раз — на том интерфейсе, через который он прошел, или на том интерфейсе, на котором он был заблокирован;
- каждый пропущенный транзитный IP-пакет отображается в журнале дважды: первый раз — на интерфейсе, через который он пришел, второй раз — на интерфейсе, через который он ушел.

По умолчанию в журнале регистрируются только заблокированные IP-пакеты. Вы можете настроить регистрацию всех IP-пакетов:

Внимание! Включение регистрации всех IP-пакетов может снижать производительность ViPNet Coordinator HW.

---

1 Откройте окно настройки журнала одним из способов:
   - Выберите **Системные настройки > Общие > Журналы.**
   - Выберите **Журналы > Журнал IP-пакетов** и нажмите **Настройка журнала.**
2 Включите регистрацию всех пакетов:
   - на всех интерфейсах: нажмите **Установить на всех интерфейсах > Регистрировать все пакеты**.
   - на определенном интерфейсе: в строке с интерфейсом выберите **Регистрировать все пакеты**.

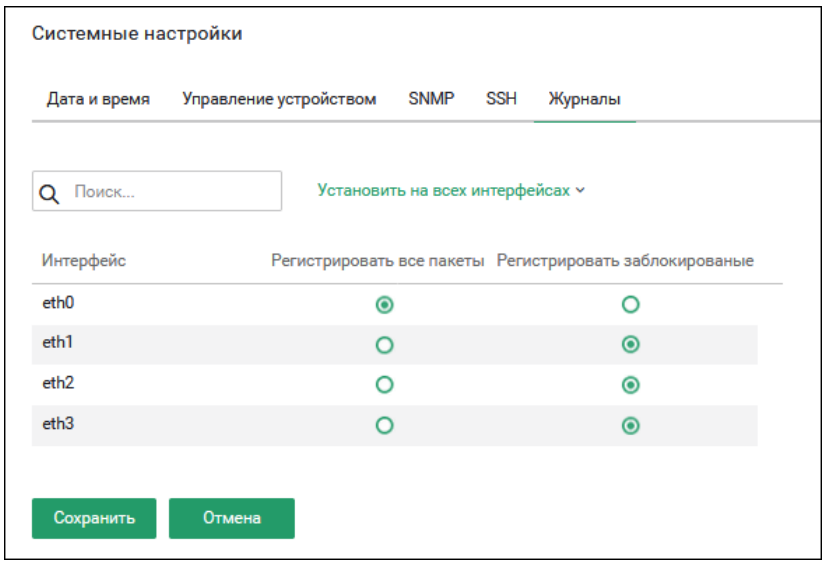

Рисунок 100. Настройка регистрации IP-пакетов

3 Нажмите **Сохранить**.

Чтобы просмотреть журнал регистрации IP-пакетов:

1 Выберите **Журналы** > **Журнал IP-пакетов**.

По умолчанию отобразятся не более 100 записей обо всех IP-пакетах, прошедших через сетевые интерфейсы ViPNet Coordinator HW за последний час.

2 Настройте вид журнала, нажмите и выберите необходимые столбцы.

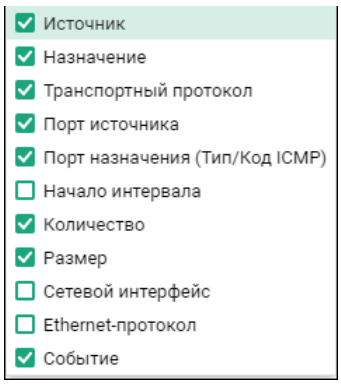

Рисунок 101. Настройка вида таблицы журнала регистрации IP-пакетов

3 Чтобы просмотреть определенные записи, нажмите **Фильтр IP-пакетов** и укажите критерии поиска IP-пакетов:

- В разделе **Признаки IP-пакетов** в соответствующих списках выберите:
  - транспортный протокол, с использованием которого передаются IP-пакеты (TCP, UDP, ICMP или другой);
  - сетевой интерфейс, через который проходят IP-пакеты (eth0, eth1 и так далее);
  - тип трафика, к которому относятся IP-пакеты;
  - тип адреса IP-пакетов (одноадресный, широковещательный или групповой);

- признак трансляции IP-пакетов (транслированные, не транслированные);
- событие межсетевого экрана, к которому относятся IP-пакеты (блокированный, пропущенный или служебный);

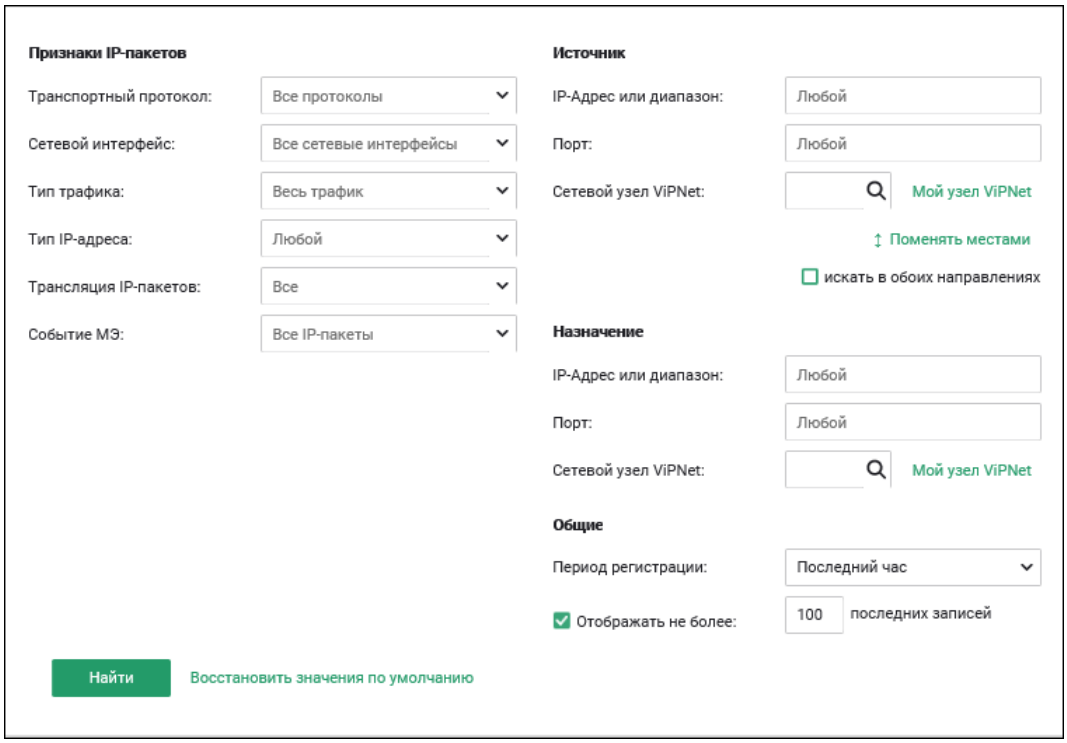

Рисунок 102. Настройка фильтра журнала регистрации IP-пакетов

- В разделе **Источник** (**Назначение**) в соответствующих полях укажите:
  - IP-адрес отправителя (получателя) или диапазон IP-адресов отправителей (получателей);
  - номер порта отправителя (получателя) в диапазоне 1—65535;
  - идентификатор сетевого узла.

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

- Чтобы указать идентификатор сетевого узла, введите его в поле **Сетевой узел** или нажмите . В открывшемся окне выберите нужный узел в списке и нажмите **Выбрать**. 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.

- Чтобы ограничить число записей, установите флажок **Отображать не более** и укажите число записей. Если флажок не установлен, будет отображено не более 1000 записей.

  Для анализа большого количества записей воспользуйтесь внешней аналитической системой. Подробнее см. документ «Настройка с помощью командного интерпретатора» раздел Экспорт журнала регистрации IP-пакетов по сети в формате CEF.

Затем нажмите **Найти**. В результате на главной странице журнала регистрации IP-пакетов отобразится список записей об IP-пакетах, отвечающих заданным критериям поиска.

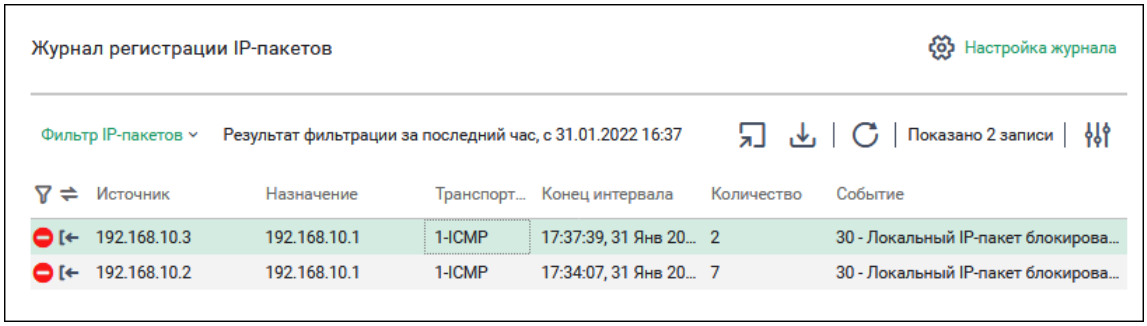

Рисунок 103. Просмотр результатов поиска в журнале IP-пакетов

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 .
- Для просмотра в новой вкладке браузера списка найденных записей нажмите .
- Для обновления списка записей об IP-пакетах на главной странице журнала IP-пакетов нажмите .
- Для изменения критериев поиска IP-пакетов:
  - Нажмите **Фильтр IP-пакетов.**
  - В открывшемся окне установите новые параметры поиска или нажмите **Восстановить значения по умолчанию** для просмотра всех IP-пакетов, прошедших через сетевые интерфейсы ViPNet Coordinator HW за последний час.
  - Нажмите **Найти.**

Просмотр статистики IP-пакетов

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

1 Выберите **Журналы** > **Статистика**. Отобразится информация о количестве открытых, зашифрованных, широковещательных открытых и широковещательных зашифрованных IP-пакетах, прошедших через все сетевые интерфейсы узла.

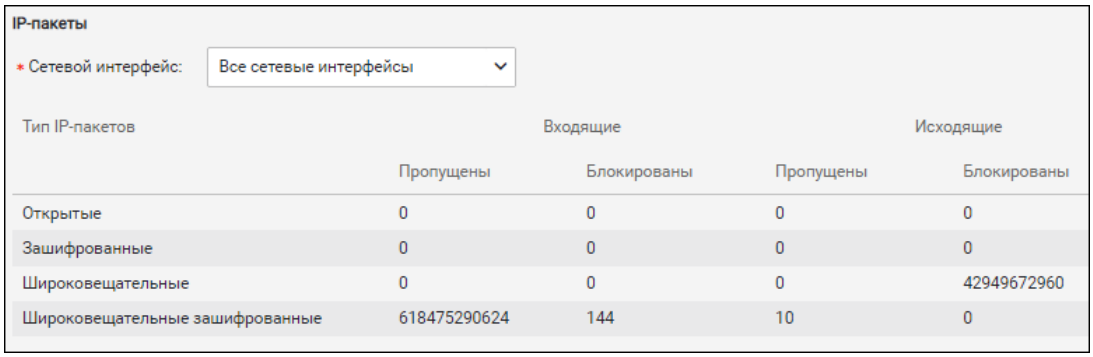

Рисунок 104. Просмотр информации о количестве IP-пакетов, прошедших через все сетевые интерфейсы ViPNet Coordinator HW

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

Просмотр статистики передачи данных

Статистика передачи данных ведется раздельно по всем интерфейсам с момента включения ViPNet Coordinator HW. Статистика учитывает текущую скорость интерфейсов и объем трафика. Данные статистики отображаются в виде графика скорости и диаграммы объема трафика с заданным интервалом обновления (по умолчанию — 3 сек.). Значения скорости отображаются в диапазоне 600 сек. от начала просмотра статистики. При работе ViPNet Coordinator HW в режиме кластера отображается статистика интерфейсов активного узла. После перезагрузки ViPNet Coordinator HW или удаления интерфейса данные статистики сбрасываются. Для ViPNet Coordinator VA статистика может быть сброшена после перезапуска интерфейса.

Чтобы просмотреть статистику передачи данных:

1 Выберите **Журналы** > **Статистика**.

По умолчанию в разделе **Передача данных** отображается статистика интерфейса `eth0`.

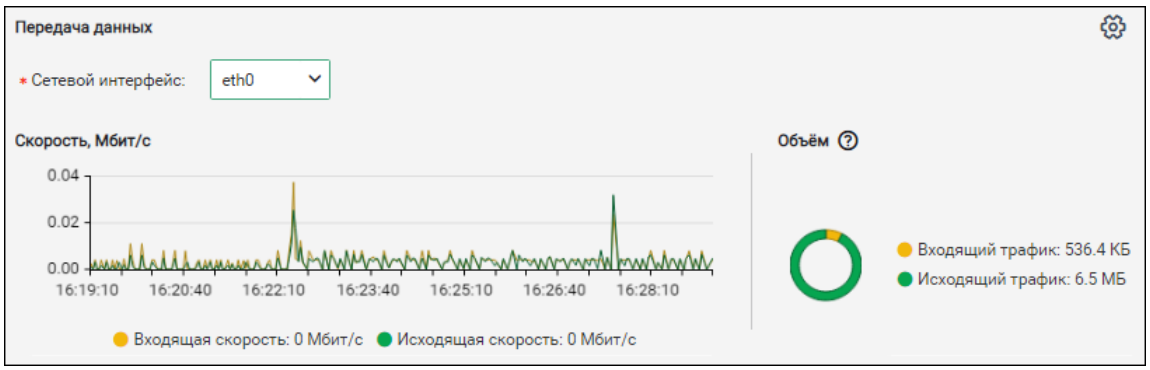

Рисунок 105. Статистика передачи данных сетевого интерфейса eth0

2 Вы можете переключаться между интерфейсами, выбирая нужный из списка **Сетевой интерфейс**.

3 Чтобы изменить интервал обновления статистики, нажмите и выберите нужный из списка.

Просмотр системного журнала

1 Выберите **Журналы** > **Системный журнал**.

По умолчанию заданы параметры для просмотра записей обо всех службах за все время работы ViPNet Coordinator HW.

2 Укажите критерии поиска записей в журнале:

- Для поиска событий, регистрируемых конкретной службой, выберите эту службу и нажмите **Применить фильтр**.
- Для поиска событий по тексту сообщения введите текстовую строку и нажмите **Применить фильтр**. Можно указать оба критерия поиска — службу и текст сообщения.
- Чтобы просмотреть записи журнала с указанного момента времени задайте дату и время в разделе **Перейти ко времени** и нажмите **Перейти**.

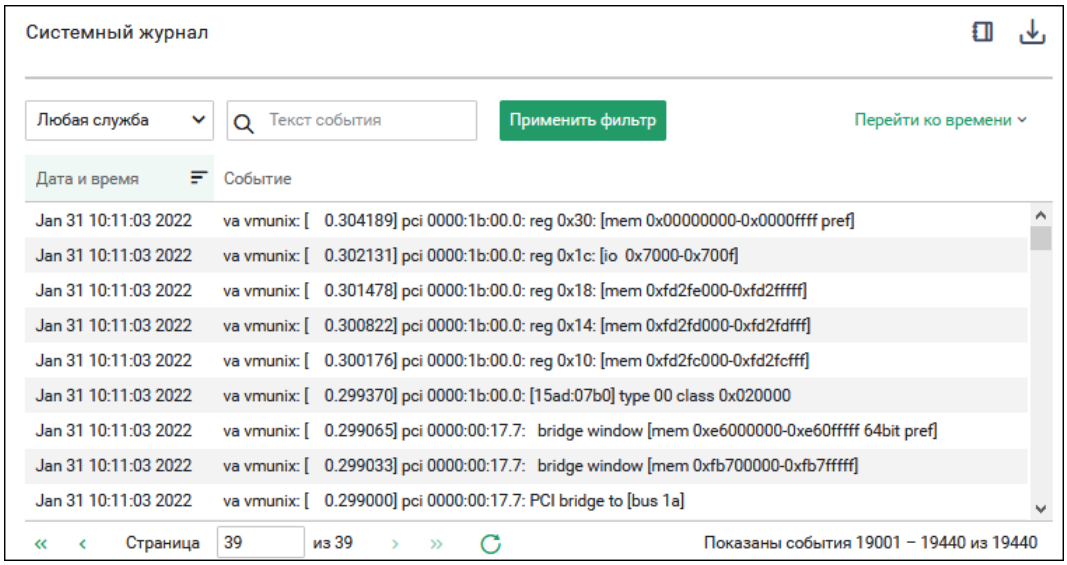

Рисунок 106. Просмотр записей в системном журнале

Системный журнал входит в диагностическую информацию (см. Экспорт диагностической информации).

Экспорт диагностической информации

1 Выберите **Системные настройки** > **Общие** > **Диагностическая информация**.

