

ViPNet Coordinator IG 5

Настройка с помощью веб-интерфейса

Версия продукта: 5.2.0

ViPNet Coordinator IG100
ViPNet Coordinator IG1000

infotecs

© АО «ИнфоТеКС», 2025

ФРКЕ.467759.003ИС4

Версия продукта 5.2.0

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

Все условия эксплуатации и ограничения на использование ViPNet Coordinator IG приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Coordinator IG.

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение ... **8**
О документе ... 9
Соглашения документа ... 10
Обратная связь ... 11

Глава 1. Работа с веб-интерфейсом ... **12**
Требования к рабочему месту ... 13
Подключение к ViPNet Coordinator IG ... 14

Глава 2. Настройка подключения к сети ... **17**
Настройка сетевых интерфейсов Ethernet ... 18
Назначение дополнительных IP-адресов ... 22
Подключение к сети Wi-Fi ... 23
Подключение к мобильной сети 3G/4G ... 26
Организация обработки трафика из нескольких VLAN ... 32
Использование агрегированных сетевых интерфейсов ... 36
Режимы работы агрегированного интерфейса ... 36
Создание агрегированного интерфейса ... 39
Просмотр ARP-таблицы ... 42
Настройка Power over Ethernet ... 43
Настройка питания внешних устройств ... 43
Настройка проверки внешних устройств ... 45

Глава 3. Настройка VPN ... **47**
Просмотр сведений о сетевых узлах ViPNet ... 48
Просмотр и изменение списка туннелируемых узлов ... 51
Настройка доступа к туннелируемым узлам в одной подсети ... 53
Настройка туннелирования на канальном уровне по технологии L2OverIP ... 55
Общие сведения об L2OverIP ... 55
Особенности реализации L2OverIP в ViPNet Coordinator IG ... 56
Настройка L2OverIP ... 56

Глава 4. Настройка фильтрации трафика ... **59**
Настройка сетевых фильтров ... 60
Типы трафика ... 60

Принципы фильтрации трафика 61
Общие сведения о сетевых фильтрах 64
Группы объектов 66
Системные группы объектов 67
Пользовательские группы объектов по умолчанию 68
Просмотр групп объектов 68
Создание и изменение групп объектов 69
Группа сетевых узлов ViPNet 70
Группа IP-адресов 71
Группа интерфейсов 72
Группа протоколов 73
Группа расписаний 74
Просмотр сетевых фильтров 76
Создание и изменение сетевых фильтров 78
Настройка регистрации IP-пакетов при срабатывании фильтров 80
Настройка фильтрации промышленных протоколов 82
Общие сведения о фильтрации промышленных протоколов 82
Основные принципы фильтрации промышленных протоколов 83
Принципы фильтрации протокола Modbus на прикладном уровне 84
Принципы фильтрации протокола МЭК 60870-5-104 на прикладном уровне 85
Создание и изменение наборов правил фильтрации промышленного протокола 86
Просмотр наборов правил промышленного протокола 92
Настройка прокси-сервера 93
Общие сведения о работе прокси-сервера 93
Настройка основных параметров прокси-сервера 94
Настройка правил контент-фильтрации трафика 97
Настройка антивирусной проверки трафика 98

Глава 5. Настройка правил трансляции адресов 100
Трансляция сетевых адресов (NAT) 101
Трансляция адреса назначения 102
Трансляция адреса источника 103
Просмотр правил трансляции адресов 104
Создание и изменение правил трансляции адресов 106

Глава 6. Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP 108
О прикладных протоколах 109
Настройка параметров обработки прикладных протоколов 111
Особенности обработки прикладных протоколов DNS, FTP, SIP и H.323 113

Глава 7. Настройка сетевых служб 117
Настройка DHCP-сервера 118
Настройка DHCP-relay 121
Настройка DNS-сервера 123
Настройка NTP-сервера 125
Настройка точки доступа к сети Wi-Fi 128
Настройка шлюза Modbus 130
Настройка интерфейса GPIO 133

Глава 8. Настройка маршрутизации 136
Общие сведения о маршрутизации 137
Принципы маршрутизации 138
Просмотр таблицы маршрутизации 142
Настройка статической маршрутизации 143
Добавление статических маршрутов 143
Настройка балансировки IP-трафика 145
Настройка маршрутов протоколов DHCP и PPP 147
Настройка административной дистанции для маршрутов DHCP-сервера 147
Настройка метрики для маршрутов DHCP-сервера 148
Настройка метрики для маршрутов PPP-протокола 150
Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола 150
Настройка OSPF 152
Общие сведения о протоколе OSPF 152
Настройка протокола OSPF 154
Настройка перераспределения маршрутов 158
Настройка BGP 160
Общие сведения о протоколе BGP 160
Настройка маршрутизатора 161
Настройка соседей 161
Настройка анонсирования подсетей 164
Мониторинг состояния маршрутизатора 166
Настройка функции MultiWAN 168
Настройка политик маршрутизации 169
Настройка проверки состояния шлюзов (DGD) 171

Глава 9. Настройка системных параметров 175
Настройка даты и времени 176
Переключение режимов работы межсетевого экрана 177
Настройка расписания перезагрузки 179

Просмотр лицензии ... 181
Просмотр серийного номера ... 182

Глава 10. Настройка параметров безопасности ... 183
Управление локальными учётными записями ... 184
Обновление справочников и ключей ... 186
Предотвращение подбора пароля учетных записей ... 187
Управление ключами локального SSH-сервера ... 188
Настройка подключения с помощью веб-интерфейса ... 189
Обновление ключей по истечении срока их действия ... 192

Глава 11. Резервное копирование и восстановление настроек ... 193
Способы резервирования и восстановления настроек ... 194
Управление индивидуальной конфигурацией ... 195
Резервное копирование индивидуальной конфигурации ... 196
Восстановление из резервной копии индивидуальной конфигурации ... 198
Управление универсальной конфигурацией ... 200
Экспорт универсальной конфигурации ... 201
Импорт настроек универсальной конфигурации ... 202

Глава 12. Работа с журналами ... 206
Настройка журналов ... 207
Журнал IP-пакетов ... 210
Журнал пакетов промышленных протоколов ... 214
Журнал аудита ... 217
Журнал СКЗИ ... 219
Журнал MFTP ... 221
Журнал DNS-запросов ... 223
Системный журнал ... 225

Глава 13. Мониторинг состояния и просмотр статистики ... 227
Просмотр состояния ... 228
Мониторинг по SNMP ... 230
Настройка SNMP-агента ... 231
Мониторинг кластера ... 238
Просмотр статистики передачи данных ... 242
Просмотр статистики IP-пакетов ... 243

Приложение А. Сетевые фильтры по умолчанию ... 244

Приложение B. Пользовательские группы протоколов по умолчанию **249**

Приложение C. События журнала IP-пакетов **253**

Приложение D. События системного журнала и журнала аудита **259**

Приложение E. Базы управляющей информации (MIB) для протокола SNMP **272**

MIB-II System 272
IF-MIB 276
IP-MIB 278
IP-FORWARD-MIB 284
Ethernet-Like MIB 288
TCP-MIB 289
UDP-MIB 292
HOST-RESOURCES-MIB 293
NOTIFICATION-LOG-MIB 297
UCD-SNMP-MIB 298
UCD-DISKIO-MIB 300
NET-SNMP-MIB 301
SNMP-MPD-MIB 304
SNMP-TARGET-MIB 305
SNMP-USER-BASED-SM-MIB 305
SNMP-VIEW-BASED-ACM-MIB 306
SNMP-FRAMEWORK-MIB 308
VIPNET-MIB 309
VIPNETMULTIWAN-MIB 311
MonitoringAgent-MIB 313
System-MonitoringAgent-MIB 313

Приложение F. Термины и сокращения **314**



Введение

О документе 9

Соглашения документа 10

Обратная связь 11

О документе

В документе описаны основные сценарии настройки программно-аппаратного комплекса ViPNet Coordinator IG 5 (далее — ViPNet Coordinator IG) с помощью веб-интерфейса.



Внимание! Веб-интерфейс доступен только в исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000. Для управления ViPNet Coordinator IG10 используйте командный интерпретатор (см. документ «Настройка с помощью командного интерпретатора»).

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.

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

Работа с веб-интерфейсом

Требования к рабочему месту 13

Подключение к ViPNet Coordinator IG 14

Требования к рабочему месту



Внимание! Удалённое подключение к ViPNet Coordinator IG разрешено только с узлов защищённой сети, для которых в ViPNet Prime настроена связь с ViPNet Coordinator IG.

- Установите разрешение экрана 1360x768 пикселей или выше.
- Используйте браузеры Microsoft Edge, Google Chrome или Mozilla Firefox последних версий.
- В настройках браузера разрешите Cookie и JavaScript и добавьте сайт в надёжные расположения.
- После обновления ПО ViPNet Coordinator IG очистите кеш браузера, иначе возможны проблемы подключения с помощью веб-интерфейса.
- Для аутентификации централизованных пользователей установите сертифицированную версию ViPNet PKI Client (при установке выберите компонент TLS Unit).
- Для защиты рабочего места установите средство антивирусной защиты.

Подключение к ViPNet Coordinator IG

Внимание! Веб-интерфейс доступен только в исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000. Для управления ViPNet Coordinator IG10 используйте командный интерпретатор (см. документ «Настройка с помощью командного интерпретатора»).

Предварительная настройка

По умолчанию встроенный межсетевой экран блокирует доступ к ViPNet Coordinator IG по HTTP/HTTPS. Чтобы разрешить доступ, создайте фильтр защищённой сети с помощью командного интерпретатора:

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

где `<идентификатор узла>` — идентификатор узла в сети ViPNet, с которого вы подключаетесь к ViPNet Coordinator IG.

О том, как использовать командный интерпретатор см. в документе «Настройка с помощью командного интерпретатора».

Подключение

1 В браузере введите: `https://<IP-адрес ViPNet Coordinator IG>:8080`

Несмотря на предупреждение о том, что самоподписанный сертификат не является доверенным, перейдите по IP-адресу.

2 Для входа под локальной учётной записью:

2.1 Введите имя учётной записи (`user` или `admin`) и пароль.

2.2 Нажмите **Войти**.

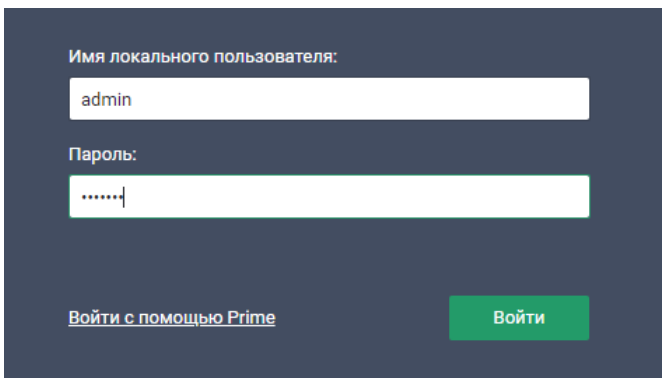


Рисунок 1. Вход под локальной учётной записью по паролю

Примечание. Для предотвращения подбора пароля учётных записей реализована прогрессивная задержка ввода пароля и оповещение о попытках подбора пароля.

3 Для входа под централизованной учётной записью:

3.1 Если в защищённой сети используется аутентификация по паролю:

3.1.1 Нажмите **Войти с помощью Prime**.

3.1.2 Введите имя централизованной учётной записи и пароль.

3.1.3 Нажмите **Войти**.

3.2 Если в защищённой сети используется аутентификация по сертификату:

3.2.1 Подключите USB-токен с сертификатом пользователя ViPNet Prime к сетевому узлу, с которого вы подключаетесь к ViPNet Coordinator IG.

3.2.2 Нажмите **Войти с помощью Prime**.

3.2.3 В окне ViPNet PKI Client выберите сертификат и введите PIN-код пользователя USB-токена.

Примечание.

- Если вы введёте некорректный PIN-код несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен).
- При ошибке аутентификации, например когда ключ на USB-токене не соответствует сертификату или нарушена целостность сертификата, учётная запись блокируется на 10 минут.

В обоих случаях издайте новый сертификат пользователя ViPNet Coordinator IG (см. документ «Настройка с помощью командного интерпретатора», раздел «Издание сертификатов»).

3.2.4 Нажмите **Войти**.

Внимание! Не отключайте USB-токен во время работы с ViPNet Coordinator IG. Иначе сессия будет завершена.

Начальная страница

При успешной аутентификации будет открыта страница **Состояние системы**:

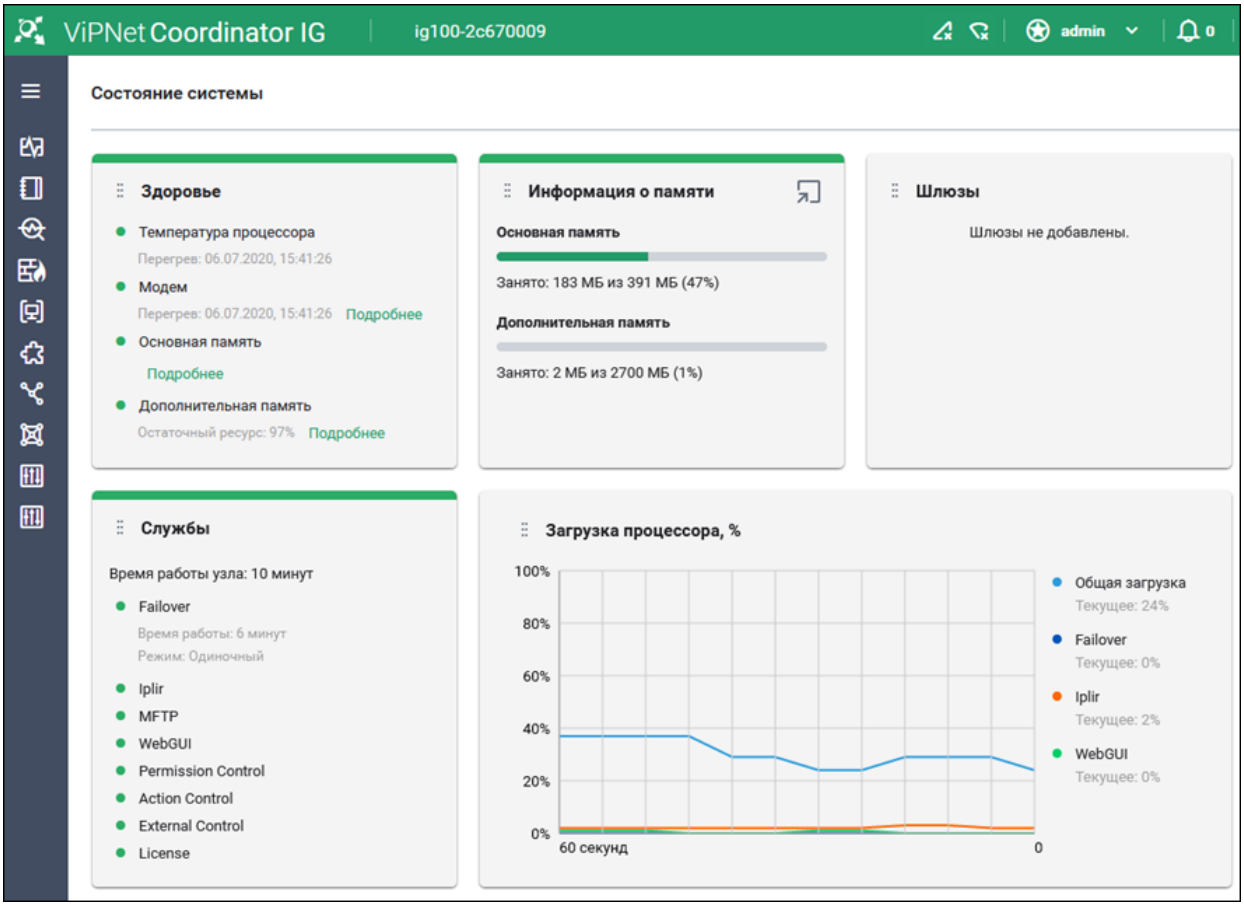


Рисунок 2. Начальная страница при входе под администратором

Завершение сессии

По окончании работы завершите сессию — нажмите **Имя учетной записи** > **Выйти**. Иначе сессия останется активной даже при закрытии вкладки или окна браузера, и завершится автоматически по истечении допустимого времени неактивности сессии (по умолчанию — 10 минут). Также сессия завершится автоматически при обнаружении попытки межсайтовой подделки запроса.

Настройка подключения

Вы можете изменить параметры подключения к ViPNet Coordinator IG или перевыпустить самоподписанный сертификат, который используется для HTTPS-соединения. Подробнее см. Настройка подключения с помощью веб-интерфейса.

Если на ViPNet Coordinator IG запущен прокси-сервер в обычном режиме, то в настройках параметров локальной сети компьютера:

1. Укажите IP-адрес и порт прокси-сервера.
2. Исключите использование прокси-сервера для локальных адресов, в том числе адресов ViPNet Coordinator IG.



2

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet 18

Назначение дополнительных IP-адресов 22

Подключение к сети Wi-Fi 23

Подключение к мобильной сети 3G/4G 26

Организация обработки трафика из нескольких VLAN 32

Использование агрегированных сетевых интерфейсов 36

Просмотр ARP-таблицы 42

Настройка Power over Ethernet 43

Настройка сетевых интерфейсов Ethernet

Примечание. Настройка сетевых интерфейсов в кластере невозможна.

1 Выберите **Сетевые настройки** > **Сетевые интерфейсы**.

2 Нажмите , чтобы включить режим редактирования.

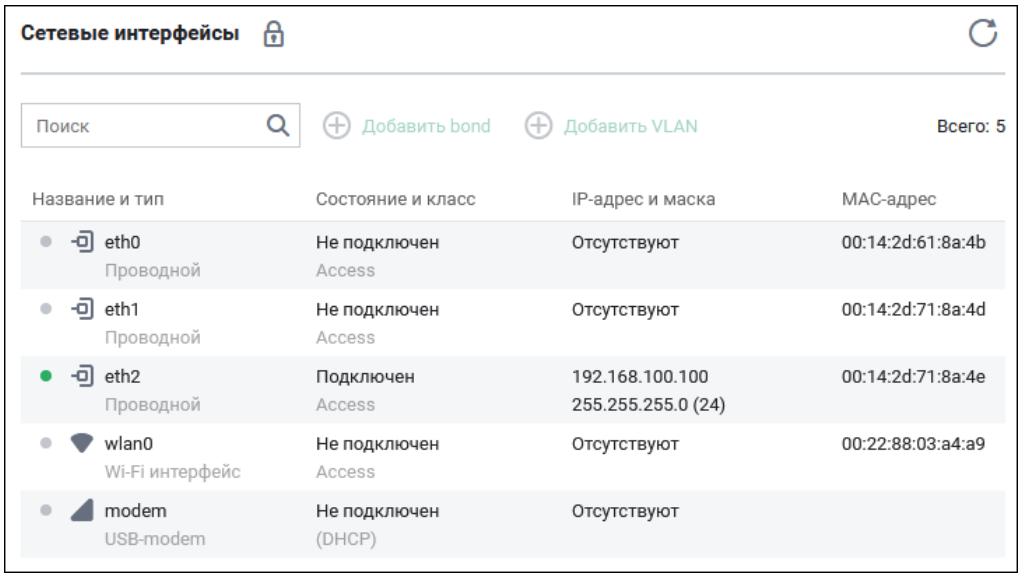


Рисунок 3. Состояние и параметры сетевых интерфейсов

3 Выберите проводной интерфейс, который вы хотите настроить (сетевым интерфейсам Ethernet, установленным в системе, присвоены имена `eth0`, `eth1` и так далее).

Справа откроется панель с настройками.

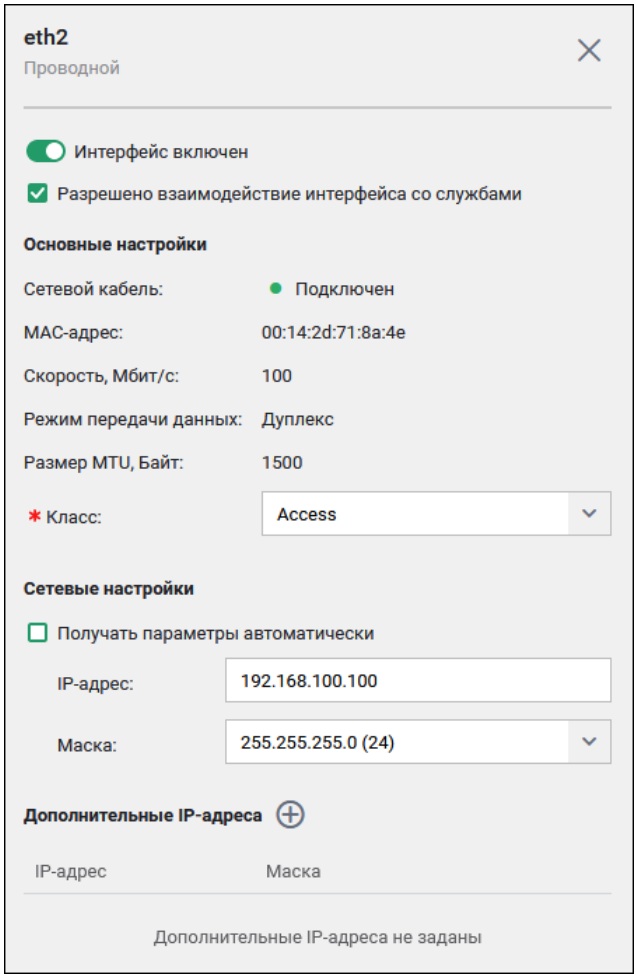


Рисунок 4. Настройка сетевого интерфейса Ethernet

4 По умолчанию для передачи данных через интерфейс используется размер MTU, равный 1500 байт. В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 вы можете изменить размер MTU, чтобы оптимизировать передачу данных через интерфейс. Для этого в поле **Размер MTU в байтах** задайте значение MTU из диапазона 1280–9000 байт.

Примечание. Для исполнения ViPNet Coordinator IG100 I4 задавайте MTU в диапазоне 1280–1518.

Чтобы вернуть значение по умолчанию, нажмите ⮌.

5 Задайте класс сетевого интерфейса (по умолчанию — `Access`):

- Если требуется, чтобы интерфейс обрабатывал трафик из нескольких VLAN (см. Организация обработки трафика из нескольких VLAN), назначьте ему класс `Trunk`.
- Если вы хотите объединить этот интерфейс с другими в составе агрегированного интерфейса, назначьте ему класс `Slave`.

6 В разделе **Сетевые настройки** выполните одно из действий:

- Чтобы присвоить интерфейсу статический IP-адрес, заполните поля **IP-адрес** и **Маска**.

Примечание. При задании IP-адреса действуют ограничения:

- Нельзя задавать IP-адрес 0.*.*.*.
- Нельзя задавать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов нельзя задавать IP-адреса, относящиеся к одной подсети или широковещательному каналу (broadcast). Если интерфейс получил от DHCP-сервера маршрут по умолчанию, который уже задан на другом интерфейсе, то такой интерфейс не будет использоваться при маршрутизации.

Вы можете задать дополнительные IP-адреса интерфейса. Для этого нажмите ⊕. Подробнее см. Назначение дополнительных IP-адресов.

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

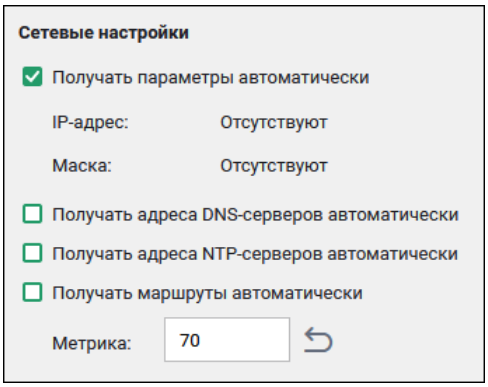


Рисунок 5. Настройка режима получения параметров интерфейса от DHCP-сервера

Выберите получаемые параметры:

- **Получать адреса DNS-серверов автоматически**;
- **Получать адреса NTP-серверов автоматически**;
- **Получать маршруты автоматически**.

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка маршрутов протоколов DHCP и PPP). Чтобы просмотреть параметры, заданные для режима DHCP на всех интерфейсах, см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

  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 её в поле **Метрика**. Подробнее о настройке метрики см. в разделе Настройка метрики для маршрутов DHCP-сервера. Чтобы вернуть значение по умолчанию, нажмите ⮌.

7 Включите интерфейс.

8 Нажмите **Сохранить**.

9 Нажмите .

Примечание. Если хотя бы на одном используемом интерфейсе Ethernet задано автоматическое получение маршрутов от DHCP-сервера, то в разделе **Маршрутизация** > **Маршрутизация** проверьте, что хотя бы один маршрут по умолчанию получен. Если такого маршрута нет, задайте статический маршрут по умолчанию.

Назначение дополнительных IP-адресов

Дополнительные IP-адреса могут быть назначены сетевому интерфейсу со статическим IP-адресом и классом `Access`. 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 IG — 128 (как физических, так и виртуальных, включая loopback).

Чтобы задать дополнительные IP-адреса:

1. Выберите **Сетевые настройки** > **Сетевые интерфейсы**.
2. Нажмите , чтобы включить режим редактирования.
3. Выберите нужный интерфейс.
4. В разделе **Дополнительные IP-адреса** нажмите .
5. Задайте IP-адрес и маску подсети.
6. Нажмите **Сохранить**.

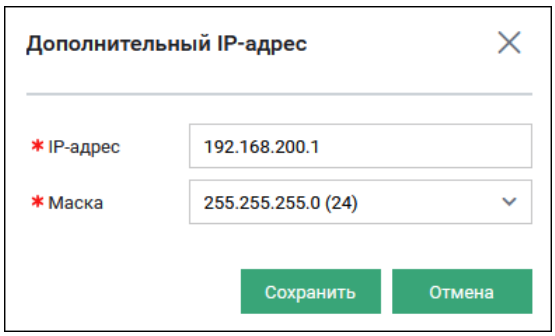


Рисунок 6. Назначение дополнительных IP-адресов

7. Чтобы добавить ещё один дополнительный IP-адрес, повторите шаги 4–6.
8. Нажмите .

Подключение к сети Wi-Fi

Примечание.

- Подключение к сети Wi-Fi возможно только в исполнениях ViPNet Coordinator IG со встроенным модулем Wi-Fi.
- Беспроводные сети, такие как Wi-Fi и 3G/4G, менее надежны, чем проводные. Воздействие различного рода помех на беспроводные сети может приводить к потерям среди IP-пакетов и снижению скорости передачи данных.
- ViPNet Coordinator IG может работать в одном из режимов: в режиме клиента или точки доступа Wi-Fi (см. Настройка точки доступа к сети Wi-Fi).

1 Выберите **Сетевые настройки > Сетевые интерфейсы**.

2 Нажмите , чтобы включить режим редактирования.

3 Выберите интерфейс `wlan0`.

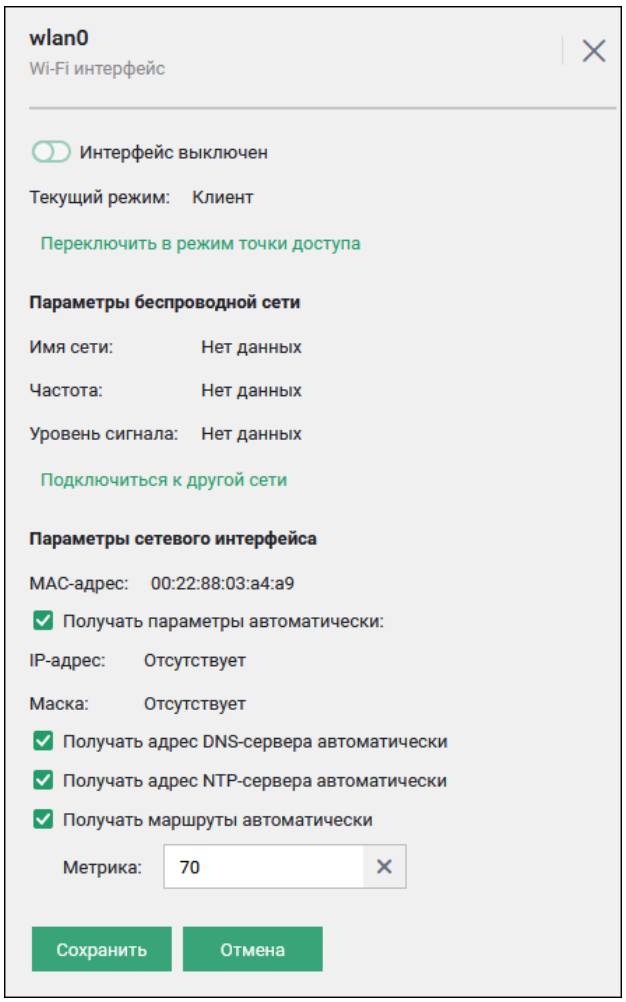


Рисунок 7. Настройка интерфейса Wi-Fi

4 Выключите интерфейс, если он активен.

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

6 В разделе **Параметры сетевого интерфейса** выполните одно из действий:

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

  Выберите получаемые параметры:

  - **Получать адрес DNS-сервера автоматически**;
  - **Получать адрес NTP-сервера автоматически**;
  - **Получать маршруты автоматически**.

    Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка маршрутов протоколов DHCP и PPP).

    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 её в поле **Метрика**. Подробнее о настройке метрики см. в разделе Настройка метрики для маршрутов DHCP-сервера. Чтобы вернуть значение по умолчанию, нажмите .

- Чтобы присвоить интерфейсу статический IP-адрес, снимите флажок с параметра **Получать параметры автоматически** и заполните поля **IP-адрес** и **Маска**.

7 Нажмите **Сохранить**.

8 В разделе **Параметры беспроводной сети** нажмите **Подключиться к другой сети**

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

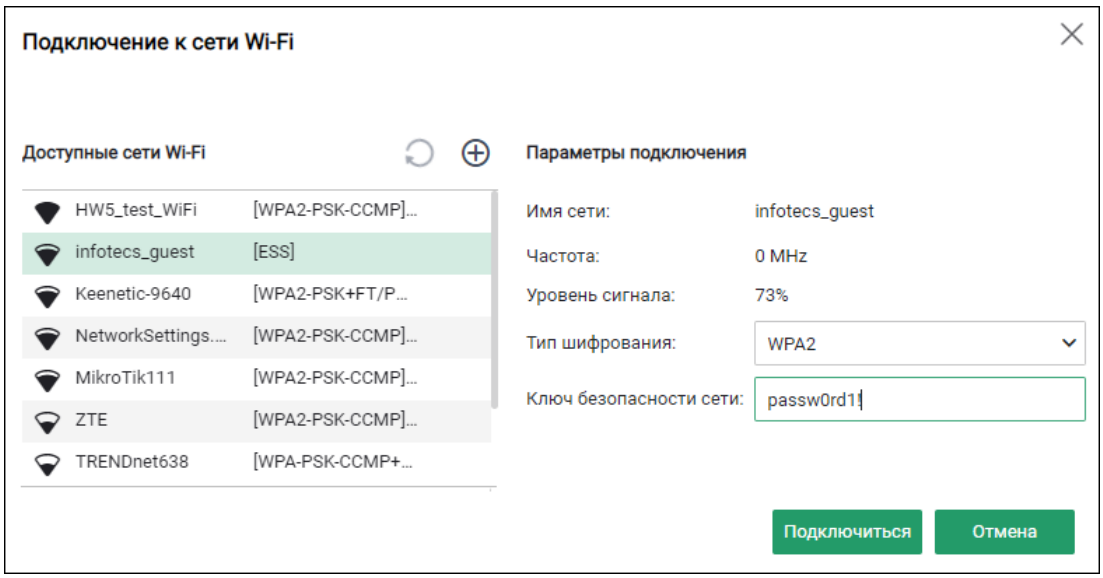


Рисунок 8. Подключение к сети Wi-Fi

10 Если сеть защищена, укажите тип шифрования и введите пароль в поле **Ключ безопасности сети**.

11 Нажмите **Подключиться**.

12 Если сеть Wi-Fi скрыта, но вы знаете её имя и параметры доступа к ней:

12.1 Нажмите  .

12.2 Введите имя сети, тип шифрования и пароль доступа к ней.

12.3 Нажмите **Подключиться**.

13 Включите  интерфейс.

14 Нажмите  .



Внимание! Модуль Wi-Fi в ViPNet Coordinator IG работает в режимах 802.11b и 802.11g. Если связь с точкой доступа Wi-Fi обрывается, настройте точку доступа на использование только указанных выше режимов. Перед новой попыткой подключения перезагрузите ViPNet Coordinator IG.

Если ViPNet Coordinator IG подключён к сети Wi-Fi, на панели вверху отображается значок  . При наведении курсора на этот значок отображается уровень сигнала Wi-Fi.

Вы можете настроить запись уровня сигнала Wi-Fi в системный журнал (см. документ «Настройка с помощью командного интерпретатора»).

Подключение к мобильной сети 3G/4G

Примечание.

- Подключение к сети 3G/4G возможно только в исполнениях ViPNet Coordinator IG со встроенным модемом.
- Беспроводные сети, такие как Wi-Fi и 3G/4G, менее надежны, чем проводные. Воздействие различного рода помех на беспроводные сети может приводить к потерям среди IP-пакетов и снижению скорости передачи данных.
- В исполнениях ViPNet Coordinator IG с поддержкой двух SIM-карт вы можете выбрать SIM-карту, которая будет использоваться при включении модема. Подробнее см. документ «Настройка с помощью командного интерпретатора».

Подключение к мобильной сети выполняется по протоколу PPP.

Для подключения к интернету вы можете пользоваться услугами любого оператора мобильной связи. Для этого приобретите SIM-карту и установите её в соответствующий разъем ViPNet Coordinator IG (см. документ «Описание аппаратных платформ», раздел «Установка SIM-карты»).

Примечание. Тариф мобильного оператора должен предусматривать использование SIM-карты в модемах.

Автоматическое подключение к мобильной сети

Чтобы подключиться к мобильной сети:

1. Выберите **Сетевые настройки** > **Сетевые интерфейсы**.
2. Нажмите , чтобы включить режим редактирования.
3. Выберите интерфейс `modem`.

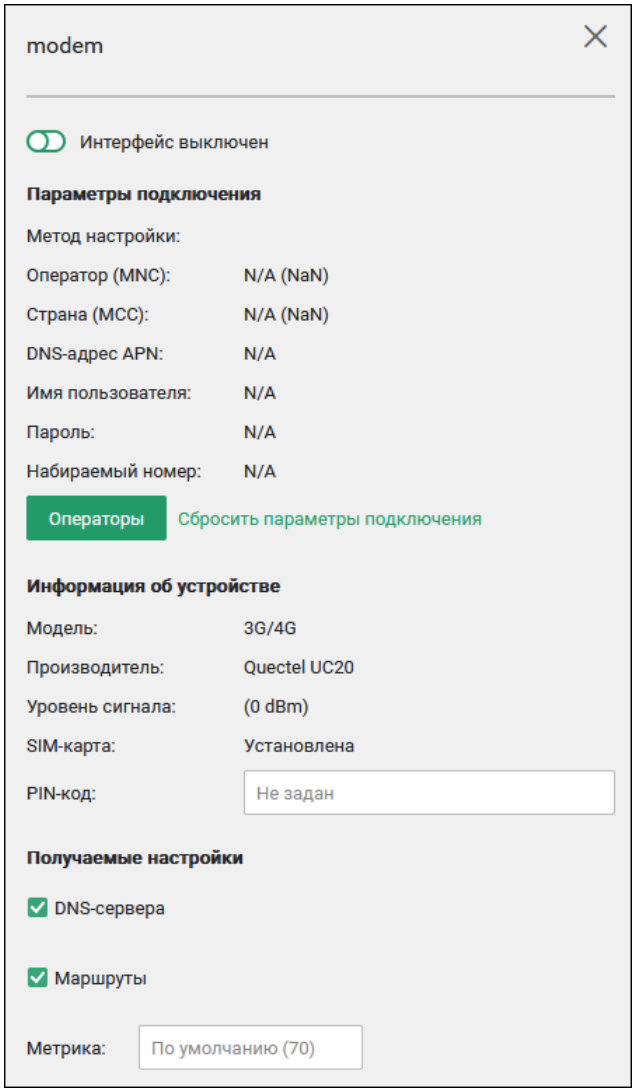


Рисунок 9. Настройка 3G/4G-модема

4 Выключите modem, если он включён.

5 Если ваша SIM-карта защищена PIN-кодом, введите его в поле **ПИН**.

6 При первом подключении модема к мобильной сети:

- на ViPNet Coordinator IG добавляется новый маршрут по умолчанию, в котором в качестве шлюза указан адрес узла сети вашего мобильного оператора;
- для нового маршрута задана метрика по умолчанию (см. Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола);
- добавляется IP-адрес DNS-сервера.

Вы можете изменить эти параметры в разделе **Получаемые настройки**:

- Если вы не хотите добавлять адрес DNS-сервера от вашего мобильного оператора, снимите флажок **Получать адреса DNS-серверов автоматически**.
- Если вы не хотите добавлять маршрут по умолчанию, снимите флажок **Получать маршруты автоматически**.

- Если вы хотите задать для добавляемого маршрута другую метрику, укажите её в поле **Метрика**. Подробнее см. Настройка метрики для маршрутов PPP-протокола.

7 Если вы ввели или изменили PIN-код, или изменили параметры в разделе **Получаемые настройки**, нажмите **Сохранить**.

8 Включите  интерфейс модема.

После включения модема ViPNet Coordinator IG проверяет SIM-карту и PIN-код. Это может занять несколько минут. Если в результате проверки переключатель модема остался в выключенном положении, значит PIN-код неверный или SIM-карта повреждена. Устраните причину ошибки и повторно включите интерфейс модема.

9 Нажмите  .

В результате мобильный оператор определится автоматически, и подключение к мобильной сети 3G/4G будет установлено. IP-адрес интерфейса появится на странице **Сетевые интерфейсы**.

Проверка и решение проблемы подключения

Если ViPNet Coordinator IG подключён к мобильной сети, вверху отображается значок  . При наведении курсора на этот значок, отображается уровень сигнала. Если модем включён, но соединение с сетью 3G/4G не устанавливается, обновите страницу в браузере.

Если ViPNet Coordinator IG не подключается к мобильной сети:

1 Запросите у вашего оператора мобильной связи настройки для подключения к мобильной сети.

2 Выберите оператора из списка мобильных операторов. Если вы не нашли оператора с нужными настройками, добавьте нового оператора.

Выбор мобильного оператора вручную

1 Нажмите  .

2 Выберите интерфейс `modem`.

3 Выключите  `modem`.

4 Нажмите **Операторы**.

5 Выберите оператора с необходимыми сетевыми настройками.

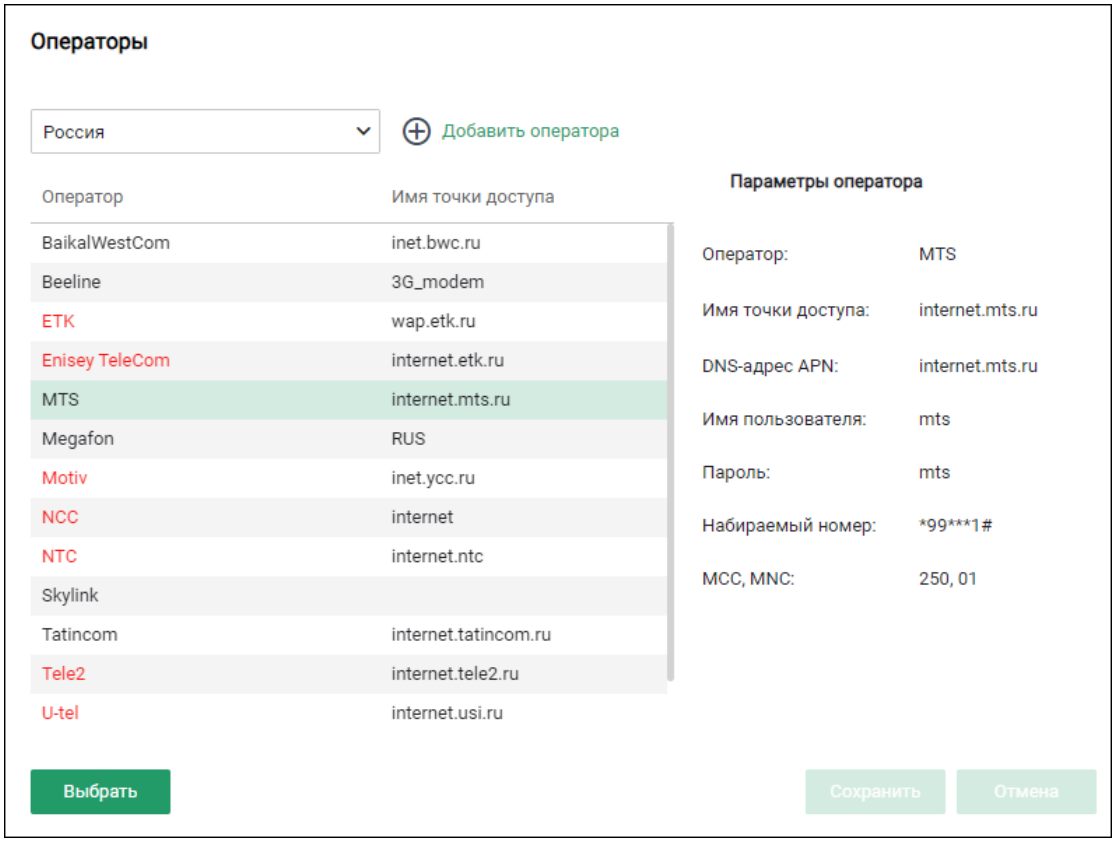


Рисунок 10. Ручной выбор оператора мобильной связи

6 Нажмите **Выбрать**.

7 Нажмите **Сохранить**.

8 Включите modem.

9 Нажмите .

Добавление нового мобильного оператора

1 Нажмите .

2 Выберите интерфейс modem.

3 Выключите modem.

4 Нажмите **Операторы**.

5 Нажмите **Добавить оператора**.

6 Выберите страну, введите наименование оператора и имя точки доступа.

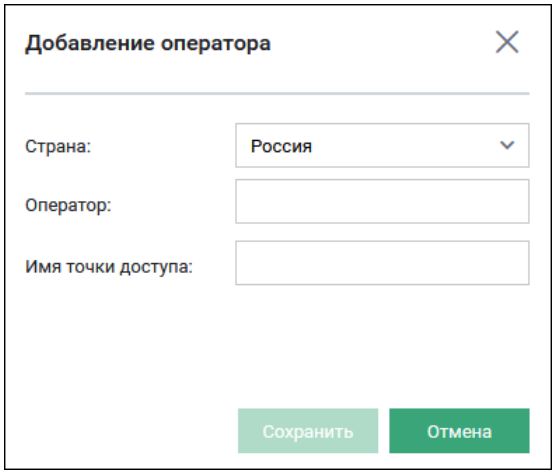


Рисунок 11. Добавление нового оператора мобильной связи

7 Нажмите **Сохранить**.

8 Выберите добавленного оператора и введите настройки подключения к мобильной сети.

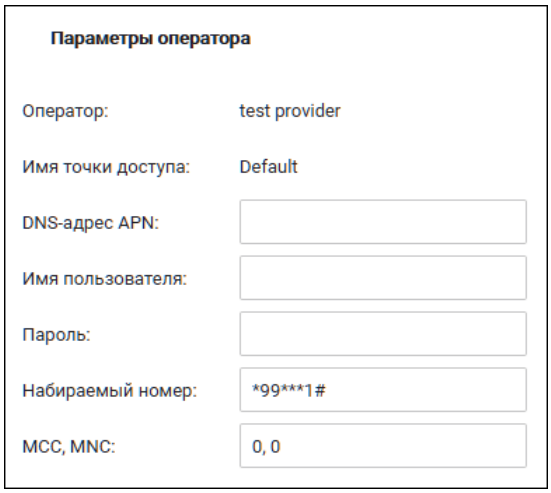


Рисунок 12. Задание параметров подключения к мобильной сети для нового оператора мобильной связи

9 Нажмите **Сохранить**, затем **Выбрать**.

10 Нажмите **Сохранить**.

11 Включите modem.

12 Нажмите .

Сброс настроек

Чтобы удалить всех мобильных операторов, добавленных пользователем, и включить режим автоматического определения оператора:

1 Нажмите .

2 Выберите интерфейс modem.

3 Выключите  modem.

4 Нажмите **Сбросить параметры подключения**.

Теперь вы можете включить интерфейс модема, и оператор мобильной сети вместе с настройками подключения будут определены автоматически.

Организация обработки трафика из нескольких VLAN

Вы можете использовать ViPNet Coordinator IG для обработки трафика в физической локальной сети, разделённой 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).

1. Подключите один из сетевых интерфейсов ViPNet Coordinator IG к коммутатору, объединяющему виртуальные сети (далее — родительский интерфейс).
2. Выберите **Сетевые настройки** > **Сетевые интерфейсы**.
3. Нажмите , чтобы включить режим редактирования.
4. Выберите родительский интерфейс. Справа появится панель с настройками.
5. Снимите флажок **Разрешено взаимодействие интерфейса со службами**.

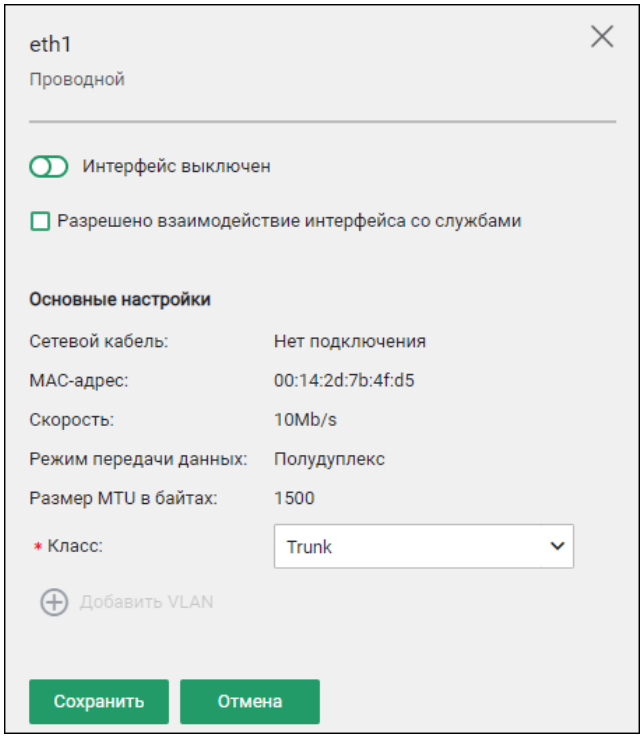


Рисунок 13. Настройка родительского интерфейса

6. В списке **Класс** выберите `Trunk`.
7. Нажмите **Сохранить**.
8. Повторно выберите этот же интерфейс.
9. Нажмите **Добавить VLAN**.

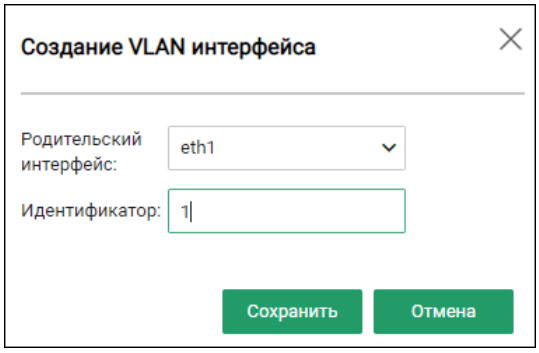


Рисунок 14. VLAN-интерфейса

9.1 В списке **Родительский интерфейс** отображаются интерфейсы класса `Trunk`. Если таких интерфейсов несколько, выберите один.

9.2 В поле **Идентификатор** введите номер создаваемого виртуального интерфейса. Виртуальному интерфейсу будет присвоено имя в формате:

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

Примечание.

- В исполнении ViPNet Coordinator IG10 I2 номера виртуальных интерфейсов 4093–4094 зарезервированы для служебного использования на физических интерфейсах `eth0` и `eth1`.
- В исполнении ViPNet Coordinator IG100 I4 номера виртуальных интерфейсов 4086–4094 зарезервированы для служебного использования на всех физических интерфейсах.
- Максимальное количество сетевых интерфейсов в ViPNet Coordinator IG — 128 (как физических, так и виртуальных, включая loopback).

9.3 Нажмите **Сохранить**.

Будет создан виртуальный интерфейс для одной из виртуальных сетей, находящихся за коммутатором. Он появится в списке всех сетевых интерфейсов.

10 В списке интерфейсов выберите созданный виртуальный интерфейс и настройте его:

10.1 Чтобы включить прохождение трафика через виртуальный интерфейс, выберите **Разрешено взаимодействие интерфейса со службами**.

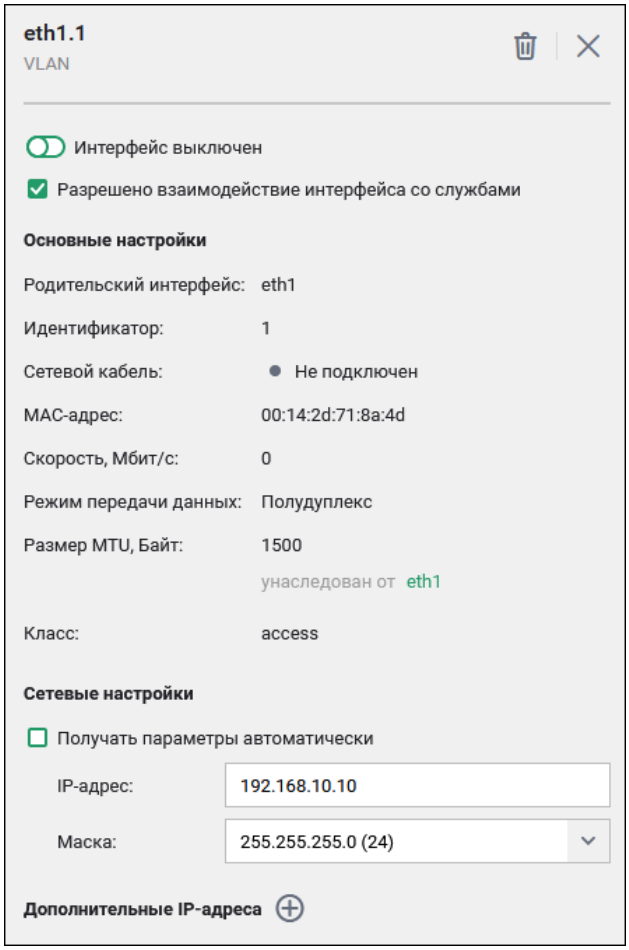


Рисунок 15. Настройка VLAN-интерфейса

10.2 В разделе **Сетевые настройки** выполните одно из действий:

- Чтобы присвоить интерфейсу статический IP-адрес, заполните поля **IP-адрес** и **Маска**.

  Вы можете задать дополнительные IP-адреса интерфейса. Для этого нажмите ⊕. Подробнее см. Назначение дополнительных IP-адресов.

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

  Выберите параметры, получаемые от DHCP-сервера: адреса DNS-серверов, адреса NTP-серверов, маршруты.

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка маршрутов протоколов DHCP и PPP). Чтобы просмотреть параметры, заданные для режима DHCP на всех интерфейсах, см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

  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 её в поле **Метрика**. Подробнее о настройке метрики см. в разделе Настройка метрики для маршрутов DHCP-сервера.

10.3 Нажмите **Сохранить**.

11 Чтобы создать виртуальные интерфейсы для других сетей, повторите шаги 9–10.

12 Для передачи данных через виртуальный интерфейс используется размер MTU, унаследованный от родительского интерфейса. В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 вы можете изменить размер MTU, чтобы оптимизировать передачу данных через интерфейс. Для этого выберите родительский интерфейс и в поле **Размер MTU в байтах** задайте новое значение из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию (1500 байт), нажмите  .

13 Включите  родительский интерфейс и нажмите **Сохранить**.

Созданные виртуальные интерфейсы включатся автоматически.

14 Нажмите  .

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

Использование агрегированных сетевых интерфейсов

Чтобы повысить надежность ваших каналов передачи данных, вы можете объединить несколько физических сетевых интерфейсов ViPNet Coordinator IG в один логический — агрегированный интерфейс. При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

Например, вы можете объединить два или три сетевых интерфейса в один агрегированный. Трафик будет передаваться через один из подчинённых физических интерфейсов. Если он выйдет из строя, трафик будет передаваться через другой подчинённый интерфейс.

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

Режимы работы агрегированного интерфейса

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

Таблица 1. Режимы работы агрегированного интерфейса

Режим	Описание
`balance-rr`	Режим, подходящий как для балансировки нагрузки на подчинённых интерфейсах, так и для защиты от сбоев. Может применяться в сетях с простой топологией. В этом режиме исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчинённые физические интерфейсы поочерёдно: первый пакет отправляется через один подчинённый интерфейс, второй пакет — через следующий подчинённый интерфейс и так далее.
`balance-xor`	Режим, предназначенный для защиты от сбоев и распределения нагрузки таким образом, чтобы пакеты от одного и того же отправителя к одному и тому же получателю всегда отправлялись через один и тот же подчинённый интерфейс. В этом режиме для определения подчинённого 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. Вы можете выбрать один из следующих алгоритмов: • `layer2` — в алгоритме используются MAC-адреса отправителя и получателя пакета, таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами;

Режим	Описание
	• `layer2+3` — в алгоритме используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протокола IPv4), таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами и IP-адресами; • `layer3+4` — в алгоритме используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии), таким образом, одинаковыми считаются сетевые узлы с одинаковыми IP-адресами, а также портами TCP или UDP.
`balance-tlb`	Режим для балансировки нагрузки на подчинённых интерфейсах используется при передаче большого числа пакетов разного размера, когда более простые режимы не распределяют нагрузку равномерно. В этом режиме учитывается размер исходящих пакетов, переданных через каждый из подчинённых физических интерфейсов, и на основе этого выполняется выбор интерфейса, через который будет передан пакет, попавший на агрегированный интерфейс. **Примечание.** Для работы агрегированного интерфейса в режиме `balance-tlb` необходимо, чтобы все подчинённые физические интерфейсы были подключены к сети через коммутатор.

Режим	Описание
802.3ad	Режим динамического агрегирования с использованием протокола LACP для комплексной балансировки нагрузки. В этом режиме агрегированный интерфейс работает следующим образом: • Среди подчинённых физических 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 агрегатора, задаваемым с помощью списка **Режим агрегатора** после создания агрегированного интерфейса. Вы можете задать один из приведённых ниже режимов выбора агрегатора: stable — режим, при котором первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчинённых физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчинённых интерфейсов текущего агрегатора. bandwidth — режим, при котором первоначально выбирается агрегатор с наибольшей пропускной способностью подчинённых физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчинённых физических интерфейсов, в агрегаторах производится перегруппировка подчинённых физических интерфейсов и выполняется выбор нового агрегатора. count — режим, при котором первоначально выбирается агрегатор с наибольшим количеством подчинённых физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчинённых физических интерфейсов, в агрегаторах производится перегруппировка подчинённых физических интерфейсов и выполняется выбор нового агрегатора. • Внутри агрегатора подчинённый физический 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 подчинённого интерфейса даже в том случае, если этот интерфейс подключён к другому сетевому узлу не напрямую. **Примечание.** Механизм MC-LAG (MLAG) в данном режиме не поддерживается. Поэтому физические порты разных ViPNet Coordinator IG нельзя использовать в одном агрегированном интерфейсе.
active-backup	Режим, предназначенный для защиты от сбоев, но не для балансировки нагрузки на подчинённых физических интерфейсах. В этом режиме один из подчинённых физических интерфейсов назначается основным (автоматически или явно с помощью списка **Основной интерфейс** после создания агрегированного интерфейса), и все исходящие пакеты отправляются через него. При этом, в случае сбоя на основном подчинённом интерфейсе пакеты будут отправляться через другие подчинённые интерфейсы.

Режим	Описание
`broadcast`	Режим предоставляет наибольшую защиту от сбоев. В этом режиме пакеты, попадающие на агрегированный интерфейс, отправляются через все подчинённые физические 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 настройки > Сетевые интерфейсы**.

2 Нажмите , чтобы включить режим редактирования.

3 Для всех сетевых интерфейсов Ethernet, которые вы хотите объединить, установите класс `Slave` (см. Настройка сетевых интерфейсов Ethernet).

4 Нажмите **Добавить bond**.

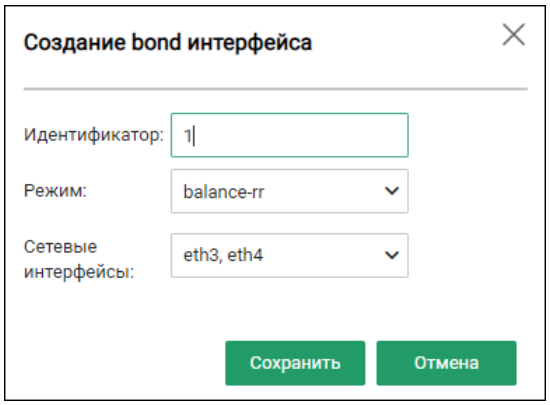


Рисунок 16. Создание агрегированного интерфейса

5 Задайте основные параметры агрегированного интерфейса:

5.1 В поле **Идентификатор** задайте номер. Созданный агрегированный интерфейс будет иметь имя `bond<номер>`.

5.2 В списке **Режим** выберите режим работы интерфейса.

5.3 В списке **Сетевые интерфейсы** последовательно выберите физические интерфейсы класса `slave`, которые вы хотите объединить. Эти интерфейсы станут подчинёнными для создаваемого агрегированного интерфейса. Ограничений на количество подчинённых интерфейсов нет. Выберите не менее одного подчинённого интерфейса.

5.4 Нажмите **Сохранить**.

6 В списке интерфейсов выберите созданный агрегированный интерфейс и настройте его:

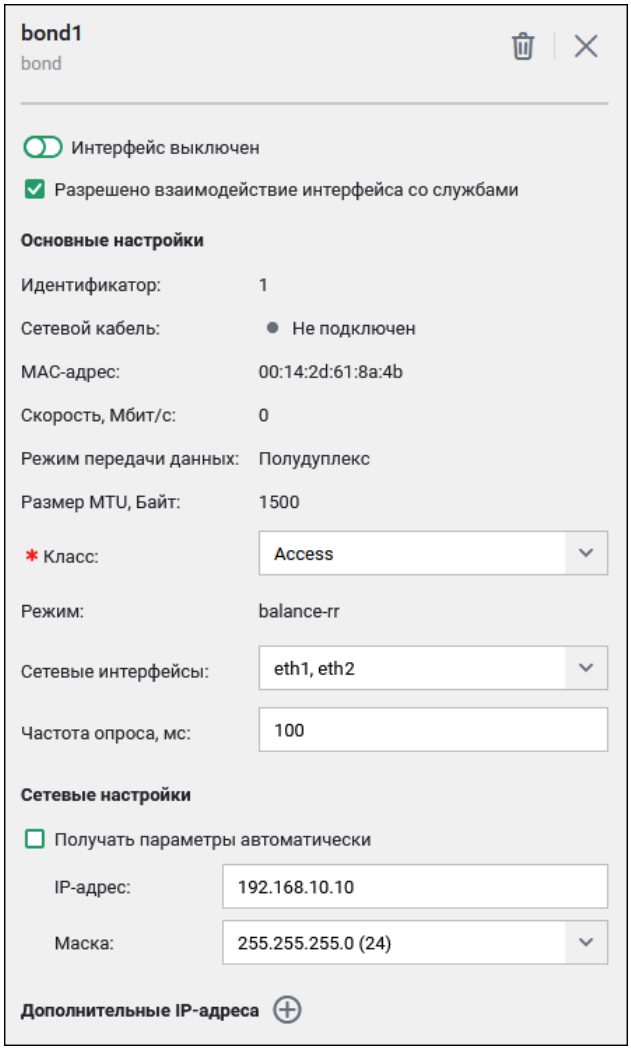


Рисунок 17. Настройка агрегированного интерфейса

6.1 Чтобы включить прохождение трафика через созданный агрегированный интерфейс, выберите **Разрешено взаимодействие интерфейса со службами**.

