

ViPNet Coordinator HW 5

Настройка с помощью веб-интерфейса

Версия продукта: 5.4.2

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

infotecs

© АО «ИнфоТеКС», 2026

ФРКЕ.465614.003ИС1

Версия продукта: 5.4.2

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 HW приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Coordinator HW.

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 ... **9**
О документе ... 10
Соглашения документа ... 11
Обратная связь ... 12

Глава 1. Работа с веб-интерфейсом ... **13**
Требования к рабочему месту ... 14
Подключение к ViPNet Coordinator HW ... 15

Глава 2. Настройка подключения к сети ... **18**
Настройка сетевых интерфейсов Ethernet ... 19
Назначение дополнительных IP-адресов ... 23
Подключение к мобильной сети 3G/4G ... 24
Подключение к сети Wi-Fi ... 26
Обработка трафика из нескольких VLAN ... 29
Настройка агрегированных сетевых интерфейсов ... 33
Режимы работы агрегированного интерфейса ... 33
Создание агрегированного интерфейса ... 36
Просмотр ARP-таблицы ... 39

Глава 3. Настройка VPN ... **40**
Просмотр сведений об узлах ViPNet ... 41
Настройка видимости узлов ... 44
Настройка туннелирования на сетевом уровне ... 47
Общие сведения о туннелировании ... 47
Ручная настройка туннелирования ... 48
Настройка доступа к туннелируемым узлам в одной подсети ... 49
Настройка туннелирования на канальном уровне ... 51
Общие сведения о L2OverIP ... 51
Особенности реализации L2OverIP ... 52
Настройка L2OverIP ... 53

Глава 4. Настройка межсетевого экрана ... **55**
О фильтрации трафика ... 56
Типы трафика ... 56

Принципы фильтрации трафика 57
Объекты сетевых фильтров и правил трансляции адресов 63
Системные объекты 63
Группы объектов «ViPNet-узлы», «IP-адреса», «Интерфейсы», «Протоколы» и «Расписания» 65
Создание и изменение групп объектов 65
Просмотр групп объектов 72
Группа объектов «Веб-клиенты» 73
Группа объектов «URL-категории» 74
Обновление базы URL-категорий 75
Настраиваемые URL-категории 77
Группа объектов «Страны» 79
Настройка SSL/TLS-инспекции трафика 83
Настройка основных параметров SSL/TLS-инспекции 83
Настройка исключений из SSL/TLS-инспекции 85
Настройка SSL-сертификата 88
Особенности SSL/TLS-инспекции 89
Настройка подключения к ICAP-серверам 92
Настройка сетевых фильтров 95
Общие сведения о сетевых фильтрах 95
Создание и изменение сетевых фильтров 97
Просмотр сетевых фильтров 101
Изменение порядка применения настраиваемых фильтров 103
Настройка регистрации IP-пакетов и сессий при срабатывании фильтров 103
Пример использования групп объектов и сетевых фильтров 105
Примеры использования транзитных фильтров 107
Настройка фильтрации трафика по пользователю 107
Настройка фильтрации трафика Torrent-клиентов 109
Деактивация транзитных фильтров после обновления ПО 110
Настройка правил трансляции адресов 111
Общие сведения о трансляции сетевых адресов 111
Трансляция адреса источника 112
Трансляция адреса назначения 113
Создание и изменение правил трансляции адресов 114
Просмотр правил трансляции адресов 116
Изменение порядка применения правил трансляции адресов 116
Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP 118
О прикладных протоколах 118
Настройка параметров обработки прикладных протоколов 122

Настройка блокировки трафика по списку IP-адресов ... 124

Глава 5. Настройка сетевых служб ... 126
Настройка DHCP-сервера ... 127
Настройка DHCP-relay ... 130
Настройка DNS-сервера ... 132
Настройка NTP-сервера ... 134
Настройка точки доступа сети Wi-Fi ... 136
Настройка взаимодействия с Active Directory ... 138
Настройка учетной записи технологического пользователя ... 139
Настройка взаимодействия с LDAP-сервером ... 142
Получение и импорт сертификатов ... 143
Настройка параметров Captive portal ... 144
Просмотр списка пользователей Active Directory и Captive portal ... 146
Регистрация событий аутентификации пользователей ... 147

Глава 6. Настройка предотвращения вторжений ... 148
Общие сведения об IPS ... 149
Параметры IPS по умолчанию ... 151
Включение и выключение IPS ... 152
Настройка параметров сетевого окружения ... 153
Управление правилами IPS ... 155
Поиск правил IPS ... 156
Просмотр и настройка правил IPS ... 158
Групповые операции с правилами IPS ... 160
Обновление базы правил IPS ... 161
Обновление базы вредоносного ПО ... 164
Настройка регистрации событий IPS ... 166

Глава 7. Настройка маршрутизации ... 167
Общие сведения о маршрутизации ... 168
Принципы маршрутизации ... 169
Просмотр таблицы маршрутизации ... 173
Настройка статической маршрутизации ... 174
Добавление статических маршрутов ... 174
Настройка балансировки IP-трафика ... 176
Настройка маршрутов протоколов DHCP и PPP ... 178
Настройка административной дистанции для маршрутов DHCP-сервера ... 178
Настройка метрики для маршрутов DHCP-сервера ... 179

Настройка метрики для маршрутов PPP-протокола ... 181
Изменение метрики по умолчанию для маршрутов от DHCP/PPP-протокола ... 181
Настройка OSPF ... 183
Общие сведения о протоколе OSPF ... 183
Настройка протокола OSPF ... 185
Настройка перераспределения маршрутов ... 189
Настройка BGP ... 191
Общие сведения о протоколе BGP ... 191
Настройка маршрутизатора ... 191
Настройка соседей ... 192
Настройка анонсирования подсетей ... 195
Мониторинг состояния маршрутизатора ... 197
Настройка MultiWAN ... 199
Настройка политик маршрутизации ... 200
Настройка проверки состояния шлюзов (DGD) ... 202

Глава 8. Настройка параметров безопасности ... 206
Управление локальными учетными записями ... 207
Параметры учетных записей ... 207
Полномочия ролей по управлению учетными записями ... 207
Управление учетными записями ... 209
Предотвращение подбора пароля учетных записей ... 210
Управление ключами локального SSH-сервера ... 212
Настройка подключения к веб-интерфейсу ... 213
Обновление ключей по истечении срока их действия ... 215

Глава 9. Настройка системных параметров ... 216
Настройка даты и времени ... 217
Перезагрузка ViPNet Coordinator HW ... 218
Выбор профиля производительности ... 219
Установка серийного номера ... 221
Просмотр лицензии ... 222

Глава 10. Резервное копирование и восстановление настроек ... 223
Управление индивидуальной конфигурацией ... 224
Резервное копирование индивидуальной конфигурации ... 224
Восстановление из резервной копии индивидуальной конфигурации ... 226
Управление универсальной конфигурацией ... 228
Экспорт универсальной конфигурации ... 229

Импорт настроек универсальной конфигурации ... 229

Глава 11. Работа с журналами ... 232
Настройка журналов ... 233
Журнал IP-пакетов ... 237
Журнал сессий ... 242
Журнал аудита ... 246
Журнал СКЗИ ... 248
Журнал MFTP ... 250
Журнал DNS-запросов ... 252
Системный журнал ... 254

Глава 12. Мониторинг работы ... 256
Просмотр состояния ... 257
Мониторинг по SNMP ... 258
Настройка SNMP-агента ... 259
Мониторинг кластера ... 267
Мониторинг ViPNet-узлов ... 269
Просмотр статистики передачи данных ... 271
Просмотр статистики IP-пакетов ... 272

Приложение A. Сетевые фильтры по умолчанию ... 273

Приложение B. Группы объектов ... 277

Приложение C. База URL-категорий ... 279

Приложение D. Типы событий журнала IP-пакетов ... 288

Приложение E. Базы управляющей информации (MIB) для протокола SNMP ... 291
MIB-II System ... 291
IF-MIB ... 295
IP-MIB ... 298
IP-FORWARD-MIB ... 304
Ethernet-Like MIB ... 308
TCP-MIB ... 309
UDP-MIB ... 312
HOST-RESOURCES-MIB ... 313
LM-SENSORS-MIB ... 319
NOTIFICATION-LOG-MIB ... 320

UCD-SNMP-MIB 321
UCD-DISKIO-MIB 325
NET-SNMP-MIB 326
SNMP-MPD-MIB 331
SNMP-TARGET-MIB 331
SNMP-USER-BASED-SM-MIB 331
SNMP-VIEW-BASED-ACM-MIB 333
SNMP-FRAMEWORK-MIB 335
VIPNET-MIB 336
VIPNETHW-MIB 338
VIPNETFWLOAD-MIB 339
MonitoringAgent-MIB 341
System-MonitoringAgent-MIB 341

Приложение F. Службы ПО ViPNet Coordinator HW 342

Приложение G. Поддерживаемые приложения 345

Приложение H. Поддерживаемые прикладные протоколы 349

Приложение I. Поддерживаемые группы приложений 352

Приложение J. Особенности фильтрации по приложениям и прикладным протоколам 360

Приложение K. Поддерживаемые MIME-типы 362

Приложение L. Формат указания IP-адресов и портов в правилах IPS 366

Приложение M. Параметры правил IPS по умолчанию 368

Приложение N. Группы правил IPS 372

Приложение O. Номера правил анализа трафика эвристическим методом 374

Приложение P. Термины и сокращения 376



Введение

О документе 10

Соглашения документа 11

Обратная связь 12

О документе

В документе описаны основные сценарии настройки многофункционального шлюза безопасности ViPNet Coordinator HW с помощью веб-интерфейса. Документ предназначен для администраторов сети ViPNet.

Соглашения документа

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, службы, интерфейса или путь



Внимание! В документе все сценарии работы с ViPNet Coordinator HW приведены для локального администратора `admin`.

В документе могут быть снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не участвуют в приведенных сценариях, могут выглядеть по-другому.

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.

  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 14

Подключение к ViPNet Coordinator HW 15

Требования к рабочему месту



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

- 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 HW 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 HW

По умолчанию подключение к ViPNet Coordinator HW с помощью веб-интерфейса запрещено. Если вы не разрешили подключение при инициализации устройства, сделайте это (см. «Подготовка к работе», раздел «После инициализации»).

Подключение с помощью веб-интерфейса следует выполнять с узлов защищённой сети, связанных с ViPNet Coordinator HW.

Аутентификация может выполняться для:

- пользователей с локальными учётными записями;
- пользователей с централизованными учётными записями, созданными в ViPNet Prime — возможна только при наличии доступа ViPNet Coordinator HW к ViPNet Prime.

По умолчанию для подключения используются протокол HTTPS (TCP-порт 8080) и самоподписанный сертификат.



Внимание! В текущей версии ПО ViPNet Coordinator HW пользователь с ролью «Сетевой администратор» может подключиться к устройству только с помощью командного интерпретатора.

Подключение

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



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

2 В окне аутентификации введите данные учётной записи:

- Для локальной учётной записи введите **Имя локального пользователя** и **Пароль**.
- Для централизованной учётной записи нажмите **Войти с помощью Prime**, затем введите **Имя учетной записи** и **Пароль**.

3 Нажмите **Войти**.

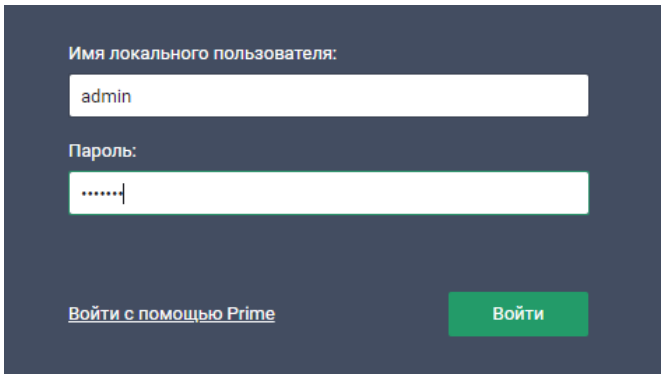


Рисунок 1. Аутентификация по паролю локального администратора admin

Примечание. Для предотвращения подбора пароля учётных записей реализована прогрессивная задержка ввода пароля, оповещение о попытках подбора пароля и временная блокировка учетной записи локального пользователя после 10-ти неудачных попыток ввода пароля.

При успешной аутентификации будет открыта начальная страница сессии пользователя.

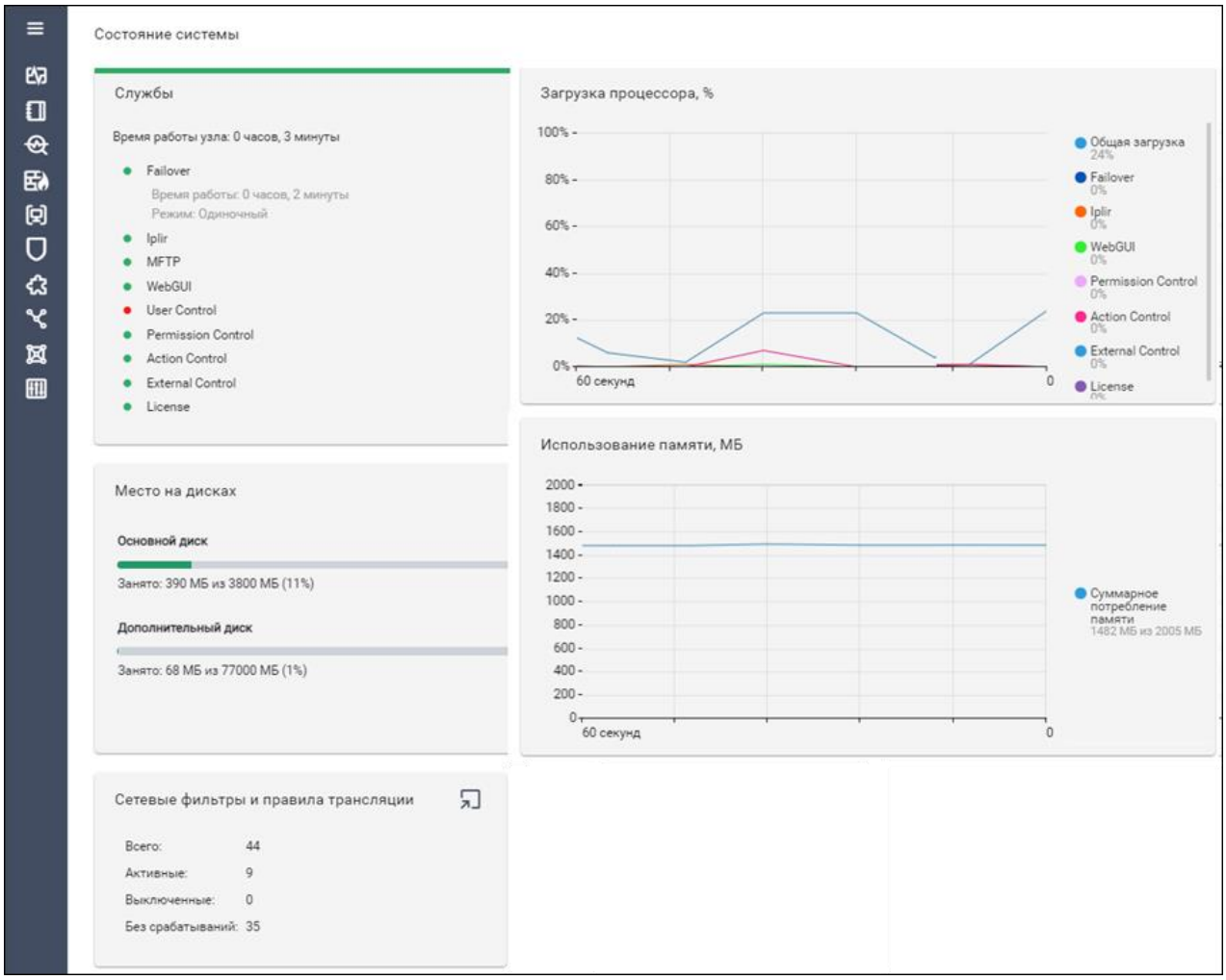


Рисунок 2. Начальная страница сессии локального администратора admin

Примечание. Если на ViPNet Coordinator HW истекают или уже истекли сроки действия ключей аутентификации, защиты или обмена, то на экран будет выведено оповещение, например **Через 7 дня(ей) истечет срок действия вашего ключа аутентификации**. Для продолжения работы нажмите **OK**.

Завершение сессии

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

Настройки подключения

Самоподписанный сертификат необходимо перевыпустить:

- Если истекает срок его действия.
- Если самоподписанный сертификат, установленный по умолчанию, не соответствует политикам безопасности вашей компании.
- Чтобы добавить IP-адреса сетевых интерфейсов и доменные имена, по которым вы будете подключаться.

Вместо самоподписанного сертификата вы можете использовать сертификат, выданный УЦ.

Подробнее о том, как перевыпустить самоподписанный сертификат и использовать сертификат УЦ см. в разделе Настройка подключения к веб-интерфейсу.



2

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet 19

Назначение дополнительных IP-адресов 23

Подключение к мобильной сети 3G/4G 24

Подключение к сети Wi-Fi 26

Обработка трафика из нескольких VLAN 29

Настройка агрегированных сетевых интерфейсов 33

Просмотр ARP-таблицы 39

Настройка сетевых интерфейсов Ethernet

Внимание! Настройка всех сетевых интерфейсов кластера невозможна.

1 Выберите **Сетевые настройки** и нажмите .

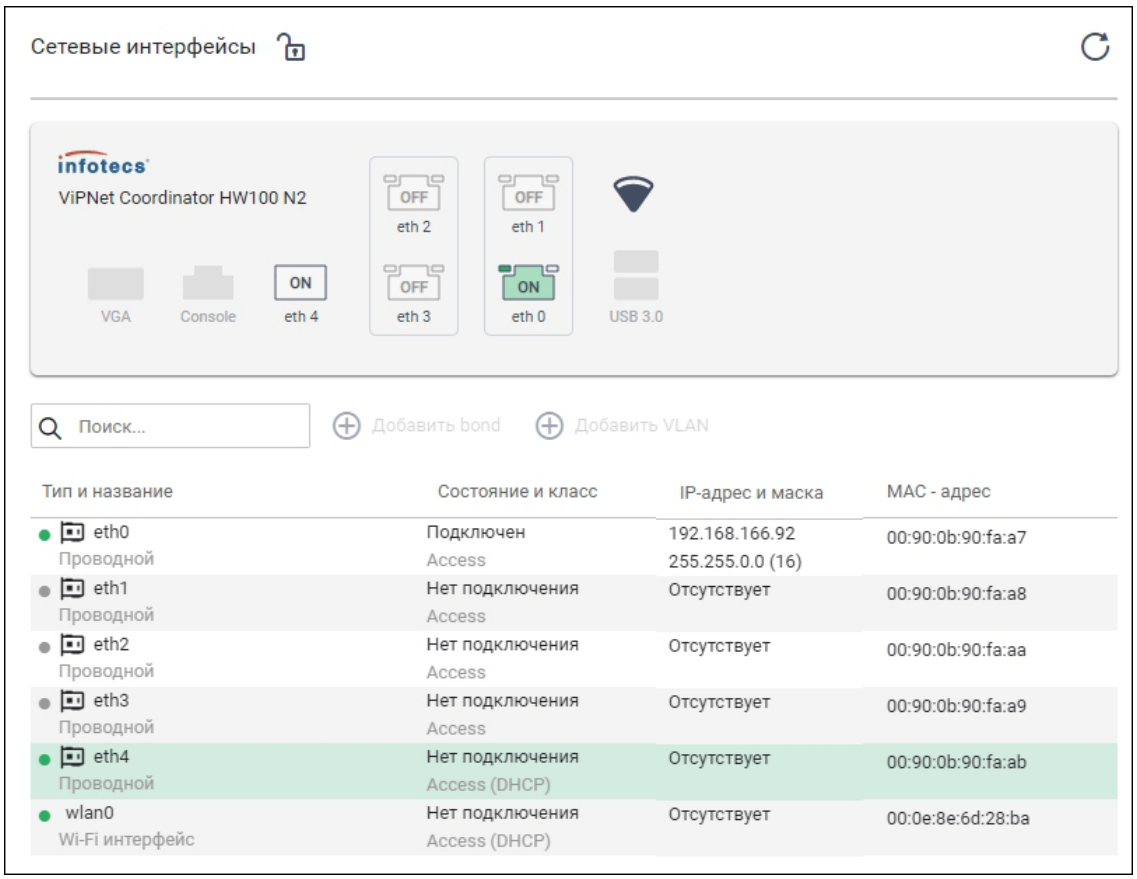


Рисунок 3. Состояние и параметры сетевых интерфейсов

Для исполнений ViPNet Coordinator HW на аппаратных платформах визуально отображается состояние физических интерфейсов:

- интерфейсы Ethernet RJ45 `eth`:
  - OFF — выключен;
  - ON — включен;
  - ON — включен, есть связь с другим сетевым устройством;
  - ON — включен, есть связь с другим сетевым устройством, идет передача данных;
- интерфейсы Ethernet SFP/SFP+ `eth`:

- — выключен;
- — включен, нет связи с другим сетевым устройством;
- — включен, есть связь с другим сетевым устройством;

- — интерфейс синхронизации кластера;
- Wi-Fi интерфейс `wlan`:
  - — выключен;
  - — включен, нет подключения к сети;
  - — включен, сеть подключена;
- интерфейс модема мобильной связи `modem`:
  - — выключен;
  - — включен, нет подключения к сети;
  - — включен, сеть подключена.

2 Щелкните интерфейс, который вы хотите настроить.

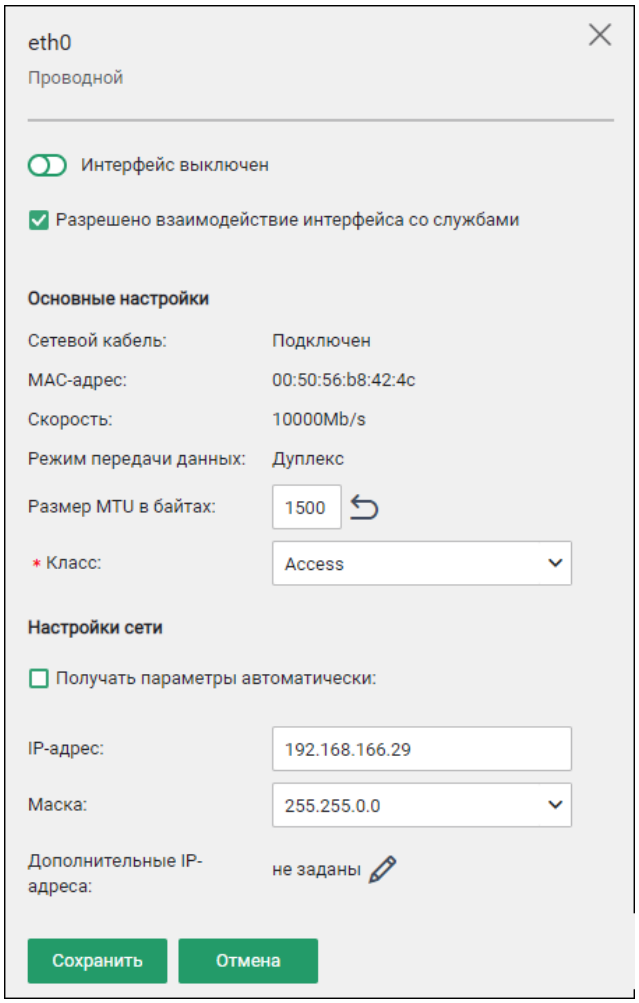


Рисунок 4. Настройка сетевого интерфейса Ethernet

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



Внимание! Для исполнения ViPNet Coordinator VA существуют ограничения:

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

4 Задайте класс интерфейса (по умолчанию — `Access`):

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

5 В разделе **Настройки сети** выполните одно из действий:

- Чтобы присвоить интерфейсу статический IP-адрес, задайте его в полях **IP-адрес** и **Маска**.



Примечание. При задании IP-адреса действуют ограничения:

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

Нажмите ✎, чтобы задать дополнительные IP-адреса интерфейса (см. Назначение дополнительных IP-адресов).

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



Внимание! IP-адрес, получаемый от DHCP-сервера, не должен принадлежать подсетям, в которые входят IP-адреса других интерфейсов ViPNet Coordinator HW.

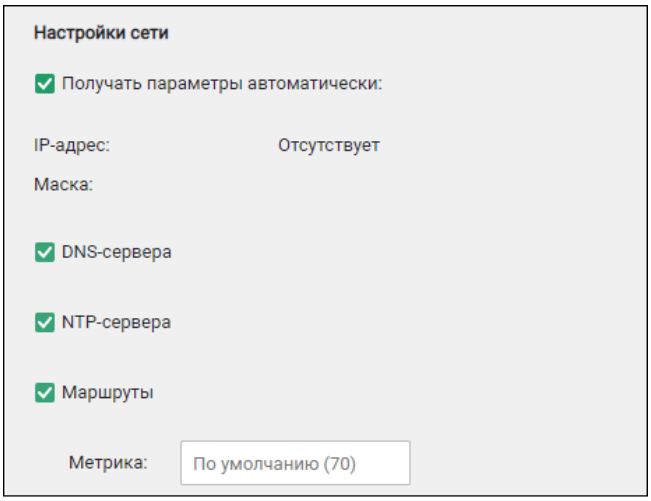


Рисунок 5. Настройка режима получения параметров интерфейса от DHCP-сервера

В этом режиме вы можете задать дополнительные параметры:

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

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (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.

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

6 Включите интерфейс.

7 Нажмите **Сохранить**.

8 Нажмите .

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 определяется исполнением ViPNet Coordinator HW. Подробнее см. документ «Подготовка к работе», раздел «Функциональные ограничения исполнений».

Чтобы задать дополнительные IP-адреса:

1. Выберите **Сетевые настройки** и нажмите .
2. Выберите нужный интерфейс.
3. В разделе **Настройки сети** нажмите .
4. Нажмите **Добавить**.
5. Задайте IP-адрес и маску подсети, затем нажмите .
6. Чтобы добавить ещё один дополнительный IP-адрес, повторите шаги 4 и 5.
7. Нажмите **Сохранить**.

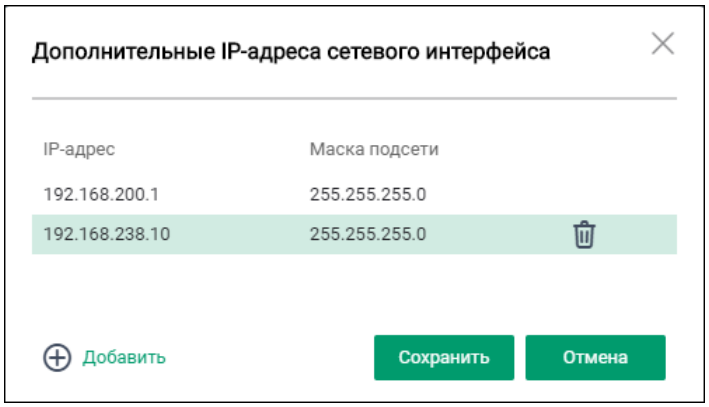


Рисунок 6. Назначение дополнительных IP-адресов

8. Нажмите **Сохранить**.
9. Нажмите .

Подключение к мобильной сети 3G/4G

Подключение к мобильной сети 3G/4G по протоколу PPP доступно на аппаратных платформах со встроенным модемом:

- HW50 A1 (если модем входит в комплект поставки);
- HW50 N3;
- HW100 N3.

До начала работы подключите необходимые услуги мобильного оператора и установите SIM-карту (см. документ «Подготовка к работе», раздел «Установка SIM-карты»).

Чтобы настроить подключение к мобильной сети:

1 Выберите **Сетевые настройки** и нажмите .

2 В списке интерфейсов щелкните интерфейс **ppp0**.

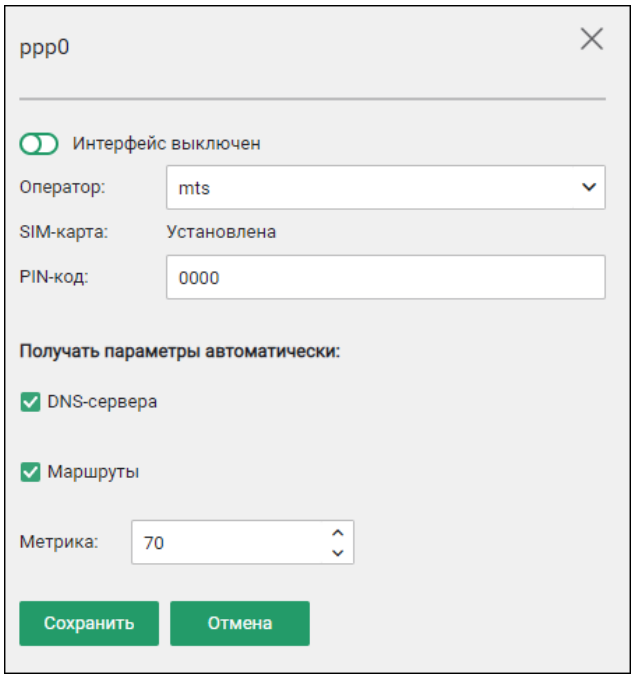


Рисунок 7. Настройка модема

3 Если интерфейс включен, выключите его.

4 В списке **Оператор** выберите название оператора, SIM-карту которого вы установили.

5 Если SIM-карта защищена, введите PIN-код.

6 При подключении к сети на ViPNet Coordinator HW, в зависимости от оператора, могут передаваться:

- Маршрут по умолчанию в сеть оператора.
- IP-адрес DNS-сервера оператора.

В разделе **Получать параметры автоматически**, в зависимости от маршрутизации в вашей сети, настройте обработку маршрута по умолчанию и адреса DNS-сервера, передаваемых оператором:

- Чтобы не получать адрес DNS-сервера, снимите флажок **DNS-сервера**.
- Чтобы не получать маршрут по умолчанию, снимите флажок **Маршруты**.
- Если вы хотите задать для маршрута по умолчанию другую метрику, укажите ее в поле **Метрика**. Подробнее см. Настройка метрики для маршрутов PPP-протокола.

7 Нажмите **Сохранить**.

8 Включите  интерфейс. Подключение может занять несколько минут:

- Если соединение с сетью 3G/4G не установится, обновите страницу настройки модема.
- Если в выводе присутствуют сообщения о неверном PIN-коде или отсутствующей (поврежденной) SIM-карте, выключите интерфейс, устраните причину ошибки (вставьте или замените SIM-карту, задайте правильный PIN-код) и заново включите интерфейс.

9 Нажмите  .

Подключение к сети Wi-Fi

Подключение ViPNet Coordinator HW к сети Wi-Fi возможно только в исполнениях со встроенными Wi-Fi-модулями:

- ViPNet Coordinator HW HW50 A, B на аппаратной платформе HW50 N2;
- ViPNet Coordinator HW HW100 C на аппаратной платформе HW100 N2.

ViPNet Coordinator HW может также работать в качестве точки доступа сети Wi-Fi (см. Настройка точки доступа сети Wi-Fi). Использование ViPNet Coordinator HW одновременно в качестве клиента и точки доступа Wi-Fi не поддерживается.

Чтобы настроить подключение:

1 Выберите **Сетевые настройки** и нажмите .

2 Щелкните интерфейс Wi-Fi (`wlan0`).

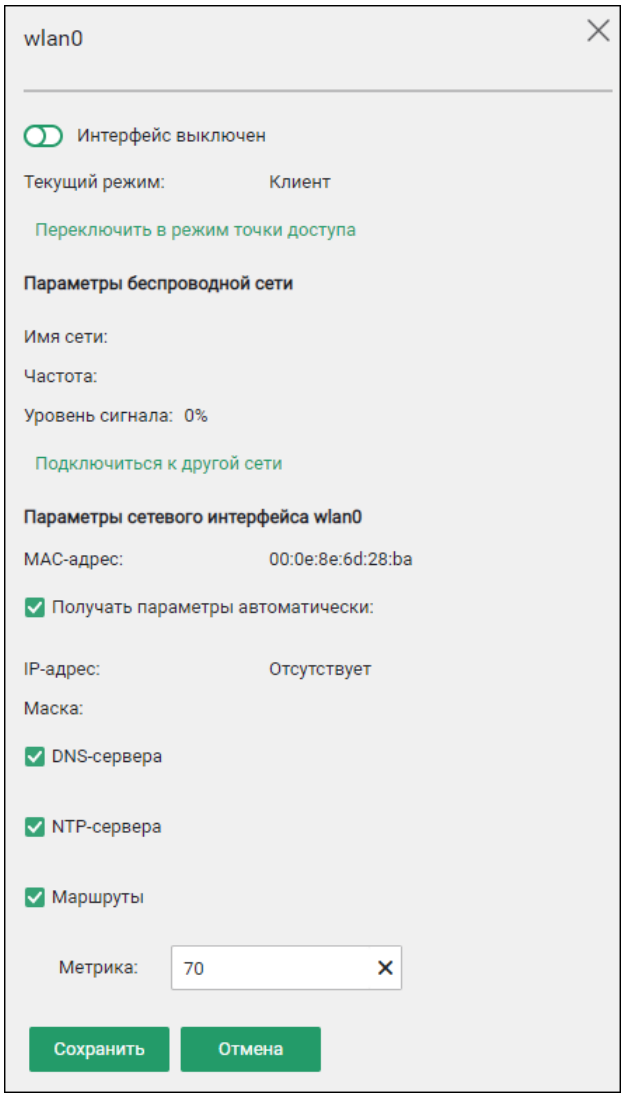


Рисунок 8. Настройка интерфейса Wi-Fi

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

4 Интерфейс Wi-Fi работает в режиме автоматического получения параметров от DHCP-сервера:

4.1 Задайте дополнительные параметры, получаемые от DHCP-сервера: адреса DNS-серверов, адреса NTP-серверов, маршруты и метрику.

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

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

4.2 Нажмите **Сохранить**.

5 Нажмите **Подключиться к другой сети**.

6 В списке доступных сетей Wi-Fi щелкните сеть, к которой вы хотите подключиться.

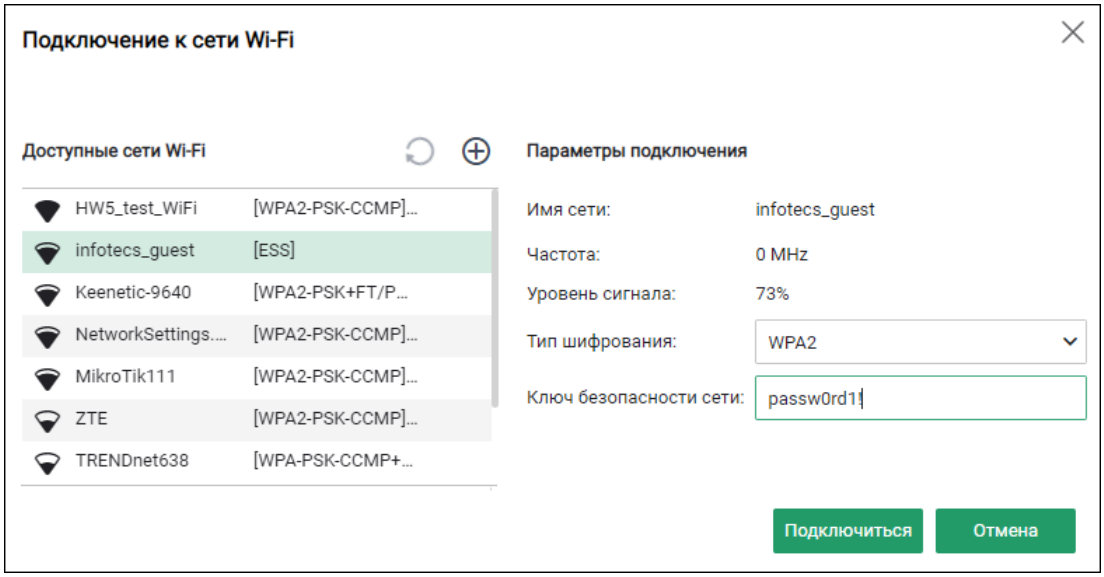


Рисунок 9. Подключение к сети Wi-Fi

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

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

8.1 Нажмите ⊕.

8.2 В разделе **Параметры подключения** укажите имя, тип шифрования и пароль доступа к скрытой сети.

8.3 Нажмите **Подключиться**.

9 В окне настроек интерфейса Wi-Fi нажмите **Сохранить**.

10 Включите интерфейс Wi-Fi.

11 Нажмите .

Обработка трафика из нескольких VLAN

Вы можете использовать ViPNet Coordinator HW 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 — родительский интерфейс — к коммутатору, объединяющему виртуальные сети.

2 Выберите **Сетевые настройки** и нажмите .

3 Щелкните родительский интерфейс.

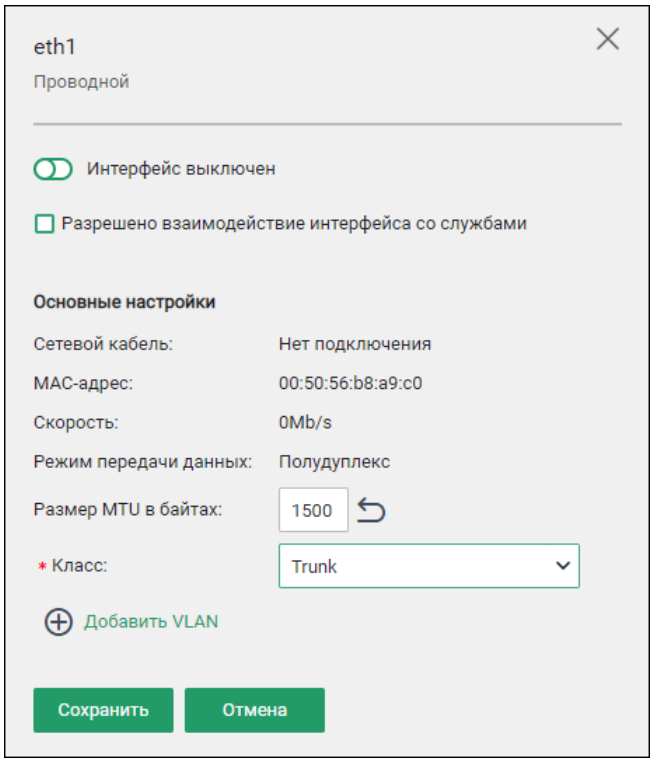


Рисунок 10. Настройка родительского интерфейса

4 Снимите флажок **Разрешено взаимодействие интерфейса со службами**.

5 В списке **Класс** выберите **Trunk** и нажмите **Сохранить**.

6 Нажмите **Добавить VLAN**.

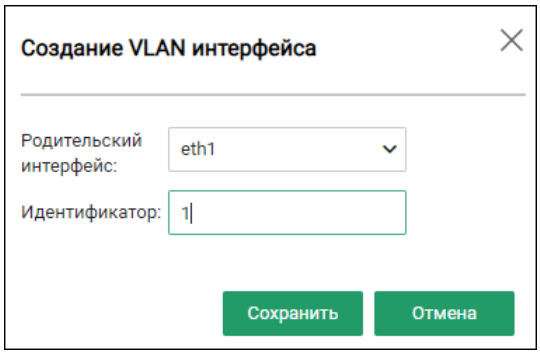


Рисунок 11. Создание VLAN-интерфейса

6.1 В списке **Родительский интерфейс** отображаются интерфейсы класса `Trunk`. Если таких интерфейсов несколько, выберите нужный вам.

6.2 В поле **Идентификатор** введите номер создаваемого VLAN-интерфейса. Создаваемому VLAN-интерфейсу будет присвоено имя в формате:

`<физический интерфейс>.<номер VLAN-интерфейса>`

6.3 Нажмите **Сохранить**.