2 Выберите файлы для формирования архива:

- **Журналы** — чтобы скачать системный журнал, журналы IP-пакетов по каждому интерфейсу и журнал MFTP.
- **Ротированные журналы** — чтобы скачать ротированные файлы системного журнала и журнала MFTP.
- **Файлы конфигурации** — чтобы скачать конфигурационную информацию, например, таблицы маршрутизации, правила фильтрации, правила трансляции и информацию о службах и интерфейсах.

3 Выберите степень сжатия архива.

4 Нажмите **Скачать**.

Файл архива в формате `<имя узла>-logs_DD-MM-YYYYTHH_MM.zip` будет сохранен в папке вашего компьютера.

Примечание. Итоговый размер архива может отличаться от значения, указанного до скачивания.

Просмотр журнала транспортных конвертов (MFTP)

Чтобы просмотреть очередь или журнал транспортных конвертов между узлом ViPNet Coordinator HW и другими узлами сети ViPNet:

1 Выберите **Журналы** > **Журнал MFTP**.

Отобразятся записи обо всех транспортных конвертах между узлом ViPNet Coordinator HW и другими узлами сети ViPNet за все время.

2 Чтобы выбрать записи из журнала для просмотра, раскройте список **Фильтр конвертов** и укажите следующие критерии поиска:

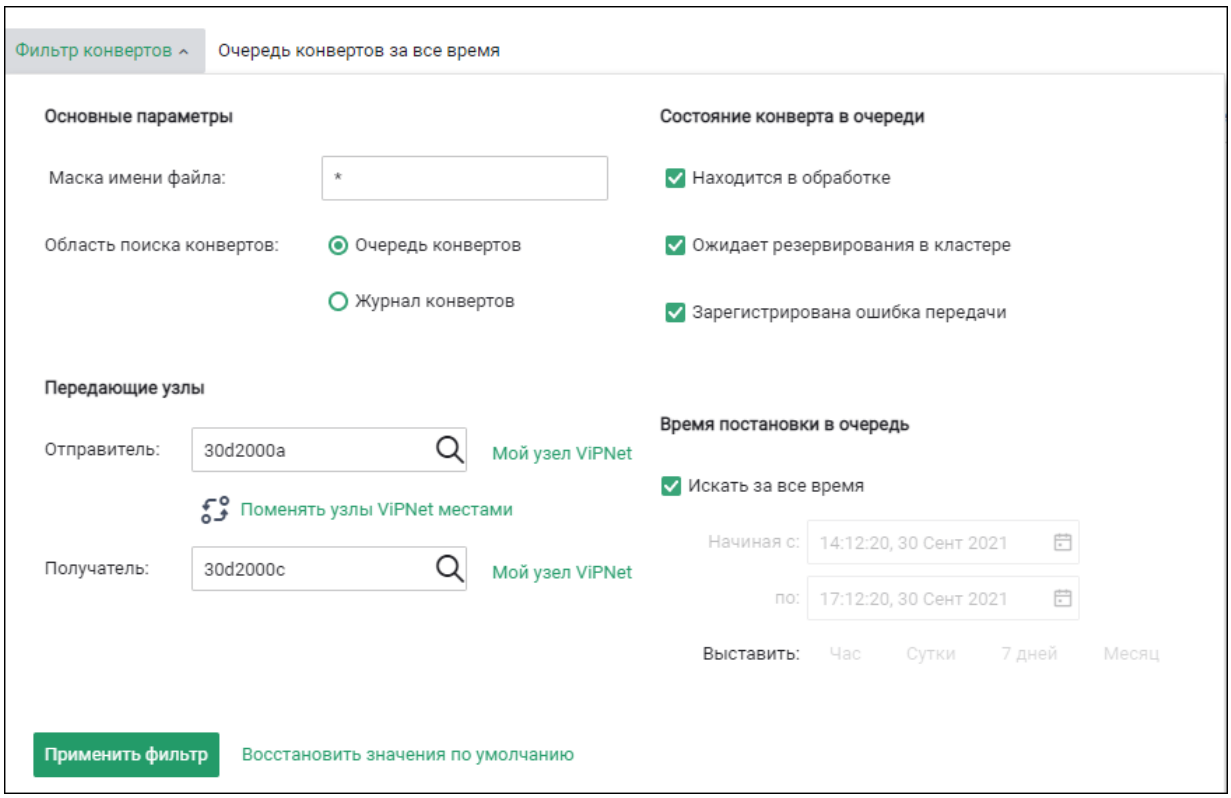

Рисунок 107. Настройка параметров журнала транспортных конвертов

- Настройте **Основные параметры**:
  - область поиска конвертов — очередь конвертов или журнал конвертов;
  - маску имени файла. По умолчанию задана маска «*» для поиска всех файлов.
- В разделе **Передающие узлы** укажите сетевые узлы ViPNet в качестве отправителя и получателя транспортных конвертов.
- Укажите сетевой узел ViPNet Coordinator HW в качестве отправителя, либо в качестве получателя транспортных конвертов.

Совет. В разделе **Передающие узлы**:

- Чтобы указать идентификатор сетевого узла, нажмите , и выберите нужный узел в списке. Чтобы указать собственный сетевой узел, нажмите **Мой узел ViPNet**.
- Вы можете поменять местами сетевые узлы отправителей и получателей.

- В разделе **Состояние конверта в очереди** или **Статус конверта в журнале** (в зависимости от выбранной области поиска конвертов) выберите состояния транспортных конвертов, информацию о которых вы хотите просмотреть.

Таблица 6. Статусы и состояния конвертов

Состояние конверта в очереди/ Статус конверта в журнале	Описание
Находится в обработке	Предназначен для данного узла и обрабатывается
Ожидает резервирования в кластере	Принят на активном узле, ожидается на пассивном
Зарегистрирована ошибка передачи	Нет связи с промежуточным узлом и узлом назначения
Принят	Предназначен данному узлу и принят
Отправлен	Отправлен на следующий узел
Удален	Удален
Поврежден	При чтении возникла ошибка

- В разделе **Время изменения статуса** или **Время постановки в очередь** укажите интервал времени, за который вы хотите просмотреть информацию о транспортных конвертах:

3 Нажмите **Применить фильтр**.

A

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 7. Фильтры защищенной сети (vpn)

Название	Источник	Назначение	Протокол	Действие
В режиме кластера (нередактируемый)				
ViPNet Service	@any	@local	udp: from 2060 to 2060	pass
ViPNet Service	@local	@any	udp: from 2060 to 2060	pass
Сервисный фильтр (нередактируемый)				
Block not original udp port	@local	@any	udp: from 0-2045 to 2046 udp: from 2047-65535 to 2046	drop
Настраиваемые фильтры				
ICMP redirect	@any	@any	ICMP:5	drop
Allow ViPNet base services	@any	@any	udp: from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet base services	@any	@any	udp: to 2046	pass
Allow DHCP Service	@any	@any	udp: from 67 to 68	pass
Allow DHCP Service	@any	@any	udp: from 68 to 67	pass

Название	Источник	Назначение	Протокол	Действие
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Allow ViPNet DBViewer	@any	@any	tcp: to 2047	pass
Allow ViPNet StateWatcher (MFTP info)	@any	@any	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 ICMP Ping	@any	@any	icmp: 8	pass
Allow SSH	@any	@any	tcp: to 22	pass
Allow DNS	@any	@any	udp: to 53, tcp: to 53	pass
Allow NTP	@any	@any	udp: to 123	pass
Allow UPS service (нет в исполнении ViPNet Coordinator VA)	@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) **Примечание**. Данный фильтр имеет самый низкий приоритет и действует для трафика, не попадающего под действие всех остальных фильтров.				
Default VPN rule	@any	@any	@any	drop

Таблица 8. Локальные фильтры открытой сети (`local`)

Название	Источник	Назначение	Протокол	Действие
В режиме кластера (нередактируемые)				
Failover test IP	@local	<список значений параметров `testip` из `failover.ini`>	icmp	pass
Failover Channel	@local	interface <имя интерфейса синхронизации>	@any	pass
Failover Channel	<IP-адрес интерфейса синхронизации второго узла кластера>	interface <имя интерфейса синхронизации>	@any	pass

Название	Источник	Назначение	Протокол	Действие
В пассивном режиме кластера (нередактируемые)				
Failover Channel	@local	iface <значение параметра `device` из `failover.ini`>	@any	pass
Failover Channel	<значение параметра `activeip` второго узла 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
Сервисные фильтры (нередактируемые)				
ViPNet Service Common In	@any	@local	tcp/udp: to 2046, 2047, 10096, 5100, 10092	drop
ViPNet Service Common Out	@local	@any	tcp/udp: from 2046	drop
Настраиваемые фильтры				
ICMP redirect	@any	@any	ICMP:5	drop
Allow DHCP Service	@any	@any	udp: from 67 to 68	pass
Allow DHCP Service	@any	@any	udp: from 68 to 67	pass
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Block ICMP timestamp response	@local	@any	icmp:14	drop
Allow ICMP type 3 code 4	@local	@any	ICMP type 3 code 4	pass
Allow ICMP Ping	@local	@any	icmp: 8	pass
Allow DNS	@local	@any	tcp/udp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Блокирующий фильтр (нередактируемый) **Примечание**. Данный фильтр имеет самый низкий приоритет и действует для трафика, не попадающего под действие всех остальных фильтров.				

Название	Источник	Назначение	Протокол	Действие
Default local rule	@any	@any	@any	drop

Таблица 9. Транзитные фильтры открытой сети (`forward`)

Название	Источник	Назначение	Протокол	Действие
Блокирующий фильтр (нередактируемый) **Примечание**. Данный фильтр имеет самый низкий приоритет и действует для трафика, не попадающего под действие всех остальных фильтров				
Default transit rule.	@any	@any	@any	drop

Таблица 10. Фильтры туннелируемых узлов (`tunnel`)

Название	Источник	Назначение	Протокол	Действие
Общие фильтры				
To all tunnel nodes	@any	@tunneledip	@any	pass
From all tunnel nodes	@tunneledip	@any	@any	pass
Блокирующий фильтр (нередактируемый) **Примечание**. Данный фильтр имеет самый низкий приоритет и действует для трафика, не попадающего под действие всех остальных фильтров				
Default tunnel rule	@any	@any	@any	drop

B

Пользовательские группы протоколов по умолчанию

Таблица 11. Пользовательские группы протоколов 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
Kerberos	TCP:to 88, TCP:to 749, UDP:to 88, UDP:to 749
L2TP	UDP:to 1701
LDAP	TCP:to 389, UDP:to 389

Имя группы протоколов	Состав группы протоколов
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
SMCMonitoring	TCP:to 2047, TCP:to 5100, TCP:to 10092
VPNBase	UDP:to 2046, UDP:from 2048 to 2048, UDP:from 2050 to 2050
Cluster	UDP:from 2060 to 2060
ClusterMonitoring	UDP:from 2060 to 2065, UDP:from 2065 to 2060
VNC	TCP:to 5900
OSPF	IP:89

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 108. Классификация событий в журнале IP-пакетов

Описание типов событий каждой подгруппы приведено в таблицах.

Таблица 12. События подгруппы ***Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные 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
7	Метод шифрования, код которого указан во входящем пакете, не поддерживается
8	IP-пакет поврежден
9	Неизвестный идентификатор сетевого узла
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 или узла, указанного в параметре `proxyid`
19	Подмена узла отправителя
26	Узел с данного координатора недоступен
70	Транзитный IP-пакет заблокирован

Таблица 13. События подгруппы ***Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные фильтрами открытой сети***

Номер события	Описание события
22	От защищенного узла получен открытый пакет
23	От защищенного узла получен открытый широковещательный пакет
24	На порт, используемый одной из служб ViPNet, получен открытый пакет
30	Локальный пакет заблокирован фильтром открытой сети
31	Транзитный пакет заблокирован фильтром открытой сети

Номер события	Описание события
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 14. 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-пакета 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
97	Заблокирован пакет с установленным флагом DF, передача которого без фрагментации невозможна
99	Заблокирован фрагментированный IP-пакет
101	Транзитный IP-пакет не может быть маршрутизирован

Номер события	Описание события
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
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
129	Получен широковещательный пакет с IP-адресом назначения, не принадлежащим подсети интерфейса
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
135	Ошибка обработки модуля ALG
136	Недостаточно памяти для выполнения трансляции адреса (NAT)
139	Отсутствуют лицензии для туннелирования на узле назначения

Таблица 15. 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 16. 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 неизвестной ViPNet сети

Таблица 17. 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

D

Записи системного журнала, связанные с аутентификацией и настройкой оборудования

Ниже приведены протоколируемые события ViPNet Coordinator HW, связанные с аутентификацией и настройкой оборудования, и соответствующие им записи в системном журнале.

Таблица 18. Протоколируемые события операционной системы Linux

Событие	Пример записей в журнале
Запуск операционной системы	`vmunix: [0.000000] Linux version 4.4.163 (vipnet@build-linux) (gcc version 6.3.0 20170516 (Debian 6.3.0-18+deb9u1)) #1 SMP Tue Mar 5 15:14:33 UTC 2019`

Завершение работы операционной системы	`rvpn_shell[2690]: [03-11 12:28:09]< 2690>(24df0740) syslog| <HALT> Command 'machine halt'.`
	`rvpn_shell[2690]: [03-11 12:28:09]< 2690>(24df0740) syslog| The session has been forced to close.`
	`rvpn_shell[2690]: [03-11 12:28:09]< 2690>(24df0740) syslog| Your administrator session has been forced to close, as another administrator session of the command line interface has been started on the terminal tty1`
	`rvpn_shell[2690]: [03-11 12:28:09]< 2690>(24df0740) syslog| with the connection address local console`

Событие	Пример записей в журнале
	rvpn_shell[2690]: [03-11 12:28:09]< 2690>(24df0740) ClUnilogFree| rvpn_shell[2690]: === ended log session at Mon Mar 11 12:28:09 2019 dhcp-relay[3226]: DHCP relays are already STOPPED dhcp-server[3240]: DHCP server is already STOPPED sshd[1701]: Received signal 15; terminating. watchquagga[1289]: Terminating on signal zdhcpd[1284]: Terminating on signal zebra[1280]: client 10 disconnected. 0 dhcp routes removed from the rib zebra[1280]: Terminating on signal zebra[1280]: IRDP: Received shutdown notification. enterpin: Using file based authentication by ViPNet password acpid: exiting syslogd: exiting on signal 15
Сброс ViPNet Coordinator HW к заводским настройкам	factory_reset.sh[554]: Deletion of keys and host links has been started factory_reset.sh[554]: Keys and host links will be deleted in 29 seconds. To cancel, press Ctrl+C ... factory_reset.sh[554]: Keys and host links will be deleted in 29 seconds. To cancel, press Ctrl+C factory_reset.sh[554]: Device has been reset to factory defaults. Press Enter to reboot

Таблица 19. События, протоколируемые при работе пользователя или администратора ViPNet Coordinator HW

Событие	Пример записей в журнале
Завершение работы операционной системы по команде	rvpn_shell[1380]: <HALT> Command 'machine halt'.
Перезагрузка операционной системы по команде	rvpn_shell[3926]: [03-11 12:18:35]< 3926>(85d0e740) syslog| <REBOOT> Command: machine reboot
Выход из командного интерпретатора, работающего в режиме пользователя	login[2675]: pam_unix(login:session): session closed for user user rvpn_shell[3214]: [03-11 17:00:58]< 3214>(48295740) syslog| <EXIT> Command 'exit'
Успешный удаленный запуск командного интерпретатора по протоколу SSH	login[2705]: pam_unix(login:session): session opened for user user by LOGIN(uid=0) Accepted password for user from 192.168.120.2 port 49449 ssh2

Событие	Пример записей в журнале
Не удалось запустить командный интерпретатор при удаленном подключении по протоколу SSH	`sshd[20448]: Failed password for user from 13.0.1.94 port 55650 ssh2`
Завершение удаленного подключения по протоколу SSH	`sshd[20448]: pam_unix(sshd:session): session closed for user user`
Успешный переход в режим администратора	`rvpn_shell[1334]: <ENABLE> Command: enable - Administrator session started.`
Не удалось перейти в режим администратора	`rvpn_shell[2748]: [03-11 12:33:32]< 2748>(2e5b1740) syslog| <ENABLE> Command 'enable'. Failed to log on as an administrator.`
Переход из режима администратора в режим пользователя	`rvpn_shell[2748]: [03-11 12:33:23]< 2748>(2e5b1740) syslog| <EXIT> Command 'exit'`

Вход в системную командную оболочку	`rvpn_shell[2748]: [03-11 18:03:53]< 2748>(2e5b1740) syslog| <I_SHELL> You have exited to the Linux system shell.`
	`rvpn_shell[2748]: [03-11 18:03:53]< 2748>(2e5b1740) syslog| The session has been forced to close.`
	`rvpn_shell[2748]: [03-11 18:03:53]< 2748>(2e5b1740) syslog| Your administrator session has been forced to close, as another administrator session of the command line interface has been started on the terminal tty1`
	`rvpn_shell[2748]: [03-11 18:03:53]< 2748>(2e5b1740) syslog| with the connection address local console`