6.2 По умолчанию созданному интерфейсу назначается класс `Access`. Если вы хотите, чтобы интерфейс обрабатывал трафик из нескольких VLAN (см. Организация обработки трафика из нескольких VLAN), назначьте ему класс `Trunk`.

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

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

6.5 В разделе **Сетевые настройки** выполните одно из действий:

- Чтобы присвоить интерфейсу статический IP-адрес, заполните поля **IP-адрес** и **Маска**.

  Вы можете задать дополнительные IP-адреса интерфейса. Для этого нажмите ⊕. Подробнее см. Назначение дополнительных IP-адресов.

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

Выберите параметры, получаемые от DHCP-сервера: адреса DNS-серверов, адреса NTP-серверов, маршруты.

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка маршрутов протоколов DHCP и PPP). Чтобы просмотреть параметры, заданные для режима DHCP на всех интерфейсах, см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

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 настройке метрики см. в разделе Настройка метрики для маршрутов DHCP-сервера. Чтобы вернуть значение по умолчанию, нажмите  .

6.6 Нажмите **Сохранить**.

7 Для передачи данных через агрегированный интерфейс используется размер MTU, равный 1500 байт. В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 вы можете изменить размер MTU, чтобы оптимизировать передачу данных через интерфейс. Для этого выберите агрегированный интерфейс и в поле **Размер MTU в байтах** задайте новое значение MTU из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию (1500 байт), нажмите  . Подчинённые интерфейсы наследуют MTU агрегированного интерфейса.

8 Последовательно включите  подчинённые физические интерфейсы, а затем агрегированный интерфейс.

9 Нажмите  .

Просмотр ARP-таблицы

Чтобы просмотреть ARP-таблицу с записями о соответствии IP-адресов и MAC-адресов:

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

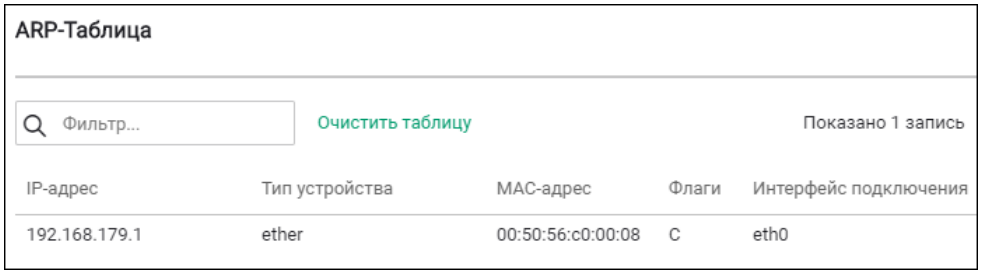


Рисунок 18. Просмотр ARP-таблицы

2 Для поиска записей в поле **Фильтр** начните вводить любой из параметров:

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

В случае сетевых сбоев вы можете очистить ARP-таблицу.

Настройка Power over Ethernet

Технология Power over Ethernet (PoE) позволяет устройству подавать питание на другие устройства через интерфейсы Ethernet, а также получать питание для собственной работы.

PoE поддерживается в исполнении ViPNet Coordinator IG100 I5.

Вы можете подключить устройства, работающие по технологии PoE, ко всем портам **LAN** на аппаратной платформе ViPNet Coordinator IG. При этом необходимо учитывать ограничения:

Таблица 2. Ограничения по мощности подключаемых устройств

Способ питания ViPNet Coordinator IG	**Максимальная мощность потребления подключённых устройств с PoE**
От блока питания	30 Вт для каждого устройства
От коммутатора по технологии PoE	15 Вт суммарно на все устройства: Одно устройство не выше 3го класса мощности или два устройства не выше 2го класса мощности

В кластере работа PoE не поддерживается.

Настройка питания внешних устройств

1. Подключите одно или несколько устройств с поддержкой PoE к портам **LAN**. Вы также можете подключить устройства после настройки питания.
2. Выберите **Сетевые настройки** > **Power over Ethernet (PoE)**.
3. Выберите сетевой интерфейс, к которому подключено устройство с PoE.
4. В поле **Максимальная мощность** укажите мощность в Ваттах, которая требуется для работы подключённого устройства.

   При этом необходимо учитывать:

   - Если заданное значение превышает мощность, выделенную на питание всех устройств (15 Вт или 60 Вт — в зависимости от источника питания ViPNet Coordinator IG), питание не будет подано на устройство.
   - Если потребляемая устройством мощность превысит заданное вами значение, сработает защита по току и устройство будет перезагружено.

   Примечание. Погрешность в расчете фактического потребления мощности составляет 3%.

5. Поле **Приоритет** определяет очерёдность подачи питания на интерфейсы. Задайте значение:

- 1 — чтобы питание сначала подавалось на этот интерфейс;
- 2 — чтобы питание сначала подавалось на интерфейс с приоритетом 1.

Если приоритеты интерфейсов равны, питание будет подано сначала на интерфейс с меньшим индексом в имени (например, сначала на `eth1`, затем на `eth2`).

Например, чтобы питание подавалось сначала на интерфейс `eth2`, а затем — на `eth1`, установите для `eth2` приоритет 1, для `eth1` — приоритет 2.

При этом:

- Если выделенной мощности (15 Вт или 60 Вт) хватит на питание устройства, подключённого к `eth2`, остаток мощности будет передан на `eth1`. Если остатка мощности не хватит для питания устройства, подключённого к `eth1`, оно будет выключено.
- Если выделенной мощности не хватит на питание устройства, подключённого к `eth2`, мощность будет передана на `eth1`.

Внимание! Если ViPNet Coordinator IG питается от блока питания, а порт **WAN** подключён к коммутатору с PoE, то при отключении блока питания мощность, выделенная на питание всех устройств, снизится до 15 Вт. При этом мощность между устройствами будет распределяться в порядке приоритетов, заданных на интерфейсах. Устройства, которым не хватило мощности, будут выключены.

---

6 При включении ViPNet Coordinator IG питание на интерфейсы подаётся после загрузки ПО ViPNet Coordinator IG. Чтобы подключённое устройство загрузилось быстрее, выберите **Подача питания до загрузки ПО**.

7 Нажмите **Сохранить**.

8 Если вы подключили несколько устройств к ViPNet Coordinator IG, повторите шаги 3–7 для другого интерфейса.

9 В столбце **PoE на интерфейсе** включите  подачу питания на каждый интерфейс, к которому подключено устройство с PoE.

Питание будет подано после определения класса устройства и при условии, что потребление мощности не превышает установленные ограничения. Если устройство не подключено, питание будет подано автоматически при подключении устройства к интерфейсу.

Таблица 3. Возможные состояния подключённых устройств

Состояние	Описание
Выключено	Устройство не подключено
Классификация	Определение мощности, которая требуется для питания устройства
Классификация выполнена	Определён класс мощности, устройство ждёт подачи питания **Примечание.** Питание может быть не подано, если максимальная мощность, заданная на интерфейсе, превышает мощность, выделенную на питание всех устройств.
Ожидание подачи питания	Подана команда включения питания

Состояние	Описание
Питание подается	Питание на устройство успешно подано
Ошибка	Питание на устройство не может быть подано **Примечание.** Описание ошибки записывается в системный журнал.

Состояния подключённых устройств также отображаются на корпусе ViPNet Coordinator IG (см. документ «Описание аппаратных платформ», раздел «Световая индикация»).

Настройка проверки внешних устройств

ViPNet Coordinator IG может автоматически проверять доступность устройств, работающих по технологии PoE. Это позволяет обнаруживать и устранять неполадки в работе устройств.

Чтобы настроить проверку доступности:

1. Выберите **Сетевые настройки** > **Power over Ethernet (PoE)**.
2. Выберите сетевой интерфейс, к которому подключено устройство с PoE.
3. Выберите **Проверять доступность устройства**.
4. Задайте IP-адрес, по которому ViPNet Coordinator IG будет проверять доступность устройства.
5. Задайте период опроса устройства в диапазоне от 1 до 120 секунд.
6. Задайте количество неудачных попыток опроса IP-адреса, после которых устройство будет считаться недоступным.

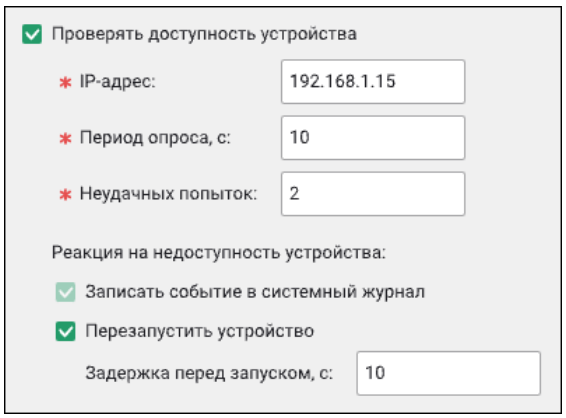


Рисунок 19. Настройка проверки доступности устройства

Примечание. Убедитесь в наличии сетевого фильтра, разрешающего ICMP-соединения. По умолчанию такой фильтр уже задан в межсетевом экране ViPNet Coordinator IG.

7. Если устройство недоступно, ViPNet Coordinator IG записывает информацию об этом в системный журнал. Также вы можете настроить перезагрузку устройства в случае его недоступности. Для этого:

7.1 Выберите **Перезапустить устройство**.

7.2 В поле **Задержка перед запуском** введите время, на которое будет отключено питание от устройства, в диапазоне от 1 до 120 секунд. Питание будет подано по истечении этого времени.

8 Нажмите **Сохранить**.

3

Настройка VPN

Просмотр сведений о сетевых узлах ViPNet 48

Просмотр и изменение списка туннелируемых узлов 51

Настройка доступа к туннелируемым узлам в одной подсети 53

Настройка туннелирования на канальном уровне по технологии L2OverIP 55

Просмотр сведений о сетевых узлах ViPNet

Вы можете просмотреть сведения об узлах ViPNet, для которых установлены связи с вашим узлом. Для этого:

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

Страница содержит список сетевых узлов, с которыми у вашего узла есть связь, а также время их последней активности.

Примечание. Активность определяется наличием трафика между координатором и узлом, например, при обмене межузловой информацией или проверке связи. Время последней активности узла хранится на ViPNet Coordinator IG до перезапуска службы `iplircfg` и отображается, даже если узел выключен.

Типы узлов:

- — клиенты ViPNet;
- — координаторы ViPNet.

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

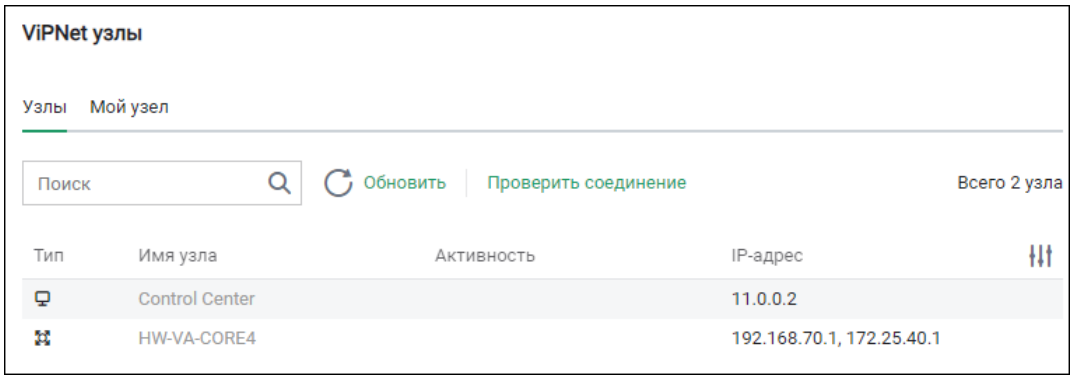


Рисунок 20. Просмотр списка узлов сети ViPNet

2 Чтобы просмотреть подробные сведения об узле, выберите его в списке. Информация об узле содержит разделы:

- общая информация: статус соединения, имя узла, версия ПО ViPNet и ОС, тип шифрования;
- IP-адреса доступа к узлу: реальные и виртуальные;
- доменные имена узла;
- настройки межсетевого экрана при подключении к внешней сети (для координаторов);
- настройки туннелирования (для координаторов).

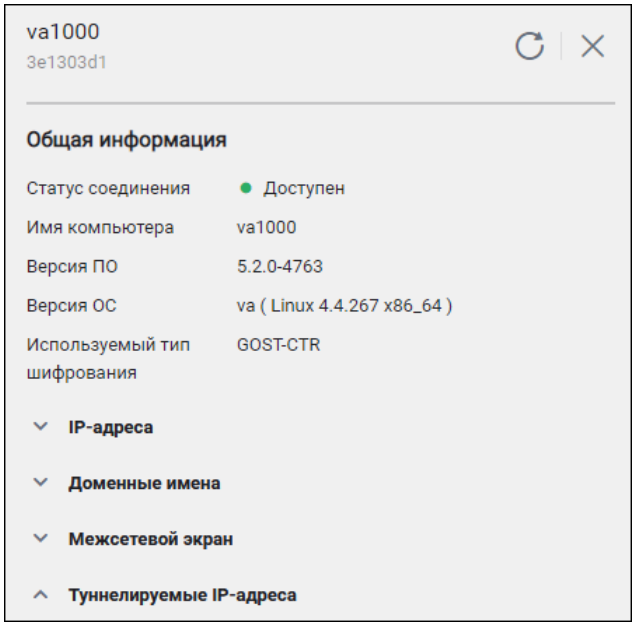


Рисунок 21. Просмотр сведений об узле ViPNet

Примечание. Чтобы изменить настройки видимости узлов, см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка видимости узлов».

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

1. Нажмите **Проверить соединение**.
2. Введите IP-адрес или доменное имя узла.
3. Нажмите **Проверить**.

Чтобы просмотреть сведения о собственном узле, перейдите на вкладку **Мой узел**.

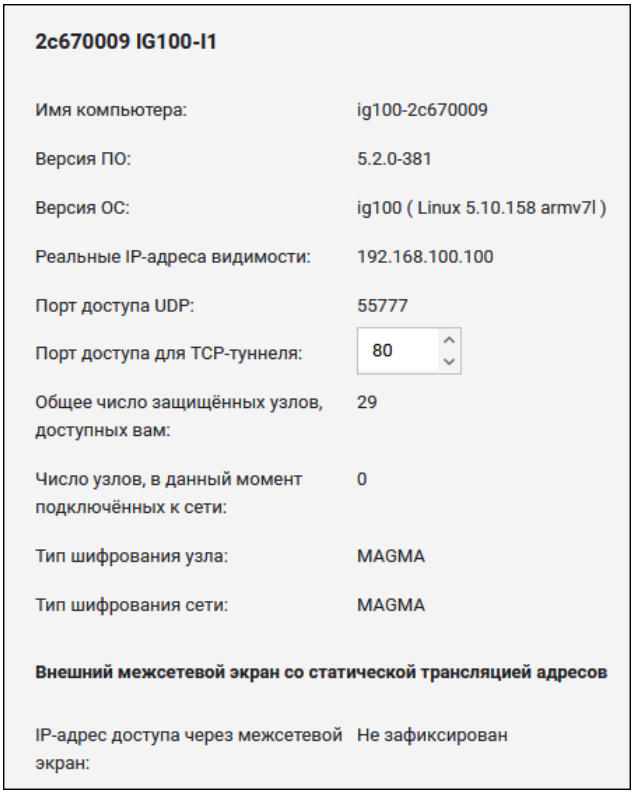


Рисунок 22. Просмотр сведений о собственном узле ViPNet

Просмотр и изменение списка туннелируемых узлов

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

Узлы, которые будут туннелироваться координатором, задаются в ViPNet Prime (см. документ «ViPNet Prime. Руководство администратора», раздел «Создание туннелируемых адресов ресурсов»). Эта информация автоматически передаётся на узлы защищённой сети в составе справочников. Для взаимодействия между узлом защищённой сети и туннелируемым узлом, а также между двумя туннелируемыми узлами, необходимо создать связи между ними в ViPNet Prime.

Если ViPNet Coordinator IG работает в условиях отсутствия связи с ViPNet Prime, вы можете настроить туннелирование локально на ViPNet Coordinator IG. Затем IP-адреса туннелируемых узлов необходимо задать вручную на каждом связанном координаторе.

Если настройки туннелирования были заданы вручную, а затем поступили из ViPNet Prime, выполняется их слияние:

- Если с настройками туннелирования из ViPNet Prime получены новые IP-адреса туннелируемых узлов, они добавляются в конфигурационный файл `iplir.conf`.
- Если заданные локально IP-адреса туннелируемых узлов отсутствуют в настройках туннелирования, полученных из ViPNet Prime, то эти IP-адреса будут удалены.

Чтобы добавить туннелируемый IP-адрес или диапазон адресов:

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

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

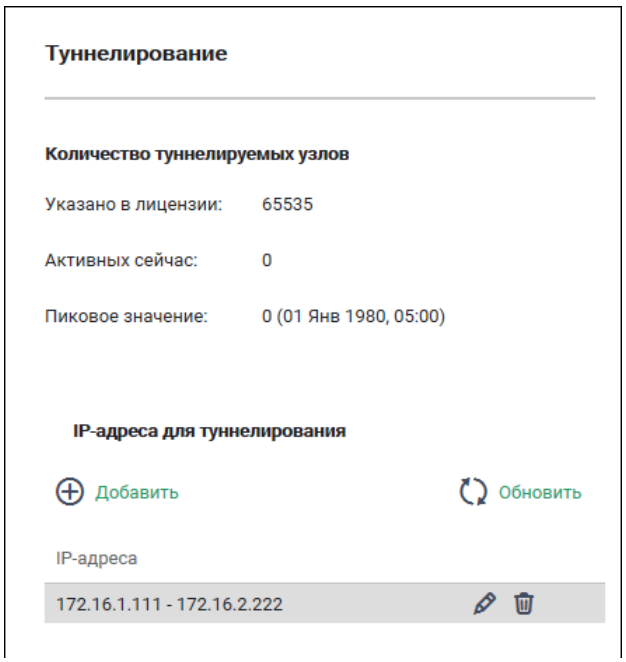


Рисунок 23. Просмотр информации о туннелируемых узлах

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

Примечание. На всех узлах, туннелируемых ViPNet Coordinator IG, укажите его в качестве шлюза по умолчанию.

Настройка доступа к туннелируемым узлам в одной подсети

Если туннелируемый узел другого координатора находится в одной подсети с ViPNet Coordinator IG, и на узле не настроена маршрутизация до ViPNet Coordinator IG через туннелирующий координатор, то трафик между туннелируемым узлом и ViPNet Coordinator IG будет блокироваться.

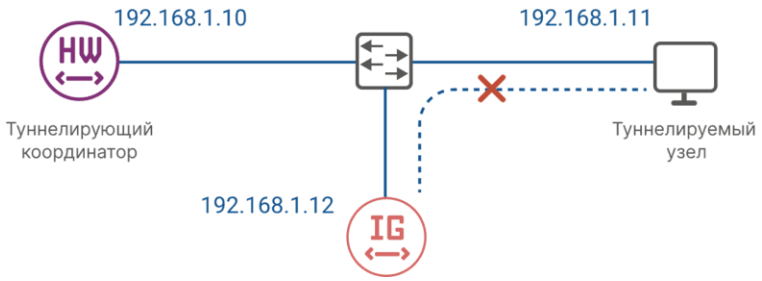


Рисунок 24: Туннелируемый узел другого координатора в одной подсети с ViPNet Coordinator IG

Чтобы решить проблему блокировки трафика, исключите узлы, туннелируемые другим координатором, из списка туннелируемых узлов, которые известны ViPNet Coordinator IG. Тогда ViPNet Coordinator IG будет обращаться к таким узлам напрямую, как к отрытым узлам.

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

2 В списке выберите туннелирующий координатор.

3 На панели справа в разделе **Туннелируемые IP-адреса** выключите **Туннелировать IP-адреса, входящие в локальную подсеть**.

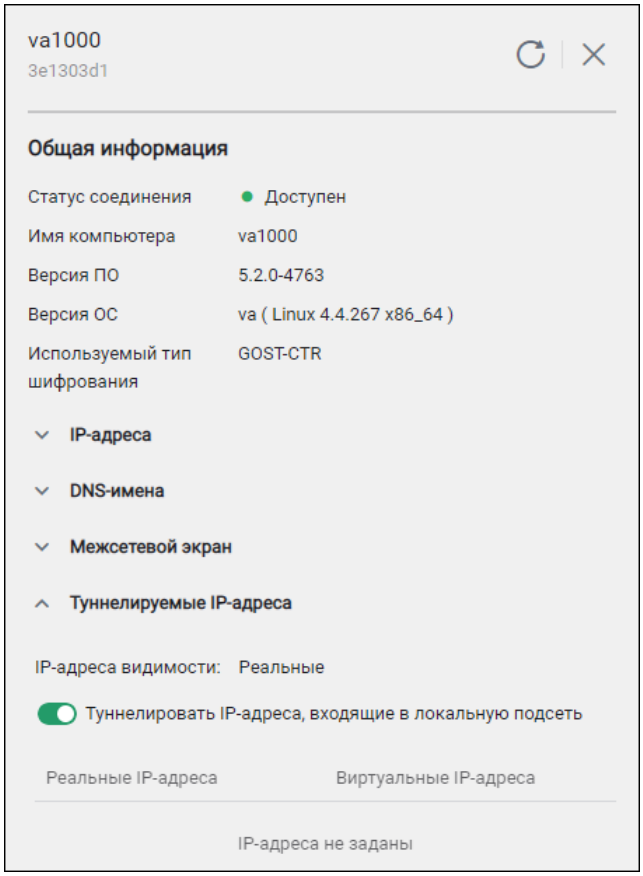


Рисунок 25. Настройка доступа к туннелируемым узлам напрямую

Настройка туннелирования на канальном уровне по технологии L2OverIP

Общие сведения об L2OverIP

ViPNet Coordinator IG 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 IG, которые установлены на границах этих сегментов. ViPNet Coordinator IG 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 IG по защищённому каналу. ViPNet Coordinator IG, получивший IP-пакеты специального формата, извлекает из них исходные кадры и передаёт получателям в своем сегменте.

С помощью L2OverIP можно объединить несколько сегментов сети:

- 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; 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 IG 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 задаётся в настройках L2OverIP. Порт, заданный для собственного сегмента сети, называется локальным. Порты, заданные на ViPNet Coordinator IG в других сегментах, называются удалёнными. Трафик самого ViPNet Coordinator IG всегда относится к порту с номером 0.

L2OverIP можно использовать в кластере. Настройка L2OverIP выполняется на активном узле. При переключении узлов кластера таблица MAC-адресов не передаётся пассивному узлу. Коммутация

кадров восстановится, когда узлы из разных сегментов, взаимодействующие друг с другом, заново отправят ARP-запросы.

Особенности реализации L2OverIP в ViPNet Coordinator IG

- Сегменты сети, объединяемые по L2OverIP, должны быть изолированы друг от друга. Сетевое взаимодействие между ними должно осуществляться только по каналам связи между ViPNet Coordinator IG, установленными на границах объединяемых сегментов.
- Для использования беспроводных интерфейсов в L2OverIP действуют ограничения:
  - нельзя использовать интерфейс модема;
  - интерфейс Wi-Fi можно использовать только со статическим IP-адресом.
- Текущая версия ViPNet Coordinator IG 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.
- Поиск IP-пакетов, переданных по L2OverIP, в журнале регистрации IP-пакетов необходимо выполнять по признакам исходных IP-пакетов: IP-адрес источника и получателя, номер TCP- и UDP-порта, интерфейс.

Настройка L2OverIP

При настройке туннелирования на канальном уровне каждый сегмент сети подключается к одному из сетевых интерфейсов ViPNet Coordinator IG, 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 IG (см. Организация обработки трафика из нескольких VLAN).

Чтобы настроить L2OverIP, на каждом ViPNet Coordinator IG:

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

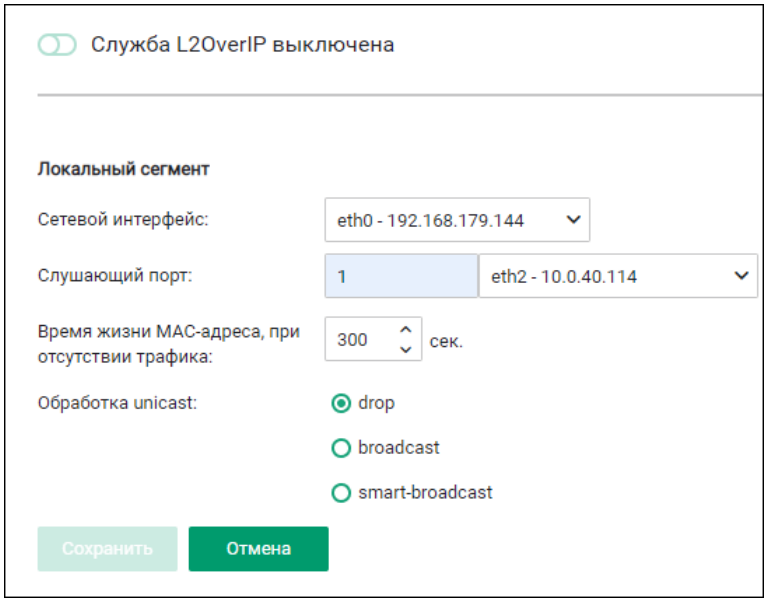


Рисунок 26. Настройка параметров соединения L2OverIP

2 В списке **Сетевой интерфейс** выберите интерфейс, подключённый к локальному сегменту сети, который требуется объединить с другим сегментом по L2OverIP.

3 Задайте параметры локального сегмента сети — уникальный номер порта сегмента в поле **Слушающий порт** и IP-адрес внешнего интерфейса в списке рядом.

4 Вы можете изменить время жизни MAC-адреса в таблице MAC-адресов виртуального коммутатора (см. Общие сведения об L2OverIP) при отсутствии трафика от этого адреса. Например, уменьшите значение, если IP-адреса узлов удалённого сегмента часто меняются.

5 Чтобы изменить режим обработки функцией L2OverIP одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя, 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 удалённые порты и на порт с номером 0;
  - кадры, принятые от удалённого 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 удалённые 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.

6 Задайте параметры удалённого сегмента сети.

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

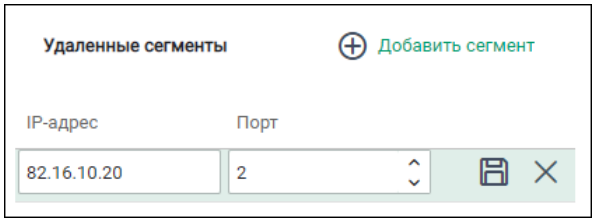


Рисунок 27. Добавление удалённого сегмента сети при создании соединения L2OverIP

В зависимости от настройки видимости удалённого ViPNet Coordinator IG укажите его реальный или виртуальный IP-адрес. Если в ViPNet Coordinator IG указано более одного реального адреса для удалённого ViPNet Coordinator IG (см. Просмотр сведений о сетевых узлах ViPNet), настройте видимость удалённого ViPNet Coordinator IG по реальным адресам и укажите его реальный IP-адрес. Для настройки видимости см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка видимости узлов».

Внимание! Если в процессе работы вы поменяете видимость удалённого узла, измените его IP-адрес в настройках L2OverIP. Затем выключите и включите службу L2OverIP.

---

7 Добавьте сетевой фильтр защищённой сети, разрешающий любые соединения по протоколу 97.

8 Нажмите **Сохранить**.

9 Включите службу L2OverIP.

На узлах локального сегмента сети укажите IP-адрес ViPNet Coordinator IG в качестве шлюза по умолчанию.

Примеры организации защищённого соединения между удалёнными сегментами сети с использованием технологии L2OverIP см. в документе «Сценарии работы», раздел «Защита соединения между удалёнными сегментами сети на канальном уровне модели OSI».

4

Настройка фильтрации трафика

Настройка сетевых фильтров 60

Настройка фильтрации промышленных протоколов 82

Настройка прокси-сервера 93

Настройка сетевых фильтров

Типы трафика

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

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

Открытый трафик может быть локальным или транзитным:

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

ViPNet Coordinator IG обрабатывает трафик, разделяя его на следующие типы:

- открытый локальный трафик — между открытым узлом и ViPNet Coordinator IG;
- защищённый трафик — трафик между узлами сети ViPNet;
- туннелируемый трафик — трафик между двумя открытыми (или открытым и защищённым) узлами, зашифрованный в пределах сети ViPNet;

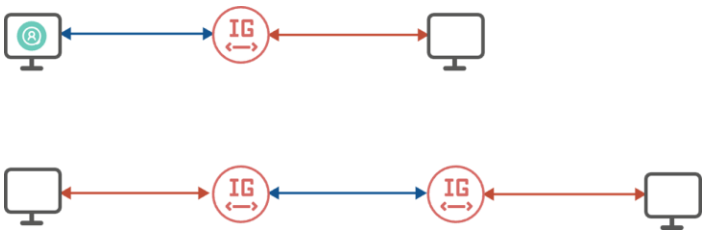


Рисунок 28. Туннелируемый трафик

- открытый транзитный трафик — трафик между открытыми (или открытым и защищённым) узлами, проходящий через координатор, который не является ни отправителем, ни получателем IP-пакетов.



Рисунок 29. Открытый транзитный трафик

Для каждого типа трафика можно настроить соответствующие сетевые фильтры.

Принципы фильтрации трафика

- Все входящие и исходящие открытые и защищённые 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.

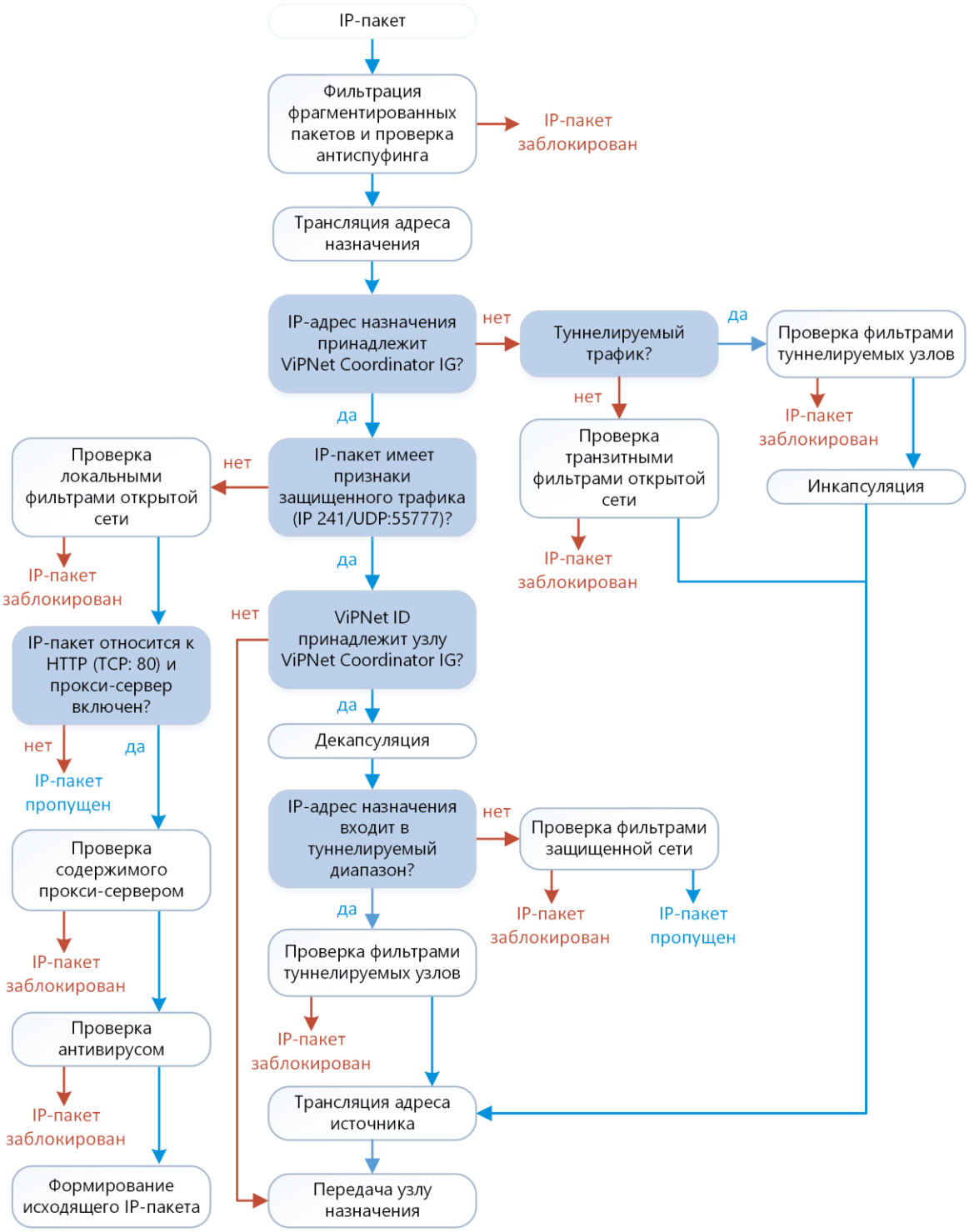


Рисунок 30. Схема фильтрации трафика

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

1 IP-пакет проверяется на фрагментацию, если эта проверка включена. Если IP-пакет фрагментирован, он блокируется, иначе — передаётся на следующий шаг проверки.

2 IP-пакет обрабатывается правилами антиспуфинга, если он включён. В результате IP-пакет блокируется или передаётся на следующий шаг проверки.

3 Случаи, в которых выполняется трансляция IP-адреса назначения (см. Трансляция адреса назначения):

- IP-пакет удовлетворяет условиям правила трансляции адресов.
- Включена обработка прикладного протокола, к которому относится IP-пакет (см. Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP).
- IP-пакет соответствует протоколу HTTP (TCP: 80) и прокси-сервер работает в «прозрачном» режиме. В этом случае с помощью трансляции адреса назначения транзитный трафик перенаправляется на ViPNet Coordinator IG и обрабатывается как локальный трафик открытой сети.

4 Если IP-пакет адресован ViPNet Coordinator IG и имеет признаки защищённого 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 IG, 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 IG, 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 IG, IP-пакет проверяется фильтрами туннелируемых узлов. В результате IP-пакет блокируется или отправляется на туннелируемый узел после трансляции адреса источника.
  - Если IP-адрес назначения в исходном IP-пакете не входит в туннелируемый диапазон ViPNet Coordinator IG, IP-пакет проверяется фильтрами защищённой сети, после чего блокируется или пропускается.

5 Если IP-пакет адресован ViPNet Coordinator IG и не имеет признаков защищённого 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 или IP-пакет не относится к протоколу HTTP, IP-пакет пропускается.

5.2 После проверки прокси-сервером выполняется антивирусная проверка, если она включена. В результате IP-пакет блокируется или формируется новый исходящий IP-пакет.

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

- Если IP-адрес отправителя входит в туннелируемый диапазон ViPNet Coordinator IG, а IP-адрес получателя входит в туннелируемый диапазон другого координатора или принадлежит защищённому узлу, IP-пакет проверяется фильтрами туннелируемых узлов. В результате IP-пакет блокируется или отправляется получателю после процедур инкапсуляции и трансляции адреса источника.

- Если IP-пакет не принадлежит туннелируемому трафику, IP-пакет проверяется транзитными фильтрами открытой сети. В результате IP-пакет блокируется или отправляется получателю после трансляции адреса источника.



Примечание. Если настроена фильтрация промышленных протоколов, то при проверке IP-пакета сетевыми фильтрами (локальными, транзитными, фильтрами защищённой сети или фильтрами туннелируемых узлов) правила фильтрации промышленных протоколов применяются в первую очередь. Подробнее см. Настройка фильтрации промышленных протоколов.

Особенности при настройке фильтрации трафика на ViPNet Coordinator IG:

- TCP-порт 2047 и UDP-порт 2046 являются служебными портами ViPNet Coordinator IG, 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, выполните команду в командном интерпретаторе:

  ```
  hostname# firewall conntrack flush
  ```

Общие сведения о сетевых фильтрах

Типы фильтров

Сетевые фильтры различаются по типу трафика (защищённый, туннелируемый, открытый локальный и транзитный), который они обрабатывают:

- Фильтры защищённой сети. Могут разрешать или блокировать обмен IP-трафиком с защищёнными узлами, с которыми ViPNet Coordinator IG имеет связь.
- Фильтры туннелируемых узлов. Могут разрешать или блокировать IP-пакеты, передаваемые между туннелируемыми узлами и узлами сети ViPNet, с которыми ViPNet Coordinator IG имеет связь.
- Локальные фильтры открытой сети. Могут разрешать или блокировать обмен IP-трафиком ViPNet Coordinator IG с открытыми узлами.
- Транзитные фильтры открытой сети. Могут разрешать либо блокировать обмен IP-трафиком между открытыми (или открытым и защищённым) узлами, проходящий через ViPNet Coordinator IG.

Сетевые фильтры для каждого типа трафика разделяются на:

- Служебные фильтры. Создаются автоматически; имеют самый высокий приоритет и недоступны для изменения.
- Фильтры, поступившие в составе политик безопасности из ViPNet Prime Policy Management. Применяются после служебных фильтров. Недоступны для изменения. В составе политик безопасности, формируемых в ViPNet Prime Policy Management, могут быть и правила трансляции адресов. При получении политики безопасности из ViPNet Prime Policy Management, она немедленно применяется на узле.
- Настраиваемые фильтры. Содержат предустановленные фильтры и фильтры, создаваемые пользователем. Применяются после фильтров, поступивших в составе политик безопасности. Доступны для изменения.
- Блокирующий фильтр по умолчанию. Применяется после всех фильтров. Недоступен для изменения.

Порядок применения фильтров

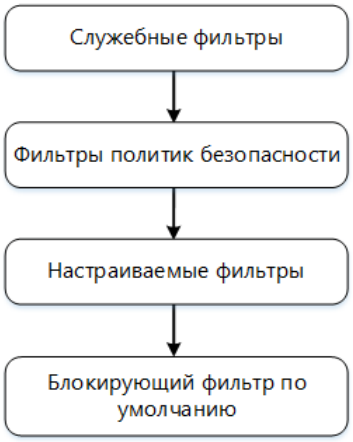


Рисунок 31. Порядок применения фильтров

Параметры фильтров

В настраиваемых сетевых фильтрах вы можете задать:

- адрес отправителя и получателя IP-пакетов, на которые действует фильтр;
- транспортные протоколы, используемые для передачи этих IP-пакетов, например, TCP, UDP, ICMP;
- расписание применения фильтра — ежедневно, еженедельно или по календарю;
- признак регистрации IP-пакетов в журнале IP-пакетов при срабатывании фильтра;
- действие, применяемое к IP-пакетам:
  - пропускать;
  - блокировать;
  - блокировать и отправить ICMP-уведомление.

Подсчёт срабатываний фильтров

В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 для каждого сетевого фильтра ведётся подсчёт срабатываний. Счётчик срабатываний запускается с момента первого включения ViPNet Coordinator IG. Сброс счётчика выполняется в ViPNet Prime. Перезагрузка ViPNet Coordinator IG, обновление ПО или переключение узлов кластера не влияют на подсчёт срабатываний. Просмотр срабатываний фильтров доступен только в веб-интерфейсе.

Группы объектов

Группы объектов позволяют упростить процессы создания и изменения сетевых фильтров и правил трансляции сетевых адресов в ViPNet Coordinator IG. 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 защищённой 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 защищённой 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 защищённой 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, 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 Prime Policy Management — группы, получаемые в составе политик безопасности, и используемые в соответствующих 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, а также при создании других пользовательских групп объектов.

Системные группы объектов

Таблица 4. 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 защищённой 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 защищённой 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 защищённой 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 IG. Можно использовать в фильтрах защищённой 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 защищённой и открытой сетей для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла.
Туннелируемые IP-адреса (`tunneledip`)	Все IP-адреса, туннелируемые координатором. Можно использовать в фильтрах туннелируемых узлов для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла.

Имя группы в веб-интерфейсе (в командном интерпретаторе)	Описание
Групповые адреса (`multicast`)	Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255). Можно использовать в локальных фильтрах открытой сети для задания 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 разрешён 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 Prime Policy Management:

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

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

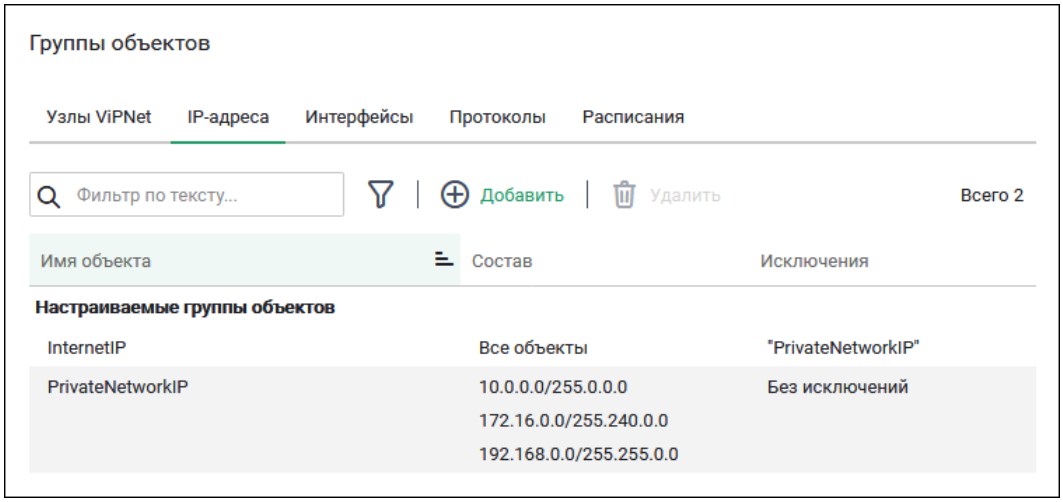


Рисунок 32. Просмотр групп IP-адресов

3 Чтобы просмотреть применение группы объектов, щёлкните её 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 .

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 IG 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**.



Примечание. Чтобы удалить группу сетевых узлов ViPNet с именем `range_<диапазон узлов>`, которая создается при конвертации правил защищенной сети во время обновления ViPNet Coordinator IG, необходимо сначала удалить все сетевые фильтры, в которых содержится эта группа.

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 IG (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**.

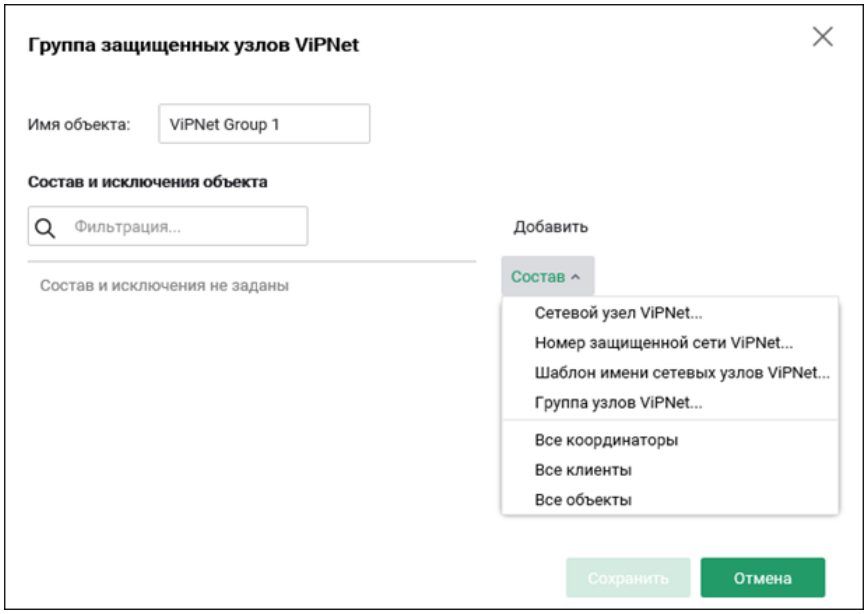


Рисунок 33. Добавление сетевого узла ViPNet в группу

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;

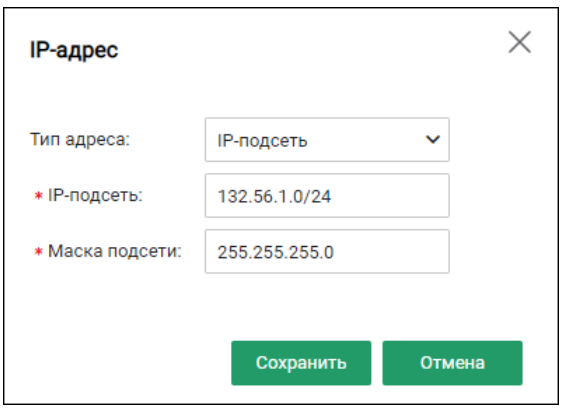


Рисунок 34. Добавление IP-адреса подсети

- **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

Группа интерфейсов

Чтобы добавить (исключить) объект:

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

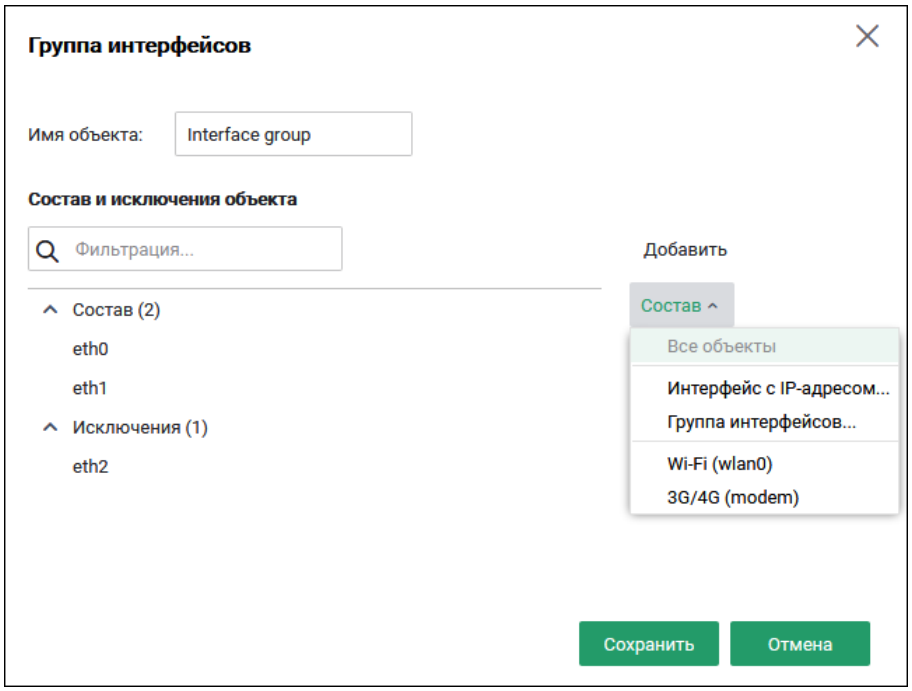


Рисунок 35. Добавление сетевых интерфейсов в группу

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 фильтров туннелируемых узлов.

Группа протоколов

Чтобы добавить (исключить) объект:

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

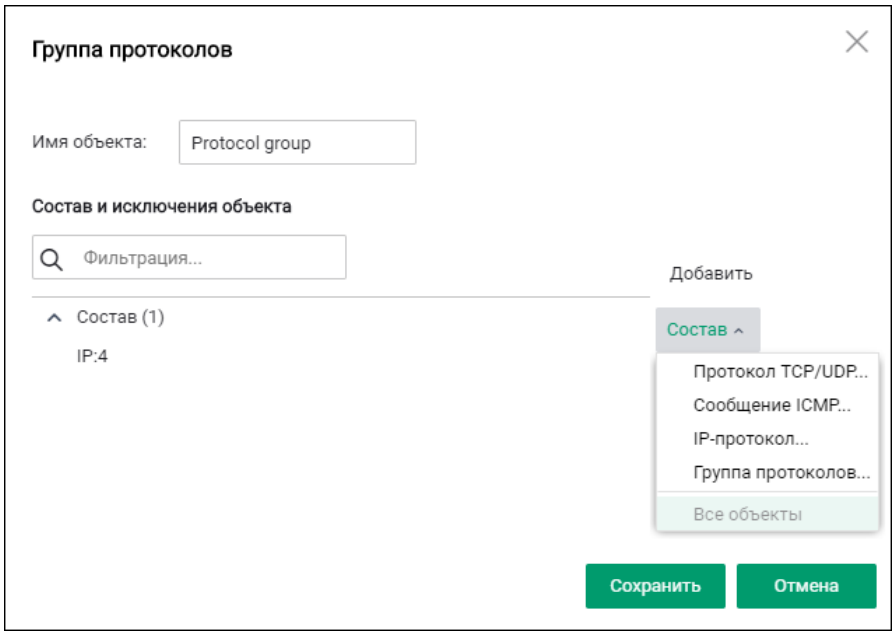


Рисунок 36. Добавление группы протоколов

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.

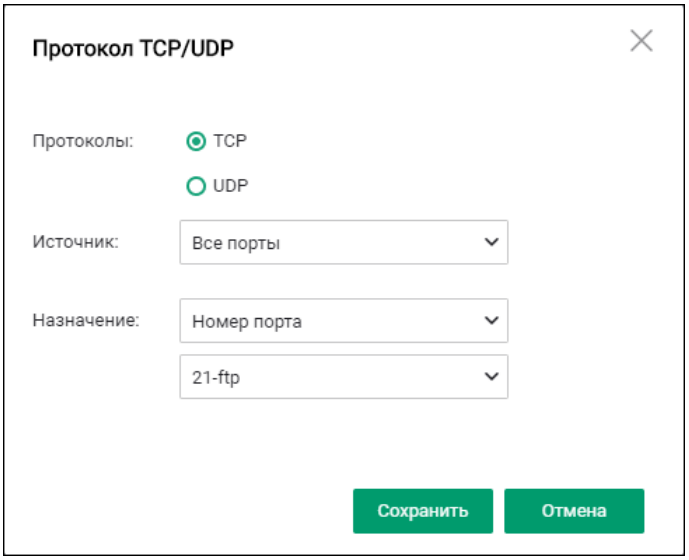


Рисунок 37. Добавление протокола в группу

- 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 её.

3 Нажмите **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать протоколы при создании и изменении сетевых фильтров и правил трансляции адресов.

Группа расписаний

Чтобы добавить объект в группу расписаний или исключить его:

1 В окне создания или редактирования группы раскройте один из списков: **Состав** или **Исключения**.

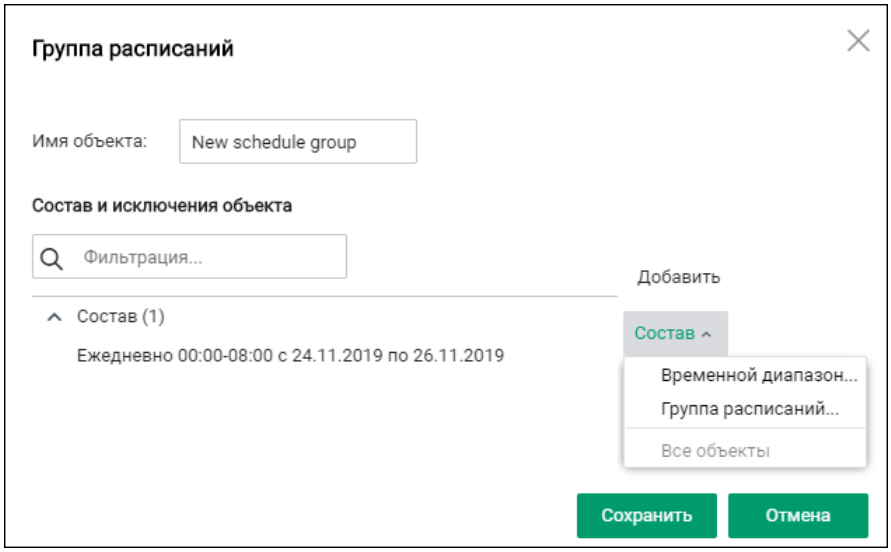


Рисунок 38. Добавление группы расписаний

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 определённые 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.

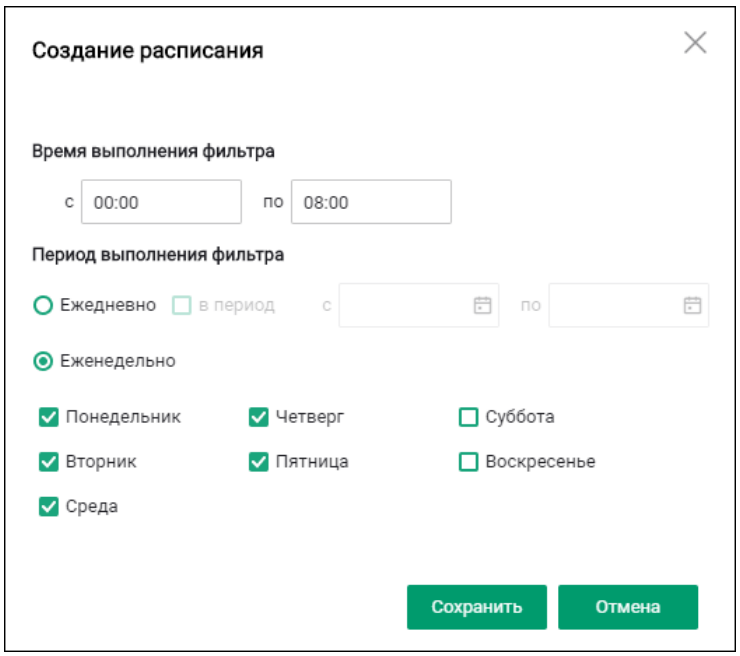


Рисунок 39. Добавление расписания в группу

- 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 и параметры фильтров.

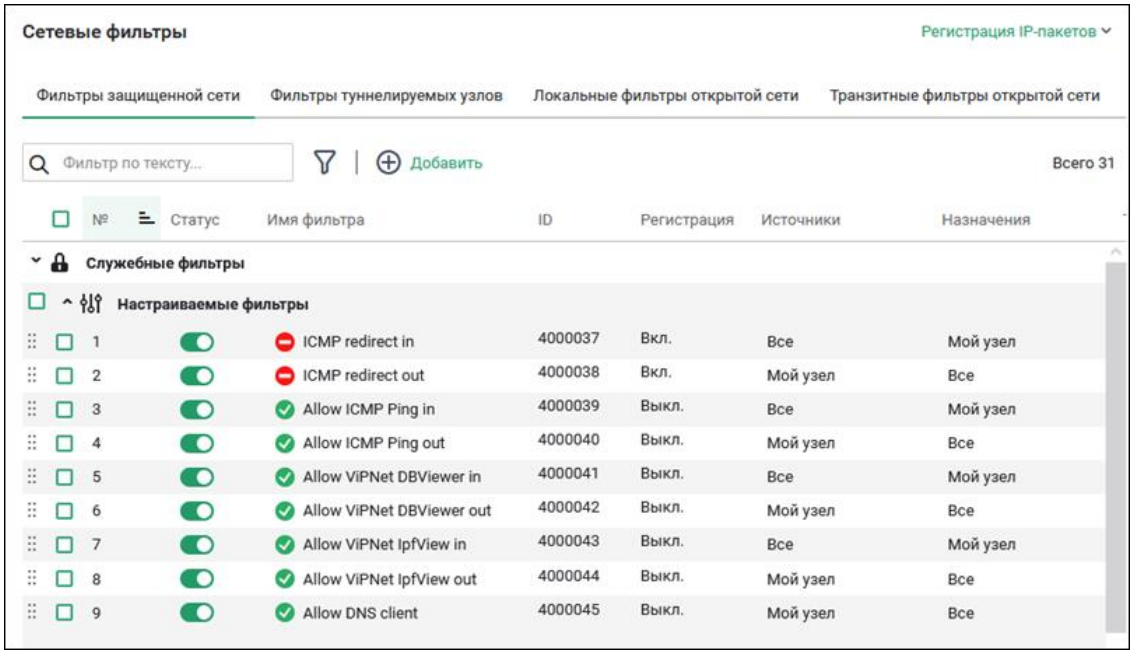


Рисунок 40. Просмотр сетевых фильтров защищённой сети

3 Чтобы просмотреть определённые фильтры, нажмите и укажите критерии поиска.

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

Счётчик срабатывания сетевых фильтров

В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 таблица содержит поле **Срабатывания**, в котором отображается количество срабатываний сетевого фильтра (см. Общие сведения о сетевых фильтрах). На основе информации о количестве срабатываний вы можете изменить порядок расположения фильтров в таблице, например передвинуть часто срабатывающие фильтры в начало таблицы, чтобы они применялись к IP-пакетам первыми. Это поможет оптимизировать производительность ViPNet Coordinator IG.

Если необходимо подсчитать количество срабатываний фильтров за определённое время, вы можете включить **Временный подсчет**. Тогда параллельно постоянному счётчику запустится временный счётчик срабатываний, и поле **Срабатывания** будет отображать значения временного счётчика. После выключения временного подсчёта снова будут отображаться значения постоянного счётчика срабатываний. Во время работы временного счётчика постоянный счётчик не останавливается.

Чтобы обновить значения срабатываний, нажмите **Обновить счетчики срабатываний** или обновите страницу в браузере.

Чтобы просмотреть сводные сведения о срабатывании сетевых фильтров:

1 Выберите **Состояние системы**.

Сводные сведения отображаются на панели **Сетевые фильтры и правила трансляции**.

2 Нажмите, чтобы просмотреть сведения подробнее или перейти на страницу настройки сетевых фильтров или правил трансляции адресов.

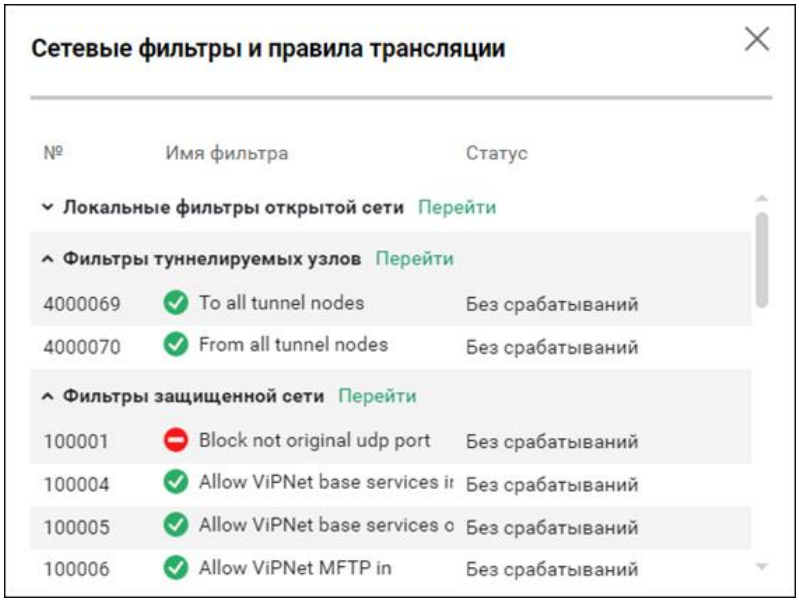


Рисунок 41. Подробные сведения о сетевых фильтрах и правилах трансляции адресов

Создание и изменение сетевых фильтров

Внимание! Максимальное количество сетевых фильтров для вашего исполнения ViPNet Coordinator IG см. в документе «Подготовка к работе» в разделе «Основные отличия аппаратных платформ». Превышение этого количества может значительно снизить производительность ViPNet Coordinator IG.