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

7 В списке интерфейсов щелкните созданный VLAN-интерфейс и настройте его:

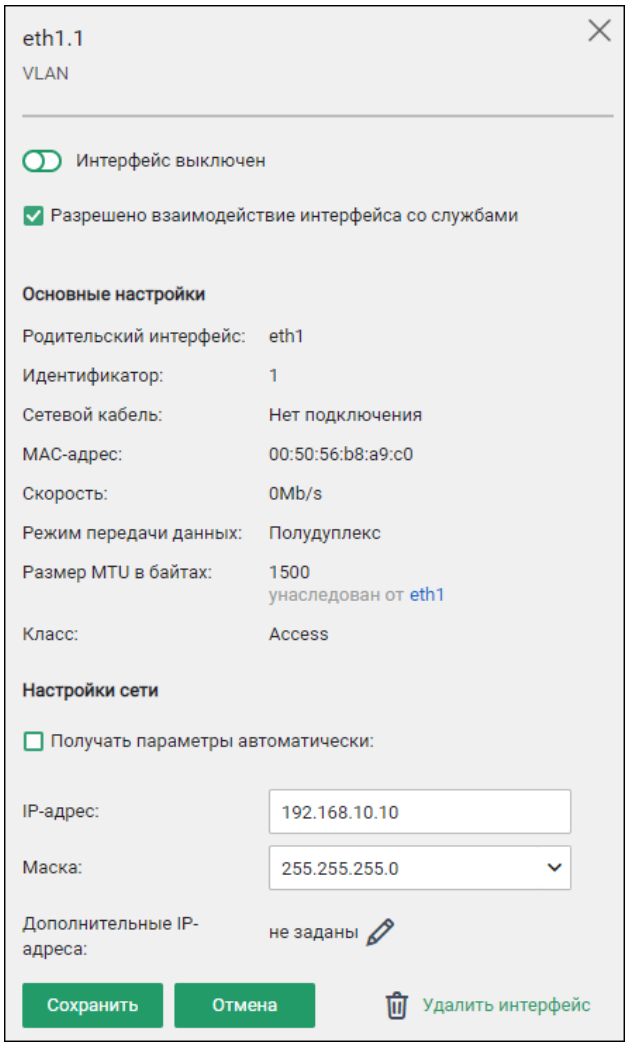


Рисунок 12. Настройка VLAN-интерфейса

7.1 Чтобы включить прохождение трафика через VLAN-интерфейс, установите флажок **Разрешено взаимодействие интерфейса со службами**.

7.2 В разделе **Настройки сети** выполните одно из действий:

- Чтобы присвоить интерфейсу статический IP-адрес, задайте его в полях **IP-адрес** и **Маска**.

  Нажмите , чтобы задайте дополнительные IP-адреса интерфейса (см. Назначение дополнительных IP-адресов).

- Чтобы включить режим автоматического получения параметров интерфейса от DHCP-сервера, установите флажок **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.

7.3 Нажмите **Сохранить**.

8 Чтобы создать VLAN-интерфейсы для других сетей, повторите шаги 6 и 7.

9 Для передачи данных через VLAN-интерфейс используется размер MTU, унаследованный от родительского интерфейса. Чтобы оптимизировать передачу данных, вы можете изменить размер MTU родительского интерфейса. Для этого откройте окно настроек интерфейса и в поле **Размер MTU в байтах** задайте новое значение из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию (1500 байт), нажмите ⮌.

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

Для исполнения ViPNet Coordinator VA существуют ограничения:

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

---

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

Созданные VLAN-интерфейсы включатся автоматически.

11 Нажмите .

Настройка агрегированных сетевых интерфейсов

Чтобы увеличить пропускную способность сетевых интерфейсов ViPNet Coordinator HW или повысить надежность канала связи, вы можете объединить несколько физических сетевых интерфейсов в один логический — агрегированный сетевой интерфейс. При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

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

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

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

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



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

Режимы работы агрегированного интерфейса

В ViPNet Coordinator HW 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; • `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.

`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 HW 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.

`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** и нажмите .

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

3 Нажмите **Добавить bond**.

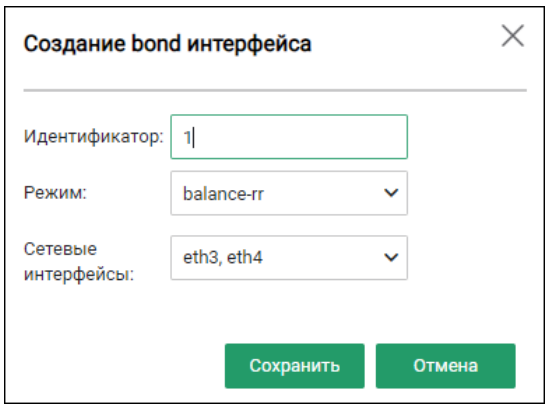


Рисунок 13. Создание агрегированного интерфейса

4 Задайте основные параметры агрегированного интерфейса:

4.1 В поле **Идентификатор** задайте номер. Вы можете создать до восьми агрегированных интерфейсов с номерами 0, 1, 2, 3, 4, 5, 6, 7. Созданный агрегированный интерфейс будет иметь имя `bond<номер>`.

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

4.3 В списке **Сетевые интерфейсы** последовательно выберите физические интерфейсы класса `slave`, которые вы хотите объединить. Эти интерфейсы станут подчиненными для создаваемого агрегированного интерфейса. Ограничения на количество подчиненных интерфейсов нет. При создании агрегированного интерфейса необходимо выбрать не менее одного подчиненного интерфейса.

4.4 Нажмите **Сохранить**.

5 В списке интерфейсов щелкните созданный агрегированный интерфейс и настройте его:

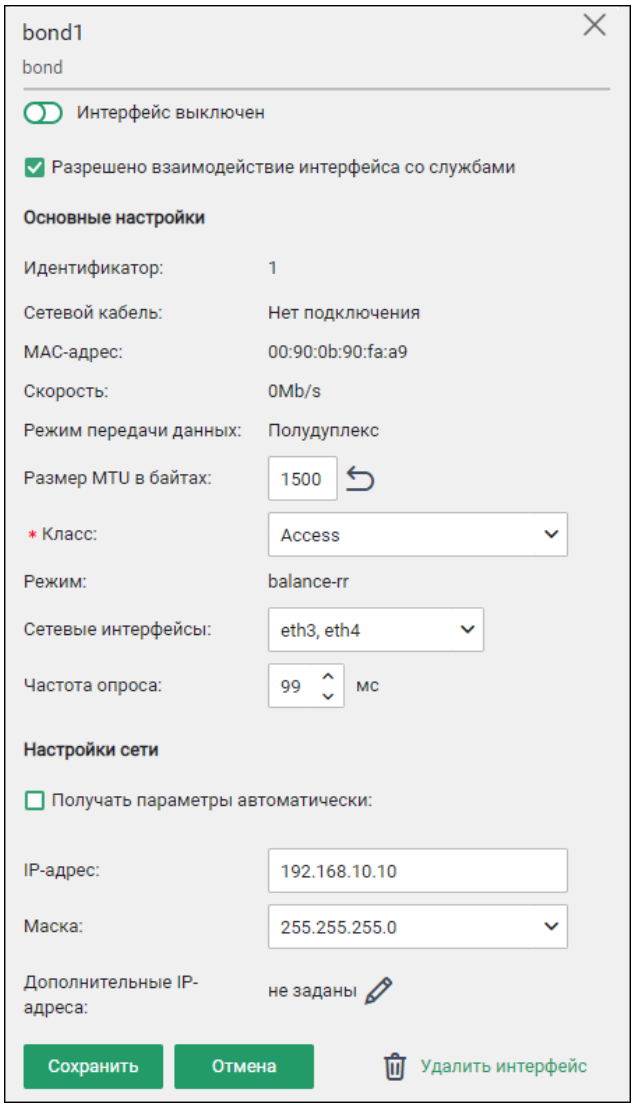


Рисунок 14. Настройка агрегированного интерфейса

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

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

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

5.4 В разделе **Настройки сети** выполните одно из действий:

- Чтобы присвоить интерфейсу статический IP-адрес, задайте его в полях **IP-адрес** и **Маска**.

  Нажмите , чтобы задайте дополнительные IP-адреса интерфейса (см. Назначение дополнительных IP-адресов).

- Чтобы включить режим автоматического получения параметров интерфейса от DHCP-сервера, установите флажок **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.

5.5 Нажмите **Сохранить**.

6 Для передачи данных через агрегированный интерфейс используется размер MTU, равный 1500 байт. Чтобы оптимизировать передачу данных через интерфейс, вы можете изменить размер MTU. Для этого откройте окно настроек интерфейса и в поле **Размер MTU в байтах** задайте новое значение MTU из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию (1500 байт), нажмите ⮌. Подчиненные интерфейсы наследуют MTU агрегированного интерфейса.

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

Для исполнения ViPNet Coordinator VA накладываются ограничения:

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

---

7 Последовательно включите подчиненные физические интерфейсы, а затем агрегированный интерфейс.

8 Нажмите .

Просмотр ARP-таблицы

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

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

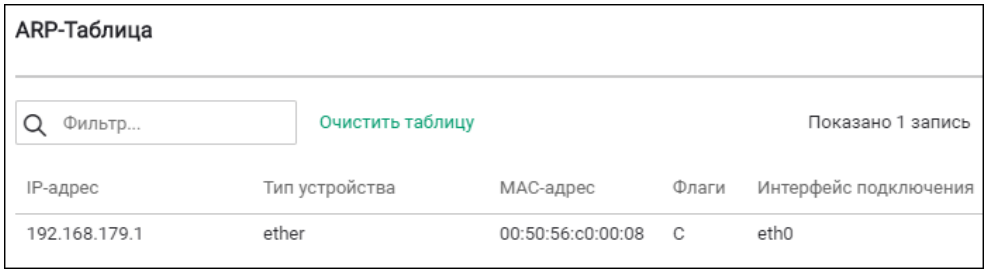


Рисунок 15. Просмотр ARP-таблицы

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

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

3 В случае сетевых сбоев вы можете очистить ARP-таблицу.



3

Настройка VPN

Просмотр сведений об узлах ViPNet 41

Настройка видимости узлов 44

Настройка туннелирования на сетевом уровне 47

Настройка туннелирования на канальном уровне 51

Просмотр сведений об узлах ViPNet

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

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

На вкладке **Узлы** отображается список сетевых узлов, с которыми у вашего узла есть связь, а также время последней активности этих узлов.

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 HW до перезапуска службы `iplircfg` и отображается, даже если узел выключен.

Типы узлов:

- — клиенты ViPNet;
- — координаторы ViPNet;

Недоступные узлы или узлы, статус которых неизвестен, отображаются серым цветом.

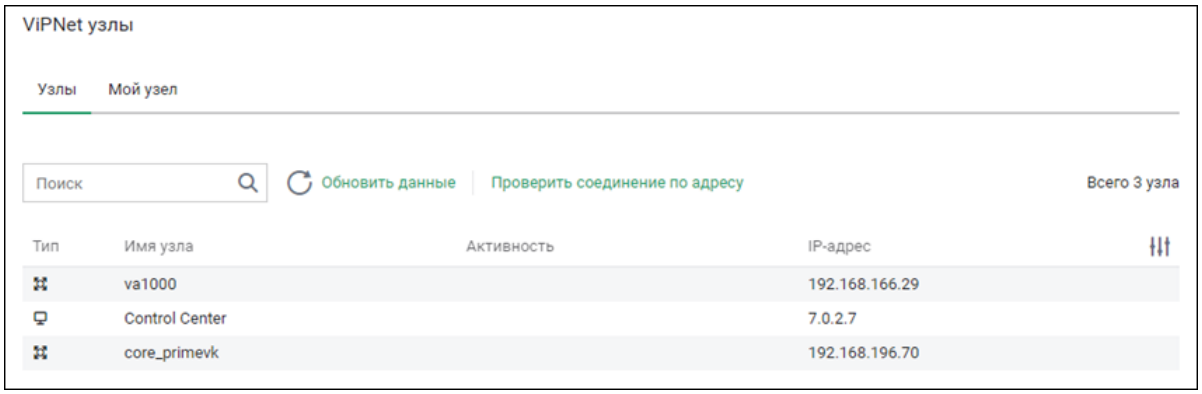


Рисунок 16. Просмотр списка узлов ViPNet

2 Чтобы просмотреть подробные сведения об узле, щелкните его в списке. Сведения содержат:

- общая информация: статус соединения, имя узла, версии 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 ViPNet);
- настройки туннелирования (для координаторов ViPNet).

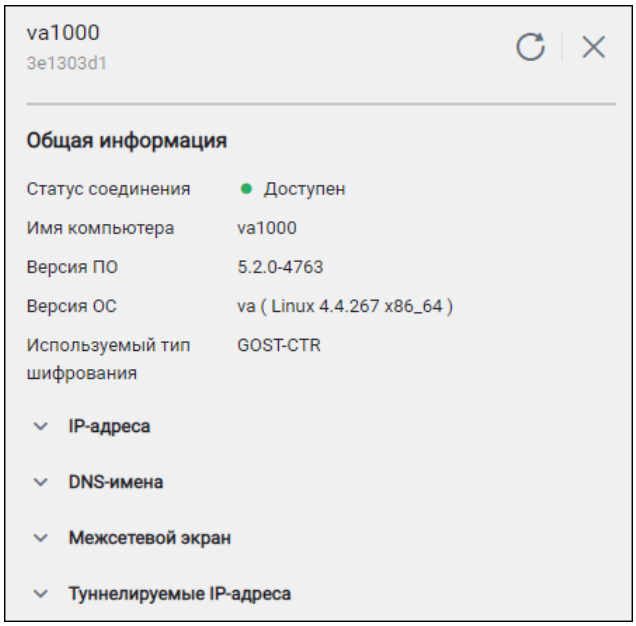


Рисунок 17. Просмотр сведений об узле ViPNet

Внимание! Если статус координатора ViPNet отображается некорректно, проверьте параметр `server_pollinterval` в секции `[misc]` файла `iplir.conf`. Значение параметра должно быть одинаковым для всех координаторов сети.

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

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

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

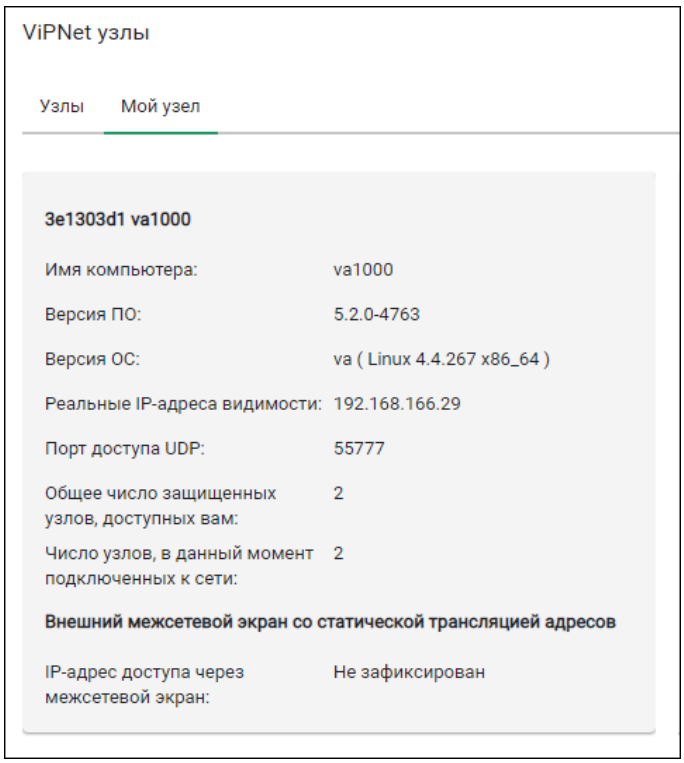


Рисунок 18. Просмотр сведений о собственном узле ViPNet

Настройка видимости узлов

При подключении удаленных пользователей к ресурсам локальной сети или при межсетевом взаимодействии через VPN-туннели может возникать пересечение IP-адресов. Например, два сетевых узла, находящиеся в разных сетях, могут иметь одинаковые частные IP-адреса. Виртуальные IP-адреса позволяют решить эту проблему без изменения текущей адресной структуры сетей.

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

По умолчанию на ViPNet Coordinator HW используются следующие настройки видимости:

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

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

Чтобы настроить видимость узлов ViPNet:

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

2 В списке выберите узел.

3 В разделе **IP-адреса** в поле **IP-адреса видимости** выберите тип видимости узла: **Реальные** или **Виртуальные**.

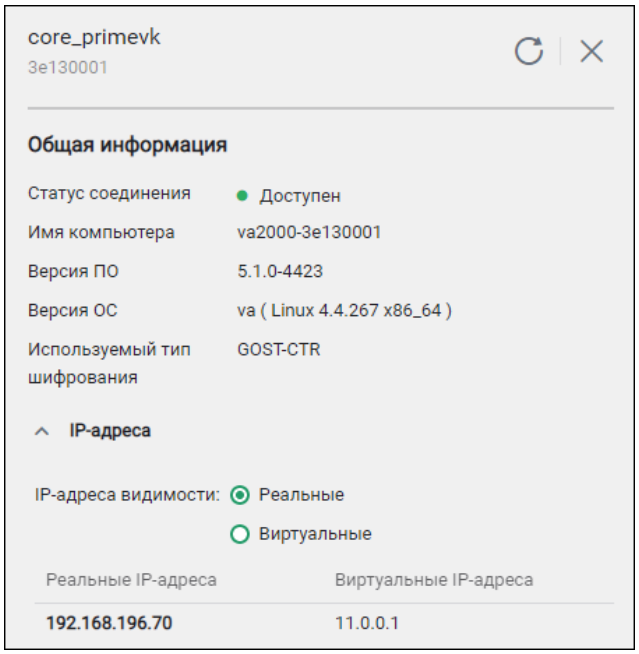


Рисунок 19. Настройка видимости узлов защищённой сети

Чтобы настроить видимость туннелируемых IP-адресов:

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

2 В списке выберите туннелирующий координатор, для которого надо настроить видимость туннелируемых IP-адресов.

3 В разделе **Туннелируемые IP-адреса** в поле **IP-адреса видимости** выберите тип видимости узла: **Реальные** или **Виртуальные**.

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

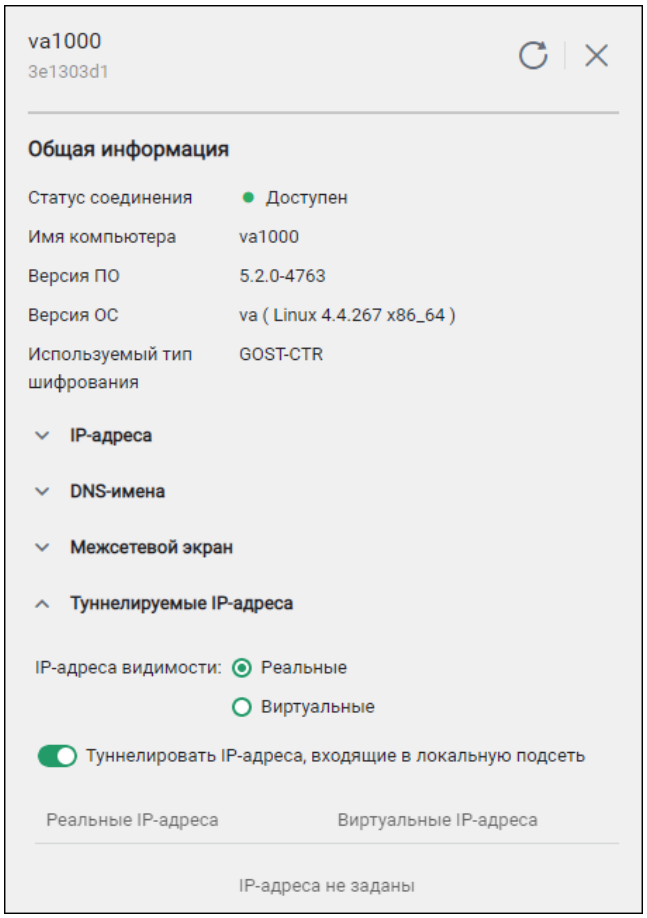


Рисунок 20. Настройка видимости туннелируемых IP-адресов

Настройка туннелирования на сетевом уровне

Общие сведения о туннелировании

Туннелирование применяется для защиты IP-трафика на потенциально опасном участке сети и для доступа к открытому узлу. Туннелирование предполагает направление IP-трафика узла не напрямую на другой узел, а через координатор, где трафик фильтруется и защищается криптографическими методами. Также настройки туннелирования открытых узлов, которые задает администратор сети ViPNet, хранятся на координаторах сети ViPNet, 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 HW работает в условиях отсутствия связи с ViPNet Prime, вы можете настроить туннелирование локально на ViPNet Coordinator HW (см. Ручная настройка туннелирования). Затем IP-адреса туннелируемых узлов необходимо задать вручную на каждом связанном координаторе.

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

- если с настройками туннелирования из ViPNet Prime получены новые IP-адреса туннелируемых узлов, то они добавляются в ViPNet Coordinator HW;
- если заданные локально IP-адреса туннелируемых узлов были удалены из настроек туннелирования, полученных из ViPNet Prime, то эти IP-адреса будут удалены.

После изменения настроек туннелирования может возникнуть конфликт между реальными IP-адресами узлов из широковещательного сегмента вашего ViPNet Coordinator HW и реальными IP-адресами узлов, туннелируемых удаленным координатором, или между реальными IP-адресами туннелируемых узлов. Чтобы устранить возможные конфликты, на координаторе, туннелирующем узлы с конфликтующими IP-адресами, задайте видимость туннелируемых узлов по виртуальным IP-адресам.

Ручная настройка туннелирования

При наличии лицензии на туннелирование хотя бы одного соединения вы можете просматривать информацию о количестве туннелируемых узлов, а также просматривать и добавлять IP-адреса сетевых узлов, туннелируемых ViPNet Coordinator HW вручную.

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

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

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

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

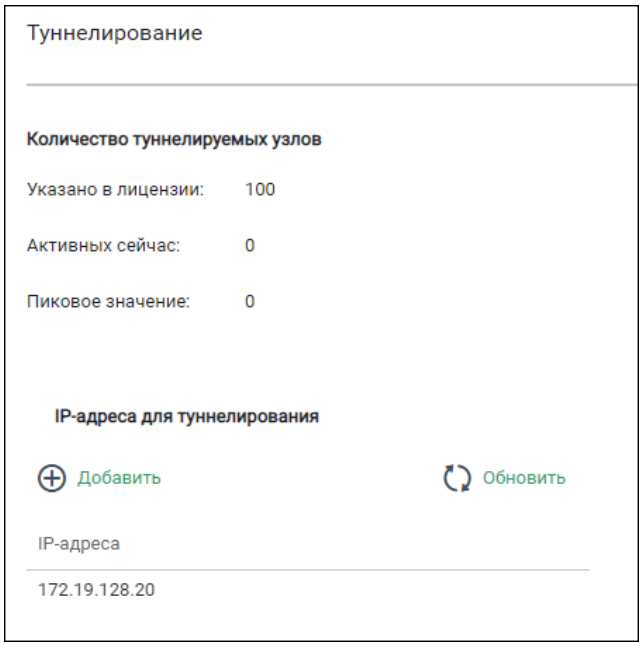


Рисунок 21. Просмотр информации о туннелируемых узлах

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

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

Настройка доступа к туннелируемым узлам в одной подсети

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

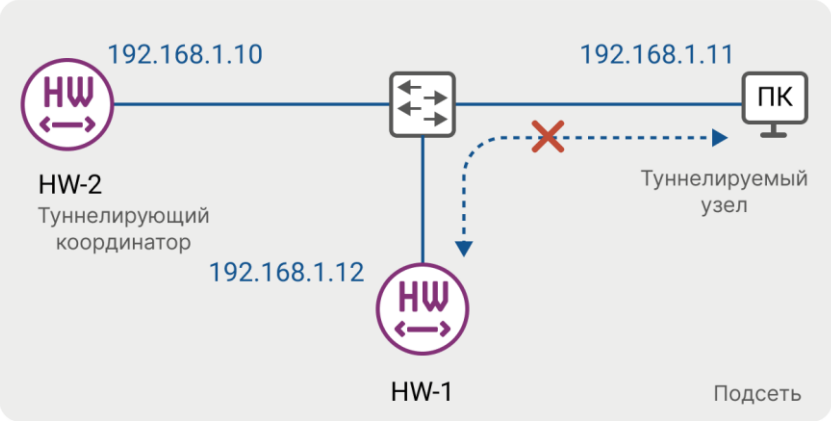


Рисунок 22. Трафик между ПК и HW-1 заблокирован

Чтобы ViPNet Coordinator HW мог обращаться к туннелируемому узлу напрямую, как к открытому, исключите узлы, туннелируемые другим координатором, из списка туннелируемых узлов ViPNet Coordinator HW:

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

2 В списке выберите туннелирующий координатор.

3 В разделе **Туннелируемые IP-адреса** выключите **Туннелировать IP-адреса, входящие в локальную подсеть**.

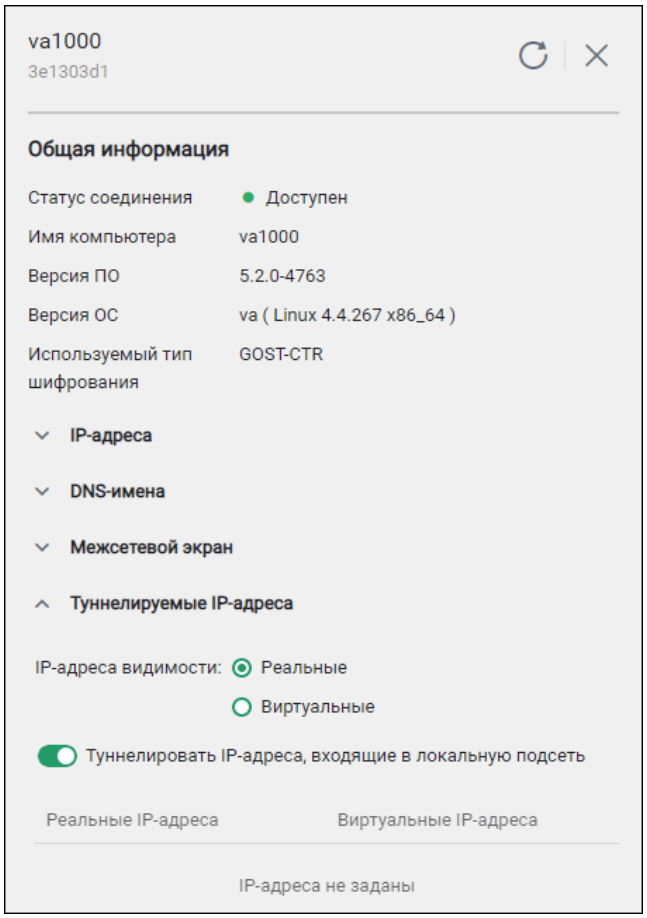


Рисунок 23. Настройка доступа к туннелируемым узлам напрямую

Настройка туннелирования на канальном уровне

Общие сведения о L2OverIP

ViPNet Coordinator HW поддерживает технологию L2OverIP, которая позволяет объединять удалённые сегменты сети на канальном уровне модели OSI так, что их узлы находятся в одном широковещательном домене.

L2OverIP предполагает взаимодействие между узлами нескольких удалённых сегментов сети через ViPNet Coordinator HW, которые установлены на границах этих сегментов. ViPNet Coordinator HW перехватывает Ethernet-кадры, отправляемые из его сегмента сети в другой, упаковывает их в зашифрованные IP-пакеты и передаёт их другому ViPNet Coordinator HW, который, в свою очередь, расшифровывает поступившие IP-пакеты, извлекает из них исходные кадры и передаёт получателям в своем сегменте.

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

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



Внимание! В исполнении HW50 технология L2OverIP поддерживается только на сетевых интерфейсах класса `access`.

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 HW работает как виртуальный сетевой коммутатор, хранящий в памяти таблицу MAC-адресов сетевых узлов, от которых поступает сетевой трафик.

Каждому сегменту сети назначается свой номер порта, который задается в настройках L2OverIP. Порт, заданный для собственного сегмента сети, называется локальным. Порты, заданные на ViPNet

Coordinator HW в других сегментах, называются удаленными. Трафик самого ViPNet Coordinator HW всегда относится к порту с номером 0.

Виртуальный коммутатор может по-разному обрабатывать одноадресные Ethernet-кадры с неизвестным MAC-адресом получателя: блокировать либо обрабатывать как многоадресные с рассылкой на все удаленные порты. Последняя возможность позволяет использовать L2OverIP для схемы, когда два ViPNet Coordinator HW объединены с помощью агрегированного канала и каждый из физических каналов работает через свою пару ViPNet Coordinator HW. Кадры, которыми обмениваются два узла из разных сегментов, могут в одном направлении постоянно пересылаться через одну пару ViPNet Coordinator HW, а в другом направлении — через другую. В этом случае адрес получателя кадров будет определяться как неизвестный, и для обработки пакетов многоадресной рассылки следует использовать режим `smart-broadcast` (см. Настройка L2OverIP).

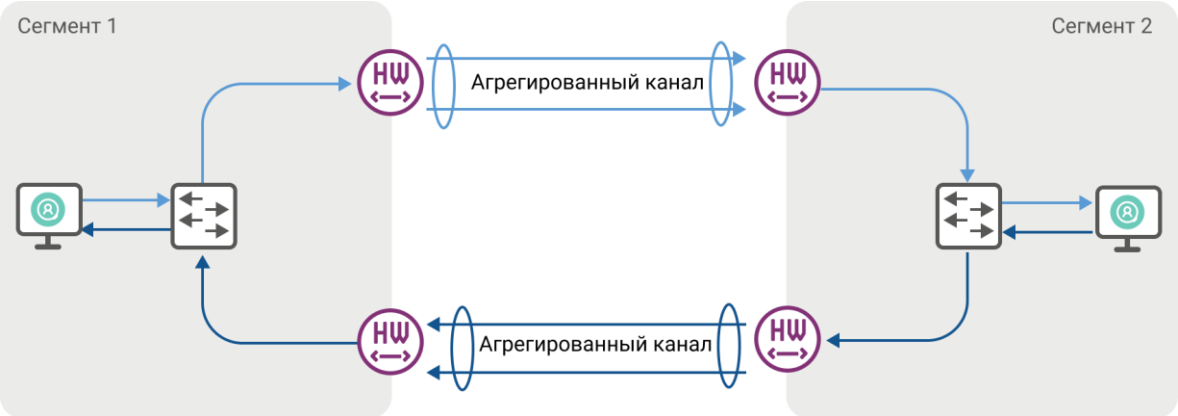


Рисунок 24. Схема работы сети с парами ViPNet Coordinator HW, объединенных с помощью агрегированных каналов

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

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

Настройка L2OverIP в кластере выполняется на активном узле. При переключении узлов кластера таблица MAC-адресов не передается пассивному узлу. Коммутация кадров восстановится, когда узлы из разных сегментов, взаимодействующие друг с другом, заново отправят ARP-запросы.

Особенности реализации L2OverIP

- Сегменты сети, объединяемые по L2OverIP, должны быть изолированы друг от друга. Сетевое взаимодействие между ними должно осуществляться только по каналам связи между ViPNet Coordinator HW, установленными на границах объединяемых сегментов.

- ViPNet Coordinator HW позволяет объединять не более 31 сегмента сети.
- Используйте не более 252 IP-адресов во всех объединяемых сегментах сети. Превышение этого количества может привести к снижению пропускной способности сети в связи с возрастанием служебного трафика в широковещательном домене.
- Для исполнения ViPNet Coordinator VA в настройках платформы виртуализации включите неразборчивый режим (Promiscuous Mode) на интерфейсе, к которому привязан адаптер виртуальной машины.
- Поиск IP-пакетов, переданных по L2OverIP, в журнале IP-пакетов необходимо выполнять по признакам исходных IP-пакетов: IP-адрес источника и получателя, номер TCP- и UDP-порта, интерфейс.

Настройка L2OverIP

При настройке туннелирования удаленных сегментов сети на канальном уровне каждый сегмент подключается к одному из сетевых интерфейсов ViPNet Coordinator HW, установленному на границе сегмента. Если сегмент сети состоит из нескольких VLAN, они должны быть объединены с помощью коммутатора в транковый порт, к которому подключается один из сетевых интерфейсов ViPNet Coordinator HW (см. Обработка трафика из нескольких VLAN).

Чтобы настроить L2OverIP, на каждом ViPNet Coordinator HW:

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

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

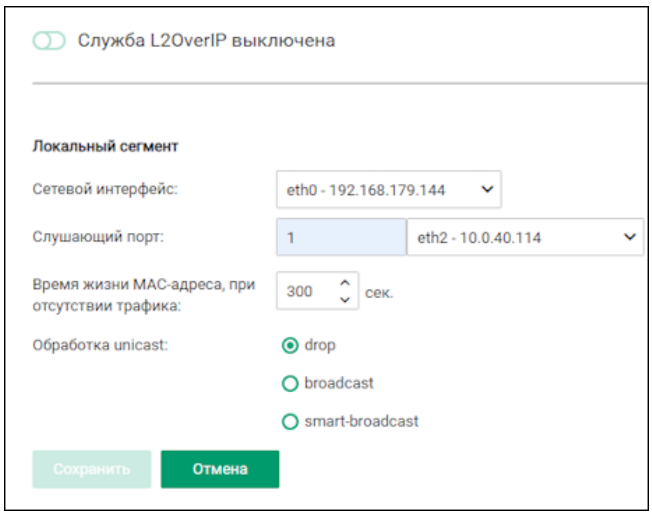


Рисунок 25. Настройка параметров соединения L2OverIP

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

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

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

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

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

7 Задайте параметры удаленного сегмента сети:

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

7.2 Укажите IP-адрес и порт удаленного сегмента сети.

7.3 Нажмите 💾.

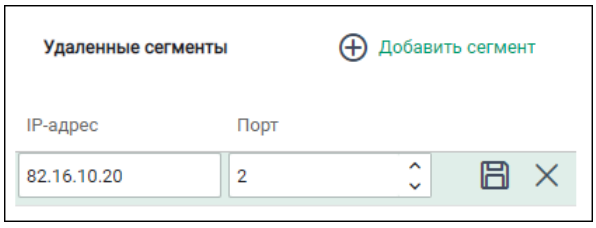


Рисунок 26. Добавление удалённого сегмента сети при создании соединения L2OverIP

8 Добавьте сетевой фильтр защищенной сети, разрешающий любые соединения по протоколу 97.

9 Нажмите **Сохранить**.

10 Включите службу L2OverIP.

Внимание! На двух ViPNet Coordinator HW, соединенных по L2OverIP, IP-адреса локального и удаленного сегментов должны быть настроены симметрично: на каждом ViPNet Coordinator HW в качестве IP-адреса удаленного сегмента должен быть указан IP-адрес видимости сетевого интерфейса, который задан на втором ViPNet Coordinator HW в качестве внешнего интерфейса локального сегмента.

4

Настройка межсетевого экрана

О фильтрации трафика 56

Объекты сетевых фильтров и правил трансляции адресов 63

Настройка SSL/TLS-инспекции трафика 83

Настройка подключения к ICAP-серверам 92

Настройка сетевых фильтров 95

Настройка правил трансляции адресов 111

Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP 118

Настройка блокировки трафика по списку IP-адресов 124

О фильтрации трафика

Типы трафика

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

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

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

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

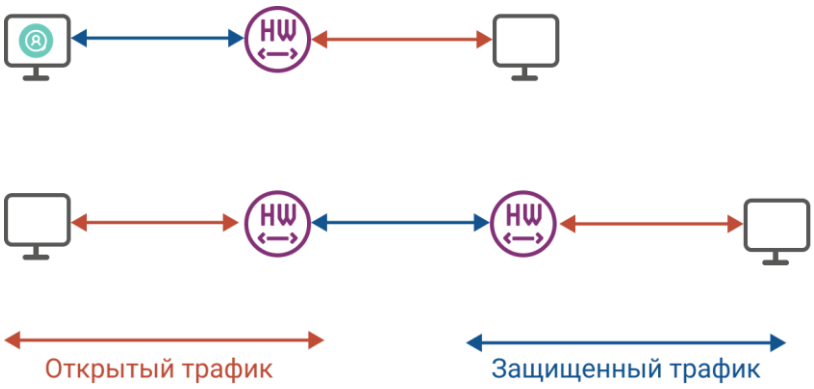


Рисунок 27. Туннелируемый трафик

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



Рисунок 28. Открытый транзитный трафик

Для каждого типа трафика можно настроить соответствующие сетевые фильтры.

Принципы фильтрации трафика

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

Внимание! TCP-порт 2047 и UDP-порт 2046 являются служебными портами ViPNet Coordinator HW, поэтому входящий открытый трафик, поступающий на эти порты, блокируется.