Выход из системной командной оболочки	Запись о событии не заносится в журнал.
Принудительное завершение сессии командного интерпретатора	`rvpn_shell: <I_CFG> Command: iplir config – starting`
Успешное изменение файла `iplir.conf`	`rvpn_shell: <I_CFG> Command: iplir.conf has been edited successfully`

Не удалось изменить содержимое файла `iplir.conf`	`rvpn_shell: <I_CFG> Command: iplir config – starting`
	`rvpn_shell: <I_CFG> Command: iplir.config: incorrect configuration`
	или
	`rvpn_shell: <I_CFG> Command: iplir config - starting`
	`rvpn_shell: <I_CFG> Command: iplir config Cannot edit config while iplir is running`

Успешная смена пароля пользователя	`rvpn_shell[1949]: <PSW> Command: 'admin password'. The new password has been set successfully.`

Событие	Пример записей в журнале
Не удалось сменить пароль пользователя	rvpn_shell[2748]: [03-11 15:53:57]< 2748>(2e5b1740) syslog| <PSW> Command 'admin password' could not be executed. The old password is incorrect.
Удаление справочников и ключей	rvpn_shell[1664]: <RMKEYS> Command ‘admin keys remove‘
Успешная установка справочников и ключей	root: Keys will be installed from usb root: Partition /dev/sdc1 was successfully mounted on /usb /sbin/unmerge[2552]: [03-11 15:14:17] Keys successfully installed from DST root: Unmerging /tmp/vipnet/abn_0004.dst to /tmp/vipnet/dst
Добавление ключей РНПК	rvpn_shell[2748]: [03-11 16:13:41]< 2748>(2e5b1740) syslog| <ADM_IMP> Command 'add spare keys'..
Изменение способа аутентификации пользователя на «Устройство»	rvpn_shell[1664]: command : admin authentication-type-token rvpn_shell[1664]: The two-factor authentication has been enabled successfully.
Локальное обновление ПО	rvpn_shell[2748]: command: admin upgrade software usb
Удаленное обновление ПО	mftp[7771]: [03-12 10:13:46]< 7771>(4565a740) StartVUpgrade| Unpacking stuff with '//usr/bin/lha -xqfw=/mnt/main/tmp///vnsftWumFZO /opt/vipnet/ccc/driv.lzh'. mftp[7771]: [03-12 10:13:51]< 7771>(4565a740) syslog| run command: /sbin/driv_upgrade.sh. Arguments: vupgrade: Check /mnt/main/opt/vipnet/user/mftpd-config.crg success. vupgrade: Check /mnt/main/etc/failoverd-config.crg success.
Задание IP-адреса для сетевого интерфейса	rvpn_shell[2748]: [03-11 16:23:15]< 2748>(2e5b1740) syslog| <IFCONF> Command inet ifconfig eth2 address 10.0.0.1 netmask 255.255.255.0 Old ifconfig value: ether 00:0c:29:95:92:ba txqueuelen 1000 (Ethernet)
Сброс настроек сетевого интерфейса	rvpn_shell[2748]: command: inet ifconfig eth2 reset
Включение сетевого интерфейса	rvpn_shell[2748]: [03-11 16:23:39]< 2748>(2e5b1740) syslog| <IFCONF> The command 'inet ifconfig eth2 up' executed.
Выключение сетевого интерфейса	rvpn_shell[2748]: [03-11 16:23:42]< 2748>(2e5b1740) syslog| <IFCONF> The command 'inet ifconfig eth2 down' executed.

Событие	Пример записей в журнале
Установка параметров скорости сетевого интерфейса	`rvpn_shell[1949]: <IFCONF_SPD> Command: inet ifconfig eth2 speed 10 duplex full autoneg on`
Добавление статического маршрута	`rvpn_shell[6176]: [08-02 14:22:53.443245]< 6176> (00007f26392cf7c0) syslog | <RT_ADD> Command: inet route add 123.45.67.89 netmask 255.255.255.0 gateway 123.45.67.1 distance 255 weight 255 table name routes table number 1024. Static route has been added successfully`
Удаление статического маршрута	`rvpn_shell[6167]: The following route was deleted: Table 1024 (ROUTES), Destination Netmask Next hop Distance Weight, ----------- ------- -------- -------- ------, 123.45.67.0 255.255.255.0 123.45.67.1 255 255`
Создание виртуального интерфейса VLAN	`rvpn_shell[2748]: [03-11 16:36:34]< 2748>(2e5b1740) syslog| <I_VLAN_ADD> Command: 'inet ifconfig eth2 vlan add 2'. The new vlan interface eth2.2 has been created.`
Удаление виртуального интерфейса VLAN	`rvpn_shell[2748]: [03-11 16:37:05]< 2748>(2e5b1740) syslog| <I_VLAN_DELETE> Command: 'inet ifconfig eth2 vlan delete 2'. The vlan interface eth2.2 has been deleted.`
Сохранение копии конфигурации VPN	`[03-11 16:38:20]< 2748>(2e5b1740) syslog| <CFG_LD> Command: admin config save test_conf.`
Загрузка копии конфигурации VPN	`rvpn_shell[1949]: <CFG_LD> Command: admin config load test_conf.`
Экспорт журнала регистрации IP-пакетов на USB-носитель	`rvpn_shell[2748]: [03-11 16:40:04]< 2748>(2e5b1740) syslog| <ADM_EXP> Command: 'admin export packetdb usb'.`
Экспорт файлов системного журнала	`rvpn_shell[2748]: [03-11 16:49:26]< 2748>(2e5b1740) syslog| <ADM_EXP> Command: admin export logs usb.`
Экспорт конфигурационной информации	`rvpn_shell[2748]: [03-11 16:49:26]< 2748>(2e5b1740) syslog| <ADM_EXP> Command: admin export dignostics usb.`
Экспорт справочников, ключей и настроек	`rvpn_shell[1949]: <ADM_EXP> Command: ‘admin export keys binary-encrypted’`

Событие	Пример записей в журнале

Изменение сетевых фильтров и правил трансляции адресов	Отображение изменения:
	`iplircfg[12145]:[03-11 17:48:05]<12145>(a0ff9700) syslog| User rules dataname has been changed.`
	`iplircfg[12145]:[03-11 17:48:05]<12145>(a0ff9700) syslog| <Rules>`
	`iplircfg[12145]:[03-11 17:48:05]<12145>(a0ff9700) syslog| + <Rule IsActive="true" xsi:type="vn:LocalRule">`
	`iplircfg[12145]:[03-11 17:48:05]<12145>(a0ff9700) syslog| + <RuleId>100001</RuleId>`
	`iplircfg[12145]:[03-11 17:48:05]<12145>(a0ff9700) syslog| </Rule>`

Включение вывода сообщений о событиях	`rvpn_shell[1949]: <DBG_ON> Command 'debug on'`
Выключение вывода сообщений о событиях	`rvpn_shell[1949]: <DBG_ON> Command 'debug off'`

Таблица 20. События, связанные с запуском или остановкой служб ViPNet Coordinator HW

Событие	Пример записей в журнале
Загрузка драйверов и запуск служб ViPNet Coordinator HW	`rvpn_shell[2748]: [03-11 16:44:37]< 2748>(2e5b1740) syslog| <ADM_VSTART> Command: 'vpn start'.`
Выгрузка драйверов и завершение работы служб ViPNet Coordinator HW	`rvpn_shell[2748]: [03-11 16:44:45]< 2748>(2e5b1740) syslog| <ADM_VSTOP> Command 'vpn stop'.`
Запуск службы `failoverd`, отвечающую за работу системы защиты от сбоев	`rvpn_shell[2748]: [03-11 16:45:28]< 2748>(2e5b1740) syslog| <F_STR> Command: failover start`
Завершение работы службы `failoverd`, отвечающую за работу системы защиты от сбоев	`rvpn_shell[2748]: [03-11 16:37:31]< 2748>(2e5b1740) syslog| <F_STP> Command: failover stop`
Запуск управляющей службы `iplircfg`	`rvpn_shell[2748]: <I_STR> Command: iplir start : command: iplir start` `rvpn_shell: <I_CFG> Command: iplir config - starting`
Завершение работы управляющей службы `iplircfg`	`rvpn_shell[2748]: <I_STP> Command: iplir stop : command: iplir stop`
Запуск транспортного сервера MFTP	`rvpn_shell[2748]: [03-11 16:38:04]< 2748>(2e5b1740) syslog| <M_STR> Command: mftp start` `mftp[3989]: [03-11 15:16:41]< 3989>(62cad740) syslog| Init MFTP manager ... OK.`

Событие	Пример записей в журнале
Завершение работы транспортного сервера MFTP	`rvpn_shell[2748]: [03-11 16:37:47]< 2748>(2e5b1740) syslog| <M_STP> Command: mftp stop` `mftp[2267]: [03-11 16:37:46]< 2267>(d7e13740) syslog| Exiting MFTP manager.`
Перезапуск веб-сервера ViPNet Coordinator HW	`rvpn_shell[2748]: [03-11 16:48:01]< 2748>(2e5b1740) syslog| <WUI_RST> Command: webui restart`

Таблица 21. События, связанные с работой системы защиты от сбоев

Событие	Пример записей в журнале
Смена режима работы узла кластера из пассивного в активный	`failoverd[5261]: [03-12 17:02:08]< 5261>(155c9740) syslog| switching to active mode`

Перезагрузка узла кластера из-за сбоя на сетевом интерфейсе	`failoverd[2341]: [03-12 17:11:54]< 2341>(2509b740) active_failed| failure detected on interface eth2`
	`failoverd[2341]: [03-12 17:11:54]< 2341>(2509b740) syslog| one or more subsystems failed, rebooting`
	`failoverd[2341]: [03-12 17:11:54]< 2341>(2509b740) syslog| Rebooted due to network error on eth2 at 03-12 17:11:54`

Перезагрузка узла кластера из-за конфликта режимов	`failoverd[2341]: [03-12 17:11:54]< 2341>(2509b740) syslog| Rebooted due to network error on eth2 at 03-12 17:11:54`
Перезагрузка узла кластера из-за обнаружения службой `failoverd` ошибки другого контролируемого сервиса	`failoverd[1411]: [02-01 21:12:54] CheckApp: [mentor.cpp]: Reached maximum count of application restarts [iplircfg] pid 0` `failoverd[1411]: Rebooted due to watcher detected error at 03-12 17:11:54`

Таблица 22. События, связанные с обменом служебной информацией между узлами ViPNet

Событие	Пример записей в журнале
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при включении узла, а затем периодически)	`iplircfg[8281]: [03-12 10:03:35]< 8281>(23aae740) ProcessMonChannel| got message: type 1 from ID 0x31DB000A (msg name '@4$2)F3S.01B')`
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при первом обращении к серверу IP-адресов сети ViPNet)	`iplircfg[2763]: [03-12 10:29:44]< 2763>(534c4740) ProcessMonChannel| got message: type 3 from ID 0x31DB000A (msg name '@!VQ`7ZS.01B')`

Событие	Пример записей в журнале
Первое обращение к серверу соединений, если сервер не является также сервером IP-адресов сети ViPNet	`iplircfg[13787]: [11-16 16:40:39] ProcessMonChannel: [src/ipserver.cpp]: got message: type 23 from ID 1C2000A (msg name '773PYNG3.2HH')`
Отключение узла ViPNet от сервера IP-адресов сети ViPNet	`iplircfg[13787]: [11-16 16:40:44] ProcessMonChannel: [src/ipserver.cpp]: got message: type 2 from ID 1C2000A (msg name '85FTKIK3.IAY')`
Проверка соединения с узлом ViPNet (запрос)	`iplircfg[8281]: [03-12 10:03:34]< 8281>(23aae740) ProcessMonChannel| got message: type 5 from ID 0x31DB000C (msg name '@')2)F3S.01B')`
Подтверждение получения сообщения (кроме уведомлений об изменении адреса доступа удаленного узла ViPNet)	`iplircfg[8281]: [03-12 10:03:34]< 8281>(23aae740) ProcessMonChannel| got message: type 7 from ID 0x31DB000A (msg name '0RUX6QK1.PJD')`
Уведомление об изменении адреса доступа удаленного узла ViPNet	`iplircfg[2763]: [03-12 10:29:43]< 2763>(534c4740) ProcessDrvChannelResolve| got message: type 50 from ID 0x31DB000A (msg name '@2VQ`7ZS.01B')`
Подтверждение получения уведомления об изменении адреса доступа удаленного узла ViPNet	`iplircfg[2763]: [03-12 10:16:09]< 2763>(534c4740) ProcessDrvChannelResolve| got message: type 70 from ID 0x31DB000A (msg name 'D09HKJAU.UYN')`

Изменение параметров адреса доступа удаленного узла ViPNet	`iplircfg[10937]: [12-07 15:33:50] CConfig.SubstNatSettings: subst proxy 01C3000A natsettings for changed ID 01C30B4D: firewallIp 79.133.171.237, port 55777`
	`iplircfg[10937]: [12-07 15:33:46] CConfig::SubstNatSettingsByProxy: subst changed proxy 01D60032 natsettings for ID 01D6004D: firewallIp 10.54.100.10, port 55777`
	`iplircfg[10937]: [12-07 15:35:26] CConfig.SetIpsForId: load natsettings for 5C1A37: firewallip = 88.151.200.50, forwardip = 88.151.200.50, port = 55777, timeout = 0, virtualip = 0, proxyid = 5C05CF, DRV_ALWAYS_USE_SERVER = yes DRV_GREEN_NODE = yes DRV_STOP_FIREWALL_IP=no`

Таблица 23. События, связанные с ошибками датчика случайных чисел (ДСЧ) и шифратора

Событие	Пример записей в журнале

Проверка при запуске и регламентная проверка ДСЧ в службах `iplircfg` и `mftpd`	`iplircfg[2736]: NewRngInitializer failure: NewRandInit has failed: 100`
	`iplircfg[2736]: Failed to initialize CSP`
	`iplircfg[2736]: Please, restart application manually.`

Событие	Пример записей в журнале

Проверка при запуске и регламентная проверка шифраторов в службах `iplircfg` и `mftpd`	`iplircfg[2370]: InitCSP has failed`
	`iplircfg[2370]: Failed to initialize CSP`
	`iplircfg[2370]: Please, restart application manually.`

Периодическая проверка ДСЧ в службах	`mftpd[1950]: [04-25 17:15:12] CPGenRandom: CPGenRandom unsuccessful, length 8, ErrorCode -2146893795`
	`mftpd[1950]: [04-25 17:15:12] EncryptData: FD 15: Can't encrypt data for alien ID 28750011: 'CCryptoApi::Encrypt()'`
	`mftpd[1950]: [04-25 17:15:12] FormINF8Data: FD 15: Can't encrypt data`
	`mftpd[1950]: [04-25 17:15:12] Init: FD 15: Can't form INF8 data`
	`mftpd[1950]: [04-25 17:15:12] SendERRCommand: FD 15 -> "ERR"`
	`mftpd[1950]: [04-25 17:15:12] ProcessMftpConnection: Can't init MFTP connection. Sock 15.`
	`mftpd[1950]: [04-25 17:15:12] CMftpConnection.Close: Close connection. Sock 15.`

Периодическая проверка шифраторов в службах	`mftpd[1950]: [04-25 17:15:12] EncryptData: FD 15: Can't encrypt data for alien ID 28750011: 'CCryptoApi::Encrypt()'`
	`mftpd[1950]: [04-25 17:15:12] FormINF8Data: FD 15: Can't encrypt data`
	`mftpd[1950]: [04-25 17:15:12] Init: FD 15: Can't form INF8 data`
	`mftpd[1950]: [04-25 17:15:12] SendERRCommand: FD 15 -> "ERR"`
	`mftpd[1950]: [04-25 17:15:12] ProcessMftpConnection: Can't init MFTP connection. Sock 15.`
	`mftpd[1950]: [04-25 17:15:12] CMftpConnection.Close: Close connection. Sock 15.`

Проверка при запуске и регламентная проверка ДСЧ в криптодрайвере	`vmunix: [ 34.573918] itcscrpt: Run CSP test.` `vmunix: [ 34.573920] itcscrpt: Driver selftest: TestLinealRecurrentGenerator failed`

Проверка при запуске и регламентная проверка шифраторов в криптодрайвере	`vmunix: [ 34.206950] itcscrpt: Run CSP test.`
	`vmunix: [ 34.206957] itcscrpt: Driver selftest: TestLowStreamImit failed`
	`vmunix: [ 34.206957] itcscrpt: Driver selftest: TestLowCloseStreamImit failed`
	`vmunix: [ 34.206958] itcscrpt: Driver selftest: TestLowStreamEnCryptCFB failed`
	`vmunix: [ 34.206959] itcscrpt: Driver selftest: TestLowStreamDeCryptCFB failed`

Событие	Пример записей в журнале

Периодическая проверка ДСЧ в криптодрайвере	`vmunix: [ 652.427598] itcscrpt: Driver selftest: TestLowStreamImit failed`
	`vmunix: [ 652.427600] itcscrpt: Driver selftest: TestLowCloseStreamImit failed`
	`vmunix: [ 652.427601] itcscrpt: Driver selftest: TestLowStreamEnCryptCFB failed`
	`vmunix: [ 652.427602] itcscrpt: Driver selftest: TestLowStreamDeCryptCFB failed`
	`vmunix: [ 652.427606] itcscrpt: Driver selftest: There are tests with failures.`

Примечание. Записи об успешной работе ДСЧ или шифратора не протоколируются.