Чтобы создать или изменить сетевой фильтр на ViPNet Coordinator IG:

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**:

4.1 При создании нового фильтра задайте его название.

4.2 Включите или выключите сетевой фильтр.

4.3 Выберите действие фильтра:

- **Блокировать трафик**.
- **Пропускать трафик**.
- **Отклонять трафик с ответом**. В этом случае выберите из списка ICMP-ответ.

4.4 Если необходимо, чтобы при срабатывании фильтра IP-пакет регистрировался в журнале IP-пакетов, выберите **Регистрировать**. Подробнее см. Настройка регистрации IP-пакетов при срабатывании фильтров.

4.5 В разделе **Добавить** задайте параметры: протоколы, источники, назначения и расписания. При задании этих параметров вы можете использовать группы объектов.

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 введённые настройки с помощью кнопок и .

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

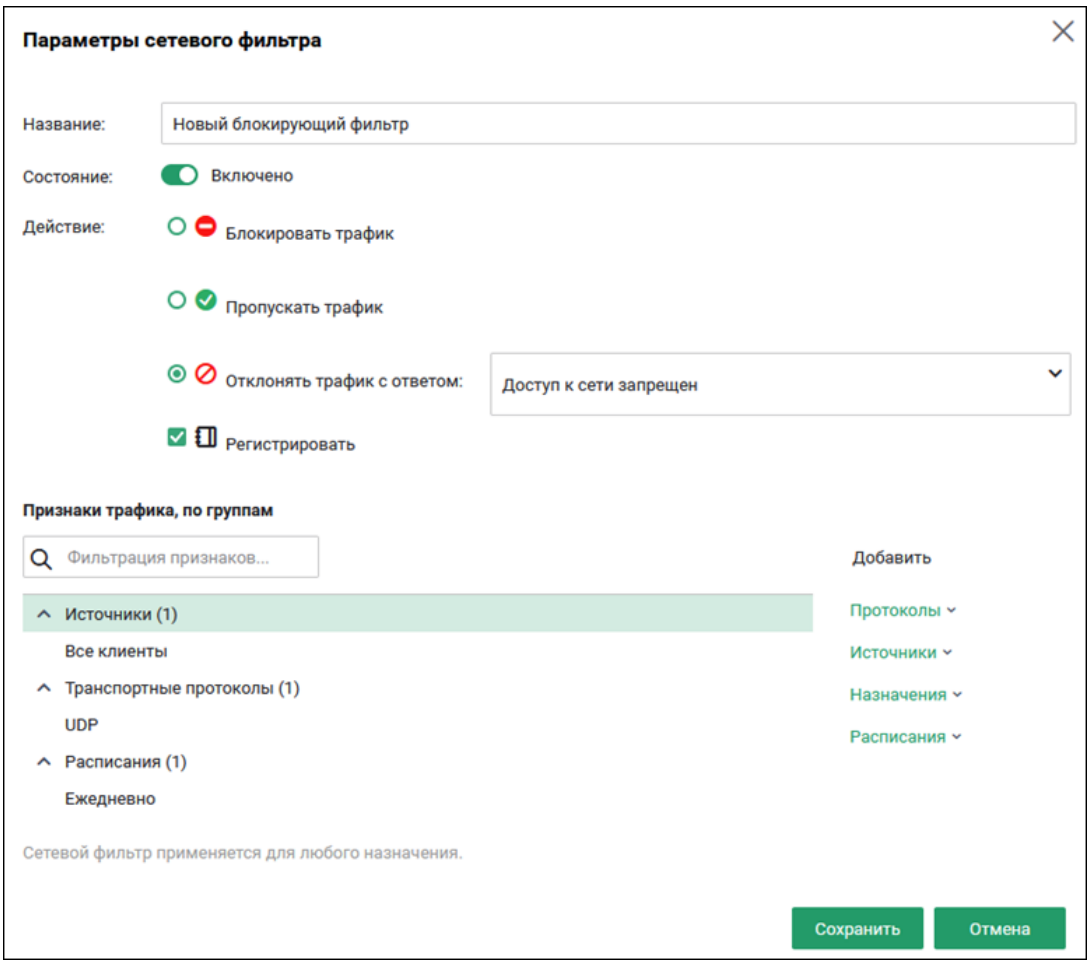


Рисунок 42. Настройка параметров сетевого фильтра

5 Нажмите **Сохранить**.

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

6 Измените приоритет фильтра, перетащив его на нужную строку с помощью значка ⠿.

7 Вверху справа нажмите **Применить всё**.

Примечание. После создания фильтра защищённой сети, локального фильтра открытой сети или фильтра туннелируемых узлов, такой фильтр не будет действовать на уже установленные соединения до истечения времени жизни этих соединений.
Транзитный фильтр открытой сети действует сразу после его создания.

Вы также можете включить или выключить один или несколько сетевых фильтров.

Если для компьютеров вашей сети вы настроили доступ в интернет через прокси-сервер ViPNet Coordinator IG, то HTTP-трафик не будет обрабатываться транзитными фильтрами открытой сети. В этом случае для фильтрации HTTP-трафика используйте средства прокси-сервера (см. Настройка правил контент-фильтрации трафика).

Настройка регистрации IP-пакетов при срабатывании фильтров

Каждый сетевой фильтр содержит параметр, который определяет, регистрировать обработанный им IP-пакет в журнале IP-пакетов или нет. Вы можете указать это в настройках сетевого фильтра. Значение параметра отображается в столбце **Регистрация** при просмотре таблицы сетевых фильтров.

Данный параметр учитывается, только если выбран способ регистрации IP-пакетов по фильтрам (если вы обновили ПО ViPNet Coordinator IG до версии 5.2.0, то по умолчанию будет выбран другой способ регистрации IP-пакетов). Подробнее о способах регистрации IP-пакетов см. Журнал IP-пакетов. При этом настройка параметра доступна независимо от используемого способа регистрации IP-пакетов.

Если хотя бы на одном сетевом интерфейсе выбран другой способ регистрации IP-пакетов (регистрация по интерфейсам), на странице сетевых фильтров выводится предупреждение:

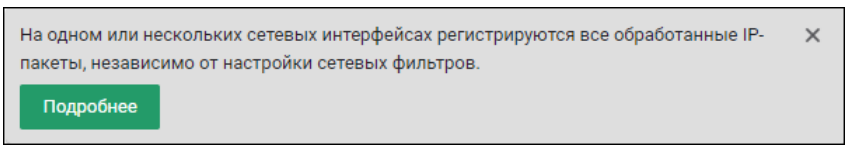


Рисунок 43. Включена регистрация IP-пакетов по интерфейсам

Вы можете включать и отключать регистрацию IP-пакетов для каждого сетевого фильтра отдельно или сразу для всех настраиваемых фильтров.

Внимание! Отключение регистрации IP-пакетов в блокирующих сетевых фильтрах может помешать расследованию инцидентов информационной безопасности.

Выборочная настройка регистрации IP-пакетов

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

2 Выберите вкладку сетевых фильтров нужного типа.

3 Выберите один или несколько сетевых фильтров с помощью флажков слева. Вы можете выбрать всю группу настраиваемых фильтров.

4 На панели инструментов откройте список **Регистрация IP-пакетов** и выберите одну из настроек: **Включить регистрацию** или **Отключить регистрацию**.

5 Вверху справа нажмите **Применить всё**.

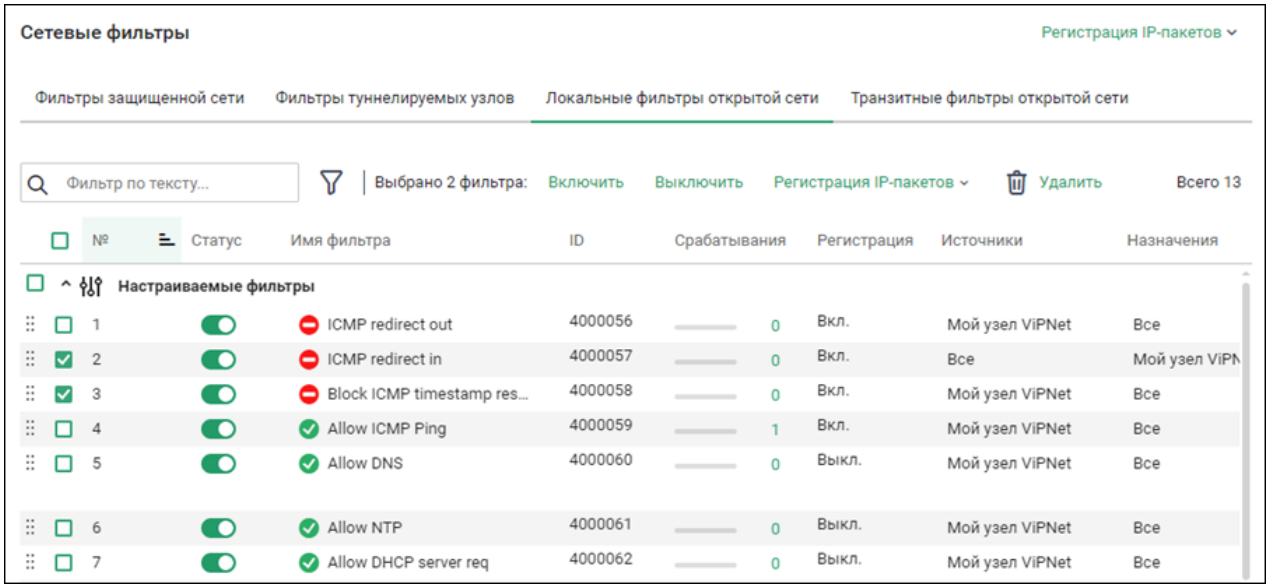


Рисунок 44. Выборочная регистрация IP-пакетов

Настройка регистрации IP-пакетов для всех настраиваемых фильтров

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

2 Вверху справа откройте список **Регистрация IP-пакетов** и выберите одну из настроек:

- **Включить для всех фильтров**.
- **Включить для блокирующих и отклоняющих фильтров**.
- **Отключить для всех фильтров**.

3 В окне подтверждения нажмите **Да**.

4 Вверху справа нажмите **Применить всё**.

Настройка фильтрации промышленных протоколов

Примечание. Фильтрация промышленных протоколов доступна на ViPNet Coordinator IG при наличии лицензии на функцию IPF. Чтобы активировать её, включите эту функцию в настройках координатора в ViPNet Prime.

Общие сведения о фильтрации промышленных протоколов

Вы можете настроить фильтрацию трафика на прикладном уровне для следующих протоколов:

- Modbus:
  - по адресам устройств;
  - по кодам функций;
  - по адресам регистров чтения и записи (для функций, которые работают с регистрами).
- МЭК 60870-5-104:
  - по общим адресам ASDU;
  - по адресам объектов информации;
  - по идентификаторам типов объектов информации.

Для фильтрации промышленного протокола на прикладном уровне необходимо сначала настроить фильтрацию на транспортном уровне. Правила транспортного уровня позволяют задавать:

- объекты промышленной сети, между которыми необходимо разрешить трафик;
- порт, используемый в промышленном протоколе.

Правила транспортного уровня определяют, какой трафик будет передан на обработку правилами прикладного уровня.

При создании правил транспортного уровня автоматически создаются разрешающие служебные фильтры межсетевого экрана, которые применяются к трафику в первую очередь. Это необходимо, чтобы трафик промышленных протоколов не блокировался предустановленными и пользовательскими сетевыми фильтрами и не пропускался без фильтрации на прикладном уровне.

Правила фильтрации промышленных протоколов создаются в составе именованных наборов правил. Каждый набор состоит из двух таблиц:

- Таблица правил транспортного уровня.

- Таблица правил прикладного уровня.

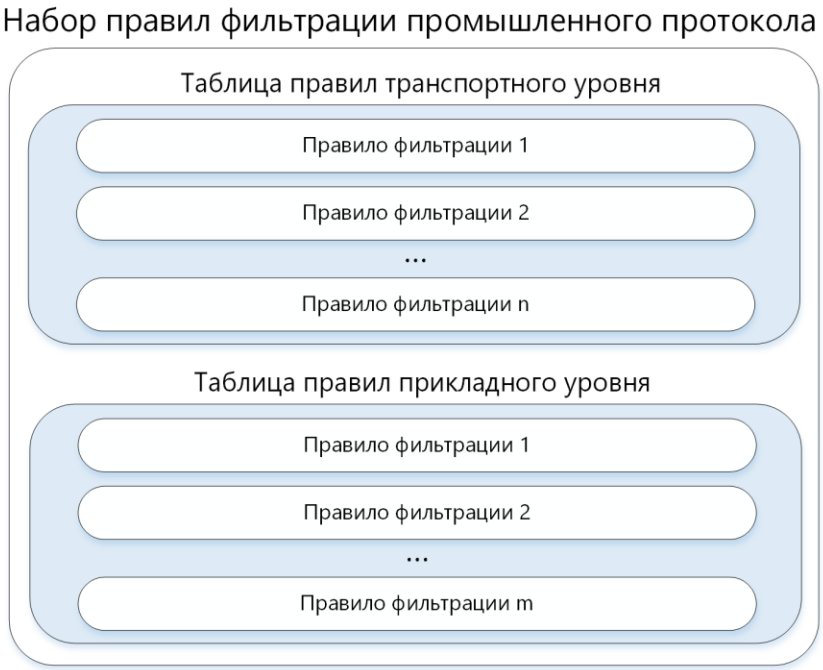


Рисунок 45. Структура набора правил фильтрации промышленного протокола

Основные принципы фильтрации промышленных протоколов

- Входящие IP-пакеты проверяются правилами фильтрации транспортного уровня при условиях:
  - Фильтрация промышленного протокола включена.
  - Создан хотя бы один набор правил промышленного протокола.
- IP-пакет обрабатывается правилами транспортного уровня всех наборов правил в порядке их расположения в таблицах правил.
- Если IP-пакет соответствует условиям правила транспортного уровня, он передаётся на обработку правилами прикладного уровня, которые содержатся в этом же наборе правил.

Примечание. Если PDU пакета содержит несколько пакетов промышленного протокола (далее – прикладные пакеты), они все передаются на проверку правилами прикладного уровня.

Другие правила транспортного уровня к этому IP-пакету уже не применяются.

- Перед обработкой правилами прикладного уровня прикладной пакет проверяется на наличие аномалий. Если аномалия обнаружена, сессия завершается и необработанные прикладные пакеты отбрасываются (критерии аномалий см. ниже).

- Прикладной пакет обрабатывается правилами прикладного уровня в порядке убывания их приоритета (расположения в таблице правил).
- Если прикладной пакет соответствует условиям правила прикладного уровня, он пропускается или блокируется этим правилом.

  Диапазоны значений в правиле фильтрации применяются следующим образом:

  - Разрешающее правило применяется, если диапазон значений в прикладном пакете полностью входит в диапазон значений, заданный в правиле.
  - Запрещающее правило применяется, если диапазон значений в прикладном пакете пересекается с диапазоном значений, заданным в правиле.

  Другие правила прикладного уровня к этому пакету уже не применяются.
- Прикладной пакет, не обработанный ни одним из правил прикладного уровня текущего набора правил, блокируется.
- IP-пакет, не обработанный ни одним из правил транспортного уровня всех наборов правил промышленных протоколов, обрабатывается остальными сетевыми фильтрами, заданными в межсетевом экране.

Принципы фильтрации протокола Modbus на прикладном уровне

- Аномалией в прикладном пакете считается:
  - Идентификатор устройства не входит в диапазон 0–255.
  - Код функций не входит в диапазон 1–127.
  - Номер регистра не входит в диапазон 0–65535.
  - Размер пакета превышает 260 байт.
  - Количество запрашиваемых регистров не входит в диапазоны:
    - 1–125 для функций с кодами: 03, 04;
    - 1–2000 для функций с кодами: 01, 02, 15;
    - 1–123 для функции с кодом 16;
    - 1–125 (чтение) 1–121 (запись) для функции с кодом 23.
- Если в правиле заданы диапазоны устройств, то диапазоны функций интерпретируются как относящиеся к каждому устройству.
- Если в правиле заданы диапазоны функций, то диапазоны регистров интерпретируются как параметры этих функций.
- Фильтрация по регистрам чтения и записи:
  - Правило, в котором заданы регистры чтения, но не заданы регистры записи, применяется для функций, запрашивающих чтение регистров (функции с кодами: 01, 02, 03, 04, 23).
  - Правило, в котором заданы регистры записи, но не заданы регистры чтения, применяется для функций, запрашивающих запись регистров (функции с кодами: 05, 06, 15, 16, 22, 23).

- Правило, в котором заданы и регистры чтения, и регистры записи, применяется для функций, запрашивающих чтение и запись регистров (функция с кодом 23).
- Правило, в котором не заданы ни регистры чтения, ни регистры записи, применяется для всех функций, независимо от того, запрашивают они доступ к регистрам или нет (фильтрация по регистрам не производится).
- Ответные пакеты не содержат номеров регистров, но к ним применяются как правила без регистров, так и правила с регистрами (регистры не учитываются). При этом, к таким пакетам применяются только разрешающие правила. Если ответный пакет не удовлетворяет ни одному разрешающему правилу, он блокируется.



Примечание. Не создавайте правила, разрешающие пакеты от любых устройств и функций (группа `@any`). Такое правило будет пропускать ответные пакеты даже с неправильными идентификаторами устройств и кодами функций.

- Разрешающее правило применяется, если диапазон регистров функции полностью входит в диапазон регистров правила.
- Запрещающее правило применяется, если диапазон регистров функции пересекается с диапазоном регистров правила.
- Диапазоны регистров правила распространяются на все, указанные в нём функции.

Принципы фильтрации протокола МЭК 60870-5-104 на прикладном уровне

- Аномалией в прикладном пакете считается:
  - Неправильный формат APCI (управляющей информации прикладного протокола). Правильный формат: байт начала, байт длины, 4 байта управления.
  - Идентификатор типа не используется (равен нулю), не входит в диапазон 1–127 или входит в один из диапазонов: 22–29, 41–44, 52–57, 65–69, 71–99, 108–109, 114–119.
  - Общий адрес ASDU не используется (равен нулю) или не входит в диапазоны: 1–255 при длине адреса в 1 байт, 1–65535 при длине адреса в 2 байта.
  - Адрес информационного объекта не входит в диапазоны: 0–255 при длине адреса в 1 байт, 0–65534 при длине адреса в 2 байта, 0–16777215 при длине адреса в 3 байта.
  - Размер APDU превышает максимальный размер, заданный настройками формата протокола.



Примечание. Неструктурированный трафик обрабатывается как аномалия.

- Если в правиле заданы диапазоны адресов ASDU, то диапазоны адресов объектов информации интерпретируются как относящиеся к каждому адресу ASDU.

- Если в правиле заданы диапазоны адресов объекта информации, то диапазоны типов объектов информации интерпретируются как параметры этих объектов информации.

Создание и изменение наборов правил фильтрации промышленного протокола

Чтобы создать или изменить набор правил фильтрации промышленного протокола:

1 Выберите **Межсетевой экран** > **Фильтрация промышленных протоколов**.

2 Выберите вкладку промышленного протокола:

- **Modbus** – для протокола Modbus;
- **МЭК104** – для протокола МЭК 60870-5-104.

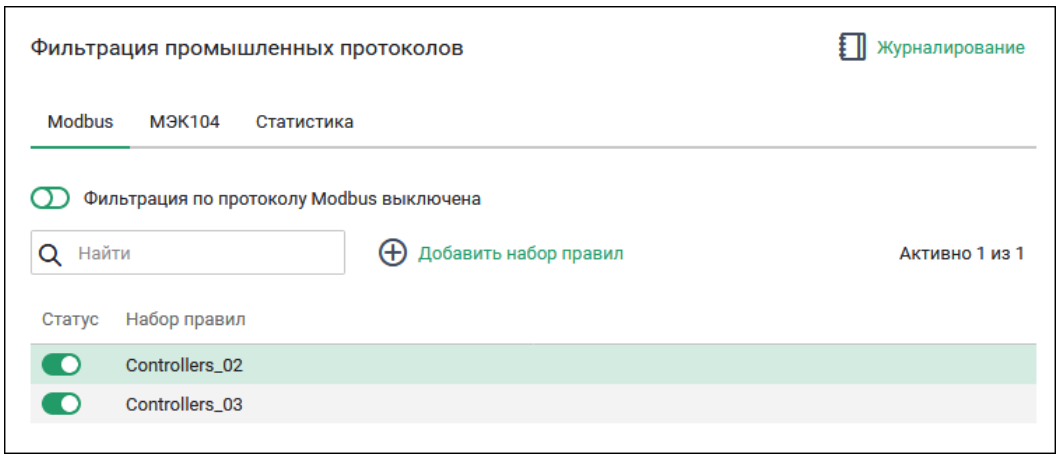


Рисунок 46. Настройка наборов правил фильтрации протокола Modbus

3 Включите фильтрацию по протоколу (по умолчанию фильтрация промышленных протоколов выключена).

4 Выполните одно из действий:

- Чтобы создать набор правил, нажмите **Добавить набор правил**;
- Чтобы изменить набор правил, наведите курсор и нажмите .

5 Включите или выключите набор правил (по умолчанию набор правил включён).

6 Задайте название набора правил.

7 Выберите вкладку типа правил, которые вы хотите создать или изменить:

- **Правила транспортного уровня**;
- **Правила прикладного уровня**.

Примечание. Правила транспортного уровня определяют, какие IP-пакеты будут обрабатываться правилами прикладного уровня. Если в наборе нет правил транспортного уровня, правила прикладного уровня не применяются, и весь трафик будет пропускаться или блокироваться на основании сетевых фильтров межсетевого экрана.

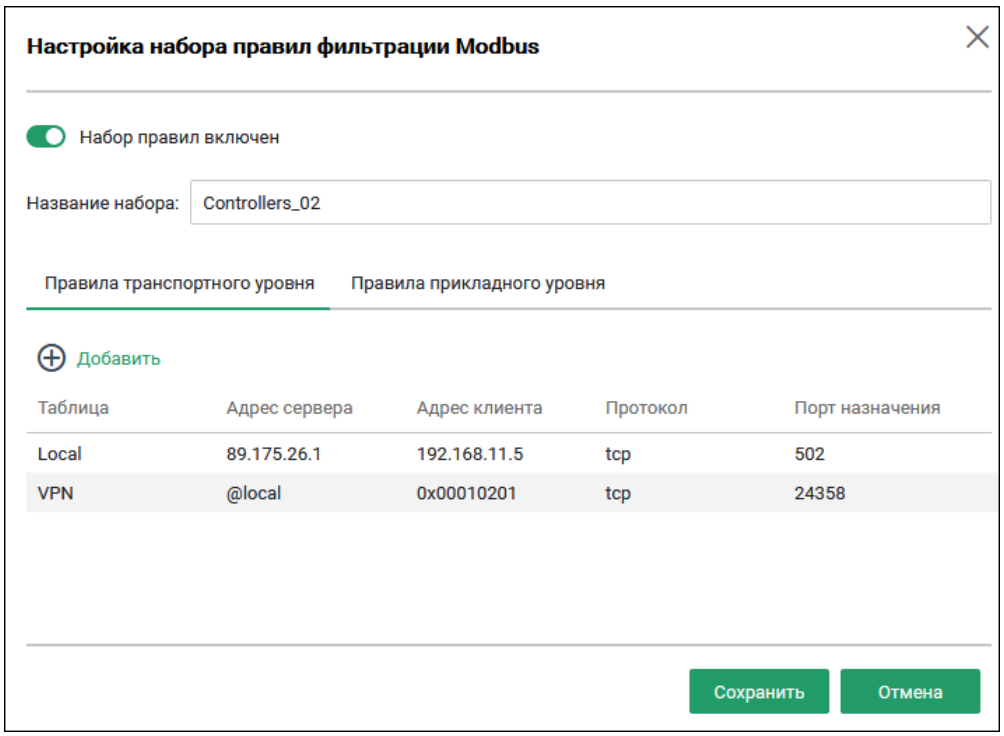


Рисунок 47. Настройка правил фильтрации транспортного уровня

8 Выполните одно из действий:

- Чтобы создать правило, нажмите ⊕ **Добавить**;
- Чтобы изменить правило, наведите курсор на него и нажмите ✎.

9 В зависимости от выбранного протокола и типа правил задайте следующие параметры:

- Для правила транспортного уровня:
  - таблица, для которой предназначено правило;
  - адрес сервера (адрес узла, который ожидает TCP-соединение): для локального, транзитного и туннелируемого трафика — IP-адрес, доменное имя, диапазон IP-адресов, список IP-адресов, список доменных имён, маска адресов подсети, системная группа объектов (`@any`, `@local` или `@remote`), пользовательские группы IP-адресов; для защищённого трафика (`vpn`) — идентификатор узла или сети ViPNet, список идентификаторов, системная группы объектов (`@any`, `@allcoordinators`, `@allclients`, `@local` или `@remote`);
  - адрес клиента (адрес узла, который запрашивает TCP-соединение) — список возможных значений совпадает с предыдущим параметром;
  - транспортный протокол — TCP;

- порт назначения (число, диапазон, список или их сочетания).

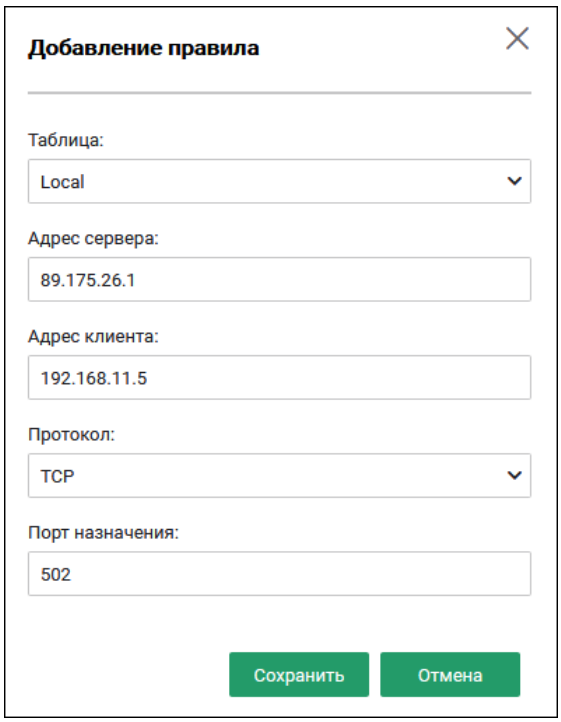


Рисунок 48. Создание правила фильтрации транспортного уровня

- Для правила прикладного уровня протокола Modbus:
  - имя правила;
  - действие правила;
  - идентификатор Modbus-устройства (число, диапазон, список или их сочетания);
  - код функции (число, диапазон, список или их сочетания);

> **Совет.** Чтобы выбрать код функции из списка допустимых значений, нажмите .

  - диапазон регистров чтения (число, диапазон, список или их сочетания);
  - диапазон регистров записи (число, диапазон, список или их сочетания).

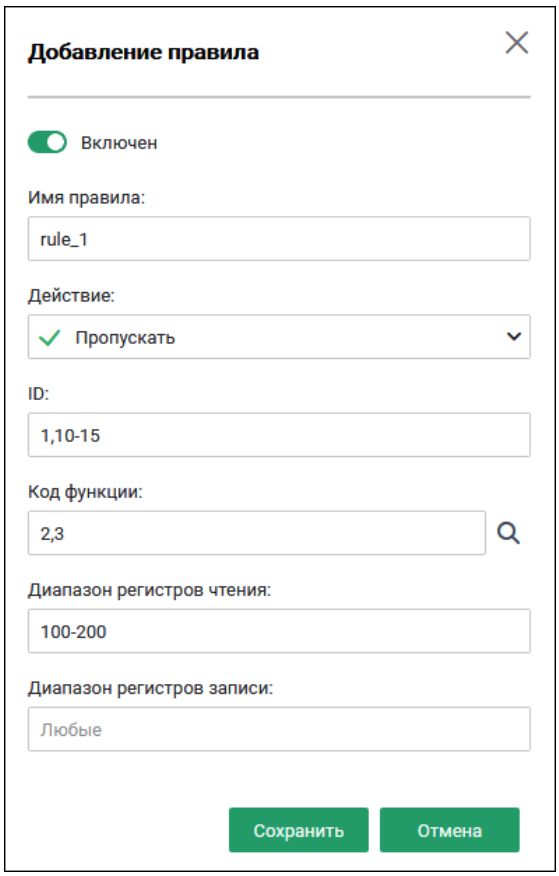


Рисунок 49. Создание правил фильтрации прикладного уровня для протокола Modbus

- Для правила прикладного уровня протокола МЭК 60870-5-104:
  - имя правила;
  - действие правила;
  - общий адрес (число, диапазон, список или их сочетания);
  - адрес объекта информации (число, диапазон, список или их сочетания);

> **Примечание.** Для фильтрации пакетов со структурированным адресом объекта информации необходимо приводить адрес к неструктурированному виду (десятичному числу).

  - идентификатор типа для объектов информации (число, диапазон, список или их сочетания).

> **Совет.** Чтобы выбрать идентификаторы типа для объектов информации из списка допустимых идентификаторов, нажмите .

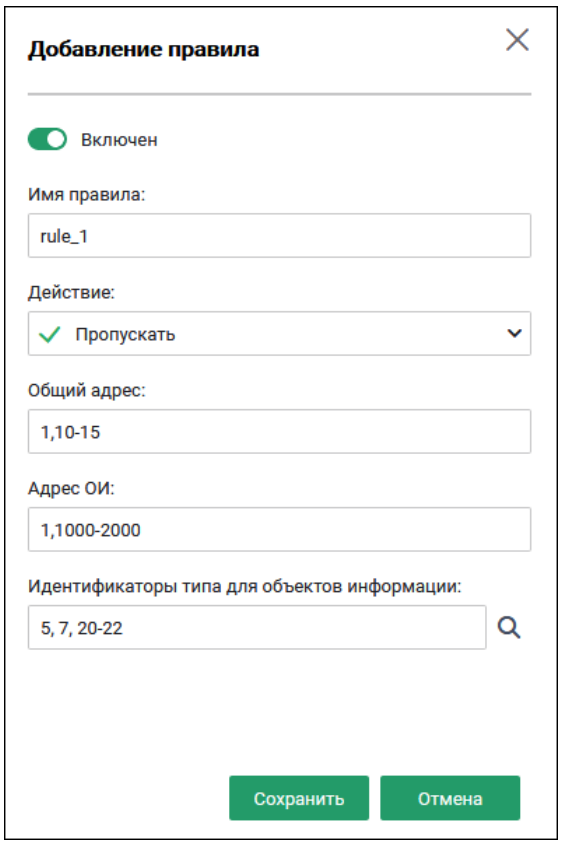


Рисунок 50. Создание правила фильтрации прикладного уровня для протокола МЭК 60870-5-104

10 Нажмите **Сохранить**.

Внимание! Максимальное количество правил прикладного уровня для вашего исполнения ViPNet Coordinator IG см. в документе «Подготовка к работе» в разделе «Основные отличия аппаратных платформ». Превышение этого количества может значительно снизить производительность ViPNet Coordinator IG.

11 Во вкладке **Правила прикладного уровня** вы можете:

- Включить или выключить правило фильтрации.
- Изменить приоритет правила. Для этого перетащите его на нужную позицию с помощью значка ⠿.

№	Статус	Имя	Действие	ID	FC	R	W
1		rule_1	Пропуск...	1, 10-15	2, 3	100-200	Любой
2		rule_2	Блокиро...	Любой	20	Любой	Любой

Рисунок 51. Настройка правил фильтрации прикладного уровня для протокола Modbus

12 Чтобы изменить формат протокола МЭК 60870-5-104:

12.1 В окне **Настройка набора правил фильтрации МЭК104** выберите вкладку **Формат протокола**.

12.2 Задайте параметры:

- длина общего адреса;
- причина передачи;
- длина адреса информационного объекта;
- максимальная длина APDU (число от 2 до 253);

Чтобы установить значения по умолчанию, нажмите **Сбросить формат**.

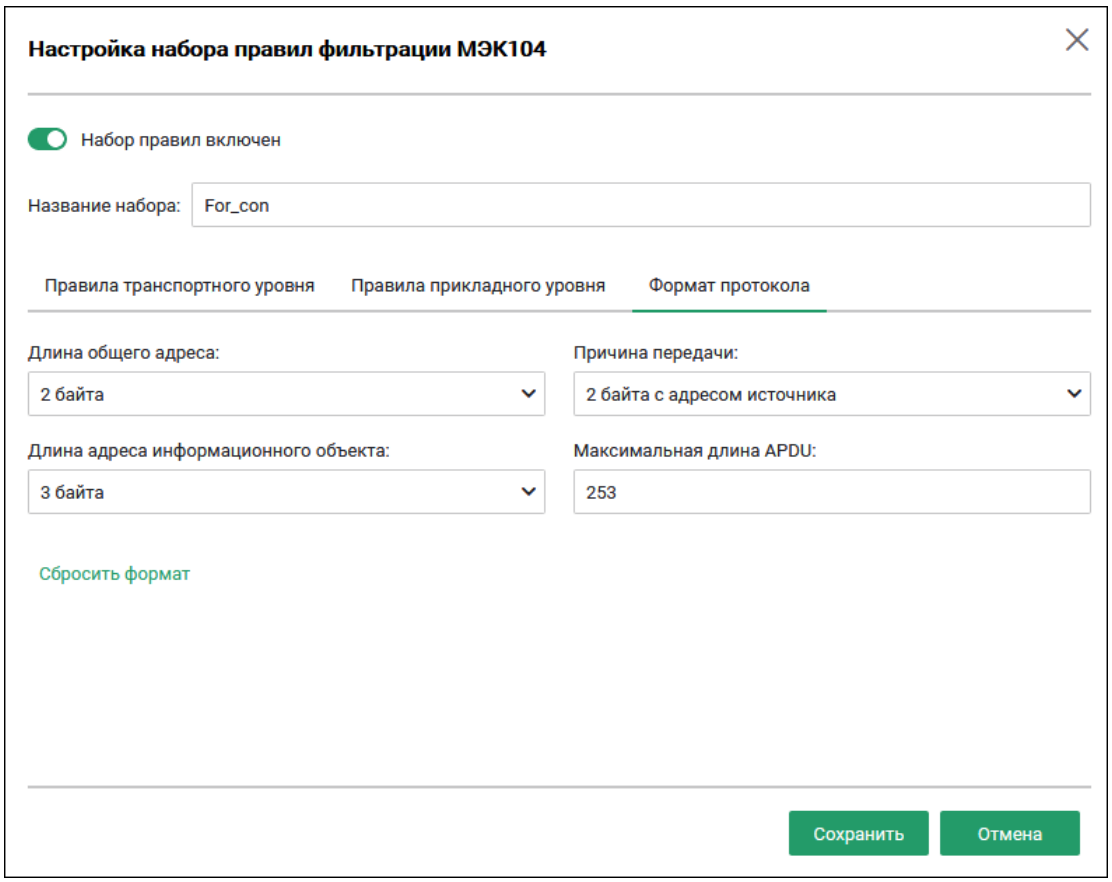


Рисунок 52. Настройка формата протокола МЭК 60870-5-104

13 Нажмите **Сохранить**.

Внимание! К уже установленным соединениям локального Modbus-трафика (открытого и защищённого) изменения в наборе правил (создание, изменение, удаление правила) применяются не сразу, а через одну минуту. В течение этого времени указанный трафик будет заблокирован. Чтобы применить изменения вручную, перезапустите шлюз Modbus (см. Настройка шлюза Modbus).

Невозможно создать два и более набора правил, в которых таблицы правил транспортного и прикладного уровней полностью совпадают, даже если эти наборы имеют разные имена. Например, нельзя создать два пустых набора правил.

Просмотр наборов правил промышленного протокола

Чтобы просмотреть набор правил промышленного протокола:

1. Выберите **Межсетевой экран** > **Фильтрация промышленных протоколов.**
2. Выберите вкладку промышленного протокола:
   - **Modbus** – для протокола Modbus;
   - **МЭК104** – для протокола МЭК 60870-5-104.

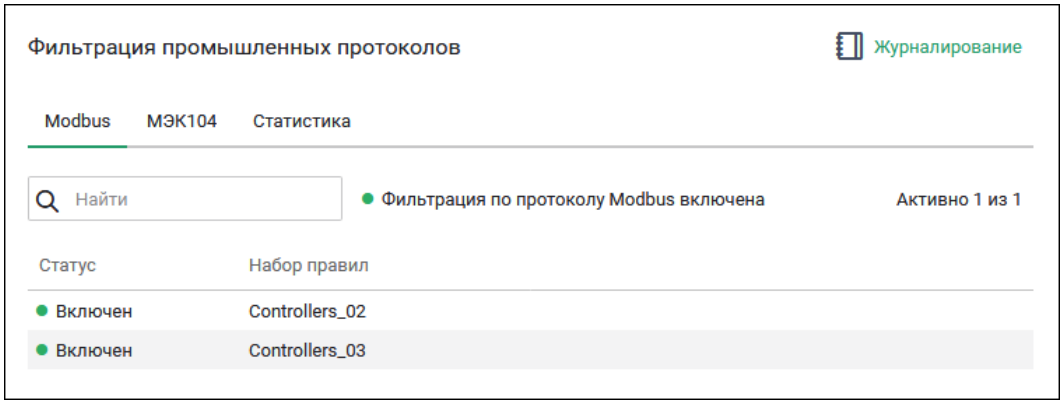


Рисунок 53. Просмотр наборов правил фильтрации протокола Modbus

3. Нажмите на набор правил, который хотите просмотреть.
4. Выберите одну из вкладок:
   - **Правила транспортного уровня**;
   - **Правила прикладного уровня**.

   В результате отобразится список правил фильтрации в порядке убывания их приоритета.

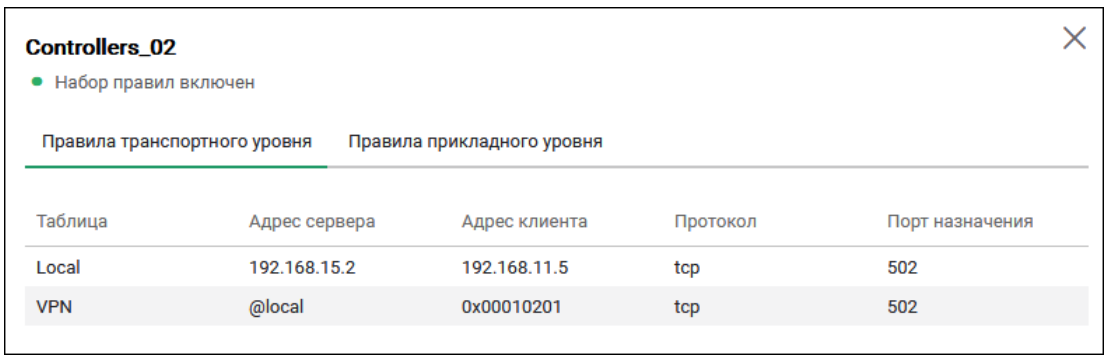


Рисунок 54. Просмотр правил фильтрации транспортного уровня

Настройка прокси-сервера

Общие сведения о работе прокси-сервера

Прокси-сервер ViPNet Coordinator IG 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 HTTP-трафика внешним антивирусом по протоколу ICAP.



Рисунок 55. Схема работы прокси-сервера ViPNet Coordinator IG

Порядок обработки запроса при обращении к интернет-ресурсу:

1 Запрос от клиента прокси-сервера поступает на ViPNet Coordinator IG:
   - Обрабатывается сетевыми фильтрами:
     - если сработал запрещающий сетевой фильтр, то передача IP-пакетов блокируется, в журнал IP-пакетов добавляется запись об этом событии (см. События журнала IP-пакетов);
     - если запрос не попал под действие ни одного из запрещающих сетевых фильтров, он передаётся на прокси-сервер.
   - Если включена контент-фильтрация трафика, то запрос обрабатывается её 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 передаётся на интернет-ресурс.
3 Ответ от интернет-ресурса поступает на ViPNet Coordinator IG:

- Обрабатывается сетевыми фильтрами аналогично шагу 1.
- Если включена функция фильтрации содержимого трафика, то ответ обрабатывается её 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 передаётся 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 IG.
- «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 IG, на котором запущен прокси-сервер.

Настройка основных параметров прокси-сервера

На ViPNet Coordinator IG:

- Выберите внешний сетевой интерфейс прокси-сервера, задайте IP-адреса, на которые прокси-сервер будет принимать запросы от пользователей («прослушивать» их), и IP-адреса локальных сетей, которым разрешено использовать прокси-сервер.
- Настройте и включите DNS-сервер (см. Настройка DNS-сервера).

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

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

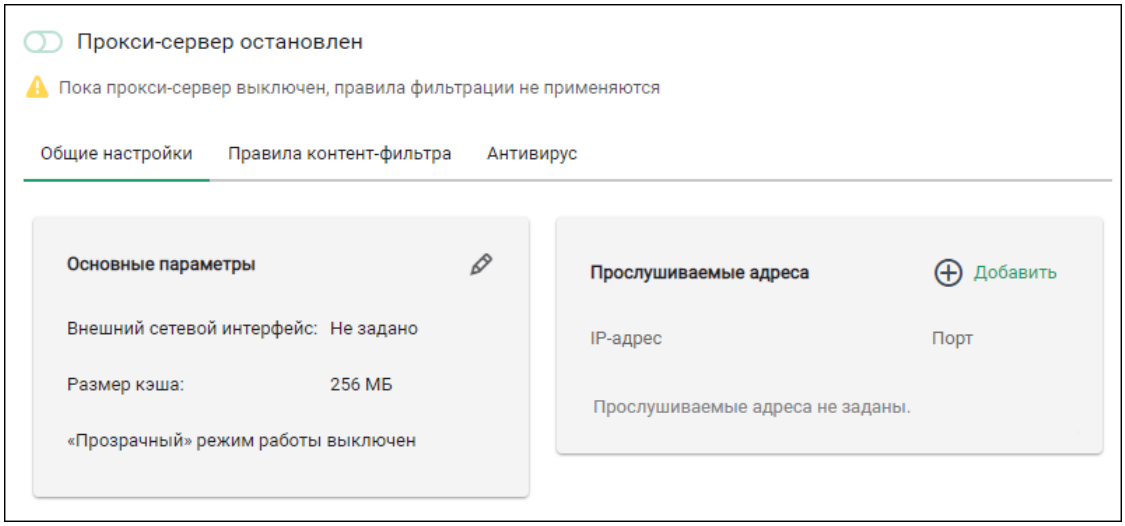


Рисунок 56. Общие настройки прокси-сервера

2 В разделе **Основные параметры** нажмите  .

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

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

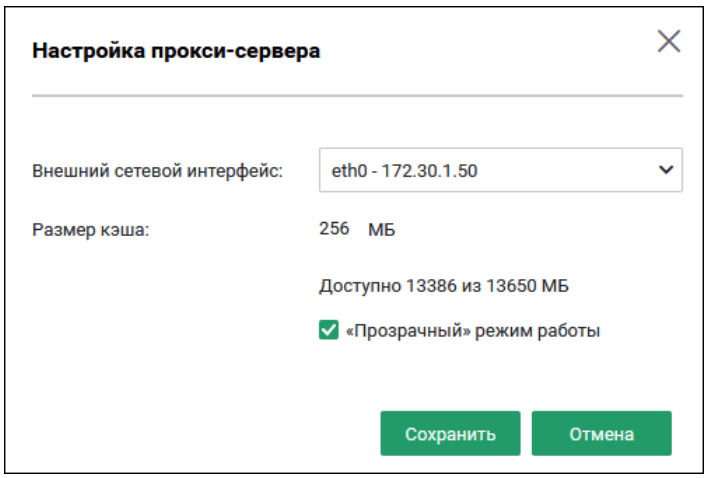


Рисунок 57. Настройка основных параметров прокси-сервера

Примечание. По умолчанию в «прозрачном» режиме работы прокси-сервера к DNS-серверу ViPNet Coordinator IG могут обращаться только защищённые узлы. Если необходимо предоставить доступ к DNS-серверу для открытых узлов, создайте локальный фильтр открытой сети `Allow DNS in`, разрешающий входящий трафик с этих узлов на DNS-сервер:

- Действие — **Пропускать трафик**.
- Источники — **Группа IP-адресов** > **InternetIP**.
- Назначения — **Мой узел**.
- Протоколы — TCP:53, UDP: 53.

2.3 Нажмите **Сохранить**.

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

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

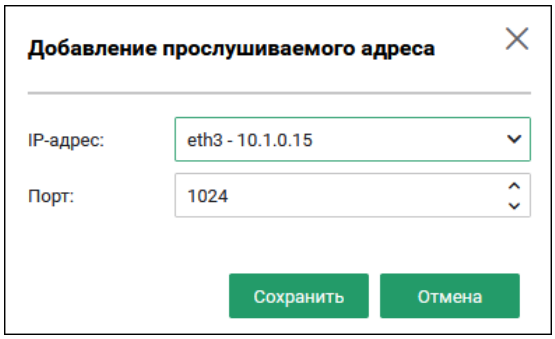


Рисунок 58. Добавление прослушиваемого адреса прокси-сервера

Примечание. Задавайте для прослушивания сетевые интерфейсы со статическими IP-адресами.

5 Нажмите **Сохранить**.

6 Запустите прокси-сервер.

При запуске прокси-сервера автоматически создаются сетевые фильтры и правила трансляции адресов, необходимые для доступа в интернет через прокси-сервер для узлов защищённой и открытой сетей. При завершении работы прокси-сервера они автоматически удаляются.

Примечание. Если для подключения к интернету ViPNet Coordinator IG использует маршрут с несколькими шлюзами (multi-hop route), для корректной работы прокси-сервера создайте локальный фильтр открытой сети:

- Действие — **Пропускать трафик**.
- Источники — **Мой узел**.
- Назначения — **Группа IP-адресов** > **InternetIP**.
- Протоколы — TCP: 21, TCP: 80, TCP: 443.

При первом запуске прокси-сервера создаётся пользовательская группа объектов `HttpProxyUsers`. По умолчанию в неё 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). Использование прокси-сервера разрешено для IP-адресов локальных сетей, входящих в группу `HttpProxyUsers`.

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.

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:

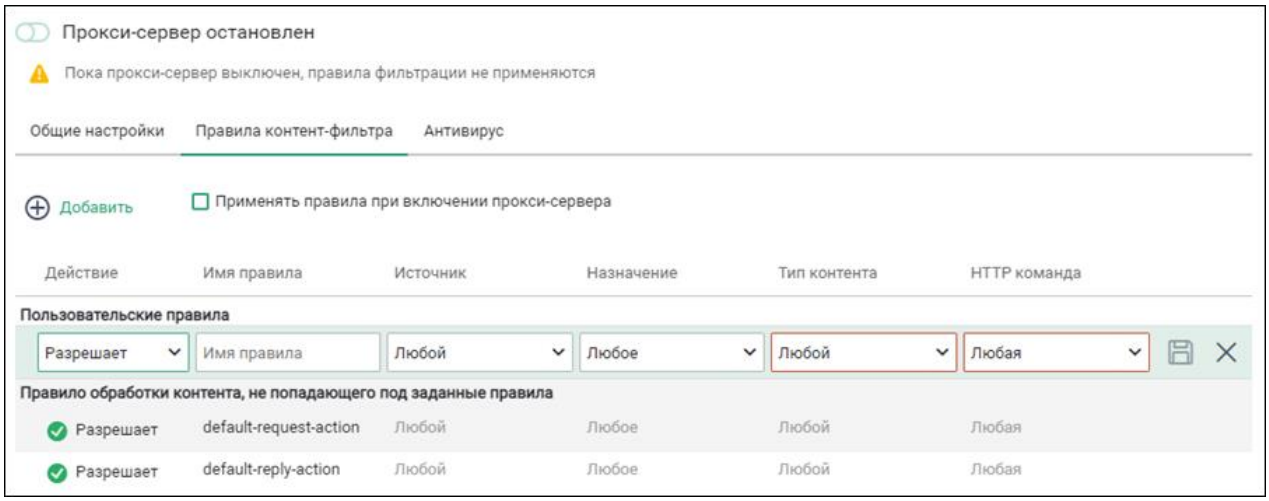


Рисунок 59. Добавление правила фильтрации

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 — удалённый HTTP-сервер.

3.4 Выберите тип контента.

MIME-тип файла может зависеть от настроек удалённого 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 трафика

Примечание. Антивирусная проверка трафика поддерживается только в исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1.

Если на ViPNet Coordinator IG запущен прокси-сервер, вы можете настроить антивирусную проверку данных, передаваемых через него по HTTP в обоих направлениях: из интернета к пользователю и от пользователя в интернет, например при добавлении вложения в сообщение электронной почты с помощью веб-интерфейса. Проверка выполняется внешним антивирусом по протоколу ICAP.

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

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

2 Остановите прокси-сервер.

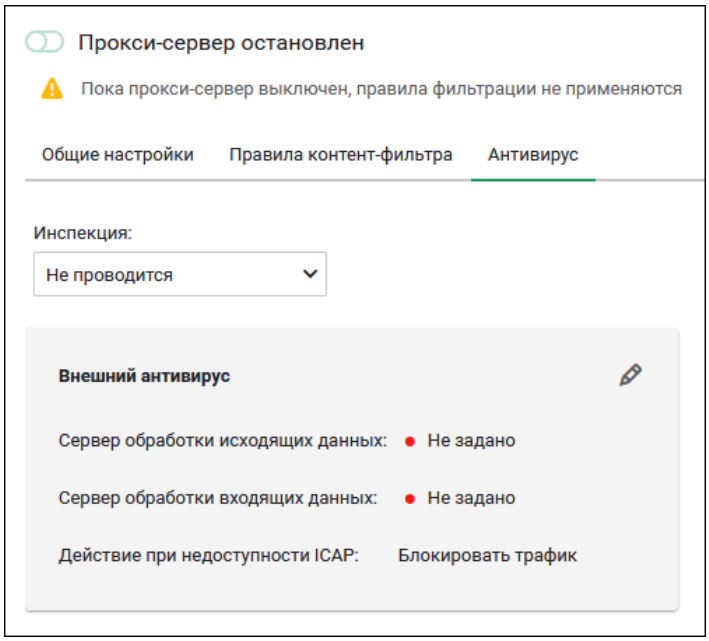


Рисунок 60. Настройка антивирусной проверки

3 В разделе **Внешний антивирус** нажмите .

4 В окне **Настройки внешнего антивируса**:

4.1 В полях **Сервер обработки исходящих данных** и **Сервер обработки входящих данных** задайте пути в формате `icap://<адрес>[:<порт>]/[<путь>]`, например: `icap://192.168.1.45:1344/`.

Вместо IP-адреса можно указать доменное имя.

В качестве параметра <путь> — путь на ICAP-сервере. Если <путь> не указан, IP-пакеты будут отправляться в корень URL.

Если <порт> не указан, будет использоваться значение по умолчанию 1344.

Внимание! В конце адреса ICAP-сервера необходимо указать символ «/».

4.2 В списке **Действие при недоступности ICAP** выберите одно из них: пропускать или блокировать трафик.

4.3 Нажмите **Сохранить**.

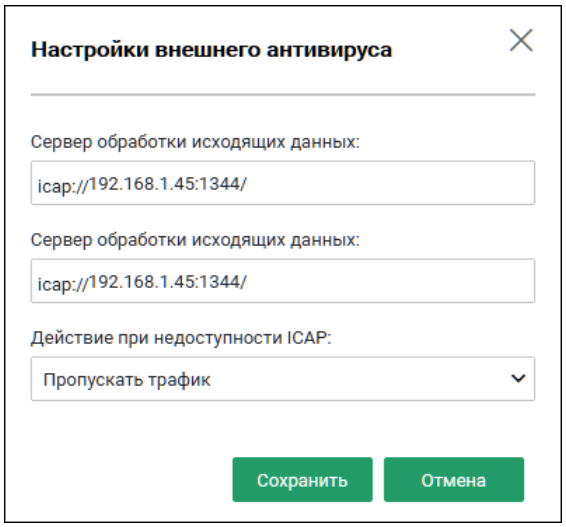


Рисунок 61. Настройка внешнего антивируса

5 Запустите прокси-сервер.

5

Настройка правил трансляции адресов

Трансляция сетевых адресов (NAT) 101

Просмотр правил трансляции адресов 104

Создание и изменение правил трансляции адресов 106

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 IG 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. 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 защищённого 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.

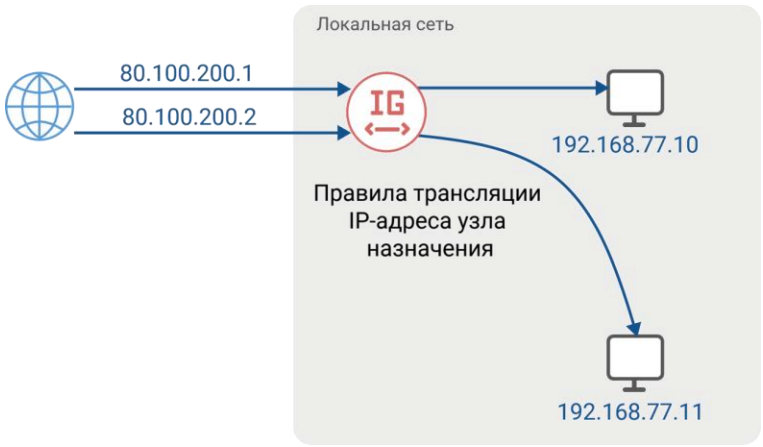


Рисунок 62. Доступ к внутренним ресурсам при помощи трансляции IP-адресов узлов назначения

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 передаётся 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.

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 63. Организация доступа в интернет при помощи 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 IG 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

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

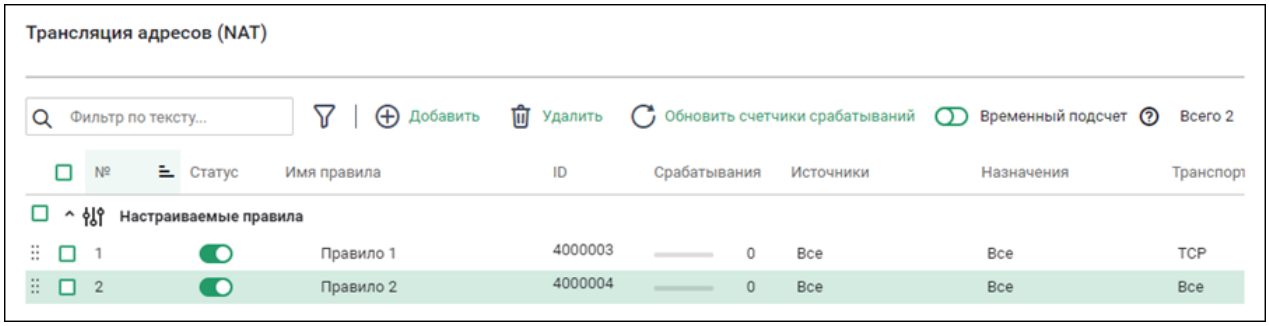


Рисунок 64. Просмотр правил трансляции адресов

2 Чтобы просмотреть определённые правила, нажмите и укажите критерии поиска.

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

Счётчик срабатывания правил

В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 таблица содержит поле **Срабатывания**, в котором отображается количество срабатываний правил трансляции адресов. На основе информации о количестве срабатываний вы можете изменить порядок расположения правил в таблице, например передвинуть часто срабатывающие правила в начало таблицы. Это поможет оптимизировать производительность ViPNet Coordinator IG.

Если необходимо подсчитать количество срабатываний правил за определённое время, мы можете включить **Временный подсчет**. Тогда параллельно постоянному счётчику запустится временный счётчик срабатываний, и поле **Срабатывания** будет отображать значения временного счётчика. После выключения временного подсчёта снова будут отображаться значения постоянного счётчика срабатываний. Во время работы временного счётчика постоянный счётчик не останавливается.

Значения срабатываний обновляются автоматически с задержкой порядка 30 секунд при переходе в раздел **Трансляция адресов (NAT)** или при обновлении страницы браузера. Чтобы обновить значения срабатываний вручную, нажмите **Обновить счетчики срабатываний**.

Чтобы просмотреть сводные сведения о срабатывании правил трансляции адресов:

1 Выберите **Состояние системы**.

Сводные сведения отображаются на панели **Сетевые фильтры и правила трансляции**.

2 Нажмите , чтобы просмотреть сведения подробнее или перейти на страницу настройки сетевых фильтров или правил трансляции адресов.

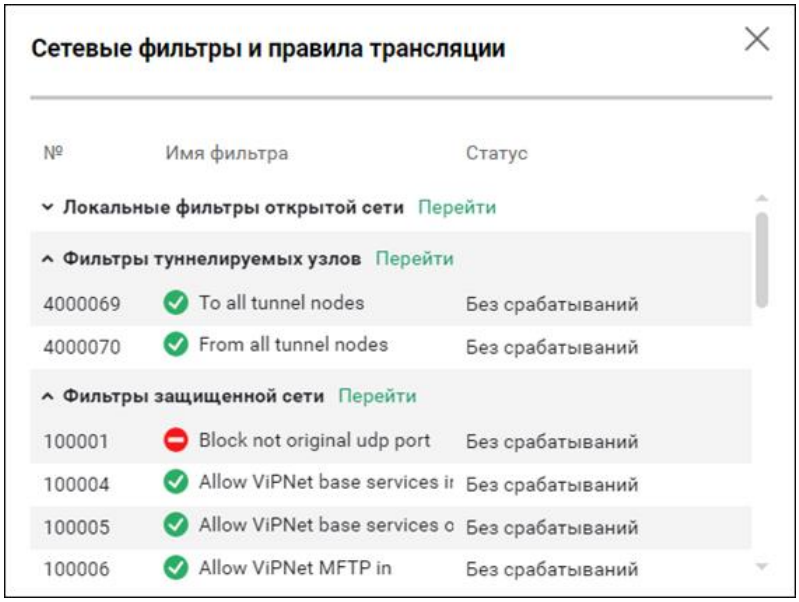


Рисунок 65. Подробные сведения о сетевых фильтрах и правилах трансляции адресов

Создание и изменение правил трансляции адресов

Примечание. Правила трансляции адресов работают только при наличии транзитных фильтров открытой сети, пропускающих трафик от узлов, к которым они будут применяться.

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 IG, выберите **Адрес исходящего интерфейса (определяется автоматически).**
- Чтобы указать другой IP-адрес для замены IP-адреса отправителя, выберите **Другой адрес** и задайте его.

Примечание. При использование другого адреса, не принадлежащего ViPNet Coordinator IG, на сетевом устройстве, расположенным за ViPNet Coordinator IG, настройте обратную маршрутизацию на ViPNet Coordinator IG (или на другое устройство, например для балансировки) для корректной обработки ответного трафика.

Если на сетевом устройстве нельзя настроить обратную маршрутизацию, используйте в качестве другого адреса только IP-адреса, принадлежащие ViPNet Coordinator IG или автоматическое определение адреса исходящего интерфейса.