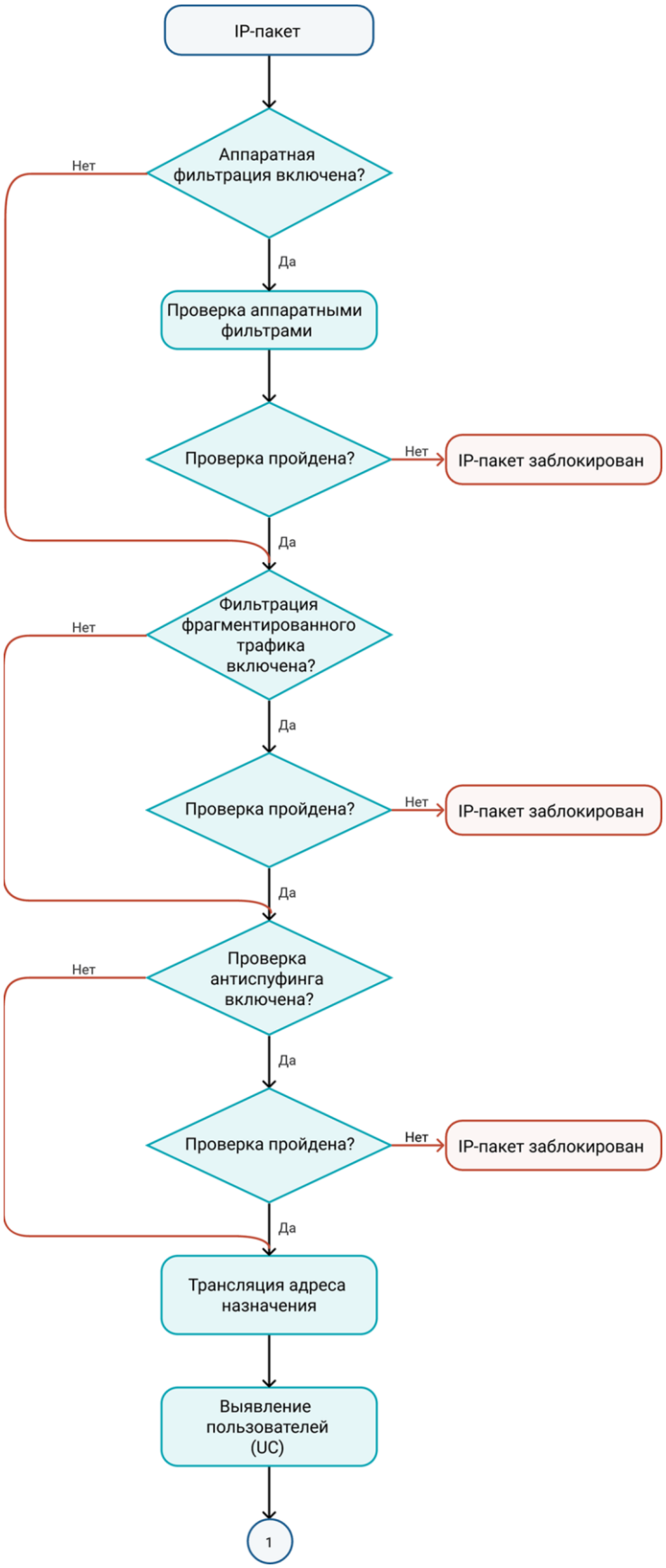


Рисунок 29. Схема фильтрации трафика. Часть 1

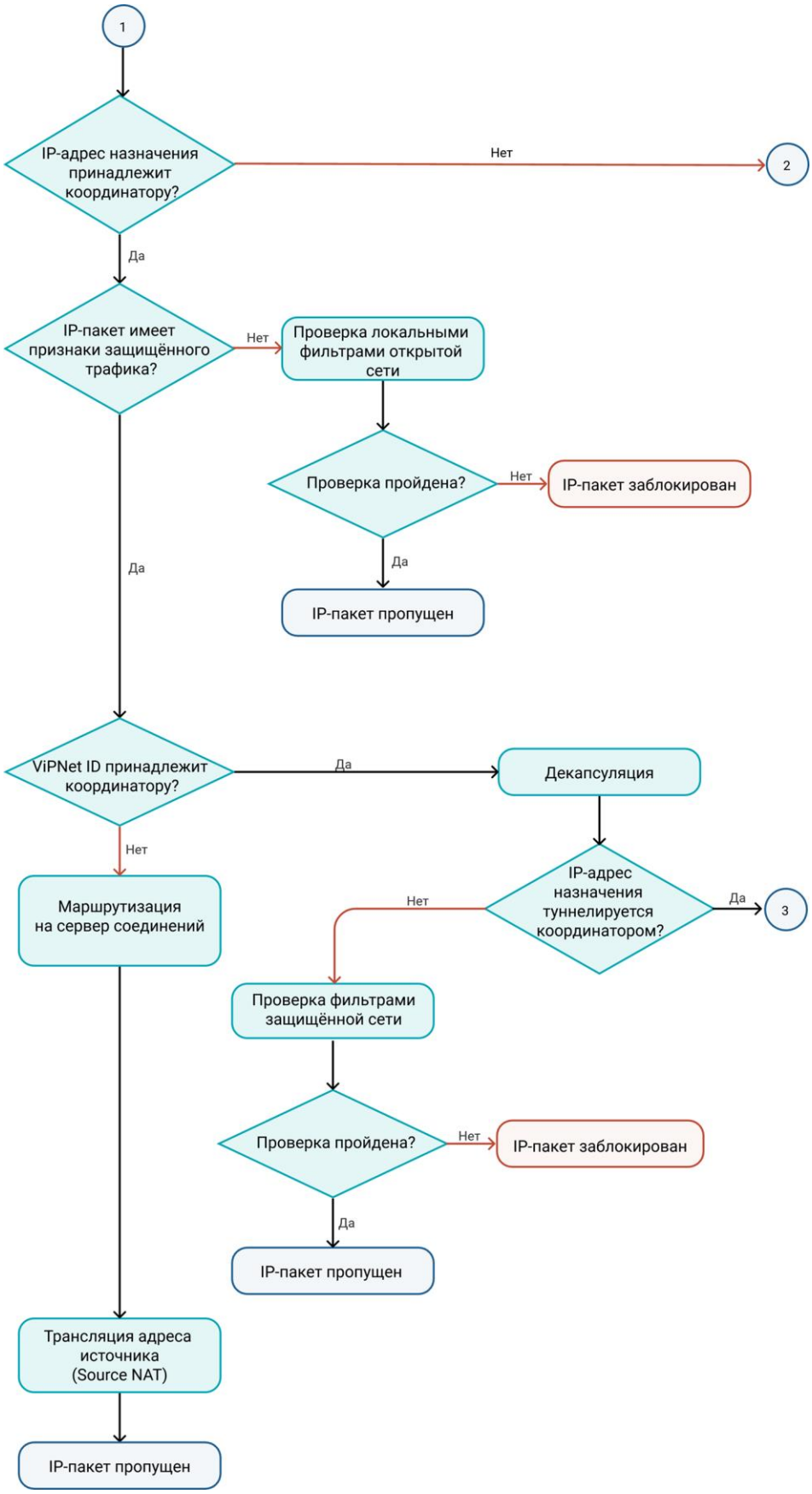


Рисунок 30. Схема фильтрации трафика. Часть 2

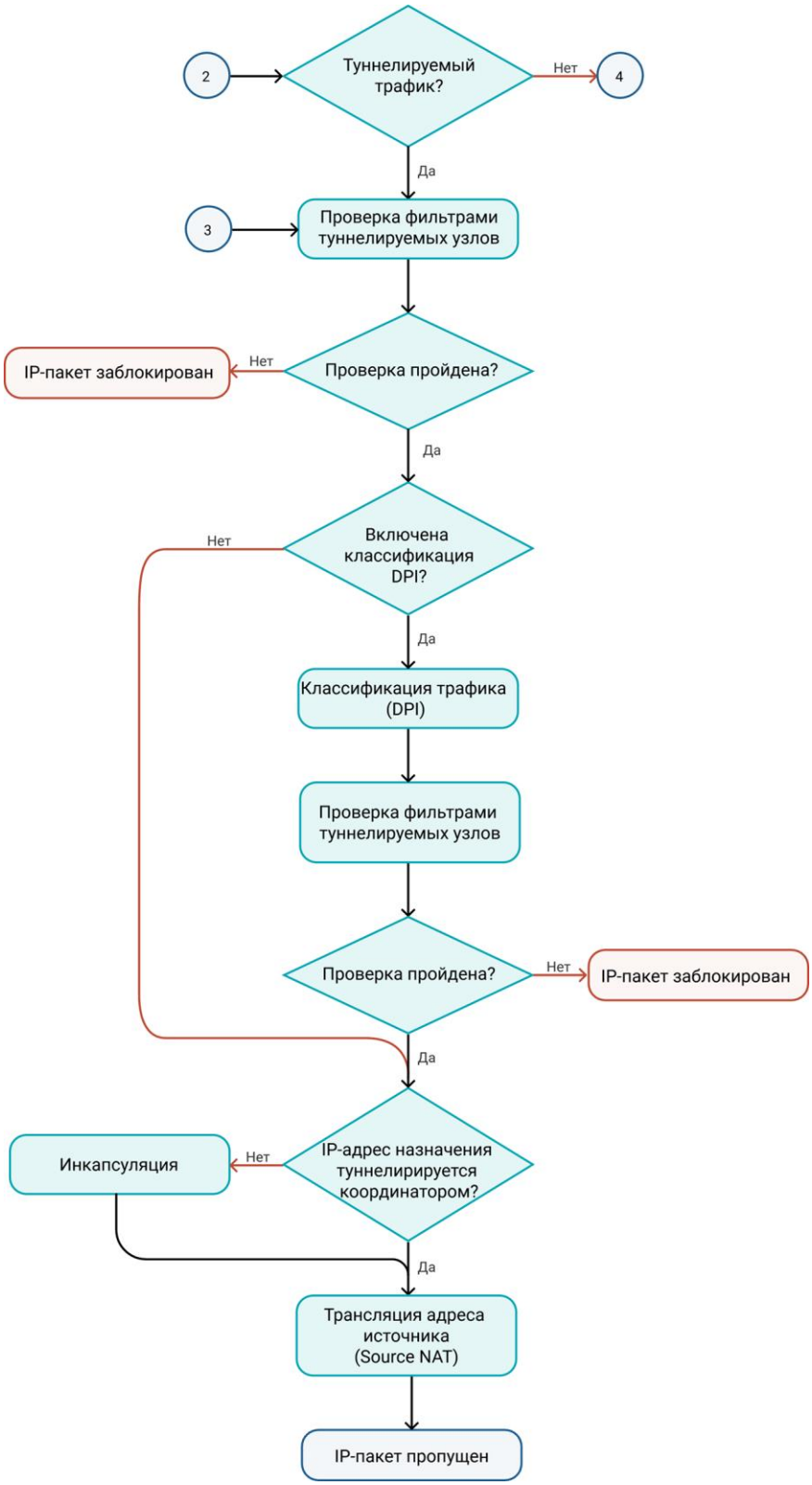


Рисунок 31. Схема фильтрации трафика. Часть 3

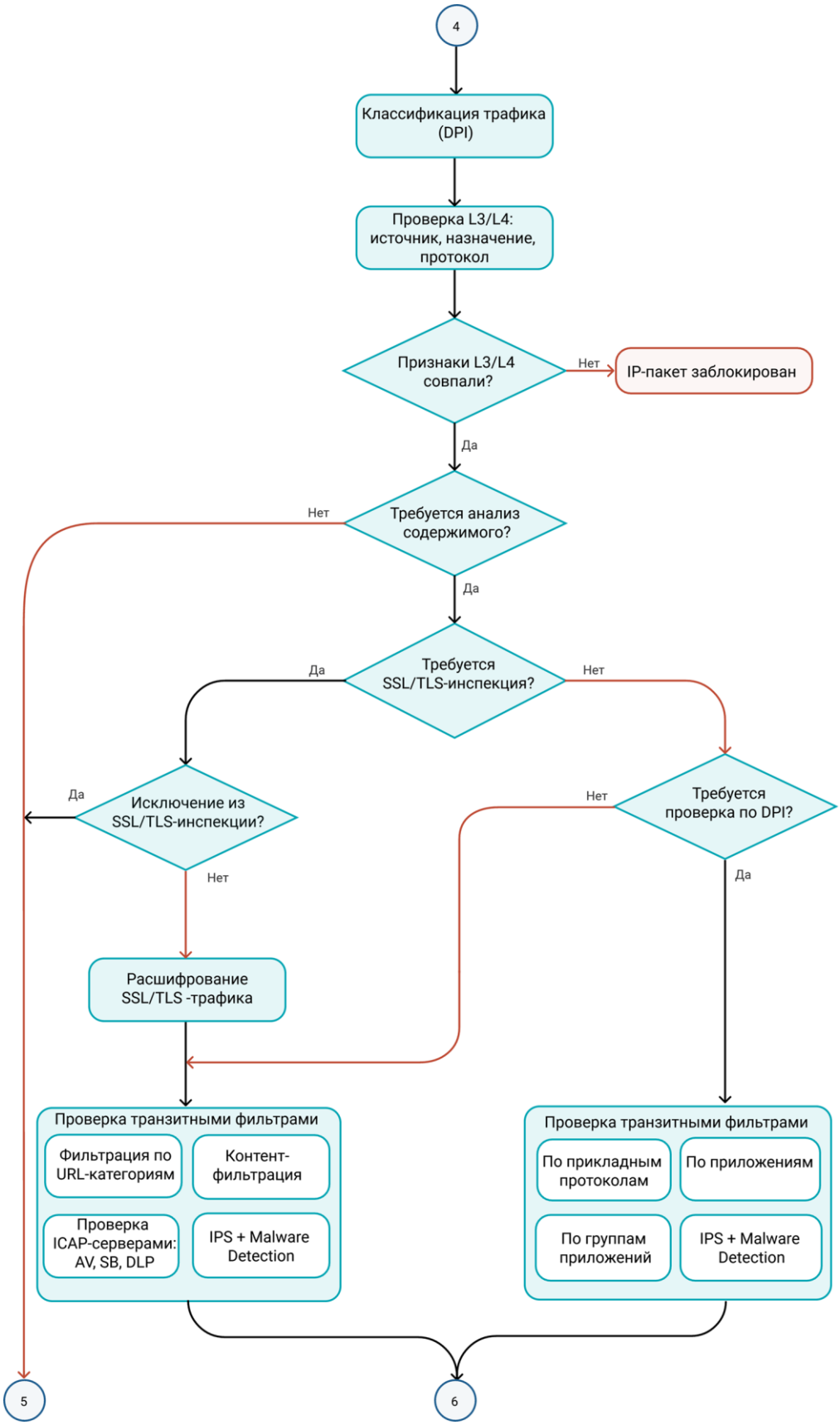


Рисунок 32. Схема фильтрации трафика. Часть 4

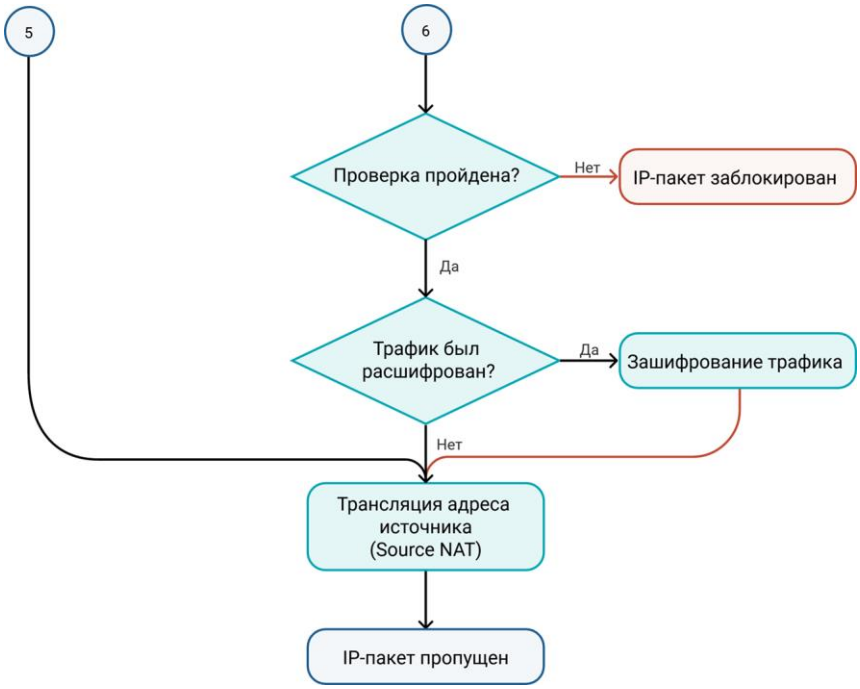


Рисунок 33. Схема фильтрации трафика. Часть 5

Объекты сетевых фильтров и правил трансляции адресов

Системные объекты, объекты и группы объектов позволяют упростить настройку сетевых фильтров и правил трансляции адресов — их можно задавать в параметрах фильтров и правил вместо перечисления отдельных объектов. К ним относятся:

- системные объекты;
- группы объектов «ViPNet-узлы», «IP-адреса», «Интерфейсы», «Протоколы» и «Расписания» (заданы по умолчанию и их можно настраивать);
- группа объектов «Веб-клиенты» (неизменяемые, заданные по умолчанию; кроме того, можно настраивать свои группы веб-клиентов);
- группа объектов «URL-категории» (неизменяемые, из базы URL-категорий; кроме того, можно настраивать свои URL-категории);
- группа объектов «Страны» (неизменяемые, из базы GeoIP);
- группы объектов, полученные из Policy Management (модуль ViPNet Prime) (их нельзя изменять и указывать в настраиваемых сетевых фильтрах и правилах трансляции).

Системные объекты

Системные объекты заданы по умолчанию. Они используются для задания адресов отправителей и получателей IP-пакетов в сетевых фильтрах и правилах трансляции адресов, а также при создании настраиваемых групп объектов (Узлы ViPNet, IP-адреса, Интерфейсы, Протоколы, Расписания). Системные объекты не отображаются в группах объектов, их нельзя ни изменить, ни удалить.

Таблица 2. Системные объекты

Имя системного объекта	Описание и область применения
`allclients` (Все клиенты)	Все клиенты, с которыми у узла есть связь. Можно использовать в фильтрах защищённой сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
`allcoordinators` (Все координаторы)	Все координаторы, с которыми у узла есть связь. Можно использовать в фильтрах защищённой сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.

`broadcast` (Широковещательные адреса)	Все широковещательные адреса. Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для идентификации широковещательных адресов получателей. Использование других адресов совместно с этой группой недопустимо.
`local` (Мой узел)	Собственный узел ViPNet Coordinator HW. Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для задания адреса отправителя для исходящих соединений узла или адреса получателя для входящих соединений узла. Использование других адресов совместно с этой группой недопустимо.
`remote` (Другие узлы)	Другие узлы (любые, кроме собственного). Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла. Использование других адресов совместно с этой группой недопустимо.
`tunneledip` (Туннелируемые IP-адреса)	Все IP-адреса, туннелируемые координатором. Можно использовать в фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
`multicast` (Групповые адреса)	Диапазон IP-адресов для групповой рассылки (224.0.0.0 – 239.255.255.255). Можно использовать в фильтрах открытой сети для задания адреса получателя. Использование других адресов совместно с этой группой недопустимо.
`any` (Любое значение)	Можно использовать в сетевых фильтрах и правилах трансляции адресов. Объект `any` обозначает: • для локальных и транзитных фильтров открытой сети — все IP-адреса; • для фильтров защищённой сети — все VPN-узлы; • для фильтров туннелируемых узлов — все IP-адреса или все VPN-узлы; • для протоколов — все протоколы; • для расписаний — все время (постоянно). Использование других условий совместно с объектом `any` недопустимо.

Группы объектов «ViPNet-узлы», «IP-адреса», «Интерфейсы», «Протоколы» и «Расписания»

Настраиваемые группы объектов:

- «ViPNet-узлы» — содержат любую комбинацию узлов сети ViPNet, используется в фильтрах защищенной сети и фильтрах туннелируемых узлов. По умолчанию не заданы.
- «IP-адреса» — содержат любую комбинацию IP-адресов, диапазонов IP-адресов и доменных имен, используется в фильтрах открытой сети, фильтрах туннелируемых узлов и правилах трансляции сетевых адресов. Состав по умолчанию:
  - `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;
- «Интерфейсы» — содержат любую комбинацию сетевых интерфейсов, используется в фильтрах открытой сети и фильтрах туннелируемых узлов. По умолчанию не заданы.
- «Протоколы» — содержат любую комбинацию сетевых протоколов и портов, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов и правилах трансляции адресов. Состав см. в приложении Группы объектов «Протоколы» по умолчанию.
- «Расписания» — содержит любую комбинацию параметров, определяющих время действия сетевого фильтра, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов. Состав по умолчанию:
  - `Workdays` — рабочие дни недели (с понедельника по пятницу);
  - `Weekends` — выходные дни недели (суббота и воскресенье).

Создание и изменение групп объектов

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

2 Выберите вкладку группы объектов:
   - **ViPNet-узлы**.
   - **IP-адреса**.
   - **Интерфейсы**.
   - **Протоколы**.
   - **Расписания**.

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

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

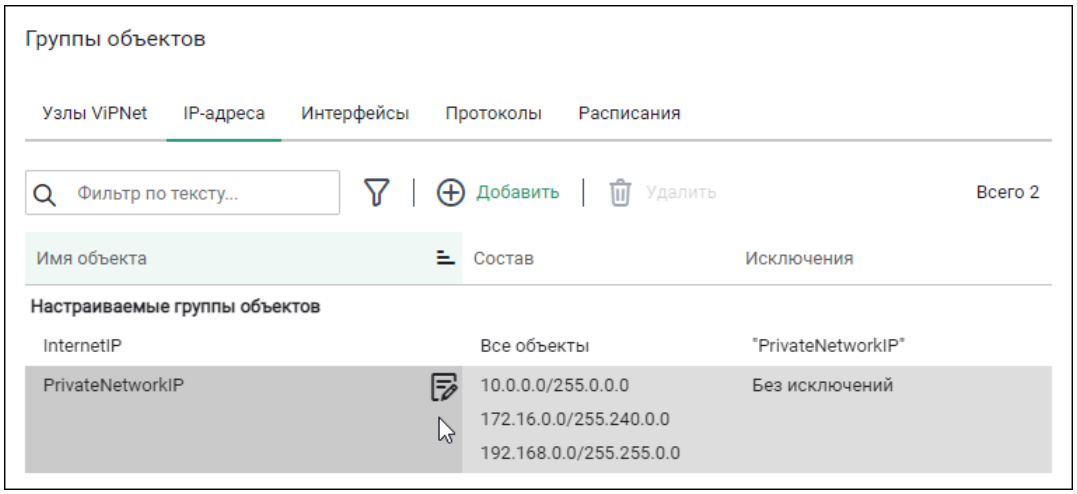


Рисунок 34. Изменение группы объектов

5 Задайте параметры:

5.1 Задайте имя группы.

> **Внимание!** Если имя группы объектов начинается с символа @, или содержит символы " и пробел, то эту группу можно использовать только в настройке ViPNet Coordinator HW с помощью веб-интерфейса; в настройке с помощью командного интерпретатора группа будет недоступна.
>
> Группы объектов из разных категорий не могут иметь одинаковые имена.

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

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

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

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

5.3 Нажмите **Сохранить**.

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

Группа сетевых узлов ViPNet

Чтобы добавить (исключить) объект:

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

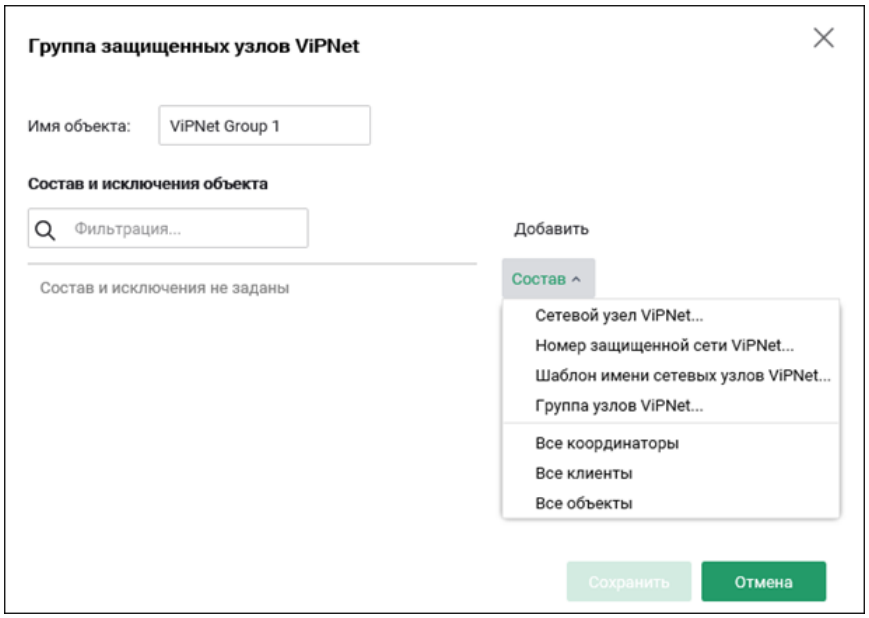


Рисунок 35. Добавление сетевого узла ViPNet в группу

Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров защищенной сети и фильтров туннелируемых узлов.

Группа IP-адресов

1. Раскройте один из списков: **Состав** (чтобы добавить объект) или **Исключения** (чтобы исключить из группы).
2. Выберите объект:
   - **IP-адрес или диапазон адресов** — выберите тип адреса, затем введите параметры;

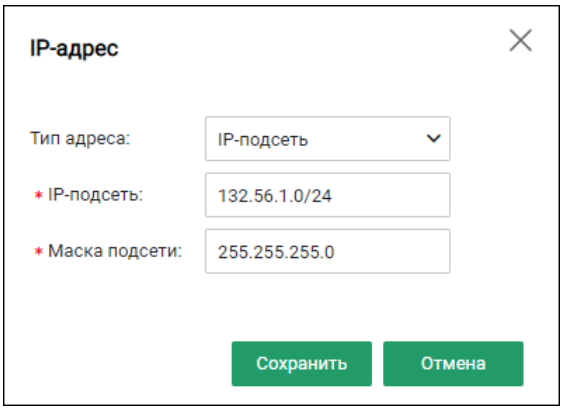


Рисунок 36. Добавление IP-адреса подсети

- **DNS-имя**;
- **Группы IP-адресов**;
- **Все объекты** (можно только добавить).

Нажмите **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров открытой сети, фильтров туннелируемых узлов и правил трансляции адресов

Группа интерфейсов

Чтобы добавить (исключить) объект:

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

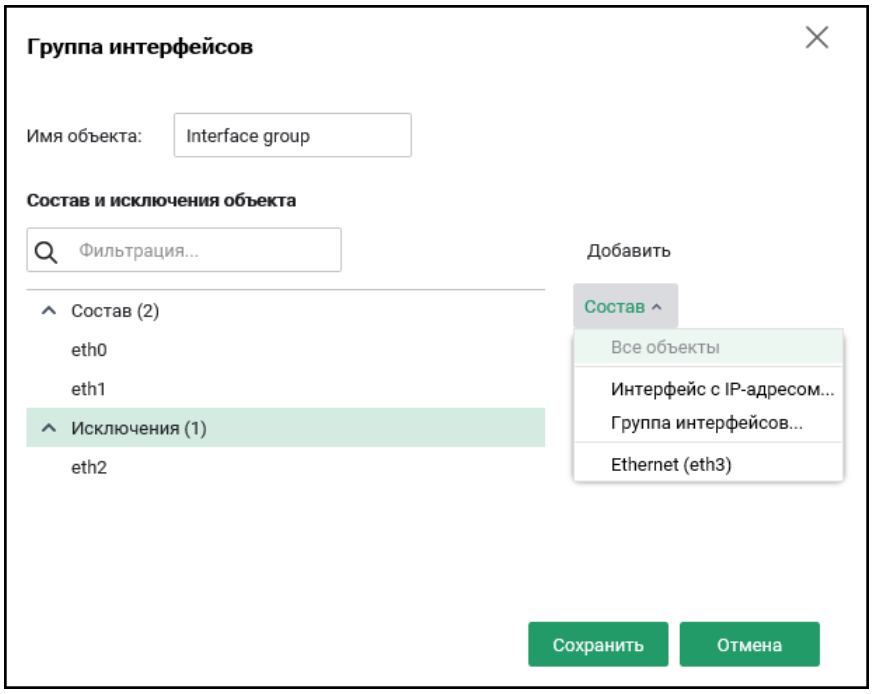


Рисунок 37. Добавление сетевых интерфейсов в группу

2 Выберите объект:

- Чтобы добавить (исключить) один или несколько интерфейсов собственного узла, выберите имя этого интерфейса (**Ethernet (eth0)**, **Ethernet (eth1)** и т.д.).
- Чтобы добавить (исключить) IP-адрес или диапазон IP-адресов интерфейсов, выберите пункт **Интерфейс с IP-адресом** и выполните одно из действий:
  - для задания одного IP-адреса в списке выберите соответствующий тип адреса и укажите этот IP-адрес;
  - для задания IP-адресов подсети в списке выберите соответствующий тип адреса и укажите адрес и маску этой подсети (по умолчанию — `255.255.255.0/24`);
  - для задания диапазона IP-адресов в списке выберите соответствующий тип адреса и укажите начальный и конечный IP-адреса этого диапазона.
- Чтобы добавить (исключить) одну или несколько групп сетевых интерфейсов, выберите **Группа интерфейсов** и установите флажки рядом с нужными группами.
- Чтобы добавить в группу все сетевые интерфейсы и группы интерфейсов, выберите **Все объекты**.

3 Нажмите **Сохранить**.



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

Группа протоколов

Чтобы добавить (исключить) объект:

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

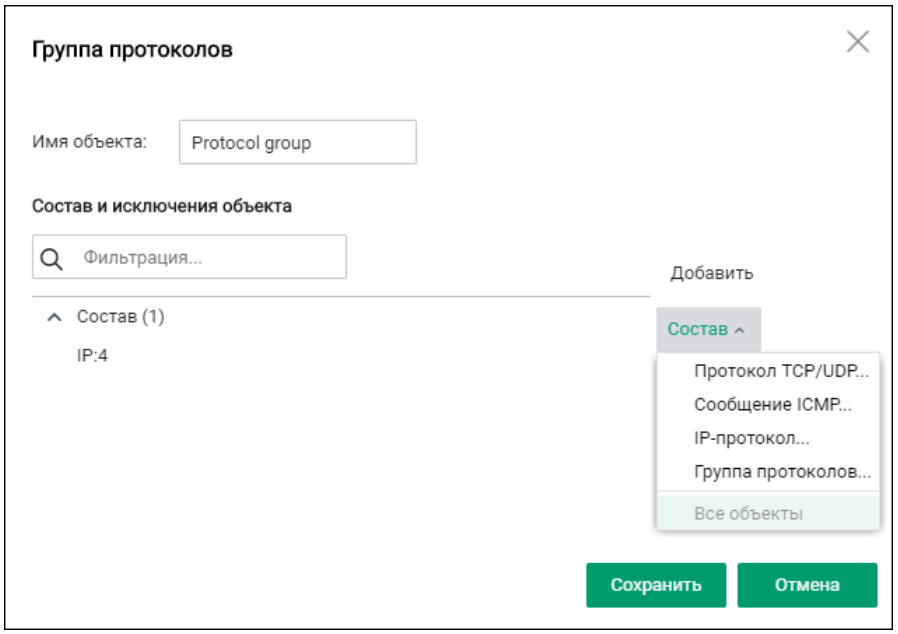


Рисунок 38. Добавление группы протоколов

2 Выберите объект:

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

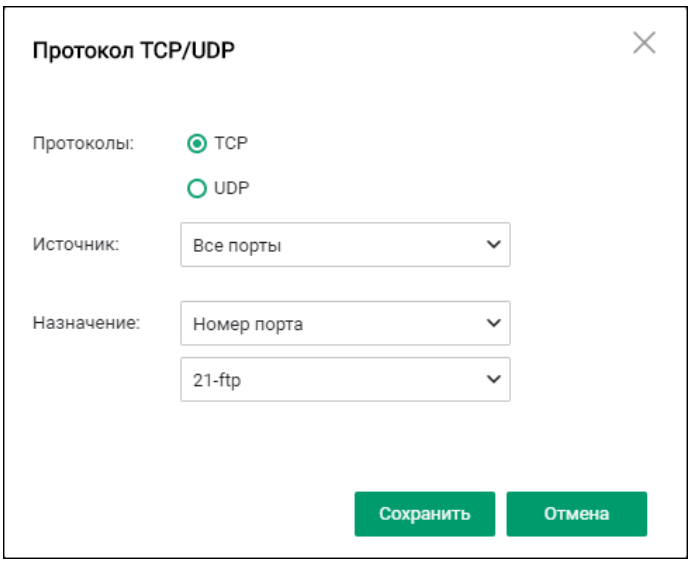


Рисунок 39. Добавление протокола в группу

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

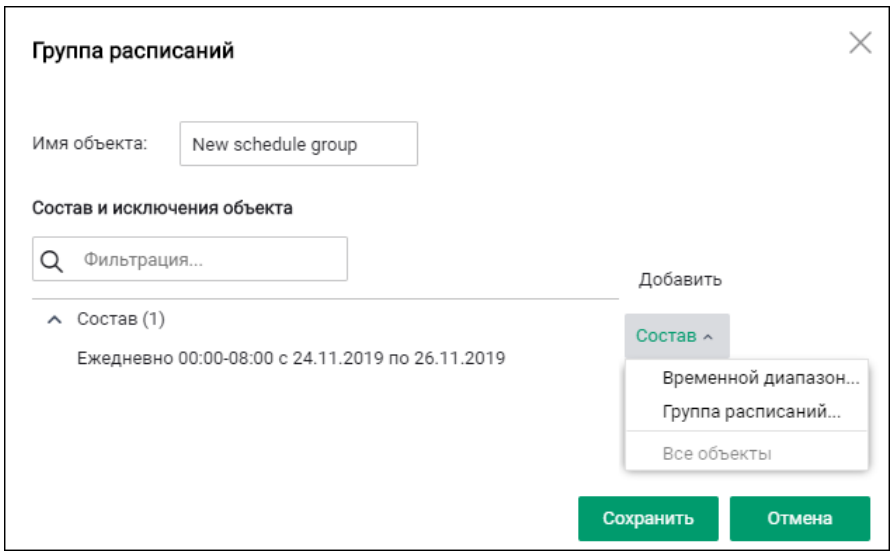


Рисунок 40. Добавление группы расписаний

2 Выберите объект:

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

укажите интервал дат, в который фильтр или правило трансляции будет применяться (не применяться) ежедневно;

- **Еженедельно** — чтобы фильтр или правило трансляции применялось (не применялось) в 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.

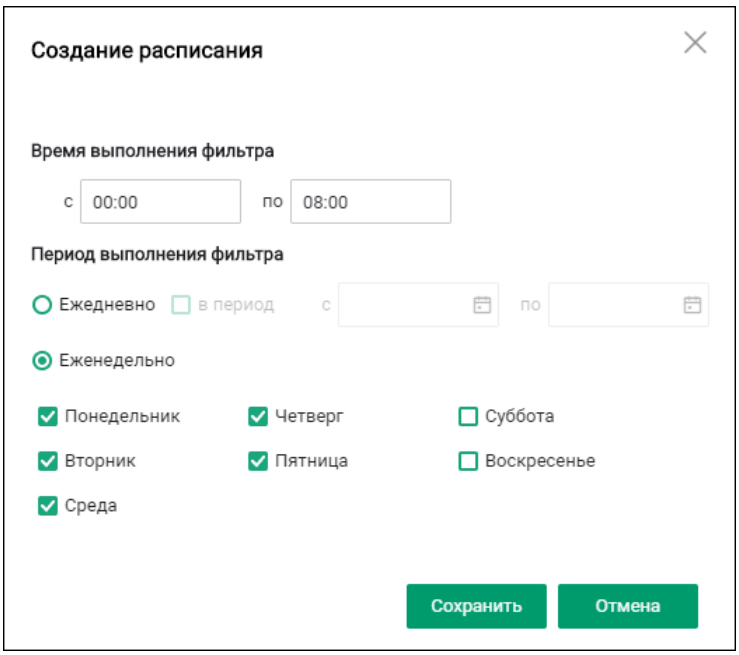


Рисунок 41. Добавление расписания в группу

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

3 Нажмите **Сохранить**.

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

Просмотр групп объектов

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

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

2 Выберите вкладку группы объектов:

- **ViPNet-узлы**.
- **IP-адреса**.
- **Интерфейсы**.
- **Протоколы**.
- **Расписания**.

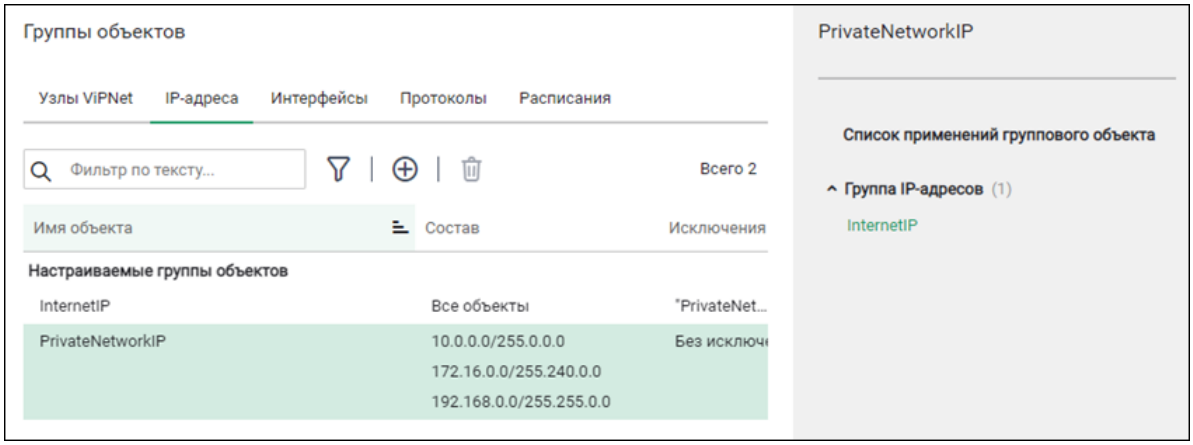


Рисунок 42. Просмотр групп IP-адресов

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

Группа объектов «Веб-клиенты»

В транзитных фильтрах открытой сети в качестве параметра фильтрации вы можете задавать группы веб-клиентов, содержащие строки из значений HTTP-заголовков User-Agent (далее — маски User-Agent).

По умолчанию заданы группы веб-клиентов для браузеров Chrome, Edge, Firefox, Opera и Yandex. Вы не можете изменить состав этих групп веб-клиентов или удалить их, но можете создать свои настраиваемые группы веб-клиентов:

1 Выберите **Межсетевой экран** > **Группы объектов** > **Веб-клиенты**.

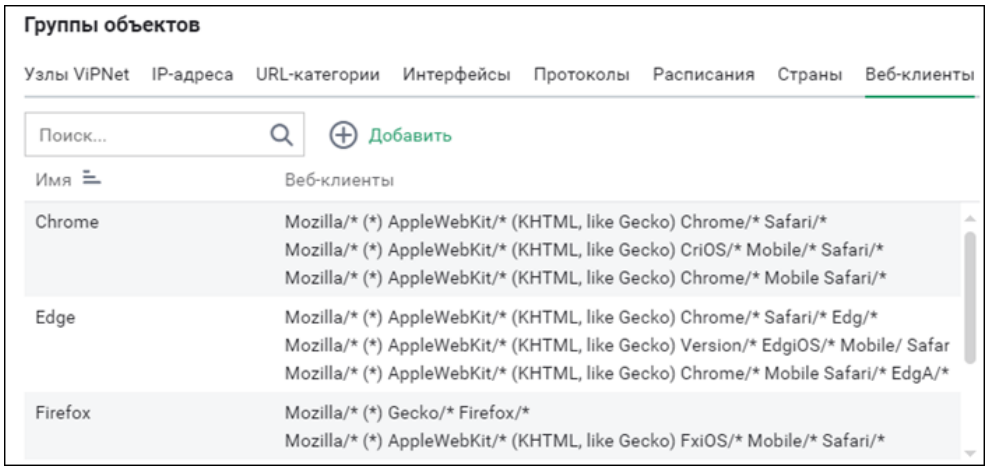


Рисунок 43. Группы объектов «Веб-клиенты» по умолчанию

2 Нажмите ⊕ **Добавить**.

3 В окне **Создание группы веб-клиентов**:

3.1 Задайте имя группы.

3.2 Последовательно добавьте в группу маски User-Agent:

3.2.1 Нажмите ⊕ **Добавить**.

3.2.2 Задайте маску.

> **Примечание.** Маска должна соответствовать синтаксису HTTP-заголовка User-Agent. Максимальное количество масок в группе — 10.

3.2.3 Нажмите **Сохранить**.

> **Примечание.** Максимальное количество настраиваемых групп веб-клиентов — 20.

3.3 Нажмите **Сохранить**.

Группа объектов «URL-категории»

В транзитных фильтрах открытой сети и фильтрах туннелируемых узлов вы можете задавать URL-категории — предварительно сформированные по определенным признакам группы адресов веб-ресурсов и масок. Используйте категории из обновляемой базы URL-категорий (см. База URL-категорий), а при необходимости создайте свои настраиваемые URL-категории.

Обновление базы URL-категорий

База URL-категорий публикуются на сервере обновления `https://updateids.infotecs.ru`, или другом, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления.

Установка базы URL-категорий

По умолчанию база URL-категорий не установлена. При наличии действующего объекта лицензирования «Обновление URL» вы можете установить базу URL-категорий с сервера или из файла. После установки список URL-категорий базы отобразится в группе **Из базы URL-категорий**.

Установка базы URL-категорий с сервера:

1. Выберите **Межсетевой экран** > **Группы объектов** > **URL-категории**.
2. Щелкните **База URL-категорий**.

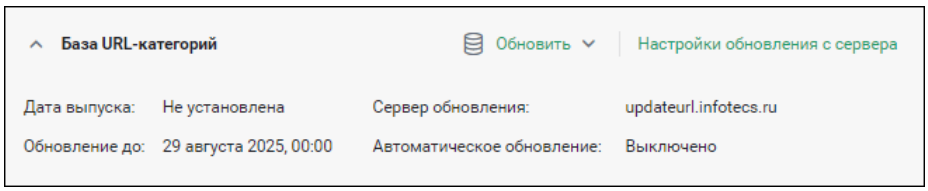


Рисунок 44. Настройка обновления базы URL-категорий

3. Нажмите **Настройки обновления с сервера**.
4. По умолчанию используется сервер `updateids.infotecs.ru`. Если у вас другой сервер, укажите его адрес в поле **Сервер обновления**.
5. Задайте имя пользователя и его пароль для подключения к серверу обновления.
6. Если для доступа к внешним ресурсам в вашей сети используется прокси-сервер:
   - **6.1** Выберите **Использовать прокси-сервер**.
   - **6.2** Задайте IP-адрес или доменное имя прокси-сервера.
   - **6.3** При необходимости измените TCP-порт (по умолчанию — 3128).