Таблица 24. События, связанные с антивирусной проверкой и контролем содержимого трафика прокси-сервера

Событие	Пример записей в журнале
Сработало запрещающее правило контроля содержимого трафика по HTTP-методу	`0 192.168.56.121 TCP_DENIED/403 4293 GET http://www.address.com/ - NONE - text/html`
Сработало запрещающее правило контроля содержимого трафика по MIME-типу	`657 192.168.56.121 TCP_DENIED_REPLY/403 3974 GET http://www.address.com/file.zip - FIRST_UP_PARENT/10.0.25.3 text/html`
Антивирус заблокировал скачивание зараженного файла	`Sep 19 20:49:01 Coord-164a0013 icap[6069]: RESPMOD 127.0.0.1 - 192.168.15.233 http://www.rexswain.com/eicar.zip INFECTED EICAR-Test-File`

E

Базы управляющей информации (MIB) для протокола SNMP

MIB-II System

MIB-II System (.1.3.6.1.2.1.1) включает в себя объекты, предназначенные для получения информации о системных параметрах сетевого узла (например, имя узла, ОС, количество и параметры сетевых интерфейсов, статистика по SNMP-сообщениям). Подробнее см. в RFC 1213.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator HW могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать имена интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 25. SNMP-параметры. MIB-II System

OID	Описание
.1.3.6.1.2.1.1.1.0	Информация о сетевом узле (имя, назначенное сетевому узлу, исполнение и версия ViPNet Coordinator HW).
.1.3.6.1.2.1.1.2.0	OID SNMP-агента.
.1.3.6.1.2.1.1.3.0	Время работы SNMP-агента с последнего запуска (sysUpTime).

OID	Описание
.1.3.6.1.2.1.1.4.0	Контактная информация администратора. Задается командой `inet snmp system contact`. Если информация не задана, параметр отсутствует.
.1.3.6.1.2.1.1.5.0	Имя, назначенное сетевому узлу. Задается командой `inet snmp system name`. Если имя не задано, параметр равен `hostname`.
.1.3.6.1.2.1.1.6.0	Место расположения сетевого узла. Задается командой `inet snmp system location`. Если не задано, параметр отсутствует.
.1.3.6.1.2.1.1.7.0	Число, означающее наличие сетевых служб на определенных уровнях модели OSI. Для каждого уровня, для которого на узле есть службы, число 2 возводится в степень (L-1) и добавляется к общей сумме. Пример для координатора: 2^(4-1)+2^(7-1)=72 – узел работает на транспортном и прикладном уровне.
.1.3.6.1.2.1.1.8.0	Значение sysUpTime с момента последнего изменения состояния или значения столбца .1.3.6.1.2.1.1.9.1.2.A из таблицы .1.3.6.1.2.1.1.9.1.
Таблица поддерживаемых MIB (.1.3.6.1.2.1.1.9.1):	
A — индекс таблицы	
.1.3.6.1.2.1.1.9.1.1.A	Индекс таблицы.
.1.3.6.1.2.1.1.9.1.2.A	OID для MIB, с которыми работает SNMP-агент.
.1.3.6.1.2.1.1.9.1.3.A	Текстовое описание MIB.
.1.3.6.1.2.1.1.9.1.4.A	Время с момента подключения MIB.
ARP-таблица (.1.3.6.1.2.1.3.1.1):	
B — индекс интерфейса, присвоенный сетевым узлом	
E — IP-адрес сетевого узла	
.1.3.6.1.2.1.3.1.1.1.B.1.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.3.1.1.2.B.1.E	MAC-адрес.
.1.3.6.1.2.1.3.1.1.3.B.1.E	IP-адрес, соответствующий MAC-адресу.
Таблица описания маршрутов (.1.3.6.1.2.1.4.21.1):	
E — IP-адрес сетевого узла или сети	
.1.3.6.1.2.1.4.21.1.1.E	IP-адрес назначения маршрутов (маршрут по умолчанию 0.0.0.0).
.1.3.6.1.2.1.4.21.1.2.E	Индекс интерфейса (1.3.6.1.2.1.2.2.1.1), через который будет производится маршрутизация.
.1.3.6.1.2.1.4.21.1.3.E	Основная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.4.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).

OID	Описание
.1.3.6.1.2.1.4.21.1.5.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.6.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.7.E	IP-адрес следующего маршрутизатора по маршруту (Next Hop).
.1.3.6.1.2.1.4.21.1.8.E	Тип маршрута: • 1 (other) — другое, не может быть причислено к другим категориям, • 2 (invalid) — некорректный, • 3 (direct) — маршрут к подключенной сети, • 4 (indirect) — маршрут к удаленной сети.
.1.3.6.1.2.1.4.21.1.9.E	Механизм маршрутизации, через который был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP.
.1.3.6.1.2.1.4.21.1.10.E	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.21.1.11.E	Маска маршрута.
.1.3.6.1.2.1.4.21.1.12.E	Дополнительная метрика протокола маршрутизации.
.1.3.6.1.2.1.4.21.1.13.E	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.11.1.0	Количество полученных сообщений SNMP.
.1.3.6.1.2.1.11.2.0	Количество отправленных сообщений SNMP.
.1.3.6.1.2.1.11.3.0	Количество полученных сообщений SNMP неподдерживаемой версии.

OID	Описание
.1.3.6.1.2.1.11.4.0	Количество полученных сообщений SNMP, адресованных неизвестному сообществу.
.1.3.6.1.2.1.11.5.0	Количество полученных сообщений SNMP, содержащих операцию, не разрешенную на сетевом узле для сообщества.
.1.3.6.1.2.1.11.6.0	Количество ошибок ASN.1 или BER при разборе SNMP-сообщений.
.1.3.6.1.2.1.11.8.0	Количество входящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.9.0	Количество входящих SNMP PDU, для которых значение поля error-status – «noSuchName».
1.3.6.1.2.1.11.10.0	Количество входящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.11.0	Количество входящих SNMP PDU, для которых значение поля error-status – «readOnly».
.1.3.6.1.2.1.11.12.0	Количество входящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.13.0	Количество успешно полученных MIB объектов с использованием Get-Request и Get-Next.
.1.3.6.1.2.1.11.14.0	Количество успешно записанных MIB объектов с использованием Set-Request.
.1.3.6.1.2.1.11.15.0	Количество успешно обработанных SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.16.0	Количество успешно обработанных SNMP Get-Next PDUs.
.1.3.6.1.2.1.11.17.0	Количество успешно обработанных SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.18.0	Количество успешно обработанных SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.19.0	Количество успешно обработанных SNMP Trap PDUs.
.1.3.6.1.2.1.11.20.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.21.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «noSuchName».
.1.3.6.1.2.1.11.22.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.24.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.25.0	Количество успешно сгенерированных исходящих SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.26.0	Количество успешно сгенерированных исходящих SNMP Get-Next PDUs.

OID	Описание
.1.3.6.1.2.1.11.27.0	Количество успешно сгенерированных исходящих SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.28.0	Количество успешно сгенерированных исходящих SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.29.0	Количество успешно сгенерированных исходящих SNMP Trap PDUs.
.1.3.6.1.2.1.11.30.0	Возможность отправки authenticationFailure traps: • 1 — разрешено, • 2 — запрещено.
.1.3.6.1.2.1.11.31.0	Количество параметров отброшенных SNMP без уведомлений в связи с несоответствием параметров агента и сервера.
.1.3.6.1.2.1.11.32.0	Количество параметров отброшенных SNMP без уведомлений в связи с проблемами proxy.

IF-MIB

IF-MIB (.1.3.6.1.2.1.2) включает в себя объекты, предназначенные для получения информации о параметрах сетевых интерфейсов сетевого узла (например, тип сетевого интерфейса, физический адрес, пропускная способность). Подробнее см. в RFC 2863.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator HW могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP вместо индексов используйте названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 26. SNMP-параметры. IF-MIB

OID	Описание
.1.3.6.1.2.1.2.1.0	Количество сетевых интерфейсов (физических, виртуальных, включая loopback).
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.2.1.2.2.1):	
A — индекс интерфейса	
.1.3.6.1.2.1.2.2.1.1.A	Индекс сетевого интерфейса (A).
.1.3.6.1.2.1.2.2.1.2.A	Описание интерфейса (производитель, название и версия оборудования или ПО).

OID	Описание
.1.3.6.1.2.1.2.2.1.3.A	Тип сетевого интерфейса: • 6 — ethernet, • 24 — localhost. Остальные значения можно посмотреть здесь.
.1.3.6.1.2.1.2.2.1.4.A	MTU (в байтах).
.1.3.6.1.2.1.2.2.1.5.A	Максимальная пропускная способность (бит/сек).
.1.3.6.1.2.1.2.2.1.6.A	MAC-адрес.
.1.3.6.1.2.1.2.2.1.7.A	Назначенное состояние интерфейса: • 1 (up) — включен, • 2 (down) — выключен, • 3 (testing) — состояние тестирования, указывает, что никакие рабочие пакеты не могут быть переданы.
.1.3.6.1.2.1.2.2.1.8.A	Текущее рабочее состояние интерфейса: • 1 (up) — включен, • 2 (down) — выключен, • 3 (testing) — состояние тестирования. Никакие рабочие пакеты не могут быть переданы, • 4 (unknown) — неизвестно, • 5 (dormant) — интерфейс ожидает внешних действий (таких как последовательная линия, ожидающая входящее соединение), • 6 (notPresent) — в интерфейсе отсутствуют компоненты (обычно аппаратные), • 7 (lowerLayerDown) — не работает из-за состояния интерфейса нижнего уровня.
.1.3.6.1.2.1.2.2.1.9.A	Время работы SNMP-агента с начала его запуска (sysUpTime) до момента перехода интерфейса в его текущее состояние.
.1.3.6.1.2.1.2.2.1.10.A	Количество полученных байт (октетов).
.1.3.6.1.2.1.2.2.1.11.A	Количество полученных одноадресных (unicast) пакетов.
.1.3.6.1.2.1.2.2.1.12.A	Количество полученных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.13.A	Количество отклоненных пакетов.
.1.3.6.1.2.1.2.2.1.14.A	Количество пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.15.A	Количество пакетов, которые были отклонены из-за неизвестного или не поддерживаемого протокола.
.1.3.6.1.2.1.2.2.1.16.A	Количество отправленных байт (октетов).
.1.3.6.1.2.1.2.2.1.17.A	Количество отправленных одноадресных (unicast) пакетов.

OID	Описание
.1.3.6.1.2.1.2.2.1.18.A	Количество отправленных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.19.A	Количество отклоненных отправленных пакетов.
.1.3.6.1.2.1.2.2.1.20.A	Количество отправленных пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.21.A	Количество исходящих пакетов в очереди на отправку.

Таблица статистики дополнительных параметров сетевых интерфейсов (.1.3.6.1.2.1.31.1.1.1):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1

.1.3.6.1.2.1.31.1.1.1.1.A	Имя интерфейса.
.1.3.6.1.2.1.31.1.1.1.2.A	Количество входящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.3.A	Количество входящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.4.A	Количество исходящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.5.A	Количество исходящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.6.A	Количество байт (октетов), принятых интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.7.A	Количество входящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.8.A	Количество входящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.9.A	Количество входящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.10.A	Количество байт (октетов), отправленных интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.11.A	Количество исходящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.12.A	Количество исходящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.13.A	Количество исходящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.14.A	Необходимость отправки trap на события linkUp/linkDown: • 1 — отправлять trap, • 2 — не отправлять trap.
.1.3.6.1.2.1.31.1.1.1.15.A	Максимальная скорость интерфейса (Мегабит/сек).
.1.3.6.1.2.1.31.1.1.1.16.A	Режим работы интерфейса: • 1 (true) — принимает все пакеты, • 2 (false) — принимает только пакеты, адресованные сетевому узлу.

OID	Описание
.1.3.6.1.2.1.31.1.1.1.17.A	Наличие физического коннектора у интерфейса: • 1 (true) — есть коннектор (для ethernet), • 2 (false) — нет коннектора (для localhost).
.1.3.6.1.2.1.31.1.1.1.18.A	Имя интерфейса, заданное администратором. Для координатора всегда равно 0.
.1.3.6.1.2.1.31.1.1.1.19.A	Время работы SNMP-агента с последнего запуска (sysUpTime) до появления разрыва в подсчете счетчиков на интерфейсе.
.1.3.6.1.2.1.31.1.5.0	Время работы SNMP-агента с последнего запуска (sysUpTime) до последнего добавления или удаления записи в таблице статистики дополнительных параметров сетевых интерфейсов.

IP-MIB

IP-MIB (.1.3.6.1.2.1.4) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу IP (например, параметры сетевых интерфейсов, статистика для IP-трафика, таблица IP-адресов). Подробнее см. в RFC 4293.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 27. SNMP-параметры. IP-MIB

OID	Описание
.1.3.6.1.2.1.4.1.0	Указывает, является ли сетевой узел маршрутизатором: • 1 — является (координатор всегда работает в данном режиме), • 2 — не является.
.1.3.6.1.2.1.4.2.0	TTL по умолчанию для IP-пакетов.
.1.3.6.1.2.1.4.3.0	Общее количество IP-пакетов, принятых сетевым узлом, включая пакеты с ошибками.
.1.3.6.1.2.1.4.4.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в заголовке пакета.
.1.3.6.1.2.1.4.5.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в адресе.
.1.3.6.1.2.1.4.6.0	Количество IP-пакетов, переданных на следующий шлюз.
.1.3.6.1.2.1.4.7.0	Количество IP-пакетов, отклонённых по причине неизвестного или неподдерживаемого протокола.
1.3.6.1.2.1.4.8.0	Количество отклоненных пакетов по причине недостатка буфера.
.1.3.6.1.2.1.4.9.0	Количество успешно доставленных IP-пакетов.

OID	Описание
.1.3.6.1.2.1.4.10.0	Количество IP-пакетов, отправленных сетевым узлом (не включая .1.3.6.1.2.1.4.6.0).
.1.3.6.1.2.1.4.11.0	Количество IP-пакетов, отклонённых по причине недостатка буфера.
.1.3.6.1.2.1.4.12.0	Количество IP-пакетов, отклоненных к дальнейшей передаче по причине отсутствия маршрута.
.1.3.6.1.2.1.4.13.0	Максимальное количество секунд ожидания сборки фрагментов.
.1.3.6.1.2.1.4.14.0	Количество принятых IP-фрагментов.
.1.3.6.1.2.1.4.15.0	Количество успешных сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.16.0	Количество ошибок сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.17.0	Количество успешно фрагментированных исходящих IP-пакетов.
.1.3.6.1.2.1.4.18.0	Количество ошибок при фрагментации исходящих IP-пакетов.
.1.3.6.1.2.1.4.19.0	Количество фрагментов IP-пакетов, сгенерированных данным сетевым узлом.

Таблица IP-адресов сетевого узла для протокола IPv4 (.1.3.6.1.2.1.4.20.1.):

E — IP-адрес

.1.3.6.1.2.1.4.20.1.1.E	IP-адрес.
.1.3.6.1.2.1.4.20.1.2.E	Указатель на интерфейс, которому присвоен этот IP-адрес (A - из таблицы .1.3.6.1.2.1.2.2.1).
.1.3.6.1.2.1.4.20.1.3.E	Маска сети.
.1.3.6.1.2.1.4.20.1.4.E	Значение наименее значимого бита в широковещательном (broadcast) IP-адресе.

Таблица разрешения IP-адресов в физические адреса (ARP-таблица) (.1.3.6.1.2.1.4.22.1.):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

E — IP-адрес

.1.3.6.1.2.1.4.22.1.1.A.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.4.22.1.2.A.E	MAC-адрес.
.1.3.6.1.2.1.4.22.1.3.A.E	IP-адрес.
.1.3.6.1.2.1.4.22.1.4.A.E	Тип маппинга: • 1 — другое, • 2 — некорректный, • 3 — динамический, • 4 — статический.
.1.3.6.1.2.1.4.23.0	Количество отклоненных маршрутов.