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 определённым 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 определённых отправителей IP-пакетов, в разделе **Добавить** раскройте список **Источники** и

укажите IP-адреса, диапазоны IP-адресов, доменные имена или группы IP-адресов (см. Группа IP-адресов).

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

10 Нажмите **Сохранить**.

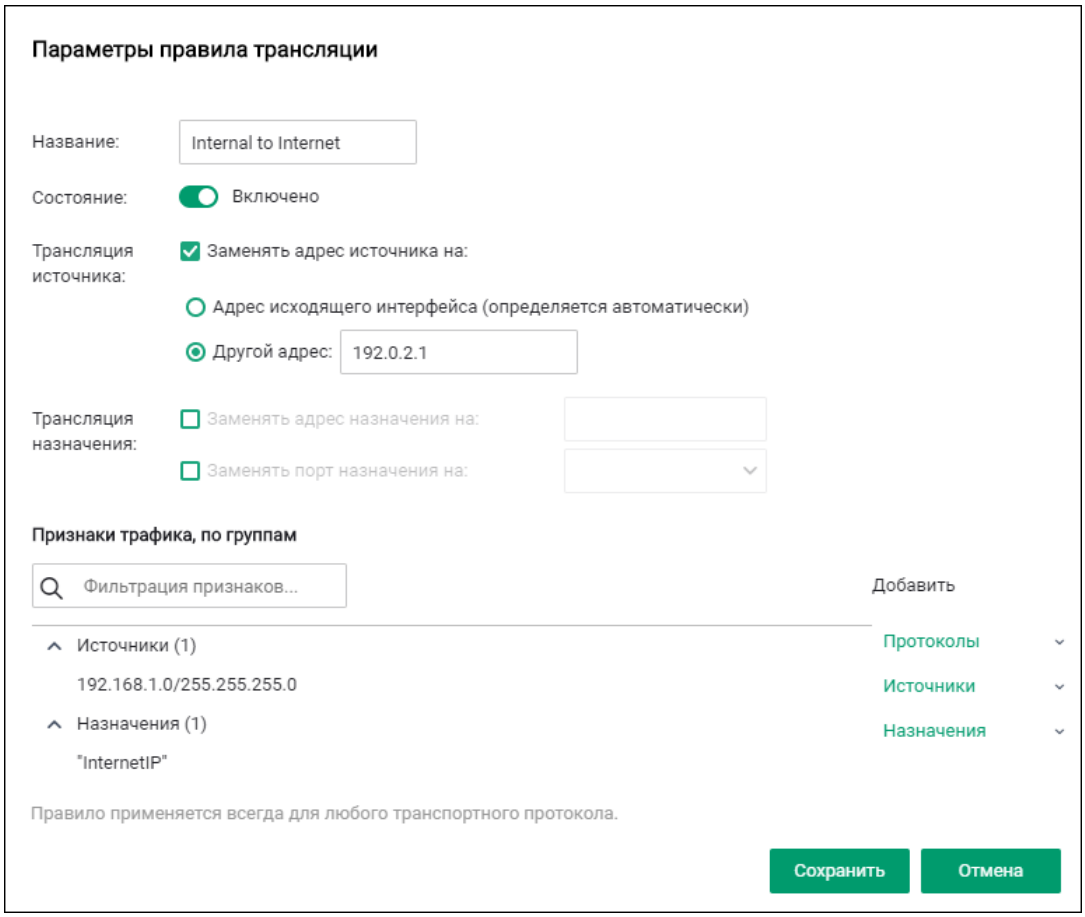


Рисунок 66. Создание правила трансляции адресов

11 Чтобы изменить приоритет правила трансляции, в списке правил наведите курсор на значок ⠿ строки правила и перетащите её на нужную позицию.

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

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

6

Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP

О прикладных протоколах 109

Настройка параметров обработки прикладных протоколов 111

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 защищённой 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 IG 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.

ViPNet Coordinator IG поддерживает также обработку промышленных прикладных протоколов, что позволяет фильтровать трафик между промышленными устройствами на прикладном уровне. Подробнее см. Настройка фильтрации промышленных протоколов. Фильтрация трафика промышленных протоколов доступна для открытого, туннелируемого и защищённого трафика.

Поддерживаемые прикладные протоколы

- 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 IG.
- SIP — для организации сеансов связи (мультимедийных конференций, телефонных соединений) и распределения мультимедийной информации.

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

- 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 CallManager).

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

Примечание. ViPNet Coordinator IG 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.

- Промышленные протоколы:
  - Modbus — для взаимодействия электронных устройств на промышленных объектах.
  - МЭК 60870-5-104 — для контроля и управления территориально распределёнными процессами в электроэнергетике.

Настройка параметров обработки прикладных протоколов

По умолчанию в ViPNet Coordinator IG включена обработка всех поддерживаемых прикладных протоколов, кроме промышленных протоколов.

Примечание.

- Настройка обработки промышленных протоколов выполняется отдельно (см. Настройка фильтрации промышленных протоколов).
- Трафик обрабатываемого прикладного протокола не должен проходить через трансляцию сетевых адресов. Это ограничение не распространяется на FTP-трафик и трафик промышленных протоколов. Для маршрутизации обратного трафика от туннелируемых узлов укажите координатор в качестве шлюза по умолчанию для таких узлов.
- Для туннелируемых узлов по умолчанию созданы фильтры, разрешающие передачу трафика по любым IP-адресам, протоколам и портам. Если вы настраиваете обработку прикладных протоколов в туннелируемом трафике, то в целях безопасности рекомендуется удалить эти фильтры и создать фильтры, разрешающие соединения между конкретными узлами по транспортным протоколам и портам, заданным в параметрах настройки прикладных протоколов.

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

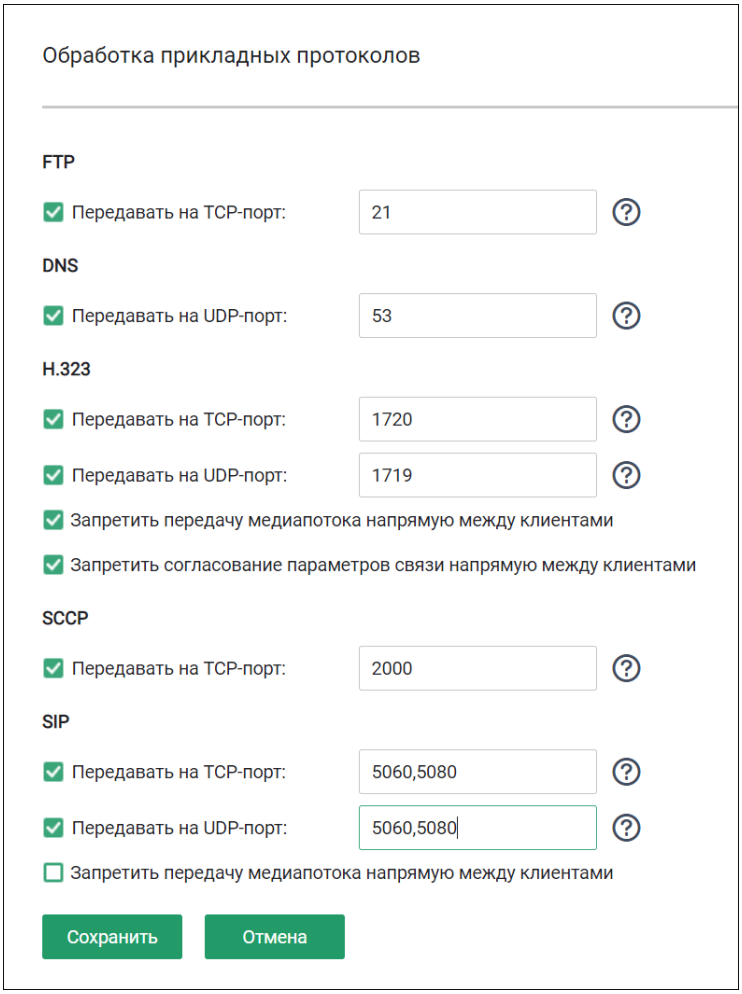


Рисунок 67. Обработка прикладных протоколов

Внимание! При выключении обработки прикладного протокола работа соответствующих сетевых служб на узле защищённой сети 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 В строке прикладного протокола:

2.1 Выберите транспортный протокол, используемый прикладным протоколом:

- **Передавать на TCP-порт**.
- **Передавать на UDP-порт**.

2.2 Введите порт, диапазон портов или список портов, разделённых запятой.

3 Настройте обработку протоколов SIP и H.323 согласно разделу Особенности обработки прикладных протоколов DNS, FTP, SIP и H.323.

4 Нажмите **Сохранить**.



Внимание! Заданные параметры обработки должны соответствовать параметрам, указанным в настройках соответствующих приложений (FTP-клиент, DNS-клиент, SIP-клиент и так далее).

После изменения настроек обработки прикладных протоколов (в том числе, включения или выключения) перезапустите приложение (например, DNS-, FTP-, SIP-клиент) или устройство (например, SIP-телефон).

Особенности обработки прикладных протоколов DNS, FTP, SIP и H.323

Обработка протокола DNS

В сетях ViPNet приложения могут использовать виртуальные IP-адреса, реально не существующие в сети и уникальные на каждом сетевом узле, что позволяет избежать конфликтов при наличии пересекающихся адресов в разных сетях.

Чтобы узлы внутренней сети ViPNet могли обращаться к удалённым узлам ViPNet по доменным именам через туннелируемый DNS-сервер, требуются дополнительные настройки на DNS-сервере и узлах сети ViPNet:

1 На DNS-сервере настройте поддержку динамического изменения DNS-записей. Как правило, по умолчанию DNS-серверы не поддерживают эту настройку.

2 Для клиентов, к которым будут обращаться по доменному имени:

   2.1 В ViPNet Prime укажите корпоративный DNS-сервер.

   2.2 На самих клиентах настройте автоматическую регистрацию на DNS-сервере.

3 На туннелирующем координаторе включите обработку протокола.

Обработка протокола FTP

При передаче файлов между клиентом и сервером по протоколу FTP устанавливается как минимум два TCP-соединения:

- для отправки команд на сервер и получения ответов от него — управляющее TCP-соединение;
- для передачи данных — дополнительное TCP-соединение.

TCP-соединения по протоколу FTP устанавливаются в следующем порядке:

1 Клиент создаёт управляющее TCP-соединение с сервером со своего порта из диапазона 1024-65535 на 21-й порт сервера.

2 В зависимости от выбранного режима передачи данных, клиент отправляет по управляющему соединению:

- в активном режиме — номер порта, открытого клиентом для получения данных с сервера;
- в пассивном режиме — запрос на номер порта сервера, к которому будет подключаться клиент.

3 Соединение устанавливается одним из двух способов:

- в активном режиме — сервер создаёт дополнительное соединение для передачи данных на указанный клиентом порт;
- в пассивном режиме — сервер по управляющему соединению передаёт клиенту номер порта, к которому клиент создаёт дополнительное соединение.

Таким образом, в активном режиме соединение для передачи данных создаёт сервер, а в пассивном — клиент.

Чтобы использовать протокол FTP:

1 Разрешите управляющее соединение. Для этого создайте сетевой фильтр, разрешающий исходящее TCP-соединение на 21-й порт FTP-сервера.

2 При использовании активного режима передачи данных разрешите дополнительное соединение. Для этого включите обработку протокола FTP, которая автоматически добавит необходимый сетевой фильтр.

Для разрешения дополнительного соединения в пассивном режиме работы настройки не требуются.

Обработка протокола SIP

При передаче мультимедийных данных по протоколу SIP создаётся управляющее и дополнительное соединение (RTP-сессия). Медиа-потоки в дополнительных соединениях могут передаваться между SIP-клиентами напрямую (т.н. режим Direct Call или Peer-to-Peer RTP) или через сервер телефонии.

Чтобы настроить связь между SIP-клиентами:

1 Убедитесь, что включена обработка протокола SIP.

2 Если хотя бы один SIP-клиент является открытым узлом, убедитесь, что для всех защищённых узлов настроена видимость по реальным IP-адресам.

3 Создайте сетевые фильтры, разрешающие управляющие соединения. Сетевые фильтры должны пропускать трафик между SIP-клиентами и сервером телефонии по транспортным протоколам и портам, заданным в параметрах обработки прикладных протоколов (по умолчанию TCP и UDP с портами 5060 и 5080):

- Если все SIP-клиенты туннелируются координаторами, создайте фильтры туннелируемых узлов.
- Если хотя бы одно SIP-устройство является открытым узлом, создайте транзитные фильтры.

Примечание. Некоторые SIP-клиенты, например SIP-клиент компании Zoiper, могут устанавливать соединения TCP и UDP не через порт 5060, а через динамический порт, выбранный произвольно из определённого диапазона. Поэтому если хотя бы один из SIP-клиентов является открытым узлом, возможность использования динамических портов необходимо отключить в настройках SIP-клиента.

4 Настройте создание сетевых фильтров для разрешения RTP-сессий:

- По умолчанию создаются фильтры, разрешающие RTP-трафик между SIP-клиентами и сервером телефонии. Для этого проверяется совпадение IP-адреса создаваемой RTP-сессии с одним из IP-адресов сигнальной сессии.
- Если на сервере телефонии настроен режим передачи RTP-трафика между SIP-клиентами напрямую (без участия сервера телефонии), снимите флажок **Запретить передачу медиапотока напрямую между клиентами** для протокола SIP и нажмите **Сохранить**.

  После этого разрешающие фильтры будут создаваться без проверки принадлежности RTP-сессии к сигнальной сессии.

Внимание! Сетевые фильтры, которые создаются для режима прямого соединения между SIP-клиентами, будут разрешать RTP-сессии между любыми IP-адресами. Поэтому не рекомендуется использовать этот режим, если ViPNet Coordinator IG размещён на границе защищаемой сети.

Обработка протокола H.323

В наборе протоколов H.323 используются сигнальные протоколы H.225 и H.245. Для передачи медиа-потоков используется RTP. При включении обработки H.323 автоматически создаются временные сетевые фильтры, разрешающие сигнальные H.245-сессии и дополнительные RTP-сессии. При этом, чтобы разрешить сигнальные H.225-сессии, необходимо создать разрешающие сетевые фильтры вручную.

Терминалы H.323 (IP-телефоны) могут устанавливать связь друг с другом напрямую или с участием контроллера зоны (gatekeeper). В зависимости от наличия контроллера зоны и режимов его работы может потребоваться настройка создания временных сетевых фильтров, разрешающих H.245- и RTP-сессии.

Чтобы настроить связь между IP-телефонами по протоколу H.323:

1 Убедитесь, что включена обработка протокола H.323.

2 При использовании IP-телефонов Yate настройте видимость туннелируемых узлов по реальным IP-адресам.

3 Создайте сетевые фильтры, разрешающие сигнальные H.225-сессии между H.323-устройствами. Сетевые фильтры должны пропускать трафик по транспортным протоколам и портам, заданным в параметрах обработки прикладных протоколов (по умолчанию UDP 1719 и TCP 1720):

- Если H.323-устройства туннелируются координаторами, создайте фильтры туннелируемых узлов.
- Если хотя бы одно H.323-устройство является открытым узлом, создайте транзитные фильтры.

4 Настройте автоматическое создание сетевых фильтров, разрешающих дополнительную сигнальную H.245-сессию, а также RTP-сессию:

В зависимости от настроек H.323-телефонии потоки сигнальных H.225- и H.245-сессий могут проходить через контроллер зоны или напрямую между IP-телефонами.

- Если пути прохождения H.255-потока и H.245-потока отличаются, например:

  ```
  H.225: IP-телефон -> контроллер зоны -> IP-телефон
  H.245: IP-телефон -> IP-телефон
  RTP: IP-телефон -> IP-телефон
  ```

  снимите флажок **Запретить согласование параметров связи напрямую между клиентами**.
- Если пути прохождения RTP-потока и родительского H.245-потока отличаются, например:

  ```
  H.225: IP-телефон -> контроллер зоны -> IP-телефон
  H.245: IP-телефон -> контроллер зоны -> IP-телефон
  RTP: IP-телефон -> IP-телефон
  ```

  снимите флажок **Запретить передачу медиапотока напрямую между клиентами**.
- Если H.225-, H.245- и RTP-сессии проходят между IP-телефонами напрямую, например:

  ```
  H.225: IP-телефон -> IP-телефон
  H.245: IP-телефон -> IP-телефон
  RTP: IP-телефон -> IP-телефон
  ```

  выберите **Запретить передачу медиапотока напрямую между клиентами** и **Запретить согласование параметров связи напрямую между клиентами**.

Примечание. В некоторых IP-телефонах (например, Yate) отсутствует H.245-сессия. Если пути прохождения RTP-потока и родительского H.225-потока отличаются, снимите флажок **Запретить передачу медиапотока напрямую между клиентами** для протокола H.323. Иначе, оставьте настройки по умолчанию.

---

5 Нажмите **Сохранить**.

7

Настройка сетевых служб

Настройка DHCP-сервера 118

Настройка DHCP-relay 121

Настройка DNS-сервера 123

Настройка NTP-сервера 125

Настройка точки доступа к сети Wi-Fi 128

Настройка шлюза Modbus 130

Настройка интерфейса GPIO 133

Настройка DHCP-сервера

В состав ViPNet Coordinator IG 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, объединённых по L2OverIP;
- в удалённых подсетях с помощью агента DHCP-relay.

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

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

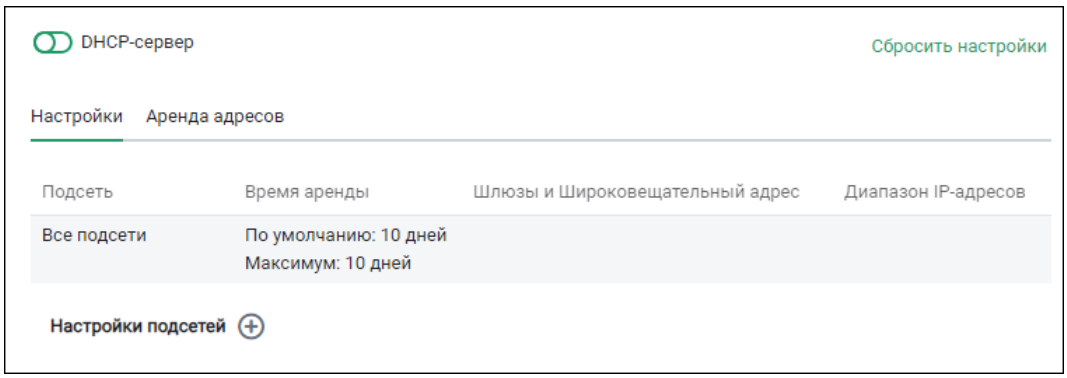


Рисунок 68. Настройка параметров DHCP-сервера

2 Выключите DHCP-сервер.

3 Чтобы добавить подсеть, клиентов которой будет обслуживать DHCP-сервер:

3.1 В разделе **Настройки подсетей** нажмите .

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

3.3 Выберите сетевой интерфейс ViPNet Coordinator IG, на котором будет работать DHCP-сервер.

Интерфейс должен быть включён, иметь статический IP-адрес, и не должен быть дополнительным.

3.4 Для удалённой подсети введите IP-адрес и маску подсети.

Удалённая подсеть должна быть настроена.

3.5 Нажмите **Сохранить**.

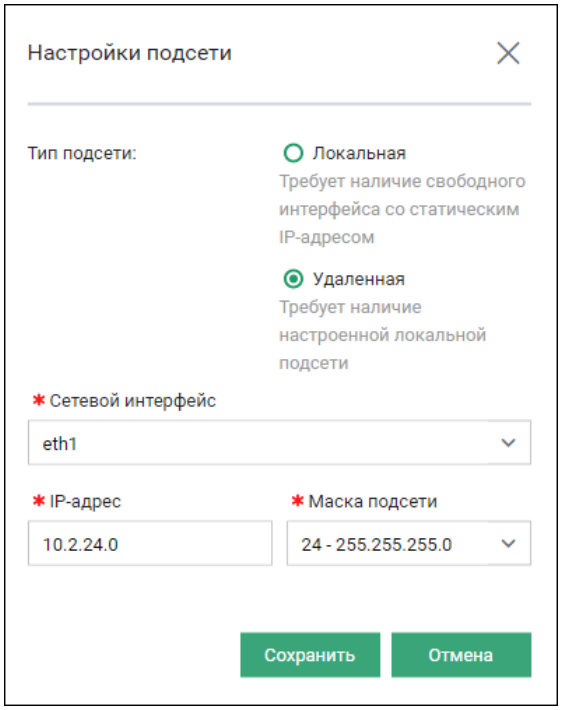


Рисунок 69. Добавление подсети для DHCP-сервера

4 Чтобы задать параметры, передаваемые DHCP-сервером своим клиентам:

4.1 Выберите подсеть.

4.2 В панели справа выберите нужный параметр и нажмите ⊕.

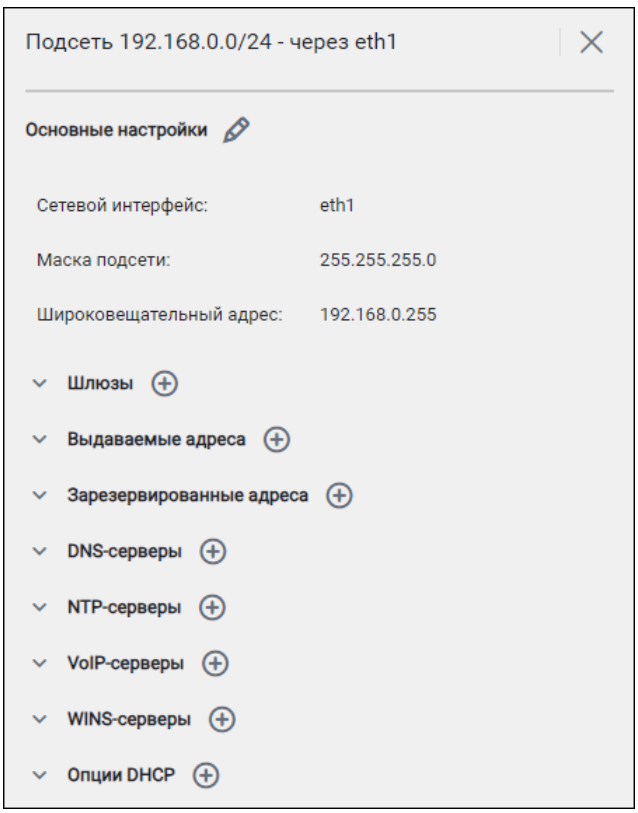


Рисунок 70. Настройка параметров, передаваемых DHCP-сервером

Например, чтобы задать интервал IP-адресов, которые должны присваиваться клиентам DHCP, нажмите ⊕ в группе **Выдаваемые адреса**. Задайте IP-адреса начала и конца диапазона. Диапазон адресов должен принадлежать подсети интерфейса и не должен включать IP-адрес самого интерфейса.

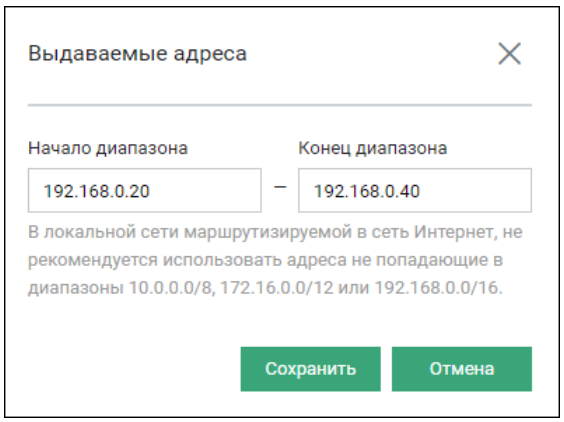


Рисунок 71. Добавление диапазона IP-адресов для DHCP-клиентов

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.

4.3 Нажмите **Сохранить**.

5 Чтобы настроить время аренды IP-адресов, выделяемых DHCP-сервером своим клиентам, нажмите ✎ в разделе **Основные настройки**.

При этом параметр **Максимальное время аренды** задаёт ограничение для клиентов, которые сами запрашивают определённое время аренды у DHCP-сервера.

6 Включите ⬤ DHCP-сервер.

Чтобы просмотреть список клиентов DHCP-сервера, перейдите на вкладку **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 IG можно использовать в качестве агента DHCP-relay. Он принимает от узлов DHCP-запросы и передаёт 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 разветвлённой сети из нескольких подсетей, в которых нет своего DHCP-сервера.

Агент DHCP-relay может работать с несколькими локальными сетями. Это могут быть как сети, подключённые к разным физическим сетевым интерфейсам ViPNet Coordinator IG, так и виртуальные локальные сети, подключённые 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 IG, могут быть защищёнными и открытыми. DHCP-сервер может быть защищённым, 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 IG, выступающего в качестве агента DHCP-relay, и не будут доставлены.

Чтобы запустить DHCP-relay:

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

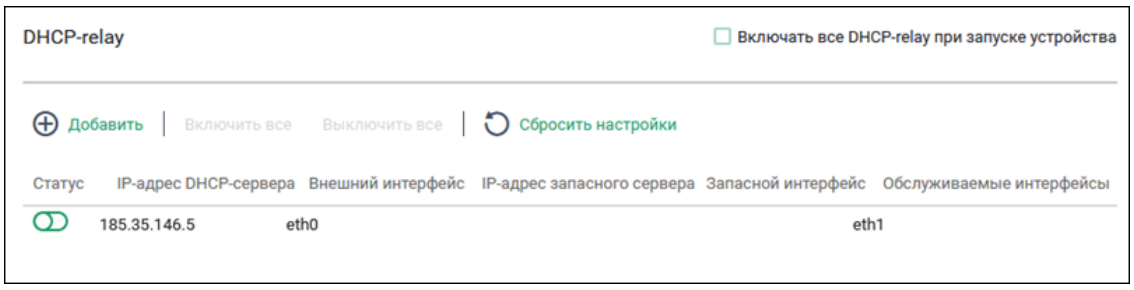


Рисунок 72. Настройка параметров DHCP-ретранслятора

2 Нажмите **Добавить**.

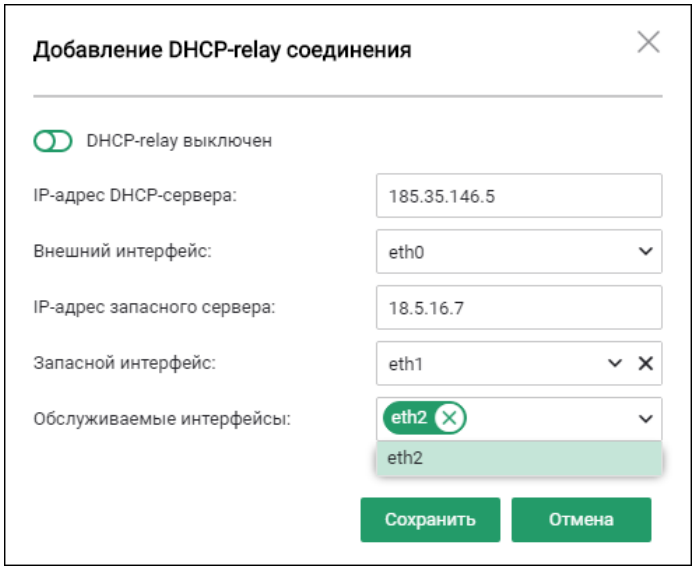


Рисунок 73. Добавление соединения DHCP-relay

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 IG, 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 IG, выберите **Включать все DHCP-relay при запуске устройства**.

Настройка DNS-сервера

DNS-сервер преобразует доменные имена в IP-адреса в ответ на запросы 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 IG, 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 IG.

  Настройте получение информации о DNS-серверах только на одном интерфейсе. Данные об адресах DNS-серверов поступают автоматически, откажитесь от их получения (см. Настройка сетевых интерфейсов Ethernet).

- 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.

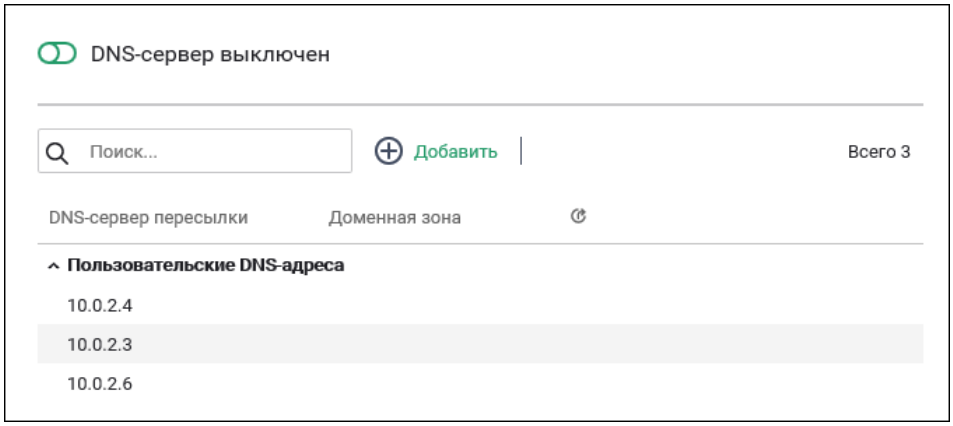


Рисунок 74. Настройка параметров DNS-сервера

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

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

По умолчанию локальный NTP-сервер синхронизирует время с публичными NTP-серверами:

- `ntp1.vniiftri.ru`;
- `ntp2.vniiftri.ru`;
- `ntp.ix.ru`.

Вы можете добавить синхронизацию времени с другими NTP-серверами (публичными или корпоративными).

Дополнительные NTP-серверы:

- 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 IG, то результат синхронизации времени на ViPNet Coordinator IG и на NTP-клиентах не определён, так как неизвестно, какой сетевой интерфейс будет включён первым и какой список дополнительных NTP-серверов получит ViPNet Coordinator IG.

  Настраивайте получение адресов NTP-серверов только на одном интерфейсе и откажитесь от их получения при настройке других интерфейсов, на которых включён режим DHCP (см. Настройка сетевых интерфейсов Ethernet).

- Добавить вручную.

Дополнительный NTP-сервер может находиться как в защищённой, так и в открытой сети:

- Если дополнительный NTP-сервер — узел защищённой сети, видимый по реальному адресу, то для успешной синхронизации времени с таким сервером настройте видимость этого узла по реальному IP-адресу.
- Если дополнительный NTP-сервер — узел открытой сети, добавьте разрешающий фильтр открытой сети для входящего трафика по UDP-порту 123.

Чтобы настроить параметры NTP-сервера:

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

  Список NTP-серверов включает в себя серверы, заданные по умолчанию, заданные пользователем и полученные автоматически от DHCP-сервера. Изменить или удалить серверы, полученные автоматически, невозможно.

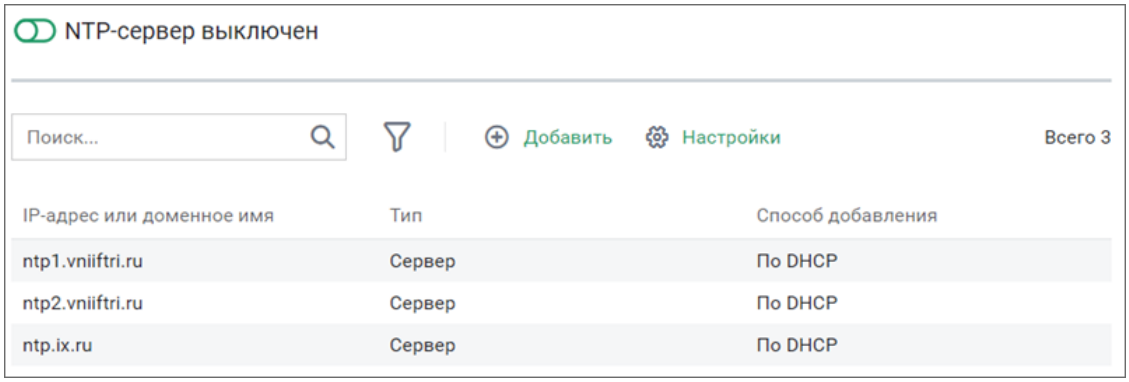


Рисунок 75. Настройка параметров NTP-сервера

2 Чтобы добавить адрес дополнительного NTP-сервера:

2.1 Нажмите **Добавить.**

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

2.3 Укажите тип:

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

2.4 Нажмите **Сохранить.**

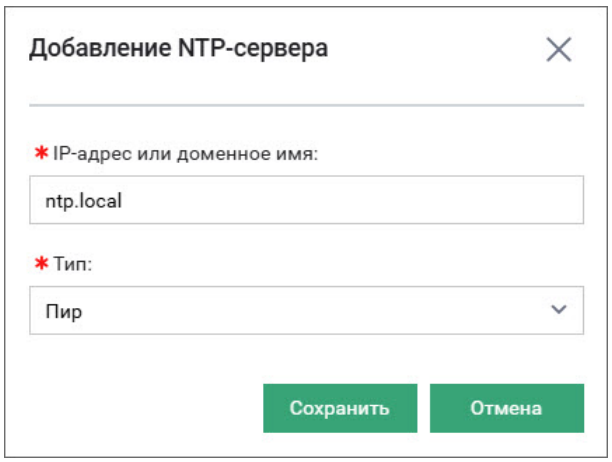


Рисунок 76. Добавление NTP-сервера

3 Нажмите **Настройки.**

4 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 четырёх дополнительных NTP-серверов. Иначе, если один из серверов выйдет из строя, у ViPNet Coordinator IG не будет достаточно информации, чтобы определить, какой из оставшихся серверов предоставляет правильное время.

---

5 Чтобы разрешить переход в изолированный режим при потере соединения с внешними NTP-серверами:

5.1 Выберите **Переходить в изолированный режим.**

5.2 Выберите уровень иерархии внешних NTP-серверов. Если ViPNet Coordinator IG не сможет установить соединение со всеми внешними NTP-серверами меньше указанного уровня в течение 5 минут, то локальный NTP-сервер перейдёт в изолированный режим.

Примечание. Разрешите переход локального NTP-сервера в изолированный режим, если ViPNet Coordinator IG используется в качестве NTP-сервера для внутренней сети. Иначе клиенты ViPNet Coordinator IG не будут получать информацию о точном времени при потере соединения с внешними NTP-серверами, так как в этом случае локальный NTP-сервер будет считаться недостоверным.

---

6 Нажмите **Сохранить**.

7 Включите **NTP-сервер** вверху слева.

Примечание. NTP-серверы, указанные по доменному имени, будут доступны, только если запущен DNS-сервер.

Информация о попытках подключения к NTP-серверам записывается в системный журнал. Если ViPNet Coordinator IG не удалось подключиться ни к одному из NTP-серверов списка, локальный NTP-сервер запускается с текущим временем ViPNet Coordinator IG (см. Настройка даты и времени). Для этого случая вы можете добавить NTP-сервер в локальной сети, с которым ViPNet Coordinator IG сможет синхронизировать время при невозможности подключения к внешним NTP-серверам.

С помощью командного интерпретатора вы можете настроить автоматический запуск NTP-сервера (см. документ «Настройка с помощью командного интерпретатора»).

Внимание! Если время на вышестоящем NTP-сервере будет изменено более чем на 1000 секунд вперёд или назад, это может привести к аварийному завершению работы NTP-сервера ViPNet Coordinator IG. В этом случае повторно запустите NTP-сервер.

Настройка точки доступа к сети Wi-Fi

Примечание.

- Использование ViPNet Coordinator IG в качестве точки доступа Wi-Fi возможно только в исполнениях со встроенным модулем Wi-Fi.
- Беспроводные сети, такие как Wi-Fi и 3G/4G, менее надежны, чем проводные. Воздействие различного рода помех на беспроводные сети может приводить к потерям среди IP-пакетов и снижению скорости передачи данных.
- ViPNet Coordinator IG может работать в одном из режимов: в режиме точки доступа или клиента сети Wi-Fi (см. Подключение к сети Wi-Fi).

Чтобы настроить ViPNet Coordinator IG в качестве точки доступа Wi-Fi:

1. Выберите **Сетевые настройки** > **Сетевые интерфейсы**.
2. Нажмите , чтобы включить режим редактирования.
3. Выберите интерфейс `wlan0`
4. Выключите Wi-Fi.

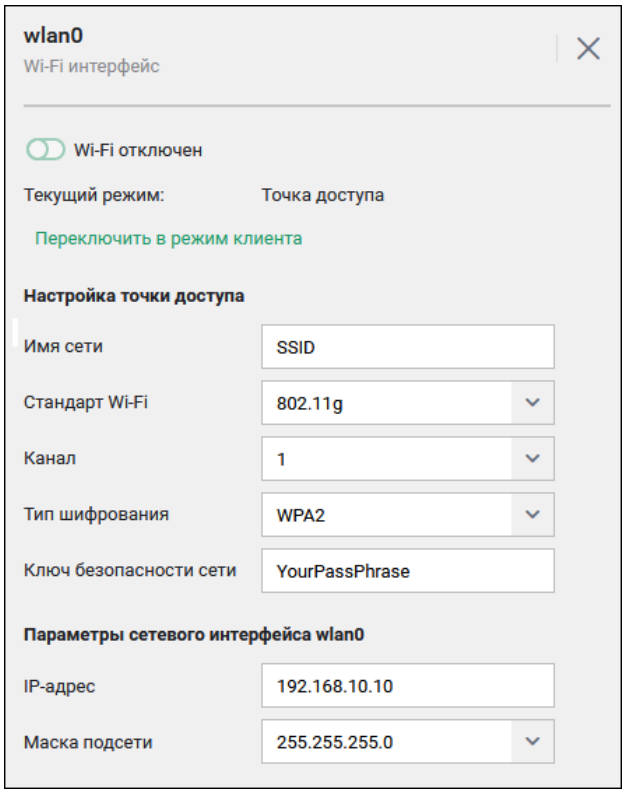


Рисунок 77. Настройка точки доступа сети Wi-Fi

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

6 В разделе **Настройки точки доступа**:

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

6.2 В списке **Стандарт Wi-Fi** выберите стандарт беспроводной связи:

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

6.3 В списке **Канал** выберите номер канала Wi-Fi.

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

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

7 В разделе **Параметры сетевого интерфейса wlan0** задайте статический IP-адрес и маску подсети. IP-адрес на `wlan0` и на любом другом интерфейсе ViPNet Coordinator IG не должны относиться к одной подсети.

8 Нажмите **Сохранить**.

9 Включите  Wi-FI.

10 Нажмите  .

11 Настройте параметры DHCP-сервера для интерфейса wlan0.

12 Для связи с устройствами, которые подключены к сети Wi-Fi, и устройствами, подключёнными к сети Ethernet, создайте транзитные фильтры открытой сети, разрешающие трафик между этими сетями.

Вы можете настроить запись уровня сигнала Wi-Fi в системный журнал (см. документ «Настройка с помощью командного интерпретатора»).

Настройка шлюза Modbus

Примечание. Шлюз Modbus поддерживается во всех исполнениях ViPNet Coordinator IG10 и ViPNet Coordinator IG100. Для использования шлюза Modbus включите эту функцию в настройках координатора в ViPNet Prime. Это можно сделать при наличии лицензии на шлюз Modbus.

Вы можете настроить шлюз Modbus на каждом из последовательных интерфейсов ViPNet Coordinator IG. Для этого:

1 Выберите **АСУ ТП** > **Последовательные интерфейсы**.

2 Нажмите **Добавить шлюз**.

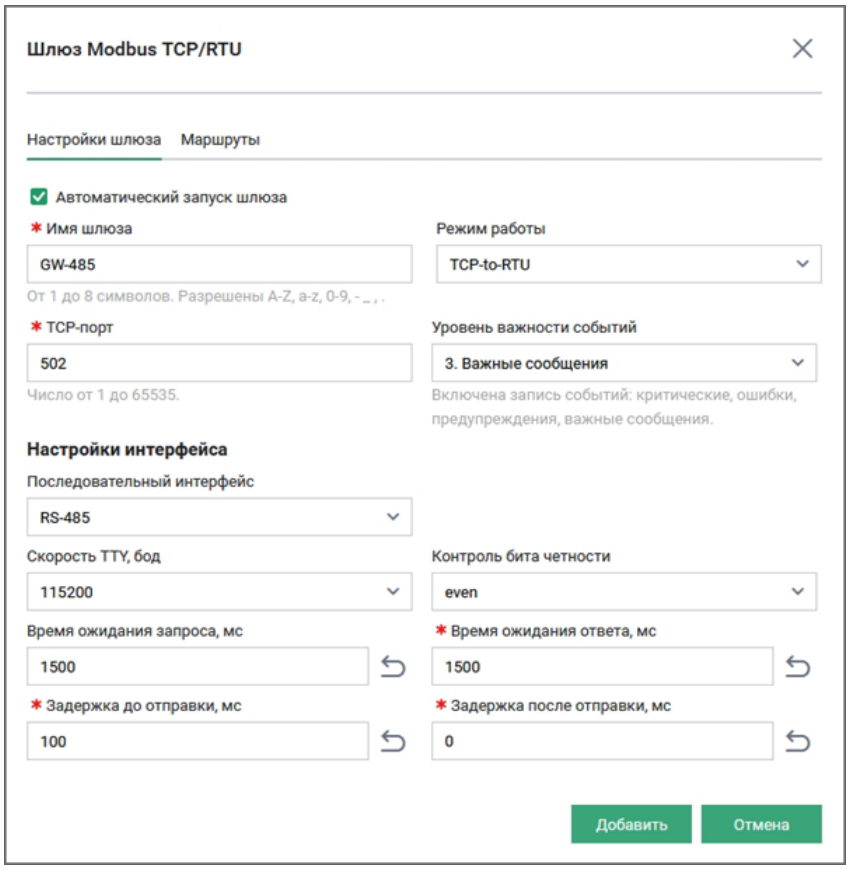


Рисунок 78. Настройка шлюза Modbus

3 Чтобы шлюз Modbus включался автоматически при загрузке ViPNet Coordinator IG, убедитесь, что выбран параметр **Автоматический запуск шлюза**.

4 Задайте произвольное имя шлюза.

5 Выберите режим работы шлюза Modbus **TCP to RTU** или **RTU to TCP** в зависимости от того, в каком направлении необходимо выполнять преобразование протокола Modbus.

6 Укажите TCP-порт.

7 В разделе **Настройки интерфейса**:

7.1 Выберите последовательный интерфейс, на котором будет работать шлюз Modbus.

Список доступных последовательных интерфейсов зависит от вашего исполнения ViPNet Coordinator IG. Если интерфейс уже используется другим шлюзом Modbus, он недоступен для выбора.

7.2 Выберите скорость TTY и контроль бита чётности.

7.3 Задайте время ожидания запроса от ведущего Modbus-устройства и время ожидания ответа от ведомого Modbus-устройства.

8 Если выбран режим работы **RTU to TCP**, настройте маршрутизацию для устройства Modbus, подключённого к ViPNet Coordinator IG по последовательной линии связи. Для этого:

8.1 Выберите вкладку **Маршруты**.

8.2 Нажмите ⊕ **Добавить**.

8.3 Задайте параметры маршрута:

- SlaveID – адрес устройства Modbus, которое необходимо маршрутизировать в сети Ethernet.
- IP-адрес и TCP-порт шлюза Modbus.
- Время ожидания запроса от ведущего Modbus-устройства и время ожидания ответа от ведомого Modbus-устройства.
- Описание маршрута (необязательно).

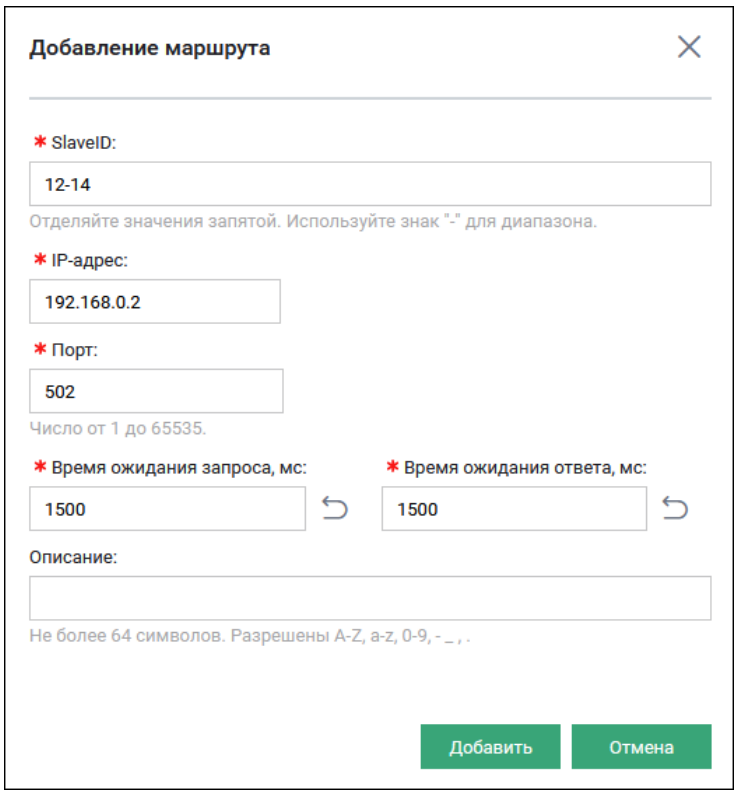


Рисунок 79. Добавление маршрута

8.4 Нажмите **Добавить**.

9 Нажмите **Добавить**.

10 В разделе созданного шлюза Modbus нажмите **Запустить**.

Вы можете запустить или остановить все настроенные шлюзы Modbus с помощью кнопок **Запустить все** и **Остановить все** на панели инструментов.

Примечание. Шлюз Modbus доступен по IP-адресам всех сетевых интерфейсов ViPNet Coordinator IG и заданному TCP-порту. Чтобы разрешить или ограничить доступ к шлюзу Modbus, настройте сетевые фильтры.

Устранение неполадок

Ошибки и другие события в работе шлюзов Modbus записываются в системный журнал. По умолчанию в журнал записываются: критические события, ошибки, предупреждения и важные события. Если этой информации недостаточно для определения причин неполадок в работе шлюза Modbus, измените уровень важности событий, записываемых в системный журнал.

Чтобы изменить уровень важности событий для одного шлюза Modbus:

1 В разделе шлюза Modbus нажмите **Остановить**.

2 Нажмите **Настроить**.

3 Выберите уровень важности событий.

4 Нажмите **Сохранить**.

5 Нажмите **Запустить**.

Чтобы изменить уровень важности событий для всех шлюзов Modbus:

1 На панели инструментов нажмите **Остановить все**.

2 Вверху справа нажмите **Настройка журнала**.

3 Выберите уровень важности событий.

4 Нажмите **Сохранить**.

5 Нажмите **Запустить все**.

Внимание! В случае возникновения нештатных условий эксплуатации, которые повлекли за собой перезагрузку ViPNet Coordinator IG или подключённых к нему устройств или узлов, проверьте работоспособность Modbus-соединений с этими устройствами и узлами. Если связь не восстановилась, остановите все шлюзы Modbus и запустите их заново.

Настройка интерфейса GPIO

На корпусе ViPNet Coordinator IG расположен интерфейс GPIO, который вы можете использовать для решения следующих задач безопасности АСУ ТП:

- Подключение датчика вскрытия внешнего шкафа;
- Подключение внешней кнопки для перевода ViPNet Coordinator IG в специальный режим функционирования;
- Сигнализация о событиях, отслеживаемых ViPNet Coordinator IG;
- Отправка сигналов о режиме работы ViPNet Coordinator IG в кластере.

Подробнее о настройке интерфейса GPIO для решения этих задач см. документ «Сценарии работы», раздел «Использование интерфейса GPIO».

В состав ViPNet Coordinator IG входит служба управления интерфейсом GPIO — `piomonitor`, с помощью которой обрабатываются сигналы интерфейса GPIO. Чтобы выполнить настройку интерфейса GPIO:

1 Выберите **АСУ ТП** > **GPIO**.

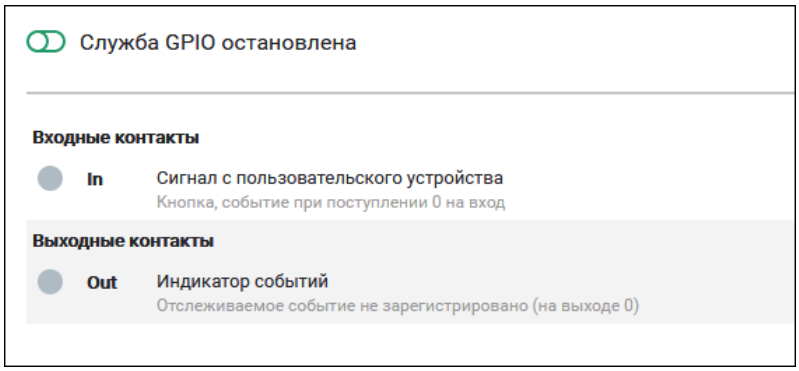


Рисунок 80. Настройка интерфейса GPIO

2 Если служба GPIO запущена, остановите ее .

3 Настройте обработку сигналов для входного контакта GPIO:

3.1 В строке контакта **In** нажмите .

3.2 В зависимости от решаемой задачи безопасности АСУ ТП выберите назначение входного контакта:

- **Сигнал с пользовательского устройства** — чтобы настроить пользовательскую обработку входящего сигнала от внешнего устройства, подключенного к интерфейсу GPIO ViPNet Coordinator IG.
- **Датчик вскрытия внешнего шкафа** — чтобы настроить обработку сигнала от датчика вскрытия внешнего шкафа, подключенного к интерфейсу GPIO ViPNet Coordinator IG.

- **Сигнал переключения режима работы ПАК** — чтобы настроить обработку сигнала от внешнего устройства для перевода ViPNet Coordinator IG в специальный режим функционирования, если ViPNet Coordinator IG работает как межсетевой экран типа «Д».

3.3 Если вы выбрали назначение контакта **Сигнал с пользовательского устройства**, настройте логику его работы, выбрав один из следующих вариантов:

- **Кнопка, событие по сигналу 1** — если вы используете внешнее устройство типа «кнопка» с активным уровнем сигнала 1.
- **Кнопка, событие по сигналу 0** — если вы используете внешнее устройство типа «кнопка» с активным уровнем сигнала 0.
- **Переключатель, событие по сигналу 1, отмена по 0** — если вы используете внешнее устройство типа «переключатель», активное положение которого — 1.
- **Переключатель, событие по сигналу 0, отмена по 1** — если вы используете внешнее устройство типа «переключатель», активное положение которого — 0.

3.4 Если вы выбрали назначение контакта **Датчик вскрытия внешнего шкафа**, настройте логику его работы, выбрав один из следующих вариантов:

- **Сигнал 1 на входе если шкаф вскрыт** — если активный уровень сигнала от датчика вскрытия шкафа — 1.
- **Сигнал 0 на входе если шкаф вскрыт** — если активный уровень сигнала от датчика вскрытия шкафа — 0.

3.5 Если вы выбрали назначение контакта **Сигнал переключения режима работы ПАК**, настройте логику его работы, выбрав один из следующих вариантов:

- **Кнопка, перевод в специальный режим по сигналу 1** — если вы используете внешнее устройство типа «кнопка» с активным уровнем сигнала 1. При использовании кнопки перевод ViPNet Coordinator IG обратно в штатный режим будет возможен только с помощью командного интерпретатора или веб-интерфейса.
- **Кнопка, перевод в специальный режим по сигналу 0** — если вы используете внешнее устройство типа «кнопка» с активным уровнем сигнала 0.
- **Переключатель, 1 на входе - специальный, 0 - штатный режим** — если вы используете внешнее устройство типа «переключатель», активное положение которого — 1. С помощью переключателя вы также сможете выполнять обратный перевод ViPNet Coordinator IG в штатный режим.
- **Переключатель, 0 на входе - специальный, 1 - штатный режим** — если вы используете внешнее устройство типа «переключатель», активное положение которого — 0.

4 Настройте обработку сигналов для выходного контакта GPIO:

4.1 В строке контакта **Out** нажмите  .

4.2 В зависимости от решаемой задачи безопасности АСУ ТП, выберите назначение выходного контакта:

- **Контроль работы кластера** — чтобы настроить отправку на выходной контакт GPIO сигнала, соответствующего текущему режиму работы ViPNet Coordinator IG в кластере. Подробнее см. в документе «Сценарии работы», раздел «Кластер с использованием шлюза Modbus и интерфейса GPIO».
- **Индикатор событий** — чтобы настроить отправку на выходной контакт GPIO сигнала, соответствующего одному из событий, отслеживаемых ViPNet Coordinator IG.

4.3 Если вы выбрали назначение контакта **Контроль работы кластера**, настройте логику его работы, выбрав один из следующих вариантов:

- **Сигнал 1 на выходе если данный узел кластера активный** — чтобы при переходе ViPNet Coordinator IG в режим активного узла кластера на выходной контакт GPIO был подан сигнал уровня 1.
- **Сигнал 0 на выходе если данный узел кластера активный** — чтобы при переходе ViPNet Coordinator IG в режим активного узла кластера на выходной контакт GPIO был подан сигнал уровня 0.

4.4 Если вы выбрали назначение контакта **Индикатор событий**, настройте логику его работы, выбрав один из следующих вариантов:

- **Сигнал 1 на выходе если произошло событие** — чтобы при регистрации отслеживаемого события на выходной контакт GPIO был подан сигнал уровня 1.
- **Сигнал 0 на выходе если произошло событие** — чтобы при регистрации отслеживаемого события на выходной контакт GPIO был подан сигнал уровня 0.

Затем выберите отслеживаемые события, при которых на выходной контакт GPIO будет отправлен сигнал.

5 По завершении настройки запустите  службу GPIO.

8

Настройка маршрутизации

Общие сведения о маршрутизации 137

Принципы маршрутизации 138

Просмотр таблицы маршрутизации 142

Настройка статической маршрутизации 143

Настройка маршрутов протоколов DHCP и PPP 147

Настройка OSPF 152

Настройка BGP 160

Настройка функции MultiWAN 168

Общие сведения о маршрутизации

ViPNet Coordinator IG поддерживает маршрутизацию 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, имеющихся в таблице маршрутизации ViPNet Coordinator IG.

Маршруты могут быть:

- статические — добавляются в таблицу маршрутизации вручную;
- динамические — добавляются в таблицу маршрутизации с помощью алгоритмов на основе информации о топологии и состоянии сети, предоставляемой протоколами динамической маршрутизации.

Динамическая маршрутизация позволяет:

- автоматически формировать таблицу маршрутизации;
- автоматически выбирать по определенным критериям лучший маршрут из нескольких доступных, в том числе, при сбое других маршрутизаторов в сети;
- распределять нагрузку IP-трафика, передаваемого в сети.

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

- статических, в том числе на основе маршрутов с несколькими шлюзами;
- получаемых по протоколам DHCP и PPP;
- динамических, формируемых протоколами OSPF, BGP (поддерживается только ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1).

Принципы маршрутизации

В ViPNet Coordinator IG 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 и BGP.
- Пользовательские таблицы маршрутизации — содержат только статические маршруты, заданные вручную, и используются для создания политик маршрутизации (см. Настройка функции MultiWAN).

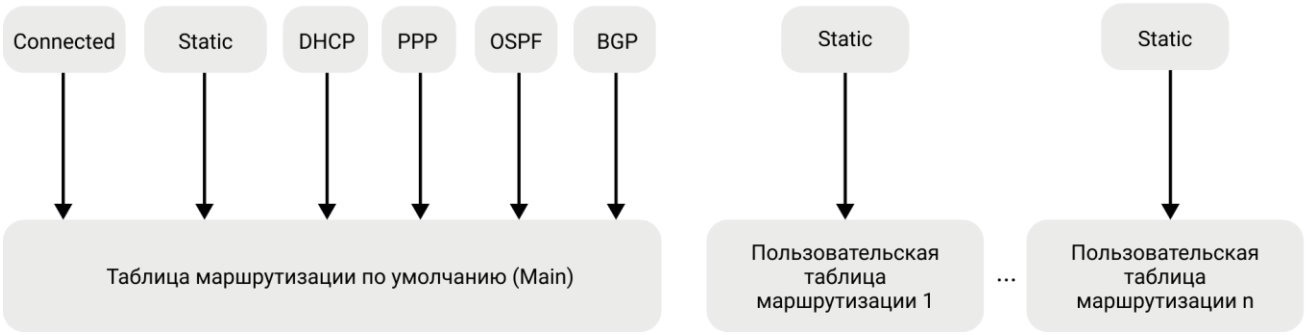


Рисунок 81. Формирование таблиц маршрутизации

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, BGP — 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.
  - Административная дистанция маршрутов протокола PPP отдельно не задаётся и равна дистанции маршрутов протокола DHCP.
  - Административная дистанция маршрутов протоколов OSPF и BGP задаётся не для конкретного маршрута, а для всех маршрутов протокола.
  - Административная дистанция статических маршрутов не может совпадать с дистанцией, заданной для маршрутов протоколов OSPF и BGP.

Примечание. Для каждого типа маршрутов задана административная дистанция по умолчанию:

- для статических маршрутов — 10;
- для маршрутов протоколов DHCP и PPP — 70;
- для маршрутов протокола OSPF — 110;
- для маршрутов протокола iBGP — 200;
- для маршрутов протокола eBGP — 20.

Для первых двух типов маршрутов вы можете изменять значение административной дистанции.

- Метрика — определяет приоритет маршрутов протоколов DHCP, PPP и OSPF. Чем меньше метрика, тем выше приоритет маршрута.
  - Для маршрутов протокола DHCP метрики указываются вручную, причём 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 маршруты в одну и ту же сеть, то будет выбран маршрут с наименьшей метрикой.
  - Для маршрутов протокола PPP метрика также может быть задана вручную в том случае, если ViPNet Coordinator IG подключён к нескольким сетям, одной из которых является сеть 3G/4G, а в другой установлен DHCP-сервер. Если метрики для маршрутов протоколов DHCP и PPP не были заданы, используется метрика по умолчанию.
  - Для маршрутов протокола OSPF метрика (стоимость) вычисляется автоматически.
- Вес — определяет долю IP-трафика, который будет проходить по маршруту через указанный шлюз. Используется в статических маршрутах и multipath-маршрутах протокола BGP. Вес задаётся для шлюза. Позволяет настроить балансировку передаваемого IP-трафика между несколькими шлюзами, когда часть IP-пакетов направляется на один шлюз, а часть — на другой.

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 IG. 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).