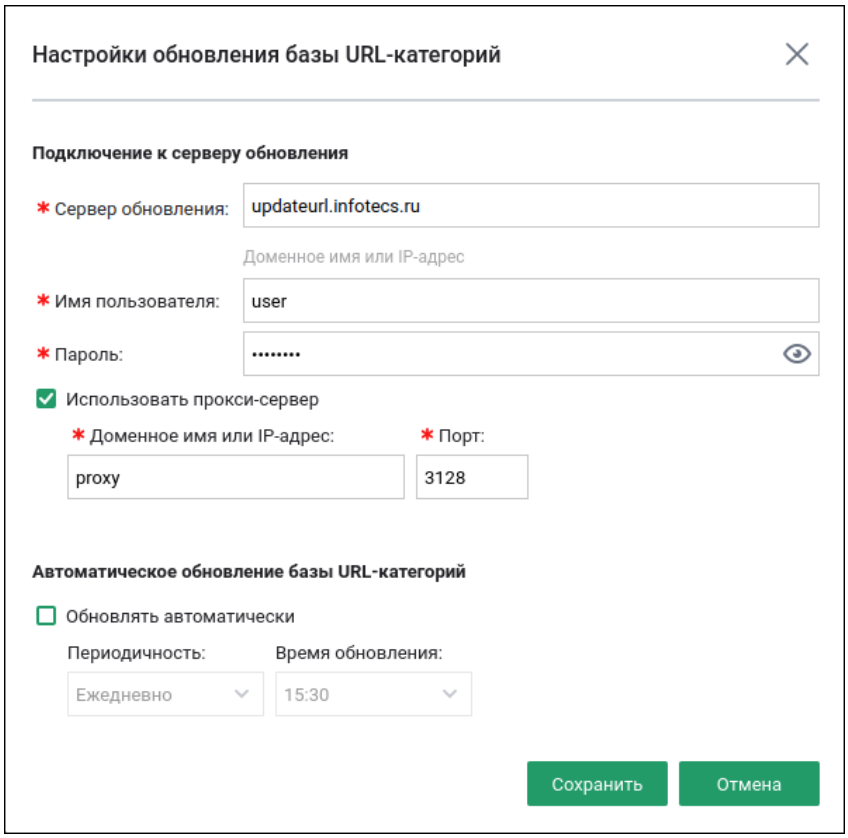


Рисунок 45. Настройка подключения к серверу

7 Нажмите **Сохранить**.

8 В списке **Обновить** выберите **С сервера**.

Дождитесь завершения установки базы URL-категорий.

Установка базы URL-категорий из файла:

1 Скачайте с сервера обновления файл базы URL-категорий в формате `*.zip` и файл электронной подписи `*.sig`.

2 Выберите **Межсетевой экран** > **Группы объектов** > **URL-категории**.

3 Щелкните **База URL-категорий**.

4 В списке **Обновить** выберите **Из файла**.

5 Выберите файл базы URL-категорий и файл электронной подписи. Нажмите **Открыть**.

Дождитесь завершения установки базы URL-категорий.

Обновление базы URL-категорий

Вы можете настроить расписание обновления базы URL-категорий с сервера или обновлять базу вручную с сервера или из файла.

Для настройки расписания обновления базы:

1 Выберите **Межсетевой экран** > **Группы объектов** > **URL-категории**.

2 Щелкните **База URL-категорий**.

3 Нажмите **Настройки обновления с сервера**.

4 Если вы уже задали сервер обновления, имя пользователя, его пароль и прокси-сервер на этапе установки базы URL-категорий, пропустите этот шаг. Иначе выполните шаги 4–6 сценария установки базы URL-категорий с сервера.

5 В разделе **Автоматическое обновление базы URL-категорий**:

5.1 Выберите **Обновлять автоматически**.

5.2 Задайте периодичность и время обновления.

6 Нажмите **Сохранить**.

Теперь база URL-категорий будет обновляться с сервера по расписанию.

Для обновления базы вручную с сервера:

1 Выберите **Межсетевой экран** > **Группы объектов** > **URL-категории**.

2 Щелкните **База URL-категорий**.

3 В списке **Обновить** выберите **С сервера** и дождитесь завершения обновления.

Для обновления для вручную из файла выполните шаги сценария установки базы URL-категорий из файла.

Настраиваемые URL-категории

Создание URL-категории

Чтобы создать настраиваемую URL-категорию и добавить в нее ресурсы:

1 Выберите **Межсетевой экран** > **Группы объектов** > **URL-категории**.

2 Нажмите **Добавить URL-категорию**.

3 В окне **Новая настраиваемая URL-категория** задайте:

3.1 Имя URL-категории.

3.2 Описание URL-категории.

3.3 Последовательно добавьте ресурсы в URL-категорию:

3.3.1 Нажмите **Добавить**.

3.3.2 Укажите адрес веб-ресурса или маску.

Внимание! При добавлении ресурса в URL-категорию необходимо учитывать все ресурсы, к которым выполняются запросы. Например, если ресурс, который определен как `*example.com*`, выполняет запросы к `static.example.org`, для корректной работы необходимо добавить оба ресурса в категорию.

3.3.3 Нажмите .

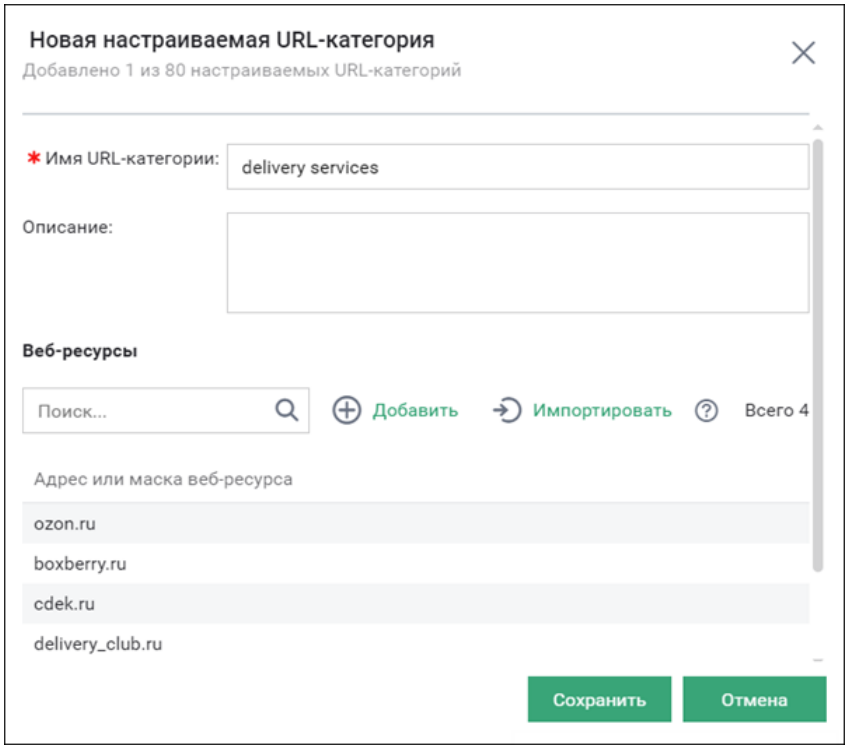


Рисунок 46. Создание настраиваемой URL-категории

3.4 Чтобы добавить ресурсы из файла:

3.4.1 Нажмите **Импортировать URL-категории**.

3.4.2 Выберите в папке файл импорта и нажмите **Открыть**.

Примечание. Требования к файлу импорта:

- Файл в формате `csv` или `txt`.
- Кодировка символов — UTF-8.
- Запись файла может состоять только из адреса веб-ресурса или маски или из адреса веб-ресурса или маски и URL-категорий, указанных через разделитель (`,` или `;`).
- Каждая следующая запись располагается на новой строке.
- В одном файле могут быть записи обоих типов.

3.4.3 В окне **Импорт**:

3.4.3.1 Нажмите **Подробнее**, чтобы просмотреть сведения о дублированных ресурсах или с недопустимыми значениями.

3.4.3.2 Нажмите **Да** для подтверждения импорта.

3.5 Нажмите **Сохранить**.

Импорт URL-категорий из файла

1 Выберите **Межсетевой экран** > **Группы объектов** > **URL-категории**.

2 Нажмите **Импортировать URL-категории**.

3 Выберите в папке файл импорта и нажмите **Открыть**.

Примечание. Требования к файлу импорта такие же, как и в сценарии создания URL-категории.

4 Нажмите **Подробнее**, чтобы просмотреть сведения об импортируемых ресурсах.

5 Нажмет **Да** для подтверждения импорта.

Экспорт **URL-категорий**

Вы можете экспортировать в файл как ресурсы одной URL-категории, так и сразу нескольких:

- Для экспорта ресурсов одной URL-категории наведите курсор на строку URL-категории в группе **Настраиваемые URL-категории** и щелкните значок . Ресурсы экспортируются в файл `<имя URL-категории>_<дата>_<время>.csv`.
- Для экспорта ресурсов нескольких URL-категорий выберите их и на панели инструментов нажмите **Экспортировать**. Ресурсы экспортируются в файл `URLcategories_<дата>_<время>.csv`.

Файлы экспорта сохраняются в папке компьютера (по умолчанию — **Загрузки**).

Группа объектов «Страны»

В локальных и транзитных фильтрах открытой сети в качестве адресов отправителя и получателя IP-пакетов вы можете задавать объекты группы «Страны» (коды стран Alpha 2 или числовые коды в соответствии с ISO-3166), содержащиеся в базе GeoIP. База публикуется на сервере обновления `https://updateids.infotecs.ru`, или другом ресурсе, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления. По умолчанию установлена база GeoIP из состава дистрибутива ViPNet Coordinator HW.

Просмотр группы объектов «Страны»

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

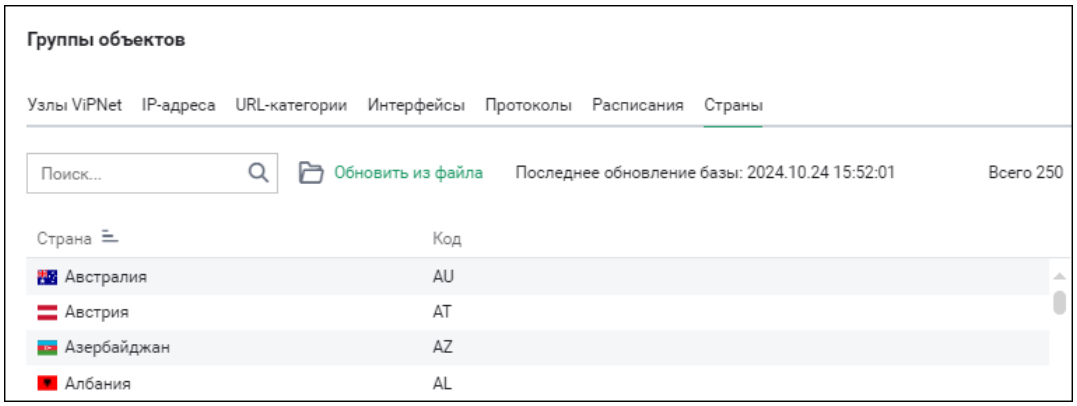


Рисунок 47. Список стран базы GeoIP

2 Чтобы просмотреть общие сведения об определенной стране, нажмите на строку страны в списке.

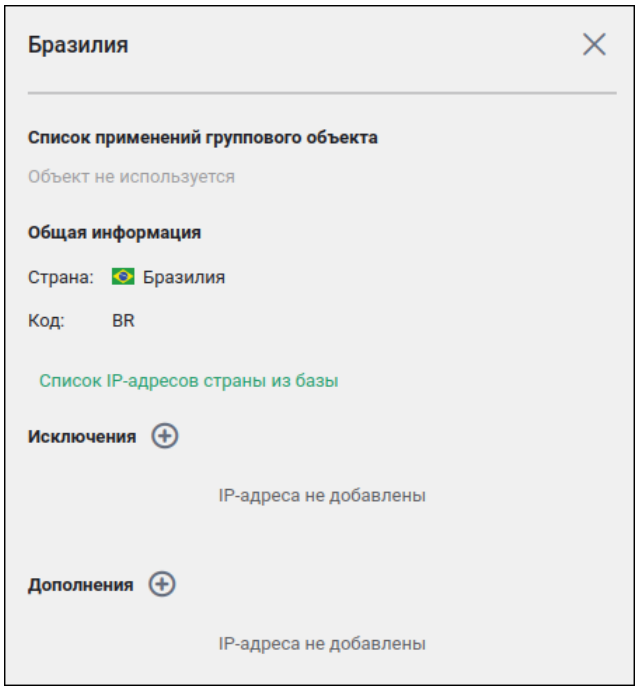


Рисунок 48. Общие сведения о стране

В разделе **Список применений группового объекта** отображаются тип и имена сетевых фильтров, в которых задана выбранная страна.

3 Чтобы просмотреть список IP-подсетей выбранной страны в базе GeoIP, нажмите **Список IP-адресов страны из базы**.

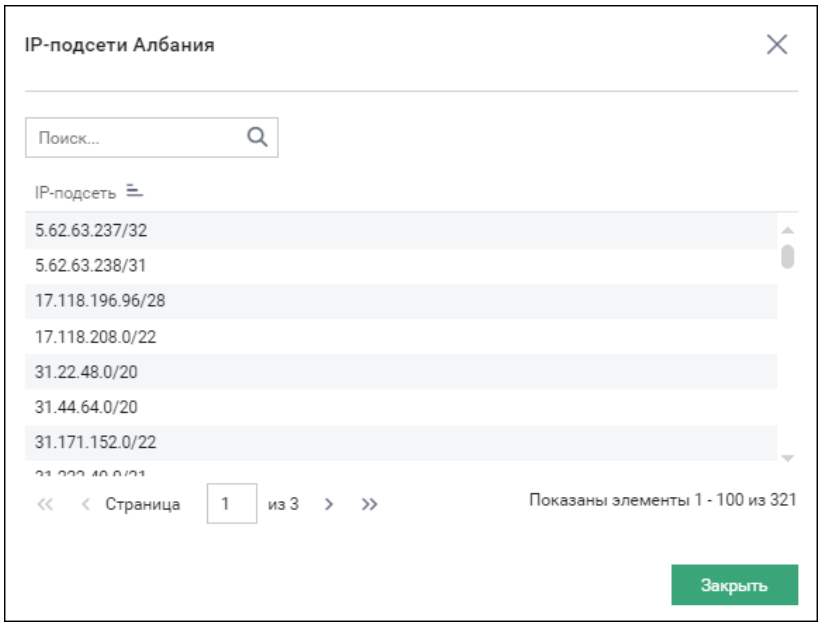


Рисунок 49. Список IP-подсетей страны

Списки исключений и дополнений IP-адресов стран

Для каждой страны вы можете настроить список исключений и дополнений IP-адресов. При фильтрации трафика IP-адрес отправителя или получателя сначала проверяется по этому списку. Если IP-адреса нет в списке, то проверка продолжается по IP-адресам страны, содержащимся в базе GeoIP. Обновление или восстановление базы GeoIP не влияет на списки исключений и дополнений IP-адресов стран. По умолчанию списки исключений и дополнений IP-адресов стран не настроены.

Чтобы добавить IP-адреса в список исключений и дополнений IP-адресов страны:

1 Нажмите на строку страны в списке.

2 Для добавления исключений:

2.1 В разделе **Исключения** нажмите ⊕ **Добавить**.

2.2 В окне **Добавление IP-адреса** добавьте адреса.

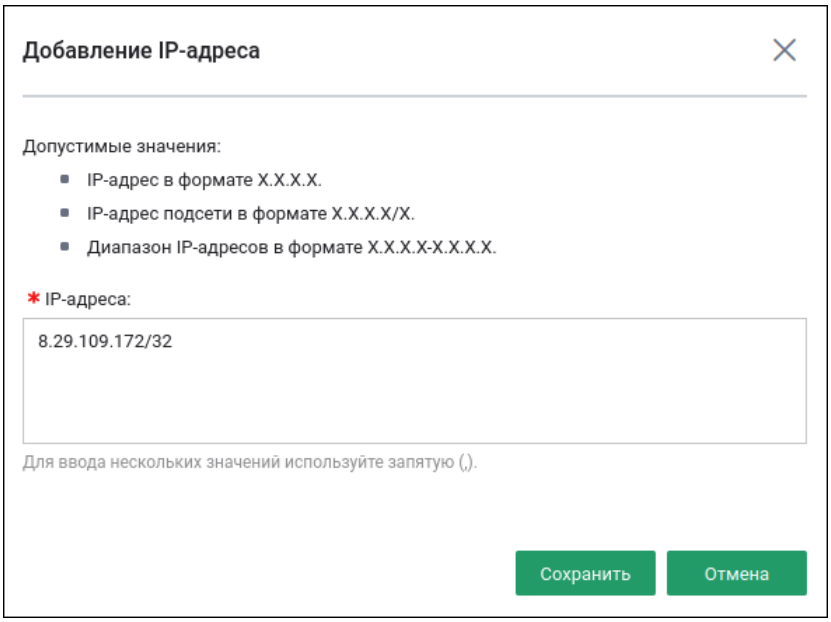


Рисунок 50. Добавление IP-адресов в список исключений и дополнений

2.3 Нажмите **Сохранить**.

3 Для добавления дополнений в разделе **Дополнения** нажмите ⊕ и выполните действия, как на шагах 2.2 и 2.3.

Обновление базы GeoIP

Чтобы поддерживать базу GeoIP в актуальном состоянии, обновляйте базу из файла вручную:

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

Дата и время последнего обновления базы GeoIP указаны в поле **Последнее обновление базы**.

2 Скачайте с сервера обновления и запишите в папку компьютера актуальную базу GeoIP (файл базы формата `*.tar.gz` и файл ЭП формата `*.tar.gz.sig`).

3 Нажмите **Обновить из файла**.

4 Выберите файлы базы и нажмите **Открыть**.

Дождитесь завершения обновления.

Настройка SSL/TLS-инспекции трафика

ViPNet Coordinator HW может инспектировать транзитный SSL/TLS-трафик между узлами сети, расположенными за ViPNet Coordinator HW, и внешними ресурсами, а именно — идентифицировать SSL/TLS-сессии с помощью DPI и расшифровывать их, используя для этого SSL-сертификат, которым подписываются сертификаты при встраивании в сессии. По умолчанию параметры SSL/TLS-инспекции заданы, но при необходимости вы можете изменить их:

- Настройка основных параметров SSL/TLS-инспекции.
- Настройка исключений из SSL/TLS-инспекции.
- Настройка SSL-сертификата.

Последовательность SSL/TLS-инспекции трафика см. в разделе Принципы фильтрации трафика на рисунке «Схема фильтрации трафика. Часть 4».

Чтобы использовать SSL/TLS-инспекцию в фильтрации транзитного трафика, создайте транзитные фильтры открытой сети с указанием параметра SSL/TLS-инспекции и параметров фильтрации:

- URL-категории;
- URL-адрес веб-ресурса, в том числе MIME-тип передаваемых данных и метод HTTP-запроса;
- проверка на ICAP-серверах:
  - антивирусная проверка;
  - проверка в песочнице;
  - проверка в DLP-системе.
- проверка IPS, в том числе Malware Detection.

Настройка основных параметров SSL/TLS-инспекции

1 Выберите **Межсетевой экран** > **SSL/TLS-инспекция** > **Настройки**.

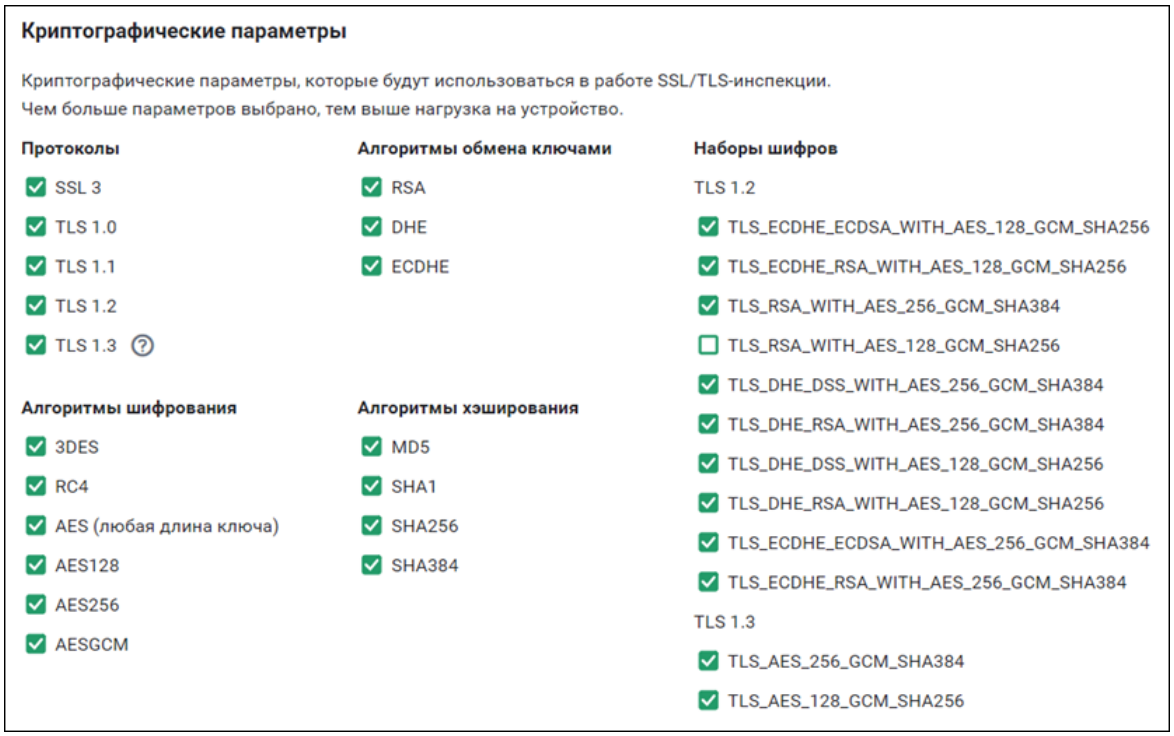


Рисунок 51. Настройка протоколов, алгоритмов и наборов шифров

2 В разделе **Криптографические параметры**:

2.1 Выберите инспектируемые протоколы:

- По умолчанию разрешены все протоколы.
- Должен быть разрешен как минимум один протокол.
- Соединение по протоколам со снятыми флажками не устанавливается.
- Если внешний ресурс не поддерживает ни один из разрешенных протоколов, соединение может установиться без встраивания в SSL-сессию.
- Использование устаревших протоколов SSL 3, TLS 1.0, TLS 1.1 потенциально небезопасно. Чтобы ViPNet Coordinator HW не устанавливал такие соединения:
  - запретите инспекцию этих протоколов — снимите флажки **SSL 3**, **TLS 1.0**, **TLS 1.1**;
  - и выключите их в исключениях SSL/TLS-инспекции.

Внимание!

При использовании протокола SSL 3 также включите протокол TLS 1.0. Рекомендуется при настройке инспекции SSL/TLS-трафика использовать протоколы, включенные по умолчанию. Иначе соединение может установиться без встраивания в SSL-сессию из-за невозможности согласовать работу по выбранному протоколу.

Если устаревший протокол разрешен и не исключен из SSL/TLS-инспекции, то соединение с внешним ресурсом может быть установлено по устаревшему протоколу, если он не поддерживает другие протоколы. При этом такое соединение будет отображаться в браузере как защищенное.

2.2 Выберите алгоритмы (обмена ключами, шифрования, хэширования) и наборы шифров для протокола TLS:

- По умолчанию разрешены все алгоритмы и наборы шифров.
- Необходимо разрешить минимум по одному алгоритму из групп обмена ключами, шифрования и хэширования.
- Трафик, в котором используются алгоритмы и наборы шифров со снятыми флажками, блокируется.
- Если протокол TLS 1.2 запрещен, то заданные наборы шифров TLS 1.2 не используется.
- Если наборы шифров TLS 1.3 запрещены, то трафик TLS 1.3 не будет расшифровываться, даже если протокол TLS 1.3 разрешен.

3 В разделах **Блокировать сессии, использующие** различные типы сертификатов и **Сессии с двусторонним TLS** выберите действие с инспектируемой SSL/TLS-сессией:

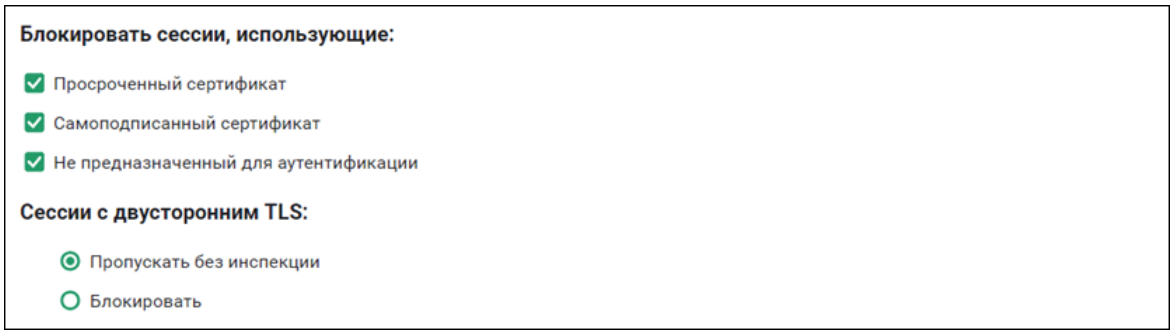


Рисунок 52. Настройка действий с инспектируемой SSL/TLS-сессий

- Действия по умолчанию:
  - сессия с просроченным сертификатом — блокировать;
  - сессия с самоподписанным сертификатом — блокировать;
  - сессия с сертификатом, не предназначенный для аутентификации — блокировать;
  - сессия с двухсторонним TLS — пропускать без инспекции.

Настройка исключений из SSL/TLS-инспекции

ViPNet Coordinator HW поддерживает работу с исключениями SSL/TLS-инспекции — протоколами и ресурсами, которые обрабатываются до расшифрования трафика. Если протокол или ресурс добавлен в исключения, то их трафик не инспектируется. По умолчанию из инспекции исключены устаревшие протоколы SSL 3, TLS 1.0 и TLS 1.1. В список исключений ресурсов по умолчанию добавлены адреса ресурсов, как правило, не требующих инспекции, например, `microsoft.com`, `google.com`, `apple.com` и другие. Вы не можете удалить эти ресурсы. В дополнение к ним, в список исключений вы можете добавить свои настраиваемые ресурсы. Кроме адресов ресурсов для работы исключений необходимы сертификаты этих ресурсов, для получения которых ViPNet Coordinator HW должен иметь доступ к интернету. Для всех ресурсов списка вы можете настроить

обработку ресурсов по их альтернативным именам (SAN), указанным в сертификатах, и расписание обновления сертификатов.

Чтобы настроить исключения SSL/TLS-инспекции:

1 Выберите **Межсетевой экран** > **SSL/TLS-инспекция** > **Исключения**.

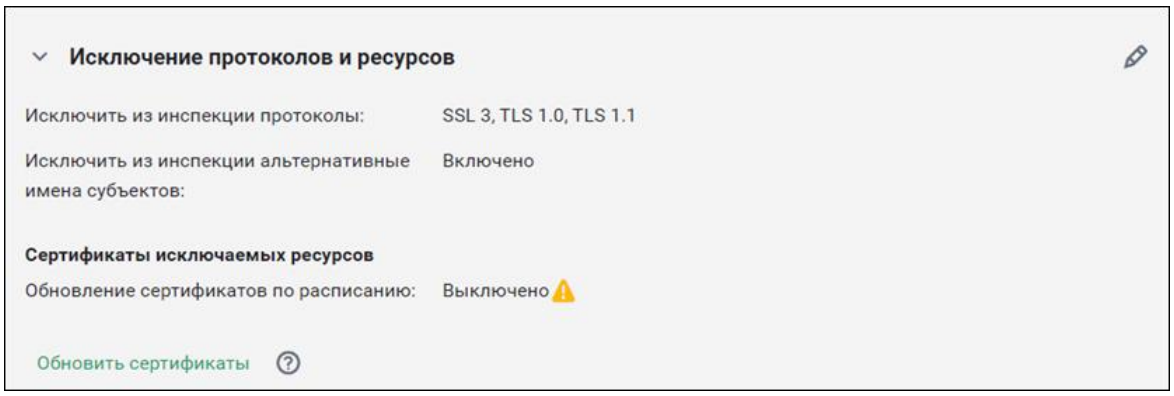


Рисунок 53. Настройка исключений SSL/TLS-инспекции

2 Нажмите , чтобы настроить исключения:

2.1 По умолчанию инспектируется трафик протоколов TLS 1.2, TLS 1.3. При необходимости измените исключения протоколов.

Внимание! Использование устаревших протоколов SSL 3, TLS 1.0, TLS 1.1 потенциально небезопасно.

2.2 Чтобы не исключать из SSL/TLS-инспекции все ресурсы списков исключений (**Ресурсы по умолчанию** и **Настраиваемые ресурсы**) по альтернативным именам, снимите флажок **Исключать из инспекции альтернативные имена субъектов (Subject Alternative Names), указанные в сертификатах ресурсов**.

2.3 По умолчанию обновление сертификатов ресурсов списков исключений по расписанию выключено. При необходимости выберите **Обновлять сертификаты ресурсов** и настройте расписание их обновления.

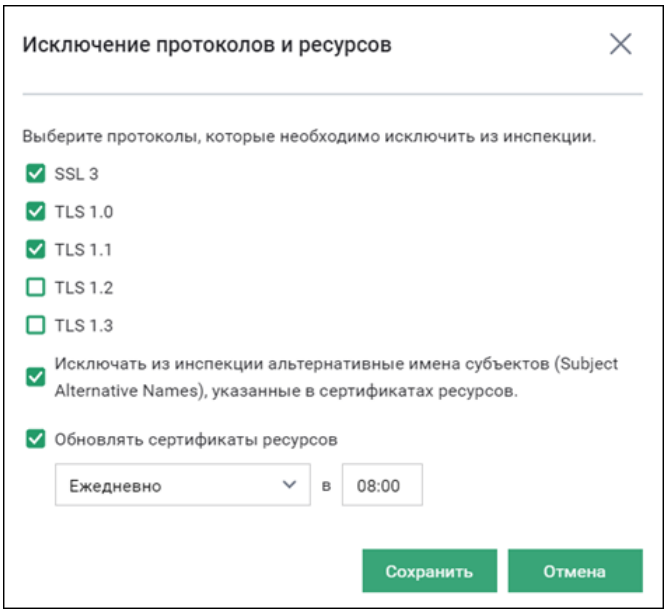


Рисунок 54. Настройка исключения ресурсов по альтернативным именам

2.4 Нажмите **Сохранить**.

3 Трафик ресурсов из списка **Ресурсы по умолчанию** инспектируется, несмотря на то, что ресурсы добавлены в список. Чтобы не инспектировать трафик ресурса из этого списка, включите его — ресурс будет перемещен в начало списка.

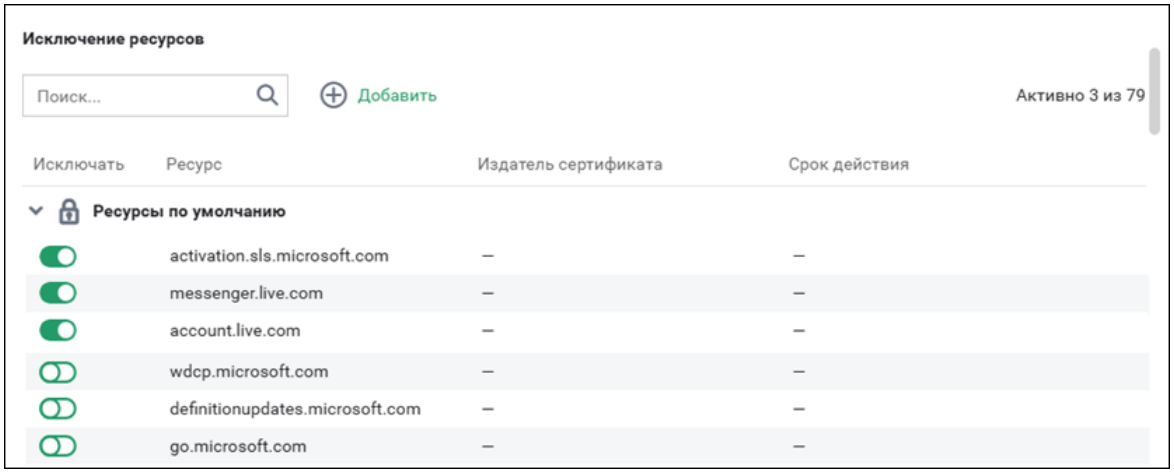


Рисунок 55. Настройка исключения ресурсов по умолчанию

4 Если сертификаты списка **Ресурсы по умолчанию** отсутствуют, нажмите **Обновить сертификаты**, чтобы загрузить их вручную.

5 Чтобы исключить из инспекции трафик ресурса, не входящего в список **Ресурсы по умолчанию**, добавьте его в список **Настраиваемые ресурсы**:

5.1 Нажмите **Добавить**.

5.2 Задайте доменное имя ресурса или маску.

Примечание. Доменное имя может состоять из букв (`A-Z`, `a-z`), цифр (`0-9`) и символов (`-` `.`). Маска позволяет задать несколько схожих доменных имен:

- состоит из символов доменного имени и символа (`*`);
- `*` означает произвольное количество символов;
- минимальное количество символов в маске, включая `*` — 5.

При добавлении ресурс должен быть доступен.

5.3 Нажмите **Добавить**.

5.4 Включите ресурс.

Настройка SSL-сертификата

По умолчанию в качестве SSL-сертификата, которым подписываются сертификаты, встраиваемые в SSL/TLS-сессии, используется самоподписанный сертификат ViPNet Coordinator HW.

Чтобы браузеры или другие приложения не выдавали предупреждение о подмене сертификата, установите SSL-сертификат в хранилище сертификатов каждого сетевого узла (или приложения), SSL/TLS-трафик которого вы хотите инспектировать:

1 Выберите **Межсетевой экран** > **SSL/TLS-инспекция** > **SSL-сертификат**.

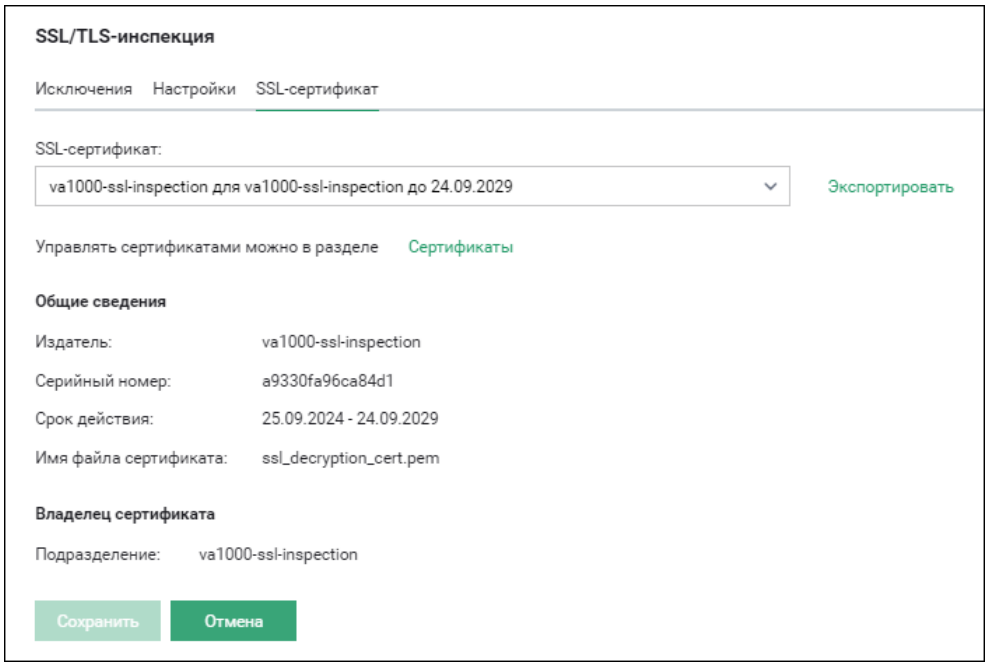


Рисунок 56. Настройка SSL-сертификата

2 Нажмите **Экспортировать**.

Файл сертификата будет сохранен в папке вашего компьютера.

3 Установите SSL-сертификат в хранилище сертификатов сетевых узлов.

В качестве SSL-сертификата вы также можете использовать сторонний сертификат, подписанный удостоверяющим центром (УЦ):

1 Проверьте поле `keyUsage` и поле `cA` расширения `BasicConstraints` стороннего сертификата:

   - `keyUsage = critical, keyCertSign`
   - `BasicConstraints: cA = TRUE`

   Если значения полей отличаются, используйте другой сторонний сертификат.

2 Нажмите **Сертификаты**, чтобы перейти в раздел управления сертификатами.

3 Импортируйте сторонний сертификат и его закрытый ключ:

   3.1 Нажмите **Импортировать**.

   3.2 В окне импорта вставьте текст стороннего сертификата или загрузите его файл.

   3.3 Нажмите **Импортировать**.

   3.4 Повторите шаги 3.1–3.3, чтобы импортировать закрытый ключ стороннего сертификата.

Примечание. Если в локальном хранилище нет корневого сертификата УЦ, которым подписан сторонний сертификат, также импортируйте и его.

---

4 Выберите **Межсетевой экран** > **SSL/TLS-инспекция** > **SSL-сертификат**.

5 В списке **SSL-сертификат** выберите сторонний сертификат.

6 Нажмите **Сохранить**.

7 В окне **Смена сертификата** для подтверждения действия нажмите **Да**.

8 Установите в хранилище сертификатов узлов SSL-сертификат и корневой сертификат УЦ (если отсутствует).

Чтобы заново использовать в качестве SSL-сертификата самоподписанный сертификат ViPNet Coordinator HW:

1 В списке **SSL-сертификат** выберите самоподписанный сертификат.

2 Нажмите **Сохранить**.

3 В окне **Смена сертификата** для подтверждения действия нажмите **Да**.

Учитывайте, что самоподписанный сертификат будет перевыпущен, поэтому экспортируйте его в папку вашего компьютера и установите в хранилище сертификатов сетевых узлов.

Особенности SSL/TLS-инспекции

- Сетевые фильтры с SSL/TLS-инспекцией рекомендуется располагать в конце списка фильтров.
- В текущей версии ViPNet Coordinator HW встраивание в SSL/TLS-сессию и срабатывание запрещающего правила фиксируется в системном журнале.

- К исключенным из SSL/TLS-инспекции ресурсам не применяются правила межсетевого экрана. Если ресурс или протокол исключен из инспекции, то его трафик считается доверенным и будет пропускаться без дальнейшей обработки межсетевым экраном. При этом трафик пропускается:
  - только в том случае, если создан сетевой фильтр, который содержит параметр SSL/TLS-инспекции;
  - только для тех узлов, для которых в таком фильтре совпадают критерии L3/L4 (адрес отправителя и адрес получателя), если они заданы.
- Возможна некорректная работа исключений SSL/TLS-инспекции для ресурсов с часто меняющимися сертификатами, например `google.com`.
- Возможна некорректная работа SSL/TLS-инспекции для ресурсов, которые используются для обновления ПО, например серверов обновления Microsoft: `https://*.update.microsoft.com`.
- Одновременно с SSL/TLS-инспекцией в сетевых фильтрах не поддерживаются:
  - фильтрация по признакам, которые обрабатываются системой DPI: **Приложения** (`dpiapp`), **Группы приложений** (`dpigroup`) и **Прикладные протоколы** (`dpiprotocol`).
  - фильтрация по действительному IP-адресу прокси-клиента (`proxy-client`);
  - фильтрация по группам объектов «Веб-клиенты» (`user-agent`);
  - действие отклонить (`reject`).
- SSL/TLS-инспекция может быть неприменима для трафика мобильных приложений:
  - Некоторые браузеры не используют системное хранилище сертификатов, поэтому они не доверяют сертификатам, встраиваемым в SSL/TLS-сессии и подписанным SSL-сертификатом ViPNet Coordinator HW. Если это поддерживается браузером, вы можете установить SSL-сертификат в хранилище сертификатов. Иначе рекомендуется использовать другой браузер или исключить необходимые ресурсы из инспекции.
  - Инспекция трафика мобильных приложений, которые используют механизмы противодействия перехвату трафика (например, SSL Pinning), приводит к недоступности сервиса. В этом случае рекомендуется исключить такие ресурсы из инспекции.
- Некоторые ресурсы вместо транспортного протокола TCP и SSL/TLS-шифрования могут использовать протокол QUIC. SSL/TLS-инспекция трафика таких ресурсов не поддерживается. Чтобы обеспечить инспекцию таких сессий, вы можете:
  - Отключить использование протокола QUIC в браузере.
  - Создать сетевой фильтр для блокировки протокола QUIC:

    ```
    hostname# firewall forward add 1 src @any dst @any dpiprotocol QUIC drop
    ```
- Не поддерживается SSL/TLS-инспекция сессий с двусторонней TLS-аутентификацией сервера и клиента (Mutual TLS). Чтобы разрешить взаимодействие сетевых узлов, которые используют двустороннюю аутентификацию, вы можете:
  - Отключить SSL/TLS-инспекцию в сетевом фильтре, разрешающем прохождение трафика между этими узлами.
  - Добавить эти узлы в список исключений SSL/TLS-инспекции.