OID	Описание
.1.3.6.1.2.1.4.31.1.1.	Таблица, содержащая статистику (счетчики) IP-трафика различных версий на сетевом узле для всех интерфейсов.
.1.3.6.1.2.1.4.31.2.0	Значение sysUpTime в момент добавления/удаления столбцов в таблицу .1.3.6.1.2.1.4.31.1.1.

Таблица префиксов IP-адресов (.1.3.6.1.2.1.4.32.1.):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

B — тип адреса:

- **значение 0 — неизвестно,**
- **значение 1 — ipv4,**
- **значение 2 — ipv6,**
- **значение 3 — ipv4z,**
- **значение 4 — ipv6z,**
- **значение 16 — dns.**

C — префикс (адрес сети)

D — длина префикса

.1.3.6.1.2.1.4.32.1.5.A.B.C.D	Источник префикса: • 1 — другое, • 2 — вручную, • 3 — общеизвестный префикс, • 4 — dhcp, • 3 — routeradv (значение получено от роутера).
.1.3.6.1.2.1.4.32.1.6.A.B.C.D	Указывает, может ли префикс использоваться как маршрут: • 1 — может, • 2 — не может.
.1.3.6.1.2.1.4.32.1.7.A.B.C.D	Указывает, может ли префикс использоваться для автоматической конфигурации адреса: • 1 — может, • 2 — не может.
.1.3.6.1.2.1.4.32.1.8.A.B.C.D	Время (в секундах), в течение которого префикс будет оставаться предпочтительным. Значение 4294967295 означает бесконечность.
.1.3.6.1.2.1.4.32.1.9.A.B.C.D	Время (в секундах), в течение которого префикс будет существовать. Значение 4294967295 означает бесконечность.

OID	Описание
Таблица адресной информации по интерфейсам (.1.3.6.1.2.1.4.34.1):	
B — тип адреса: • **значение 0 — неизвестно,** • **значение 1 — ipv4,** • **значение 2 — ipv6,** • **значение 3 — ipv4z,** • **значение 4 — ipv6z,** • **значение 16 — dns.** **E — IP-адрес**	
.1.3.6.1.2.1.4.34.1.3.B.E	Индекс сетевого интерфейса.
.1.3.6.1.2.1.4.34.1.4.B.E	Тип адреса: • 1 (unicast) — одноадресный, • 2 (anycast) — к ближайшему узлу, • 3 (broadcast) — широковещательный.
.1.3.6.1.2.1.4.34.1.5.B.E	Ссылка на строку таблицы префиксов.
.1.3.6.1.2.1.4.34.1.6.B.E	Происхождение адреса: • 1 (other) — другое, • 2 (manual) — назначен вручную, • 4 (dhcp) — назначен по dhcp, • 5 (linklayer) — назначен механизмом автоконфигурации протокола IPv6 (SLAAC), • 6 (random) — назначен случайным образом.
.1.3.6.1.2.1.4.34.1.7.B.E	Статус адреса: • 1 (preferred) — предпочтительный, • 2 (deprecated) — устарел, • 3 (invalid) — недействителен, • 4 (inaccessible) — недоступен, • 5 (unknown)— неизвестен, • 6 (tentative) — предварительный, • 7 (duplicate) — дублированный, • 8 (optimistic) — оптимистичный.
.1.3.6.1.2.1.4.34.1.8.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента создания записи.
.1.3.6.1.2.1.4.34.1.9.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента изменения записи.

OID	Описание
.1.3.6.1.2.1.4.34.1.10.B.E	Статус строки: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.2.1.4.34.1.11.B.E	Механизм хранения строки: • 1 (other) — другое, • 2 (volatile) — изменяемая, • 3 (nonvolatile) — энергонезависимая, • 4 (permanent) — постоянная, • 5 (readOnly) — только для чтения.

Таблица трансляции MAC IP (.1.3.6.1.2.1.4.35.1):

A — индекс интерфейса из таблицы .1.3.6.1.2.1.2.2.1.1 MIB-II

B — тип адреса:

- **0 — неизвестно,**
- **1 — ipv4,**
- **2 — ipv6,**
- **3 — ipv4z,**
- **4 — ipv6z,**
- **16 — dns.**

E — IP-адрес

.1.3.6.1.2.1.4.35.1.4.A.B.E	Транслируемый MAC-адрес.
.1.3.6.1.2.1.4.35.1.5.A.B.E	Время работы SNMP-агента с момента последнего запуска (sysUpTime) до момента изменения MAC-адреса.
.1.3.6.1.2.1.4.35.1.6.A.B.E	Тип маппинга: • 1 (other) — другое, • 2 (invalid) — недопустимое значение, • 3 (dynamic) — динамическое, • 4 (static) — статическое, • 5 (local) — предоставляется для собственного адреса интерфейса объекта.

OID	Описание
.1.3.6.1.2.1.4.35.1.7.A.B.E	Статус маппинга: • 1(reachable) — подтвержден, • 2 (stale) — не подтвержден, • 3 (delay) — ожидание, • 4 (probeprobe) — активное, • 5 (invalid) — недействителен, • 6 (unknown) — не определен, • 7 (incomplete) — выполняется разрешение адреса.
.1.3.6.1.2.1.4.35.1.8.A.B.E	Статус строки: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.2.1.5.1.0	Общее число ICMP-запросов, полученных сетевым узлом.
.1.3.6.1.2.1.5.2.0	Число ICMP-запросов с ошибкой, полученных сетевым узлом.
.1.3.6.1.2.1.5.3.0	Количество сообщений о недоступности заданного сетевого узла, полученных данным сетевым узлом.
.1.3.6.1.2.1.5.4.0	Количество сообщений об истечении времени ожидания ответа, полученных сетевым узлом.
.1.3.6.1.2.1.5.5.0	Количество полученных сообщений ICMP Parameter Problem.
.1.3.6.1.2.1.5.6.0	Количество полученных сообщений ICMP Source Quench.
.1.3.6.1.2.1.5.7.0	Количество полученных сообщений ICMP Redirect messages.
.1.3.6.1.2.1.5.8.0	Количество полученных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.9.0	Количество полученных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.10.0	Количество полученных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.11.0	Количество полученных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.12.0	Количество полученных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.13.0	Количество полученных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.14.0	Количество ICMP сообщений, отправленных сетевым узлом.
.1.3.6.1.2.1.5.15.0	Количество ICMP сообщений, которые сетевой узел не смог отправить из-за проблем с ICMP.
.1.3.6.1.2.1.5.16.0	Количество отправленных сообщений ICMP Destination Unreachable.

OID	Описание
.1.3.6.1.2.1.5.17.0	Количество отправленных сообщений ICMP Time Exceeded.
.1.3.6.1.2.1.5.18.0	Количество отправленных сообщений ICMP Parameter Problem.
1.3.6.1.2.1.5.19.0	Количество отправленных сообщений ICMP Source Quench.
1.3.6.1.2.1.5.20.0	Количество отправленных сообщений ICMP Redirect.
1.3.6.1.2.1.5.21.0	Количество отправленных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.22.0	Количество отправленных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.23.0	Количество отправленных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.24.0	Количество отправленных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.25.0	Количество отправленных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.26.0	Количество отправленных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.29.1	Таблица счетчиков ICMP сообщений с указанием версии протокола IP.
.1.3.6.1.2.1.5.30.1	Таблица счетчиков входящих-исходящих ICMP пакетов с указанием версии протокола IP.

IP-FORWARD-MIB

IP-FORWARD-MIB (.1.3.6.1.2.1.4.24) включает в себя объекты, предназначенные для получения информации о параметрах маршрутизации сетевого узла. Подробнее см. в RFC 4292.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 28. SNMP-параметры. IP-FORWARD-MIB

OID	Описание
Таблица маршрутизации сетевого узла (.1.3.6.1.2.1.4.24.4.1):	
.1.3.6.1.2.1.4.24.4.1.1.A.B.C.D	Адрес назначения маршрута (A).
.1.3.6.1.2.1.4.24.4.1.2.A.B.C.D	Маска адреса назначения маршрута (B).
.1.3.6.1.2.1.4.24.4.1.3.A.B.C.D	Параметр, обозначающий значение поля IP TOS Field (C).
.1.3.6.1.2.1.4.24.4.1.4.A.B.C.D	Адрес следующего маршрутизатора в маршруте (D).
.1.3.6.1.2.1.4.24.4.1.5.A.B.C.D	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2.1 IF-MIB.

OID	Описание
.1.3.6.1.2.1.4.24.4.1.6.A.B.C.D	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения.
.1.3.6.1.2.1.4.24.4.1.7.A.B.C.D	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.4.1.8.A.B.C.D	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.24.4.1.9.A.B.C.D	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.4.24.4.1.10.A.B.C.D	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.4.1.11.A.B.C.D	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.12.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.13.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.4.24.4.1.14.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.15.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.16.A.B.C.D	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление
1.3.6.1.2.1.4.24.6.0	Количество текущих корректных маршрутов из таблицы .1.3.6.1.2.1.4.24.7.1
Таблица маршрутизации сетевого узла с указанием версии протокола IP (.1.3.6.1.2.1.4.24.7.1):	
.1.3.6.1.2.1.4.24.7.1.7	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2 IF-MIB.
.1.3.6.1.2.1.4.24.7.1.8	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения, • 5 (blackhole) — маршрут, по которому пакеты теряются без сообщений об ошибках.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.9	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.7.1.10	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.24.7.1.11	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.7.1.12	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.13	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.14	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.15	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.16	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.17	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

Ethernet-Like MIB

Ethernet-Like MIB (1.3.6.1.2.1.10) включает в себя объекты, предназначенные для получения статистической информации о работе интерфейсов сетевого узла. Подробнее см. в RFC 3635.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 29. SNMP-параметры. Ethernet-Like MIB

OID	Описание
Таблица статистики Ethernet-интерфейсов (.1.3.6.1.2.1.10.7.2.1): **A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB**	
.1.3.6.1.2.1.10.7.2.1.1.A	Индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB.
.1.3.6.1.2.1.10.7.2.1.2.A	Количество ошибок на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.3.A	Количество FCS ошибок на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.4.A	Количество фреймов, вовлеченных в SingleCollision на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.5.A	Количество фреймов, вовлеченных в MultiplyCollision на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.6.A	Количество ошибок SQE TEST ERROR на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.7.A	Количество фреймов, для которых первая попытка отправки была отложена на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.8.A	Количество обнаружения коллизий на интерфейсе, при котором коллизия обнаружена позднее одного slotTime.
.1.3.6.1.2.1.10.7.2.1.9.A	Количество фреймов, которые не удалось передать в связи с коллизиями.
.1.3.6.1.2.1.10.7.2.1.10.A	Количество фреймов, которые не удалось передать в связи с проблемами MAC уровня.
.1.3.6.1.2.1.10.7.2.1.11.A	Количество ошибок передачи в связи с потерей carrier sense condition на интерфейсе.

OID	Описание
.1.3.6.1.2.1.10.7.2.1.13.A	Количество фреймов, принятых на интерфейсе, размер которых превышал максимально допустимый.
.1.3.6.1.2.1.10.7.2.1.16.A	Количество фреймов, которые не удалось принять на интерфейсе в связи с ошибками MAC уровня.
.1.3.6.1.2.1.10.7.2.1.17.A	Идентификатор чипа, который реализует Ethernet-интерфейс.
.1.3.6.1.2.1.10.7.2.1.18.A	Количество ошибок.
.1.3.6.1.2.1.10.7.2.1.19.A	Текущей режим дуплекса на интерфейсе: • 1 — unknown, • 2 — halfDuplex, • 3 — fullDuplex. Для неподключенных интерфейсов параметр равен 1.
1.3.6.1.2.1.10.7.2.1.20.A	Возможность контроля скорости передачи на интерфейсе: • 1 — разрешено, • 2 — запрещено.
.1.3.6.1.2.1.10.7.2.1.21AA	Статус контроля скорости передачи на интерфейсе: • 1 — выключен, • 2 — включен, • 3 — неизвестно.

TCP-MIB

TCP-MIB (.1.3.6.1.2.1.6) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу TCP (например, количество отправленных сегментов, активных соединений). Подробнее см. в RFC 4022.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 30. SNMP-параметры. TCP-MIB

OID	Описание
.1.3.6.1.2.1.6.1.0	Алгоритм определения тайм-аута для повторной передачи неопознанных октетов.
.1.3.6.1.2.1.6.2.0	Минимальное допустимое значение тайм-аута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.3.0	Максимальное допустимое значение тайм-аута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.4.0	Максимальное количество TCP-соединений. При динамическом определении, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.6.5.0	Количество прямых переходов TCP-соединений из состояния CLOSED в состояние SYN-SENT.
.1.3.6.1.2.1.6.6.0	Количество прямых переходов TCP-соединений из состояния LISTEN в состояние SYN-RCVD.
.1.3.6.1.2.1.6.7.0	Количество прямых переходов TCP-соединений в состояние CLOSED из состояния SYN-SENT или SYN-RCVD, а также прямых переходов в состояние LISTEN из состояния SYN-RCVD.
.1.3.6.1.2.1.6.8.0	Количество переходов TCP-соединений в состояние CLOSED из состояния ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.9.0	Количество TCP-соединений, находящихся в состоянии ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.10.0	Количество полученных сегментов, в том числе с ошибками. Включает только количество полученных сегментов на соединениях, установленных в настоящий момент.
.1.3.6.1.2.1.6.11.0	Количество отправленных сегментов.
.1.3.6.1.2.1.6.12.0	Общее количество повторно отправленных сегментов.

Таблица TCP-соединений для протокола IPv4 (.1.3.6.1.2.1.6.13.1):

A - локальный IP-адрес

B - локальный порт

C - удаленный IP-адрес

D - удаленный порт

OID	Описание
.1.3.6.1.2.1.6.13.1.1.A.B.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения, • 4 (synReceived) — ожидание подтверждения после того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения TCP.
.1.3.6.1.2.1.6.14.0	Количество сегментов с ошибками.
.1.3.6.1.2.1.6.15.0	Количество отправленных сегментов с флагом RST.

Таблица TCP-соединений для протоколов IPv4 и IPv6 (.1.3.6.1.2.1.6.19.1):

V1 — версия протокола IP для локального адреса,

A — локальный IP-адрес,

B — локальный порт,

V2 — версия протокола IP для удаленного адреса,

C — удаленный IP-адрес,

D — удаленный порт

.1.3.6.1.2.1.6.19.1.7.V1.4.A.B.V2.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения, • 4 (synReceived) — ожидание подтверждения после

OID	Описание
	того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения.
.1.3.6.1.2.1.6.19.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, связанного с этим соединением. Если такого процесса нет, параметр равен 0.
Таблица открытых TCP-портов (.1.3.6.1.2.1.6.20.1): **V1 — версия протокола IP для локального адреса,** **A — локальный IP-адрес,** **B — локальный порт**	
.1.3.6.1.2.1.6.20.1.4.V1.4.A.B	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

UDP-MIB

UDP-MIB (.1.3.6.1.2.1.7) включает в себя объекты, предназначенные для получения информации о различных характеристиках работы сетевого узла по протоколу UDP (например, общее количество полученных и отправленных датаграмм). Подробнее см. в RFC 4113.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 31. SNMP-параметры. UDP-MIB

OID	Описание
.1.3.6.1.2.1.7.1.0	Количество входящих UDP-датаграмм.
.1.3.6.1.2.1.7.2.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.

OID	Описание
.1.3.6.1.2.1.7.3.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.
.1.3.6.1.2.1.7.4.0	Количество исходящих UDP-датаграмм.
Таблица открытых UDP-портов для протокола IPv4 (.1.3.6.1.2.1.7.5.1): **A — IP-адрес локального порта,** **B — номер локального порта.**	
.1.3.6.1.2.1.7.5.1.1.A.B	IP-адрес локального порта.
.1.3.6.1.2.1.7.5.1.2.A.B	Номер порта.
Таблица открытых UDP-соединений (.1.3.6.1.2.1.7.7.1): **V1 — версия IP-протокола для локального адреса,** **A — IP-адрес локального порта,** **B — номер локального порта,** **V2 — версия IP-протокола для удаленного адреса,** **C — IP-адрес удаленного порта,** **D — номер удаленного порта.**	
.1.3.6.1.2.1.7.7.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

HOST-RESOURCES-MIB

HOST-RESOURCES-MIB (.1.3.6.1.2.1.25) включает в себя объекты, предназначенные для получения информации о системных параметрах и оборудовании сетевого узла. Подробнее см. RFC 2790.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 32. SNMP-параметры. HOST-RESOURCES-MIB

OID	Описание
.1.3.6.1.2.1.25.1.1.0	Время работы системы с последнего запуска.