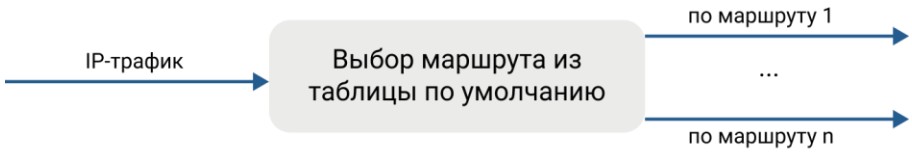


Рисунок 82. Маршрутизация при политике по умолчанию

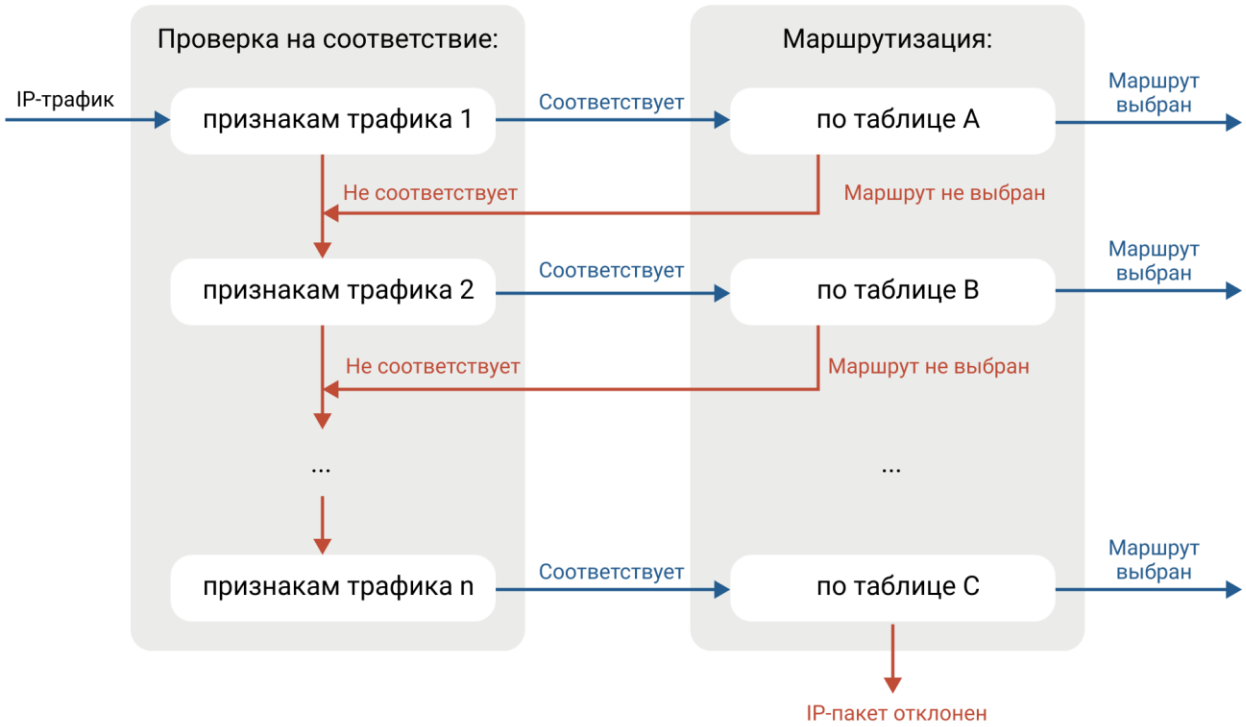


Рисунок 83. Маршрутизация при пользовательской политике

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, PPP, OSPF, BGP). 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 применяются правила:

- Из нескольких лучших маршрутов DHCP в одну сеть будет выбран маршрут с наименьшей метрикой. Если метрики равны, маршруты будут выбраны в соответствии со стратегией 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 в одну и ту же сеть объединяются в один маршрут с несколькими шлюзами (multi-hop route):
  - Статические маршруты — по признаку одинаковых административных дистанций маршрутов.
  - Маршруты DHCP и PPP — по признаку одинаковых метрик маршрутов.
  - Маршруты OSPF и BGP — маршрутизаторами OSPF и BGP.

  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.**

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

Для просмотра списка маршрутов от конкретного источника:

- выберите вкладку **Статическая**, **DHCP** или **OSPF**;
- выберите **Маршрутизация** > **BGP-маршрутизация** > **Мониторинг** > **BGP-таблица**.

Настройка статической маршрутизации

Если ViPNet Coordinator IG 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 IG 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.

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 .

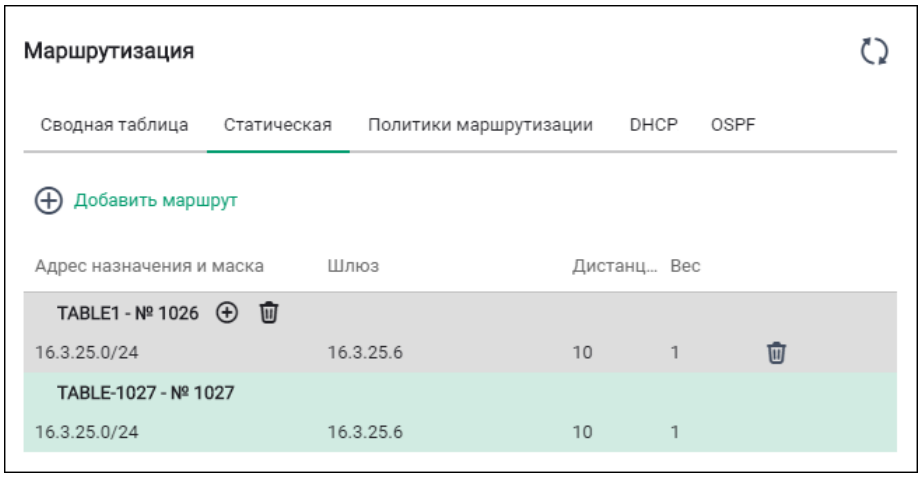


Рисунок 84. Список статических маршрутов

3 Задайте параметры маршрута:

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

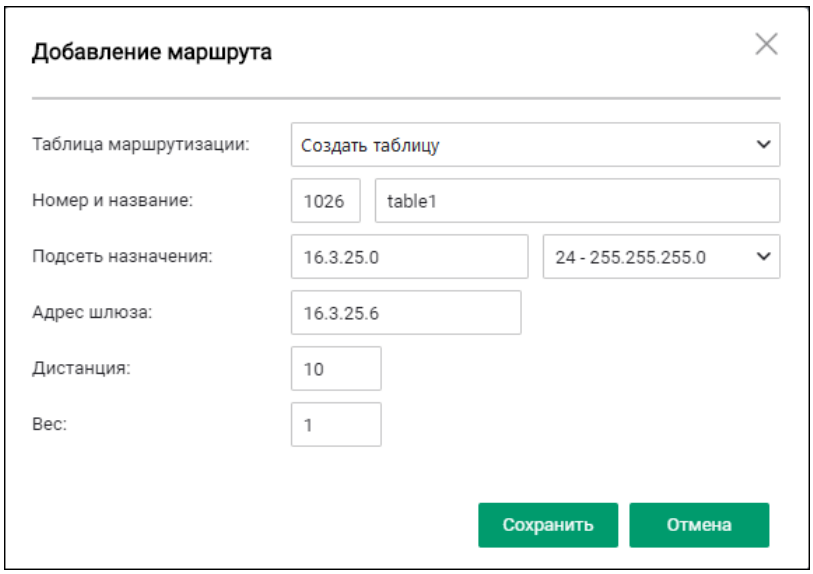


Рисунок 85. Добавление статического маршрута

- 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:

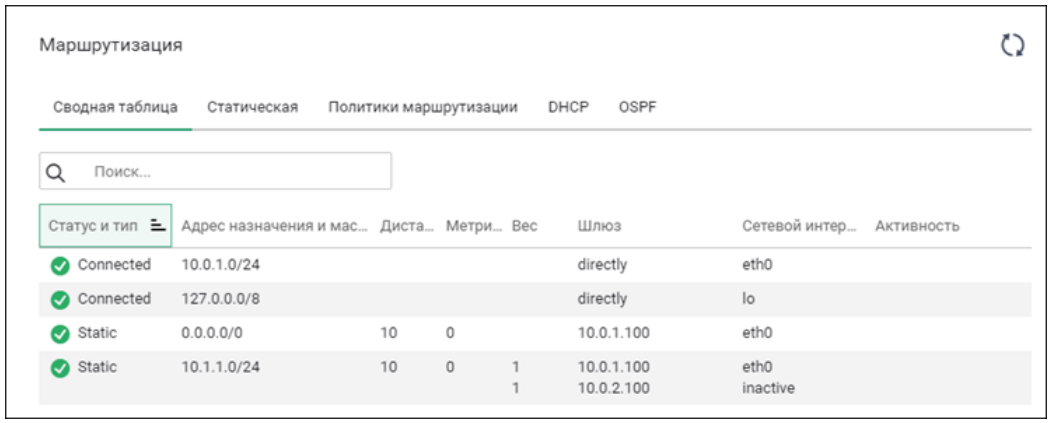


Рисунок 86. Распределение нагрузки между статическими маршрутами в одну сеть

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 маршрутов протоколов DHCP и PPP

Если на каком-либо сетевом интерфейсе ViPNet Coordinator IG включен режим DHCP и настроено автоматическое получение маршрутов (см. Настройка сетевых интерфейсов Ethernet), 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 IG подключен к сети 3G/4G и получает информацию для маршрута по умолчанию от PPP-сервера провайдера (см. Подключение к мобильной сети 3G/4G), 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 IG настроено взаимодействие с DHCP-сервером, от которого поступают маршруты, а также настроена статическая маршрутизация (см. Настройка статической маршрутизации) или динамическая маршрутизация (см. Настройка OSPF), 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.

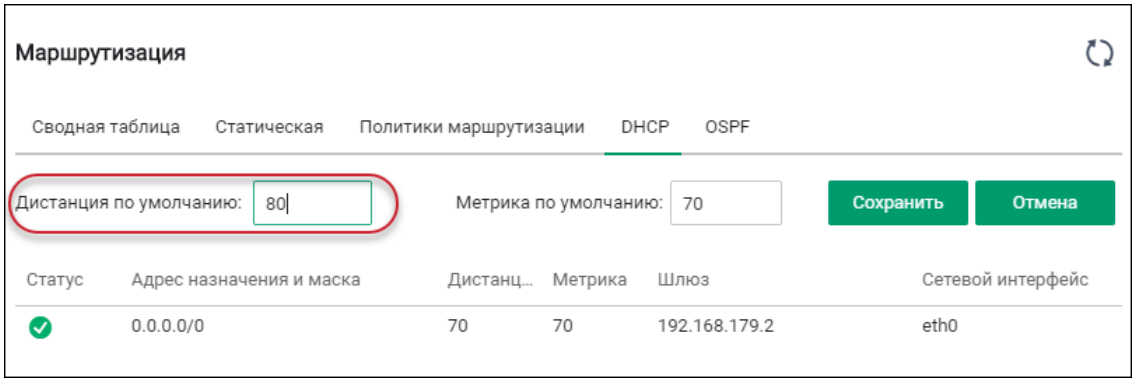


Рисунок 87. Задание административной дистанции маршрутам DHCP-сервера

Настройка метрики для маршрутов DHCP-сервера

Если на ViPNet Coordinator IG 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 IG 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 (см. Настройка сетевых интерфейсов Ethernet).
- VLAN (см. Организация обработки трафика из нескольких VLAN).
- Wi-Fi (wlan) (см. Подключение к сети Wi-Fi).
- 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 настройки** и нажмите .

2 Выберите сетевой интерфейс.

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**.

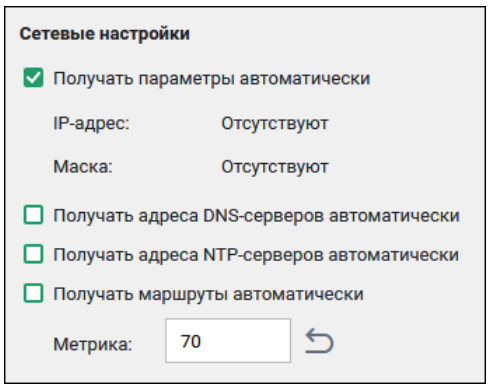


Рисунок 88. Настройка режима получения параметров интерфейса от DHCP-сервера

5 Нажмите .

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

Настройка метрики для маршрутов PPP-протокола

Одновременно с подключением к мобильной сети ViPNet Coordinator IG может быть подключен к другим сетям, в которых маршруты распространяются по DHCP-протоколу. В этом случае ViPNet Coordinator IG также будет получать маршруты по умолчанию в эти сети. Чтобы маршрут по умолчанию PPP-протокола имел приоритет выше, чем маршруты по умолчанию DHCP-протокола, задайте метрику для PPP-протокола (далее — специфичную метрику). Причем она должна быть меньше любой метрики маршрутов по умолчанию, полученных по DHCP-протоколу. 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.

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

1 Выберите **Сетевые настройки** и нажмите .

2 Выберите интерфейс модема.

3 Если интерфейс включен, выключите его.

4 Убедитесь, что в разделе **Получаемые настройки** установлен флажок **Маршруты**.

5 Введите значение в поле **Метрика**.

6 Нажмите **Сохранить**.

7 Включите интерфейс.

8 Нажмите .

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

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

Если для маршрутов 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.

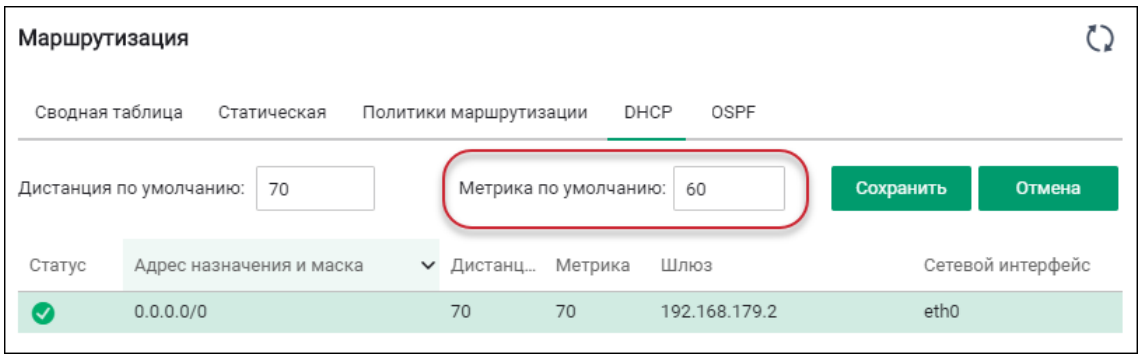


Рисунок 89. Задание метрики по умолчанию

Настройка OSPF

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

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

В процессе настройки маршрутизации по протоколу OSPF вам потребуется:

- включить использование протокола OSPF;
- указать сети, к которым подключён ViPNet Coordinator IG и которые будут участвовать в маршрутизации по протоколу OSPF, и области маршрутизации;
- создать ряд сетевых фильтров.

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

При необходимости вы также можете настроить Настройка перераспределения маршрутов.

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 IG 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 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.

3.1.2 Способ аутентификации:

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

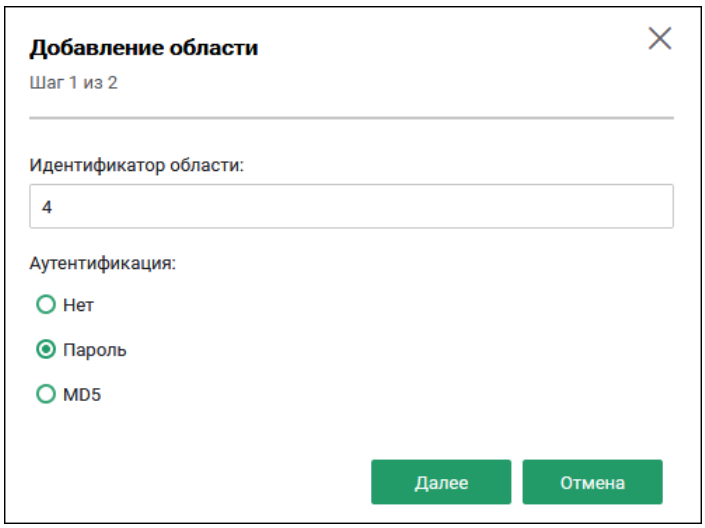


Рисунок 90. Добавление области

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.

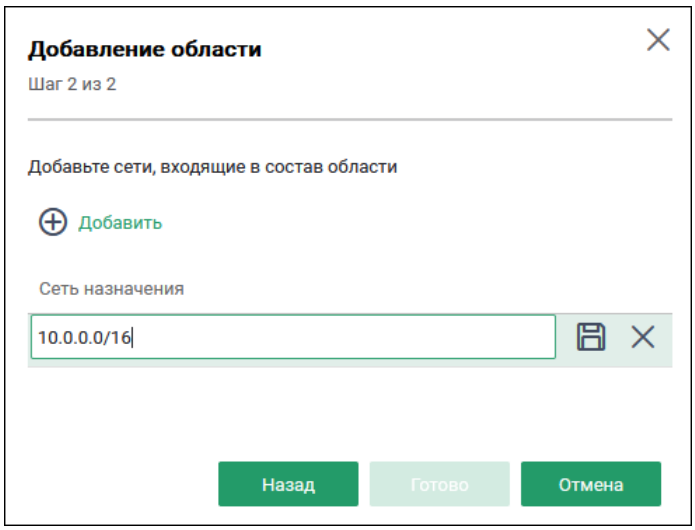


Рисунок 91. Добавление подсети

3.4 Нажмите **Готово.**

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

4.1 В строке интерфейса нажмите .

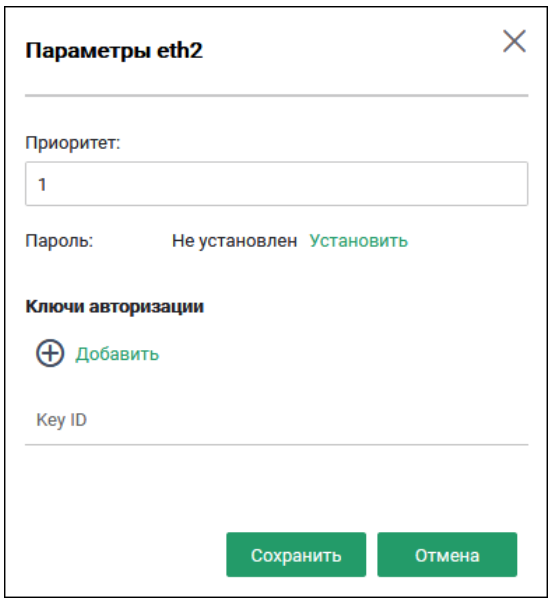


Рисунок 92. Настройка параметров интерфейса

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.**

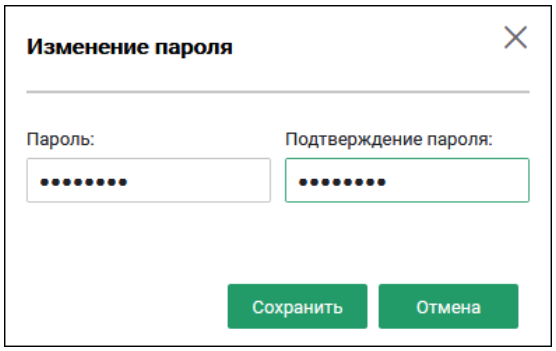


Рисунок 93. Установка пароля

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**.

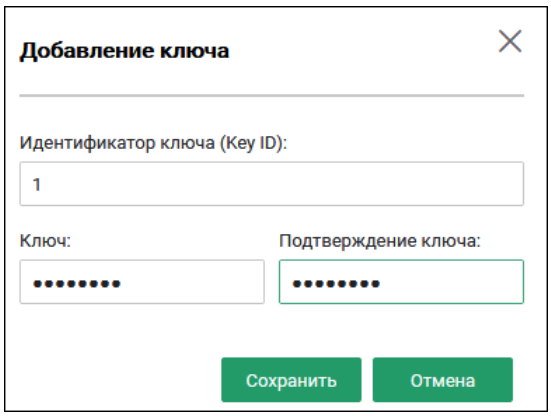


Рисунок 94. Добавление ключа

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 IG:

Таблица 5. 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 IG.

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

Таблица 6. 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 7. 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.
- IG-1 расположен на границе автономных областей и является граничным маршрутизатором.
- На IG-1 настроены статические маршруты в сеть партнера.

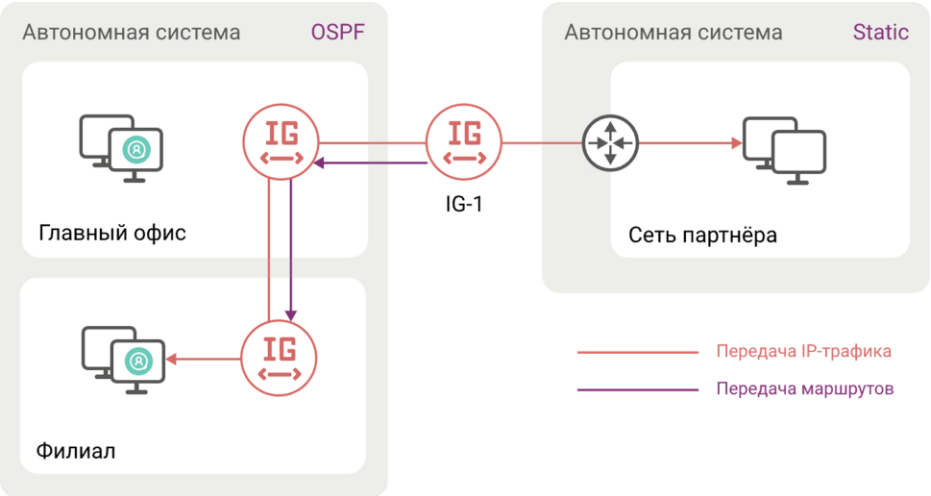


Рисунок 95. Перераспределение маршрутов

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 IG-1:

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

2 Включите службу OSPF.

3 Перейдите в **Настройки службы**.

4 Выберите **Статические** в разделе **Типы распространяемых маршрутов**.

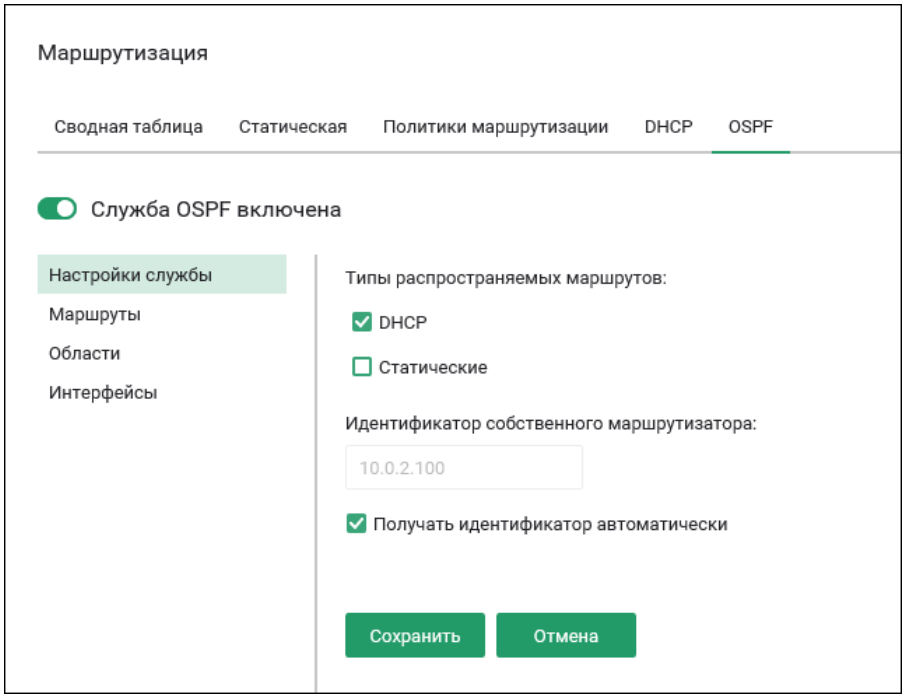


Рисунок 96. Включение перераспределения маршрутов DHCP-сервера

5 Нажмите **Сохранить**.

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

Примечание. Если в сети партнера используются динамические маршруты от DHCP-сервера, выберите **DHCP** в группе **Типы распространяемых маршрутов**.

Также на граничном маршрутизаторе должно быть настроено получение маршрутов от DHCP-сервера сети партнера.

Настройка BGP

Примечание.

- Протокол BGP поддерживается только в исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1.
- BGP-маршруты не синхронизируются между узлами кластера.

Общие сведения о протоколе BGP

BGP (Border Gateway Protocol) — протокол динамической маршрутизации, предназначенный для обмена маршрутами между автономными системами (AS). AS — это совокупность IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с интернетом.

Маршрутизатор ViPNet Coordinator IG поддерживает протокол BGP для обмена маршрутами с соседними маршрутизаторами, а также для передачи параметров, позволяющих выбрать лучшие маршруты.

Таблица 8. Порядок выбора лучшего маршрута

№	Параметр маршрута	Критерий выбора	Анонсирование
1	Вес (`weight`)	Выбирается маршрут с наибольшим весом	Нет
2	Значение `local preference`	Выбирается маршрут с наибольшим значением	Только внутри AS
3	Локальный или внешний	Локальные маршруты имеют приоритет	Нет
4	Длина (`AS-path`)	Выбирается маршрут наименьшей длины	Да
5	Происхождение (`Origin`)	Маршруты, полученные через IGP имеют приоритет	Да
6	Значение `MED`	Выбирается маршрут с наименьшим `MED`	Только внутри AS и в соседнюю AS
7	eBGP или iBGP	Маршруты eBGP имеют приоритет	Нет
8	Значение `Router ID`	Выбирается маршрут с наименьшим `Router ID`	Нет
9	Адрес соседа	Выбирается маршрут с наименьшим адресом	Нет

Настройка маршрутизатора

Включите BGP-маршрутизацию и настройте маршрутизатор:

1 Выберите **Маршрутизация** > **BGP-маршрутизация**.

2 Включите **BGP-маршрутизация**.

3 Выберите **Маршрутизатор** > **Основные настройки**.

4 Задайте номер собственной AS (целое число из диапазона 1–4294967295).

5 По умолчанию задан автоматический выбор идентификатора маршрутизатора. Чтобы назначить его вручную:

5.1 Снимите флажок **Получать автоматически**.

5.2 Укажите идентификатор в формате A.B.C.D (может принимать значение от 0.0.0.1 до 255.255.255.255).

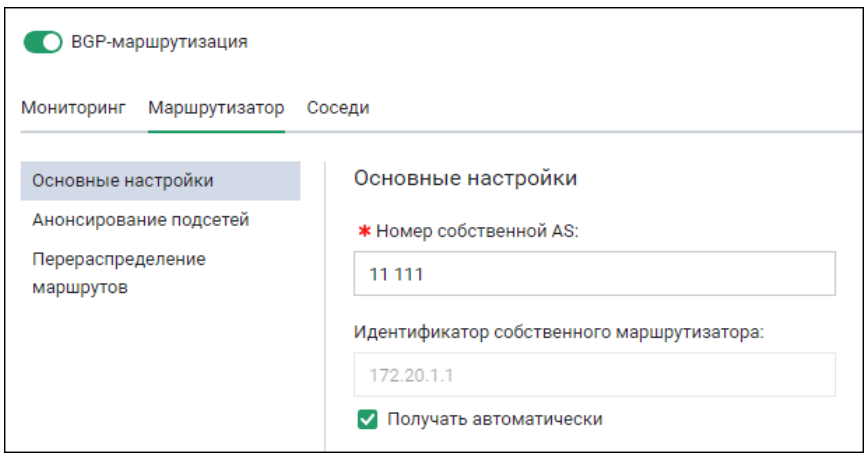


Рисунок 97. Основные настройки маршрутизатора

6 Нажмите **Сохранить**.

Настройка соседей

Добавление соседа

Внимание! Текущая версия ViPNet Coordinator IG не поддерживает автоматическое создание разрешающих сетевых фильтров BGP-сессий при добавлении соседа. Создайте их вручную, в зависимости от типа узла соседа (открытый или защищённый). После удаления соседа также удалите эти фильтры.

Таблица 9. Разрешающие сетевые фильтры BGP-сессий

Имя фильтра	Источник	Назначение	Транспортный протокол	Расписание
BGP neighbor <IP-адрес соседа> out	Мой узел (@local)	<IP-адрес соседа>/(Имя узла сети ViPNet)	to TCP: <номер порта в настройке соседа; по умолчанию 179>	Всегда
BGP neighbor <IP-адрес соседа> in	<IP-адрес соседа>/(Имя узла сети ViPNet)	Мой узел (@local)	to TCP: 179	Всегда

1 Выберите **Маршрутизация** > **BGP-маршрутизация** > **Соседи**.

2 Нажмите **Добавить соседа**.

2.1 Укажите:

2.1.1 Номер AS соседа (целое число из диапазона 1–4294967295).

2.1.2 IP-адрес соседа.

2.1.3 TCP-порт доступа к соседу (по умолчанию — 179).

2.2 Чтобы при установке BGP-сессии с соседом использовать MD5-аутентификацию, выберите одноимённый флажок и задайте пароль.

2.3 Чтобы настроить TTL:

2.3.1 Выберите **Настроить TTL**.

2.3.2 Задайте TTL одним из способов:

- Выберите **TTL Security** и укажите максимальное количество «переходов» до соседа.
- Выберите **eBGP-multihop** и укажите точное значение TTL.

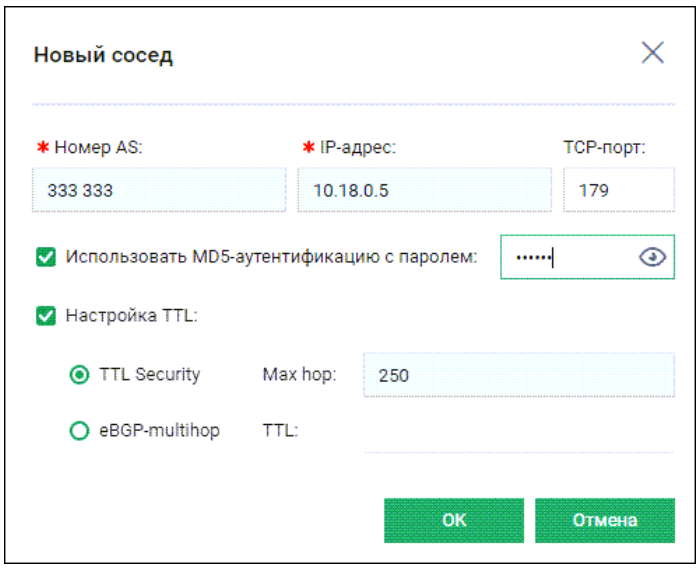


Рисунок 98. Добавление соседа

2.4 Нажмите **OK**.

Просмотр списка соседей

1 Выберите **Маршрутизация** > **BGP-маршрутизация** > **Соседи**.

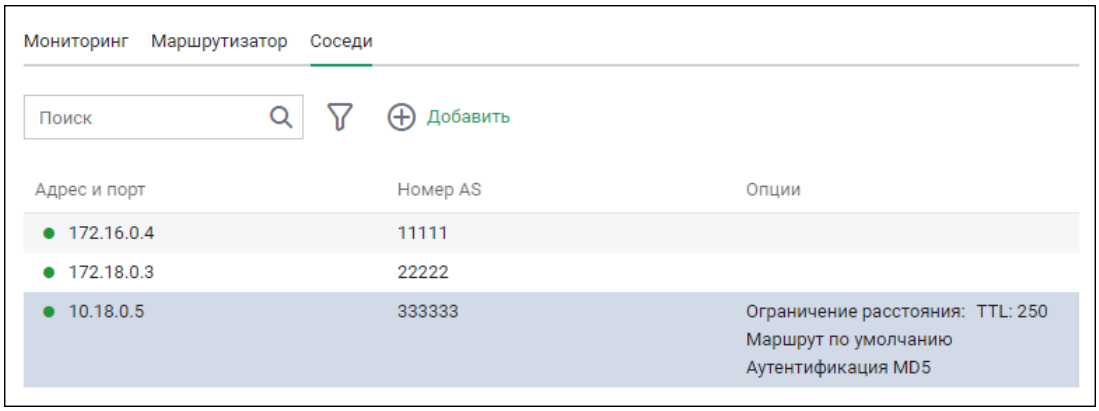


Рисунок 99. Список соседей

2 Чтобы просмотреть список соседей, сформированный по признакам фильтрации, нажмите и выберите флажками признаки.

Просмотр и изменение настроек соседа

1 В списке соседей щёлкните строку с нужным соседом.

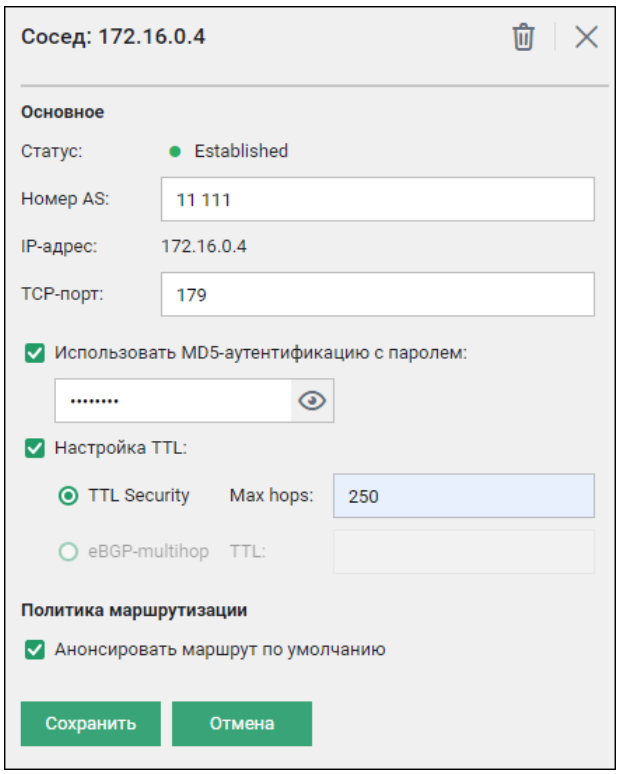


Рисунок 100. Изменение настроек соседа

2 При необходимости:

2.1 Измените настройки соседа, в том числе анонсирование маршрута по умолчанию.

2.2 Нажмите **Сохранить**.

Настройка анонсирования подсетей

По умолчанию маршрутизатор не распространяет информацию об известных ему подсетях и маршрутах. При этом он может получает эту информацию от соседей и пересылать её дальше, не передавая информацию о собственных подсетях. Для её передачи используются анонсирование из заданного списка подсетей и перераспределение подключённых и статических маршрутов, полученных от соседей.

Анонсирование подсетей

Чтобы добавить анонсируемую подсеть:

1 Выберите **Маршрутизация** > **BGP-маршрутизация** > **Маршрутизатор** > **Анонсирование подсетей**.

2 Нажмите **Добавить подсеть**.

2.1 Задайте IP-адрес и выберите из списка маску подсети.

2.2 Нажмите **Сохранить**.

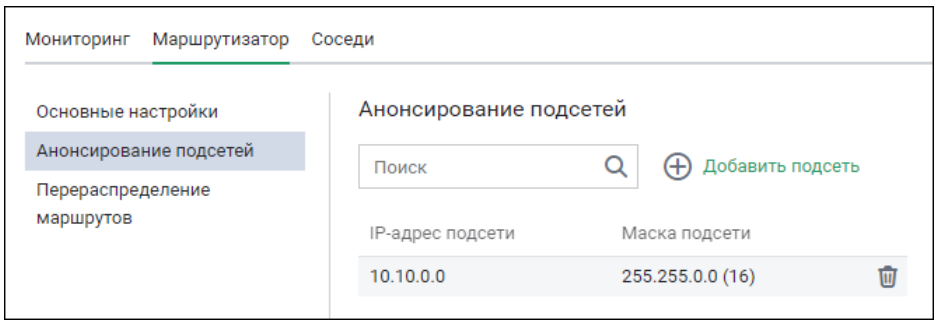


Рисунок 101. Добавление анонсируемой подсети

Перераспределение маршрутов

Внимание! Текущая версия ViPNet Coordinator IG не поддерживает создание карт маршрутов в веб-интерфейсе. Но вы можете настроить их в командном интерпретаторе и использовать для фильтрации перераспределяемых маршрутов. Подробнее см. «Настройка с помощью командного интерпретатора», раздел «Настройка карт маршрутов».

Чтобы настроить перераспределение маршрутов:

1 Выберите **Маршрутизация** > **BGP-маршрутизация** > **Маршрутизатор** > **Перераспределение маршрутов**.

2 Выберите флажками типы перераспределяемых маршрутов:

- **Подключенные маршруты**.
- **Статические маршруты**.

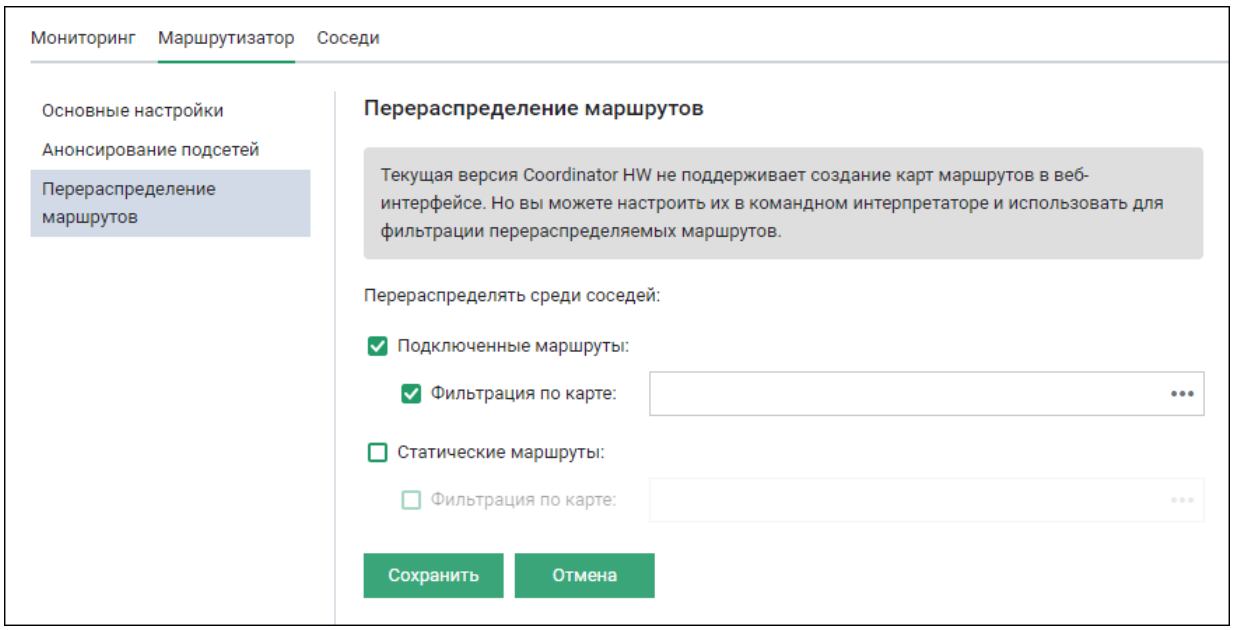


Рисунок 102. Выбор типа перераспределяемых маршрутов и фильтрации по картам маршрутов

3 Для каждого типа маршрутов вы можете настроить фильтрацию по карте маршрутов:

3.1 Выберите флажок **Фильтрация по карте**.

3.2 Нажмите •••.

3.3 Выберите карту маршрутов в списке.

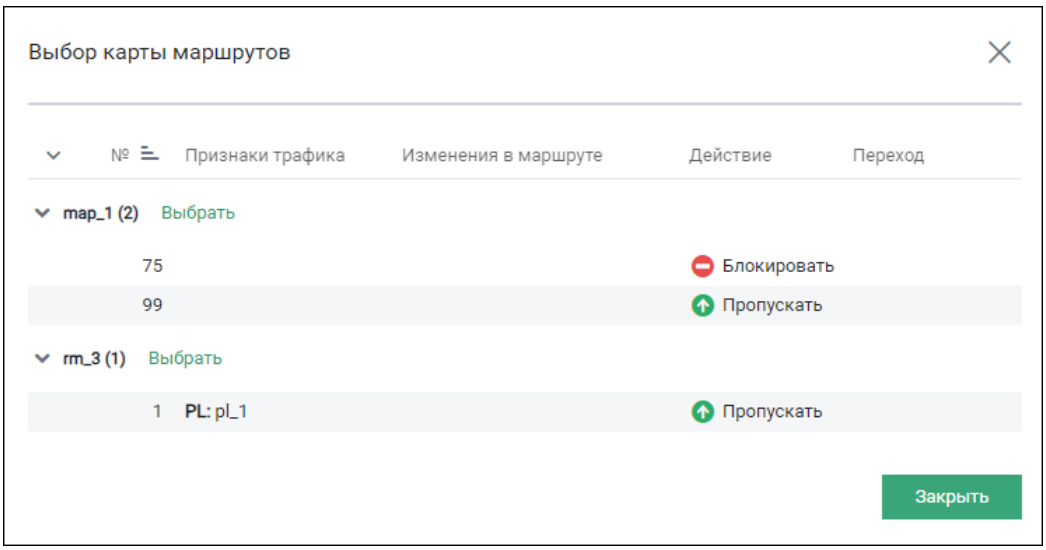


Рисунок 103. Выбор карты маршрутов

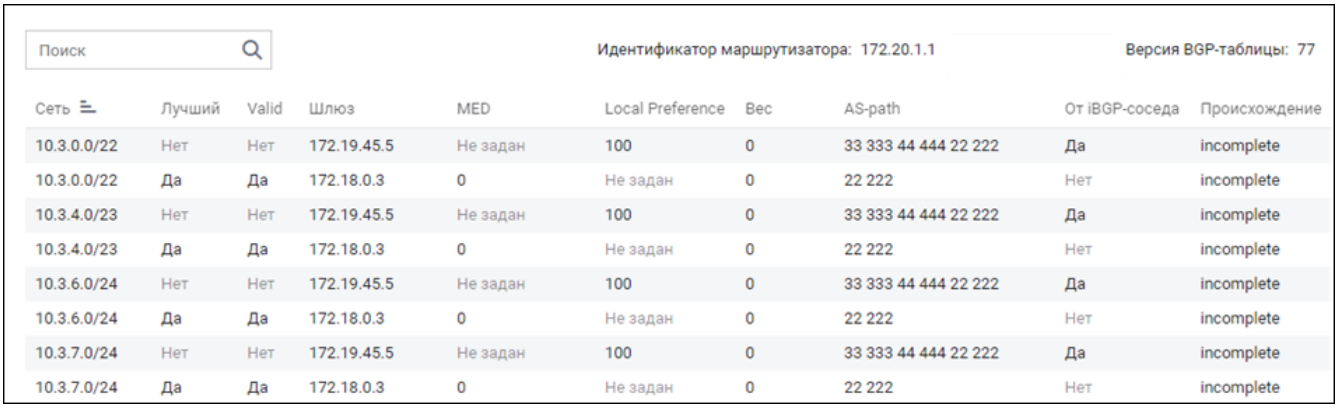
3.4 Нажмите **Выбрать**.

4 Нажмите **Сохранить**.

Мониторинг состояния маршрутизатора

Просмотр BGP-таблицы маршрутизатора

Выберите **Маршрутизация** > **BGP-маршрутизация** > **Мониторинг** > **BGP-таблица**.



Сеть	Лучший	Valid	Шлюз	MED	Local Preference	Вес	AS-path	От iBGP-соседа	Происхождение
10.3.0.0/22	Нет	Нет	172.19.45.5	Не задан	100	0	33 333 44 444 22 222	Да	incomplete
10.3.0.0/22	Да	Да	172.18.0.3	0	Не задан	0	22 222	Нет	incomplete
10.3.4.0/23	Нет	Нет	172.19.45.5	Не задан	100	0	33 333 44 444 22 222	Да	incomplete
10.3.4.0/23	Да	Да	172.18.0.3	0	Не задан	0	22 222	Нет	incomplete
10.3.6.0/24	Нет	Нет	172.19.45.5	Не задан	100	0	33 333 44 444 22 222	Да	incomplete
10.3.6.0/24	Да	Да	172.18.0.3	0	Не задан	0	22 222	Нет	incomplete
10.3.7.0/24	Нет	Нет	172.19.45.5	Не задан	100	0	33 333 44 444 22 222	Да	incomplete
10.3.7.0/24	Да	Да	172.18.0.3	0	Не задан	0	22 222	Нет	incomplete

Рисунок 104. BGP-таблица

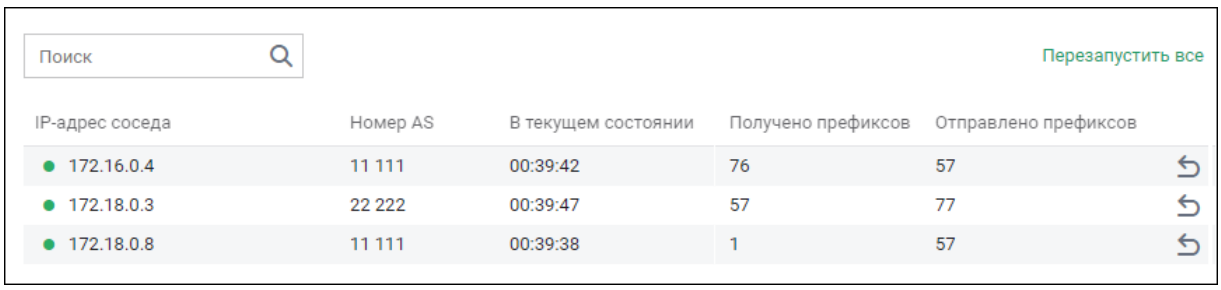
В списке по каждому маршруту отображаются:

- адрес назначения;
- признак лучшего маршрута;
- признак валидности маршрута;
- шлюз;
- дополнительные параметры маршрута: **MED**, **Local Preferencs**, **Вес маршрута**, **AS-path**, **Получен от iBGP-соседа**, **Происхождение**.

BGP-таблица обновляется автоматически каждые 10 секунд.

Просмотр BGP-сессий

1 Выберите **Маршрутизация** > **BGP-маршрутизация** > **Мониторинг** > **BGP-сессии**.



IP-адрес соседа	Номер AS	В текущем состоянии	Получено префиксов	Отправлено префиксов
172.16.0.4	11 111	00:39:42	76	57
172.18.0.3	22 222	00:39:47	57	77
172.18.0.8	11 111	00:39:38	1	57

Рисунок 105. Список BGP-сессий с соседями

В списке по каждой сессии отображаются:

- состояние сессии:

- — Idle;
- — Connect, Active, Open Sent, Open Confirm;
- — Established;

- IP-адрес соседа;
- номер AS соседа;
- время нахождения сессии в текущем состоянии;
- количество полученных и отправленный префиксов.

Состояние сессий обновляется автоматически каждые 10 секунд.

2 Чтобы перезапустить определённую сессию, нажмите и подтвердите перезапуск.

3 Чтобы перезапустить все сессии, нажмите **Перезапустить все** и подтвердите перезапуск.

Настройка функции MultiWAN

Если для доступа ViPNet Coordinator IG 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.

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

Ограничения при настройке MultiWAN

- Добавляйте маршруты только в пользовательские таблицы маршрутизации, а таблицу по умолчанию изменяйте лишь в крайнем случае.
- Не добавляйте в пользовательские таблицы маршрутизации маршруты, противоречащие маршрутам в таблице по умолчанию.
- Не используйте маршруты, получаемые по протоколам DHCP и OSPF (или отключите автоматическое получение маршрутов по DHCP). Такие маршруты записываются в таблицу по умолчанию и будут задействованы с высшим приоритетом. Поэтому канал с динамической маршрутизацией всегда будет основным.
- Перед активацией политики маршрутизации убедитесь, что она настроена корректно и не нарушит связь ViPNet Coordinator IG с узлом, с которого вы настраиваете ViPNet Coordinator IG.
- Не используйте в качестве интернет-шлюза узел ViPNet, иначе при проверке состояния шлюза (DGD) он может ошибочно определиться как нерабочий.
- После добавления проверки шлюза по протоколу TCP и портам 80 и 443 необходимо создать разрешающий сетевой фильтр: источник — **Мой узел ViPNet**, назначение — IP-адрес шлюза, порты назначения — 80 и 443.

Основные сценарии использования функции MultiWAN см. документе «Сценарии работы», в разделе «Использование функции MultiWAN для резервирования каналов связи».

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**.

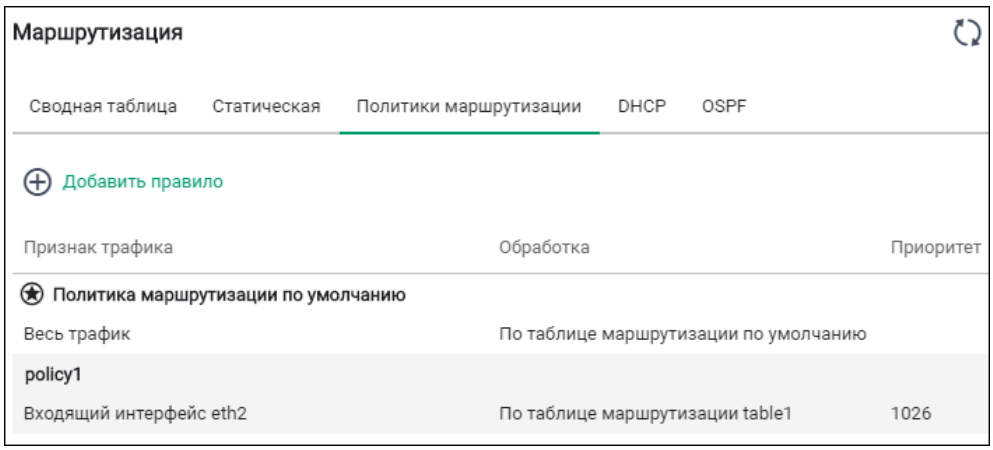


Рисунок 106. Настройка политик маршрутизации

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

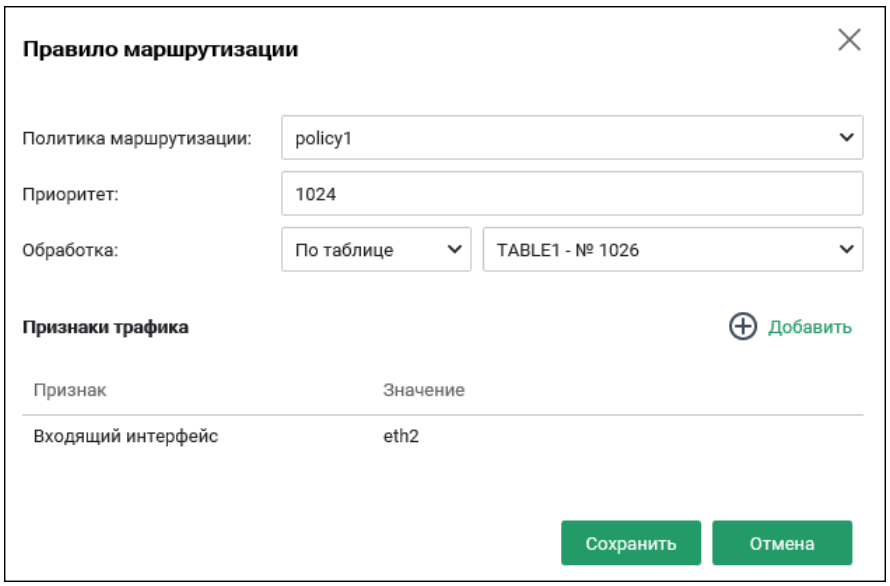


Рисунок 107. Добавление правила маршрутизации

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 IG), 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 IG через веб-интерфейс.

Настройка проверки состояния шлюзов (DGD)

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

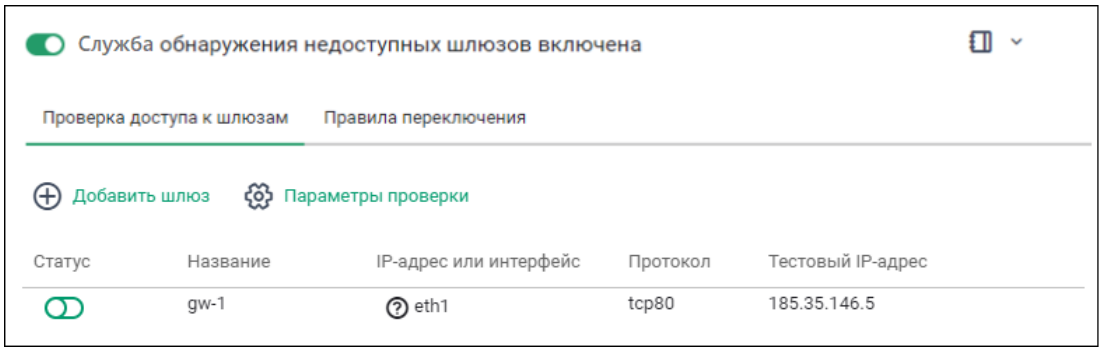


Рисунок 108. Настройка проверки состояния шлюзов

2 Включите **Службу обнаружения недоступных шлюзов**.

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

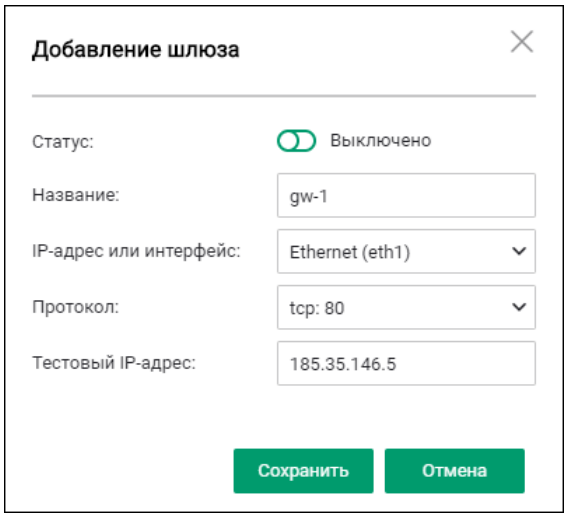


Рисунок 109. Добавление проверки доступности шлюза

- произвольное название шлюза;
- IP-адрес шлюза (если IP-адрес назначен статически) или сетевой интерфейс ViPNet Coordinator IG (если интерфейс получает IP-адрес по DHCP);

> **Примечание.** В качестве интерфейса вы также 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.

Внимание! Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере — это может привести к циклической перезагрузке обоих узлов кластера.

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:

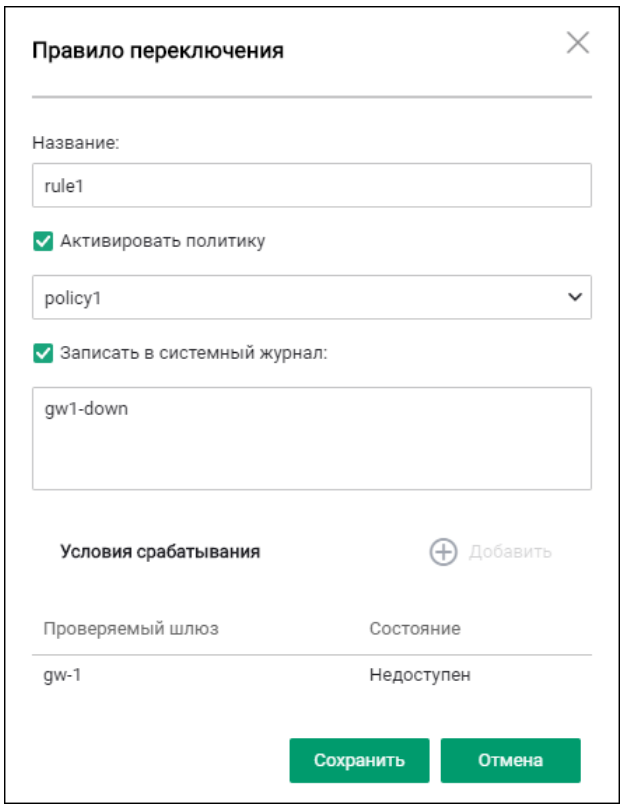


Рисунок 110. Добавление правила проверки состояния шлюза

- 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 задать параметры проверки доступности шлюзов:

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

7.2 Нажмите **Параметры проверки**.

7.3 Введите нужные значения.

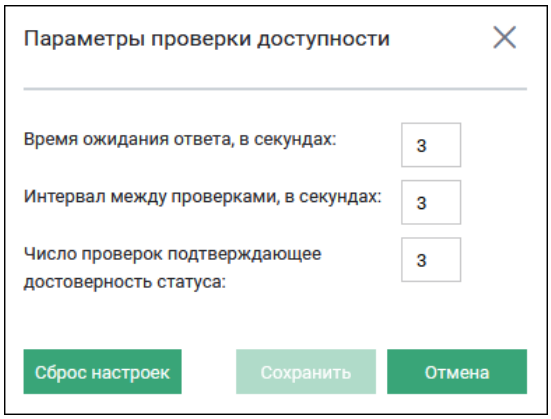


Рисунок 111. Окно настроек проверки доступности шлюза

Чтобы сбросить параметры к значениям по умолчанию, нажмите **Сброс настроек**.

7.4 Нажмите **Сохранить**.

8 Чтобы задать параметры регистрации событий службы в системном журнале:

8.1 Вверху справа нажмите .

8.2 По умолчанию события службы записываются в системный журнал. Чтобы отключить запись событий, снимите флажок **Вести журнал проверок шлюзов и переключений политик**.

8.3 Выберите уровень важности событий, записываемых в системный журнал.

Примечание. После настройки функции MultiWAN вы можете узнать, какая политика маршрутизации действует в настоящий момент времени. Для этого выберите **Маршрутизация** > **Маршрутизация** > **Политики маршрутизации**. Действующая в настоящий момент политика будет выделена в списке.

9

Настройка системных параметров

Настройка даты и времени 176

Переключение режимов работы межсетевого экрана 177

Настройка расписания перезагрузки 179

Просмотр лицензии 181

Просмотр серийного номера 182

Настройка даты и времени

Внимание!

- Если дата или время отличаются на узлах сети ViPNet, защищённые соединения между ними могут блокироваться. Рекомендуем настраивать синхронизацию системного времени по протоколу NTP.
- Если вы измените время более чем на сутки, ViPNet Coordinator IG будет блокировать весь сетевой трафик. Чтобы возобновить обработку трафика, перезагрузите ViPNet Coordinator IG.

Чтобы настроить дату и время:

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

2 Укажите часовой пояс, дату и время.

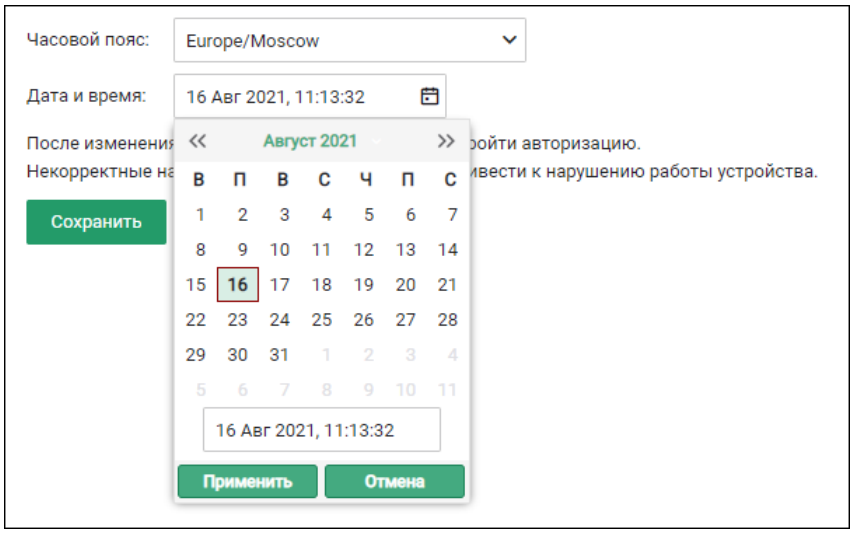


Рисунок 112. Настройка даты и времени

3 Нажмите **Сохранить**.

После изменения даты и времени соединение с ViPNet Coordinator IG будет завершено. Подключитесь повторно.