Настройка подключения к ICAP-серверам

ViPNet Coordinator HW поддерживает взаимодействие с внешними ICAP-серверами в режимах инспекции и репликации HTTP-трафика.

Режим инспекции трафика

В режиме инспекции трафика ICAP-сервер выполняет одну из проверок, соответствующую его типу:

- антивирусную проверку;
- проверку в песочнице (Sandbox-системе);
- проверку в DLP-системе (предотвращение утечек информации).

Проверена совместимость ViPNet Coordinator HW по протоколу ICAP с внешними системами, указанными в таблице ниже. Также возможна работа с другими системами, которые поддерживают взаимодействие по протоколу ICAP.

Таблица 3. Внешние системы, с которыми проверено взаимодействие

Тип	Название	Производитель
Антивирус	Kaspersky Web Traffic Security	АО «Лаборатория Касперского»
Песочница (Sandbox-система)	AVSOFT ATHENA	ООО «АВ Софт»
DLP-система	SearchInform КИБ	ООО «СёрчИнформ»

Проверки задаются в транзитных фильтрах открытой сети. В одном фильтре вы можете указать только один тип проверки.

Одновременно вы можете использовать несколько ICAP-серверов разных типов. При этом трафик пересылается на все из них. В случае, если используется несколько серверов одного типа, ViPNet Coordinator HW ожидает получение ответа:

- если трафик пропущен — от всех из них;
- если трафик заблокирован — от первого ответившего ICAP-сервера.

В зависимости от ответа срабатывают транзитные фильтры открытой сети.

Также вы можете настроить предварительную проверку трафика ICAP-сервером на основании части сообщения, что позволяет увеличить скорость обработки трафика МЭ.

Внимание! При обнаружении вируса проверяемый файл может быть скачан частично из-за особенности потоковой проверки. При этом скачанный фрагмент файла не несет угрозы.

Режим репликации трафика

В режиме репликации трафик пересылается на ICAP-сервер без ожидания ответа от него.

Настройка подключения к ICAP-серверу

1 Выберите **Межсетевой экран** > **ICAP-серверы**.

2 Нажмите **Добавить**.

3 На вкладке **Подключение к серверу**:

3.1 Задайте имя сервера. При необходимости добавьте описание.

3.2 Введите параметры доступа к серверу — IP-адрес или доменное имя, TCP-порт.

3.3 Выберите тип сервера.

3.4 Выберите режим взаимодействия с сервером:

- **Инспекция трафика** — ожидать ответ ICAP-сервера;
- **Репликация трафика** — не ожидать ответ ICAP-сервера.

3.5 Выберите режимы обработки трафика и задайте путь к серверу для выбранных режимов:

- **REQMOD** — режим модификации запроса;
- **RESPMOD** — режим модификации ответа.

4 Если выбран режим **Инспекция трафика**, на вкладке **Обработка трафика**:

4.1 Задайте время ожидания ответа от ICAP-сервера (по умолчанию — 30 секунд).

4.2 Чтобы обрабатывать трафик в случае недоступности сервера (режим `bypass`), нажмите **Пропускать трафик, если ICAP-сервер недоступен**.

4.3 Вы можете включить предварительную проверку данных ICAP-сервером на основании части сообщения, чтобы увеличить скорость обработки трафика МЭ. Для этого:

4.3.1 Нажмите **Использовать режим ICAP Preview**.

4.3.2 В появившемся поле введите объём данных, которые передаются на сервер в режиме предпросмотра.

4.4 Настройте передачу информации о пользователе на сервер:

4.4.1 Выберите данные: **Имя пользователя**, **IP-адрес**, **MAC-адрес**.

4.4.2 В появившемся поле **Заголовок параметра** введите имя заголовка, который используется для передачи данных выбранного типа на сервер. Имя пользователя может передаваться на сервер в формате Base64, для этого нажмите **Кодировать в base64**.

4.4.3 Повторите шаг 4.4 для каждого параметра.

4.5 Нажмите **Сохранить**.

5 Включите  передачу трафика на ICAP-сервер.

Настройка сетевых фильтров

Общие сведения о сетевых фильтрах

Типы фильтров

Фильтры различаются по типу IP-трафика (защищенный, туннелируемый, открытый локальный и транзитный), который они обрабатывают:

- Фильтры защищенной сети — разрешают или блокируют обмен IP-трафиком с узлами сети ViPNet, с которыми ViPNet Coordinator HW имеет связь.
- Фильтры туннелируемых узлов — разрешают или блокируют IP-трафик между туннелируемыми узлами и узлами сети ViPNet, с которыми ViPNet Coordinator HW имеет связь.
- Локальные фильтры открытой сети — разрешают или блокируют IP-трафик между ViPNet Coordinator HW и открытыми узлами.
- Транзитные фильтры открытой сети — разрешают или блокируют IP-трафик между открытыми (или открытым и защищенным) узлами, проходящий через ViPNet Coordinator HW.

Также фильтры разделяются на группы:

- Служебные фильтры — предустановленные фильтры, применяющиеся первыми при обработке IP-пакета; недоступны для изменения пользователем.
- Фильтры политик безопасности — фильтры и правила трансляции адресов в составе политик безопасности Policy Management (модуль ViPNet Prime); применяются немедленно после поступления политик на ViPNet Coordinator HW; недоступны для изменения пользователем.
- Настраиваемые фильтры — фильтры, предустановленные по умолчанию и фильтры, создаваемые пользователем; доступны для изменения пользователем.
- Блокирующий фильтр по умолчанию; недоступен для изменения пользователем.

Порядок применения фильтров

Сетевые фильтры применяются в порядке, указанном на рисунке ниже.

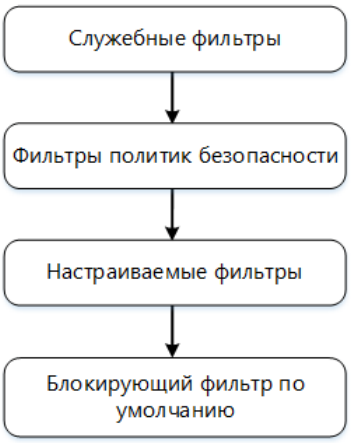


Рисунок 57. Порядок применения фильтров

Настройка сетевых фильтров

В настраиваемых сетевых фильтрах вы можете задать следующие параметры:

- адрес отправителя и получателя IP-пакетов, на которые действует фильтр;
- протоколы, используемые для передачи этих IP-пакетов: TCP, UDP, ICMP, IP и группы протоколов;
- для транзитного фильтра открытой сети и фильтра туннелируемых узлов:
  - приложения;
  - прикладные протоколы;
  - группы приложений и прикладных протоколов;
  - пользователи Active Directory или Captive Portal;
  - фильтрация по URL-категориям;
- расписание применения фильтра — ежедневно, еженедельно или по календарю;
- для транзитного фильтра открытой сети:
  - SSL/TLS-инспекция трафика;
  - проверка IPS;
  - проверку на ICAP-серверах (только в настройке с помощью командного интерпретатора):
    - антивирусная проверка;
    - проверка в песочнице;
    - проверка в DLP-системе;
  - контентная фильтрация с указанием URL-адреса веб-ресурса, HTTP-метода и MIME-типа;
  - фильтрация по действительному IP-адресу прокси-клиента;

- фильтрация по группам объектов «Веб-клиенты»;
- регистрация IP-пакетов при срабатывании фильтра;
- регистрация сессий при срабатывании фильтра;
- действие, применяемое к IP-пакетам:
  - блокировать;
  - пропускать;
  - отклонить и отправить ICMP-уведомление.

Эти параметры вы можете использовать при настройке фильтра как с помощью командного интерпретатора, так и с помощью веб-интерфейса.

Максимальное количество сетевых фильтров зависит от исполнения ViPNet Coordinator HW (см. документ «Подготовка к работе», раздел «Рекомендованное количество сетевых фильтров»).

Подсчет срабатываний фильтров

Для каждого фильтра ведется постоянный подсчет срабатываний, начиная с момента первого включения ViPNet Coordinator HW до первого сброса срабатываний из ViPNet Prime вручную, и далее — между сбросами срабатываний из ViPNet Prime. Перезагрузка ViPNet Coordinator HW, обновление ПО или переключение узлов кластера не влияют на подсчет срабатываний. Просмотр срабатываний фильтров доступен только в веб-интерфейсе ViPNet Coordinator HW.

Создание и изменение сетевых фильтров

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

2 Выберите вкладку сетевых фильтров нужного типа:
   - **Фильтры защищенной сети**.
   - **Фильтры туннелируемых узлов**.
   - **Локальные фильтры открытой сети**.
   - **Транзитные фильтры открытой сети**.

3 Выполните одно из действий:
   - Чтобы создать фильтр, на панели инструментов нажмите **Добавить**.
   - Чтобы изменить фильтр, наведите указатель мыши на поле названия фильтра и нажмите .
   - Чтобы быстро изменить значения в полях фильтра, наведите указатель мыши на соответствующее поле и нажмите .

4 В окне **Создание сетевого фильтра** или **Параметры сетевого фильтра**:

4.1 При создании нового фильтра задайте его название.

4.2 При необходимости сразу включите фильтр **Включено**.

4.3 Выберите действие фильтра:

- **Блокировать трафик**.

Примечание. Применение блокирующего фильтра защищенной сети либо блокирующего локального фильтра открытой сети, либо блокирующего фильтра туннелируемых узлов к установленному соединению не блокирует его работу до истечения времени жизни соединения. После этого при попытке повторного соединения на него уже будет действовать новый блокирующий фильтр.

Блокирующий транзитный фильтр открытой сети действует сразу после его применения. Если разрешенное ранее соединение попадает под действие блокирующего транзитного фильтра, то оно будет заблокировано сразу, не дожидаясь истечения времени жизни соединения.

- **Пропускать трафик**.
- **Отклонять трафик с ответом**. В этом случае также выберите из списка нужный ответ.

4.4 При необходимости включите регистрацию IP-пакетов при срабатывании фильтра.

4.5 При необходимости включите регистрацию сессий при срабатывании фильтра. Вы можете настроить регистрацию определенных состояний сессии. По умолчанию отслеживается начало и окончание сессии.

Примечание. При отслеживании всех состояний в журнале сессий регистрируются внутренние состояния сессии в соответствии с протоколом 3–4 уровня OSI.

4.6 Для транзитных фильтров открытой сети вы можете включить инспекцию трафика:

- **SSL/TLS-инспекция**

  Подробнее см. Настройка SSL/TLS-инспекции трафика.

- **Предотвращение вторжений (IPS) и обнаружение вредоносного ПО**

  Подробнее см. Настройка предотвращения вторжений.

4.7 В зависимости от типа фильтра в разделе **Добавить** задайте параметры:

Примечание. При задании этих параметров вы можете использовать объекты и группы объектов сетевых фильтров (см. Объекты сетевых фильтров и правил трансляции адресов).

- для фильтров защищенной сети:
  - протоколы: IP, TCP, UDP, ICMP;
  - источники: ViPNet-узлы;

- назначения: ViPNet-узлы;

- для фильтров туннелируемых узлов:
  - пользователей Active Directory и Captive Portal;
  - приложения и группы приложений, классифицируемые DPI;
  - протоколы: IP, TCP, UDP, ICMP, группы протоколов, а также протоколы, классифицируемые DPI;
  - источники: ViPNet-узлы, IP-адреса, их диапазоны и группы, DNS-имена, туннелируемые IP-адреса;
  - назначения: ViPNet-узлы, IP-адреса, их диапазоны и группы, DNS-имена, туннелируемые IP-адреса;
- для локальных фильтров открытой сети:
  - протоколы: IP, TCP, UDP, ICMP, группы протоколов;
  - источники: ViPNet-узлы, IP-адреса, их диапазоны и группы, DNS-имена, MAC-адреса, страны;
  - назначения: ViPNet-узлы, IP-адреса, их диапазоны и группы, DNS-имена, страны;
- для транзитных фильтров открытой сети:
  - пользователей Active Directory и Captive Portal;
  - приложения и группы приложений, классифицируемые DPI;
  - протоколы: IP, TCP (в том числе флаги), UDP, ICMP, группы протоколов, а также протоколы, классифицируемые DPI;
  - источники: IP-адреса, их диапазоны и группы, DNS-имена, MAC-адреса, IP-адреса из HTTP-заголовка XFF, группы веб-клиентов, страны;
  - назначения: IP-адреса, их диапазоны и группы, DNS-имена, веб-ресурс, URL-категории, страны.

Примечание. Если вы указали приложения, учитывайте ограничения, действующие для некоторых приложений (см. Особенности фильтрации по приложениям и прикладным протоколам). Если вы выбрали отдельное приложение или прикладной протокол, то вы не можете выбрать группу приложений и наоборот.

Если вы уже указали приложение, то выбор прикладных протоколов будет ограничен протоколами, которые поддерживает выбранное приложение.



При создании транзитных фильтров открытой сети и фильтров туннелируемых узлов необходимо учитывать следующие особенности использования параметров приложения и прикладного протокола для блокировки неизвестного трафика:

- приложение **Unknown** — классификация приложения завершена, приложение не определено (не входит в список известных приложений). Может использоваться для блокировки всех неизвестных приложений.
- прикладной протокол **Unknown** — классификация протокола завершена, протокол не определен (не входит в список известных прикладных протоколов). Может использоваться для блокировки всех неизвестных прикладных протоколов.

Примечание. Сетевые фильтры, в которых заданы пользователи сети, имеют ограничения:

- Имена пользователей должны быть на латинице.
- Если IP-пакет попадает под действие сетевого фильтра, в котором задан пользователь, то IP-адрес этого пользователя сопоставляется с адресом источника или назначения IP-пакета. Фильтр сработает в том случае, если адрес источника или назначения IP-пакета совпадет с адресом пользователя AD или СР.
- В случае, когда на одном сетевом узле, подключенном к контроллеру домена AD, выполнили вход несколько пользователей, то будут действовать сетевые фильтры для последнего пользователя, который вошел в домен.

Примечание. При задании адреса веб-ресурса учитывайте **Действие по отношению к странице ресурса**:

- **Включать** (по умолчанию) — при совпадении адреса веб-ресурса фильтр срабатывает с заданным в нем действием.
- **Исключать** — при совпадении адреса веб-ресурса фильтр срабатывает с инверсией заданного в нем действия. Аналог префикса `!` при задании URL-адреса фильтра, создаваемого в командном интерпретаторе.

Например, выбор **Исключать** для веб-ресурса `cloud.mail.ru` в фильтре с действием **Пропускать** означает блокировку этого ресурса при срабатывании фильтра.

Рекомендуется в одном фильтре сначала добавить один или несколько адресов веб-ресурсов с действием **Исключать**, затем один адрес веб-ресурса с действием **Включать**.

4.8 По умолчанию фильтр действует всегда. При необходимости задайте расписание его действия:

- укажите временной диапазон;
- выберите расписание из группы расписаний.

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

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

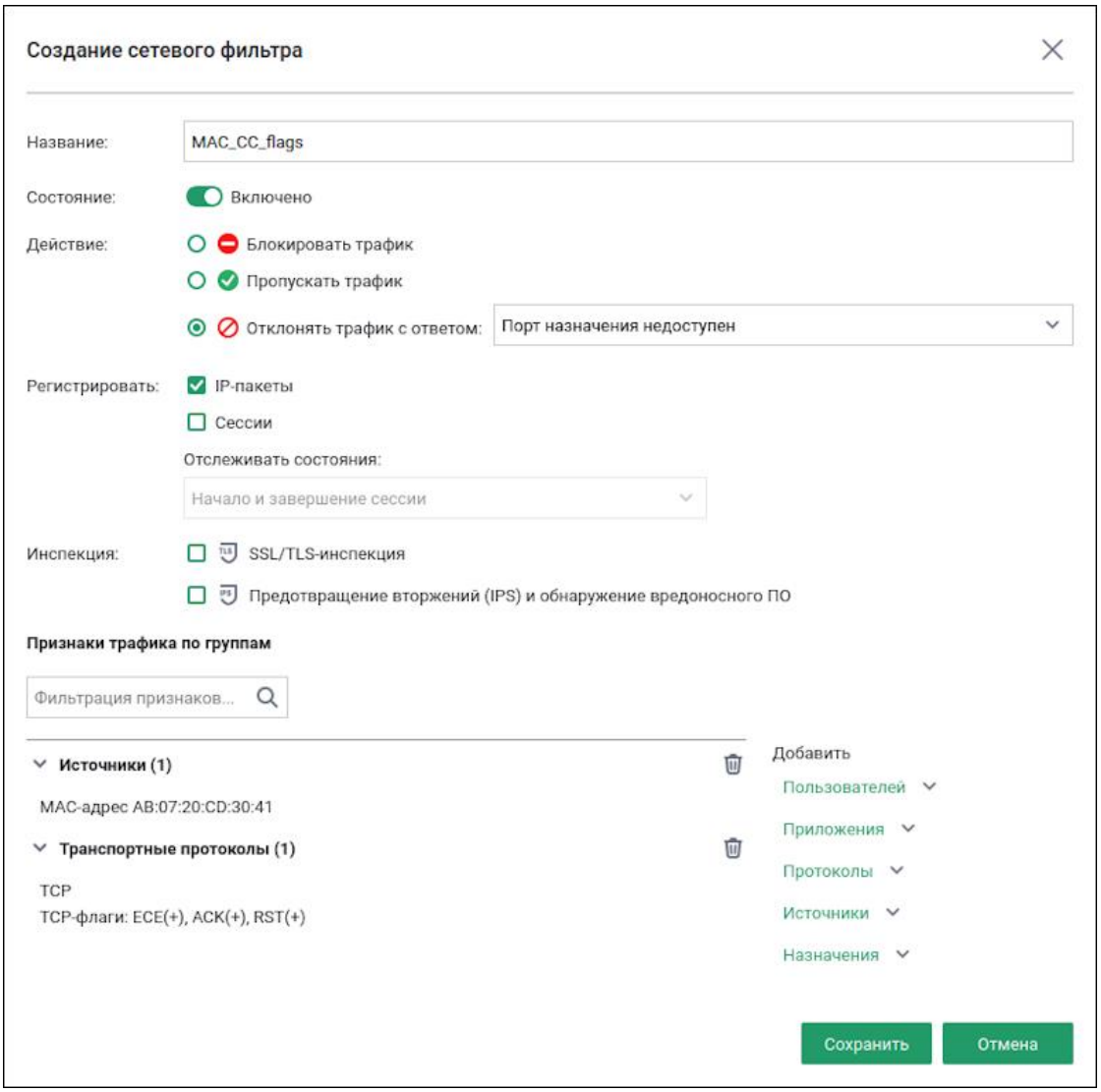


Рисунок 58. Настройка параметров транзитного фильтра открытой сети

5 Нажмите **Сохранить**.

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

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

7 На панели справа сверху нажмите **Применить все**.

Просмотр сетевых фильтров

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

2 Выберите вкладку сетевых фильтров нужного типа, чтобы посмотреть список и параметры фильтров.

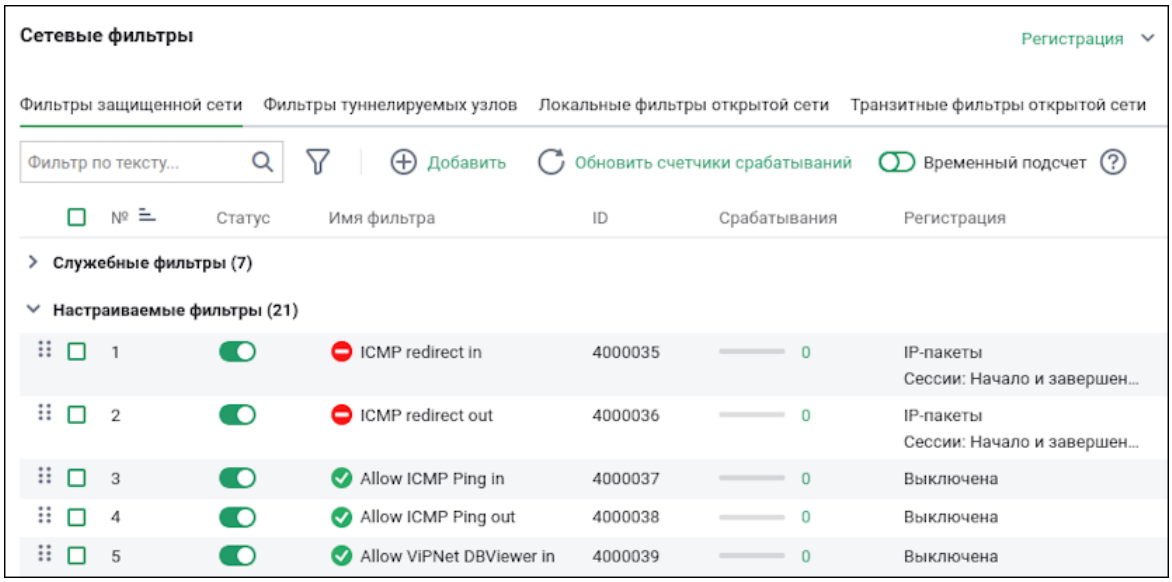


Рисунок 59. Просмотр сетевых фильтров защищенной сети

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

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

По умолчанию в поле **Срабатывания** отображаются значения постоянного подсчета срабатываний фильтров (см. Общие сведения о сетевых фильтрах). Для удобства отслеживания частоты срабатывания фильтров вы можете включить **Временный подсчет** срабатываний по каждому типу фильтров: подсчет и отображение срабатываний начнутся заново с момента включения. При этом постоянный подсчет срабатываний будет продолжен. Чтобы вернуться к отображению значений постоянного подсчета срабатываний, выключите **Временный подсчет**.

Значения срабатываний в обоих режимах обновляются автоматически с задержкой порядка 30 секунд при открытии вкладки типа фильтров или при обновлении страницы браузера. Чтобы обновить значения срабатываний вручную, нажмите **Обновить счетчики срабатываний**.

Чтобы просмотреть сводные или подробные сведения о сетевых фильтрах и правилах трансляции адресов:

1 Выберите **Состояние системы**.



Рисунок 60. Сводные сведения о сетевых фильтрах и правилах трансляции адресов

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

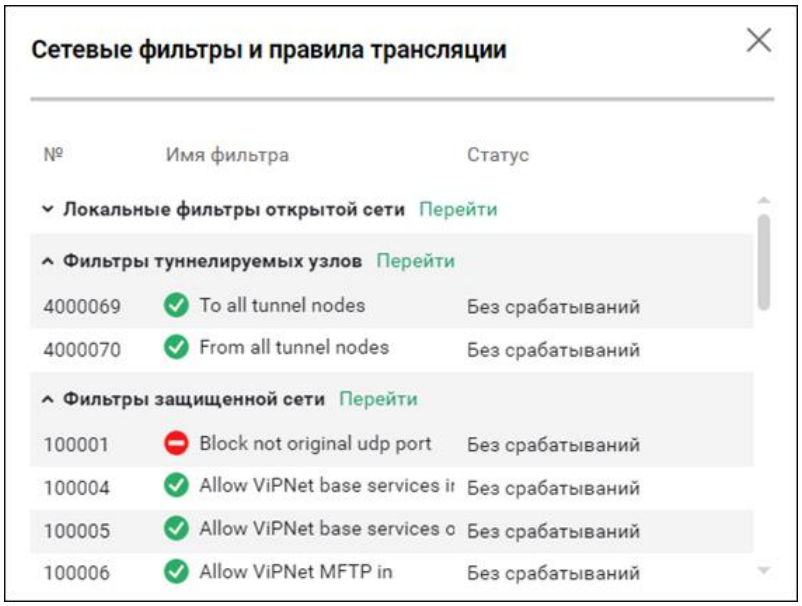


Рисунок 61. Подробные сведения о сетевых фильтрах и правилах трансляции адресов

Изменение порядка применения настраиваемых фильтров

Необходимость изменения порядка применения настраиваемых фильтров может быть вызвана как изменением последовательности фильтрации IP-пакетов, так и частотой срабатывания фильтров.

Фильтры, срабатывающие наиболее часто, целесообразно применять первыми. Это позволит оптимизировать скорость фильтрации трафика.

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

2 Выберите вкладку фильтров нужного типа.

3 В разделе **Настраиваемые фильтры** наведите указатель мыши на значок строки фильтра и перетащите ее на нужную позицию.

4 Нажмите **Применить все**.

Изменение порядка применения настраиваемых фильтров влияет на подсчет срабатываний. Чтобы подсчет соответствовал новому порядку применения фильтров, сбросьте значения срабатываний в ViPNet Prime.

Настройка регистрации IP-пакетов и сессий при срабатывании фильтров

Каждый сетевой фильтр содержит параметры, которые определяют:

- регистрировать обработанные им IP-пакеты в журнале IP-пакетов или нет;
- регистрировать сессию в журнале сессий или нет.

Вы можете указать это в настройках сетевого фильтра. Значение параметров отображаются в столбце **Регистрация** при просмотре таблицы сетевых фильтров.

Значение параметра по регистрации IP-пакетов учитывается, только если выбран способ регистрации IP-пакетов по фильтрам. При этом настраивать этот параметр в сетевых фильтрах вы можете независимо от используемого способа регистрации IP-пакетов. Подробнее о способах регистрации IP-пакетов см. Журнал IP-пакетов.

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

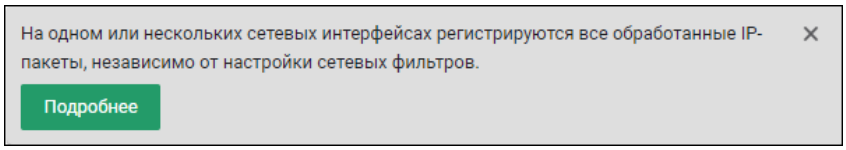


Рисунок 62. Включена регистрация IP-пакетов по интерфейсам

В таком случае, чтобы включить регистрацию IP-пакетов по фильтрам, см. документ «Настройка с помощью командного интерпретатора», раздел «Журнал IP-пакетов».

Выборочная настройка регистрации IP-пакетов настраиваемых фильтров

Чтобы настроить регистрацию IP-пакетов при срабатывании определённых настраиваемых фильтров:

1. Выберите **Межсетевой экран** > **Сетевые фильтры**.
2. Выберите вкладку сетевых фильтров нужного типа.
3. Выберите нужные фильтры с помощью флажков.
4. На панели инструментов выберите меню **Регистрация IP-пакетов** одну из настроек:
   - **Включить регистрацию**.
   - **Отключить регистрацию**.
5. Нажмите **Применить все**.

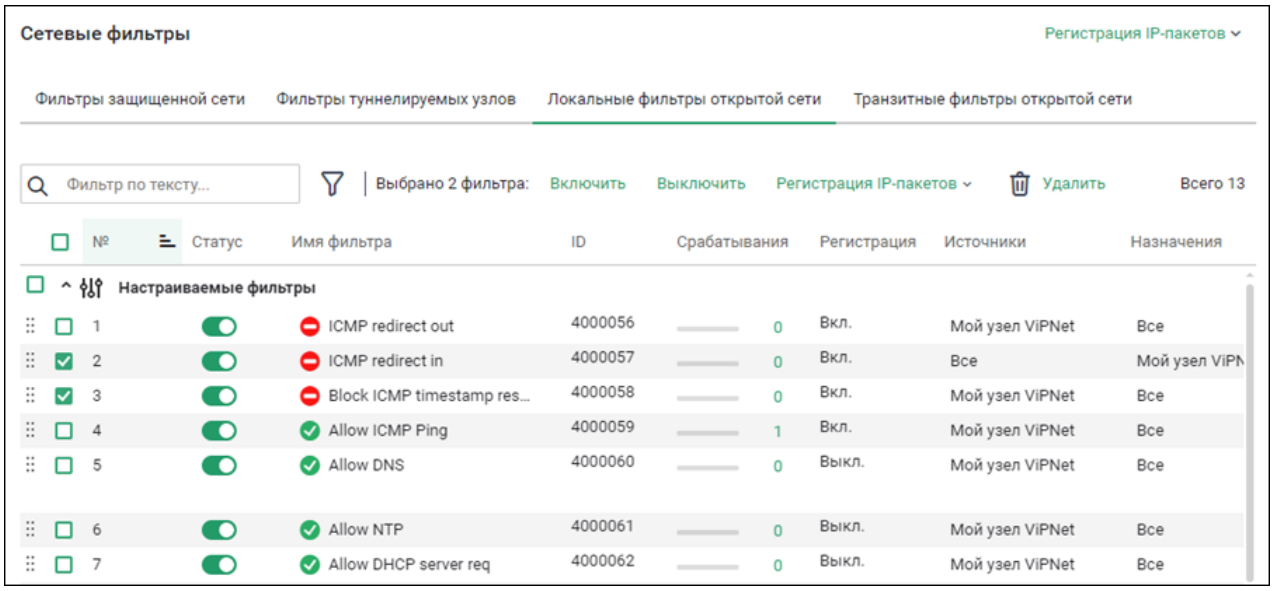


Рисунок 63. Выборочная регистрация IP-пакетов

Чтобы настроить регистрацию IP-пакетов всех настраиваемых фильтров нужного типа, на шаге 3 выберите с помощью флажка группу настраиваемых фильтров.

Настройка регистрации IP-пакетов всех настраиваемых фильтров

Чтобы настроить регистрацию IP-пакетов при срабатывании всех настраиваемых фильтров всех типов:

1. Выберите **Межсетевой экран** > **Сетевые фильтры**.
2. Выберите в меню **Регистрация IP-пакетов** одну из настроек:
   - **Включить для всех фильтров**.
   - **Включить для блокирующих и отклоняющих фильтров**.
   - **Отключить для всех фильтров**.
3. В окне подтверждения нажмите **Да**.
4. Нажмите **Применить все**.

Пример использования групп объектов и сетевых фильтров

Допустим, в компании координатор ViPNet Coordinator HW туннелирует почтовый сервер. Требуется организовать обмен электронными письмами с удаленными пользователями, использующими внешние почтовые серверы, и доступ таких пользователей к электронным письмам на защищенном почтовом сервере.

Обмен электронными письмами с внешними почтовыми серверами выполняется по протоколам SMTP, POP3 и IMAP. Поэтому надо создать сетевой фильтр, разрешающий прием и передачу IP-пакетов по 25-му порту протокола TCP (для протокола SMTP), а также по 110-му и 143-му портам (для протоколов POP3 и IMAP соответственно).

Чтобы создать группу почтовых протоколов SMTP, POP3 и IMAP:

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

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

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

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

2.2.1 **Протоколы** — **TCP.**

2.2.2 **Источник** — **Все порты.**

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

2.2.4 Нажмите **Сохранить**.

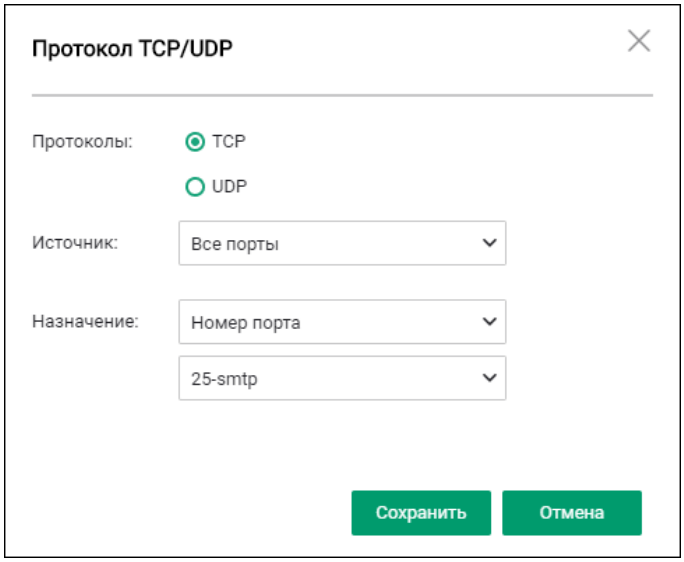


Рисунок 64. Добавление протокола SMTP в группу

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

3 Нажмите **Сохранить**.

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

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

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

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

2.1 Укажите имя сетевого фильтра.

2.2 Включите фильтр в поле **Состояние**.

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

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

2.4.1 Выберите ранее созданную группу почтовых протоколов.

2.4.2 Нажмите **Сохранить**.

2.5 Нажмите **Сохранить**.

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

Примеры использования транзитных фильтров

По умолчанию весь транзитный трафик блокируется на ViPNet Coordinator HW. Вы можете создавать транзитные фильтры и использовать их для управления трафиком.

Настройка фильтрации трафика по пользователю

Предположим, что вам нужно настроить фильтрацию трафика для пользователя `ivanov` таким образом, чтобы:

- разрешить отправку электронных писем только с помощью корпоративного почтового приложения Microsoft Outlook и запретить использование сторонних почтовых сервисов;
- запретить доступ к социальной сети Facebook;
- запретить доступ к облачным файловым сервисам Dropbox и Google Drive.

Для настройки фильтрации трафика:

1 Выберите **Межсетевой экран** > **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

2 Нажмите **Добавить**.

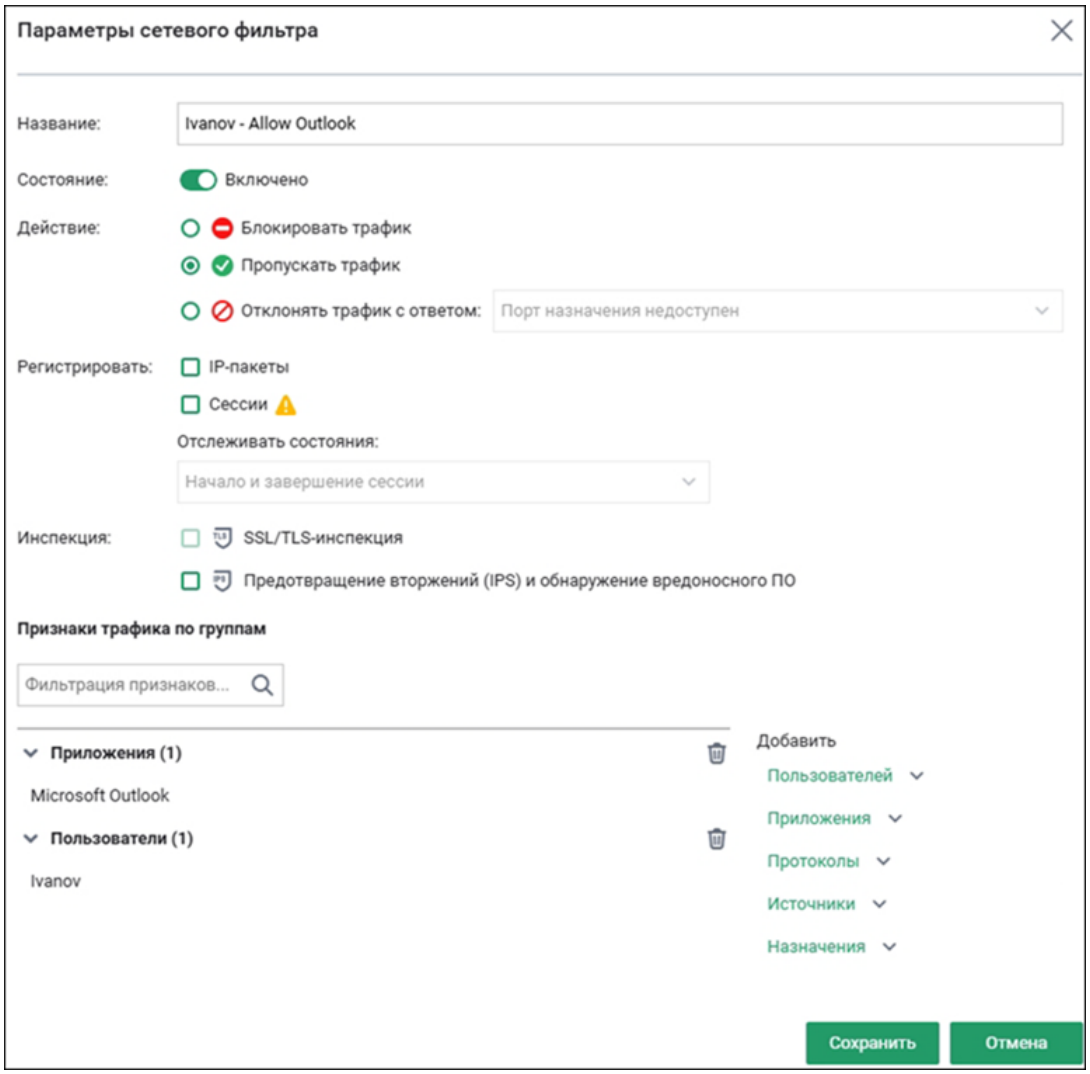


Рисунок 65. Добавление транзитного фильтра открытой сети

3 Создайте транзитный фильтр открытой сети, который будет разрешать отправку писем в приложении Microsoft Outlook для пользователя `Ivanov`:

3.1 В поле **Название** укажите название фильтра — `Ivanov - Allow Outlook`.

3.2 Установите переключатель **Состояние** в положение **Включено**.

3.3 Установите переключатель **Действие** в положение **Пропускать трафик**.

3.4 В разделе **Добавить** раскройте список **Пользователей**, выберите **Ввести имя пользователя** и добавьте пользователя `Ivanov`.

3.5 В разделе **Добавить** раскройте список **Приложения**, выберите **Приложения** и добавьте приложение `Microsoft Outlook`.

3.6 Нажмите **Сохранить**.

4 Создайте транзитный фильтр открытой сети, который будет блокировать отправку писем через сторонние почтовые сервисы для пользователя `Ivanov`:

4.1 В поле **Название** укажите название фильтра — `Ivanov - Block other mail services`.

4.2 Установите переключатель **Состояние** в положение **Включено**.

4.3 Установите переключатель **Действие** в положение **Блокировать трафик**.

4.4 В разделе **Добавить** раскройте список **Пользователей**, выберите **Ввести имя пользователя** и добавьте пользователя `Ivanov`.

4.5 В разделе **Добавить** раскройте список **Приложения**, выберите **Группы приложений** и добавьте группу приложений `Mail`.

4.6 Нажмите **Сохранить**.

5 По аналогии создания блокирующего фильтра для группы приложений Mail создайте транзитный фильтр открытой сети, который будет блокировать трафик приложений социальной сети Facebook и облачных файловых сервисов Dropbox и Google Drive. В качестве значения **Приложения** выберите `Facebook`, `Dropbox` и `Google Drive`**,** а для значения **Пользователей** укажите `Ivanov`**.**

6 На странице **Сетевые фильтры** нажмите **Применить все**.

Настройка фильтрации трафика Torrent-клиентов

Чтобы заблокировать работу Torrent-клиентов на компьютерах локальной сети, создайте запрещающий сетевой фильтр `Block BitTorrent` для протоколов BitTorrent (обмен файлами между Torrent-клиентами) и Teredo (инкапсуляция пакетов IPv6 в IPv4, позволяющая Torrent-клиентам обмениваться файлами при блокировке BitTorrent):

1 Выберите **Межсетевой экран** > **Сетевые фильтры** > **Транзитные** и нажмите **Добавить**:

2 Настройте параметры фильтра:

2.1 В поле **Название** укажите название фильтра — `Block BitTorrent`.

2.2 Включите фильтр.

2.3 Выберите **Действие по отношению к трафику** > **Блокировать трафик**.

2.4 Выберите **Добавить** > **Сервисы и приложения** > **Прикладные протоколы** , затем выберите в списке:

- `BitTorrent`;
- `Teredo`.

2.5 Нажмите **Сохранить**.

3 На странице **Сетевые фильтры** нажмите **Применить все**.