OID	Описание
.1.3.6.1.2.1.25.1.2.0	Системное время на сетевом узле (значение передается в виде строки байт): • 1-2 байт — год, • 3 байт — месяц, • 4 байт — день, • 5 байт — часы, • 6 байт — минуты, • 7 байт — секунды, • 8 байт — десятые секунды, • 9 байт — «направление» от UTC (соответствующие коды символов ascii), • 10 байт — часы от UTC, • 11 байт — минуты от UTC. Если часовой пояс неизвестен, то последние 3 байта отсутствуют.
1.3.6.1.2.1.25.1.3.0	Индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1, с которого загружается сетевой узел.
.1.3.6.1.2.1.25.1.4.0	Параметры при загрузке сетевого узла (в том числе название аппаратной платформы — для координатора).
.1.3.6.1.2.1.25.1.5.0	Количество сессий пользователя.
.1.3.6.1.2.1.25.1.6.0	Количество процессов загруженных или исполняемых на сетевом узле.
.1.3.6.1.2.1.25.1.7.0	Максимальное поддерживаемое сетевым узлом количество процессов. Если количество не ограничено, параметр равен 0.
1.3.6.1.2.1.25.2.2.0	Объем RAM (в килобайтах).
Таблица локальных логических хранилищ сетевого узла (.1.3.6.1.2.1.25.2.3.1):	
A — индекс хранилища	
.1.3.6.1.2.1.25.2.3.1.1.A	Идентификатор, присвоенный сетевым узлом (A).
.1.3.6.1.2.1.25.2.3.1.2.A	OID, присвоенный данному типу хранилища: 1.3.6.1.2.1.25.2.1 + • 1 — устройство не может быть причислено к какой-либо другой категории, • 2 — RAM, • 3 — виртуальная память, временное хранилище, SWAP, • 4 — не извлекаемые НЖМД, • 5 — извлекаемые НЖМД.
.1.3.6.1.2.1.25.2.3.1.3.A	Описание хранилища.

OID	Описание
.1.3.6.1.2.1.25.2.3.1.4.A	Размер в байтах объектов (размеры секторов/блоков/буферов/пакетов), размещенных в данном хранилище.
.1.3.6.1.2.1.25.2.3.1.5.A	Общее количество секторов/блоков/буферов/пакетов в хранилище.
.1.3.6.1.2.1.25.2.3.1.6.A	Количество использованных секторов/блоков/буферов/пакетов в хранилище.
.1.3.6.1.2.1.25.2.3.1.7.A	Количество ошибок операций записи по причине недостатка места.

Таблица устройств сетевого узла (.1.3.6.1.2.1.25.3.2.1):

B — индекс устройства

.1.3.6.1.2.1.25.3.2.1.1.B	Идентификатор, присвоенный сетевым узлом (B).
.1.3.6.1.2.1.25.3.2.1.2.B	OID, присвоенный данному типу устройства: 1.3.6.1.2.1.25.3.1 + • 1 — применяется, если не может быть отнесено к другой группе, • 2 — применяется, если устройство не опознано, • 3 — CPU (ядра), • 4 — сетевой интерфейс, • 5 — принтер, • 6 — жесткий диск (HDD, SSD), • 10 — видеоустройство, • 11 — аудиоустройство, • 12 — сопроцессор, • 13 — клавиатура, • 14 — модем, • 15 — параллельный порт, • 16 — манипулятор типа мышь, • 17 — последовательный порт, • 18 — ленточное хранилище, • 19 — часы, • 20 — энергозависимая память, • 21 — энергонезависимая память.
.1.3.6.1.2.1.25.3.2.1.3.B	Описание устройства.
.1.3.6.1.2.1.25.3.2.1.4.B	ID продукта.

OID	Описание
.1.3.6.1.2.1.25.3.2.1.5.B	Текущий статус устройства: • 1 — статус неизвестен (unknown), • 2 — работает (running), • 3 — предупреждение (warning), • 4 — проверка (testing), • 5 — не работает (down).
.1.3.6.1.2.1.25.3.2.1.6.B	Счетчик количества ошибок на устройстве.

Таблица загрузки процессоров сетевого узла (.1.3.6.1.2.1.25.3.3.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.3.1.1.B	ID продукта.
.1.3.6.1.2.1.25.3.3.1.2.B	Средняя нагрузка на ядро за последнюю минуту.

Таблица сетевых устройств (.1.3.6.1.2.1.25.3.4.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.4.1.1.B	Индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB.

Таблица дисков сетевого узла (.1.3.6.1.2.1.25.3.6.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.6.1.1.B	Доступ к диску: • 1 — чтение и запись, • 2 — чтение.
.1.3.6.1.2.1.25.3.6.1.2.B	Тип устройства: • 1 — применяется, если не может быть отнесено к другой группе, • 2 — неизвестен, • 3 — жесткий диск, • 4 — дискета, • 5 — оптический диск ROM, • 6 — оптический диск WORM, • 10 — оптический диск RW, • 11 — RAM диск.
.1.3.6.1.2.1.25.3.6.1.3.B	Возможность извлечения диска: • 1 — Разрешено, • 2 — Запрещено.
.1.3.6.1.2.1.25.3.6.1.4.B	Размер диска (в килобайтах). Если диск извлекаемый и он извлечен, параметр равен 0.

Таблица разделов сетевого узла (.1.3.6.1.2.1.25.3.7.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

D — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

OID	Описание
.1.3.6.1.2.1.25.3.7.1.1.B.D	Индекс устройства (D).
.1.3.6.1.2.1.25.3.7.1.2.B.D	Описание раздела.
.1.3.6.1.2.1.25.3.7.1.3.B.D	ID раздела в операционной системе — октетная строка.
.1.3.6.1.2.1.25.3.7.1.4.B.D	Размер раздела (в килобайтах).
.1.3.6.1.2.1.25.3.7.1.5.B.D	Файловая система, используемая в разделе. Если файловой системы нет, параметр равен 0.

Таблица файловых систем сетевого узла (.1.3.6.1.2.1.25.3.8.1):

E — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

.1.3.6.1.2.1.25.3.8.1.1.E	Индекс устройства (E).
.1.3.6.1.2.1.25.3.8.1.2.E	Корневая папка файловой системы (точка монтирования).
.1.3.6.1.2.1.25.3.8.1.3.E	Описание удаленного сервера, с которого смонтирована файловая система. Может включать корневую папку файловой системы (точка монтирования) на удаленном сервере. Для локальных файловых систем параметр содержит пустую строку.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.4.E	OID, присвоенный данному типу файловой системы: 1.3.6.1.2.1.25.3.9 + • 1 — Применяется, если не может быть отнесена к другой группе, • 2 — Если тип файловой системы неизвестен, • 3 — BFFS, • 4 — System V, • 5 — DOS FAT, • 6 — OS/2 HPFS, • 7 — MHFS, • 8 — MFS, • 9 — NTFS, • 10 — VNode File System, • 11 — Journaled File System, • 12 — ISO 9660 File System for CD, • 13 — RockRidge File System for CD, • 14 — NFS File System, • 15 — Netware File System, • 16 — Andrew File System, • 17 — OSF DCE Distributed File System, • 18 — AppleShare File System, • 19 — RFS File System, • 20 — Data General DGCFS, • 21 — SVR4 Boot File System, • 22 — Windows FAT32, • 23 — Linux EXT2 File System.
.1.3.6.1.2.1.25.3.8.1.5.E	Права доступа к файловой системе: • 1 — запись, чтение, • 2 — чтение.
.1.3.6.1.2.1.25.3.8.1.6.E	Возможность запуска с файловой системы: • 1 — возможно, • 2 — невозможно.
.1.3.6.1.2.1.25.3.8.1.7.E	Указывает на связь файловой системы и хранилищ.
.1.3.6.1.2.1.25.3.8.1.8.E	Дата последнего полного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.9.E	Дата последнего частичного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.
Таблица ПО, запущенного на сетевом узле (.1.3.6.1.2.1.25.4.2.1):	
F — индекс ПО	
.1.3.6.1.2.1.25.4.2.1.1.F	Индекс запущенного ПО (F).
.1.3.6.1.2.1.25.4.2.1.2.F	Наименование запущенного ПО.
.1.3.6.1.2.1.25.4.2.1.3.F	ID ПО производителя.
.1.3.6.1.2.1.25.4.2.1.4.F	Папка, из которой запущено ПО.
.1.3.6.1.2.1.25.4.2.1.5.F	Параметры, с которыми запущено ПО.
.1.3.6.1.2.1.25.4.2.1.6.F	Тип программного обеспечения: • 1 — неизвестно, • 2 — ОС, • 3 — драйвер устройства, • 4 — приложение.
.1.3.6.1.2.1.25.4.2.1.7.F	Текущее состояния ПО: • 1 — запущено (running), • 2 — работоспособно (runnable), • 3 — неработоспособно (notRunnable), • 4 — работает некорректно (invalid).
Таблица с потреблением каждого ПО ЦПУ и ОЗУ (.1.3.6.1.2.1.25.5.1.1):	
F — индекс ПО из таблицы .1.3.6.1.2.1.25.4.2.1	
.1.3.6.1.2.1.25.5.1.1.1.F	Количество процессорного времени, выделенного ПО, в сантисекундах (0,01 с).
.1.3.6.1.2.1.25.5.1.1.2.F	Количество занимаемой оперативной памяти (в килобайтах).

LM-SENSORS-MIB

LM-SENSORS-MIB (.1.3.6.1.4.1.2021) включает в себя объекты, предназначенные для получения информации от различных датчиков, которые установлены в оборудовании сетевого узла.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 33. SNMP-параметры. LM-SENSORS-MIB

OID	Описание
Таблица температурных датчиков сетевого узла (.1.3.6.1.4.1.2021.13.16.2.1):	
A — индекс температурного датчика	
.1.3.6.1.4.1.2021.13.16.2.1.1.A	Индекс температурного датчика (A).
.1.3.6.1.4.1.2021.13.16.2.1.2.A	Имя температурного датчика.
.1.3.6.1.4.1.2021.13.16.2.1.3.A	Температура (в м°C).
Таблица датчиков скорости вращения вентиляторов (.1.3.6.1.4.1.2021.13.16.3.1):	
B — индекс датчика скорости вращения вентилятора	
.3.6.1.4.1.2021.13.16.3.1.1.B	Индекс датчика скорости вращения вентилятора (B).
.3.6.1.4.1.2021.13.16.3.1.2.B	Имя датчика скорости вращения вентилятора.
.3.6.1.4.1.2021.13.16.3.1.3.B	Скорость вращения вентилятора (в оборотах в минуту). Если вентилятор не подключен, параметр равен 0.

Таблица 34. Температурные датчики

Платформа	Имя датчика	Описание	Предельное значение
HW10 F1	gpu_thermal-virtual-0: temp1	Температура графического ядра	+115 °C (+115 000 м°C)
	soc_thermal-virtual-0: temp1	Температура ядра процессора	+115 °C (+115 000 м°C)
HW50 N1, N2, N3	Core 0	Температура ядра процессора	+110 °C (+110 000 м°C)
HW50 N4	Core 0 Core 2	Температура ядер процессора	+90 °C (+90 000 м°C)
HW50 A1	Core0 Core1 Core2 Core3	Температура ядер процессора	+110 °C (+110 000 м°C)
HW100 N1, N2, N3	Core 0	Температура ядер процессора	+105 °C (+105 000 м°C)
	Core 1		
HW100 Q1, Q2	Physical id 0	Температура процессора	+75 °C (+75 000 м°C)
	Core 6	Температура ядер процессора	+75 °C (+75 000 м°C)
	Core 12		
HW1000 Q4	Core 0	Температура ядер процессора	+80 °C (+80 000 м°C)
	Core 1		
	Physical id 0	Температура процессора	+80 °C (+80 000 м°C)

Платформа	Имя датчика	Описание	Предельное значение
	temp1	Температура модуля памяти	+105 °C (+105 000 м°C)
HW1000 Q5, Q6	Core 0	Температура ядер процессора	+80 °C (+80 000 м°C)
	Core 1		
	Physical id 0	Температура процессора	+80 °C (+80 000 м°C)
	jc42-i2c-*:temp1	Температура модуля памяти	+105 °C (+105 000 м°C)
HW1000 Q7, Q8, Q9	Core 0	Температура ядер процессора	+80 °C (+80 000 м°C)
	Core 1		
	Core 2		
	Core 3		
	Physical id 0	Температура процессора	+80 °C (+80 000 м°C)
	temp1	Температура модуля памяти	+119 °C (+119 000 м°C)
HW1000 Q10	Core 0	Температура ядер процессора	+73 °C (+73 000 м°C)
	Core 2		
	Core 4		
	Core 6		
	Core 8		
	Core 10		
	Core 12		
	Core 14		
	Physical id 0	Температура процессора	+73 °C (+73 000 м°C)
	SYSTIN	Температура материнской платы	+80 °C (+80 000 м°C)
	CPUTIN	Температура центрального процессора	+80 °C (+80 000 м°C)
HW2000 Q4	Core 0	Температура ядер процессора 1	+71 °C (+71 000 м°C)
	Core 1		
	Core 2		
	Core 3		
	Core 4		
	Core 5		
	Physical id 0	Температура процессора 1	+71 °C (+71 000 м°C)
	coretemp-isa-0001: Core 0	Температура ядер процессора 2	+71 °C (+71 000 м°C)

Платформа	Имя датчика	Описание	Предельное значение
	coretemp-isa-0001: Core 1		
	coretemp-isa-0001: Core 2		
	coretemp-isa-0001: Core 3		
	coretemp-isa-0001: Core 4		
	coretemp-isa-0001: Core 5		
	Physical id 1	Температура процессора 2	+71 °C (+71 000 м°C)
HW2000 Q5	Core 0	Температура ядер процессора	+80 °C (+80 000 м°C)
	Core 1		
	Core 2		
	Core 3		
	Core 4		
	Core 5		
	Physical id 0	Температура процессора	+80 °C (+80 000 м°C)
HW5000 Q1	Core 0	Температура ядер процессора 1	+75 °C (+75 000 м°C)
	Core 1		
	Core 2		
	Core 3		
	Core 4		
	Core 5		
	Physical id 0	Температура процессора 1	+75 °C (+75 000 м°C)
	coretemp-isa-0001: Core 0	Температура ядер процессора 2	+75 °C (+75 000 м°C)
	coretemp-isa-0001: Core 1		
	coretemp-isa-0001: Core 2		
	coretemp-isa-0001: Core 3		
	coretemp-isa-0001: Core 4		
	coretemp-isa-0001: Core 5		
	Physical id 1	Температура процессора 2	+75 °C (+75 000 м°C)
HW5000 Q2	Core 0	Температура ядер процессора	+78 °C (+78 000 м°C)
	Core 1		
	Core 2		
	Core 3		

Платформа	Имя датчика	Описание	Предельное значение
	Core 4		
	Core 5		
	Core 6		
	Core 7		
	Physical id 0	Температура процессора	+78 °C (+78 000 м°C)

Внимание! Рекомендуемые значения скорости вращения вентиляторов находятся в промежутке 5 000 - 9 000 оборотов в минуту. Если значение скорости выше 15 000 или ниже 1 000 оборотов в минуту обратитесь в службу поддержки ИнфоТеКС.

Имена датчиков скорости могут отличаться в зависимости от ревизии аппаратной платформы.

Таблица 35. Датчики скорости вращения вентиляторов

Платформа	Количество датчиков	Имя
HW1000 Q4, Q5, Q6	2	fan3 fan4
HW1000 Q7, Q8, Q9	3	FRNT_FAN1 FRNT_FAN2 FRNT_FAN3
HW1000 Q10	2	SYS_FAN1 SYS_FAN2
HW2000 Q4	6	fan3 fan6 fan9 nct7904-i2c-0-2d:fan1, nct7904-i2c-0-2d:fan2, nct7904-i2c-0-2d:fan4
HW2000 Q5	3	FRNT_FAN1 FRNT_FAN2 FRNT_FAN3

Платформа	Количество датчиков	Имя
HW5000 Q1	6	fan3 fan6 fan9 nct7904-i2c-0-2d:fan1, nct7904-i2c-0-2d:fan2, nct7904-i2c-0-2d:fan4
HW5000 Q2	3	FRNT_FAN1 FRNT_FAN2 FRNT_FAN3

NOTIFICATION-LOG-MIB

NOTIFICATION-LOG-MIB (.1.3.6.1.2.1.92) включает в себя объекты, предназначенные для получения информации о журналах событий. Подробнее см. в RFC 3014.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 36. SNMP-параметры. NOTIFICATION-LOG-MIB

OID	Описание
.1.3.6.1.2.1.92.1.1.1.0	Максимальное количество записей, которое может хранить таблица журналов .1.3.6.1.2.1.92.1.3.1.1 (таблица не поддерживается в ViPNet Coordinator HW). Если ограничений нет, параметр равен 0.
.1.3.6.1.2.1.92.1.1.2.0	Время, в течение которого SNMP-агент должен хранить уведомления (в минутах). Если время не ограничено, параметр равен 0.
.1.3.6.1.2.1.92.1.2.1.0	Количество записей в таблице журналов .1.3.6.1.2.1.92.1.3.1.1 (таблица не поддерживается ViPNet Coordinator HW).
.1.3.6.1.2.1.92.1.2.2.0	Количество записей, отброшенных из-за необходимости освобождения места под новые, или по причине превышения значений параметров .1.3.6.1.2.1.92.1.1.1.0 или 1.3.6.1.2.1.92.1.1.3.1.3. Не включает в себя количество записей, удаленных в связи с истечением времени .1.3.6.1.2.1.92.1.1.2.0.