Переключение режимов работы межсетевого экрана

Если ViPNet Coordinator IG инициализирован как межсетевой экран типа «Д», он может работать в следующих режимах:

- Штатный. Работают все функции ViPNet Coordinator IG. Недоступно: обновление справочников и ключей, обновление ПО, управление копиями конфигураций VPN, импорт настроек.
- Регламентного обслуживания. Предназначен для обновления справочников и ключей, обновления ПО, управления копиями конфигураций VPN, импорта настроек, а также регламентного обслуживания защищаемых узлов.
- Специальный. Предназначен для чрезвычайных ситуаций в работе системы. Межсетевой экран по умолчанию настроен пропускать любой сетевой трафик. Обновление справочников и ключей, обновление ПО, управление копиями конфигураций VPN, импорт настроек недоступны.

Каждому из режимов соответствует свой набор сетевых фильтров. Все ваши действия с пользовательскими сетевыми фильтрами (создание, изменение, удаление) применяются только для текущего режима работы межсетевого экрана. Предустановленные сетевые фильтры для каждого из режимов работы приведены в приложении.

Чтобы переключить режим работы ViPNet Coordinator IG:



Внимание! Не переключайте режим работы ViPNet Coordinator IG одновременно разными способами. Иначе, это может нарушить работоспособность ViPNet Coordinator IG. Способы переключения режимов работы см. в документе «Подготовка к работе», в разделе «Режимы работы».

1 Выберите **Системные настройки** > **Режим работы**.

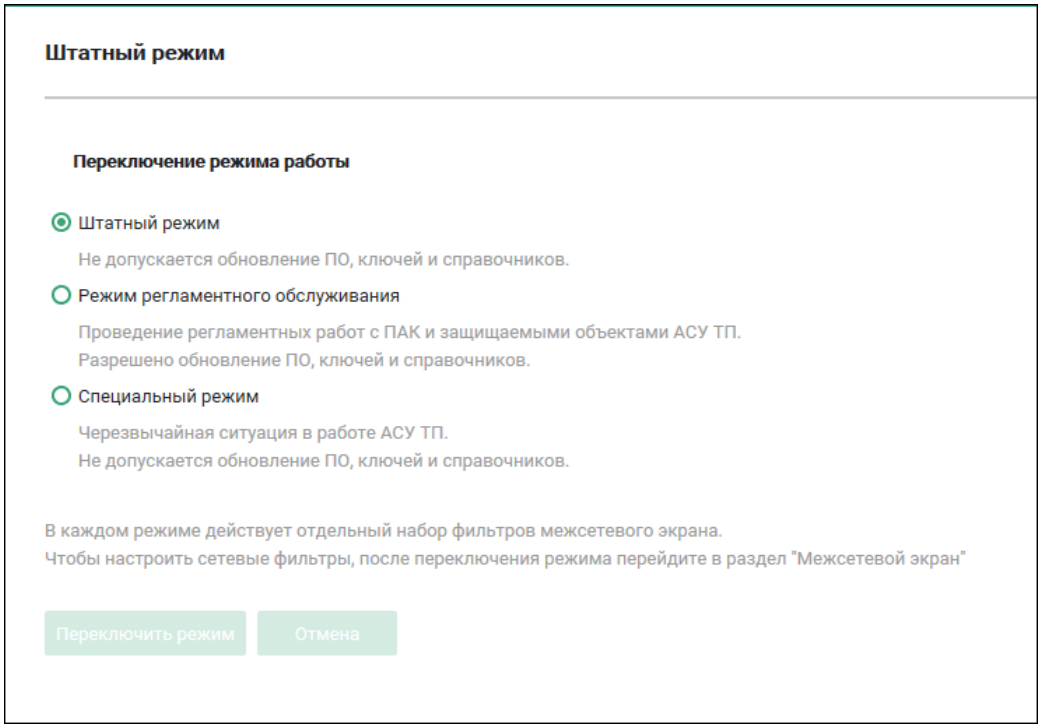


Рисунок 113. Переключение режимов работы межсетевого экрана

2 Выберите режим работы межсетевого экрана.

3 Нажмите **Переключить режим**.

Настройка расписания перезагрузки

Вы можете удалённо перезагрузить ViPNet Coordinator IG, 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.

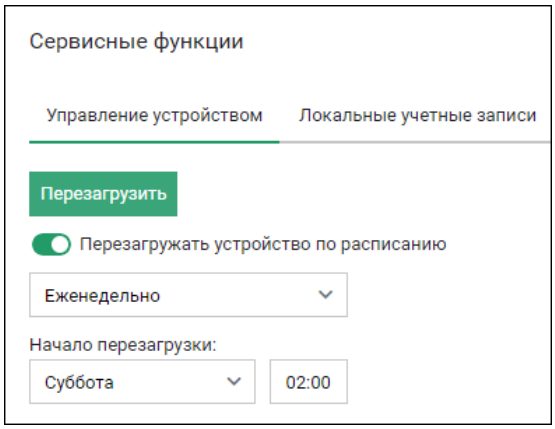


Рисунок 114. Перезагрузка ViPNet Coordinator IG

После перезагрузки соединение с ViPNet Coordinator IG через веб-интерфейс будет завершено. Повторно подключитесь.

Настройка перезагрузки в кластере

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».

Просмотр лицензии

Лицензия определяет функциональные характеристики ViPNet Coordinator IG. Чтобы просмотреть сведения о платформе и версии ПО ViPNet Coordinator IG, серийном номере, лицензии или ознакомиться с лицензионным соглашением:

1 В правой верхней части страницы нажмите и перейдите на вкладку **Лицензия** — в окне отобразятся сведения об основном и дополнительных объектах лицензирования:

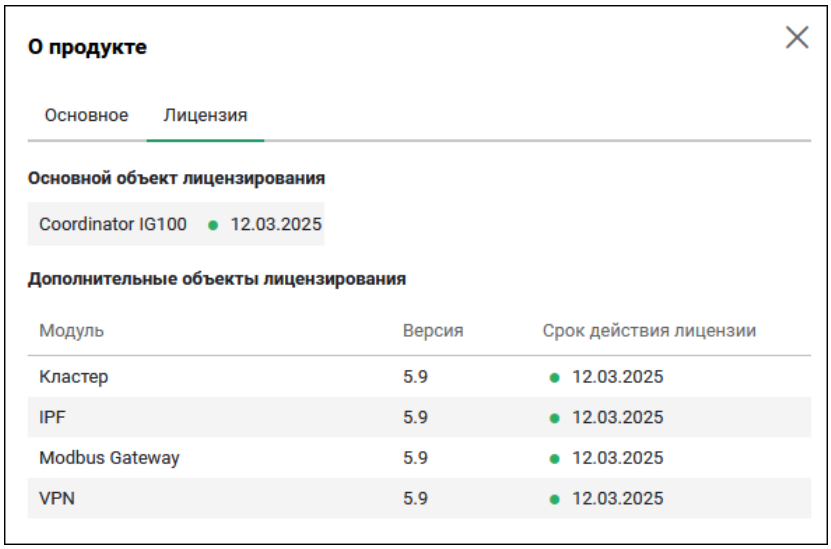


Рисунок 115. Сведения о лицензиях ViPNet Coordinator IG

2 Нажмите **Лицензионное соглашение**, чтобы ознакомиться с ним.

Просмотр серийного номера

Вверху справа нажмите .

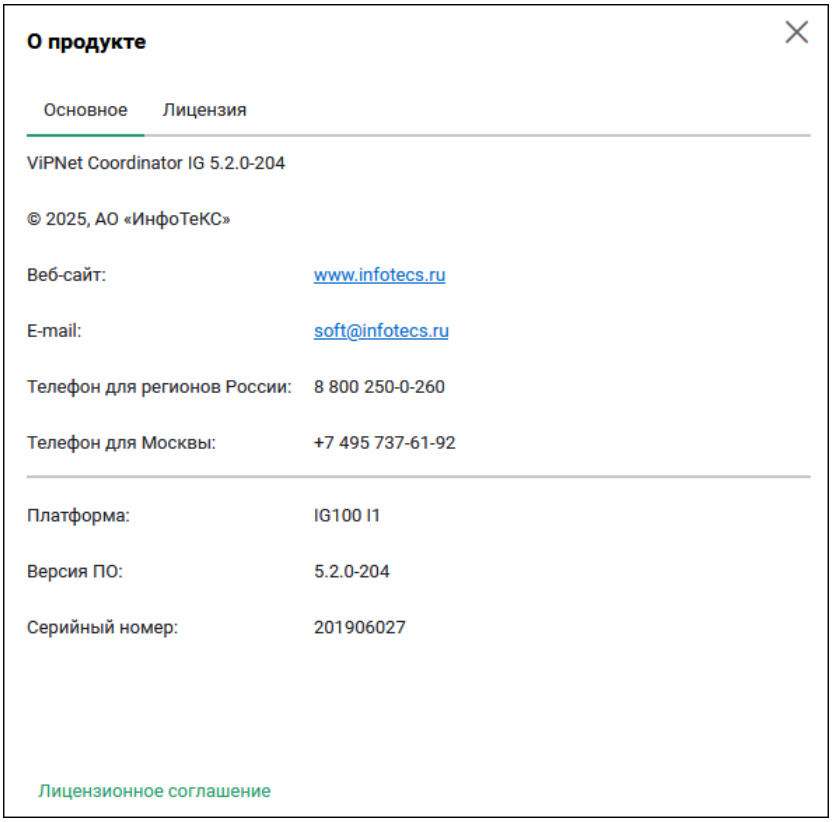


Рисунок 116. Просмотр информации об аппаратной платформе, версии ПО и серийного номера

Если серийный номер не задан, вы можете ввести его вручную. Это возможно, если вы выполнили обновление ПО ViPNet Coordinator IG с версии 5.1.0 или ниже. В этих версиях серийный номер не был записан в память. Чтобы ввести серийный номер:

1. Нажмите .
2. Введите серийный номер, указанный на этикетке вашего ViPNet Coordinator IG.
3. Нажмите .

10

Настройка параметров безопасности

Управление локальными учётными записями 184

Обновление справочников и ключей 186

Предотвращение подбора пароля учетных записей 187

Управление ключами локального SSH-сервера 188

Настройка подключения с помощью веб-интерфейса 189

Обновление ключей по истечении срока их действия 192

Управление локальными учётными записями

Учётная запись admin

Пароль локальной учётной записи администратора `admin` задаётся при инициализации ViPNet Coordinator IG и не имеет ограничения по сроку действия. Чтобы изменить его:

1 Выберите **Системные настройки** > **Сервисные функции** > **Локальные учетные записи**.

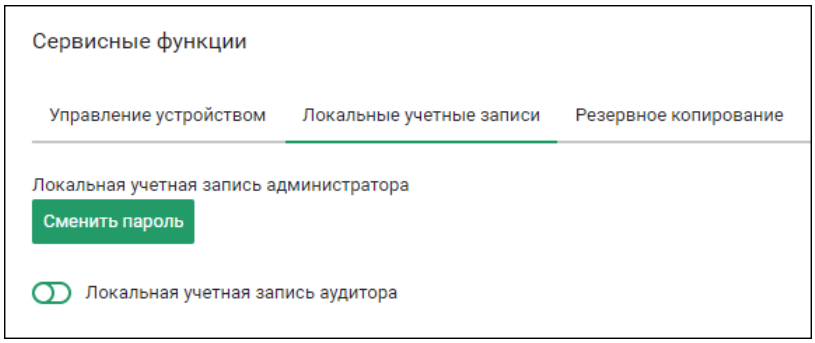


Рисунок 117. Изменение пароля локальной учётной записи admin; локальная учётная запись аудитора user отключена

2 Задайте новый пароль и нажмите **Продолжить**.

Учётная запись user

После инициализации ViPNet Coordinator IG локальная учётная запись аудитора `user` заблокирована. Чтобы разблокировать её, задайте пароль:

1 Выберите **Системные настройки** > **Сервисные функции** > **Локальные учетные записи**.

2 С помощью переключателя включите учётную запись локального аудитора.

3 Задайте пароль и нажмите **Продолжить**.

Теперь локальная учётная запись `user` включена.

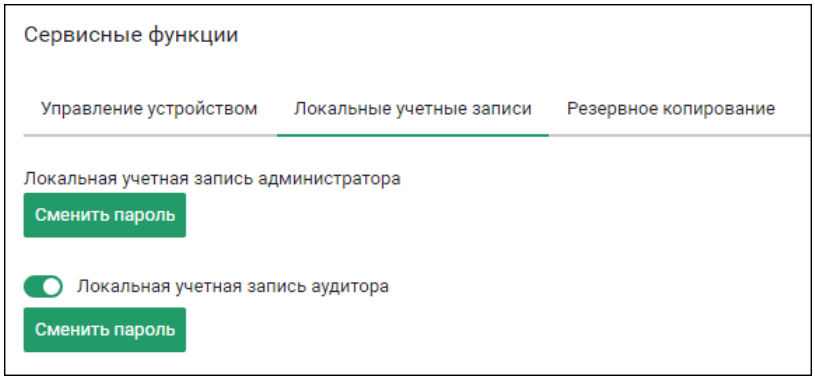


Рисунок 118. Локальная учетная записи аудитора user активирована

Чтобы заблокировать локальную учётную запись аудитора `user` и сбросить её пароль, выключите переключатель.

Управление локальными учётными записями в кластере

Пароли локальных учётных записей синхронизируются между узлами кластера. Пароль можно изменить только на активном узле кластера. Если узлы кластера переключились до того, как активный узел передал новый пароль на пассивный, доступ на узел, который стал активным, вы можете получить по старому паролю.

Обновление справочников и ключей

Если администратор защищённой сети добавляет или удаляет связи вашего ViPNet Coordinator IG с другими узлами защищённой сети, новые справочники и ключи обмена будут переданы с ViPNet Prime на ViPNet Coordinator IG.

Согласуйте с администратором защищённой сети дату и время изменения связей с учётом особенностей:

- Если ViPNet Coordinator IG используется как межсетевой экран типа «Д», необходимо переключить его в режим регламентного обслуживания перед обновлением справочников и ключей (см. Переключение режимов работы межсетевого экрана). Иначе справочники и ключи не будут обновлены. Администратор защищённой сети может сделать это удалённо с помощью ViPNet Prime Policy Management.
- Если уровень загрузки процессора ViPNet Coordinator IG близок к 100%, то во время обновления справочников и ключей возможны потери IP-пакетов и снижение производительности. Обновляйте справочники и ключи, когда нагрузка на ViPNet Coordinator IG минимальна. Вы можете посмотреть уровень загрузки процессора в окне **Состояние системы** (см. Просмотр состояния).

Информация о принятых обновлениях ключей записывается в журнал СКЗИ.

Для просмотра информации об установленных ключах обмена см. документ «Настройка с помощью командного интерпретатора», раздел «Просмотр сведений о ключе защиты обновлений и ключах обмена».

Предотвращение подбора пароля учетных записей

Для предотвращения подбора пароля реализована прогрессивная задержка ввода пароля, а также оповещение о попытках подбора пароля:

- Каждая неудачная попытка ввода пароля увеличивает счётчик ошибок аутентификации на единицу. Счётчик ошибок аутентификации индивидуален для каждой учётной записи.
- После трех неудачных попыток ввода пароля, следующий ввод станет доступным через 3 секунды. Каждая последующая неудачная попытка ввода:
  - увеличивает задержку;
  - считается попыткой подбора пароля.
- Каждая ошибка аутентификации регистрируется в системном журнале, а попытка подбора пароля — в журнале СКЗИ.
- Счётчик ошибок аутентификации сбрасывается после успешного ввода пароля или после 10 неудачных попыток подряд.
- Счётчик попыток подбора пароля является общим для всех локальных учётных записей, и отображается (если он больше нуля) в центре оповещений.

Чтобы просмотреть попытки подбора пароля:

1 Нажмите .

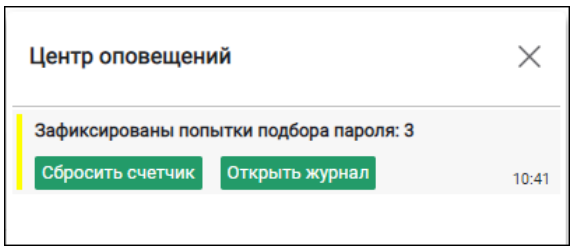


Рисунок 119. Оповещение о попытках подбора пароля

2 Чтобы просмотреть подробные сведения о попытках подбора пароля в журнале СКЗИ, нажмите **Открыть журнал**.

3 Чтобы сбросить счётчик попыток подбора пароля, нажмите **Сбросить счетчик**.

Управление ключами локального SSH-сервера

SSH-ключи используются для аутентификации при подключении к ViPNet Coordinator IG 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**.

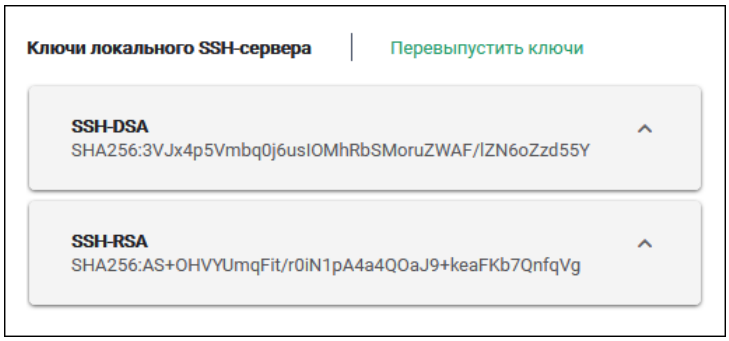


Рисунок 120. Ключи локального SSH-сервера

2 Нажмите **Перевыпустить ключи**.

3 Нажмите **Продолжить**.

Настройка подключения с помощью веб-интерфейса

Подключение к ViPNet Coordinator IG с помощью веб-интерфейса обеспечивает служба `WebUI`. По умолчанию служба использует протокол HTTPS (TCP-порт 8080) и самоподписанный сертификат, который генерируется при инициализации ViPNet Coordinator IG.

Вы можете:

- перевыпустить самоподписанный сертификат, например, если закончился срок его действия;
- использовать сертификат, изданный в удостоверяющем центре (далее — УЦ);
- изменить TCP-порт 8080;
- переключить работу службы `WebUI` на HTTP.

Перевыпуск самоподписанного сертификата

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

2 Нажмите **Перевыпустить самоподписанный сертификат для WebUI** и укажите параметры в соответствии с требованиями политик безопасности вашей организации:

2.1 В разделе **Владелец сертификата** — страну, регион, город, организацию, подразделение, адрес электронной почты.

2.2 В разделе **Параметры сертификата**:

- Длина RSA-ключа в битах: 2048, 3072, 4096.
- Алгоритм хэширования: sha256, sha384, sha512.
- Срок действия сертификата.
- IP-адреса сетевых интерфейсов и доменные имена, по которым вы будете подключаться.

2.3 Нажмите **Создать**.

3 Войдите в ViPNet Coordinator IG повторно.

Настройка использования сертификата, изданного удостоверяющим центром

Для издания сертификата в УЦ необходимо создать запрос на сертификат и передать его в УЦ. Вы можете создать запрос на сертификат в ViPNet Coordinator IG или с помощью стороннего ПО. Если запрос на сертификат создан с помощью стороннего ПО, начните настройку с шага 4.

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

2 Нажмите **Создать запрос на сертификат** и задайте:

2.1 В разделе **Владелец сертификата** — данные о местоположении.

2.2 В разделе **Параметры сертификата** — обязательные параметры:

- Имя файла запроса.
- Длина RSA-ключа в битах: 2048, 3072, 4096.
- Алгоритм хэширования: sha256, sha384, sha512.
- IP-адреса сетевых интерфейсов и доменные имена, по которым вы будете подключаться.

3 Нажмите **Создать запрос**.

4 Отправьте файл запроса в УЦ вместе с требованиями:

- УЦ должен использовать алгоритм хэширования SHA-2.
- Сертификат должен быть подписан с использованием алгоритма RSA.
- Файл сертификата должен быть в кодировке DER или Base64.

5 Получите в УЦ сертификат.

6 Импортируйте сертификат в ViPNet Coordinator IG:

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

6.2 Нажмите **Импортировать**.

6.3 Вставьте текст сертификата или загрузите файл сертификата.

Примечание. Если запрос на сертификат был создан с помощью стороннего ПО, импортируйте закрытый ключ и сертификат.

Поддерживаются файлы с расширениями PEM и CER. В контейнере PEM (`*.pem`) используется стандарт PKCS#12.

6.4 Нажмите **Импортировать**.

7 Установите импортированный сертификат для службы `WebUI`:

7.1 Выберите **Системные настройки** > **Общие** > **Веб-интерфейс**.

7.2 Выберите сертификат из списка.

7.3 Нажмите **Сохранить**.

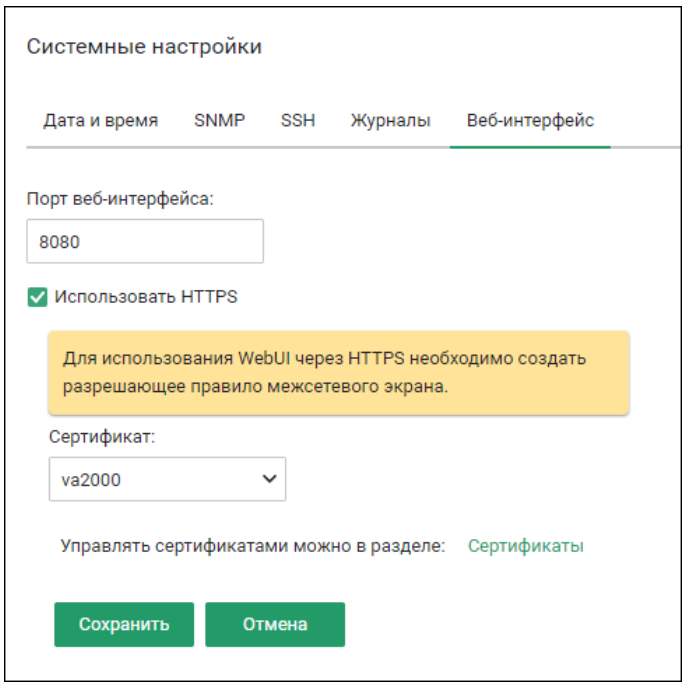


Рисунок 121. Параметры подключения с помощью веб-интерфейса

8 Войдите в ViPNet Coordinator IG повторно.

Изменение TCP-порта

1 Выберите **Системные настройки** > **Общие** > **Веб-интерфейс**.

2 Измените номер TCP-порта в поле **Порт веб-интерфейса**.

3 Нажмите **Сохранить**.

4 Измените номер TCP-порта в сетевом фильтре, который разрешает подключение к веб-интерфейсу (см. Создание и изменение сетевых фильтров) (`Allow ViPNet WebGUI`).

5 Войдите в ViPNet Coordinator IG повторно.

Переключение на протокол HTTP

1 Выберите **Системные настройки** > **Общие** > **Веб-интерфейс**.

2 Снимите флажок **Использовать HTTPS**.

3 Нажмите **Сохранить**.

4 Войдите в ViPNet Coordinator IG повторно.

Обновление ключей по истечении срока их действия

Ключи имеют ограниченный срок действия:

- ключ защиты обновлений — 15 месяцев;
- ключи обмена — 15 месяцев;
- ключ и соответствующий ему сертификат пользователя — 12 месяцев.

Истечение срока действия ключа защиты обновлений и ключей обмена не накладывает ограничений на работу ViPNet Coordinator IG. Но мы рекомендуем обновить ключи, чтобы гарантировать защиту трафика между узлами.

Истечение срока действия сертификата локального пользователя заблокирует ему доступ к ViPNet Coordinator IG через консоль, если в защищённой сети используется аутентификация по сертификату.

По умолчанию за 30 дней до истечения срока действия ключа появляется соответствующее сообщение после аутентификации в веб-интерфейсе или командном интерпретаторе. Если вы увидели сообщение о скором истечении срока действия:

- ключа защиты обновлений или ключа обмена — сообщите об этом администратору ViPNet Prime. Он сформирует новый ключ и вышлет его на ViPNet Coordinator IG.

Примечание.

- Если ViPNet Coordinator IG используется как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания перед обновлением ключей. Иначе ключи не будут обновлены. Администратор ViPNet Prime может сделать это с помощью ViPNet Prime Policy Management.
- Не обновляйте ключи, когда уровень загрузки процессора ViPNet Coordinator IG близок к 100%. Иначе во время обновления возможны потери IP-пакетов и снижение производительности. Чтобы проверить уровень загрузки процессора см. Просмотр состояния.

- сертификата пользователя — издайте новый сертификат (см. документ «Настройка с помощью командного интерпретатора», раздел «Издание сертификатов»).

С помощью командного интерпретатора вы можете настроить оповещение об истечении срока действия ключей и сертификата.

11

Резервное копирование и восстановление настроек

Способы резервирования и восстановления настроек 194

Управление индивидуальной конфигурацией 195

Управление универсальной конфигурацией 200

Способы резервирования и восстановления настроек

Вы можете сохранить настройки ViPNet Coordinator IG, чтобы иметь возможность восстановить их в будущем или перенести часть настроек на другой координатор.

Совокупность настроек называется копией конфигурации ViPNet Coordinator IG.

Таблица 10. Виды копий конфигурации ViPNet Coordinator IG

Вид копии конфигурации	Назначение	Создание	Хранение
Копия конфигурации VPN	Быстрое переключение между конфигурациями VPN и межсетевого экрана	Вручную	Память ViPNet Coordinator IG
Индивидуальная конфигурация	Восстановление настроек ViPNet Coordinator IG	Автоматически и вручную	Сервер ViPNet Prime, USB-носитель или сетевой узел
Универсальная конфигурация	Перенос настроек с одного ViPNet Coordinator IG на другой	Вручную	USB-носитель или сетевой узел

Для использования копий конфигураций VPN см. документ «Настройка с помощью командного интерпретатора», раздел «Управление копиями конфигураций VPN».

Управление индивидуальной конфигурацией

Индивидуальная конфигурация позволяет осуществлять возврат настроек ViPNet Coordinator IG к состоянию, которое было на момент создания этой конфигурации.

Индивидуальная конфигурация может использоваться:

- Для восстановления настроек ViPNet Coordinator IG в случае сбоя или некорректного обновления ПО.
- При замене неисправного ViPNet Coordinator IG, в том числе в составе кластера.

При экспорте файл индивидуальной конфигурации (`*.ecf`) зашифровывается на ключе обмена, который используется для защиты соединения ViPNet Coordinator IG с ViPNet Prime. Чтобы восстановить настройки из файла индивидуальной конфигурации, на ViPNet Coordinator IG должен быть установлен тот же ключ обмена, который использовался при экспорте. Если ключ обмена был обновлён на ViPNet Coordinator IG, создайте новую резервную копию индивидуальной конфигурации.

Индивидуальная конфигурация содержит:

- настройки защищённой сети;
- настройки сетевых интерфейсов;
- настройки PoE;
- настройки маршрутизации и статические маршруты, если такие созданы;
- сетевые фильтры и правила трансляции адресов;
- режим работы межсетевого экрана;
- правила фильтрации промышленных протоколов;
- настройки параметров обработки прикладных протоколов;
- настройки шлюза Modbus и интерфейса GPIO;
- настройки системы защиты от сбоев;
- настройки транспортного сервера MFTP;
- журналы и настройки протоколирования;
- настройки дополнительных служб (DHCP-сервера и других);
- настройки туннелирования;
- текущие ключи для соединений по протоколу SSH.

Резервное копирование индивидуальной конфигурации

Резервное копирование индивидуальной конфигурации может быть выполнено:

- Автоматически — на сервер ViPNet Prime один раз в сутки.
- Вручную — на сервер ViPNet Prime или папку компьютера, с которого вы подключились к ViPNet Coordinator IG.



Примечание.

- При управлении ViPNet Coordinator IG с помощью командного интерпретатора вы можете создать резервную копию на USB-носитель, подключенный к ViPNet Coordinator IG. При этом резервное копирование на другой узел, кроме сервера ViPNet Prime, недоступно.
- На время резервного копирования создаётся сетевой фильтр, разрешающий подключение к серверу ViPNet Prime, и останавливаются службы `vpn` и `mftp`. По завершении копирования фильтр будет удалён, а службы будут запущены заново.

Независимо от того, как была создана резервная копия, на сервере ViPNet Prime хранится только последняя копия конфигурации — каждая последующая копия затирает предыдущую. По умолчанию автоматическое резервное копирование выключено.

Шаблон имени файла индивидуальной конфигурации: `<имя сетевого узла>-<время создания файла>.ecf`.

Формат времени создания файла: `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды. Время записывается в системе UTC.

Автоматическое резервное копирование

Чтобы настроить автоматическое резервное копирование:

1 Выберите **Системные настройки** > **Сервисные функции** > **Резервное копирование**.

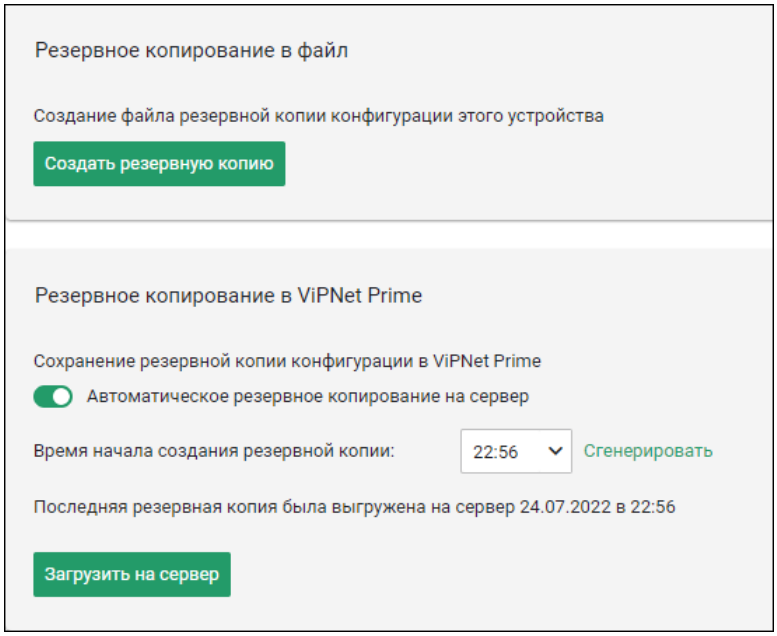


Рисунок 122. Настройка резервного копирования индивидуальной конфигурации

2 В разделе **Резервное копирование в ViPNet Prime** включите **Автоматическое резервное копирование на сервер**.

3 Задайте время создания резервной копии:

3.1 Чтобы установить точное время создания резервной копии, выберите его из списка.

3.2 Чтобы выбрать интервал, из которого будет случайным образом выбираться время создания резервной копии:

3.2.1 Нажмите **Сгенерировать**.

3.2.2 Выберите из списков начало и окончание интервала времени.

3.2.3 Нажмите **Сгенерировать**.

Теперь резервная копия индивидуальной конфигурации будет создаваться и сохраняться на сервере ViPNet Prime ежедневно, в заданное время.

Примечание. Расписание резервного копирования настраивается только на активном узле кластера.

Резервное копирование вручную

Чтобы однократно создать копию конфигурации на сервере ViPNet Prime, нажмите **Загрузить на сервер**. Дождитесь завершения операции. Время загрузки последней резервной копии на сервер обновится.

Чтобы создать резервную копию и сохранить её в папке компьютера, с которого вы подключились к ViPNet Coordinator IG:

1 В разделе **Резервное копирование в файл** нажмите **Создать резервную копию**.

2 Дождитесь завершения операции. Файл индивидуальной конфигурации будет сохранён в папке **Загрузки**.

Восстановление из резервной копии индивидуальной конфигурации

1 Если копия индивидуальной конфигурации хранится на сервере ViPNet Prime, скачайте её.

2 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания.

3 Выберите **Системные настройки** > **Сервисные функции** > **Резервное копирование**.

4 В разделе **Восстановление** нажмите **Восстановить**.

5 Выберите файл резервной копии и нажмите **Далее**.

6 Просмотрите параметры подключения к ViPNet Coordinator IG, которые будут восстановлены из резервной копии.

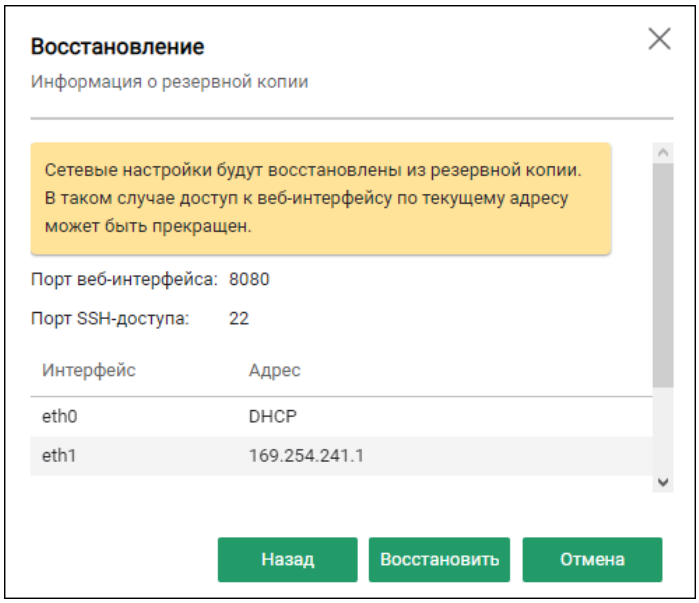


Рисунок 123. Параметры подключения к ViPNet Coordinator IG после восстановления настроек

Внимание! Если вы подключены к сетевому интерфейсу, который после восстановления настроек должен получить IP-адрес по DHCP, связь с ViPNet Coordinator IG будет потеряна. В этом случае подключитесь через консоль после восстановления настроек и перезапустите сетевой интерфейс, последовательно выполнив команды:

1 `inet ifconfig <интерфейс> down`

2 `inet ifconfig <интерфейс> up`

7 Нажмите **Восстановить**.

8 Дождитесь сообщения о завершении восстановления настроек и нажмите **Перезагрузить устройство**.

Управление универсальной конфигурацией

Универсальная конфигурация позволяет переносить настройки с одного ViPNet Coordinator IG на другой. Оба ViPNet Coordinator IG должны быть одного исполнения, но могут отличаться версией ПО. Перенос настроек возможен с версии ПО, не ниже 4.3.2.

При экспорте настроек ViPNet Coordinator IG версии 5.2.0 универсальная конфигурация будет содержать следующие группы настроек:

- настройки межсетевого экрана (сетевые фильтры для всех режимов работы, правила трансляции адресов, группы объектов);
- настройки шлюзов Modbus;
- правила фильтрации промышленных протоколов;
- настройки интерфейса GPIO;
- настройки сетевых интерфейсов;
- таблицы и политики статической маршрутизации.

Файл универсальной конфигурации (`*.vbe`) зашифровывается на пароле, который задаётся при экспорте конфигурации.

Особенности импорта настроек

- При импорте настроек вы можете выбрать, какие группы настроек импортировать, а какие нет.
- Настройки, выбранные для импорта, можно добавить к текущим настройкам на ViPNet Coordinator IG или заменить их. Возможность добавления настроек доступна не для всех групп.
- Если конфигурация была создана в ViPNet Coordinator IG, работающем как межсетевой экран типа «Д»:
  - в ViPNet Coordinator IG с типом «Д» импортируются сетевые фильтры для всех режимов;
  - в ViPNet Coordinator IG с типом «А/Б» импортируются сетевые фильтры только из того режима, в котором эта конфигурация была создана.
- Если конфигурация была создана в ViPNet Coordinator IG, работающем как межсетевой экран типа «А/Б», сетевые фильтры импортируются в штатный режим работы независимо от типа межсетевого экрана на вашем ViPNet Coordinator IG.
- При импорте настроек шлюза Modbus:
  - Если конфигурация была создана в ViPNet Coordinator IG, поддерживающем только один шлюз Modbus:

- при выборе замены настроек, они переносятся на первый последовательный интерфейс подходящего типа (RS-232 или RS-485) с присвоением имени шлюза `modbus1`;
- при выборе добавления настроек, они переносятся на свободный последовательный интерфейс подходящего типа с присвоением имени шлюза `modbus1` или `modbus2`. Если свободного интерфейса нет, настройки не переносятся.

  - Если конфигурация была создана в ViPNet Coordinator IG, поддерживающем несколько шлюзов Modbus:
    - при выборе замены настроек, они переносятся на соответствующие последовательные интерфейсы подходящего типа без замены имён шлюзов;
    - при выборе добавления настроек, они переносятся на свободные последовательные интерфейсы подходящего типа с присвоением имени шлюза `modbus<свободный порядковый номер>`. Если свободного интерфейса нет, настройки не переносятся.
  - Если добавляемый маршрут содержит адрес Modbus-устройства, для которого уже заданы маршруты, такой маршрут не будет добавлен.

- При импорте правил фильтрации промышленных протоколов:
  - Если имя добавляемого набора правил совпадает с именем существующего набора правил, такой набор правил будет добавлен с дополнительным суффиксом в имени.
  - Если содержимое добавляемого набора правил совпадает с существующим набором правил, такой набор не будет добавлен.

Экспорт универсальной конфигурации

1 Выберите **Системные настройки** > **Сервисные функции** > **Экспорт и импорт настроек**.

2 В разделе **Экспорт конфигурации** нажмите **Экспортировать**.

3 Добавьте комментарий.

4 Задайте пароль защиты файла конфигурации. Вы можете использовать прописные и строчные буквы латинского алфавита, цифры и символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

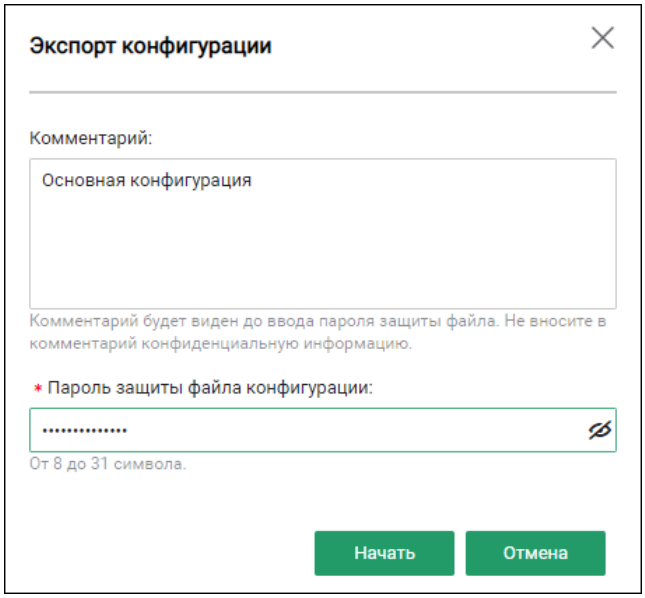


Рисунок 124. Экспорт универсальной конфигурации

5 Нажмите **Начать** и дождитесь завершения экспорта.

Файл универсальной конфигурации будет сохранён в папке **Загрузки** вашего компьютера.

Шаблон имени файла универсальной конфигурации: `<имя сетевого узла>-<время создания файла>.vbe`.

Формат времени создания файла: `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды. Время записывается в системе UTC.

Импорт настроек универсальной конфигурации

Примечание. Если импорт настроек через веб-интерфейс недоступен по причине нарушения работоспособности ViPNet Coordinator IG, вы можете импортировать настройки в режиме инициализации. Подробнее см. документ «Настройка с помощью командного интерпретатора» раздел «Импорт настроек универсальной конфигурации»

1 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания.

2 Выберите **Системные настройки** > **Сервисные функции** > **Экспорт и импорт настроек**.

3 В разделе **Импорт конфигурации** нажмите **Импортировать**.

4 Выберите файл универсальной конфигурации и нажмите **Далее**.

5 Введите пароль защиты файла конфигурации.

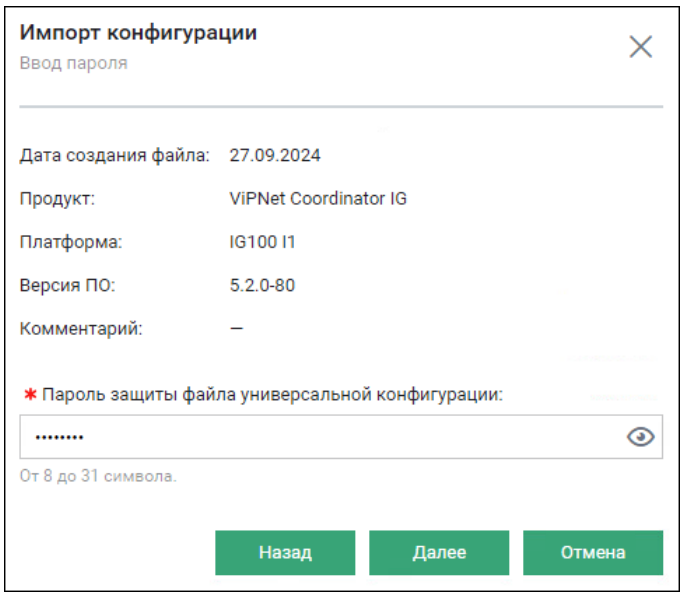


Рисунок 125. Ввод пароля защиты файла конфигурации

6 Выберите группы импортируемых настроек и способ импорта каждой из них (**Заменить** или **Добавить**).

Примечание. Если у вас одно из исполнений ViPNet Coordinator IG10, и вы хотите импортировать все настройки, рекомендуется сделать это в два этапа: сначала импортируйте одну часть настроек (например, настройки МЭ, сетевые настройки, таблицы и политики статической маршрутизации), затем после шага 9 повторите сценарий импорта (шаги 2–10), но на шаге 6 выберите оставшуюся часть настроек.

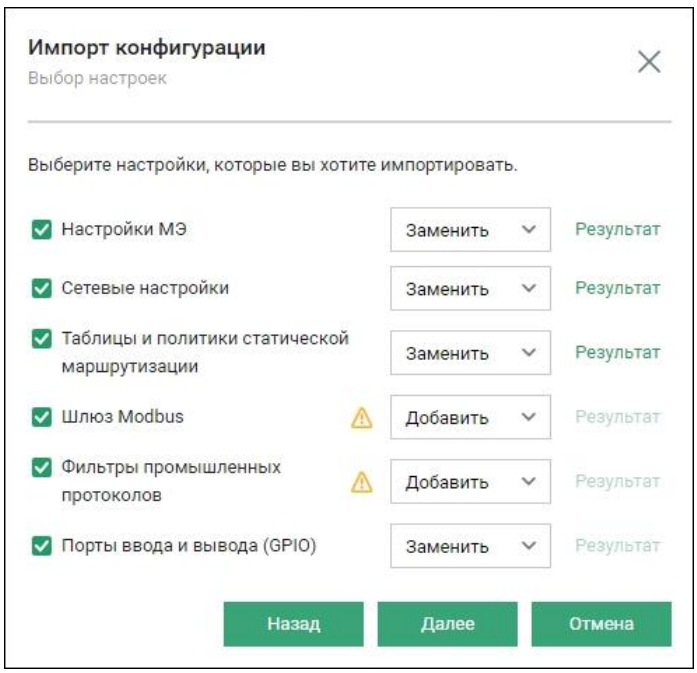


Рисунок 126. Выбор групп настроек и способа импорта

Чтобы просмотреть, как изменятся настройки вашего ViPNet Coordinator IG после импорта, нажмите **Результат** напротив соответствующей группы настроек.

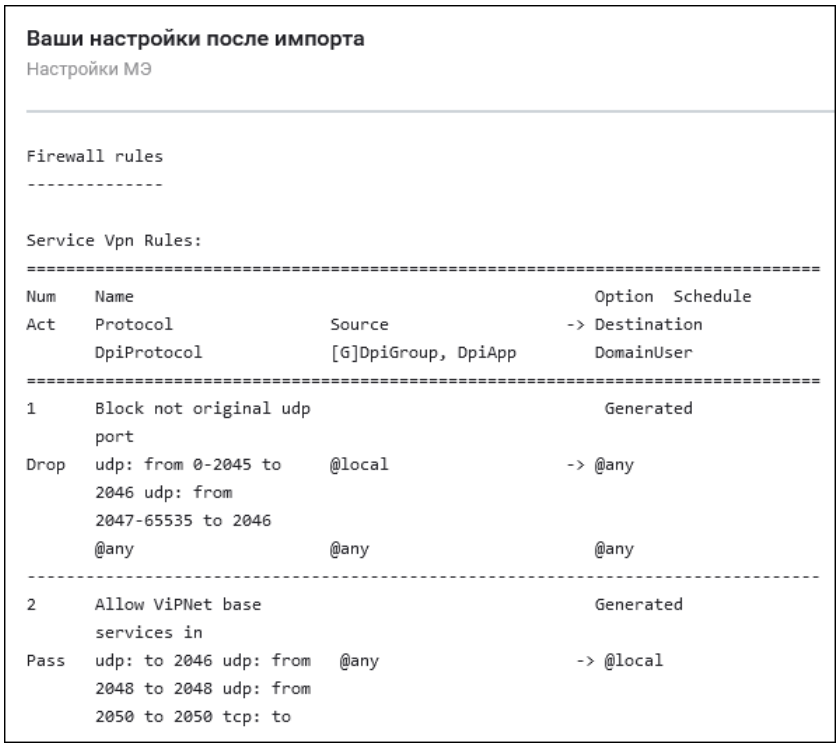


Рисунок 127. Просмотр импортируемых настроек группы firewall

7 Запомните параметры подключения к ViPNet Coordinator IG из раздела **Параметры подключения после импорта,** если до импорта были заданы другие параметры, и нажмите **Импортировать.**

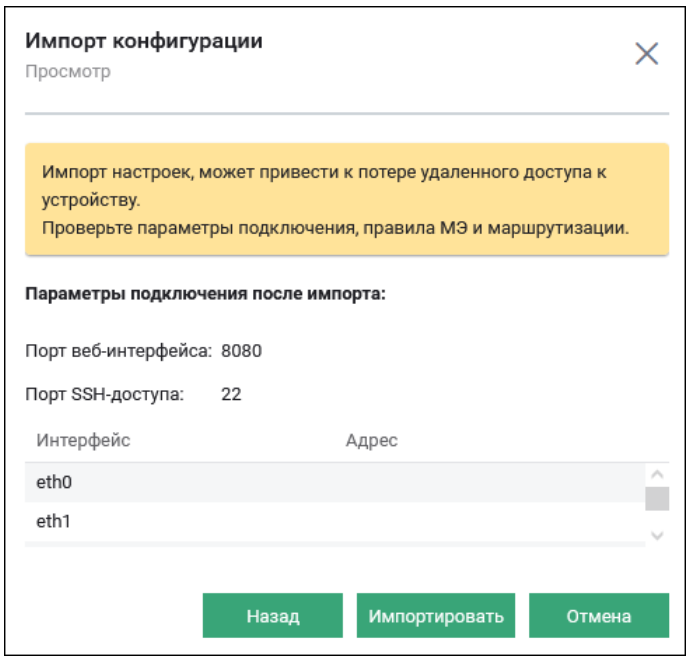


Рисунок 128. Параметры подключения к ViPNet Coordinator IG после импорта настроек

8 Дождитесь завершения импорта настроек и нажмите **Закрыть**.

9 Перезагрузите ViPNet Coordinator IG.

10 Если установлен режим межсетевого экрана типа «Д», переключите ViPNet Coordinator IG обратно в штатный режим работы.

12

Работа с журналами

Настройка журналов 207

Журнал IP-пакетов 210

Журнал пакетов промышленных протоколов 214

Журнал аудита 217

Журнал СКЗИ 219

Журнал MFTP 221

Журнал DNS-запросов 223

Системный журнал 225

Настройка журналов

Чтобы настроить параметры ведения журналов:

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

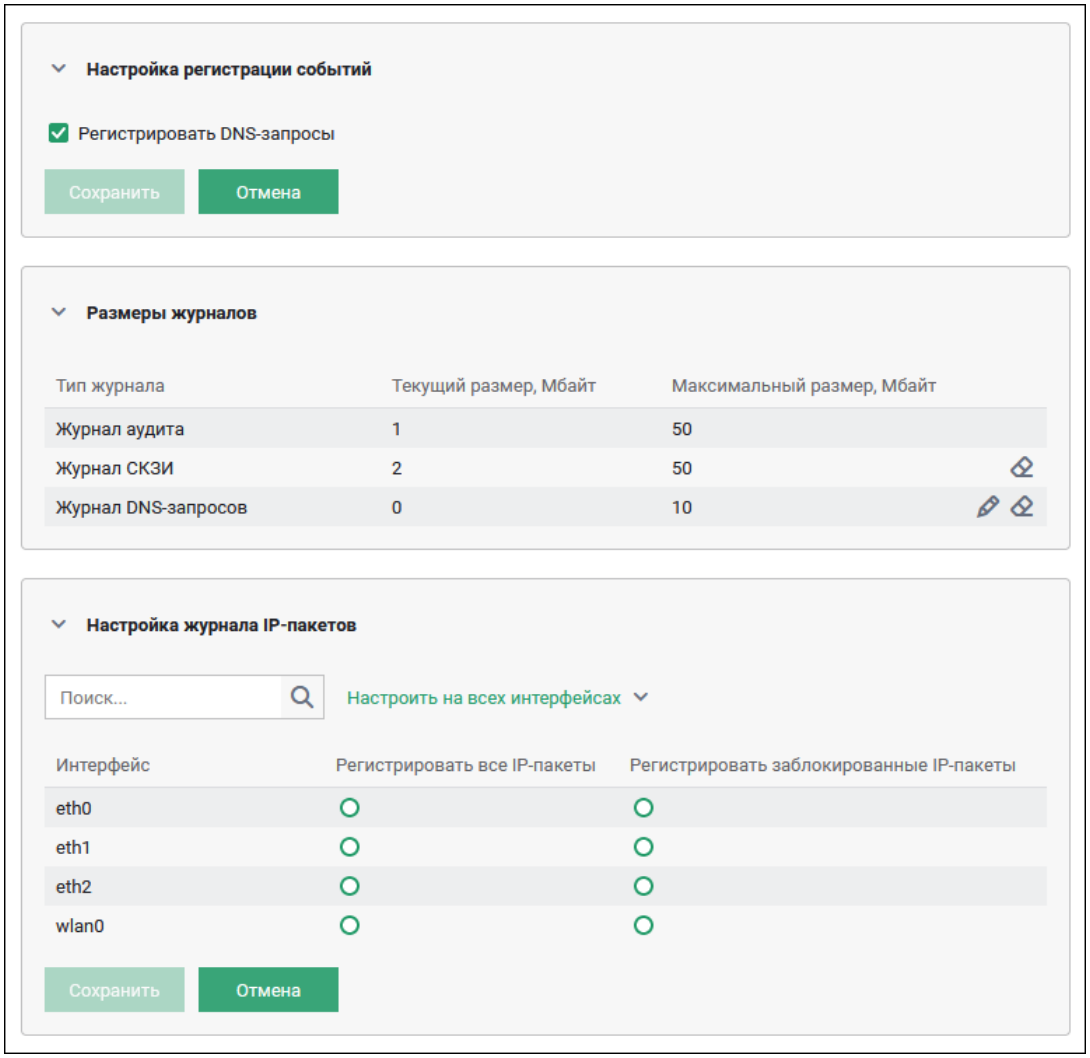


Рисунок 129. Настройка журналов

2 Чтобы настроить условия регистрации IP-пакетов в журнале IP-пакетов:

2.1 Откройте раздел **Настройка журнала IP-пакетов**.

Примечание. Настройка условий регистрации IP-пакетов на любом из сетевых интерфейсов отключает регистрацию IP-пакетов по сетевым фильтрам на этом интерфейсе. То есть параметр каждого фильтра, отвечающий за регистрацию IP-пакетов при его срабатывании, будет игнорироваться. Подробнее о способах регистрации пакетов см. в разделе Журнал IP-пакетов.

Чтобы снова включить регистрацию IP-пакетов по сетевым фильтрам на одном или на всех интерфейсах, измените настройки конфигурационного файла с помощью командного интерпретатора. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Журнал IP-пакетов».

2.2 Чтобы настроить регистрацию IP-пакетов на всех сетевых интерфейсах, в списке **Настроить на всех интерфейсах** выберите:

- **Регистрировать заблокированные IP-пакеты** — на всех интерфейсах будут регистрироваться только заблокированные и отклонённые IP-пакеты.
- **Регистрировать все IP-пакеты** — на всех интерфейсах будут регистрироваться заблокированные, отклонённые и пропущенные IP-пакеты.

2.3 Чтобы настроить регистрацию IP-пакетов на определённом сетевом интерфейсе, выберите напротив имени интерфейса, какие пакеты (все или только заблокированные) будут регистрироваться в журнале IP-пакетов.

Если для интерфейса не будет выбран ни один из вариантов, на нём продолжит действовать регистрация IP-пакетов по сетевым фильтрам (подробнее о способах регистрации IP-пакетов см. в разделе Журнал IP-пакетов).

2.4 Нажмите **Сохранить**.

3 Чтобы изменить максимальный размер журналов или очистить их:

3.1 Откройте раздел **Размеры журналов**.

3.2 Для изменения максимального размера журнала нажмите  и введите новое значение.

Максимальный размер журнала DNS-запросов вы можете задать в диапазоне: 1–50 Мбайт.

Примечание. Если новое значение максимального размера журнала меньше его текущего размера, наиболее старые записи будут автоматически удалены.

Максимальный размер журналов аудита и СКЗИ вы можете изменить только с помощью командного интерпретатора (см. документ «Настройка с помощью командного интерпретатора», раздел «Журналы аудита и СКЗИ»).

3.3 Для очистки журнала нажмите  .

Очистка журнала аудита недоступна. При переполнении журнала старые записи будут автоматически заменяться новыми.

Перед очисткой журнала СКЗИ, он будет скачан на ваш компьютер.

4 Чтобы настроить регистрацию DNS-запросов:

4.1 Откройте раздел **Настройка регистрации событий**.

4.2 По умолчанию ведение журнала DNS-запросов включено, DNS-запросы регистрируются после запуска DNS-сервера. Чтобы отключить ведение журнала, снимите флажок **Регистрировать DNS-запросы**.

4.3 Нажмите **Сохранить**.

Журнал IP-пакетов

ViPNet Coordinator IG может регистрировать IP-пакеты в журнале одним из способов:

- Регистрация по сетевым фильтрам. У каждого сетевого фильтра есть параметр, который указывает, регистрировать обработанные им IP-пакеты или нет. По умолчанию этот параметр включён на всех сетевых фильтрах с действием **Блокировать трафик** и **Отклонять трафик с ответом**, поэтому регистрируются только заблокированные и отклонённые IP-пакеты. Вы можете включить или отключить регистрацию IP-пакетов на любом сетевом фильтре отдельно (см. Настройка регистрации IP-пакетов при срабатывании фильтров).

  Этот способ используется по умолчанию после инициализации ViPNet Coordinator IG.

- Регистрация по сетевым интерфейсам:
  - Каждый пропущенный и заблокированный локальный IP-пакет отображается в журнале один раз — на том интерфейсе, через который он прошёл, 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 пришёл, второй раз — на интерфейсе, через который он ушёл.

  Этот способ использовался в ViPNet Coordinator IG более ранних версий и будет по умолчанию использоваться после обновления ПО ViPNet Coordinator IG до версии 5.2.0. При этом параметр регистрации IP-пакетов у сетевых фильтров игнорируется.

Для каждого сетевого интерфейса может быть выбран только один из способов регистрации IP-пакетов:

- Чтобы включить регистрацию IP-пакетов по интерфейсам, см. Настройка журналов.
- Чтобы включить регистрацию IP-пакетов по фильтрам, см. документ «Настройка с помощью командного интерпретатора», раздел «Журнал IP-пакетов».

Широковещательные (`registerbroadcast`) и служебные (`registerevents`) IP-пакеты регистрируются только по интерфейсам независимо от способа регистрации других IP-пакетов.

Примечание. В кластере журнал IP-пакетов можно просмотреть только на активном узле.

Чтобы просмотреть журнал IP-пакетов:

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

  По умолчанию отобразятся не более 100 записей обо всех IP-пакетах, зарегистрированных в журнале за последний час.

2 Чтобы настроить вид отображения записей, нажмите и выберите параметры, которые будут отображаться в журнале.

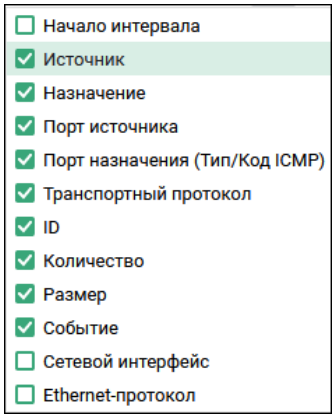


Рисунок 130. Настройка вида таблицы журнала регистрации IP-пакетов

3 Чтобы выбрать определённые записи журнала, используйте фильтр:

3.1 Нажмите **Фильтр IP-пакетов**.

3.2 В разделе **Признаки IP-пакетов** выберите:

- транспортный протокол, с использованием которого передаются IP-пакеты;
- сетевой интерфейс, через который проходят IP-пакеты;
- тип трафика, к которому относятся IP-пакеты;
- тип адреса IP-пакетов;
- признак трансляции IP-пакетов;
- событие межсетевого экрана, к которому относятся IP-пакеты;
- код события в журнале;
- сетевой фильтр, который сработал при обработке IP-пакетов.

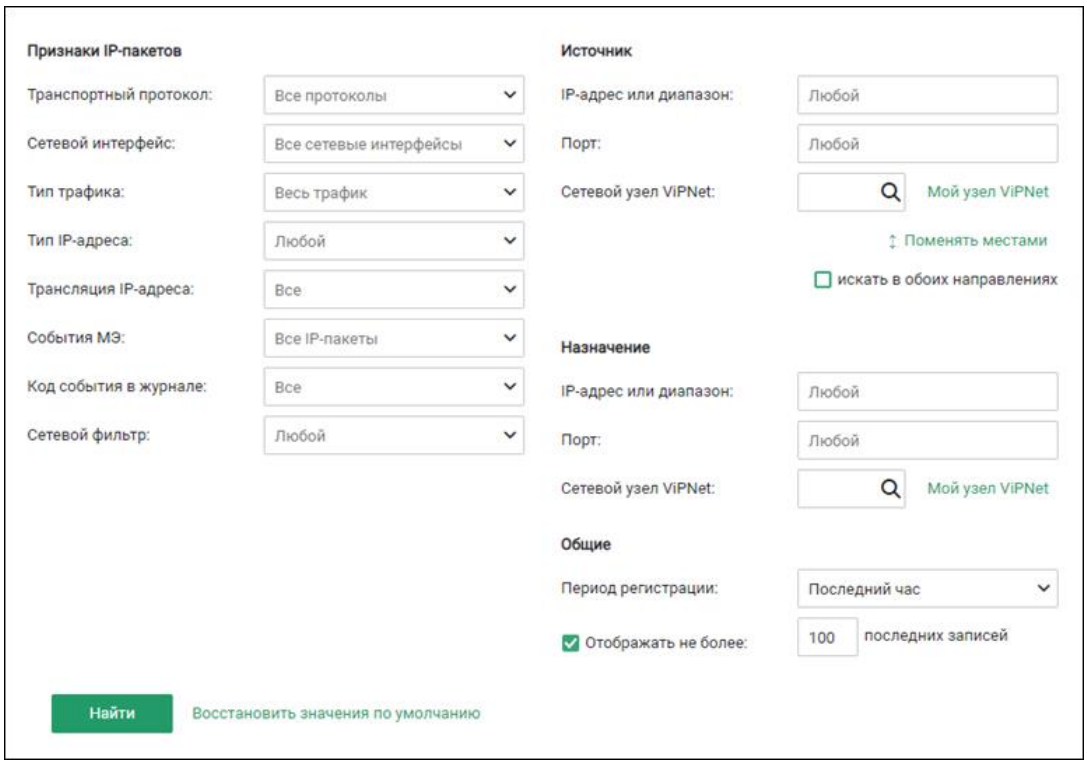


Рисунок 131. Настройка фильтра журнала IP-пакетов

3.3 В разделах **Источник** и **Назначение** укажите:

- IP-адрес отправителя (получателя) или диапазон IP-адресов отправителей (получателей);
- номер порта отправителя (получателя);
- идентификатор узла ViPNet.