Деактивация транзитных фильтров после обновления ПО

После обновления ПО ViPNet Coordinator HW могут измениться схемы описания прикладных протоколов, приложений и групп приложений. В этом случае транзитные фильтры будут изменены:

- Если транзитный фильтр содержит параметр (прикладной протокол, приложение или группу приложений), который отсутствует в новой схеме, то такой параметр не учитывается и помечается как неподдерживаемый (**Unsupported**).
- Если в транзитном фильтре остаются только неподдерживаемые параметры, то фильтр помечается как неактивный (**Inactive**) и не используется для фильтрации трафика.

При отображении в веб-интерфейсе неподдерживаемый прикладной протокол, приложение, группа приложений выделяются красным цветом.

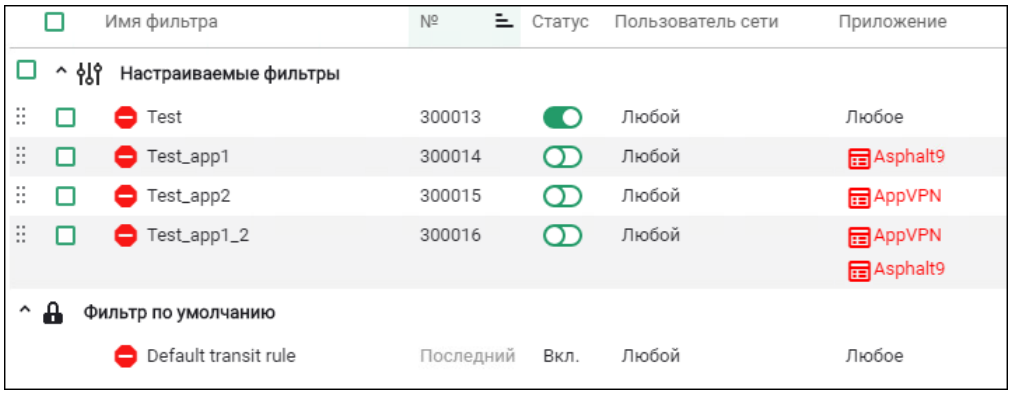


Рисунок 66. Отображение неактивных фильтров

Вы можете изменить неактивный фильтр, задав поддерживаемые прикладные протоколы, приложения или группы приложений, а затем активировать его.

Настройка правил трансляции адресов

Общие сведения о трансляции сетевых адресов

Трансляция сетевых адресов (NAT) — механизм преобразования IP-адресов одной сети в IP-адреса другой сети в соответствии с RFC 2663.



Внимание! Правила трансляции сетевых адресов, описанные в этом разделе, относятся только к открытому трафику.

ViPNet Coordinator HW может выполнять:

- Трансляцию адреса источника (динамическую трансляцию или masquerading).

  В этом случае при прохождении через координатор IP-пакетов от отправителей с частными IP-адресами в них заменяется адрес отправителя на внешний (реальный) адрес интерфейса координатора или адрес из другой сети. 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.
  - Для балансировки нагрузки сети.

- Трансляцию адреса назначения (статическая трансляция или port forwarding).

  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 настраивается с помощью правил. При этом координатор должен иметь как минимум два сетевых интерфейса:

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

- внутренний — имеет частный IP-адрес.

Подсчет срабатываний правил трансляции адресов

Для каждого правила трансляции сетевых адресов ведется постоянный подсчет срабатываний, начиная с момента первого включения ViPNet Coordinator HW до первого сброса срабатываний из ViPNet Prime вручную, и далее — между сбросами срабатываний из ViPNet Prime. Перезагрузка ViPNet Coordinator HW, обновление ПО или переключение узлов кластера не влияют на подсчет срабатываний. Просмотр срабатываний правил трансляции адресов доступен только в веб-интерфейсе ViPNet Coordinator HW.

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 67. Организация доступа в интернет при помощи правила трансляции IP-адреса источника

Если на координаторе настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через координатор из локальной сети в интернет, будут преобразованы:

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

запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.

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

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.

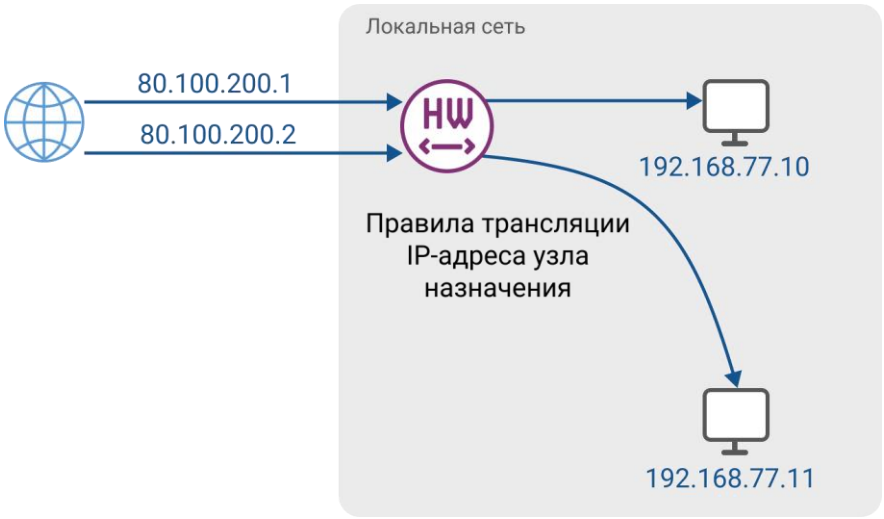


Рисунок 68. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

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

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) локальным IP-адресом в соответствии с правилом. Затем пакет 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.

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 HW, 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 HW, на сетевом устройстве, расположенным за ViPNet Coordinator HW, настройте обратную маршрутизацию на ViPNet Coordinator HW (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 HW 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**.

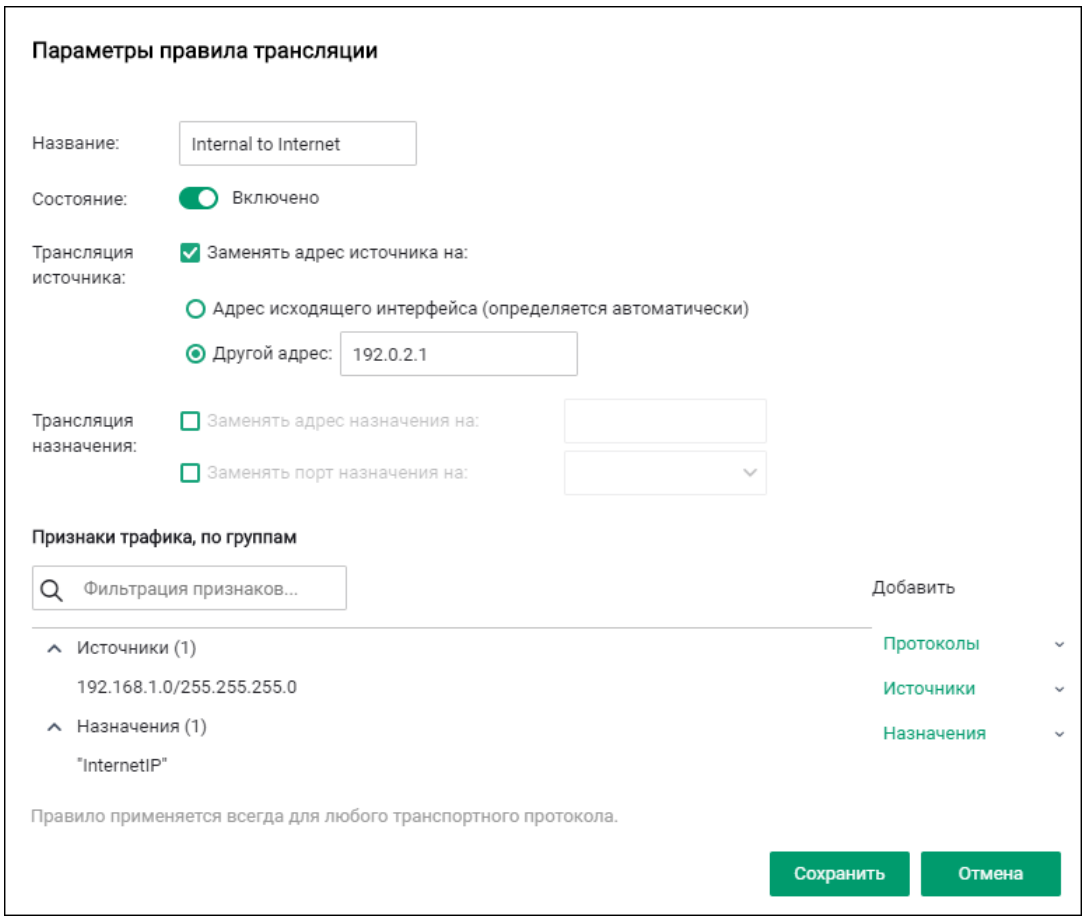


Рисунок 69. Создание правила трансляции адресов

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.

Просмотр правил трансляции адресов

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

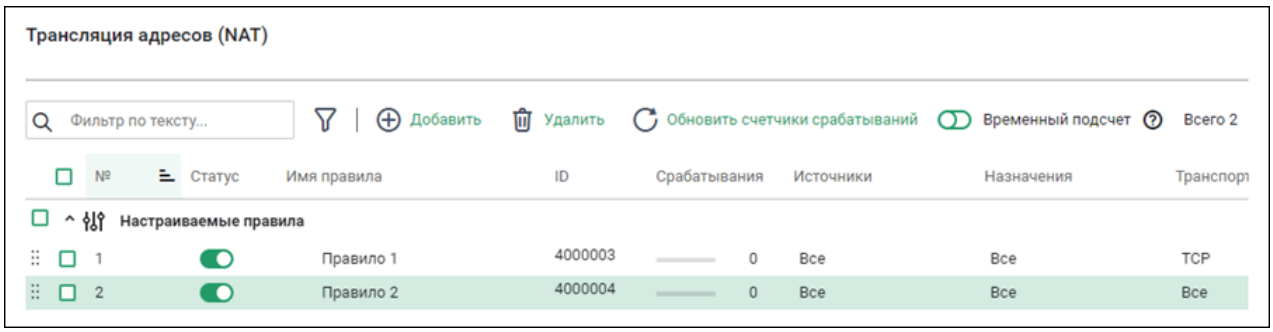


Рисунок 70. Просмотр правил трансляции адресов

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

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

По умолчанию в поле **Срабатывания** отображаются значения постоянного подсчета срабатываний правил трансляции (см. Общие сведения о трансляции сетевых адресов). Для удобства отслеживания частоты срабатывания правил вы можете включить **Временный подсчет** срабатываний: подсчет и отображение срабатываний начнутся заново с момента включения. При этом постоянный подсчет срабатываний продолжается. Чтобы вернуться к отображению значений постоянного подсчета срабатываний, выключите **Временный подсчет**.

Значения срабатываний в обоих режимах 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**.

Изменение порядка применения правил трансляции адресов

Необходимость изменения порядка применения правил трансляции адресов может быть вызвана частотой их срабатывания. Правила, срабатывающие наиболее часто, целесообразно переместить в начало списка. Это позволит оптимизировать скорость обработки трафика.

1 Выберите **Межсетевой экран** > **Правила трансляции (NAT)**.

2. В списке правил наведите указатель мыши на значок строки правила и перетащите ее на нужную позицию.
3. Нажмите **Применить все**.

Изменение порядка применения правил трансляции влияет на подсчет срабатываний. Чтобы подсчет соответствовал новому порядку применения правил, сбросьте значения срабатываний в ViPNet Prime.

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

О прикладных протоколах

Прикладные протоколы обеспечивают работу пользовательских сетевых сервисов, например, IP-телефонии, DNS-службы, FTP-службы. При использовании данных служб IP-адреса часто передаются в теле IP-пакета. Эта особенность может повлиять на доступность сервисов в защищенной сети с виртуальной адресацией или трансляцией сетевых адресов. Кроме того, некоторые прикладные протоколы, помимо управляющего соединения, открывают для передачи данных дополнительные соединения на случайно выбранный порт. Поскольку номер порта заранее неизвестен, то для IP-пакетов невозможно создать разрешающий сетевой фильтр, следовательно, соединение будет заблокировано.

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

- Подмену виртуального IP-адреса узла защищённой сети в теле IP-пакета на реальный.
- Статическую и динамическую трансляцию IP-адреса при передаче транзитного трафика (только для протокола FTP).
- Включение сетевого фильтра, пропускающего IP-пакеты, для дополнительного соединения на случайно выбранный порт, который используется прикладным протоколом. При этом для установления управляющего соединения с открытыми узлами на узле необходимо задать соответствующие фильтры открытой сети.



Внимание! Обработка прикладного протокола в сетевом трафике, проходящем трансляцию сетевых адресов назначения, поддерживается только для прикладного протокола FTP в случае, когда FTP-клиент создает соединение с ViPNet Coordinator HW, который перенаправляет трафик к FTP-серверу по открытому каналу.

В ViPNet Coordinator HW можно настроить обработку следующих прикладных протоколов:

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

  Команды FTP-протокола EPRT и EPSV, используемые некоторыми FTP-клиентами, не поддерживаются ViPNet Coordinator HW.
- H.323 — для передачи мультимедийных данных в IP-сетях (IP-телефония, видео- и аудиоконференции).

Передача мультимедийных данных с использованием протокола H.323 возможна только между телекоммуникационными серверами, туннелируемыми ViPNet Coordinator HW. При этом на координаторе должен быть разрешен весь туннелируемый трафик, поскольку между телекоммуникационными серверами могут устанавливаться дополнительные соединения.

- SCCP — для передачи сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты (Cisco Unity Connection и Cisco Unified Communication Manager (CallManager)).

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

  Примечание. ViPNet Coordinator HW также поддерживает обработку прикладного протокола Cisco NetMeeting для организации 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.

- SIP — для установки соединений, включающих обмен мультимедийными данными между клиентами (IP-телефония, видео- и аудиоконференции).

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

  Для некоторых SIP-клиентов могут не обрабатываться такие дополнительные данные, как телефонные справочники, информация о доступности абонента и другие.

По умолчанию установка соединения с открытыми узлами запрещена. Чтобы разрешить ее, создайте разрешающий сетевой фильтр.

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 удаленным 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 DNS-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).

Установка TCP-соединений по протоколу FTP происходит в следующем порядке:

1. Клиент создает 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:
   - номер порта, открытого клиентом для получения данных с сервера (активный режим);
   - запрос на номер порта сервера, к которому будет подключаться клиент (пассивный режим).
3. В зависимости от используемого режима передачи данных, соединение устанавливается одним из двух способов:
   - сервер создает дополнительное соединение для передачи данных на указанный клиентом порт (активный режим);
   - сервер по управляющему соединению передает клиенту номер порта, к которому клиент создает дополнительное соединение (пассивный режим).

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

Для установки управляющего и дополнительного соединений в активном или пассивном режиме работы протокола FTP:

1. Создайте фильтр открытой сети, разрешающий исходящее TCP-соединение на 21-й порт FTP-сервера.
2. Для разрешения дополнительного соединения в активном режиме работы включите обработку протокола FTP, которая добавляет необходимый сетевой фильтр.
3. Для разрешения дополнительного соединения в пассивном режиме работы настройки не требуются.

Обработка протокола SIP

SIP-клиент отправляет запрос (например, приглашение для установки соединения, подтверждение приема ответа на запрос, завершение соединения) другому SIP-клиенту с указанием его SIP-адреса. В зависимости от способа установки соединения запрос направляется второму клиенту либо напрямую, либо через SIP-сервер. Вызываемый клиент передает вызывающему клиенту ответ на запрос (например, информацию об успешной обработке запроса, отклонении вызова, ошибке при обработке запроса). По умолчанию TCP- и UDP-соединения устанавливаются через порты 5060 и 5080.

Чтобы установить соединение между SIP-клиентами:

1. Убедитесь, что включена обработка протокола SIP.
2. Если хотя бы один из SIP-клиентов является открытым узлом, создайте фильтр открытой сети, разрешающий входящее и исходящее соединение по протоколам TCP и UDP на порты 5060 и 5080.



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 определенного диапазона. Поэтому если хотя бы один из SIP-клиентов является открытым узлом, возможность использования динамических портов необходимо отключить в настройках SIP-клиента.

При установке соединений между SIP-клиентами действуют ограничения:

- Между SIP-клиентами нельзя использовать статическую или динамическую трансляцию IP-адресов.
- Если хотя бы один из SIP-клиентов является открытым узлом, то для всех узлов защищённой сети должна быть настроена видимость по реальным IP-адресам.

Настройка параметров обработки прикладных протоколов

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

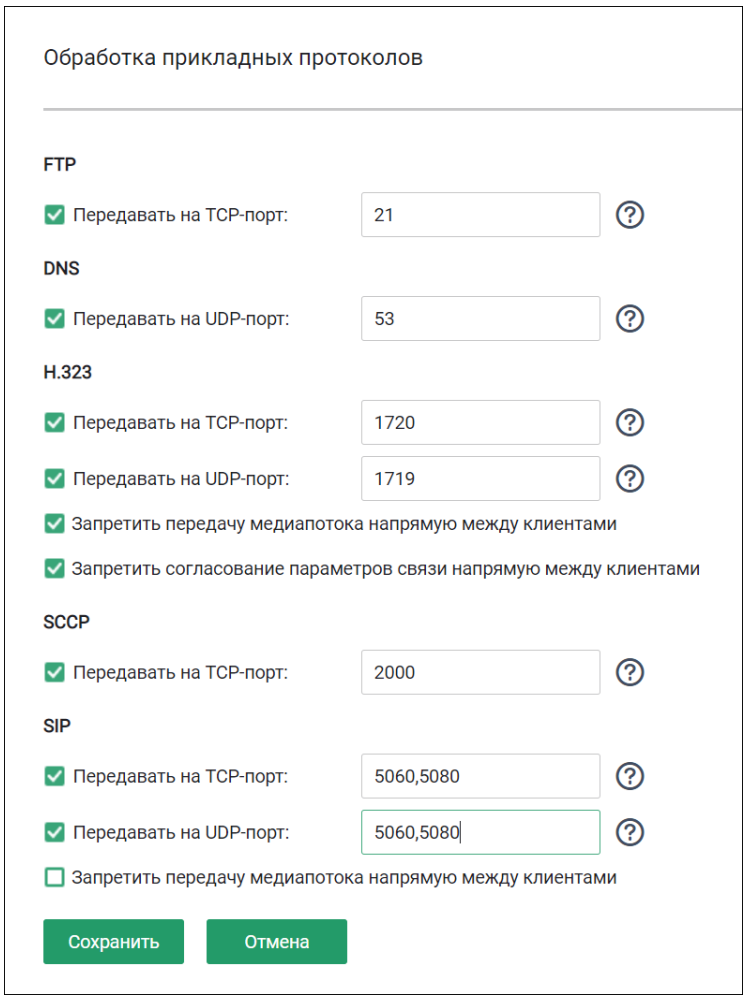


Рисунок 71. Обработка прикладных протоколов

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. Чтобы включить использование прикладного протокола установите флажок.

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

4 Настройте режим подключения для протоколов SIP и H323:

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

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

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



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

5 Нажмите **Сохранить**.



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

Настройка блокировки трафика по списку IP-адресов

Вы можете настроить блокировку сетевого трафика от узлов, IP-адреса которых входят в заранее подготовленный список.

Список IP-адресов задается в файле в формате CSV или TXT. Файл должен быть сохранен в кодировке UTF-8.

Каждый адрес указывается в файле в отдельной строке и может быть задан в виде:

- IP-адреса (например `192.168.10.5`);
- подсети IP-адресов (задаётся в формате адресации CIDR, например `192.168.10/24`);
- диапазона IP-адресов (задаётся через дефис, например `192.168.10.5-192.168.10.255`).

Допускается наличие дополнительных данных (заголовки, порт, страна и т.д.) в строках, при этом адрес должен быть указан в начале строки. При загрузке списка будут считаны только адреса, дополнительные данные будут проигнорированы.

Примечание. Во избежание некорректной обработки списка не рекомендуется задавать адреса в формате, который может считываться неоднозначно. Например:

- строка `192.168.150.1700` будет импортирована как `192.168.150.170`;
- `192.168.150.23-1` — как `192.168.150.23`;
- `192.168.150.0/255.255.0.0` — как `192.168.150.0/25`.

Дополнительные данные рекомендуется разделять от записи IP-адреса каким-либо символом, например пробелом или точкой с запятой.

Максимальный размер списка — 50 Мбайт.

Чтобы загрузить список адресов для блокировки:

1. Выберите **Межсетевой экран** > **Блокировка по спискам**.
2. В разделе **Блокировка по списку IP-адресов** нажмите **Загрузить список**.
3. Выберите файл списка.

После загрузки списка будет автоматически включена блокировка заданных IP-адресов — будут созданы служебные сетевые фильтры `Block addresses from blocklist DB` для блокировки транзитного и локального трафика. Загруженные из файла адреса будут отображаться в таблице.

Примечание. В связи с особенностями реализации, в текущей версии ViPNet Coordinator HW:

- В веб-интерфейсе для созданных служебных сетевых фильтров не отображаются поля **Источники** и **Назначения**. Источниками и назначениями для них являются IP-адреса, заданные в списке блокировки.
- В командном интерпретаторе в выводе команды `firewall rules show` служебные фильтры отображаются в группе настраиваемых, поэтому нумерация фильтров в веб-интерфейсе и в командном интерпретаторе не совпадает.
- В журнале аудита загрузка и удаление списка IP-адресов фиксируются как операции со списком в базе GeoIP.

Вы можете **Обновить** или **Удалить** загруженный ранее список IP-адресов:

- При обновлении текущий список будет полностью заменен на новый.
- При удалении списка блокировка по IP-адресам будет автоматически выключена.



5

Настройка сетевых служб

Настройка DHCP-сервера 127

Настройка DHCP-relay 130

Настройка DNS-сервера 132

Настройка NTP-сервера 134

Настройка точки доступа сети Wi-Fi 136

Настройка взаимодействия с Active Directory 138

Настройка взаимодействия с LDAP-сервером 142

Просмотр списка пользователей Active Directory и Captive portal 146

Регистрация событий аутентификации пользователей 147

Настройка DHCP-сервера

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

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

- в одной сети с DHCP-сервером, в том числе в сегментах сети, 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**.

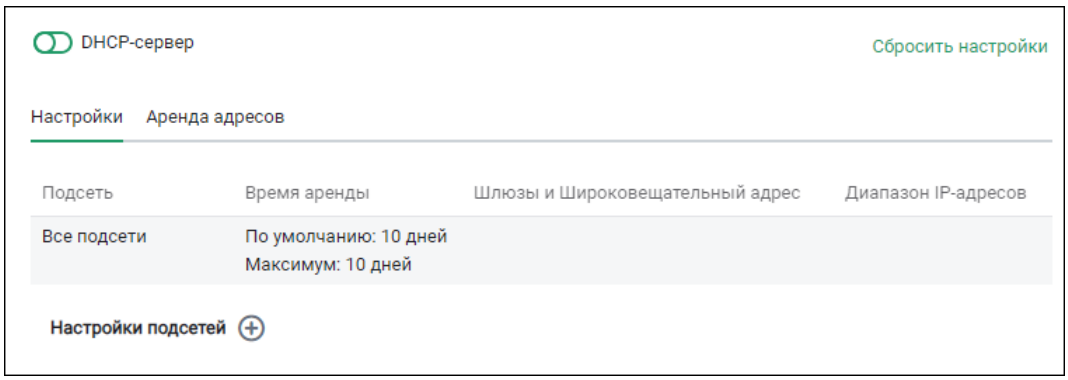


Рисунок 72. Настройка параметров DHCP-сервера

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 HW, 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**.

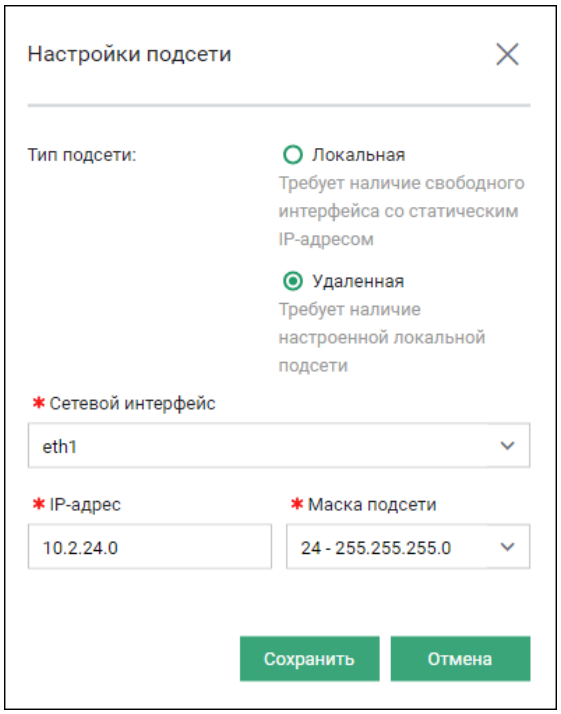


Рисунок 73. Добавление подсети для DHCP-сервера

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

4.1 Выберите подсеть.

4.2 В панели справа выберите нужный параметр и нажмите ⊕.

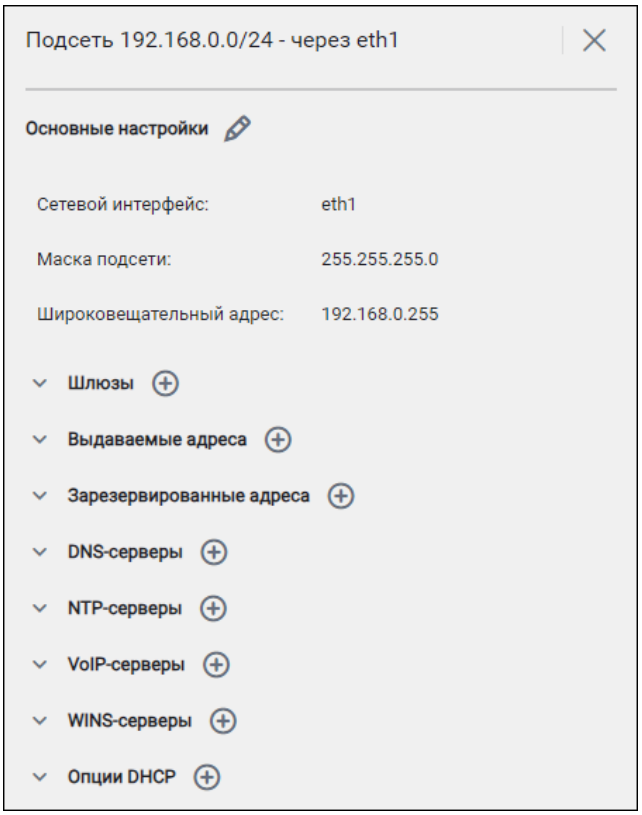


Рисунок 74. Настройка параметров, передаваемых DHCP-сервером

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.

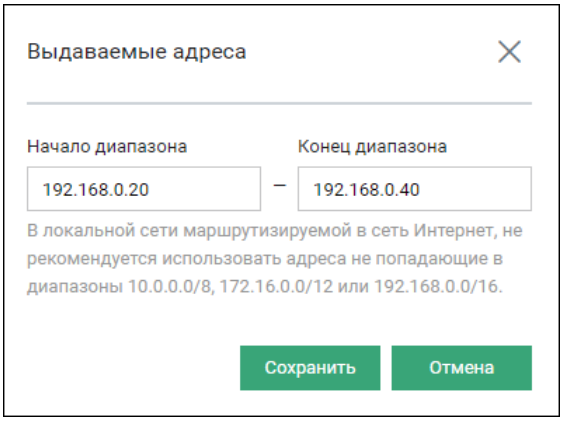


Рисунок 75. Добавление диапазона IP-адресов для DHCP-клиентов

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 HW 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 HW, 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.

К DHCP-серверу через ViPNet Coordinator HW могут обращаться узлы защищённой сети и открытые узлы. 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 HW, выступающего в качестве агента DHCP-relay, и не будут доставлены.

Чтобы запустить DHCP-relay:

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

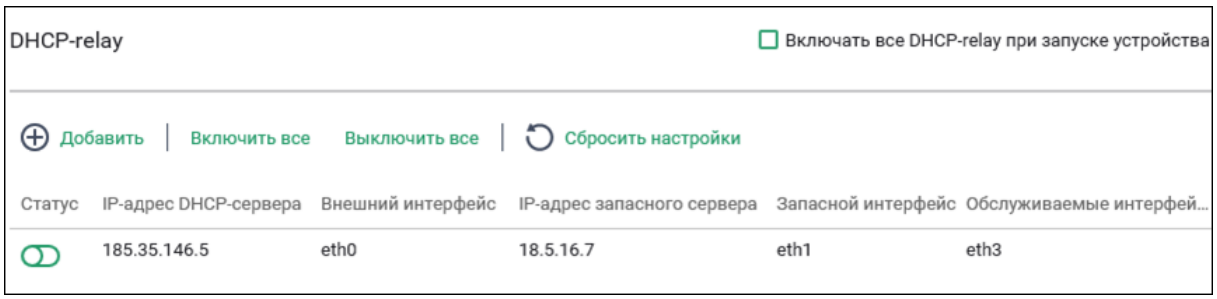


Рисунок 76. Настройка параметров DHCP-relay

2 Нажмите **Добавить**.

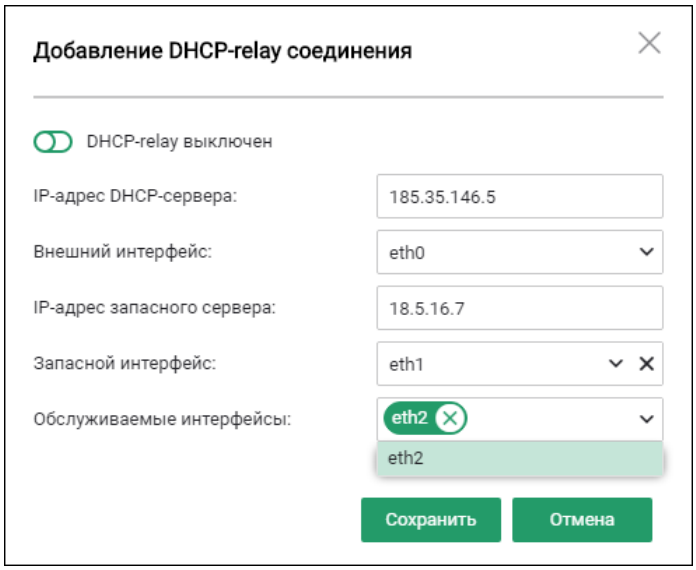


Рисунок 77. Добавление соединения DHCP-relay

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

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

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

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

7 Нажмите **Сохранить**.

8 Включите созданную копию DHCP-relay.

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

Настройка DNS-сервера

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 HW, то результат обработки собственных DNS-запросов и запросов DNS-клиентов не определен, так как неизвестно, какой интерфейс будет включен первым и какой список DNS-серверов пересылки получит ViPNet Coordinator HW.

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

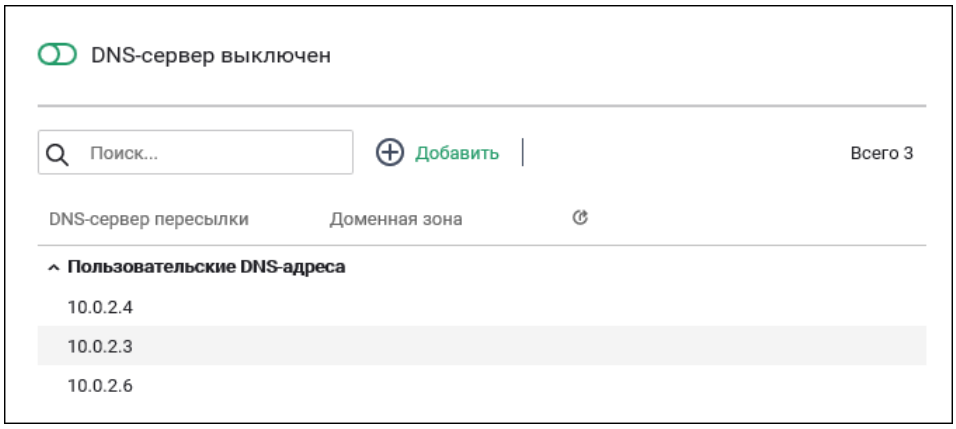


Рисунок 78. Настройка параметров DNS-сервера

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

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

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

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



Примечание. Не устанавливайте одновременно синхронизацию времени на платформе виртуализации и виртуальной машине ViPNet Coordinator HW. Если это необходимо, то для синхронизации используйте один и тот же NTP-сервер.

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

  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 защищенной, так и в открытой сети:

- Если дополнительный NTP-сервер — узел защищенной сети, видимый по реальному адресу, то в файле `iplir.conf` в секции `[id]` для этого узла установите параметр `visibility` в значение `real`. Описание секции и параметра см. в документе «Справочник команд и конфигурационных файлов», в разделе «Файл iplir.conf».
- Если дополнительный NTP-сервер — узел открытой сети, добавьте разрешающий фильтр открытой сети для входящего трафика от NTP-сервера.

Чтобы настроить локальный NTP-сервер:

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

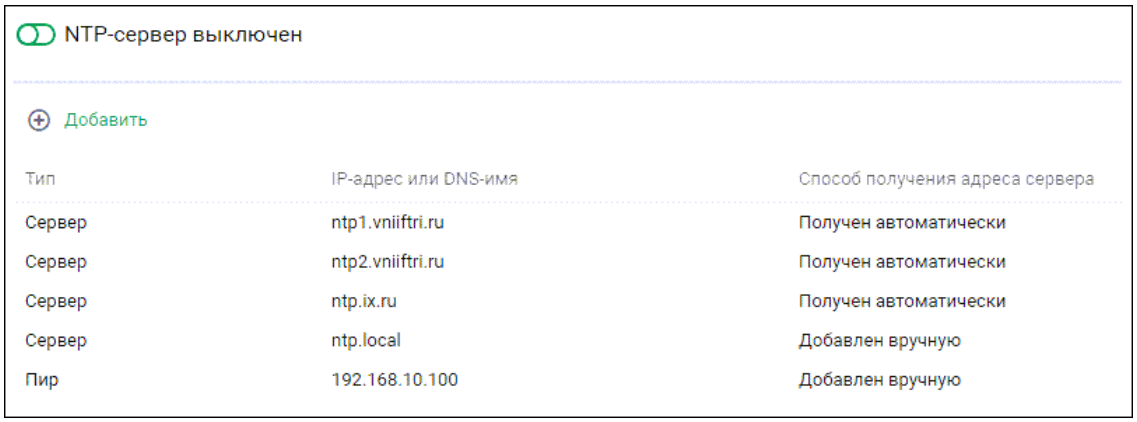


Рисунок 79. Список дополнительных NTP-серверов

Список дополнительных NTP-серверов содержит серверы, заданные по умолчанию, заданные пользователем, полученные автоматически от DHCP-сервера. Изменить или удалить NTP-серверы, полученные автоматически, невозможно.

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

2.1 Выберите тип добавляемого NTP-сервера:

- **Сервер** — работает в одностороннем режиме (рассылка данных времени);
- **Пир** — работает в двустороннем режиме (рассылка и получение данных времени).

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

Примечание. NTP-серверы, заданные доменным именем, будут доступны только при работающем DNS-сервер (см. Настройка DNS-сервера).

2.3 Нажмите .

3 Включите NTP-сервер.

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

Настройка точки доступа сети Wi-Fi

Использование ViPNet Coordinator HW в качестве точки доступа сети Wi-Fi возможно только в исполнениях со встроенными Wi-Fi-модулями:

- ViPNet Coordinator HW50 A, B на аппаратной платформе HW50 N2;
- ViPNet Coordinator HW100 C на аппаратной платформе HW100 N2.

ViPNet Coordinator HW может также работать в качестве клиента сети Wi-Fi (см. Подключение к сети Wi-Fi). Использование ViPNet Coordinator HW одновременно в качестве клиента и точки доступа Wi-Fi не поддерживается.

Чтобы настроить точку доступа:

1 Выберите **Сетевые интерфейсы** и нажмите .

2 Щелкните интерфейс Wi-Fi (`wlan0`).

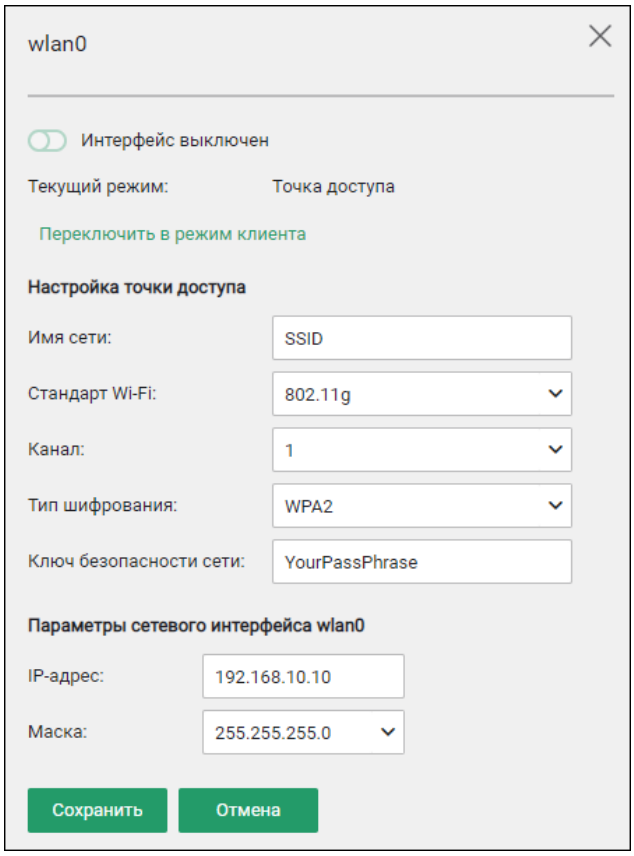


Рисунок 80. Настройка точки доступа сети Wi-Fi

3 Если установлен режим клиента, нажмите **Переключить в режим точки доступа**.

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

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

6 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.

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

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

8 Задайте статический IP-адрес и маску подсети интерфейса `wlan0`.

9 Нажмите **Сохранить**.

10 Если интерфейс Wi-Fi выключен, включите его с помощью переключателя в списке интерфейсов.

11 Включите  интерфейс Wi-Fi.

12 Настройте параметры DHCP-сервера для интерфейса Wi-Fi.

13 Нажмите  .

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

Настройка взаимодействия с Active Directory

Если в вашей сети используется служба каталогов Active Directory, то вы можете настроить ее взаимодействие с ViPNet Coordinator HW, чтобы использовать имена пользователей сети в фильтрах туннелируемых узлов и транзитных фильтрах открытой сети. Для этого:

1. На контроллерах доменов настройте учетную запись технологического пользователя (см. Настройка учетной записи технологического пользователя).
2. На ViPNet Coordinator HW настройте его подключение к контроллерам доменов.



Внимание!

Необходимо обеспечить доверенный канал передачи данных между ViPNet Coordinator HW и внешними системами (в том числе взаимодействующими системами защиты информации других типов), например выделенный физический канал или сеть ViPNet. Допускается осуществлять защиту каналов передачи данных организационными мерами, исключающими возможность утечки или перехвата защищаемых данных, или с помощью сертифицированных средств криптографической защиты информации.

При настройке учитывайте:

- ViPNet Coordinator HW поддерживает контроллеры домена:
  - Windows Server 2012 R2 (английская и русская версии).
  - Windows Server 2016 (английская и русская версии).
- Максимальное количество контроллеров доменов, подключаемых к ViPNet Coordinator HW — 10.
- ViPNet Coordinator HW периодически опрашивает контроллеры доменов для проверки их доступности и обновления списка активных пользователей. При недоступности контроллера домена ViPNet Coordinator HW будет предпринимать попытки соединиться с ним в течение 5 минут. Наличие нескольких недоступных контроллеров доменов может привести к существенным временным задержкам при обновлении списка активных пользователей.
- Для каждого контроллера домена установлено допустимое время отсутствия связи с ним (по умолчанию — 1800 секунд). Если по истечении этого времени связь с контроллером домена не восстановлена:
  - пользователи, связанные только с ним, удаляются из списка активных;
  - открытые пользовательские сессии остаются активными;
  - обработка трафика транзитными фильтрами открытой сети и фильтрами туннелируемых узлов по пользователям, удаленным из списка активных, не проводится.