UCD-SNMP-MIB

UCD-SNMP-MIB (.1.3.6.1.4.1.2021) включает в себя объекты, предназначенные для получения информации о характеристиках и состоянии оборудования сетевого узла (например, состояние оперативной памяти и жесткого диска). Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 37. SNMP-параметры. UCD-SNMP-MIB

OID	Описание
.1.3.6.1.4.1.2021.4.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.4.2.0	Фиктивное имя, всегда равно объему виртуальной памяти.
.1.3.6.1.4.1.2021.4.3.0	Объем виртуальной памяти (swap) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.4.0	Объем доступной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.5.0	Объем физической памяти (RAM) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.6.0	Объем доступной физической памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.7.0	Объем виртуальной памяти, выделенный для текстовых страниц (в кибибайтах).
.1.3.6.1.4.1.2021.4.9.0	Объем физической памяти (RAM), выделенный для текстовых страниц (в кибибайтах). Не выводится, если операционная система не выделяет текстовые страницы от других используемых в RAM.
.1.3.6.1.4.1.2021.4.11.0	Общий объем доступной памяти (RAM + swap) (в кибибайтах).
.1.3.6.1.4.1.2021.4.12.0	Минимальный объем свободной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.13.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory).
.1.3.6.1.4.1.2021.4.14.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена.
.1.3.6.1.4.1.2021.4.15.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кешированной памяти.
.1.3.6.1.4.1.2021.4.16.0	Объем виртуальной памяти, занятый текстовыми страницами (в кибибайтах).
.1.3.6.1.4.1.2021.4.17.0	Объем физической памяти (RAM), занятый текстовыми страницами (в кибибайтах). Не выводится если операционная система не выделяет текстовые страницы от других используемых в RAM.
.1.3.6.1.4.1.2021.4.18.0	Объем виртуальной памяти на сетевом узле (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.3.0.

OID	Описание
.1.3.6.1.4.1.2021.4.19.0	Объем доступной виртуальной памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.4.0.
.1.3.6.1.4.1.2021.4.20.0	Объем физической памяти на сетевом узле (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.5.0.
.1.3.6.1.4.1.2021.4.21.0	Объем свободной физической памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.6.0.
.1.3.6.1.4.1.2021.4.22.0	Общий объем доступной памяти (RAM + swap) (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.11.0.
.1.3.6.1.4.1.2021.4.23.0	Минимальный объем свободной виртуальной памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.12.0.
.1.3.6.1.4.1.2021.4.24.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory). 64-битный аналог .1.3.6.1.4.1.2021.4.13.0.
.1.3.6.1.4.1.2021.4.25.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена. 64-битный аналог .1.3.6.1.4.1.2021.4.14.0.
.1.3.6.1.4.1.2021.4.26.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кешированной памяти. 64-битный аналог .1.3.6.1.4.1.2021.4.15.0.
.1.3.6.1.4.1.2021.4.100.0	Признак, что объем виртуальной памяти меньше минимально установленного значения.
.1.3.6.1.4.1.2021.4.101.0	Сообщение о том, что доступный объем виртуальной памяти меньше минимально установленного значения.
Таблица сведений о разделах (.1.3.6.1.4.1.2021.9.1)	
B — индекс диска, присвоенный сетевым узлом	
.1.3.6.1.4.1.2021.9.1.1.B	Индекс раздела (B).
.1.3.6.1.4.1.2021.9.1.2.B	Точка монтирования раздела.
.1.3.6.1.4.1.2021.9.1.3.B	Устройство (или tmpfs), на котором находится раздел.
.1.3.6.1.4.1.2021.9.1.4.B	Минимальный объем свободного места на разделе (в килобайтах) до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.5.B	Минимальный объем свободного места на разделе (в процентах) от общего до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.6.B	Общий объём раздела (в килобайтах).
.1.3.6.1.4.1.2021.9.1.7.B	Свободное место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.8.B	Занятое место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.9.B	Занятое место в разделе (в процентах).
.1.3.6.1.4.1.2021.9.1.10.B	Процент использования инодов в разделе.

OID	Описание
.1.3.6.1.4.1.2021.9.1.100.B	Флаг ошибки, сигнализирующий о том, что свободного места в разделе осталось меньше заданного значения .1.3.6.1.4.1.2021.9.1.4.B или .1.3.6.1.4.1.2021.9.1.5.B: • 0 — нет ошибки, • 1 — есть ошибка.
.1.3.6.1.4.1.2021.9.1.101.B	Сообщение об ошибке. Если параметр .1.3.6.1.4.1.2021.9.1.10.B равен 0, сообщение пустое.
.1.3.6.1.4.1.2021.9.1.11.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если раздел менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.6.B.
.1.3.6.1.4.1.2021.9.1.12.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если раздел менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.13.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если свободно менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.7.B.
.1.3.6.1.4.1.2021.9.1.14.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если свободно менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.15.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если занято менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.8.B
.1.3.6.1.4.1.2021.9.1.16.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если занято менее 2ТБайт, параметр равен 0.

Таблица информации о средней загрузке системы за 1, 5, 15 минут (1.3.6.1.4.1.2021.10.1)

C — индекс, присвоенный сетевым узлом (постоянный):

- **1 — значение для 1 минуты,**
- **2 — значение для 5 минут,**
- **3 — значение для 15 минут**

.1.3.6.1.4.1.2021.10.1.1.C	Индекс значения средней загрузки: • 1 — 1 минута, • 2 — 5 минут, • 3 — 15 минут
.1.3.6.1.4.1.2021.10.1.2.C	Имя загрузки (по умолчанию: Load-1, Load-5, Load-15).
.1.3.6.1.4.1.2021.10.1.3.C	Средняя загрузка системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.4.C	Пороговое значение загрузки системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.5.C	Загрузка системы в процентах (в виде целого числа).
.1.3.6.1.4.1.2021.10.1.6.C	Загрузка системы в процентах (в виде числа с плавающей точкой).

OID	Описание
.1.3.6.1.4.1.2021.10.1.100.C	Флаг, сигнализирующий о превышении средней загрузки порогового значения.
.1.3.6.1.4.1.2021.10.1.101.C	Сообщение о превышении порогового значения.
.1.3.6.1.4.1.2021.10.1.0	Фиктивный индекс, всегда равен 1.
.1.3.6.1.4.1.2021.10.2.0	Фиктивное имя, всегда равно systemStats.
.1.3.6.1.4.1.2021.11.3.0	Среднее количество информации (в килобайтах), записанное на диск за минуту.
.1.3.6.1.4.1.2021.11.4.0	Среднее количество информации (в килобайтах), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.5.0	Среднее количество информации (в блоках данных), записанных на диск за минуту.
.1.3.6.1.4.1.2021.11.6.0	Среднее количество информации (в блоках данных), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.7.0	Среднее количество системных прерываний за минуту.
.1.3.6.1.4.1.2021.11.8.0	Среднее количество переключений контекста за минуту.
.1.3.6.1.4.1.2021.11.9.0	Процент времени, занятого пользовательскими процессами (за минуту).
.1.3.6.1.4.1.2021.11.10.0	Процент времени, когда процессор занят системными процессами (за минуту).
.1.3.6.1.4.1.2021.11.11.0	Процент времени, когда процессор не занят процессами (за минуту).
.1.3.6.1.4.1.2021.11.50.0	Количество тиков процессорного времени, затраченного на исполнения user-level code.
.1.3.6.1.4.1.2021.11.51.0	Количество тиков процессорного времени, затраченного на исполнение reduced-priority code.
.1.3.6.1.4.1.2021.11.52.0	Количество тиков процессорного времени, затраченного на исполнение system-level code.
.1.3.6.1.4.1.2021.11.53.0	Количество тиков процессорного времени, проведенного в состоянии idle.
.1.3.6.1.4.1.2021.11.54.0	Количество тиков процессорного времени, затраченного на исполнение ожидания ввода-вывода.
.1.3.6.1.4.1.2021.11.55.0	Количество тиков процессорного времени, затраченного на исполнение kernel-level code.
.1.3.6.1.4.1.2021.11.56.0	Количество тиков процессорного времени, затраченного на исполнение аппаратных прерываний.
.1.3.6.1.4.1.2021.11.57.0	Количество блоков, отправленное блочному устройству (диску).
.1.3.6.1.4.1.2021.11.58.0	Количество блоков, полученное блочным устройством (диском).

OID	Описание
.1.3.6.1.4.1.2021.11.59.0	Количество обработанных аппаратных прерываний.
.1.3.6.1.4.1.2021.11.60.0	Количество выполненных переключений контекста.
.1.3.6.1.4.1.2021.11.61.0	Количество тиков процессорного времени, затраченного на исполнение программных прерываний.
.1.3.6.1.4.1.2021.11.62.0	Количество блоков, помещенных в виртуальную память.
.1.3.6.1.4.1.2021.11.63.0	Количество блоков, извлеченных из виртуальной памяти.
.1.3.6.1.4.1.2021.11.64.0	Количество тиков процессорного времени, затраченного кодом гипервизора (если узел работает в виртуальной среде).
.1.3.6.1.4.1.2021.11.65.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре.
.1.3.6.1.4.1.2021.11.66.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре с пониженным приоритетом.
.1.3.6.1.4.1.2021.11.67.0	Количество ядер процессоров.
.1.3.6.1.4.1.2021.100.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.100.2.0	Ключевое слово CVS.
.1.3.6.1.4.1.2021.100.3.0	Строка времени из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.4.0	Строка времени из ctime.
.1.3.6.1.4.1.2021.100.5.0	Идентификатор из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.6.0	Опции конфигурации SNMP-агента.
.1.3.6.1.4.1.2021.101.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.101.2.0	Фиктивная строка, всегда равная snmp.
.1.3.6.1.4.1.2021.101.100.0	Признак ошибки SNMP-агента.
.1.3.6.1.4.1.2021.101.101.0	Описание ошибки SNMP-агента.

UCD-DISKIO-MIB

UCD-DISKIO-MIB (.1.3.6.1.4.1.2021.13.15) включает в себя объекты, предназначенные для получения информации о состоянии памяти и дискового пространства сетевого узла. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 38. SNMP-параметры. UCD-DISKIO-MIB

OID	Описание
Таблица значений текущих параметров оперативной памяти, виртуальной памяти, дискового пространства и их загрузки (.1.3.6.1.4.1.2021.13.15.1.1.)	
A — индекс таблицы	
.1.3.6.1.4.1.2021.13.15.1.1.1.A	Индекс таблицы (A).
.1.3.6.1.4.1.2021.13.15.1.1.2.A	Описание устройства, полученное от ОС. Для координатора принимает значения: ram0-ram15 loop0-loop7 sda, sda1, sda2, sdb1, sdb2, sdb3
.1.3.6.1.4.1.2021.13.15.1.1.3.A	Количество байт, считанных с устройства с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.4.A	Количество байт, записанных на устройство с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.5.A	Количество операций доступа к устройству на чтение.
.1.3.6.1.4.1.2021.13.15.1.1.6.A	Количество операций доступа к устройству на запись.
.1.3.6.1.4.1.2021.13.15.1.1.9.A	Средняя загрузка устройства за 1 минуту (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.10.A	Средняя загрузка устройства за 5 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.11.A	Средняя загрузка устройства за 15 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.12.A	Количество операций доступа к устройству на чтение. 64-разрядный параметр.
.1.3.6.1.4.1.2021.13.15.1.1.13.A	Количество байт, записанных на устройство с момента запуска. 64-разрядный параметр.
.1.3.6.1.4.1.2021.13.15.1.1.14.A	Время использования диска с момента запуска (в микросекундах).

NET-SNMP-MIB

NET-SNMP-MIB (1.3.6.1.4.1.8072) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 39. SNMP-параметры. NET-SNMP-MIB

OID	Описание
Таблица, содержащая все OID, зарегистрированные MIB-модулями в SNMP-агенте (.1.3.6.1.4.1.8072.1.2.1.1):	

OID	Описание
A – имя MIB-модуля	
B – OID MIB-модуля	
C – приоритет MIB-модуля	
.1.3.6.1.4.1.8072.1.2.1.1.4.A.B.C	Имя модуля, который зарегистрировал OID.
.1.3.6.1.4.1.8072.1.2.1.1.5.A.B.C	Биты, означающие режим работы OID.
.1.3.6.1.4.1.8072.1.2.1.1.6.A.B.C	Таймаут для модуля.
Таблица заскриптованных расширений (.1.3.6.1.4.1.8072.1.3.2.2.1):	
D – идентификатор расширения	
.1.3.6.1.4.1.8072.1.3.2.2.1.2.D	Путь к бинарному файлу или скрипту для запуска.
.1.3.6.1.4.1.8072.1.3.2.2.1.3.D	Аргументы для команды.
.1.3.6.1.4.1.8072.1.3.2.2.1.4.D	Стандартные вводные для команды.
.1.3.6.1.4.1.8072.1.3.2.2.1.5.D	Продолжительность времени, в течение которого результат выполнения команды кешируется (секунд).
.1.3.6.1.4.1.8072.1.3.2.2.1.6.D	Механизм запуска команды: • 1 — fork-and-exec, • 2 — run via a sub-shell.
.1.3.6.1.4.1.8072.1.3.2.2.1.7.D	Механизм исполнения команды: • 1 — run-on-read, • 2 — run-on-set, • 3 — run-command.
.1.3.6.1.4.1.8072.1.3.2.2.1.20.D	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.4.1.8072.1.3.2.2.1.21.D	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

OID	Описание
Таблица результатов выполнения скриптов (.1.3.6.1.4.1.8072.1.3.2.3.1):	
D – идентификатор расширения	
.1.3.6.1.4.1.8072.1.3.2.3.1.1.D	Первая строка в результате запуска команды.
.1.3.6.1.4.1.8072.1.3.2.3.1.2.D	Полный результат запуска команды одной строки.
.1.3.6.1.4.1.8072.1.3.2.3.1.3.D	Количество строк в результате запуска команды.
.1.3.6.1.4.1.8072.1.3.2.3.1.4.D	Значение, возвращенное командой.
Таблица результатов выполнения команды построчно (.1.3.6.1.4.1.8072.1.3.2.4.1):	
D – идентификатор расширения	
E – номер строки (с единицы)	
.1.3.6.1.4.1.8072.1.3.2.4.1.D.E	Единичная строка вывода команды.
.1.3.6.1.4.1.8072.1.5.1.0	Время, на которое кешируется значение OID по умолчанию (в секундах), если оно не задано в параметре .1.3.6.1.4.1.8072.1.5.3.1.2.F.
.1.3.6.1.4.1.8072.1.5.2.0	Статус кеширования: • 1 — включено, • 2 — выключено.
Таблица кешированных OID (.1.3.6.1.4.1.8072.1.5.3.1):	
F – OID, значение которого кешировано	
.1.3.6.1.4.1.8072.1.5.3.1.2.F	Время, на которое кешируется значение OID (в секундах).
.1.3.6.1.4.1.8072.1.5.3.1.3.F	Статус записи: • 1 (enabled) — включена, • 2 (disabled) — выключена, • 3 (empty) — пустая, • 4 (cached) — кешированная, • 5 (expired) — истекла.
1.3.6.1.4.1.8072.1.7.1.1.0	Статус режима debug SNMP-агента: • 1 — включен, • 2 — выключен.
.1.3.6.1.4.1.8072.1.7.1.2.0	Переключатель вывода для debug: • 1 — вывод всех значений, • 2 — фильтрация вывода. Для работы переключателя параметр .1.3.6.1.4.1.8072.1.7.1.1.0 должен быть равен 1.
.1.3.6.1.4.1.8072.1.7.1.3.0	Переключатель вывода сырого дампа пакетов: • 1 — включен, • 2 — выключен.

OID	Описание
Таблица результатов debug (.1.3.6.1.4.1.8072.1.7.1.4.1):	
G – префикс идентификатора	
.1.3.6.1.4.1.8072.1.7.1.4.4.G	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
Таблица форм вывода сообщений SNMP-агента (.1.3.6.1.4.1.8072.1.7.2.1.1):	
H – уровень важности событий:	
0 – emergency	
1 – alert	
2 – critical	
3 – error	
4 – warning	
5 – notice	
6 – info	
7 – debug	
I – идентификатор журнала	
.1.3.6.1.4.1.8072.1.7.2.1.1.3.H.I	Форма вывода сообщений для данной строки: • 1 — stdout, • 2 — stderr, • 3 — file, • 4 — syslog, • 5 — callback.
.1.3.6.1.4.1.8072.1.7.2.1.1.4.H.I	Максимальное значение, для которого применима данная строка: • 0 — emergency, • 1 — alert, • 2 — critical, • 3 — error, • 4 — warning, • 5 — notice, • 7 — debug.