3.4 В разделе **Общие**:

- В поле **Период регистрации** укажите период времени, за который вы хотите просмотреть информацию об IP-пакетах.
- Чтобы ограничить число записей, выберите **Отображать не более** и укажите число записей. Иначе будет отображено не более 100 записей.

Совет. Для анализа большого количества записей вы можете воспользоваться внешней аналитической системой. Подробнее см. документ «Настройка с помощью командного интерпретатора» раздел «Экспорт журнала IP-пакетов по сети в формате CEF».

3.5 Нажмите **Найти**.

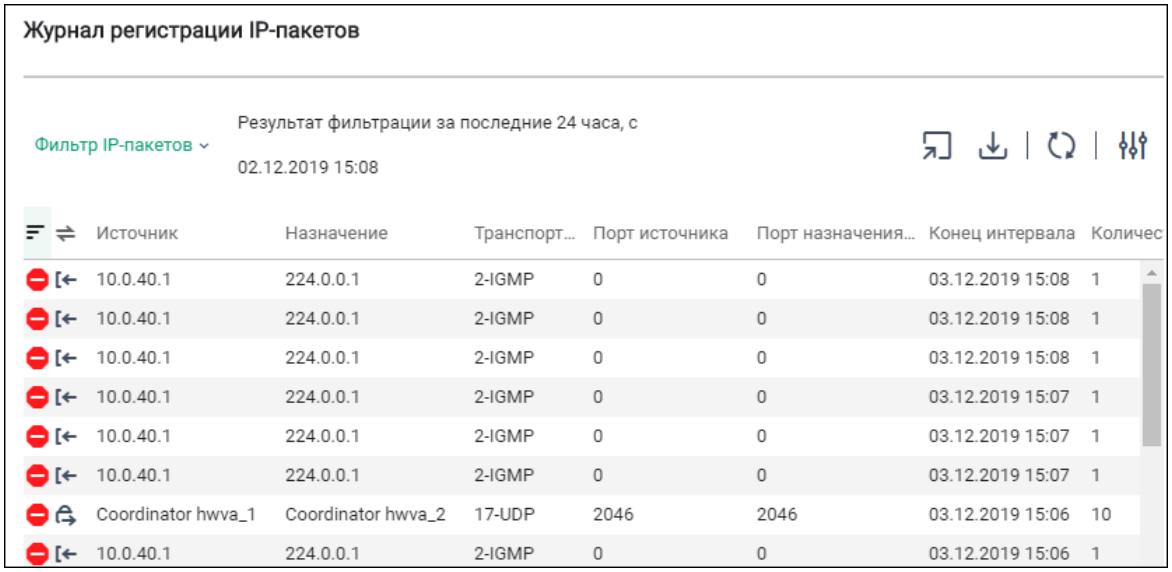


Рисунок 132. Просмотр результатов поиска в журнале IP-пакетов

4 Выполните одно из действий со списком выбранных записей:

- Для просмотра подробной информации об IP-пакете выберите запись в списке.
- Для экспорта списка выбранных записей в файл формата `xls` нажмите .
- Для просмотра списка выбранных записей в новой вкладке браузера нажмите .

Журнал пакетов промышленных протоколов

Служба IPF ведет журнал, в который вносится информация обо всех пакетах, обработанных правилами фильтрации промышленных протоколов на прикладном уровне. Информация о каждом обработанном пакете вносится в журнал один раз, без разделения на сетевые интерфейсы.

Чтобы просмотреть журнал пакетов промышленных протоколов:

1. Выберите **Журналы** > **Журнал пакетов АСУ ТП**.
2. Выберите вкладку промышленного протокола:
   - **Modbus**;
   - **МЭК 60870-5-104**.

   По умолчанию отобразятся не более 100 записей обо всех пакетах, обработанных правилами фильтрации промышленных протоколов за последний час.
3. Чтобы настроить вид журнала, нажмите вверху справа и выберите отображаемые столбцы.
4. Чтобы просмотреть определенные записи, нажмите **Фильтр IP-пакетов**:
   - В разделе **Признаки IP-пакетов** выберите:
     - транспортный протокол, по которому передаются IP-пакеты;
     - тип IP-адреса;
     - событие, с которым зарегистрированы IP-пакеты.
   - В разделе ниже укажите значения параметров выбранного промышленного протокола.

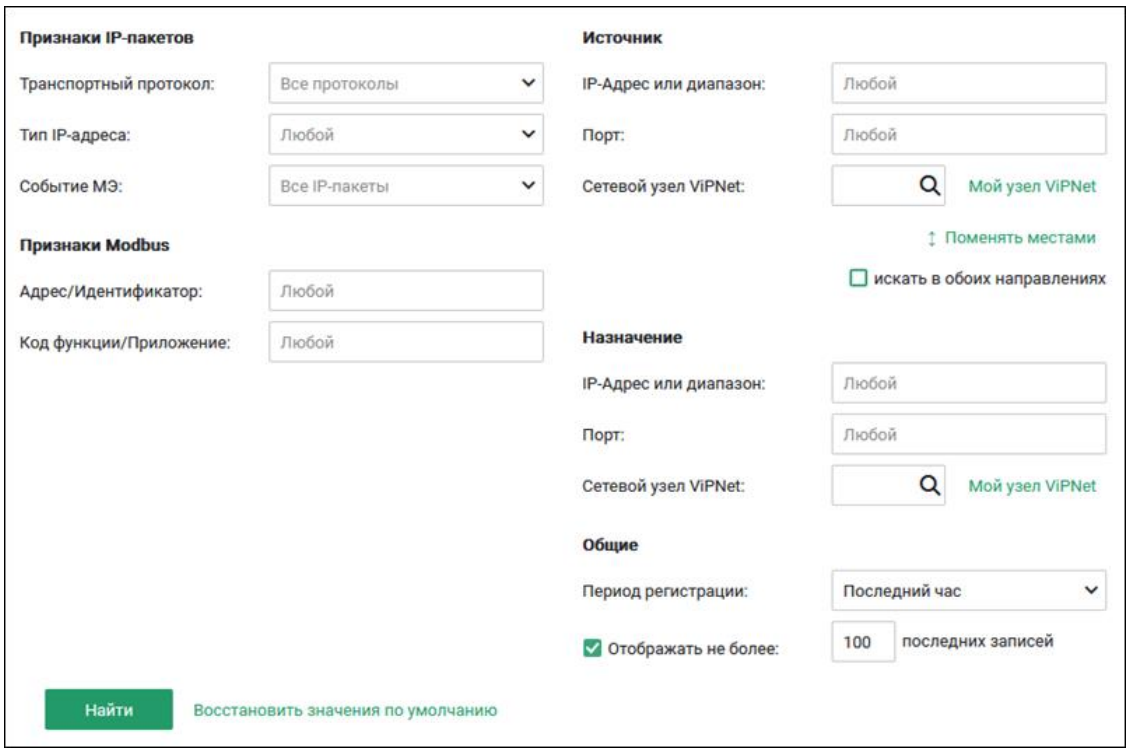


Рисунок 133. Настройка фильтра журнала пакетов промышленных протоколов

- В разделах **Источник** (**Назначение**) укажите:
  - IP-адрес или диапазон IP-адресов отправителя (получателя);
  - номер порта отправителя (получателя);
  - идентификатор узла ViPNet.
- В разделе **Общие**:
  - В поле **Период регистрации** укажите диапазон времени, в течение которого были зарегистрированы IP-пакеты.
  - Чтобы ограничить число записей, выберите **Отображать не более** и укажите число записей. Если флажок не установлен, будет отображено не более 100 записей.

Нажмите **Найти**. В результате отобразится список записей об IP-пакетах, отвечающих заданным критериям поиска.

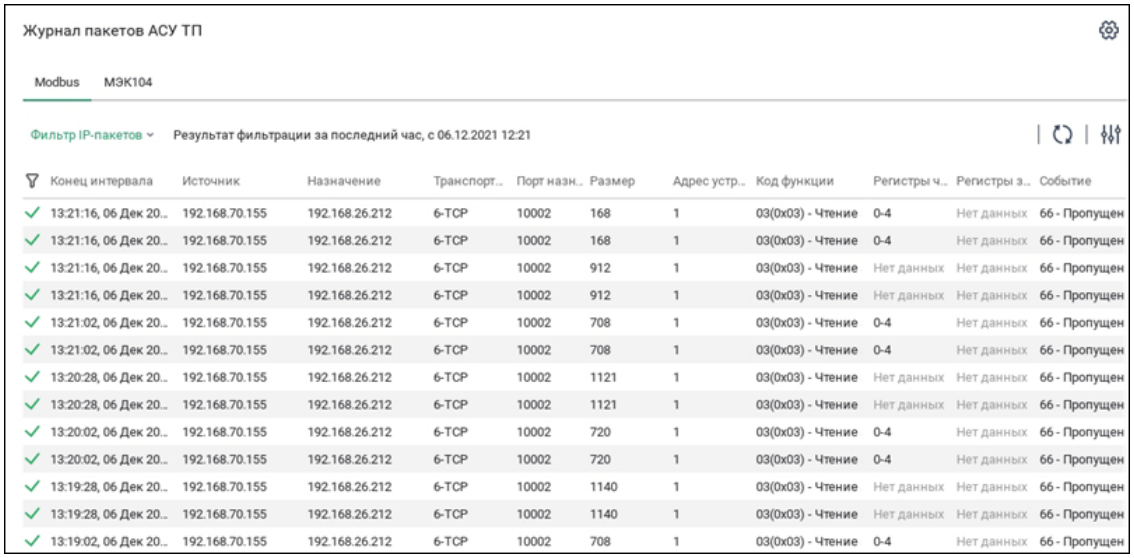


Рисунок 134. Просмотр результатов поиска в журнале пакетов промышленных протоколов

5 Выполните одно из действий со списком выбранных записей:

- Для просмотра подробной информации щелкните дважды запись в списке.
- Для обновления списка записей нажмите вверху справа.

Вы можете настроить параметры ведения журнала. Для этого вверху справа нажмите .

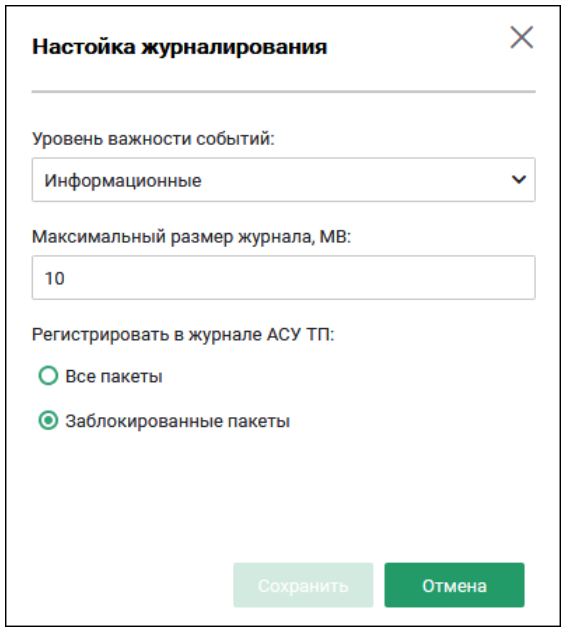


Рисунок 135. Настройка ведения журнала пакетов промышленных протоколов

По умолчанию в журнал записываются только заблокированные пакеты. Чтобы включить регистрацию пропущенных пакетов, выберите **Все пакеты** и нажмите **Сохранить**.

Журнал аудита

В журнале аудита регистрируются события, связанные с выполнением запросов пользователей, в том числе от ViPNet Prime и служебных запросов ViPNet Coordinator IG. Журнал ведётся локально и ротируется.

Чтобы просмотреть журнал аудита:

1 Выберите **Журналы** > **Журнал аудита**.

По умолчанию заданы параметры для просмотра всех записей. В строке записи о событии отображаются:

- дата и время события;
- инициатор:
  - имя учётной записи пользователя — запросы пользователей;
  - **System** — служебный запрос;
  - **System.Prime** — запрос ViPNet Prime;
- результат: **Успешно** или **Ошибка;**
- описание события.

2 Чтобы настроить вид отображения записей, нажмите и выберите нужные флажки.

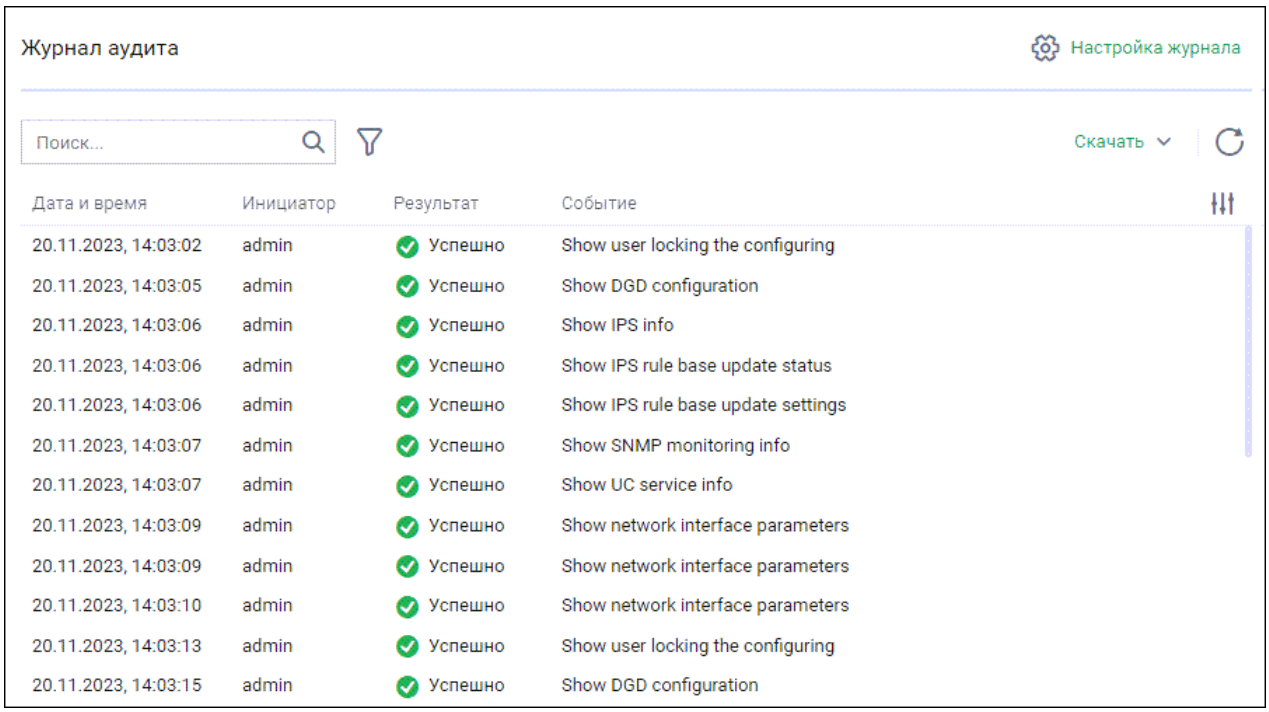


Рисунок 136. Просмотр журнала аудита

3 Для поиска записей в журнале вы можете использовать:

3.1 Поиск по тексту: начните вводить текст в поле **Поиск**.

3.2 Поиск по параметрам:

3.2.1 нажмите ;

3.2.2 выберите из списков **Результат**, **Инициатор** и **Период регистрации** параметры поиска;

3.2.3 нажмите **Применить**.

4 Чтобы скачать файл журнала, содержащий все записи, выберите **Скачать** > **Скачать весь журнал**.

Файл журнала в формате `<имя узла>-audit-logs_DD-MM-YYYYTHH_MM.tar.gz` будет сохранён в папке вашего компьютера.

5 Чтобы скачать файл журнала, содержащий записи, найденные на шаге 3, выберите **Скачать** > **Скачать отфильтрованный журнал**.

Файл журнала будет сохранён в папке вашего компьютера.

Журнал СКЗИ

В журнале СКЗИ регистрируются события, связанные с выполнением криптографических запросов. Журнал ведётся локально и не ротируется.

Чтобы просмотреть журнал СКЗИ:

1 Выберите **Журналы** > **Журнал СКЗИ**.

По умолчанию заданы параметры для просмотра всех записей. В строке записи о событии отображаются:

- дата и время события;
- инициатор:
  - **User, Admin**, учетные записи централизованных пользователей — запросы пользователей;
  - **System** — служебный запрос;
  - **System.Prime** — запрос ViPNet Prime;
- результат: **Успешно** или **Ошибка;**
- описание события.

2 Чтобы настроить вид отображения записей, нажмите и выберите нужные флажки.

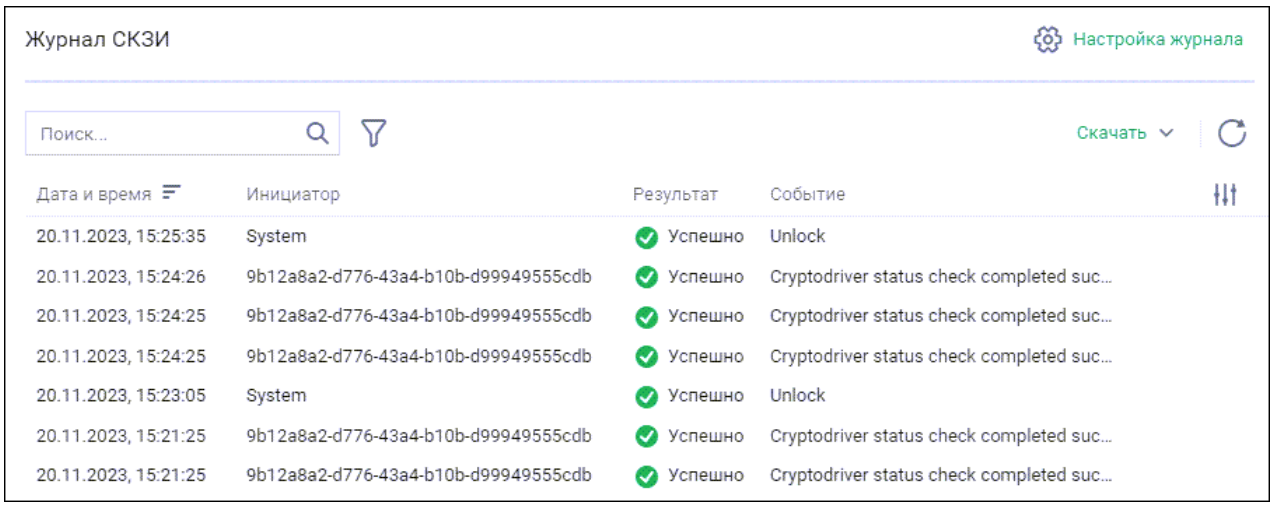


Рисунок 137. Просмотр журнала СКЗИ

3 Для поиска записей в журнале вы можете использовать:

3.1 Поиск по тексту: начните вводить текст в поле **Поиск**.

3.2 Поиск по параметрам:

3.2.1 нажмите ;

3.2.2 выберите из списков **Результат**, **Инициатор** и **Период регистрации** параметры поиска;

3.2.3 нажмите **Применить**.

4 Чтобы скачать файл журнала, содержащий все записи, выберите **Скачать** > **Скачать весь журнал**.

Файл журнала в формате `<имя узла>-crypto-logs_DD-MM-YYYYTHH_MM.tar.gz` будет сохранён в папке вашего компьютера.

5 Чтобы скачать файл журнала, содержащий записи, найденные на шаге 3, выберите **Скачать** > **Скачать отфильтрованный журнал**.

Файл журнала будет сохранён в папке вашего компьютера.

6 Чтобы скачать файл журнала, содержащий все записи, и очистить журнал на ViPNet Coordinator IG, выберите **Скачать** > **Скачать с очисткой журнала**.

Файл журнала будет сохранён в папке загрузки вашего компьютера, а все записи журнала на ViPNet Coordinator IG будут удалены.

Журнал MFTP

Транспортный сервер MFTP работает в транзитном режиме, обеспечивая передачу транспортных конвертов MFTP между узлами сети ViPNet, поддерживающими работу с дистрибутивом ключей `dst`.

Чтобы просмотреть журнал MFTP:

1 Выберите **Журналы** > **Журнал MFTP**.

Отобразятся записи обо всех транспортных конвертах за последние три часа.

2 Чтобы настроить вид отображения записей, нажмите и выберите нужные флажки.

3 Чтобы выбрать записи из журнала для просмотра, раскройте список **Фильтр конвертов** и укажите критерии поиска:

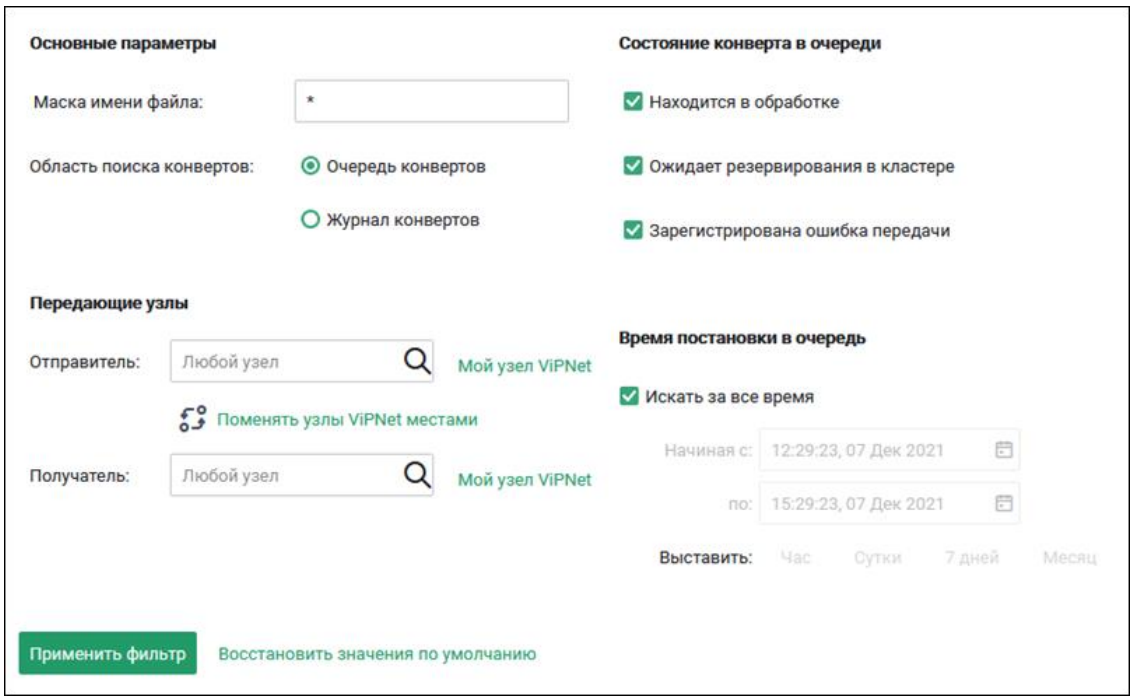


Рисунок 138. Настройка параметров журнала транспортных конвертов

- 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 IG 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.
- В разделе **Время изменения статуса** укажите интервал времени, за который вы хотите просмотреть информацию о транспортных конвертах.

4 Нажмите **Применить фильтр**.

Журнал DNS-запросов

В журнале DNS-запросов регистрируются события, связанные с обработкой запросов локальным DNS-сервером ViPNet Coordinator IG:

- дата и время запроса;
- IP-адрес, с которого поступил запрос;
- запрошенное доменное имя;
- тип запрошенной DNS-записи:
  - A — адрес в формате IPv4;
  - AAAA — адрес в формате IPv6;
  - CNAME — каноническое имя;
  - DNAME — псевдоним доменного имени;
  - DS — отпечаток ключа подписи DNSSEC;
  - HINFO — информация об узле;
  - ISDN — адрес в формате ISDN;
  - KEY — открытый ключ DNSSEC;
  - LOC — географическое месторасположение домена.

Журнал ведётся локально и ротируется.

Чтобы просмотреть журнал DNS-запросов:

1 Выберите **Журналы** > **Журнал DNS-запросов**.

По умолчанию отображаются события за последний час:

- дата и время события;
- IP-адрес источника;
- доменное имя;
- тип записи.

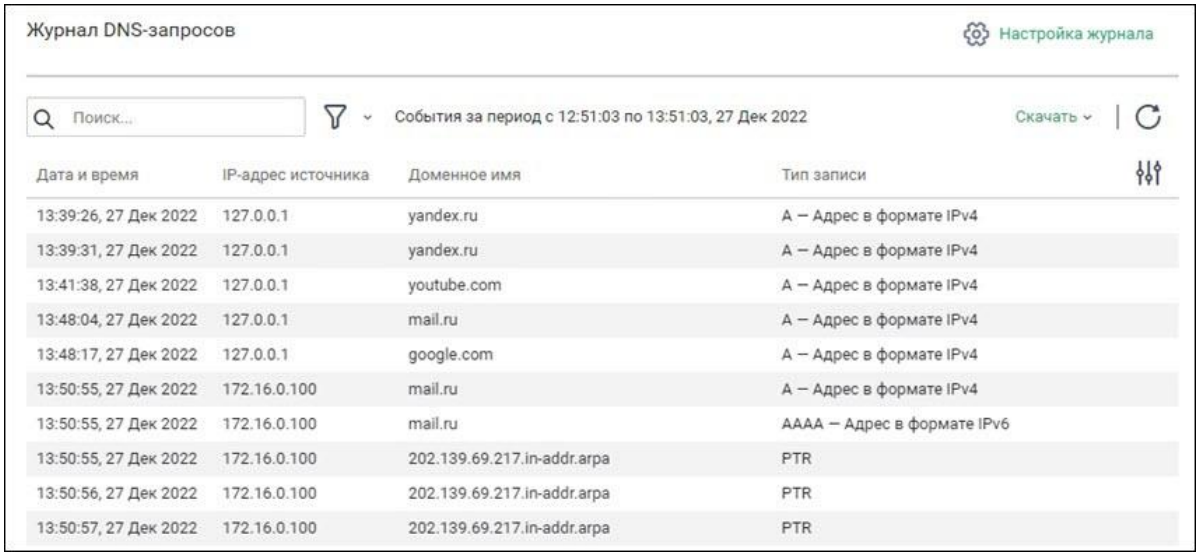


Рисунок 139. Просмотр журнала DNS-запросов

2 Чтобы настроить вид отображения записей, нажмите и выберите нужные флажки.

3 Для поиска записей в журнале вы можете использовать:

3.1 Поиск по тексту: начните вводить текст в поле **Поиск**.

3.2 Поиск по параметрам:

3.2.1 нажмите ;

3.2.2 задайте параметры поиска: **IP-адрес источника**, **Тип записи** и **Период регистрации**;

3.2.3 нажмите **Применить**.

4 Чтобы скачать файл журнала, содержащий все записи, выберите **Скачать** > **Скачать весь журнал**.

Файл журнала в формате `namedlog_tmp.csv` будет сохранён в папке вашего компьютера.

5 Чтобы скачать файл журнала, содержащий записи, найденные на шаге 3, выберите **Скачать** > **Скачать отфильтрованный журнал**.

Файл журнала будет сохранён в папке вашего компьютера.

Системный журнал

Системный журнал ведётся локально или удалённо, файлы журнала ротируются.

Чтобы просмотреть системный журнал при локальном хранении:

1 Выберите **Журналы** > **Системный журнал**.

По умолчанию заданы параметры для просмотра записей всех служб.

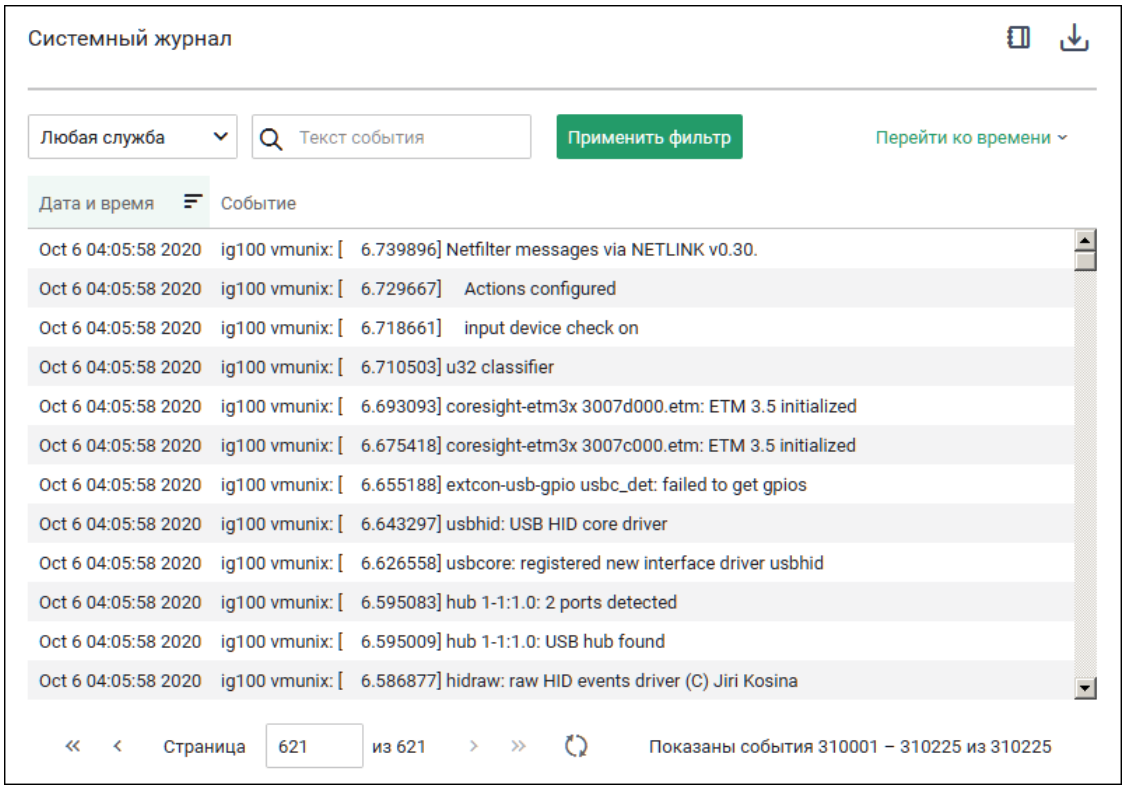


Рисунок 140. Просмотр записей в системном журнале

2 Для поиска записей в журнале используйте фильтры:

- Для поиска событий, регистрируемых определённой службой, выберите её и при введите текст события, затем нажмите **Применить фильтр**.
- Чтобы просмотреть записи журнала с указанного момента времени, нажмите **Перейти ко времени**, выберите дату и время в календаре, затем нажмите **Перейти**.

3 Чтобы скачать zip-архив, содержащий системный журнал:

3.1 Нажмите .

3.2 Выберите степень сжатия архива.

3.3 По умолчанию, в архив добавляются ротированные файлы журнала. Если добавлять файлы не нужно, снимите флажок **Включить в архив ротированные файлы журнала**.

3.4 Нажмите **Скачать**.

Файл архива журнала в формате `<имя узла>-logs_DD-MM-YYYYTHH_MM.zip` будет сохранён в папке вашего компьютера.



Примечание. Итоговый размер архива может отличаться от значения, указанного до скачивания.

Примеры событий системного журнала см. в приложении События системного журнала и журнала аудита.

13

Мониторинг состояния и просмотр статистики

Просмотр состояния 228

Мониторинг по SNMP 230

Просмотр статистики передачи данных 242

Просмотр статистики IP-пакетов 243

Просмотр состояния

Чтобы просмотреть информацию о состоянии ViPNet Coordinator IG, выберите **Состояние системы**.

Страница содержит разделы:

- **Здоровье —** информация о состоянии процессора, модема и дисковой памяти. Раздел доступен для исполнений ViPNet Coordinator IG100. Время отображается с учётом заданного для ViPNet Coordinator IG часового пояса.
- **Информация о памяти** — объём доступной дисковой памяти. Чтобы просмотреть подробную информацию о дисковой памяти, нажмите .
- **Шлюзы** — информация о настроенных шлюзах Modbus (доступно для исполнений ViPNet Coordinator IG100).
- **Службы** — состояние служб ViPNet Coordinator IG.
- **Загрузка процессора** — график загрузки процессора.
- **Использование памяти** — график потребления оперативной памяти.

Примечание. Если служба системы защиты от сбоев остановлена, информация не отображается.
В кластере информация отображается только для активного узла.

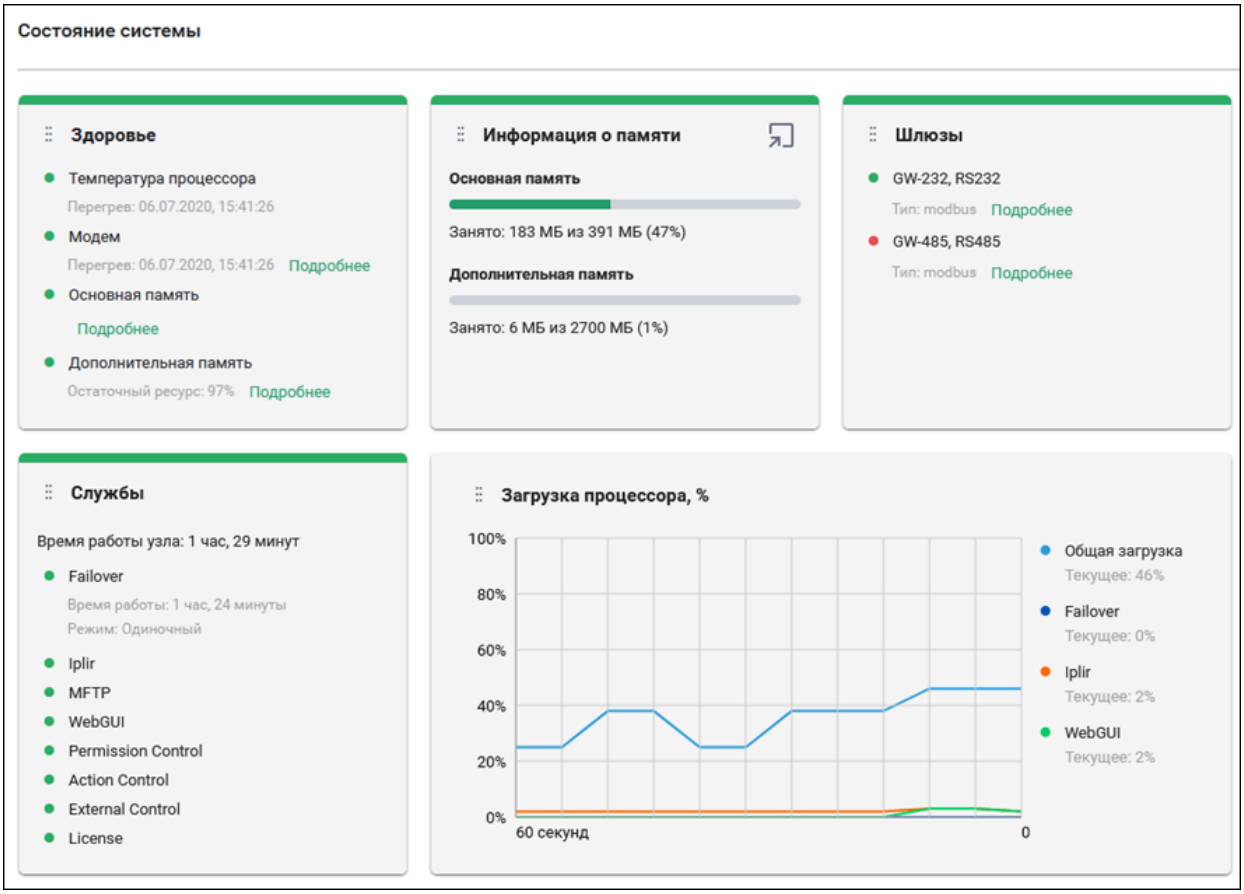


Рисунок 141. Просмотр состояния ViPNet Coordinator IG

Мониторинг по SNMP

С помощью SNMP-агента, входящего в состав ПО ViPNet Coordinator IG, вы можете удалённо получать информацию о работе ViPNet Coordinator IG, а также настраивать автоматическое уведомление 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 IG 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 IG вы можете использовать любую программу, предназначенную для получения информации по протоколу SNMP (SNMP-менеджер), например:

- ViPNet Prime (модуль Network Visibility System).
- Утилита snmpwalk (пакет net-snmp).
- 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 IG на UDP-порт 161;
- с ViPNet Coordinator IG 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 IG и получает в ответ значения необходимых параметров.
- Передача уведомлений — SNMP-агент ViPNet Coordinator IG автоматически отправляет SNMP-уведомления на сервер мониторинга при наступлении определённого события.

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

Если вы включили передачу SNMP-уведомлений, то после включения или перезагрузки ViPNet Coordinator IG доставка первых уведомлений о старте служб `iplircfg`, `mftpd`, `webgui` и `failoverd` на сервер мониторинга не гарантирована. Причина — отсутствие связи с сервером мониторинга во время инициализации сетевой подсистемы.

Если вы импортируете в сервер мониторинга MIB-файлы, поддерживаемые ViPNet Coordinator IG, 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 уведомления от ViPNet Coordinator IG 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 IG 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. ViPNet Coordinator IG ответит на SNMP-запрос, если community в запросе совпадает с любым из community, заданных на ViPNet Coordinator IG.

  Для получения SNMP-уведомлений сервером мониторинга в настройках его SNMP-менеджера, а также в настройках ViPNet Coordinator IG, необходимо задать community для уведомлений.
- В SNMPv3 создаются учётные записи пользователей SNMP. ViPNet Coordinator IG ответит на SNMP-запрос, если данные пользователя в запросе совпадают с данными любого из пользователей, заданных на ViPNet Coordinator IG:
  - имя пользователя;
  - пароль пользователя и алгоритм хэширования пароля;
  - ключ и алгоритм шифрования (если заданы).

  Для получения SNMP-уведомлений сервером мониторинга в настройках его SNMP-менеджера укажите данные одного из пользователей SNMP, заданных на ViPNet Coordinator IG. При использовании уведомлений типа TRAP в настройках SNMP-менеджера дополнительно к учётным 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 IG:

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

  На странице отображаются текущие настройки SNMP-агента.

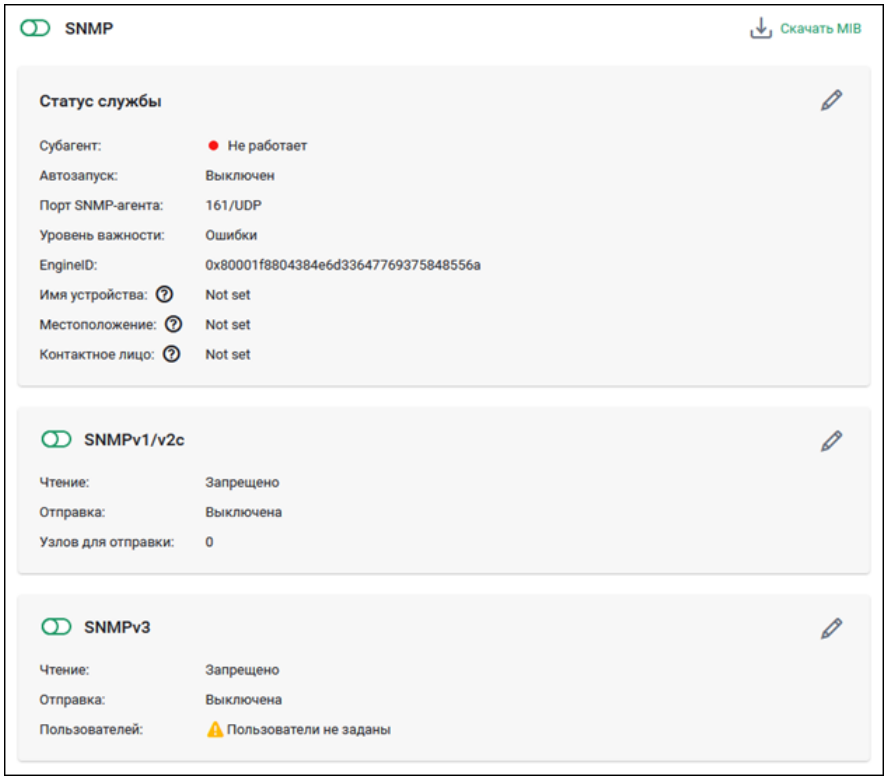


Рисунок 142. Настройка мониторинга по протоколу SNMP

2 Чтобы настроить основные параметры SNMP-агента, нажмите  в разделе **Статус службы**.

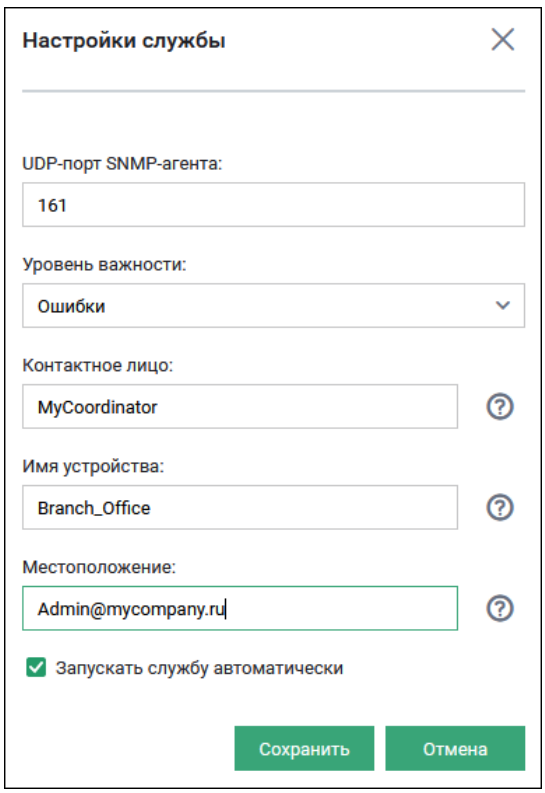


Рисунок 143. Настройка службы SNMP

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

2.2 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.

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

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

Примечание. Параметры **Имя устройства** и **Местоположение** не синхронизируются между узлами кластера. Если кластер уже развёрнут, чтобы изменить их на пассивном узле, подключитесь к нему с помощью консоли и выполните необходимые команды (подробнее см. в документе «Настройка с помощью командного интерпретатора», в разделе «Настройка SNMP-агента»).

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

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

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

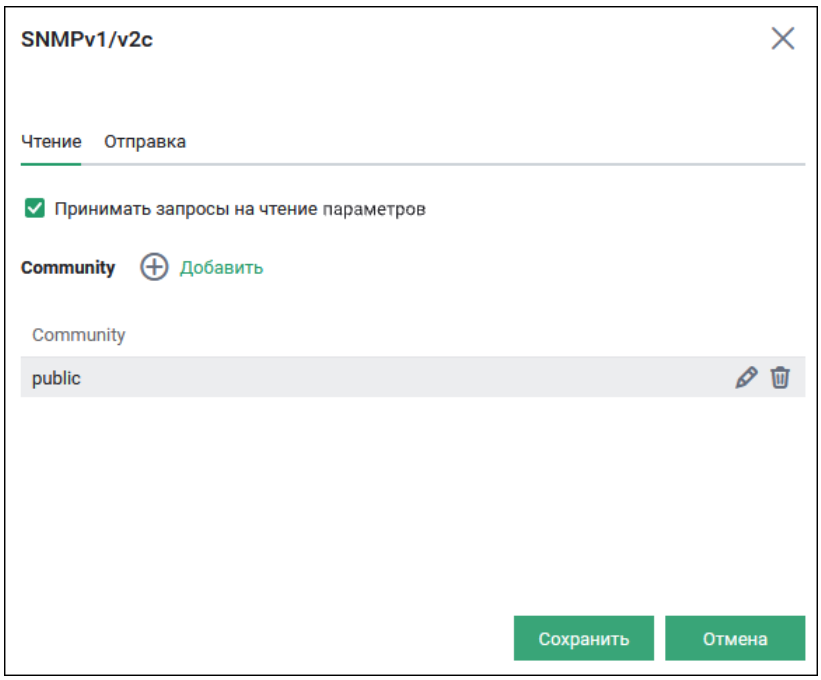


Рисунок 144. Настройка чтения SNMP-параметров

3.2 Чтобы разрешить чтение SNMP-параметров, выберите **Принимать запросы на чтение параметров**.

3.3 Выполните одно из действий:

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

  Максимальное количество community для чтения — 16.
- Чтобы изменить community, наведите на него курсор и нажмите .
- Чтобы удалить community, наведите на него курсор и нажмите .

3.4 Выберите вкладку **Отправка** для настройки отправки SNMP-уведомлений.

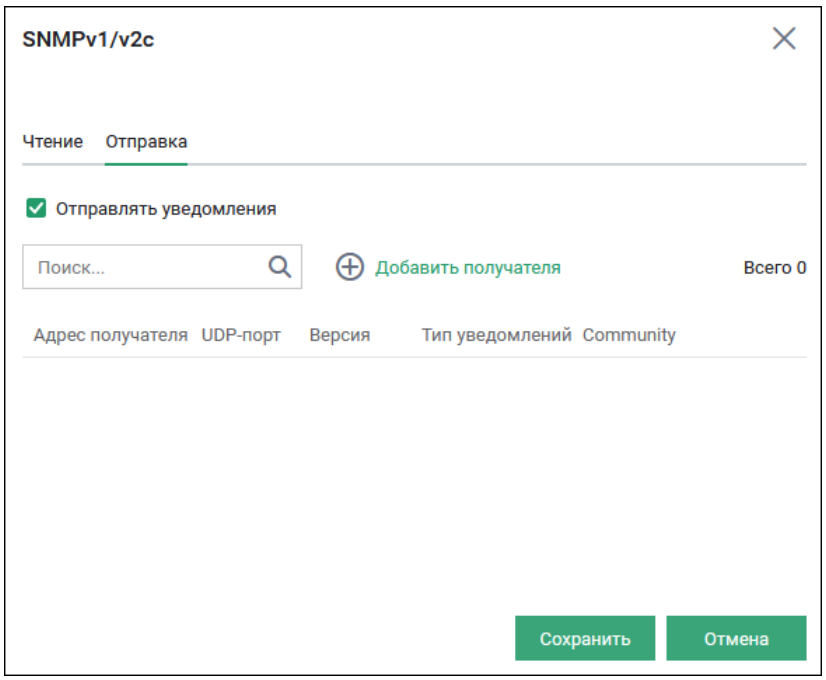


Рисунок 145. Настройка отправки SNMP-уведомлений

3.5 Чтобы включить отправку SNMP-уведомлений, выберите **Отправлять уведомления**.

3.6 Чтобы добавить сетевой узел для отправки SNMP-уведомлений, нажмите ⊕ **Добавить получателя**. Максимальное количество сетевых узлов — 16.

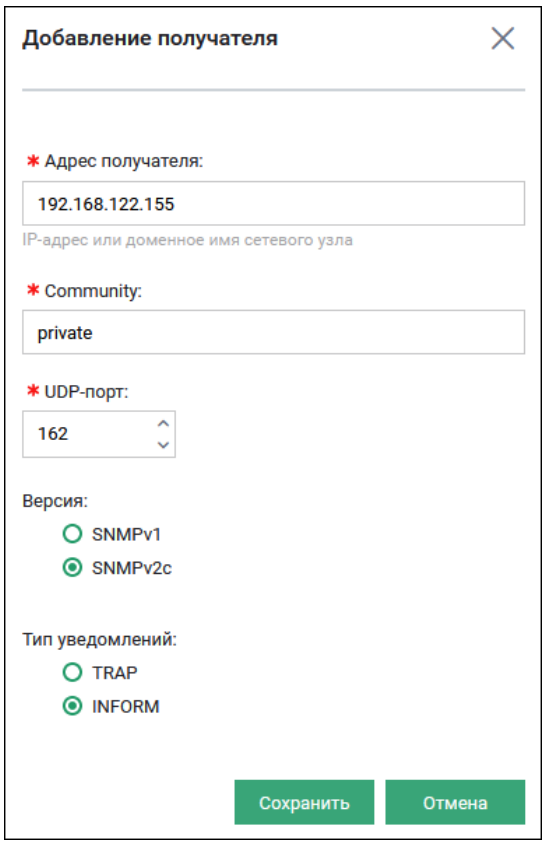


Рисунок 146. Добавление узла для отправки уведомлений в SNMP v1 и v2c

3.7 Задайте параметры:

- Адрес сервера мониторинга в поле **Адрес получателя**.
- Community, которое задано на сервере мониторинга (trap community).
- Порт, на который будут отправляться SNMP-уведомления (по умолчанию UDP 162).

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

- Версию протокола SNMP, по которому будут отправляться SNMP-уведомления.
- Тип SNMP-уведомлений.

3.8 Включите **SNMP v1/v2c**.

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

4.1 Чтобы разрешить чтение SNMP-параметров, выберите **Принимать запросы на чтение параметров** на вкладке **Разрешения**.

4.2 Чтобы включить отправку SNMP-уведомлений, выберите **Отправлять уведомления**.

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

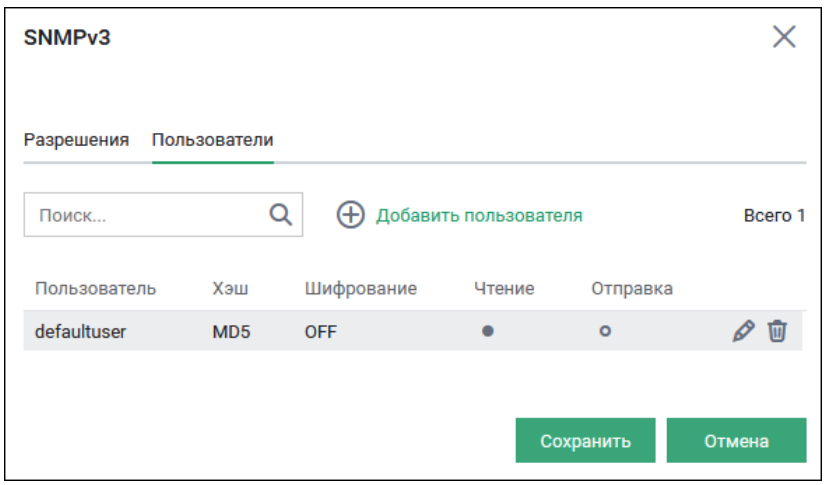


Рисунок 147. Настройка протокола SNMPv3

- Чтобы добавить пользователя для чтения SNMP-параметров ViPNet Coordinator IG, 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 .

4.4 В окне **Добавление пользователя** задайте параметры:

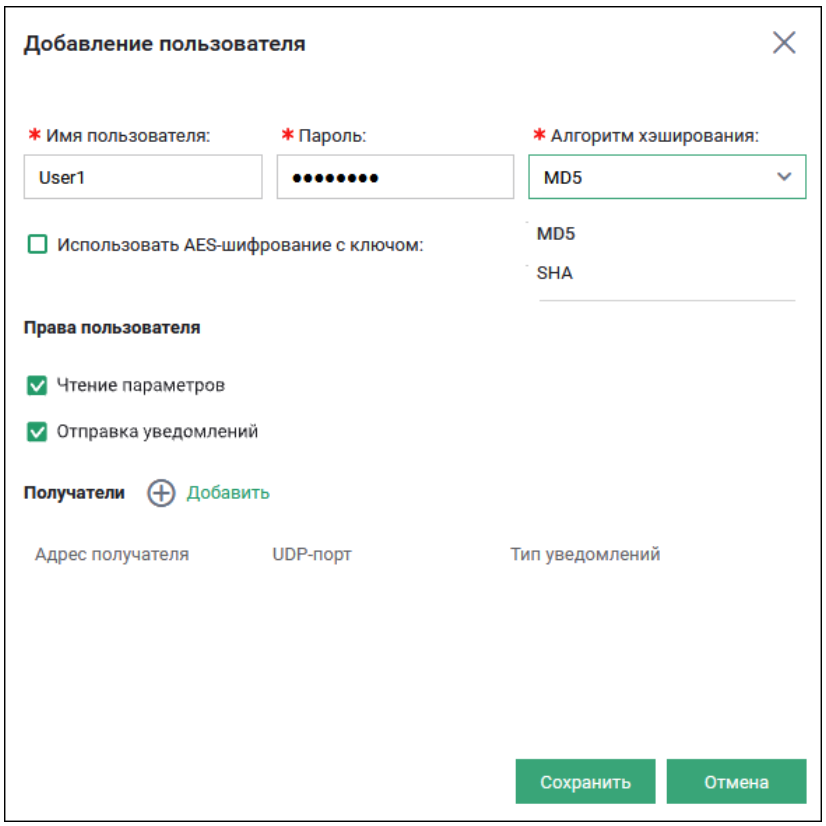


Рисунок 148. Добавление пользователя для чтения SNMP-параметров

- 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 шифровать трафик между сервером мониторинга и ViPNet Coordinator IG, выберите **Использовать AES-шифрование с ключом** 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.

> **Примечание.** Если задан ключ шифрования, его необходимо указывать в SNMP-запросах наряду с другими данными пользователя SNMP.

- Чтобы разрешить чтение SNMP-параметров для пользователя, выберите **Чтение параметров.**
- Чтобы разрешить отправку SNMP-уведомлений для пользователя, выберите **Отправка уведомлений**.

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

4.5 В окне **Добавление получателя** задайте параметры:

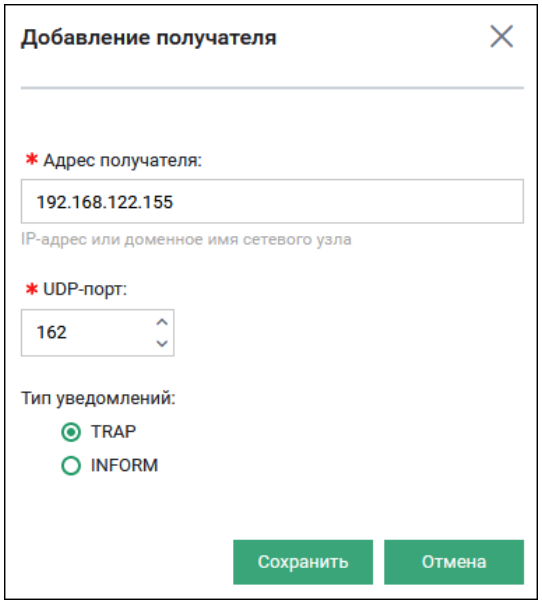


Рисунок 149. Добавление узла для отправки уведомлений в SNMP3

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

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

- Тип уведомлений.

4.6 Включите **SNMP v3**.

5 Включите **SNMP**.

Чтобы скачать MIB-файлы, поддерживаемые ViPNet Coordinator IG, 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-уведомления. 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 IG кластера создается community для режима кластера. SNMP-запрос с таким community будет адресован конкретному ViPNet Coordinator IG независимо от его текущего режима работы в кластере (активный или пассивный). При переключении системы защиты от сбоев в одиночный режим, community для режима кластера автоматически удаляется.
- При использовании SNMPv3 каждому узлу кластера назначается свой контекст (строка, идентифицирующая ViPNet Coordinator IG 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.

Настройки будут переданы на пассивный узел при последующей синхронизации.

Примечание. Если на момент развёртывания кластера SNMP-агент уже настроен на одном из ViPNet Coordinator IG, запускайте `failover` в режиме кластера сначала на ViPNet Coordinator IG 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 Выключите , а затем включите SNMP.

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

3.1 Выберите вкладку **Мониторинг узлов кластера**.

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

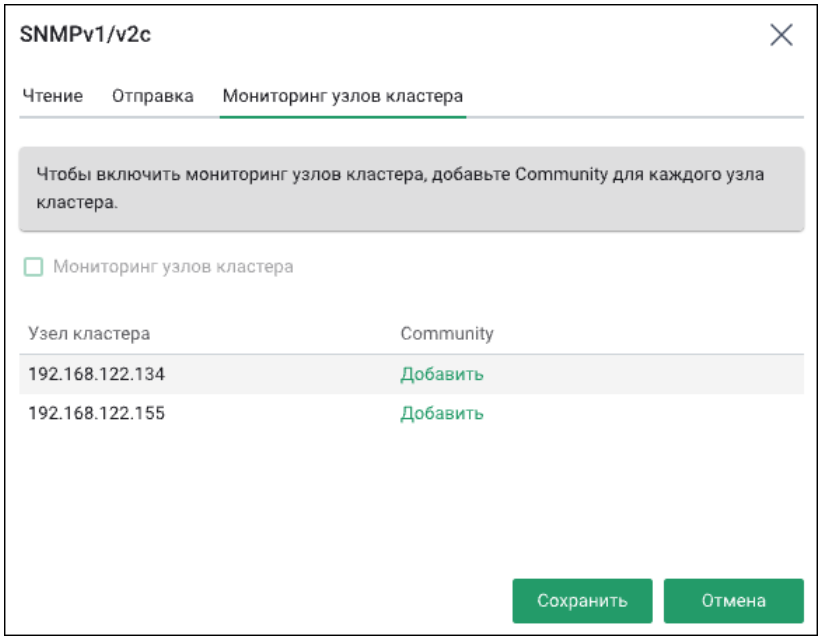


Рисунок 150. Настройка чтения SNMP-параметров в кластере

3.3 Введите community, отличное от других.

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

3.4 Чтобы разрешить чтение SNMP-параметров узлов кластера, выберите **Мониторинг узлов кластера**.

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

4.1 Выберите вкладку **Контексты кластера**.

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

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

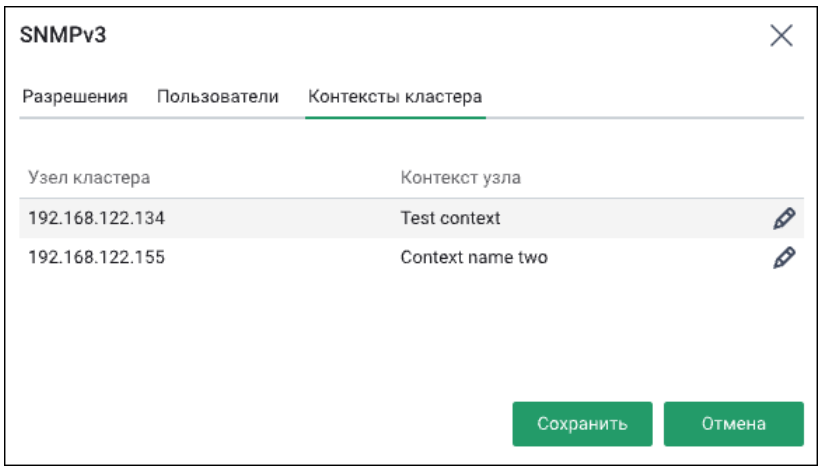


Рисунок 151. Просмотр контекстов для узлов кластера

5 В зависимости от версии протокола SNMP используйте созданные community 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 соответствующего узла кластера.
- При использовании протокола SNMPv3 отправляйте SNMP-запрос с учётными 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.