- Если сетевые узлы, с которых подключаются пользователи, и контроллер домена туннелируются разными ViPNet Coordinator HW, настройте между узлами и контроллером видимость по реальным IP-адресам.

Настройка учетной записи технологического пользователя

Соответствие пользователей сети и IP-адресов устройств, с которых было выполнено подключение, определяется по журналу контроллера домена. Чтобы служба `uc` ViPNet Coordinator HW могла получать данные журнала, создайте учетную запись технологического пользователя для подключения ViPNet Coordinator HW к контроллеру домена и настройте ее полномочия:

1 С помощью оснастки консоли управления **Active Directory Users and Computers**:

1.1 Создайте учетную запись технологического пользователя с произвольным именем, например Иван Петров (`ivan.petrov@test.vn.com`).

1.2 Включите учетную запись технологического пользователя в группы:

- **Читатели журнала событий (Event Log Readers)**.
- **Пользователи DCOM (Distributed COM Users)**.
- **Операторы сервера (Server operator)**.
- **Пользователи домена (Domain Users)**.



Примечание. Учетная запись технологического пользователя может не обладать правами **Администратор домена**.

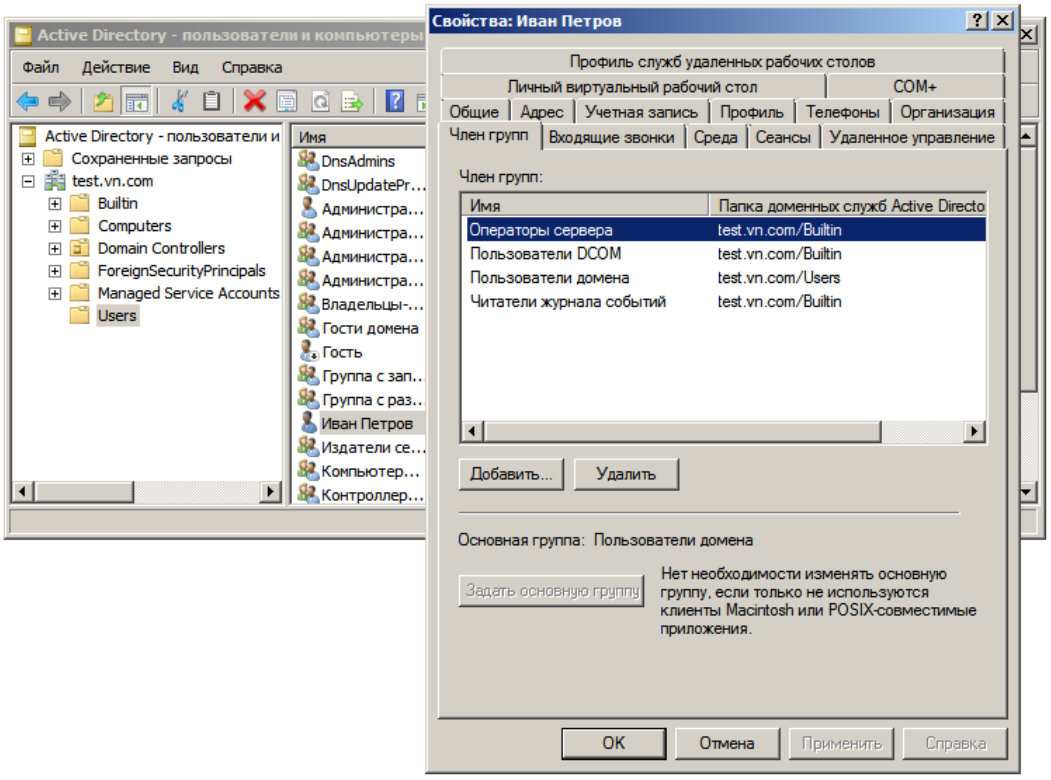


Рисунок 81. Создание учетной записи технологического пользователя Иван Петров

2 С помощью оснастки консоли управления **Windows Management Infrastructure**:

2.1 Добавьте учетную запись технологического пользователя Иван Петров (`ivan.petrov@test.vn.com`) в разделы инфраструктуры WMI:

- **Root/CIMV2**.
- **Root/directory/LDAP**.

2.2 В каждом из перечисленных разделов выберите:

- **Enable Account (Включить учетную запись)**.
- **Remote Enable (Включить удалённо)**.

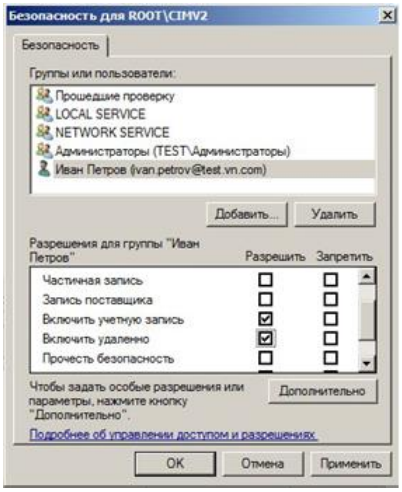


Рисунок 82. Добавление учетной записи технологического пользователя Иван Петров (ivan.petrov@test.vn.com) в инфраструктуру WMI и задание полномочий

Настройка взаимодействия с LDAP-сервером

В ряде случаев невозможно реализовать политику безопасного доступа пользователей из внутренней сети компании в Интернет с использованием аутентификации в службе каталогов Active Directory:

- в IT-инфраструктуре компании не используется служба каталогов Active Directory;
- сотрудники компании используют мобильные устройства с iOS и Android, которые нельзя аутентифицировать в Active Directory.

Тогда для аутентификации пользователей, в том числе подключающихся с мобильных устройств, используются Captive portal, встроенный в ViPNet Coordinator HW, и LDAP-сервер:

1. Пользователь подключается к внутренней сети (например, через точку доступа Wi-Fi, подключенную к ViPNet Coordinator HW) и переходит в браузере на внешний веб-ресурс.
2. ViPNet Coordinator HW переадресует запрос пользователя на страницу аутентификации Captive portal.
3. Пользователь вводит имя и пароль, Captive portal отправляет запрос на LDAP-сервер для проверки данных учетной записи пользователя.
4. LDAP-сервер отправляет на Captive portal результат проверки учетных данных пользователя.
5. Если проверка пользователя на LDAP-сервере прошла успешно, то пользователь видит на странице Captive portal ссылку для перехода на запрошенный веб-ресурс.

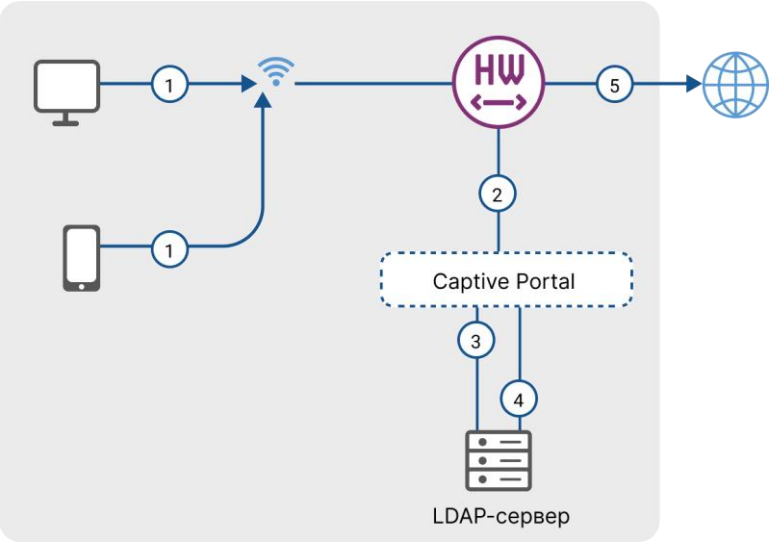


Рисунок 83. Аутентификация пользователей с помощью Captive portal и LDAP-сервера

Примечание. Во внутренней сети компании должен быть установлен LDAP-сервер. Для хранения учетных данных пользователей в LDAP-каталоге должны использоваться следующие атрибуты:

- `uid` — для имени пользователя.
- `userPassword` — для пароля пользователя.

Captive portal определяет пользователей по их уникальным IP-адресам и поэтому не сможет определить пользователей, которые находятся за NAT с трансляцией адреса источника.

Чтобы настроить взаимодействие с LDAP-сервером:

1 Получите и импортируйте в локальное хранилище ViPNet Coordinator HW необходимые сертификаты (см. Получение и импорт сертификатов).

2 Настройте параметры Captive portal (см. Настройка параметров Captive portal).

После этого доступ в Интернет будет определяться правилами межсетевого экрана. Для пользователей, не прошедших аутентификацию, доступ в Интернет будет заблокирован, в том числе запросы к внешним DNS-серверам. Поэтому для нормальной работы пользователей во внутренней сети используйте локальные DNS-серверы (см. Настройка DNS-сервера).

Получение и импорт сертификатов

Импортируйте в локальное хранилище сертификатов ViPNet Coordinator HW:

- Корневой сертификат УЦ, выпустившего сертификат LDAP-сервера. Корневой сертификат необходим для проверки подлинности сертификата LDAP-сервера. Вы можете загрузить его с сайта УЦ, указанного в сертификате LDAP-сервера.
- Сертификат веб-сервера Captive portal. Сертификат обеспечивает защиту данных (логина и пароля), которые пользователь передает при аутентификации на Captive portal. Для получения сертификата создайте запрос в формате PKCS#12 и передайте его в УЦ; в ответ на запрос вы получите сертификат веб-сервера Captive portal.

Примечание. Вы можете создать запрос на сертификат не только в ViPNet Coordinator HW, но и с помощью других средств. В этом случае начните выполнять действия с шага 5 и импортируйте в локальное хранилище не только сертификат, но и закрытый ключ, которым он подписан.

Для получения и импорта сертификатов в локальное хранилище:

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

2 Создайте запрос на сертификат веб-сервера Captive portal:

2.1 Нажмите **Создать запрос на сертификат** и укажите:

- имя файла запроса;
- размер ключа RSA: 2048;

- алгоритм хэширования: sha256;
- IP-адрес или доменное имя ресурса.

2.2 Нажмите **Сохранить**.

3 Нажмите , чтобы выгрузить файл запроса в папку компьютера.

4 Перешлите файл запроса в УЦ и получите сертификат веб-сервера Captive portal.

5 Скопируйте сертификат веб-сервера Captive portal и корневой сертификат УЦ, выдавшего сертификат LDAP-сервера в папку компьютера и импортируйте их в локальное хранилище сертификатов:

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

5.2 Нажмите **Импортировать**.

5.3 Нажмите **Загрузить файл**, выберите файл и нажмите **Открыть**.

5.4 Нажмите **Импортировать**.

Примечание. При настройке ViPNet Coordinator HW с помощью веб-интерфейса вы можете импортировать только сертификаты в кодировке Base64, подписанные открытым ключом RSA.

Сертификат веб-сервера Captive portal появится в списке установленных сертификатов. Если вы создавали запрос на сертификат Captive portal не с помощью ViPNet Coordinator HW, то в этом случае также импортируйте закрытый ключ сертификата Captive portal.

6 Импортируйте на устройства пользователей, проходящих аутентификацию через Captive portal, корневой сертификат УЦ, выдавшего сертификат веб-сервера Captive portal и список аннулированных сертификатов этого УЦ.

Настройка параметров Captive portal

Настройте параметры взаимодействия Captive portal с LDAP-сервером:

1 Выберите **Межсетевой экран** > **Пользователи сети** > **Captive portal** и нажмите .

2 Установите флажок **Использовать Captive Portal для аутентификации пользователей сети**.

3 Задайте параметры подключения к Captive portal:

- адрес LDAP-сервера;
- выделенное имя (DN, Distinguished Name) учетной записи администратора LDAP-сервера, которая обладает правами на чтение записей LDAP-сервера;
- выделенное имя (DN, Distinguished Name) базы поиска, от которой начинаются операции поиска в LDAP-каталоге.
- Режим соединения с LDAP-сервером.

4 Выберите из списков корневой сертификат удостоверяющего центра, выдавшего сертификат LDAP-сервера и сертификат веб-сервера Captive portal.

5 Задайте имя гостевой сети, которое пользователи будут видеть на странице аутентификации Captive portal.

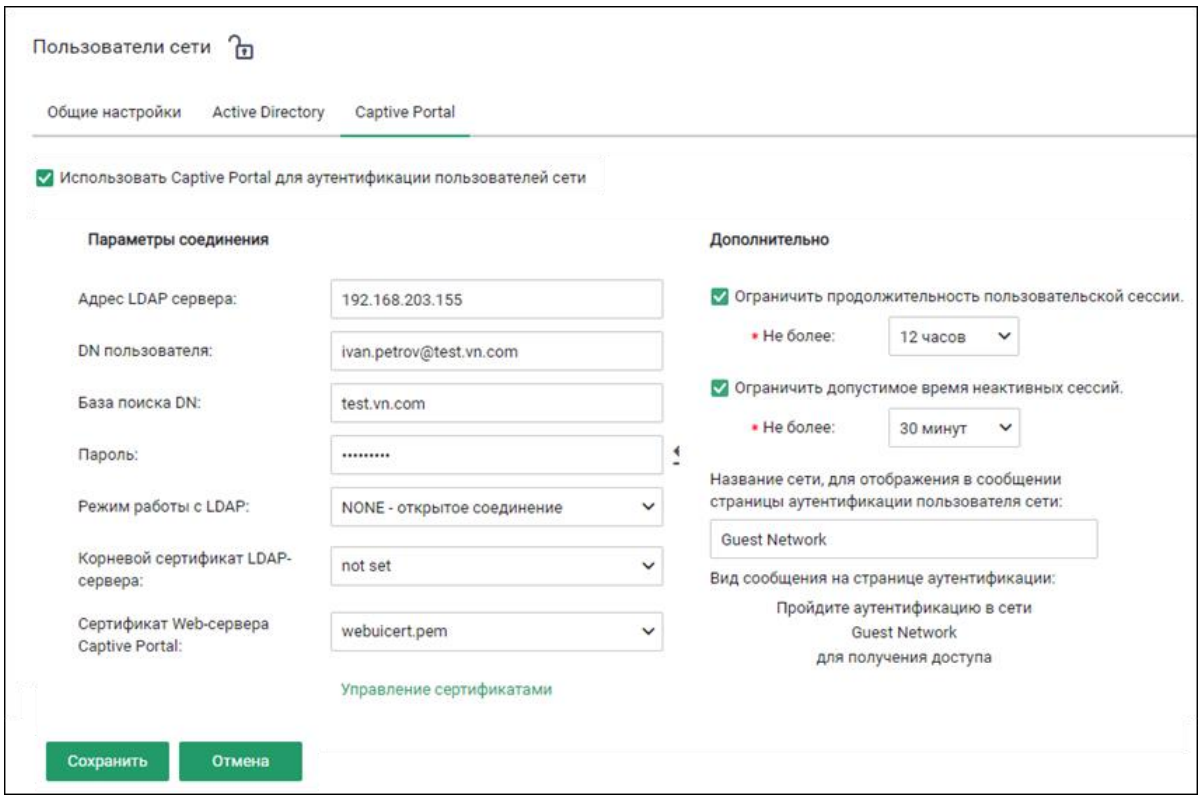


Рисунок 84. Настройка параметров Captive portal

6 Нажмите **Сохранить**.

7 Нажмите .

Чтобы сбросить настройки взаимодействия Captive portal с LDAP-сервером:

1 Нажмите .

2 Снимите флажок **Использовать Captive Portal для аутентификации пользователей сети**.

3 Нажмите .

Просмотр списка пользователей Active Directory и Captive portal

Выберите **Межсетевой экран** > **Пользователи сети** > **Общие настройки**.

Формат списка активных пользователей:

- имя пользователя и его IP-адрес;
- тип пользователя (по умолчанию скрыт):
  - AD — пользователь домена Active Directory;
  - CP — пользователь, аутентифицированный с помощью Captive Portal;
- время начала и оставшееся время жизни сессии пользователя (отображается, если для пользователей Captive portal заданы ограничения продолжительности сессии).

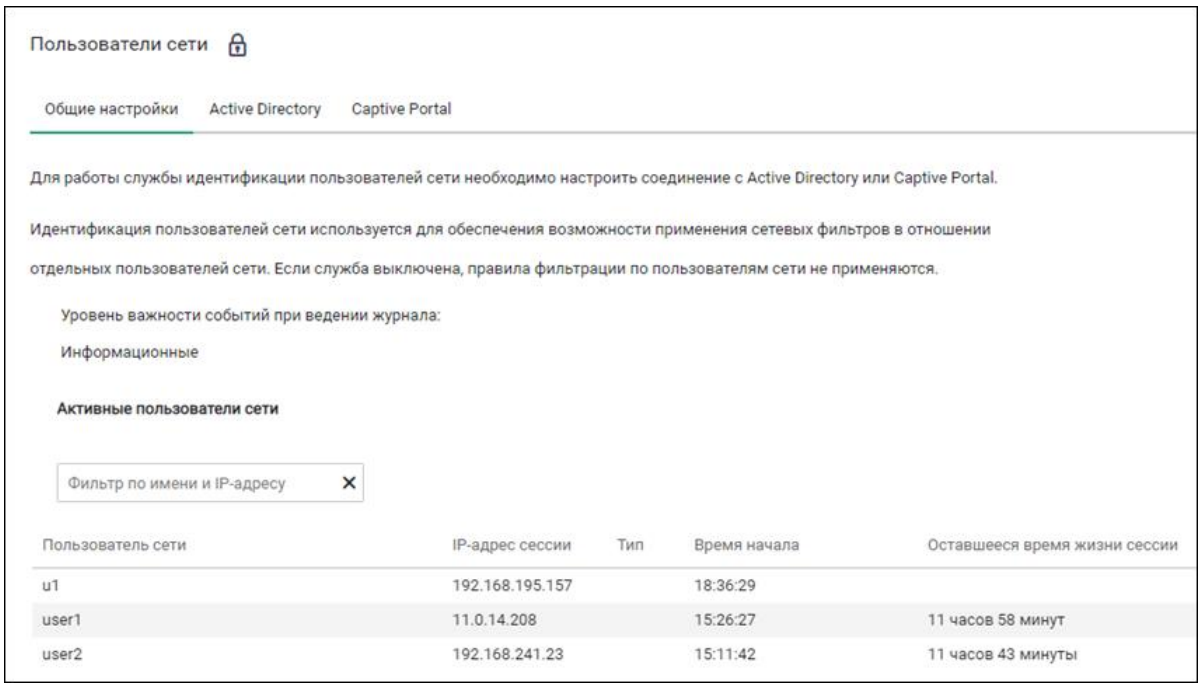


Рисунок 85. Активные пользователи Active Directory и Captive portal

Примечание. Список активных пользователей AD формируется на основе журнала безопасности контроллера домена. Если пользователь AD вышел из сети, то он будет отображаться в списке активных пользователей до тех пор, пока с этого IP-адреса в сеть не войдет другой пользователь AD.

Регистрация событий аутентификации пользователей

События, связанные с аутентификацией пользователей Active Directory и Captive Portal, регистрируются в системном журнале. По умолчанию установлен уровень важности регистрируемых событий **Информационные**.

Внимание! Не рекомендуется изменять уровень важности регистрируемых событий, установленный по умолчанию. Повышение уровня важности событий ведет к увеличению размера системного журнала и к снижению производительности ViPNet Coordinator HW.

Чтобы изменить уровень важности регистрируемых событий:

1 Выберите **Межсетевой экран** > **Пользователи сети** > **Общие настройки** и нажмите .

2 Выберите из списка **Уровень важности событий при ведении журнала** нужный уровень:

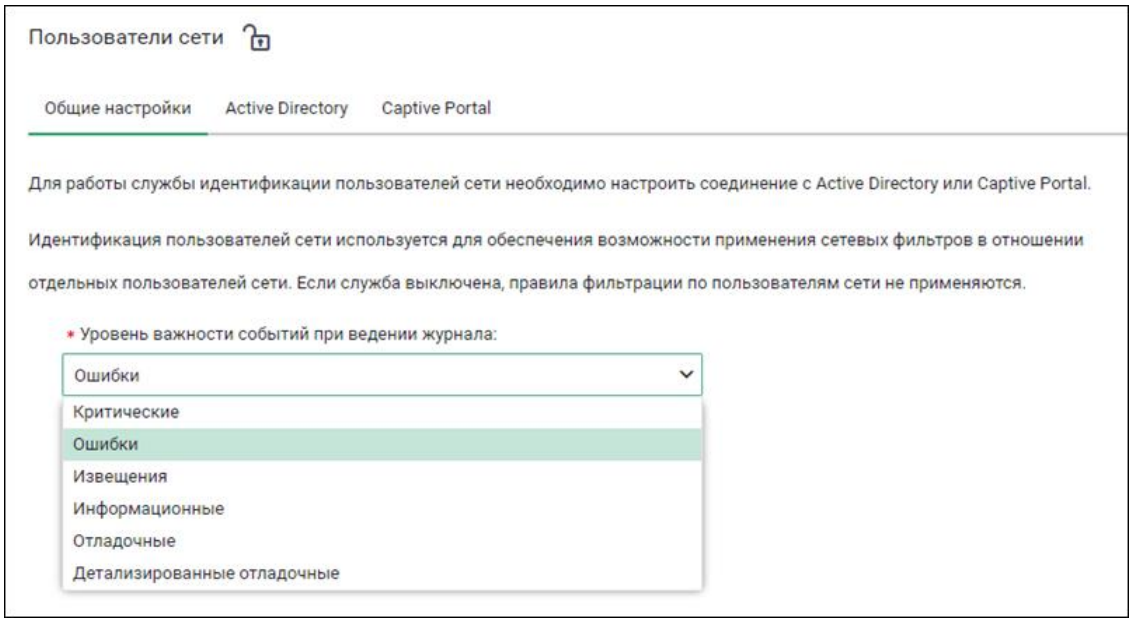


Рисунок 86. Настройка уровня важности событий

3 Нажмите .



6

Настройка предотвращения вторжений

Общие сведения об IPS 149

Параметры IPS по умолчанию 151

Включение и выключение IPS 152

Настройка параметров сетевого окружения 153

Управление правилами IPS 155

Обновление базы правил IPS 161

Обновление базы вредоносного ПО 164

Настройка регистрации событий IPS 166

Общие сведения об IPS

В ViPNet Coordinator HW входит система предотвращения вторжений IPS (Intrusion Prevention System). IPS предназначена для обнаружения и нейтрализации сетевых атак и вредоносного ПО (Malware Detection). Использование IPS расширяет возможности ViPNet Coordinator HW по защите сетей. Для анализа сетевого трафика в IPS применяются следующие методы:

- Для обнаружения сетевых атак:
  - Сигнатурный метод — анализ заголовков протоколов и содержимого IP-пакетов, а именно:
    - заголовков транспортных протоколов, по которым необходимо отслеживать IP-пакеты (протокол, IP адреса и порты источника и получателя);
    - заголовков и параметров прикладных протоколов;
    - содержимого IP-пакетов с целью обнаружения сигнатур сетевых атак.
  - Эвристический метод — обнаружение признаков сетевых угроз:
    - аномалий в служебных заголовках IP-пакетов;
    - аномалий при декодировании и фрагментации IP-пакетов;
    - попыток сканирования портов и удаленного выполнения произвольного кода.
- Для обнаружения вредоносного ПО — обнаружение вредоносных сигнатур в содержимом IP-пакетов по протоколам HTTP, HTTPS, SMTP, IMAP, POP3, FTP и SMB.



Внимание! При обнаружении вредоносного ПО проверяемый файл может быть скачан частично из-за особенности потоковой проверки. При этом скачанный фрагмент файла не несет угрозы.

Правила обнаружения сетевых атак (далее — правила IPS) входят в состав базы правил IPS. Сигнатуры вредоносного ПО входят в состав базы вредоносного ПО. Обе базы формируются специалистами ИнфоТеКС, регулярно обновляются и публикуются на официальном сервере обновления ИнфоТеКС (см. Обновление базы правил IPS).

Каждое срабатывание правила IPS или обнаружение сигнатуры вредоносного ПО регистрируется:

- в системном журнале — краткая информация о событии;
- в журнале IP-пакетов — подробная информация о событии.

Особенности анализа сетевого трафика и регистрации событий

- В некоторых случаях для обнаружения угрозы выполняется анализ цепочки IP-пакетов и к моменту срабатывания блокирующего правила часть пакетов уже будет пропущена для обработки.

- Во время анализа пакета может сработать несколько правил IPS. При этом в системном журнале регистрируются все события, а в журнале IP-пакетов регистрируется событие на срабатывание первого правила или блокирующего правила (при наличии такого).
- IPS может пропустить отложенную атаку, если от момента открытия сессии атаки до момента отправки вредоносного ПО в этой сессии на ViPNet Coordinator HW открывались и закрывались другие сессии.
- В IPS отсутствует в явном виде режим обнаружения угроз без их блокировки (IDS). Для работы IPS в режиме обнаружения необходимо для всех блокирующих правил IPS вручную переключить действие при их срабатывании с **Блокировать** на **Предупреждать**. Поскольку для каждого правила IPS действие при срабатывании настраивается индивидуально, то при настройке IPS в режиме обнаружения угроз используйте групповые операции с правилами (см. Групповые операции с правилами IPS).

Особенность применения лицензии IPS



Внимание! После назначения лицензии, разрешающей использование IPS, перезагрузите ViPNet Coordinator HW. Иначе обнаружение и предотвращение вторжений будет недоступно.

Параметры IPS по умолчанию

Таблица 4. Параметры IPS по умолчанию

Параметр	Значение
Предотвращение вторжений	Включено
Обнаружение вредоносного ПО	Выключено
Включение IPS при перезагрузке	Разрешено
Сервер обновления базы правил IPS и базы вредоносного ПО	https://updateids.infotecs.ru
Обновление базы правил IPS и базы вредоносного ПО по расписанию	Выключено
Расписание обновления базы правил IPS и базы вредоносного ПО	Ежедневно, время обновления выбирается случайное
База правил IPS	Из состава дистрибутива
База вредоносного ПО	Не установлена, необходимо установить с сервера обновления или с USB-носителя
Уровень важности событий IPS, регистрируемых в системном журнале	Уровень 3 (информационные)

В дальнейшем вы можете настроить параметры IPS в соответствии с политиками безопасности вашей сети.

Включение и выключение IPS

Внимание! Не рекомендуется выключать IPS без необходимости, поскольку ваша сеть станет потенциально незащищенной от сетевых атак, воздействия сетевых вирусов и попыток эксплуатации уязвимостей в программном обеспечении.

Если вы решили выключить IPS:

1. Выберите **Предотвращение вторжений** и нажмите .
2. Выключите **Предотвращение вторжений включено**.
3. Нажмите .

Чтобы заново включить IPS:

1. Нажмите .
2. Включите **Предотвращение вторжений выключено**.
3. Нажмите .

Если IPS запущен, то при наличии действующей лицензии «Обновление Malware Detection» вы можете включить обнаружение вредоносного ПО:

1. Нажмите .
2. Выберите **Методы анализа**.
3. Включите **Обнаружение вредоносного ПО**.

Настройка параметров сетевого окружения

Для корректной работы правил IPS, снижения количества ложных срабатываний, а также уменьшения нагрузки на процессор при обработке трафика настройте параметры сетевого окружения IPS:

- IP-адреса узлов сети, для защиты которой установлен ViPNet Coordinator HW.
- IP-адреса узлов внешних сетей, представляющих угрозу безопасности защищаемой сети.
- IP-адреса и порты сетевых сервисов, функционирующих в защищаемой сети (серверов DNS, SMTP, SQL, веб-сервисов и т.д.).

Параметры сетевого окружения задаются переменными, которые применяются в сигнатурных правилах IPS для определения направления следования пакетов. Параметры следования пакетов в правилах определяются IP-адресами и портами источников и получателей пакетов. Если пакет не удовлетворяет параметрам следования, то дальнейший анализ его содержания на соответствие условиям данного правила прекращается. Перечень переменных и их значения по умолчанию см. в приложении Параметры правил IPS по умолчанию.

Для настройки параметров сетевого окружения:

1 Выберите **Предотвращение вторжений** и нажмите .

2 Выберите **Правила IPS** и нажмите **Настройки правил**.

3 В списке **Параметры сети** внесите изменения в поля переменных `$HOME_NET` и `$EXTERNAL_NET` в соответствии с адресацией вашей сети.

Подробнее см. в приложении Формат указания IP-адресов и портов в правилах IPS.

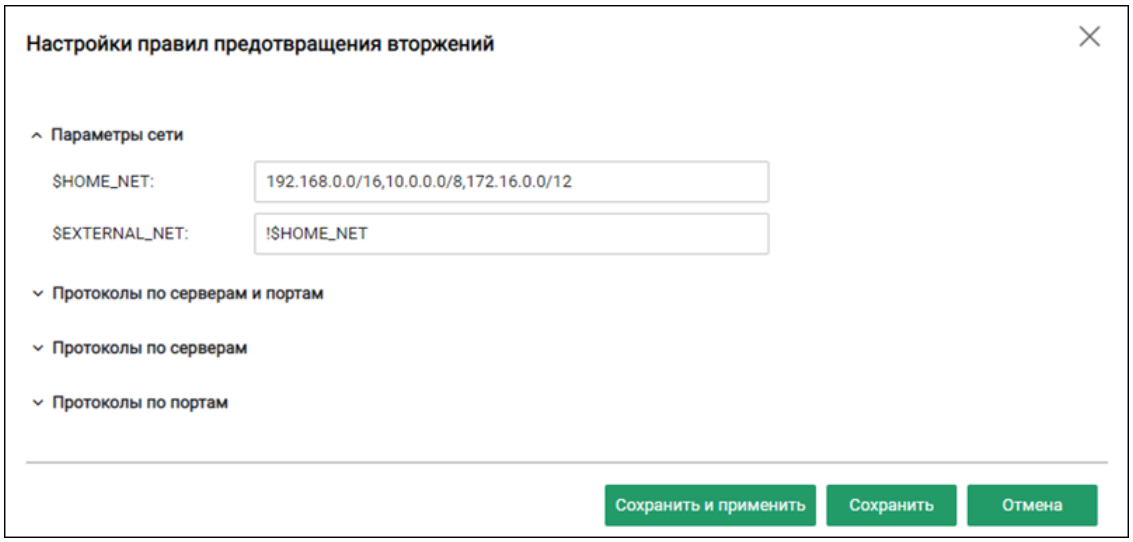


Рисунок 87. Настройка параметров сетевого окружения

4 Повторите шаг 3 для настройки IP-адресов и портов доверенных ресурсов в списках **Протоколы по серверам и портам**, **Протоколы по серверам**, **Протоколы по портам**.

5 Нажмите **Сохранить и применить**.

6 Нажмите  .

Управление правилами IPS

Правила IPS — это записи в базе правил, описывающие алгоритмы анализа трафика. Правила IPS разделены на группы:

- Группы сигнатурных правил.

  Сигнатурные правила распределены по группам в соответствии с типами и целями угроз (сетевых атак). Состав групп определён в базе правил.

  Примеры групп:

  - **dos** — содержит сигнатуры атак, направленных на отказ в обслуживании;
  - **policy** — содержит сигнатуры атак, направленных на нарушение политики информационной безопасности;
  - **web_server** — содержит сигнатуры атак, направленных на веб-серверы.
- Группы эвристических правил.

  Состав групп эвристических правил определён в базе правил. Специальные правила распределены по следующим группам:

  - **decoder** — правила, выявляющие аномалии в заголовках пакетов при их первичном декодировании (например, несоответствие минимальной длины заголовка пакета);
  - **sensitive data** — правила, срабатывающие при обнаружении в сетевом трафике конфиденциальной информации (например, номера банковских карт, адреса электронной почты и прочее);
  - **preprocessor** — правила, выявляющие аномалии в процессе предварительной обработки пакетов протоколов.

Для каждого правила IPS определены:

- Режим активности — режим определяет, используется ли данное правило для анализа трафика.
- Режим блокировки пакетов — режим определяет, блокируется ли вредоносный пакет при срабатывании правила. Данный режим присутствует только у определённого набора сигнатурных правил.

Для идентификации правил IPS используются атрибуты:

- Название — наименование правила, содержащее описание угрозы.

  Примеры названий правил:

  - `ET DOS ntop Basic Auth DOS inbound`
  - `ARPSPOOF UNICAST ARP REQUEST`
  - `AM DNSBL GET request to bad domain beta.guildwars2.com`
- Идентификатор правила.

  Правилу IPS присваивается уникальный идентификатор в формате `<тип.номер.версия>`:

- Сигнатурным правилам присваиваются семизначные номера в диапазоне от 2000000 до 3999999. Сигнатурным правилам соответствует тип 1.
- Перечень номеров эвристических правил представлен в приложении (см. Номера правил анализа трафика эвристическим методом).

- Класс — классификационный идентификатор правила.

  Класс объединяет совокупность (коллекцию) правил, схожих по общим признакам. Класс характеризует как тип угрозы (например, сетевая активность программы-трояна), так и признаки её реализации (например, попытка сканирования сети или успешная атака). Правила из разных классов могут быть распределены по разным группам.

  Примеры классов правил:

  - **trojan activity** — обнаружена сетевая троянская программа;
  - **successful dos** — успешная DoS атака;
  - **attempted admin** — попытка получения привилегий администратора.

Поиск правил IPS

Для удобства просмотра и настройки правил IPS вы можете использовать текстовый поиск по атрибутам правил. Поиск позволяет находить вхождение произвольного текста в значениях атрибутов правил IPS:

- Название.
- Комментарий.
- Протокол.
- Адреса источников.
- Порты источников.
- Направление.
- Адреса назначений.
- Порты назначений.
- Класс правила.
- Идентификатор.

Например, вы можете найти правила, в которые входит строка «macOS»:

1 Выберите **Предотвращение вторжений** > **Правила IPS**.

2 В поле поиска введите macOS.

Примечание. Поиск правил выполняется по мере ввода символов.

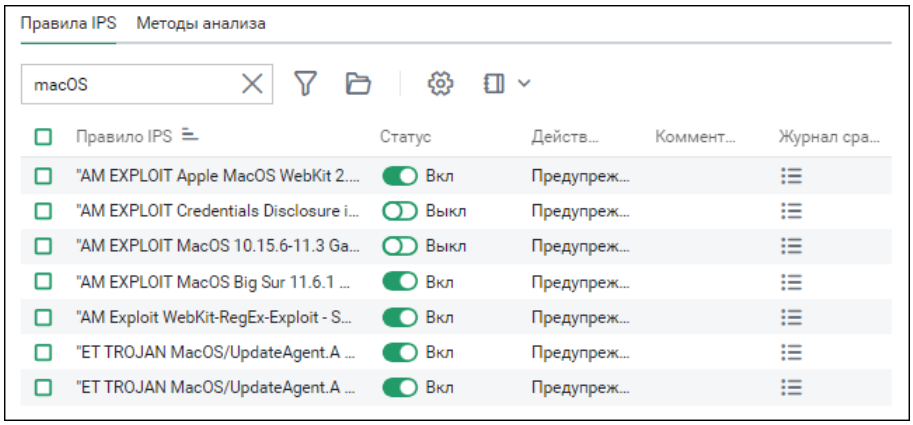


Рисунок 88. Текстовый поиск правил IPS

Также вы можете настроить отображение правил IPS с помощью фильтра:

1 Нажмите .

2 Выберите параметры фильтрации:

- Активность правила IPS.
- Действие правила IPS.
- Комментарий в правиле IPS.

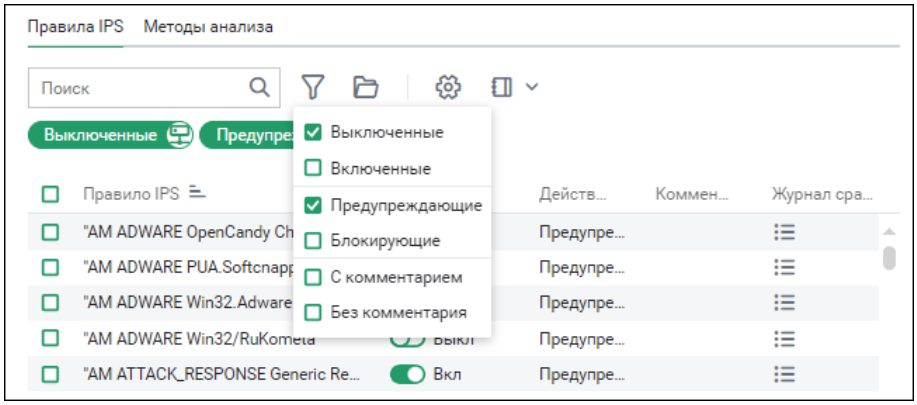


Рисунок 89. Поиск правил IPS с помощью фильтра

Кроме этого, вы можете настроить отображение только определенных групп правил IPS:

1 Нажмите .

2 Выберите группы правил IPS.

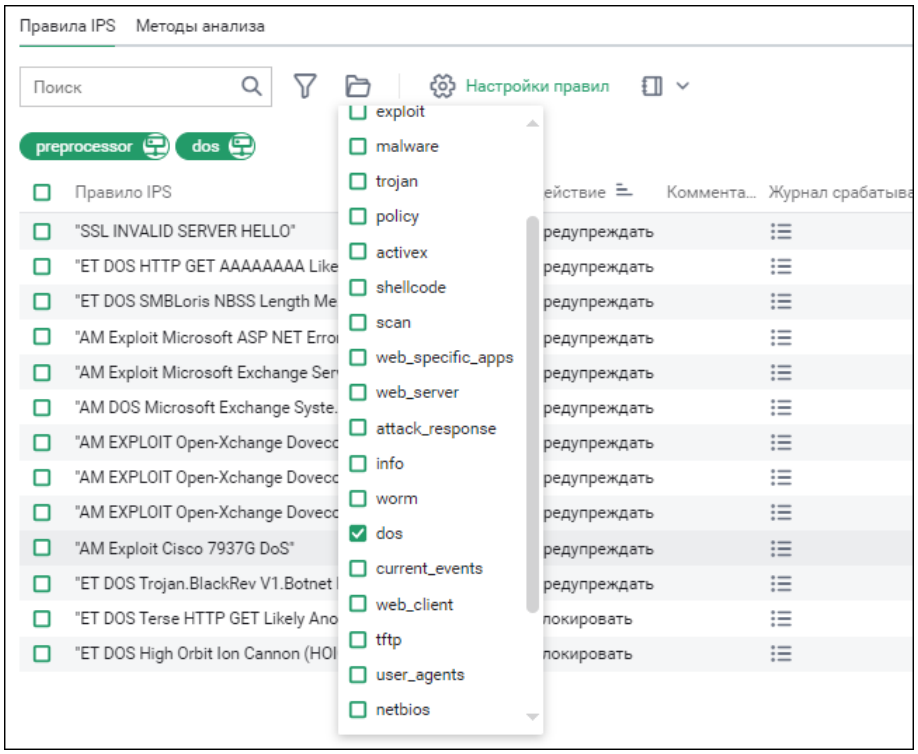


Рисунок 90. Поиск правил IPS по группам

Просмотр и настройка правил IPS

Чтобы настроить одиночное правило IPS:

1 Выберите **Предотвращение вторжений** > **Правила IPS** и нажмите .

2 Найдите правило в списке и щелкните строку с ним.