OID	Описание
.1.3.6.1.4.1.8072.1.7.2.1.1.5.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
VACM таблица доступа сетевого узла (.1.3.6.1.4.1.8072.1.9.1.1.): **J – имя группы:** **K – префикс контекста доступа** **L – модель безопасности доступа** **M – уровень безопасности доступа** **N – способ аутентификации**	
.1.3.6.1.4.1.8072.1.9.1.1.2.J.K.L.M.N	Механизм выбора совпадений в VACM: • 1 — exact (полное совпадение), • 2 — prefix (совпадает префикс).
.1.3.6.1.4.1.8072.1.9.1.1.3.J.K.L.M.N	Значение секции ViewName.
.1.3.6.1.4.1.8072.1.9.1.1.4.J.K.L.M.N	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.4.1.8072.1.9.1.1.5.J.K.L.M.N	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-MPD-MIB

SNMP-MPD-MIB (.1.3.6.1.6.3.11) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 40. SNMP-параметры. SNMP-MPD-MIB

OID	Описание
.1.3.6.1.6.3.11.2.1.1.0	Количество полученных SNMP-пакетов, заблокированных по причине неподдерживаемой или неизвестной модели безопасности.
.1.3.6.1.6.3.11.2.1.2.0	Количество полученных SNMP-пакетов, заблокированных по причине ошибок в SNMP-сообщении.
.1.3.6.1.6.3.11.2.1.3.0	Количество полученных SNMP-пакетов, заблокированных по причине несоответствия pduType.

SNMP-TARGET-MIB

SNMP-TARGET-MIB (.1.3.6.1.6.3.12) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 41. SNMP-параметры. SNMP-TARGET-MIB

OID	Описание
.1.3.6.1.6.3.12.1.1.0	Параметр для совместной работы нескольких SNMP-менеджеров, для одновременной работы с таблицами данного MIB.
.1.3.6.1.6.3.12.1.4.0	Количество полученных SNMP-пакетов, заблокированных по причине недоступного контекста.
.1.3.6.1.6.3.12.1.5.0	Количество полученных SNMP-пакетов, заблокированных по причине неизвестного контекста.

SNMP-USER-BASED-SM-MIB

SNMP-USER-BASED-SM-MIB (.1.3.6.1.6.3.15) включает в себя объекты, предназначенные для получения информации о параметрах и событиях безопасности SNMP-агента.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 42. SNMP-параметры. SNMP-USER-BASED-SM-MIB

OID	Описание
.1.3.6.1.6.3.15.1.1.1.0	Количество заблокированных SNMP-пакетов по причине запроса неизвестного или недоступного уровня безопасности.
.1.3.6.1.6.3.15.1.1.2.0	Количество заблокированных SNMP-пакетов по причине появления вне определённого (доверенного) SNMP-агентом окна.
.1.3.6.1.6.3.15.1.1.3.0	Количество заблокированных SNMP-пакетов по причине использования неизвестного SNMP-агенту имени пользователя.
.1.3.6.1.6.3.15.1.1.4.0	Количество заблокированных SNMP-пакетов по причине обращения к неизвестному SNMP-агенту snmpEngineID.
.1.3.6.1.6.3.15.1.1.5.0	Количество заблокированных SNMP-пакетов по причине отсутствия ожидаемого значения digest value.
.1.3.6.1.6.3.15.1.1.6.0	Количество заблокированных SNMP-пакетов по причине невозможности их расшифровки.
.1.3.6.1.6.3.15.1.2.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицей .1.3.6.1.6.3.15.1.2.2.1.
Таблица параметров безопасности пользователя (.1.3.6.1.6.3.15.1.2.2.1):	
A – EngineID пользователя	
B – имя пользователя	
.1.3.6.1.6.3.15.1.2.2.1.3.A.B	Имя пользователя в формате модели безопасности.
.1.3.6.1.6.3.15.1.2.2.1.4.A.B	Ссылка на другую строку таблицы, в которой создана копия пользователя из текущей строки.
.1.3.6.1.6.3.15.1.2.2.1.5.A.B	Тип протокола аутентификации пользователя.
.1.3.6.1.6.3.15.1.2.2.1.8.A.B	Тип протокола конфиденциальности пользователя.
.1.3.6.1.6.3.15.1.2.2.1.11.A.B	Параметр для определения факта смены ключей пользователя.
.1.3.6.1.6.3.15.1.2.2.1.12.A.B	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.6.3.15.1.2.2.1.13.A.B	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-VIEW-BASED-ACM-MIB

SNMP-VIEW-BASED-ACM-MIB (.1.3.6.1.6.3.16) включает в себя объекты, предназначенные для получения информации о правах доступа к SNMP-параметрам.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 43. SNMP-параметры. SNMP-VIEW-BASED-ACM-MIB

OID	Описание
Таблица доступных контекстов сетевого узла (.1.3.6.1.6.3.16.1.1):	
A – строка контекста	
.1.3.6.1.6.3.16.1.1.1.A	Строка контекста.
Таблица групп доступа (.1.3.6.1.6.3.16.1.2.1):	
B – модель безопасности	
C – имя безопасности	
.1.3.6.1.6.3.16.1.2.1.3.B.C	Имя группы
.1.3.6.1.6.3.16.1.2.1.4.B.C	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.6.3.16.1.2.1.5.B.C	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
Таблица прав доступа к группам (.1.3.6.1.6.3.16.1.4.1): **D – имя группы** **E – контекст доступа** **F – модель безопасности** **G – уровень безопасности**	
.1.3.6.1.6.3.16.1.4.1.4.D.E.F.G	Формат совпадения: • 1 (exact) — полное совпадение, • 2 (prefix) — совпадает префикс.
.1.3.6.1.6.3.16.1.4.1.5.D.E.F.G	Имя view на просмотр.
.1.3.6.1.6.3.16.1.4.1.6.D.E.F.G	Имя view на запись.
.1.3.6.1.6.3.16.1.4.1.7.D.E.F.G	Имя view для уведомлений.
.1.3.6.1.6.3.16.1.4.1.8.D.E.F.G	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.4.1.9.D.E.F.G	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.6.3.16.1.5.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицами данного MIB.

OID	Описание
Таблица с параметрами view для семей поддеревьев (.1.3.6.1.6.3.16.1.5.2.1.):	
H – имя view	
I – поддерево	
.1.3.6.1.6.3.16.1.5.2.1.3.H.I	Маска, заданная для view.
.1.3.6.1.6.3.16.1.5.2.1.4.H.I	Тип view: • 1 — included, • 2 — excluded.
.1.3.6.1.6.3.16.1.5.2.1.5.H.I	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.5.2.1.6.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-FRAMEWORK-MIB

SNMP-FRAMEWORK-MIB (.1.3.6.1.6.3.10) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 44. SNMP-параметры. SNMP-FRAMEWORK-MIB

OID	Описание
.1.3.6.1.6.3.10.2.1.1.0	Идентификатор SNMP-engine.
.1.3.6.1.6.3.10.2.1.2.0	Количество инициализаций SNMP-engine после создания идентификатора.
.1.3.6.1.6.3.10.2.1.3.0	Время, прошедшее с последнего изменения количества инициализаций SNMP-engine (в секундах).

OID	Описание
.1.3.6.1.6.3.10.2.1.4.0	Максимальная длина входящего и исходящего SNMP-сообщения (в байтах).

VIPNET-MIB

VIPNET-MIB (.1.3.6.1.4.1.10812) включает в себя объекты, предназначенные для получения информации о параметрах сетевых узлов ViPNet. Для получения этой информации используется ветвь: `.iso.org.dod.internet.private.enterprises.infotecs.vipnet` (.1.3.6.1.4.1.10812.1).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 45. SNMP-параметры. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.1.1	Шестнадцатеричный идентификатор сети ViPNet.
.1.3.6.1.4.1.10812.1.1.2	Шестнадцатеричный идентификатор сетевого узла ViPNet.
.1.3.6.1.4.1.10812.1.1.3	Имя пользователя узла ViPNet.
.1.3.6.1.4.1.10812.1.1.4	Время работы ViPNet Coordinator HW (сбрасывается каждый раз при перезапуске службы `iplircfg`).
.1.3.6.1.4.1.10812.1.1.5	Шестнадцатеричный идентификатор, включающий в себя идентификаторы узла ViPNet и сети ViPNet.
.1.3.6.1.4.1.10812.1.1.7	Имя узла ViPNet.
.1.3.6.1.4.1.10812.1.2.1	Количество сетевых интерфейсов.
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.4.1.10812.1.2.2):	
.1.3.6.1.4.1.10812.1.2.2.1.1	Номер интерфейса.
.1.3.6.1.4.1.10812.1.2.2.1.2	Системное имя интерфейса.
.1.3.6.1.4.1.10812.1.2.2.1.3	Устаревший параметр, всегда равен 0.
.1.3.6.1.4.1.10812.1.2.2.1.4	Количество пропущенных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.5	Количество блокированных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.6	Количество пропущенных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.7	Количество блокированных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.8	Количество пропущенных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.9	Количество блокированных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.10	Количество пропущенных исходящих зашифрованных пакетов.

OID	Описание
.1.3.6.1.4.1.10812.1.2.2.1.11	Количество блокированных исходящих зашифрованных пакетов.

Таблица объектов, описывающих ViPNet-клиентов, для которых координатор является сервером IP-адресов (.1.3.6.1.4.1.10812.1.4.1)

.1.3.6.1.4.1.10812.1.4.1.1.1	Шестнадцатеричный идентификатор сетевого узла ViPNet.
.1.3.6.1.4.1.10812.1.4.1.1.2	Имя сетевого узла ViPNet.
.1.3.6.1.4.1.10812.1.4.1.1.3	IP-адрес точки доступа (FirewallIP).
.1.3.6.1.4.1.10812.1.4.1.1.4	TCP/UDP порт точки доступа.

Таблица объектов, описывающих состояние служб iplircfg, failoverd, mftpd, webgui-fcgi-server (.1.3.6.1.4.1.10812.1.7.1):

.1.3.6.1.4.1.10812.1.7.1.1.1	Индекс службы.
.1.3.6.1.4.1.10812.1.7.1.1.2	Имя службы: • Failover — `failoverd`, • Iplir — `iplircfg`, • Mftp — `mftpd`, • Webgui — `webgui-fcgi-server`.
.1.3.6.1.4.1.10812.1.7.1.1.3	Состояние служб: • 0 (unknown) — состояние неизвестно, • 1 (shutdown) — работа службы завершена, • 2 (running) — служба работает.
.1.3.6.1.4.1.10812.1.7.1.1.4	Время работы службы.
.1.3.6.1.4.1.10812.1.8.1.0	Режим работы службы `failoverd`: • 0 (single) — одиночный, • 1 (cluster passive) — режим кластера, узел работает в пассивном режиме, • 2 (cluster active) — режим кластера, узел работает в активном режиме, • 3 (cluster switch) — режим кластера, узел меняет режим работы в текущий момент.
.1.3.6.1.4.1.10812.1.8.2.0	Время последнего переключения службы failover в текущий режим работы.
.1.3.6.1.4.1.10812.1.8.3.0	IP-адрес интерфейса синхронизации другого узла кластера.
.1.3.6.1.4.1.10812.1.8.4.0	Количество сетевых соединений, находящихся в кеше узла кластера.
.1.3.6.1.4.1.10812.1.8.5.0	Системное имя интерфейса синхронизации.

Таблица доступности соединений в канале между узлами кластера (.1.3.6.1.4.1.10812.1.8.6):

X – индекс таблицы

.1.3.6.1.4.1.10812.1.8.6.1.1.X	Индекс таблицы.

OID	Описание
.1.3.6.1.4.1.10812.1.8.6.1.2.X	IP-адрес интерфейса синхронизации.
.1.3.6.1.4.1.10812.1.8.6.1.3.X	Статус доступности узла: • 1 — доступен, • 2 — недоступен.
Таблица с информацией о ПАК (.1.3.6.1.4.1.10812.1.10.1)	
.1.3.6.1.4.1.10812.1.10.1.1	Запись таблицы
.1.3.6.1.4.1.10812.1.10.1.1.1.1	Индекс строки
.1.3.6.1.4.1.10812.1.10.1.1.2.1	Наименование параметра: Serial number
.1.3.6.1.4.1.10812.1.10.1.1.3.1	Серийный номер

SNMP-агент ViPNet Coordinator HW может отправлять оповещения:

Таблица 46. SNMP-оповещения. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.0.1	Запуск службы `iplircfg`.
.1.3.6.1.4.1.10812.1.0.2	Остановка службы `iplircfg`.
.1.3.6.1.4.1.10812.1.0.3	Запуск службы `mftpd`.
.1.3.6.1.4.1.10812.1.0.4	Остановка службы `mftpd`.
.1.3.6.1.4.1.10812.1.0.7	Запуск службы `failoverd`.
.1.3.6.1.4.1.10812.1.0.8	Остановка службы `failoverd`.
.1.3.6.1.4.1.10812.1.0.9	Переключение службы `failoverd` из пассивного режима в активный.
.1.3.6.1.4.1.10812.1.0.10	Запуск службы `webgui`.
.1.3.6.1.4.1.10812.1.0.11	Остановка службы `webgui`.
.1.3.6.1.4.1.10812.1.0.12	Потеря связи с пассивным узлом кластера.
.1.3.6.1.4.1.10812.1.0.13	Восстановление связи с пассивным узлом кластера.
.1.3.6.1.4.1.10812.1.0.16	Изменение IP-адреса и порта точки доступа к ViPNet-клиенту.

MonitoringAgent-MIB

MonitoringAgent-MIB (.1.3.6.1.4.1.10812.4) включает в себя объекты, предназначенные для получения информации о характеристиках SNMP-агента (например, версия, уникальный идентификатор).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 47. SNMP-параметры. MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.3.1	Версия агента мониторинга.
.1.3.6.1.4.1.10812.4.3.2	Идентификатор инсталляции агента мониторинга.

System-MonitoringAgent-MIB

System-MonitoringAgent-MIB (.1.3.6.1.4.1.10812.4.20) включает в себя объекты, предназначенные для получения информации об устройстве, на котором запущен SNMP-агент.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 48. SNMP-параметры. System-MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.20.5.0	Идентификатор устройства в HEX-формате.
.1.3.6.1.4.1.10812.4.20.9.0	Уникальный идентификатор устройства в виде строки.

F

Термины и сокращения

DGD (Dead Gateway Detection)

Технология проверки доступности шлюза путем отправки эхо-запросов через определенный промежуток времени. Если в течение определенного времени ответ не поступил, считается, что данный шлюз недоступен. Данная технология может определять политику маршрутизации в зависимости от доступности шлюзов.

L2OverIP

Технология, которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов сети смогут взаимодействовать друг с другом в одном широковещательном домене. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

MAC-адрес

Уникальный идентификатор, присваиваемый каждому сетевому интерфейсу в сетях Ethernet.

MIME-тип

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

MTU (Maximum Transmission Unit)

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

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.

SNMP (Simple Network Management Protocol)

Интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. Используется в системах сетевого управления для контроля подключенных к сети устройств. Позволяет собирать данные с контролируемого устройства и отправлять их управляющему элементу, на котором выполняется контроль.

SNMP-агент

Программное обеспечение, которое запускается на устройстве и передает информацию о его работе на специальный сервер по протоколу SNMP.

ViPNet Policy Manager

Программа для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Prime

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

Включает в себя основные функциональные модули:

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

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;

- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу сетевых 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 выполняется 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, образованный из нескольких физических интерфейсов Ethernet, объединенных на канальном уровне сетевой модели OSI.

Административная дистанция

Характеристика маршрута. 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 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.

Защищенный узел

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

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 ViPNet Coordinator HW, один из которых (активный) выполняет функции координатора сети ViPNet, а другой (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet Coordinator HW на активном ViPNet Coordinator HW, пассивный ViPNet Coordinator HW переключается в активный режим для выполнения функций. При этом сбойный ViPNet Coordinator HW 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.

Ключ обмена

Симметричный ключ, известный отправителю и получателю зашифрованной информации, которой обмениваются сетевые узлы ViPNet. Используется для зашифрования и расшифрования передаваемых данных.

Координатор (ViPNet-координатор)

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

Маршрут

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

Метрика маршрута

Параметр, определяющий приоритет маршрута передачи IP-трафика.

Область маршрутизации

Одна или несколько IP-сетей, в которых происходит обмен информацией по определенному протоколу, в частности, по протоколу OSPF.

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 целое число в десятичном формате.

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.

Политики безопасности

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

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 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 защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

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.

Транспортный конверт

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

Транспортный сервер MFTP

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

Туннелирование

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

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.