Просмотр статистики передачи данных

Статистика передачи данных ведётся раздельно по всем интерфейсам с момента включения ViPNet Coordinator IG. Статистика учитывает текущую скорость интерфейсов и объём трафика. Данные статистики отображаются в виде графика скорости и диаграммы объёма трафика с заданным интервалом обновления (по умолчанию — 3 секунды). Значения скорости отображаются в диапазоне 600 секунд от начала просмотра статистики. После перезагрузки ViPNet Coordinator IG или удаления интерфейса данные статистики сбрасываются.

При работе ViPNet Coordinator IG в режиме кластера отображается статистика интерфейсов активного узла.

Чтобы просмотреть статистику передачи данных:

1 Выберите **Статистика**.

По умолчанию в разделе **Передача данных** отображается статистика интерфейса `eth0`.

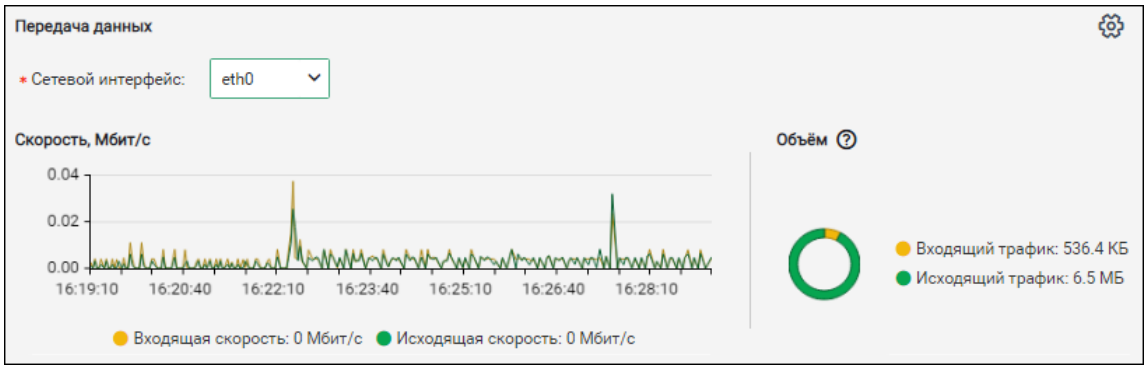


Рисунок 152. Статистика передачи данных сетевого интерфейса eth0

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 статистики IP-пакетов

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

1 Выберите **Статистика**. Отобразится информация о количестве открытых, зашифрованных, широковещательных открытых и широковещательных зашифрованных IP-пакетов, прошедших через все сетевые интерфейсы узла.

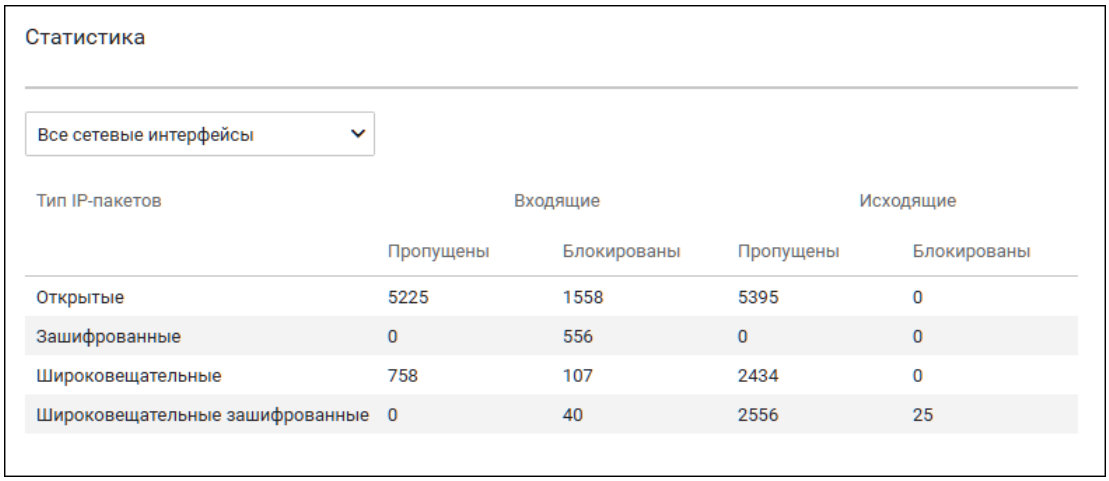


Рисунок 153. Просмотр информации о количестве IP-пакетов, прошедших через все сетевые интерфейсы ViPNet Coordinator IG

2 Чтобы просмотреть информацию о количестве IP-пакетов, прошедших через определённый сетевой интерфейс ViPNet Coordinator IG, выберите этот интерфейс в списке.

A

Сетевые фильтры по умолчанию

Для межсетевого экрана типа «А/Б» и типа «Д» при работе в штатном режиме и режиме регламентного обслуживания

Таблица 11. Фильтры защищённой сети (vpn)

Название	Источник	Назначение	Протокол	Действие
Фильтры, добавляемые в режиме кластера (нередактируемые)				
ViPNet Service in	@any	@local	udp: from 2060 to 2060	pass
ViPNet Service out	@local	@any	udp: from 2060 to 2060	pass
Служебные фильтры (нередактируемые)				
Block not original udp port	@local	@any	udp: from 0–2045 to 2046, from 2047–65535 to 2046	drop
Allow ViPNet base services out	@local	• @any — при наличии лицензии VPN; • @AllCoordinators — при отсутствии лицензии VPN	udp: to 2046, from 2048 to 2048, from 2050 to 2050 tcp: to 2046	pass

Название	Источник	Назначение	Протокол	Действие
Allow ViPNet base services in	@any — при наличии лицензии VPN; @AllCoordinators — при отсутствии лицензии VPN	@local	udp: to 2046, from 2048 to 2048, from 2050 to 2050 tcp: to 2046	pass
Allow ViPNet MFTP in	@any	@local	tcp: to 5000–5003	pass
Allow ViPNet MFTP out	@local	@any	tcp: to 5000–5003	pass
Allow ViPNet Control services out	@local	<идентификатор ViPNet Prime>	@any	pass
Allow ViPNet Control services in	<идентификатор ViPNet Prime>	@local	@any	pass
Настраиваемые фильтры				
ICMP redirect in	@any	@local	icmp: 5	drop
ICMP redirect out	@local	@any	icmp: 5	drop
Allow ICMP Ping in	@any	@local	icmp: 8	pass
Allow ICMP Ping out	@local	@any	icmp: 8	pass
Allow ViPNet DBViewer in	@any	@local	tcp: to 2047	pass
Allow ViPNet DBViewer out	@local	@any	tcp: to 2047	pass
Allow ViPNet IpfView in	@any	@local	tcp: to 20001	pass
Allow ViPNet IpfView out	@local	@any	tcp: to 20001	pass
Allow DNS client	@local	@any	udp: to 53, tcp: to 53	pass
Allow DNS server	@any	@local	udp: to 53, tcp: to 53	pass
Allow NTP client	@local	@any	udp: to 123	pass
Allow NTP server	@any	@local	udp: to 123	pass
Allow DHCP client req	@local	@any	udp: from 68 to 67	pass
Allow DHCP client resp	@any	@local	udp: from 67 to 68	pass
Allow DHCP server req	@local	@any	udp: from 67 to 68	pass
Allow DHCP server resp	@any	@local	udp: from 68 to 67	pass

Название	Источник	Назначение	Протокол	Действие
Allow DHCP-Relay service in	@any	@local	udp: from 67 to 67	pass
Allow DHCP-Relay service out	@local	@any	udp: from 67 to 67	pass
Allow SSH client	@local	@any	tcp: to 22	pass
Allow syslog outgoing	@local	@any	udp: to 514	pass
Allow cef outgoing	@local	@any	udp: to 5001	pass
Allow SNMP	@any	@local	udp: to 161	pass
Allow SNMP traps	@local	@any	udp: to 162	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 12. Фильтры туннелируемых узлов (`tunnel`)

Название	Источник	Назначение	Протокол	Действие
Настраиваемые фильтры				
To all tunnel nodes	@any	@tunneledip	@any	pass
From all tunnel nodes	@tunneledip	@any	@any	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 13. Локальные фильтры открытой сети (`local`)

Название	Источник	Назначение	Протокол	Действие
Фильтры, добавляемые в режиме кластера (нередактируемые)				
Failover test IP	@local	<список значений параметров `testip` из `failover.ini`>	icmp	pass
Failover Channel in	@remote	interface <имя интерфейса синхронизации>	@any	pass
Failover Channel out	interface <имя интерфейса синхронизации>	@remote	@any	pass
Служебные фильтры (нередактируемые)				

Название	Источник	Назначение	Протокол	Действие
ViPNet Service Common In	@any	@local	tcp/udp: to 2046, to 2047, to 10096, to 5100, to 10092	drop
ViPNet Service Common Out	@local	@any	tcp/udp: from 2046	drop
Настраиваемые фильтры				
ICMP redirect out	@local	@any	icmp: 5	drop
ICMP redirect in	@any	@local	icmp: 5	drop
Block ICMP timestamp response	@local	@any	icmp: 14	drop
Allow ICMP Ping	@local	@any	icmp: 8	pass
Allow DNS	@local	@any	udp: to 53, tcp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Allow DHCP server req	@local	@any	udp: from 67 to 68	pass
Allow DHCP server resp	@any	@local	udp: from 68 to 67	pass
Allow DHCP-Relay service out	@local	@any	udp: from 67 to 67	pass
Allow DHCP-Relay service in	@any	@local	udp: from 67 to 67	pass
Allow ICMP blackhole response	@local	@any	icmp: 3/4	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 14. Транзитные фильтры открытой сети (`forward`)

Название	Источник	Назначение	Протокол	Действие
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Для межсетевого экрана типа «Д» при работе в специальном режиме

Таблица 15. Фильтры защищённой сети (`vpn`), фильтры туннелируемых узлов (tunnel), локальные фильтры открытой сети (`local`) и транзитные фильтры открытой сети (`forward`)

Название	**Источник**	**Назначение**	**Протокол**	**Действие**
Настраиваемые фильтры				
Allow all	@any	@any	@any	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

B

Пользовательские группы протоколов по умолчанию

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

Таблица 16. Пользовательские группы протоколов, настроенные по умолчанию

Имя группы протоколов	Состав группы протоколов
ABB-ESCP	TCP: to 6316, UDP: to 6316
ANSI-C12	TCP: to 1153, UDP: to 1153
BACNET	TCP: to 47808, UDP: to 47808
CITRIX	TCP: to 1494
Cluster	UDP: from 2060 to 2060
ClusterMonitoring	UDP: from 2060 to 2065, UDP: from 2065 to 2060
DNP3	TCP: to 20000, UDP: to 20000
DNS	UDP: to 53
DHCP	UDP: from 67-68 to 67-68
EHS	TCP: to 4535, UDP: to 4535
EHS-SSL	TCP: to 4536, UDP: to 4536
EIBnet	TCP: to 3671, UDP: to 3671
EtherCAT	TCP: to 34980, UDP: to 34980
EtherNET-IPoverTLS	TCP: to 2221

Имя группы протоколов	Состав группы протоколов
EtherNET-IPoverDTLS	UDP: to 2221
EtherNET-IP_I_O	TCP: to 2222, TCP: to 44818, UDP: to 44818
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
IEC-60870-5-104	TCP: to 2404, UDP: to 2404
IEC-60870-5-104-secure	TCP: to 19998
IEC61850	TCP: to 29999
IEEE-MMS	TCP: to 651, UDP: to 651
IEEE-MMS-SSL	TCP: to 695, UDP: to 695
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
LonWorks	TCP: to 2540, TCP: to 2541, UDP: to 2540, UDP: to 2541
LotusNotes	TCP: to 1352
MFTP	TCP: to 5000-5003
ModbusTcp	TCP: to 502, UDP: to 502
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
OSPF	IP: 89

Имя группы протоколов	Состав группы протоколов
OPC_UA	TCP: to 4840, UDP: to 4840
OPC_UA_TLS-SSL	TCP: to 4843, UDP: to 4843
PING	ICMP: 8
POP3	TCP: to 110
Postgres	TCP: to 5432
PPTP	TCP: to 1723
Profinet	TCP: to 34962, TCP: to 34963, TCP: to 34964, UDP: to 34962, UDP: to 34963, UDP: to 34964
PTPEven	TCP: to 319, UDP: to 319
PTPGeneral	TCP: to 320, UDP: to 320
Radius	TCP: to 1812, TCP: to 1813, UDP: to 1812, UDP: to 1813
RadiusDA	TCP: to 3799
Radsec	TCP: to 2083, UDP: to 2083
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
SNTP-HEARTBEAT	TCP: to 580, UDP: to 580
SSH	TCP: to 22
StateWatcher	TCP: to 2047, TCP: to 5100, TCP: to 10092
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
ViPNetBase	UDP: to 2046, UDP: from 2048 to 2048, UDP: from 2050 to 2050
WindowsMobileDevices	TCP: to 990, TCP: to 999, TCP: to 5678, TCP: to 5721, TCP: to 26675
WindowsMobileDevices2	UDP: to 5679
VNC	TCP: to 5900

Имя группы протоколов	Состав группы протоколов
ZigBee	TCP: to 17754, UDP: to 17754
ZigBeeIP	TCP: to 17755, TCP: to 17756, UDP: to 17755, UDP: to 17756
Z-Wave	TCP: to 4123, UDP: to 4123
Z-Wave-SSL-TLS	TCP: to 41230
Z-Wave-DTLS	UDP: to 41230
Z-Wave-Secure	TCP: to 44123

C

События журнала IP-пакетов

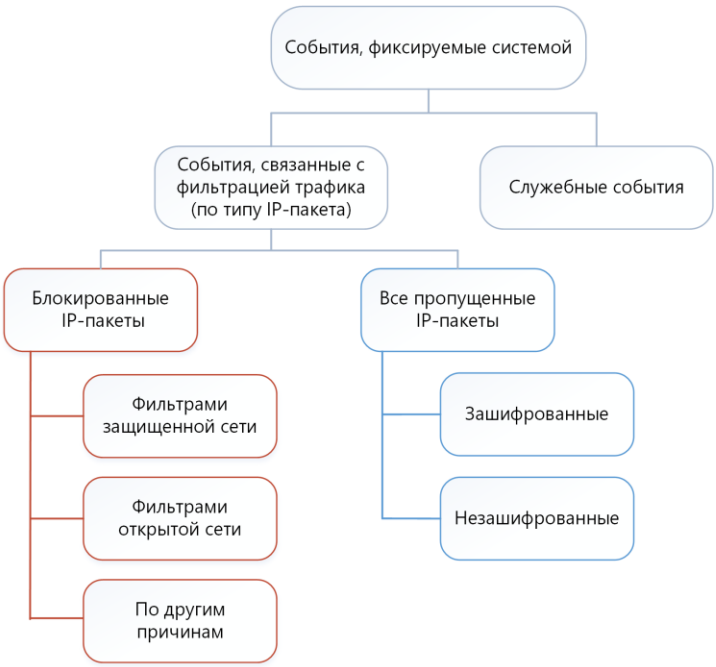


Рисунок 154. Классификация событий в журнале IP-пакетов

Таблица 17. События блокирования IP-пакетов фильтрами защищённой сети

Номер	Описание события
1	Не найден ключ для передачи пакета сетевому узлу с идентификатором, указанным в пакете
2	Неверное значение имитозащитной вставки пакета. Защищённые данные или открытая информация в пакете были изменены при передаче
3	Входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет заблокирован фильтром защищённой сети

Номер	Описание события
4	Слишком большой таймаут пакета, то есть время его отправки отличается от времени его получения на величину, большую указанной в соответствующей настройке
5	Входящий пакет отправлен сетевым узлом с версией драйвера ViPNet, не совместимой с версией драйвера ViPNet на сетевом узле получателя
7	Метод шифрования, код которого указан во входящем пакете, не поддерживается
8	IP-пакет повреждён
9	Неизвестный идентификатор сетевого узла
11	IP-пакет заблокирован фильтром защищённой сети с ICMP или TCP RST ответом
13	Превышено максимальное время пребывания пакета в сети
14	Неверный адрес получателя пакета
15	Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов
16	Исчерпана лицензия на количество туннелируемых узлов
17	Неверный IP-адрес получателя
18	Неизвестный IP-адрес получателя
19	Подмена узла отправителя
26	Узел с данного координатора недоступен
27	Входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет заблокирован фильтром защиты канала управления с генерацией REJECT сообщения ICMP
70	Транзитный IP-пакет заблокирован
71	Формат Iplir-пакета отличен от согласованного

Таблица 18. События блокирования IP-пакетов локальными фильтрами открытой сети

Номер	Описание события
20	Заблокирован открытый пакет
21	Идентификатор отправителя пакета неизвестен
22	От защищённого узла получен открытый пакет
23	От защищённого 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	Описание события
32	Широковещательный пакет заблокирован фильтром открытой сети
33	Пакет заблокирован фильтром антиспуфинга
34	Локальный IP-пакет заблокирован фильтром открытой сети с ICMP или TCP RST ответом
35	Транзитный IP-пакет заблокирован фильтром открытой сети с ICMP или TCP RST ответом
36	IP-пакет заблокирован фильтром для туннелируемых узлов с ICMP или TCP RST ответом
37	Пакет заблокирован фильтром туннелируемых ресурсов
39	Пакет заблокирован фильтром по умолчанию при загрузке компьютера

Таблица 19. События блокирования IP-пакетов по другим причинам

Номер	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 её 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
94	Недостаточно памяти
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
98	Недостаточно ресурсов для обработки IP-пакета

Номер	Описание события
99	Заблокирован фрагментированный IP-пакет
100	IP-пакет заблокирован в ходе инспекции состояния соединения
101	Транзитный IP-пакет не может быть маршрутизирован
103	Количество установленных соединений превышает допустимое значение, заданное в соответствующих настройках
104	Соединение заблокировано, так как параметры исходящих пакетов (socketpair) для этого соединения совпадают с такими параметрами для ранее установленного соединения
105	Не удалось выделить динамический порт для правила трансляции адресов (в пуле нет свободных портов)
111	Не найден ключ обмена
112	Неверное значение имитозащитной вставки в незашифрованном пакете версии 4.2
113	Неизвестный идентификатор сетевого узла отправителя
115	Не удалось найти маршрут для IP-пакета в таблице маршрутизации
116	Не найден сетевой адаптер
117	Не удалось определить MAC-адрес получателя пакета по его IP-адресу
118	Ошибка при шифровании исходящего IP-пакета для защищённого узла
119	Получен зашифрованный IP-пакет неизвестного формата, который не может быть расшифрован
120	Ошибка при отправке IP-пакета защищённому узлу из-за проблем с доступом к этому узлу
121	Ошибка в работе кластера
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)

Номер	Описание события
137	Шифрование исходящего IP-пакета с использованием данного алгоритма запрещено (тесты алгоритма не прошли)
138	Заблокирован IP-пакет на публичный DNS-сервер
139	Отсутствуют лицензии для туннелирования на узле назначения
147	Заблокирован IP-пакет с неизвестным протоколом

Таблица 20. События пропуска зашифрованных IP-пакетов

Номер	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 21. События пропуска незашифрованных IP-пакетов

Номер	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 ПО
65	Пропущен зашифрованный IP-пакет неизвестной ViPNet сети

Таблица 22. Служебные события

Номер	Описание события
42	Изменился IP-адрес сетевого узла
46	Изменились параметры доступа к сетевому узлу
47	Истёк 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

Номер	Описание события
50	IP-адрес перерегистрирован с другого узла на данный узел. Произведена перерегистрация адреса на данный узел. Если есть проблемы со связью, рекомендуется хотя бы для одного из конфликтных узлов, для которого это возможно, или для туннелируемых адресов узла с конфликтным адресом включить опцию «Использовать виртуальный адрес»
51	IP-адрес уже зарегистрирован на другом узле. Перерегистрация адреса на данный узел не произведена. Если есть проблемы со связью, рекомендуется хотя бы для одного из конфликтных узлов или для туннелируемых адресов узла с конфликтным адресом, для которого это возможно, включить опцию «Использовать виртуальный адрес»
110	Новый IP-адрес сетевого узла зарегистрирован на DNS-сервере
114	Пропущен зашифрованный IP-пакет для незарегистрированного узла ViPNet

D

События системного журнала и журнала аудита

Таблица 23. События, связанные с работой пользователя ViPNet Coordinator IG

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Перезагрузка по команде	`rvpn_shell[8548]: [02-01 09:46:09.213821]<8548>(00007f68d2725c40)[L3] | Command:'machine reboot'`	`Restart device SUCCESS`
Успешный запуск командного интерпретатора с помощью консоли	`login[23583]: pam_aauth(login:auth): granted access to user admin by LOGIN(uid=0)` `login[23583]: pam_aauth(login:session): session opened for user admin by LOGIN(uid=0)`	`User logon SUCCESS`

Выход из командного интерпретатора, работающего в режиме просмотра	`rvpn_shell[19591]: <EXIT> logout success`
	`...`
	`login[19247]: pam_aauth(login:session): session closed for user user`
		`Logoff SUCCESS`

Принудительное завершение сессии командного интерпретатора	`rvpn_shell[14381]: Session is forcefully terminated`	—

Событие	Пример записи в системном журнале	Пример записи в журнале аудита

Успешный удалённый запуск командного интерпретатора по протоколу SSH	`sshd[14734]: pam_aauth(sshd:auth): granted access to user user by (uid=0)`
	`sshd[14731]: Accepted keyboard-interactive/pam for user from 192.168.16.39 port 58168 ssh2`
	`sshd[14731]: pam_aauth(sshd:session): session opened for user user by (uid=0)`
	`...`
	`rvpn_shell[14742]: <LOGIN> Command: login - User logged in`
		`User logon SUCCESS`

Не удалось запустить командный интерпретатор при удалённом подключении по протоколу SSH	`aauth-tool[20299]: error: failed to login user user through AA: 8448` `sshd[20297]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.16.39 user=user`	`User logon FAILED`
Завершение удалённого подключения по протоколу SSH	`sshd[20626]: Received disconnect from 192.168.16.39 port 60808:11: disconnected by user` `sshd[20626]: Disconnected from 192.168.16.39 port 60808`	`Logoff SUCCESS`
Переход из режима настройки в режим просмотра	`rvpn_shell[10662]: <EXIT> Command 'exit'` `rvpn_shell[10662]: <EXIT> skip logout (admin mode)`	—
Изменение даты или времени	`rvpn_shell[13785]: <management> [ig100-2c670024] [local] [Single Mode] Set device date and time [success] [admin] Details: Command:'machine set date 2023-09-25 09:55:05 '`	`Set device date and time SUCCESS`
Переключение в режим регламентного обслуживания	`rvpn_shell[15197]: Mode switched successfully!` `rvpn_shell[15197]: service mode`	—
Успешное изменение файла `iplir.conf`	`rvpn_shell: <I_CFG> Command: iplir config - iplir.conf has been edited successfully.`	`SetIplirConfig SUCCESS`

Не удалось изменить файл `iplir.conf`	`rvpn_shell[26362]: error: Configuration checking failed`
	`rvpn_shell[26362]: Roll back the changes and restore the previous version of the file`
	или
	`rvpn_shell[26362]: error: Changing the settings is invalid when the process iplir is running. Please stop the process (iplir stop)`
		`SetIplirConfig FAILED`

Успешная смена пароля администратора	`rvpn_shell[26362]: The new password has been successfully set.`	`Set local administrator password SUCCESS`

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Не удалось сменить пароль администратора	rvpn_shell[29610]: error: Entered passwords do not match. rvpn_shell[29610]: <management> [ig100-2c670024] [local] [Single Mode] Set local administrator password [failed] [admin] Details: Command:'admin passwd '	Set local administrator password FAILED
Удаление справочников и ключей	rvpn_shell[31061]: <management> [ig100-2c670024] [local] [Single Mode] Delete host links and keys [success] [admin] Details: Command:'admin remove keys ' rvpn_shell[31061]: [02-01 13:54:06.144942]< 31061>(00007fd698e8dc40)[L3] | Command:'admin remove keys ' finished with rc=0 AAA__b141b9_7ae3c6_7a9cf8_60fafd rc=0 done	Delete host links and keys SUCCESS
Успешная установка справочников и ключей	keysetup[2242]: User password was correct and ds5-file VEM_ig10_vipnet_base_x86_64_5.1.0-4977.ds5 installed successfully	—
Локальное обновление ПО	rvpn_shell[8141]: /sbin/driv_upgrade.sh: process 8528 has been created	Update software locally using a USB drive SUCCESS
Задание IP-адреса для сетевого интерфейса	rvpn_shell[14053]: <management> [ig100-2c670024] [local] [Single Mode] Set network interface address [success] [admin] Details: Command:'inet ifconfig eth1 address 172.16.100.200 netmask 255.255.255.0 '	Set network interface address SUCCESS
Сброс настроек сетевого интерфейса	rvpn_shell[14053]: <management> [ig100-2c670024] [local] [Single Mode] Reset network interface [success] [admin] Details: Command:'inet ifconfig eth1 reset ' rvpn_shell[14053]: [02-01 14:19:26.401259]< 14053>(00007ff757d34c40)[L3] | Command:'inet ifconfig eth1 reset ' finished with rc=0 AAA__fe5ce7_c48cd8_b47d02_77fe14 rc=0 done	Reset network interface SUCCESS
Включение сетевого интерфейса	vmunix: [13614.681497] vmxnet3 0000:0b:00.0 eth1: NIC Link is Up 10 Mbps	Set network interface state SUCCESS
Выключение сетевого интерфейса	rvpn_shell[14053]: <management> [ig100-2c670024] [local] [Single Mode] Set network interface state [success] [admin] Details: Command:'inet ifconfig eth1 down '	Set network interface state SUCCESS

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Добавление статического маршрута	itcs-controld[5303]: [02-01 14:51:13.350100]<5303>(00007f192ee01700)[L3] | System::Routing<SR_ADD_ROUTE> Run command 'Command: inet route add' successful rvpn_shell[5154]: [02-01 14:51:13.354015]<5154>(00007ff178884c40)[L3] | Command:'inet route add distance=5,gateway=172.16.100.1,host=172.16.100.0,netmask=255.255.255.0,table_name=,table_number=254,weight=5' finished with rc=0 AAA__839737_b01001_4c11d5_b8e4a9 rc=0 done	Add static route SUCCESS
Удаление статического маршрута	itcs-controld[5303]: [02-01 14:56:52.463374]<5303>(00007f192f602700)[L3] | System::Routing<RT_DEL> Command: inet route delete 172.16.100.0. The following route was deleted: Table 254 (MAIN), Destination Netmask Next hop Distance Weight, ----------- ------- -------- -------- ------, 172.16.100.0 255.255.255.0 172.16.100.1 5 5 , itcs-controld[5303]: [02-01 14:56:52.463416]<5303>(00007f192f602700)[L3] | System::Routing<SR_DELETE_ROUTE_COMMON> 'Command: inet route delete' successful	Delete route SUCCESS
Создание виртуального интерфейса VLAN	rvpn_shell[5154]: New VLAN interface eth1.5 was created. ... rvpn_shell[5154]: <management> [va2000-3e130499] [local] [Single Mode] Add VLAN interface [success] [admin] Details: Command:'inet ifconfig eth1 VLAN add 5 '	Add VLAN interface SUCCESS
Удаление виртуального интерфейса VLAN	<management> [ig100-2c670024] [local] [Single Mode] Delete VLAN interface [success] [admin] Details: Command:'inet ifconfig eth1 vlan delete 5 '	Delete VLAN interface SUCCESS
Сохранение копии конфигурации VPN	rvpn_shell[5154]: <management> [ig100-2c670024] [local] [Single Mode] Current ViPNet configuration backing up [success] [admin] Details: Command:'vpn config save test_config '	Current ViPNet configuration backing up SUCCESS
Загрузка копии конфигурации VPN	rvpn_shell[5154]: <management> [ig100-2c670024] [local] [Single Mode] Load VPN configuration backup [success] [admin] Details: Command:'vpn config load test_config '	Load VPN configuration backup SUCCESS
Экспорт журнала регистрации IP-пакетов на USB-носитель	rvpn_shell[13459]: [02-06 15:57:56.005795]<13459>(00007fec1de51c40)[L3] | Command:'machine logs export network-traffic usb netlog' export_packetdb.sh[14737]: File successfully copied. Unmounting USB drive..	Export IP packet log to a USB drive SUCCESS

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Экспорт системного журнала	`export_log.sh[16540]: Copying logs_ig_3e130499_ig10-3e130499_2023_02_01_15_35_34.tar.gz to USB drive. Press —C to abort` `export_log.sh[16540]: File successfully copied. Unmounting USB drive...`	`Export event log SUCCESS`
Экспорт индивидуальной конфигурации на сервер ViPNet Prime	`export_appliance_configuration_file_to_usb.sh [20293]: File successfully copied. Unmounting USB drive..` `rvpn_shell[18277]: <management> [ig100-2c670024] [local] [Single Mode] Schedule configuration backup [success] [admin] Details: Command:'machine backup export '`	`Export configuration backup SUCCESS`

Экспорт индивидуальной конфигурации на USB-носитель	`export_appliance_configuration_file_to_usb.sh [4650]: File successfully copied. Unmounting USB drive..`
	`...`
	`export_appliance_configuration_file_to_usb.sh [4650]: ig100-2c670024-20230922T034846Z.ecf copied successfully.`
		`Export configuration backup SUCCESS`

Импорт индивидуальной конфигурации	`import_appliance_configuration_file.sh[12361]: Installing configuration /tmp/vipnet/ig100-2c670024-20230922T034846Z.ecf in /tmp/vipnet...`
	`...`
	`import_appliance_configuration_file_from_usb.sh[12361]: Settings successfully imported. You may remove the USB drive.`
		`Configuration import initiated SUCCESS`

Импорт универсальной конфигурации	`import_appliance_configuration_file.sh[9135]: Installing configuration /tmp/vipnet/ig100-2c670024-20230922T033003Z.vbe in /tmp/vipnet...`
	`...`
	`import_appliance_configuration_file.sh[8954]: Settings successfully imported. You may remove the USB drive.`
		`Configuration import initiated SUCCESS`

Экспорт универсальной конфигурации на USB-носитель	`export_appliance_configuration_file_to_usb.sh [8619]: File successfully copied. Unmounting USB drive..`
	`...`
	`export_appliance_configuration_file_to_usb.sh [8619]: ig100-2c670024-20230922T033003Z.vbe copied successfully.`
		`Export configuration backup SUCCESS`

Событие	Пример записи в системном журнале	Пример записи в журнале аудита

Изменение сетевых фильтров и правил трансляции адресов	Отображение изменения:
	`pncmd: [02-01 16:46:40.780465]< 24801>(00007f50d34c87c0)[L3] syslog | A rule was deleted:`
	`vpncmd: [02-01 16:46:40.780527]< 24801>(00007f50d34c87c0)[L3] syslog | Type:User ID:4000001 local src @any dst @local service @HTTP pass Enabled`
	`iplircfg[19943]: [02-01 16:46:40.797926]< 19943>(00007fdfc67fc700)[L3] syslog | User rules dataname has been changed.`
		`Add firewall filter SUCCESS`

Изменение правил фильтрации протокола Modbus	`rvpn_shell[4322]: <management> [ig100-2c670024] [local] [Single Mode] Ipf read/write request [success] [admin] Details: Command:'{"request":{"action":"update","objec t":"modbus","data":[{"name":"Rules_01","id":" 3361850049","clientid":"3580193441","enabled" :"true","fw_rule":[{"id":"0","name":"ipf_modb us_Rules_01_0","fw_table":"local","proto":"tc p","client_ip":{"sequence":[{"value":"192.168 .30.51"}]},"server_ip":{"sequence":[{"value": "10.10.10.12"}]},"server_port":{"sequence":[{ "value":"502"},{"value":"503"}]}}],"rule":[{" name":"Rule01","action":"pass","enabled":"tru e","id":{"sequence":[{"value":"2"},{"value":" 6"}]},"fc":{"sequence":[{"value":"3","upper": "4"}]},"r":{"sequence":[{"value":"30","upper" :"50"}]}}]}]}} '`	`Ipf read/write request SUCCESS`
Перевыпуск ключей локального SSH-сервера	`rvpn_shell[20540]: <management> [ig100-2c670024] [local] [Single Mode] Delete SSH local keys [success] [admin] Details: Command:'admin ssh remove key local '`	`Delete SSH local keys SUCCESS`
Издание сертификата администратора	`itcs-aad[1079]: [10-13 09:59:23.085637]<1079>(000000006f0fb3d0)[L0] | AUDIT ActionIsFinished: user:"admin" action System:AA:CreateLocalAdminCertificate ticket AAA_6deba6_lcl6ca_acbeb6_lc29fd`	—
Включение фильтрации протокола МЭК 60870-5-104 на прикладном уровне	`rvpn_shell[23329]: <management> [ig100-2c670024] [local] [Single Mode] Ipf read/write request [success] [admin] Details: Command:'{"request":{"action":"toggle","objec t":"iec104","data":[{"enabled":"true"}]}} '`	`Ipf read/write request SUCCESS`
Выключение фильтрации протокола Modbus на прикладном уровне	`rvpn_shell[16716]: <management> [ig100-2c670024] [local] [Single Mode] Ipf read/write request [success] [admin] Details: Command:'{"request":{"action":"toggle","objec t":"modbus","data":[{"enabled":"false"}]}} '`	`Ipf read/write request SUCCESS`
Включение вывода сообщений о событиях	`rvpn_shell[23693]: [02-01 16:52:13.269594]< 23693>(00007f07bbdaec40)[L3] | Command:'debug on'`	`Turn debug notification on/off SUCCESS`

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Выключение вывода сообщений о событиях	`rvpn_shell[23693]: [02-01 16:54:29.797997]<23693>(00007f07bbdaec40)[L3] | Command:'debug off'`	`Turn debug notification on/off SUCCESS`

Таблица 24. События, связанные с запуском или остановкой служб ViPNet Coordinator IG

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Запуск службы `failoverd`, отвечающей за систему защиты от сбоев	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop failover daemon [success] [admin] Details: Command:'failover start '`	`Start failover daemon SUCCESS`
Завершение работы службы `failoverd`, отвечающей за систему защиты от сбоев	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop failover daemon [success] [admin] Details: Command:'failover stop '`	`Stop failover daemon SUCCESS`
Запуск управляющей службы `iplircfg`	`hwvipmod[16584]: Loading ViPNet modules ...` `rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop iplir daemon [success] [admin] Details: Command:'iplir start '`	`Start iplir daemon SUCCESS`
Завершение работы управляющей службы `iplircfg`	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop iplir daemon [success] [admin] Details: Command:'iplir stop '`	`Stop iplir daemon SUCCESS`
Перезапуск веб-сервера ViPNet Coordinator IG	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Restart web server [success] [admin] Details: Command:'webui restart '`	`Restart web server SUCCESS`
Запуск службы шлюза Modbus	`rvpn_shell[18999]: <management> [ig100-2c670024] [local] [Single Mode] Turn ModbusGateway on/off [success] [admin] Details: Command:'mbgw start '`	`Update ModbusGateway config SUCCESS`
Завершение работы службы шлюза Modbus	`rvpn_shell[18999]: <management> [ig100-2c670024] [local] [Single Mode] Turn ModbusGateway on/off [success] [admin] Details: Command:'mbgw stop '`	`Update ModbusGateway config SUCCESS`
Запуск службы `piomonotor`	`rvpn_shell[18320]: <management> [ig100-2c670024] [local] [Single Mode] Turn PIO_MONITOR on/off [success] [admin] Details: Command:'piomonitor on '`	`Turn PIO_MONITOR on`
Завершение работы службы `piomonotor`	`rvpn_shell[17495]: <management> [ig100-2c670024] [local] [Single Mode] Turn PIO_MONITOR on/off [success] [admin] Details: Command:'piomonitor off '`	`Turn PIO_MONITOR off`

Таблица 25. События, связанные с обменом служебной информацией с управляющим ПО

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Применение обновления информации об управляющем ПО	`itcs-external-controld[4378]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Applying Manager Information Updates Details: Starting ApplyPolicy`	`Applying Manager Information Updates SUCCESS/FAIL`
Применение изменений фильтров межсетевого экрана из управляющего ПО	`itcs-external-controld[4378]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Apply firewall filters received from the management software Details: Starting ApplyPolicy`	`Apply firewall filters received from the management software SUCCESS/FAIL`

Применение обновления лицензии от управляющего ПО	`itcs-external-controld[4742]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Applying a license upgrade from a control application Details: Starting ApplyPolicy`
	`...`
	`itcs-external-controld[4742]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Applying a license upgrade from a control application Details: Finish`
		`Applying a license upgrade from a control application SUCCESS/FAIL`

Подключение к транспортному серверу UT5	`Connection established, subcribed to publisher endpoint`	—
Отсутствие подключения к транспортному серверу UT5	`Connection error: <Connection timed out! Wait and repeat connection...>`	—

Таблица 26. События, связанные с работой системы защиты от сбоев

Событие	Пример записи в системном журнале

Переключение узла кластера в активный режим	`failoverd[6976]: [02-02 10:13:38.300387]< 6976>(00007f054f9847c0)[L2] Exit | active server not responding, switching to active mode`
	`failoverd[6976]: [02-02 10:13:38.300423]< 6976>(00007f054f9847c0)[L1] syslog | switching to active mode`
	`vmunix: [ 320.636326] [DUP] switch cluster mode: passive (1) => active (2)`

Переключение узла кластера в пассивный режим из-за отсутствия физического соединения на сетевом интерфейсе	`vmunix: [ 4927.663675] vmxnet3 0000:0b:00.0 eth1: NIC Link is Down`
	`failover-node[31518]: Configuring state of daemons for passive mode`
	`vmunix: [ 4940.296325] [DUP] switch cluster mode: active (2) => passive (1)`

Событие	Пример записи в системном журнале
Перезагрузка узла кластера из-за конфликта режимов	`failoverd[18143]: [02-02 13:04:44.026129]< 18143>(00007f4db882e7c0)[L1] syslog | Rebooted due conflict mode at Thu Feb 2 13:04:44 2023`

Перезагрузка узла кластера из-за обнаружения службой `failoverd` ошибки другой контролируемой службы	`failoverd[6973]: [02-02 12:19:35.032019]< 6973>(00007f9a752617c0)[L1] CheckApp | Reached maximum count of application restarts [iplircfg] pid 2008`
	`failoverd[6973]: [02-02 12:19:35.032029]< 6973>(00007f9a752617c0)[L3] OnInvokeEventCmd | Rebooting the appliance in order to recover`
	`failoverd[6973]: [02-02 12:19:35.470798]< 6973>(00007f9a752617c0)[L1] syslog | one or more subsystems failed, rebooting`
	`failoverd[6973]: [02-02 12:19:35.470823]< 6973>(00007f9a752617c0)[L1] syslog | Rebooted due to watcher detected error at Thu Feb 2 12:19:35 2023`
	`syslogd (GNU inetutils 1.9.4): restart`

Таблица 27. События, связанные с обменом служебной информацией между узлами ViPNet

Событие	Пример записи в системном журнале
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при включении узла, а затем периодически)	`iplircfg[7226]: [02-02 15:11:38.237440]< 7226>(00007fcb66e40980)[L2] | got message: type 1 from ID 0x3E130001 (msg name 'YY0N29WO.KI5')`
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при первом обращении к серверу IP-адресов)	`iplircfg[5095]: [01-23 10:14:59.709058]< 5095>(00007ff998c2f980)[L2] | got message: type 3 from ID 0x3E130001 (msg name 'GJ5ZUZSZ.JJ0')`
Первое обращение к серверу соединений, если сервер не является сервером IP-адресов	`iplircfg[1684]: [02-07 21:28:10.979295]< 1684>(00007f5563f66980)[L2] | got message: type 23 from ID 0x3E1305DA (msg name 'AAZD}YP7.493')`
Отключение узла ViPNet от сервера IP-адресов	`iplircfg[29142]: [02-02 13:36:53.678221]< 29142>(00007f40cc3a3980)[L2] | got message: type 2 from ID 0x3E130001 (msg name 'DKNYU56I.BV1')`
Проверка соединения с узлом ViPNet (запрос)	`iplircfg[29142]: [02-02 13:33:36.169191]< 29142>(00007f40cc3a3980)[L2] | got message: type 5 from ID 0x3E1304A5 (msg name '6RB8POLJ.DGC')`
Подтверждение получения сообщения (кроме уведомлений об изменении адреса доступа удалённого узла ViPNet)	`iplircfg[29142]: [02-02 13:33:36.320283]< 29142>(00007f40cc3a3980)[L2] | got message: type 7 from ID 0x3E1304A5 (msg name 'UOPO9T1T.DRR')`

Событие	Пример записи в системном журнале
Уведомление об изменении адреса доступа удалённого узла ViPNet	`iplircfg[29142]: [02-02 13:46:06.699250]< 29142>(00007f40cc3a3980)[L2] | got message: type 50 from ID 0x3E130002 (msg name 'NTP964KK.0FJ')`
Подтверждение получения уведомления об изменении адреса доступа удалённого узла ViPNet	`iplircfg[7226]: [02-02 15:03:56.491499]< 7226>(00007fcb66e40980)[L2] | got message: type 70 from ID 0x3E130001 (msg name '31J92W9V.6YN')`
Изменение параметров адреса доступа удалённого узла ViPNet	`iplircfg[25757]: [02-02 15:23:54.171023]< 25757>(00007fbcf1f9f980)[L2] | load natsettings for 0x3E130193: firewallip=192.168.166.105 port=55888 timeout=25 virtualip=0.0.0.1 proxyid=0x3E130001 DRV_ALWAYS_USE_SERVER=no DRV_GREEN_NODE=yes DRV_STOP_FIREWALL_IP=no DRV_ELAPSE=no DRV_BROADCAST_HOST=no DRV_INCAPS_FORCE_REAL_ADDR=yes`

Таблица 28. События, связанные с состоянием оборудования и беспроводных соединений

Событие	Пример записей в журнале
Достижение критического порога температур процессора	`vmunix: [60487.978244] CPU critical temps 105`
Достижение критического порога температур модема	`usbmodemd[6709]: RequestTemp: temp 71000 is max`
Достижения критического порога напряжения на модеме	`usbmodemd[6709]: RequestVoltage: voltage 32000 out of range`
Опрос уровня сигнала Wi-Fi	`root: [WifiClient] Station cc:2d:e0:90:d8:c7; signal: -49 dBm; connected time: 246 seconds`
Запуск модема	`usbmodemd[5544]: USBModemDevice: found support modem VID/PID: 05c6:9003, VendorModel: Quectel UC20` `usbmodemd[5544]: NetworkSettingInit: MCC/MNC 250/99`
Неисправность SIM-карты или её отсутствие	`usbmodemd[6709]: SimInit: sim card not insert`
Состояние SIM-карты невозможно определить	`usbmodemd[6709]: SimInit: unknown status`
SIM-карта готова к работе, ввод PIN-кода не требуется	`usbmodemd[5544]: SimInit: pin status READY`
Требуется PIN-код для SIM-карты	`usbmodemd[5544]: SimInit: pin status SIM PIN`
PIN-код для SIM-карты введён успешно	`usbmodemd[5544]: SimInit: enter pin OK`
Инициализация SIM-карты	`usbmodemd[5544]: SimInit: sim card initialization`

Событие	Пример записей в журнале
Обнаружены мобильные сети	`usbmodemd[6709]: FillNetworksList: networks Beeline,MTS,MegaFon,TELE2`
Опрос состояния текущего мобильного соединения	`usbmodemd[5045]: RequestNetworkName: network MegaFon (3G)`
Опрос уровня сигнала мобильного соединения	`usbmodemd[5045]: RequestSignalLevel: signal level 19`
Опрос счётчика исходящего трафика за текущую сессию мобильного соединения (в байтах)	`usbmodemd[5045]: PPPTrafficInfo: update traffic info, tx=854 rx=485`
Опрос состояния службы установки соединения по модему	`usbmodemd[5544]: PPPManager: check pppd, pid=5553`
Опрос количества подключений к мобильной сети с момента запуска службы установки соединения по модему	`usbmodemd[5544]: PPPManager: connect count 1`

Таблица 29. События, связанные с доступностью каналов связи в режиме работы MultiWAN

Событие	Пример записей в журнале
Шлюз недоступен	`dgdd[19471]: next hop: GW-1 switched from up to down`
Шлюз доступен	`dgdd[19471]: next hop: GW-1 switched from down to up`
Переключение политики маршрутизации	`dgdd[19471]: dgd rule: performing action: preference 10, type 1, command 'policy route-GW-1'`

Таблица 30. События, связанные с работой устройств, подключенных по технологии PoE

Событие	Пример записей в журнале
Число неудачных попыток опроса устройства достигло значения, при котором устройство считается недоступным	`igpoed[5610]: Error | channel eth1 restart; error: 2 icmp checks failed`
Превышение ограничения потребляемого тока	`igpoed[4401]: Error | channel eth1 in error: port overcurrent timeout`
Превышение ограничения потребляемого тока при подаче питания	`igpoed[4401]: Error | channel eth1 in error: port startup overcurrent timeout`
Превышение заданного	`igpoed[4401]: Error | channel eth1 in error: port current limit`

Событие	Пример записей в журнале
пользователем ограничения потребляемой мощности	`timeout`
Блокировка устройства при пониженном напряжении	`igpoed[4401]: Error | channel eth1 in error: port analog supply under voltage lockout`
Выход из режима блокировки при пониженном напряжении	`igpoed[4401]: Error | channel eth1 in error: port digital supply under voltage lockout`
Перегрев контроллера	`igpoed[2153]: Error | channel eth1 in error: port overtemperature`
Ошибка связи с микросхемой PoE	`igpoed[2153]: Error | channel eth1 in error: communication error`
Неисправность полевого транзистора	`igpoed[2153]: Error | channel eth1 in error: port mosfet has failed`

Таблица 31. События, связанные с ошибками датчика случайных чисел (ДСЧ) и шифратора

Событие	Пример записей в журнале

Проверка при запуске и регламентная проверка ДСЧ в криптодрайвере	`uprngd: uprngd 0x7f2963fff700 lcuprng.c :434 core_normative_control Normative control was successfully completed.`
	`itcshubd[17962]: <crypto> [ig100-2c670024] [local] [Single Mode] CryptoEvent0 [failed] [] Details: SoftToken 0x7f55da5ad700 Reglament inspection passed`
	`itcshubd[17962]: SoftToken 0x7f55da5ad700 Reglament inspection passed`

Событие	Пример записей в журнале
Проверка при запуске и регламентная проверка шифраторов в криптодрайвере	itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem GOST status=0 (0x854CAC47) itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem GOST status=0 (0x854CAC47) itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem FIPS status=8000000 (0x854CAC47) itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem FIPS status=8000000 (0x854CAC47) itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem CUSTOM status=8000000 (0x854CAC47) itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem CUSTOM status=8000000 (0x854CAC47)

Примечание. Записи об успешной работе ДСЧ или шифратора не протоколируются.

Таблица 32. События антивирусной проверки и контент-фильтрации

Событие	Пример записей в журнале
Сработало запрещающее правило контроля содержимого трафика по HTTP-методу	(squid): 1 172.16.50.5 TCP_DENIED/403 19183 GET http://kremlin.ru/ - NONE/- text/html
Сработало запрещающее правило контроля содержимого трафика по MIME-типу	(squid): 58 172.16.100.5 TCP_DENIED_REPLY/403 19248 GET http://static.kremlin.ru/media/events/files/ru/QdJ0ybmN7Kocwc8eyTGosdyuylM6qXpj.pdf - DIRECT/95.173.136.78 text/html
Средство антивирусной защиты заблокировало скачивание заражённого файла	(squid): ICAP: 13 172.16.100.5 icap://192.168.32.11:1344/virus_scan RESPMOD http://www.virusanalyst.com/eicar.zip

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 IG могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 33. SNMP-параметры. MIB-II System

OID	Описание
.1.3.6.1.2.1.1.1.0	Информация о сетевом узле (имя узла, информация об ОС).
.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.
.1.3.6.1.2.1.1.8.0	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).
.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).

OID	Описание
.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.
.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.

OID	Описание
.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.
.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.

OID	Описание
.1.3.6.1.2.1.11.30.0	Возможность отправки authenticationFailure traps: • 1 - разрешено, • 2 – запрещено.

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 IG могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 34. 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).
.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.

OID	Описание
.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.
.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.

OID	Описание
.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.
.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.

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 35. 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, отклонённых сетевым узлом по причине ошибок в заголовке пакета.
.1.3.6.1.2.1.4.5.0	Количество входящих IP-пакетов, отклонённых 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 отклонённых IP-пакетов по причине недостатка буфера.
.1.3.6.1.2.1.4.9.0	Количество успешно доставленных IP-пакетов.
.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, отклонённых 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.

OID	Описание
.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.
1.3.6.1.2.1.4.20.1.5.E	Максимальный размер входящего фрагментированного IP-пакета, который сетевой узел может собрать на этом интерфейсе.

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 отклонённых маршрутов.
.1.3.6.1.2.1.4.31.1.1.	Таблица, содержащая статистику (счётчики) IP-трафика различных версий на сетевом узле для всех интерфейсов.

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

OID	Описание
.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.
.1.3.6.1.2.1.4.33.0	Служебный объект, необходимый для синхронизации изменений параметров IP-MIB при взаимодействии с несколькими SNMP менеджерами. Используется только в случае записи данных в OID.

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.

OID	Описание
.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.
.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 её в статус active, • 5 (createAndWait) — создание строки и перевод её 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.

OID	Описание
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.
.1.3.6.1.2.1.4.35.1.7.A.B.E	Статус маппинга: • 1(reachable) — подтверждён, • 2 (stale) — не подтверждён, • 3 (delay) — ожидание, • 4 (probeprobe) — активное, • 5 (invalid) — недействителен, • 6 (unknown) — не определён, • 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 её в статус active, • 5 (createAndWait) — создание строки и перевод её 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.

OID	Описание
.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.
.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.

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 36. 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.
.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).

OID	Описание
.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.
.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 37. 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, вовлечённых в SingleCollision на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.5.A	Количество фреймов, вовлечённых 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	Текущий режим дуплекса на интерфейсе: • 1 — unknown, • 2 — halfDuplex, • 3 — fullDuplex. Для неподключённых 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 38. SNMP-параметры. TCP-MIB

OID	Описание
.1.3.6.1.2.1.6.1.0	Алгоритм определения таймаута для повторной передачи неопознанных октетов.
.1.3.6.1.2.1.6.2.0	Минимальное допустимое значение таймаута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.3.0	Максимальное допустимое значение таймаута 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 39. 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 40. 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 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

.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.

OID	Описание
.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 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).

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 41. 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 IG). 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 IG).
.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 42. SNMP-параметры. UCD-SNMP-MIB

OID	Описание
.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).
.1.3.6.1.4.1.2021.4.13.0	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.
.1.3.6.1.4.1.2021.4.27.0	Объем памяти (в кибибайтах), доступный для запуска новых приложений без вымещения данных в swap.
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).

OID	Описание
.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.
.1.3.6.1.4.1.2021.9.1.6.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).
.1.3.6.1.4.1.2021.9.1.11.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если раздел менее 2ТБ, параметр равен .1.3.6.1.4.1.2021.9.1.6.B.
.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 2ТБ, параметр равен .1.3.6.1.4.1.2021.9.1.7.B.
.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 2ТБ, параметр равен .1.3.6.1.4.1.2021.9.1.8.B

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).
.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.
.1.3.6.1.4.1.2021.11.5.0	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.

OID	Описание
.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.
.1.3.6.1.4.1.2021.11.57.0	Количество блоков, отправленное блочному устройству (диску).
.1.3.6.1.4.1.2021.11.58.0	Количество блоков, полученное блочным устройством (диском).
.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.
.1.3.6.1.4.1.2021.11.67.0	Количество ядер процессоров.
.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.
.1.3.6.1.4.1.2021.101.100.0	Признак 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 43. 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.

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 44. 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.
.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 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.
.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.

OID	Описание
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 – тип 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 45. 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.

OID	Описание
.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 46. 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 47. 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.

OID	Описание
.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.

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 48. 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

OID	Описание
.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.
.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.

OID	Описание
.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.
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 49. 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).
.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 50. SNMP-параметры. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.1.1.0	Шестнадцатеричный идентификатор сети ViPNet.
.1.3.6.1.4.1.10812.1.1.2.0	Шестнадцатеричный идентификатор сетевого узла ViPNet.
.1.3.6.1.4.1.10812.1.1.3.0	Имя пользователя узла ViPNet.
.1.3.6.1.4.1.10812.1.1.4.0	Время работы ViPNet Coordinator IG (сбрасывается каждый раз при перезапуске службы iplircfg).
.1.3.6.1.4.1.10812.1.1.5.0	Шестнадцатеричный идентификатор, включающий в себя идентификаторы узла ViPNet и сети ViPNet.
.1.3.6.1.4.1.10812.1.1.7.0	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.X	Номер сетевого интерфейса X, где X — индекс интерфейса.
.1.3.6.1.4.1.10812.1.2.2.1.2.X	Имя сетевого интерфейса X.
.1.3.6.1.4.1.10812.1.2.2.1.3.X	Устаревший параметр, всегда равен 0.
.1.3.6.1.4.1.10812.1.2.2.1.4.X	Количество пропущенных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.5.X	Количество блокированных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.6.X	Количество пропущенных исходящих незашифрованных пакетов.

OID	Описание
.1.3.6.1.4.1.10812.1.2.2.1.7.X	Количество блокированных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.8.X	Количество пропущенных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.9.X	Количество блокированных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.10.X	Количество пропущенных исходящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.11.X	Количество блокированных исходящих зашифрованных пакетов.

Таблица объектов, описывающих состояние служб iplircfg, failoverd, mftpd, webgui-fcgi-server, remote_management (.1.3.6.1.4.1.10812.1.7.1):

.1.3.6.1.4.1.10812.1.7.1.1.2.Y	Индекс службы с индексом Y: • 1 — failoverd, • 2 — iplircfg, • 3 — mftpd, • 4 — webgui-fcgi-server, • 5 — external-controld.
.1.3.6.1.4.1.10812.1.7.1.1.3.Y	Состояние службы с индексом Y: • 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.Y	Время работы службы с индексом Y.
.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.
.1.3.6.1.4.1.10812.1.8.6.1.2.X	IP-адрес интерфейса синхронизации.

OID	Описание
.1.3.6.1.4.1.10812.1.8.6.1.3.X	Статус доступности узла: • 1 — доступен, • 2 — недоступен.
Таблица сведений о ViPNet Coordinator IG (.1.3.6.1.4.1.10812.1.10.1):	
.1.3.6.1.4.1.10812.1.10.1.1.1.X	Индекс строки.
.1.3.6.1.4.1.10812.1.10.1.1.2.X	Serial number — имя параметра.
.1.3.6.1.4.1.10812.1.10.1.1.3.X	Значение параметра Serial number.

SNMP-агент ViPNet Coordinator IG может отправлять уведомления:

Таблица 51. SNMP-уведомления. 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.
.1.3.6.1.4.1.10812.1.0.14	Запуск службы external-controld.
.1.3.6.1.4.1.10812.1.0.15	Остановка службы external-controld.

VIPNETMULTIWAN-MIB

VIPNETMULTIWAN-MIB (.1.3.6.1.4.1.10812.14) включает в себя объекты, предназначенные для получения информации об используемых ViPNet Coordinator IG каналах связи и доступности шлюзов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 52. SNMP-параметры. VIPNETMULTIWAN-MIB

OID	Описание
Таблица доступности шлюзов (.1.3.6.1.4.1.10812.14.1):	
X – индекс таблицы	
.1.3.6.1.4.1.10812.14.1.1.1.X	Индекс таблицы (порядковый номер шлюза).
.1.3.6.1.4.1.10812.14.1.1.2.X	Имя шлюза.
.1.3.6.1.4.1.10812.14.1.1.3.X	Состояние проверки шлюза: • 1 – проверяется, • 2 – не проверяется, • 3 – состояние не определено.
.1.3.6.1.4.1.10812.14.1.1.4.X	Способ проверки доступности шлюза: • 1 – ICMP, • 2 – TCP 80, • 3 – TCP 443, • 4 – способ не определен (N/A).
.1.3.6.1.4.1.10812.14.1.1.5.X	IP-адрес шлюза.
.1.3.6.1.4.1.10812.14.1.1.6.X	IP-адрес для проверки доступности шлюза.
.1.3.6.1.4.1.10812.14.1.1.7.X	Количество успешных проверок доступности шлюза.
.1.3.6.1.4.1.10812.14.1.1.8.X	Количество неудачных проверок доступности шлюза.
.1.3.6.1.4.1.10812.14.1.1.9.X	Имя и состояние сетевого интерфейса шлюза: • 1 – включен (up), • 2 – выключен (down), • 3 – состояние не определено (N/A). Параметр содержит пустую строку, если на сетевом интерфейсе шлюза задан статический IP-адрес.
.1.3.6.1.4.1.10812.14.1.1.10.X	Состояние сетевого интерфейса шлюза: • 1 – включен (up), • 2 – выключен (down), • 3 – состояние не определено (N/A).
.1.3.6.1.4.1.10812.14.1.1.11.X	Дата и время последнего изменения состояния шлюза.
.1.3.6.1.4.1.10812.14.2.1	Имя политики маршрутизации.

SNMP-агент ViPNet Coordinator IG может отправлять уведомления:

Таблица 53. SNMP-уведомления. VIPNETMULTIWAN-MIB

OID	Описание
.1.3.6.1.4.1.10812.14.0.1	Изменение состояния шлюза.

OID	Описание
.1.3.6.1.4.1.10812.14.0.2	Смена активной политики маршрутизации.

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 54. SNMP-параметры. MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.3.1.0	Версия агента мониторинга.
.1.3.6.1.4.1.10812.4.3.2.0	Идентификатор инсталляции агента мониторинга.
.1.3.6.1.4.1.10812.4.4	Таблица плагинов агента мониторинга.
.1.3.6.1.4.1.10812.4.5	Таблица функциональных возможностей 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 55. 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

PDU (Protocol Data Unit)

Общая для всех физических уровней часть пакета протокола. Содержит данные пакета.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

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

ViPNet Prime

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

Включает в себя основные функциональные модули:

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

Администратор сети ViPNet

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

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удалённых узлов в приложениях ViPNet.

Дистрибутив ключей

Набор, содержащий:

- ключи обмена;
- ключ защиты обновлений;
- справочники с информацией об узлах защищенной сети;
- лицензия.

Формируется в ViPNet Prime на основе заданных связей между узлами. Необходим для инициализации и работы ViPNet Coordinator IG.

Для узлов защищенной сети поколения 5 используется дистрибутив ключей `ds5`, для узлов поколения 4 — `dst`.

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 IG 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 IG, 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 IG на активном ViPNet Coordinator IG, пассивный ViPNet Coordinator IG переключается в активный режим для выполнения функций. При этом сбойный ViPNet Coordinator IG 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.

Ключи защиты обновлений

Ключи защиты обновлений обеспечивают безопасное удаленное обновление ключей обмена из ключевого центра ViPNet Prime и их хранение в ViPNet Coordinator IG.

Ключи обмена

На ключах обмена защищается канал передачи данных между двумя связанными узлами сети ViPNet.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Открытый трафик

Поток незашифрованных IP-пакетов.

Открытый узел

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

Политики безопасности

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

Сервер IP-адресов

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

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента функцию сервера соединений выполняет координатор, назначенный сервером IP-адресов.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сеть ViPNet

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

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами 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.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

Шлюз Modbus

Программно-аппаратная функциональность, выполняющая преобразование трафика интерфейса Ethernet в интерфейсы RS-232 и RS-485 и обратно для обеспечения взаимодействия Ethernet- и Modbus-устройств.