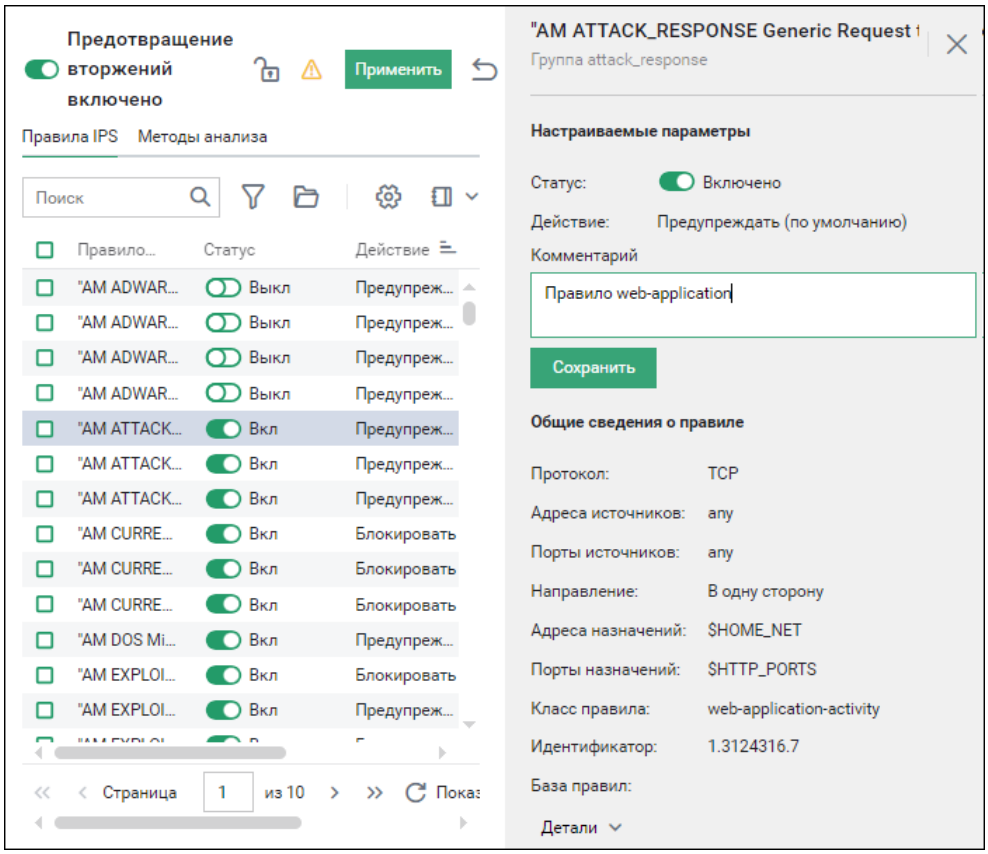


Рисунок 91. Настройка правила IPS

3 На панели **Настраиваемые параметры** вы можете:

- Изменить статус правила IPS.
- Изменить действие при срабатывании правила IPS.

> **Примечание.** Если для правила IPS по умолчанию задано действие **Предупреждать**, то его нельзя изменить на действие **Блокировать**.

- В поле **Комментарий** добавить примечание.

4 Нажмите **Сохранить**.

5 Нажмите **Применить**.

6 Нажмите .

Журнал событий для выбранного правила IPS соответствует журналу регистрации IP-пакетов, отфильтрованному по выбранному правилу. Для его просмотра нажмите в строке выбранного правила.

Групповые операции с правилами IPS

Для удобства настройки правил IPS вы можете использовать групповые операции. Например, если в вашей сети не используются сервисы, работающие по протоколу netbios, вы можете сразу выключить все правила, которые срабатывают на попытки вторжений с использованием netbios:

1 Выберите **Предотвращение вторжений** > **Правила IPS** и нажмите .

2 Нажмите и выберите группу **netbios**.

3 Установите флажок рядом с заголовком столбца **Правило IPS**.

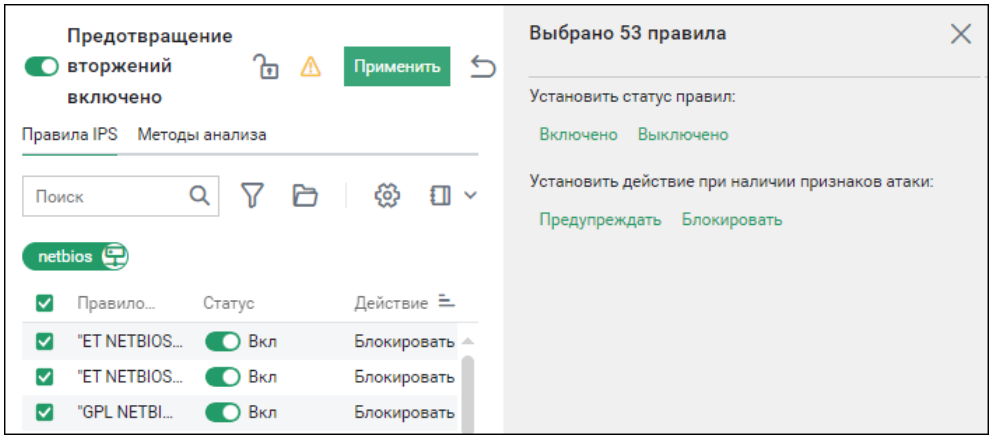


Рисунок 92. Групповая операция с правилами IPS

Общее количество выбранных правил IPS отображается на панели групповой настройки.

4 Нажмите **Выключено**, чтобы выключить выбранные правила.

5 Нажмите **Применить**.

6 Нажмите .

Аналогичным образом вы можете установить действие для группы выбранных правил IPS, например, выбрать **Предупреждать**, чтобы только регистрировать обнаруженные угрозы, без их блокировки.

Обновление базы правил IPS

База правил IPS публикуется на сервере обновления `https://updateids.infotecs.ru`, или другом, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления.

По умолчанию установлена база правил IPS из состава дистрибутива ViPNet Coordinator HW. При наличии действующей лицензии «Обновление базы правил IPS» вы можете:

- обновить базу правил IPS с сервера, в том числе настроить обновление по расписанию;
- скачать базу правил IPS с сервера, скопировать её в папку компьютера и обновить из файла.

Внимание! Убедитесь, что сервер обновлений доступен на ViPNet Coordinator HW по доменному имени, иначе добавьте DNS-сервер пересылки (см. Настройка DNS-сервера).

Во время обновления базы работа IPS не прерывается.

Обновление по расписанию

1 Выберите **Предотвращение вторжений** > **Методы анализа**.

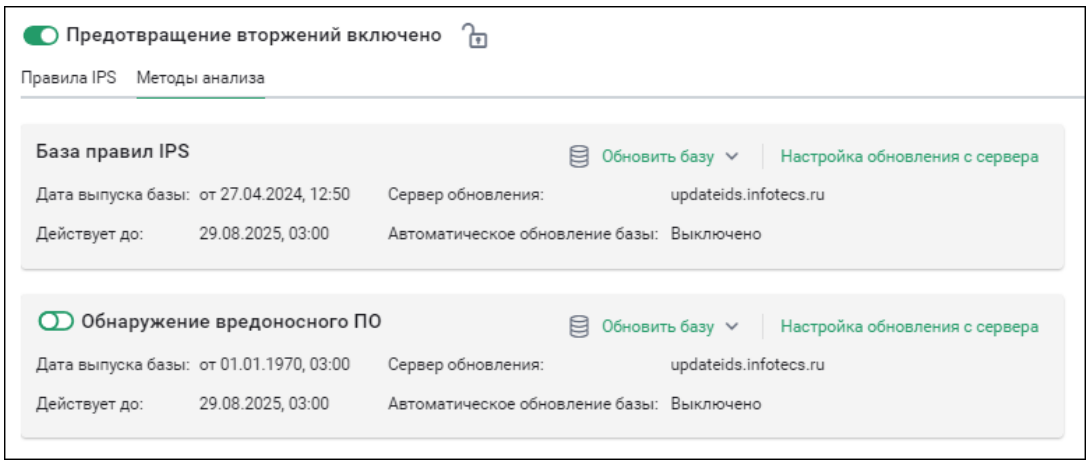


Рисунок 93. Настройка обновления базы правил IPS и базы вредоносного ПО

2 На панели **База правил IPS** нажмите **Настройки обновления с сервера**.

3 При необходимости задайте другой сервер обновления.

4 Задайте имя пользователя и его пароль.

5 Если политики безопасности вашей компании запрещают подключение к внешним серверам напрямую, вы можете обновлять базу через прокси-сервер в вашей сети:

5.1 Выберите **Использовать прокси-сервер**.

5.2 Задайте адрес прокси-сервера и при необходимости измените порт.

Примечание. В зависимости от типа узла прокси-сервера (открытый или защищенный), создайте разрешающий сетевой фильтр (локальный фильтр открытой сети или фильтр защищенной сети), пропускающий трафик от ViPNet Coordinator HW на TCP-порт прокси-сервера.

6 Настройте расписание:

6.1 Выберите **Обновлять автоматически**.

6.2 Выберите периодичность и время обновления.

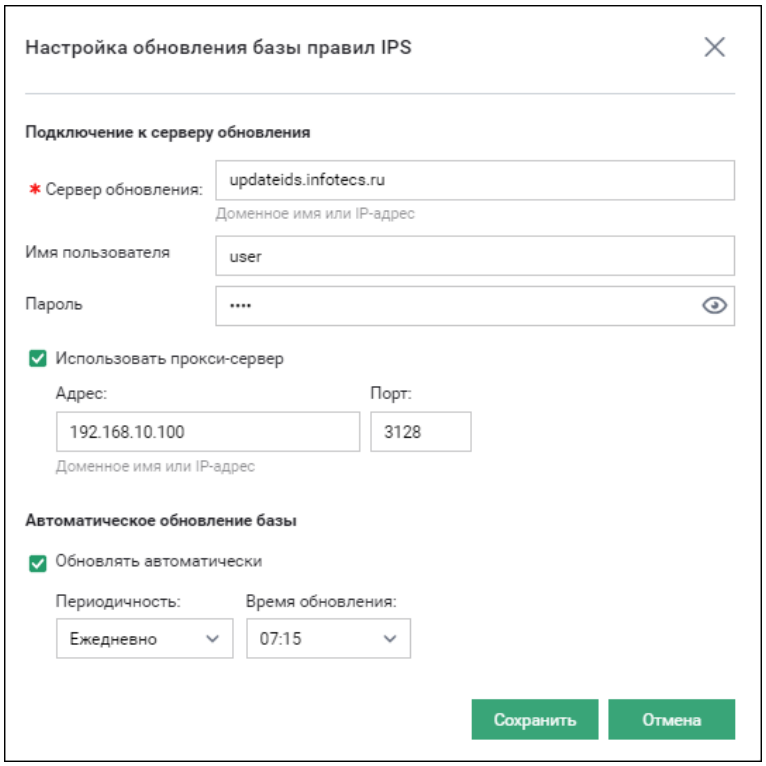


Рисунок 94. Настройка обновления базы правил IPS

7 Нажмите **Сохранить**.

8 В списке **Обновить** выберите **С сервера**.

Дождитесь завершения обновления. Теперь база правил IPS будет обновляться по расписанию. Если на шаге 6 вы не настроили обновление по расписанию, отслеживайте актуальность базы правил IPS самостоятельно и обновляйте её вручную (шаг 8).

Обновление из файла

Если политики безопасности вашей компании запрещают подключение к внешним серверам, вы можете обновить базу правил IPS из файла:

1 Скачайте с сервера обновления и скопируйте в папку компьютера файлы актуальной базы правил IPS (файл базы формата `*.tgz` и файл ЭП формата `*.tgz.sig`).

2 На панели **База правил IPS** в списке **Обновить** выберите **Из файла**.

3 Выберите файлы базы и нажмите **Открыть**.

Дождитесь завершения обновления.

Далее отслеживайте актуальность базы правил IPS самостоятельно и обновляйте её из файла.

Обновление базы вредоносного ПО

База вредоносного ПО публикуются на сервере обновления `https://updateids.infotecs.ru`, или другом, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления.

По умолчанию база вредоносного ПО не установлена. При наличии действующей лицензии «Обновление Malware Detection» вы можете:

- обновить базу вредоносного ПО с сервера, в том числе настроить обновление по расписанию;
- скачать базу вредоносного ПО с сервера, скопировать её в папку компьютера и обновить из файла.

Если вы не включили обнаружение вредоносного ПО ранее, включите его сейчас:

1 Выберите **Предотвращение вторжений** > **Методы анализа**.

2 Обновите базу вредоносного ПО из файла или настройте обновление по расписанию.

3 Включите **Обнаружение вредоносного ПО**.

Обновление по расписанию

1 На панели **Обнаружение вредоносного ПО** нажмите **Настройки обновления с сервера**.

2 Настройте обновление аналогично шагам 3–7 сценария обновления базы правил IPS по расписанию.

3 В списке **Обновить** выберите **С сервера**.

Дождитесь завершения обновления. Теперь база вредоносного ПО будет обновляться по расписанию. Если вы не настроили обновление по расписанию, отслеживайте актуальность базы самостоятельно и обновляйте её вручную (шаг 3).

Обновление из файла

Если политики безопасности вашей компании запрещают подключение к внешним серверам, вы можете обновить базу вредоносного ПО из файла:

1 Скачайте с сервера обновления и скопируйте в папку компьютера файлы актуальной базы вредоносного ПО (файл базы формата `*.tgz` и файл ЭП формата `*.tgz.sig`).

2 На панели **Обнаружение вредоносного ПО** в списке **Обновить** выберите **Из файла**.

3 Выберите файлы базы и нажмите **Открыть**.

Дождитесь завершения обновления.

Далее отслеживайте актуальность базы вредоносного ПО самостоятельно и обновляйте её из файла.

Настройка регистрации событий IPS

События, связанные с работой IPS, регистрируются в системном журнале. Уровень детализации записей в журнале зависит от установленного уровня важности регистрируемых событий.

Чтобы установить минимальный уровень важности регистрируемых событий:

1 Выберите **Предотвращение вторжений** > **Правила IPS** и нажмите .

2 Нажмите .

3 Выберите из списка **Уровень важности событий** нужный уровень.

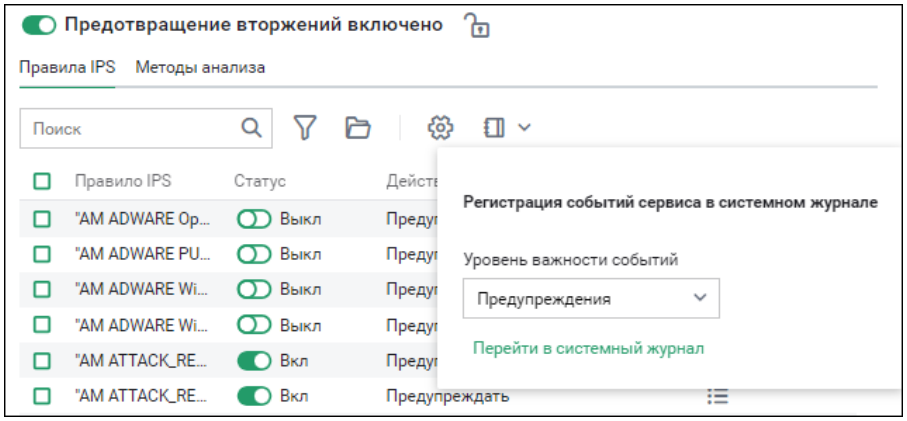


Рисунок 95. Выбор уровня важности регистрируемых событий IPS

По умолчанию установлен уровень важности событий — **Информационные**. При этом в системном журнале ViPNet Coordinator HW регистрируются следующие события: **Критические**, **Ошибки**, **Предупреждения** и **Информационные**. Для устранения неполадок в работе системы предотвращения вторжений вы можете настроить получение диагностических сообщений, установив уровень важности событий **Отладочные** или **Детализированные отладочные**.

4 В некоторых случаях при изменении уровня важности событий требуется перезапуск IPS:

- Для немедленной установки нового уровня важности событий нажмите **Перезапустить**.
- Чтобы оставить текущий уровень важности событий без изменений, нажмите **Отложить перезапуск**. При этом внесение изменений будет отложено до следующего запуска IPS.

5 Нажмите .

7

Настройка маршрутизации

Общие сведения о маршрутизации 168

Принципы маршрутизации 169

Просмотр таблицы маршрутизации 173

Настройка статической маршрутизации 174

Настройка маршрутов протоколов DHCP и PPP 178

Настройка OSPF 183

Настройка BGP 191

Настройка MultiWAN 199

Общие сведения о маршрутизации

ViPNet Coordinator HW 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 HW.

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 HW 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.

Принципы маршрутизации

В ViPNet Coordinator HW для хранения маршрутов используются:

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

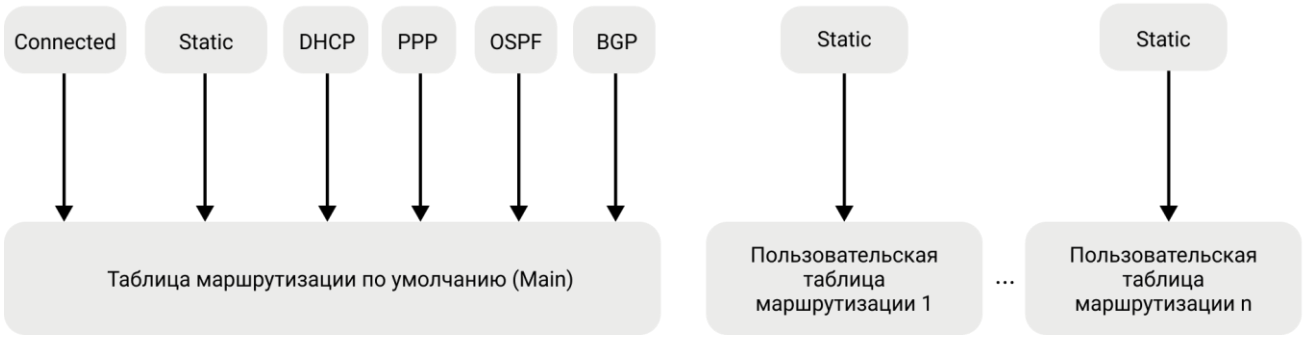


Рисунок 96. Формирование таблиц маршрутизации

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, для маршрутов остальных типов изменить это значение невозможно.

- 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 HW 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, то 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 HW. Политика использует маршруты из таблицы маршрутизации по умолчанию (Main). Настройка политики недоступна.

- Одну из пользовательских политик маршрутизации — создаются пользователем. С помощью таких политик вы можете разделить IP-трафик по признакам и маршрутизировать его по разным таблицам маршрутизации (см. Настройка функции MultiWAN).

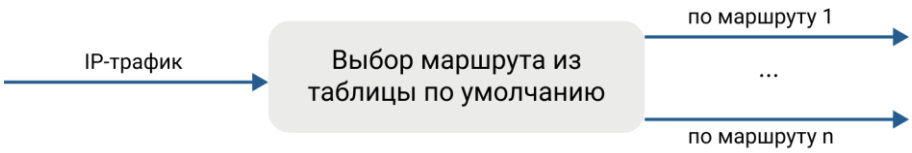


Рисунок 97. Маршрутизация при политике по умолчанию

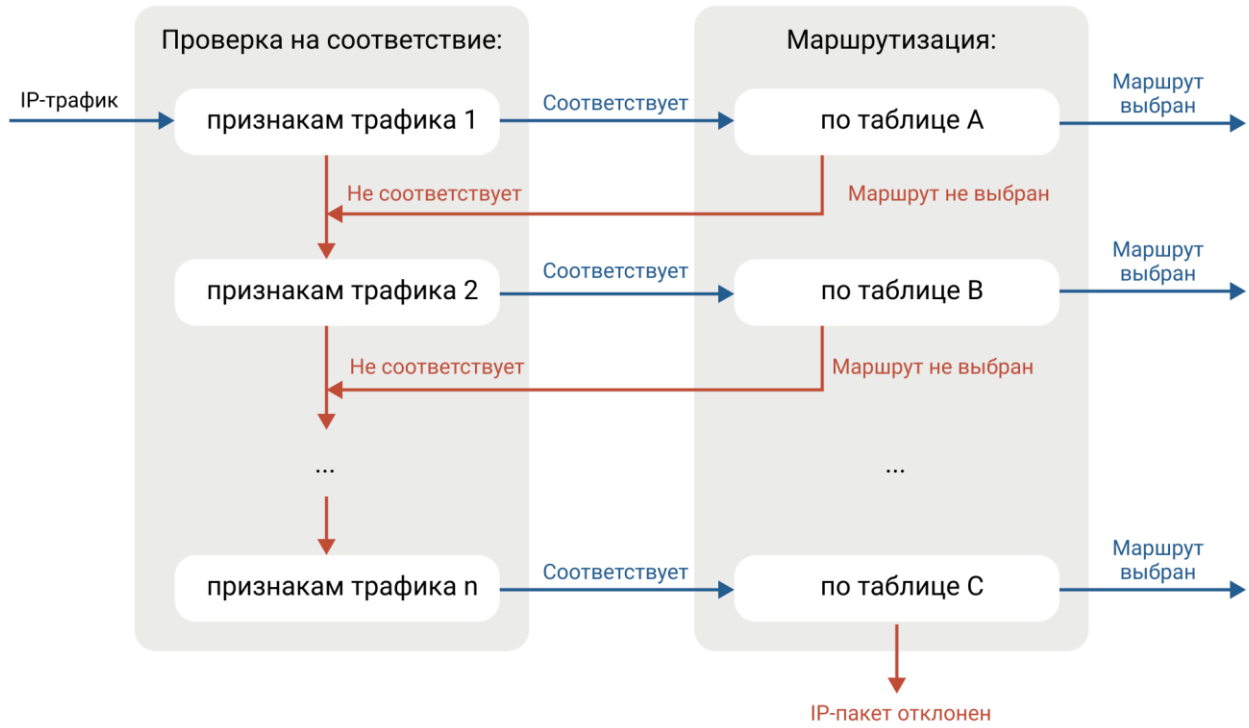


Рисунок 98. Маршрутизация при пользовательской политике

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.**

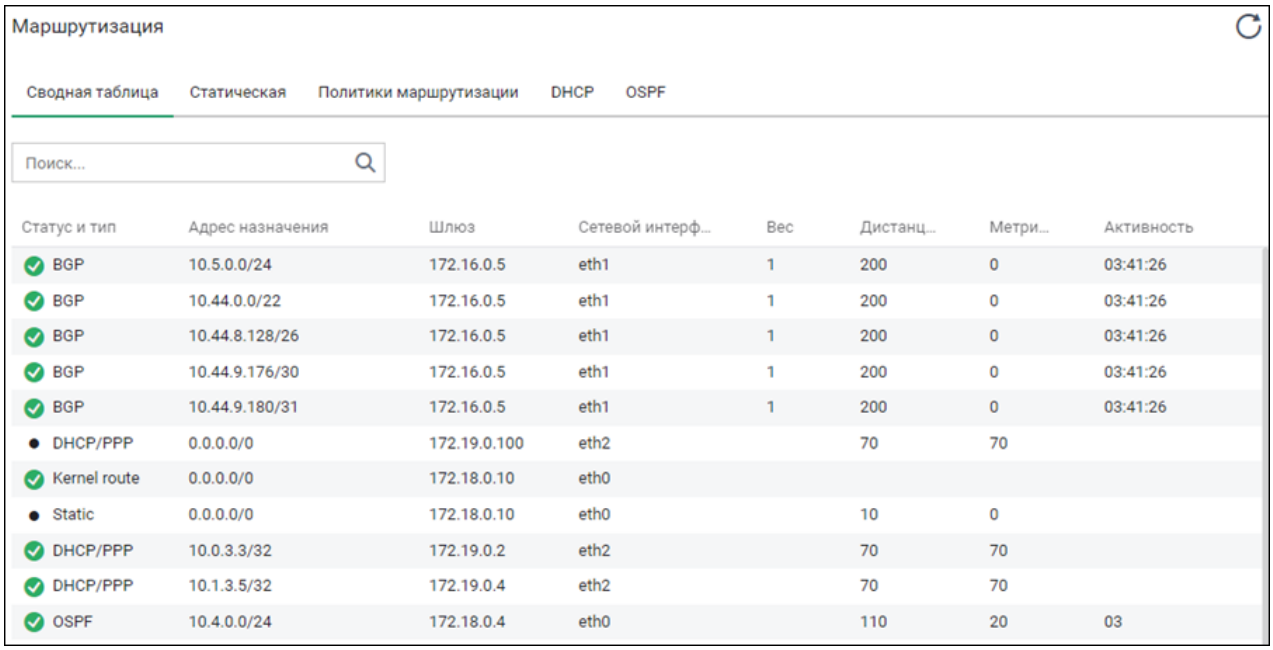


Рисунок 99. Просмотр общей таблицы маршрутизации

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

Примечание. Вес статического маршрута отображается при наличии нескольких маршрутов в одну сеть. Если маршрут единственный, его вес принимается равным единице.

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

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

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 .

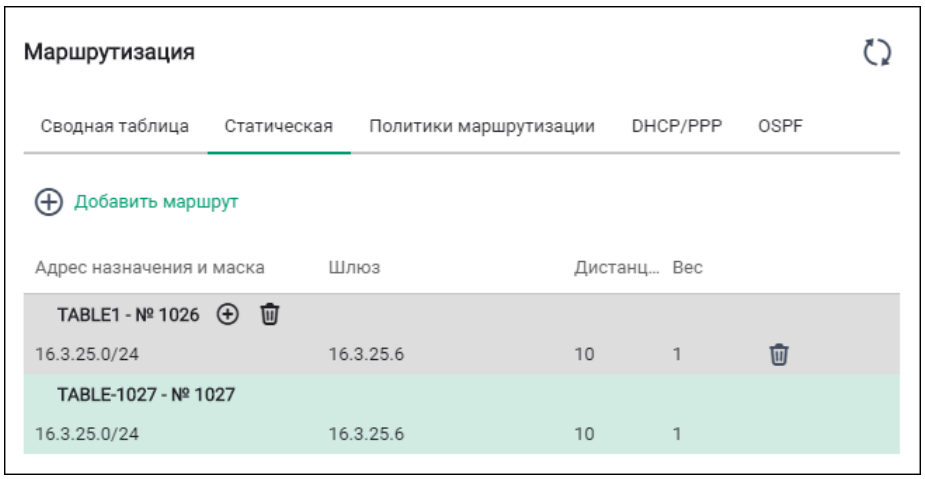


Рисунок 100. Список статических маршрутов

3 Задайте параметры маршрута:

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

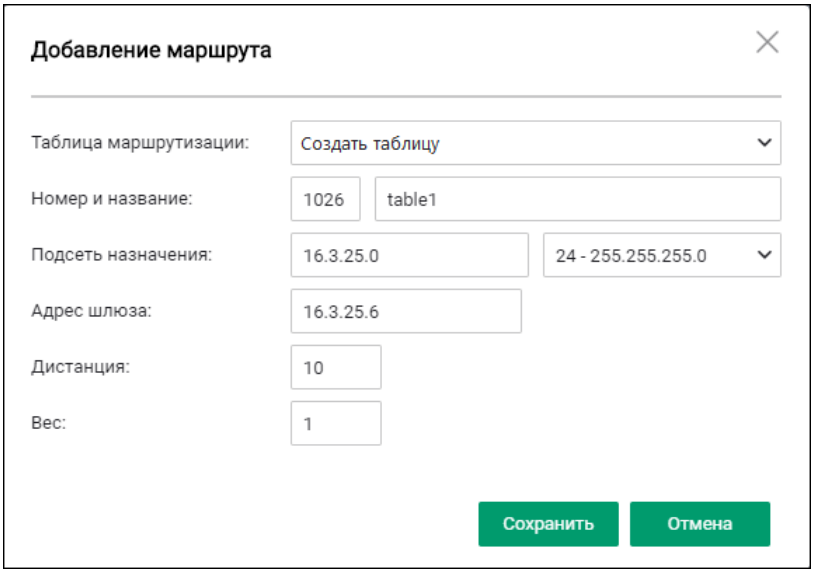


Рисунок 101. Добавление статического маршрута

- 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:

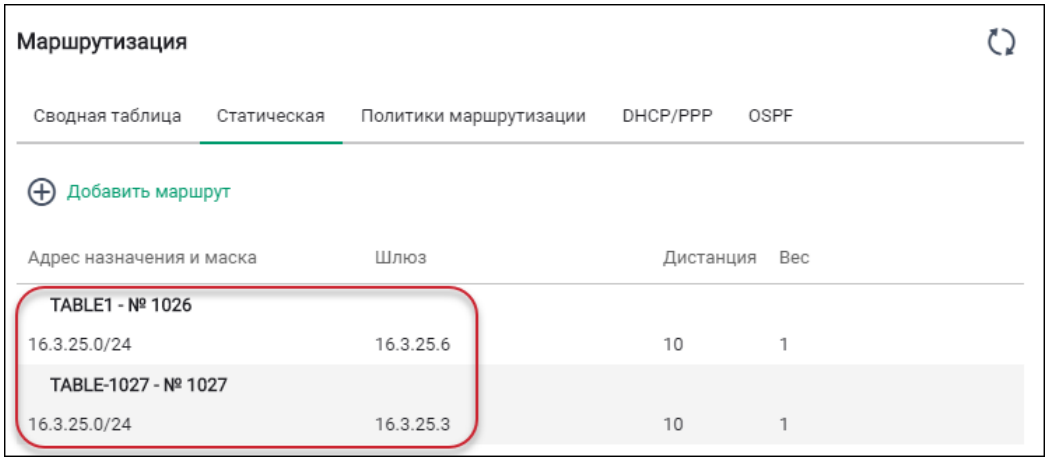


Рисунок 102. Распределение нагрузки между статическими маршрутами в одну сеть

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 HW 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 HW 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 HW 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.

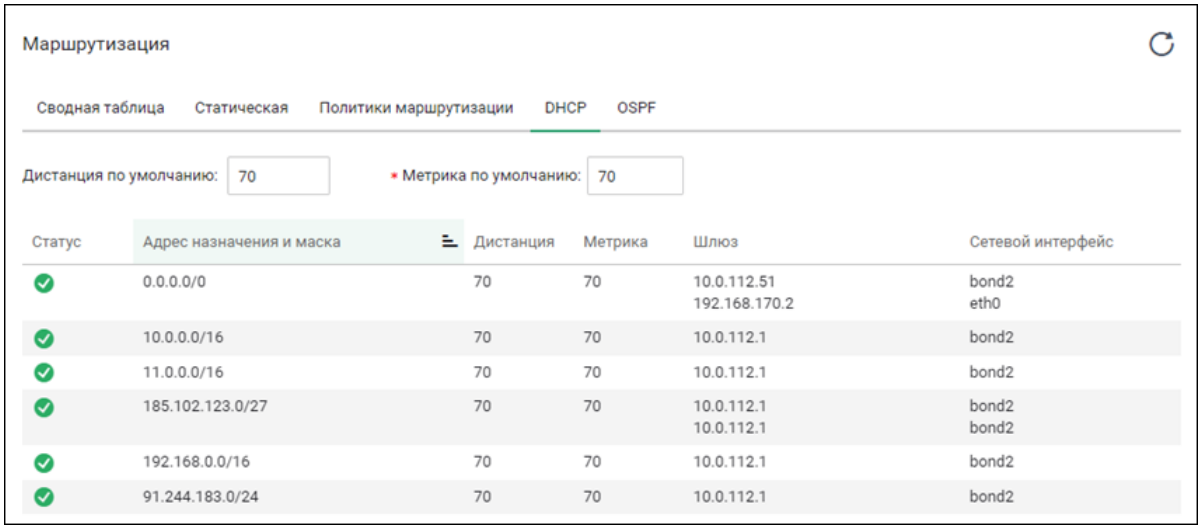


Рисунок 103. Задание административной дистанции маршрутам DHCP-сервера

Настройка метрики для маршрутов DHCP-сервера

Если на ViPNet Coordinator HW режим DHCP включён 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 лучший маршрут, чтобы использовать его при маршрутизации трафика. Параметром, позволяющим выбрать лучший маршрут, выступает метрика маршрута. Её можно задать на каждом сетевом интерфейсе, на котором включён режим DHCP, чтобы определить приоритет маршрутов DHCP-сервера на разных сетевых интерфейсах. Чем меньше значение метрики, тем выше приоритет маршрута. Если на разных сетевых интерфейсах заданы одинаковые метрики, то поступившие маршруты в одну и ту же сеть будут объединены в один маршрут с несколькими шлюзами.

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

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

- Ethernet (см. Настройка сетевых интерфейсов Ethernet).
- VLAN (см. Обработка трафика из нескольких VLAN).
- Wi-Fi (wlan) (см. Подключение к сети Wi-Fi) — нет в исполнении ViPNet Coordinator VA.
- Агрегированный интерфейс.

При этом должны выполняться следующие условия:

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

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

Чтобы настроить метрику для маршрутов, поступающих от DHCP-сервера:

1 Выберите **Сетевые 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**.

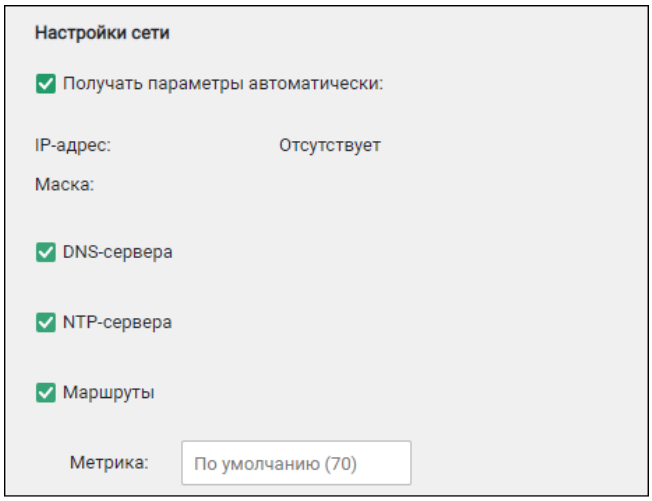


Рисунок 104. Настройка режима получения параметров интерфейса от DHCP-сервера

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 HW может быть подключен к другим сетям, в которых маршруты распространяются по DHCP-протоколу. В этом случае ViPNet Coordinator HW 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.

1 Выберите **Сетевые настройки** и нажмите .

2 Щелкните интерфейс **ppp0**.

3 Если интерфейс включен, выключите его.

4 Убедитесь, что 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 ее значение в указанном поле. После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

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

Если для маршрутов 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.

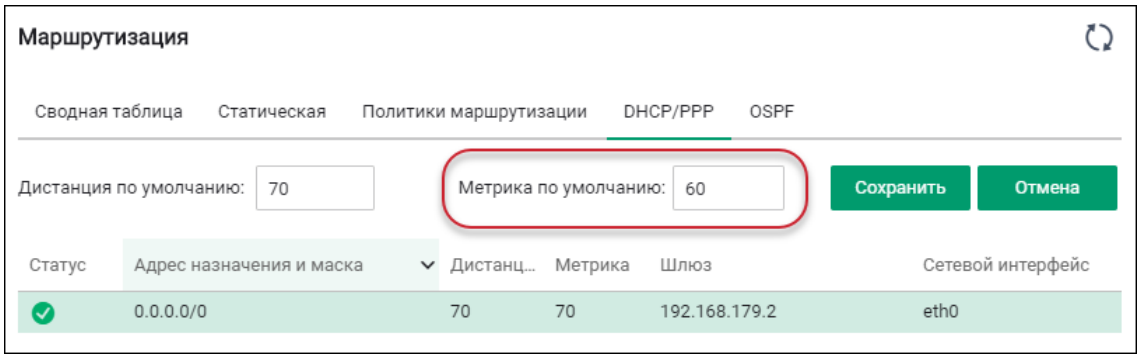


Рисунок 105. Задание метрики по умолчанию

Настройка OSPF

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

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

В процессе настройки маршрутизации по протоколу OSPF вам потребуется:

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



Внимание! При использовании OSPF необходимо настроить аутентификацию.

Если ViPNet Coordinator HW непосредственно связан с другими координаторами, рекомендуется при задании IP-адреса доступа этих координаторов указывать метрику `1`. В этом случае при наличии нескольких альтернативных маршрутов защищенный 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 HW имеет ограничения: из RFC 2328 не поддерживаются:

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

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

OSPF-маршрутизация работает следующим образом:

1. OSPF-маршрутизаторы устанавливают связь друг с другом посредством многоадресной (multicast) рассылки.
2. OSPF-маршрутизаторы начинают обмениваться сообщениями типа LSA (Link State Advertisements), в которых передают информацию о состоянии каналов связи с помощью однонаправленной (unicast) рассылки.
3. При получении LSA-сообщения информация из него заносится в базу данных (link state database). Если LSA-сообщение содержит новую информацию о канале связи по сравнению с той, которая содержится в базе данных, то оно передаётся маршрутизаторам-соседям.
4. На каждом маршрутизаторе по алгоритму Дейкстры (SPF algorithm) вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость. Таким образом, каждый OSPF-маршрутизатор имеет собственное представление о состоянии каналов связи и топологии сети, но при этом все маршрутизаторы используют одну базу данных состояний каналов связи для вычисления кратчайших маршрутов.

Межсетевая среда, в которой находятся OSPF-маршрутизаторы, представляется как совокупность областей маршрутизации, соединённых друг с другом через некоторую базовую область.

Выделяют следующие типы областей маршрутизации:

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

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

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

Выделяют следующие типы маршрутизаторов:

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

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

Протокол OSPF поддерживает два способа аутентификации:

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

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

Настройка 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).

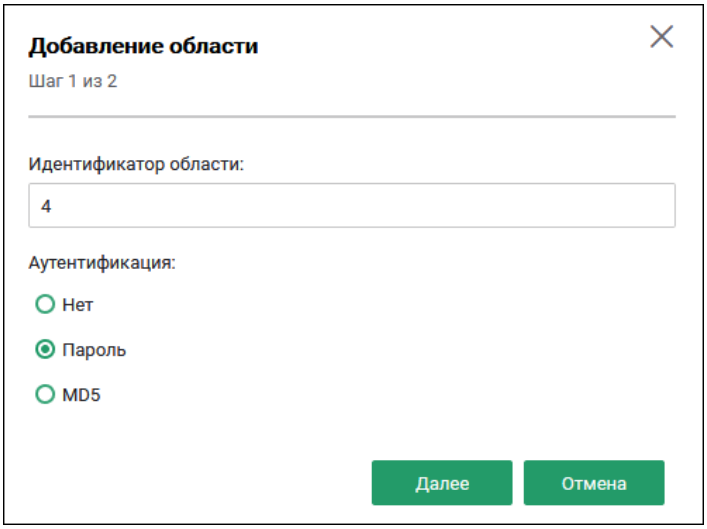


Рисунок 106. Добавление области

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.

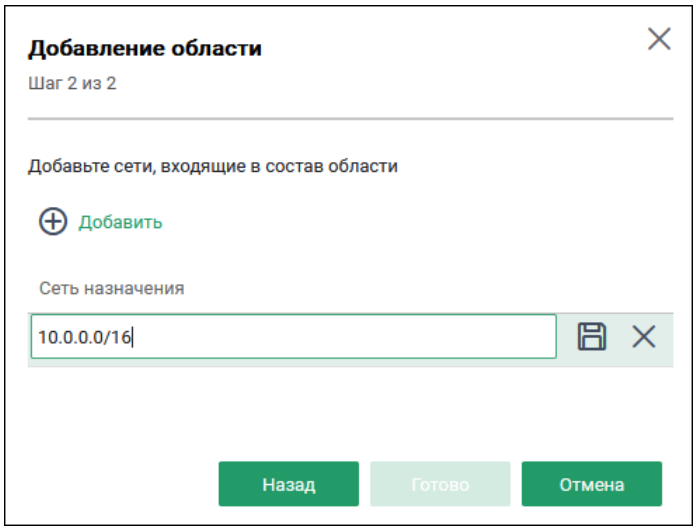


Рисунок 107. Добавление подсети

3.4 Нажмите **Готово.**

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

4.1 В строке интерфейса нажмите .

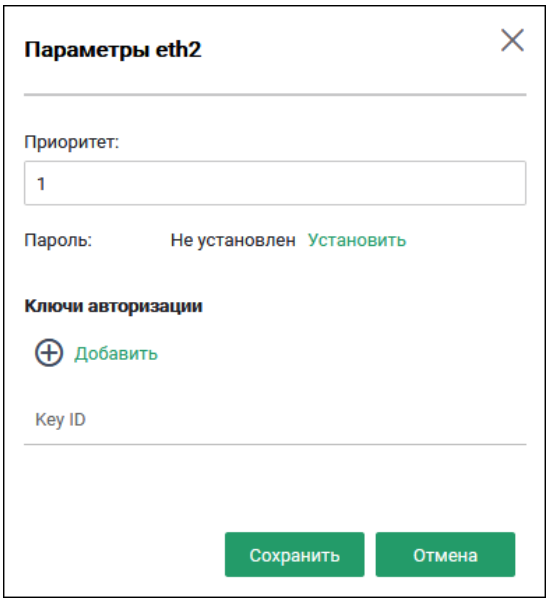


Рисунок 108. Настройка параметров интерфейса

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.**

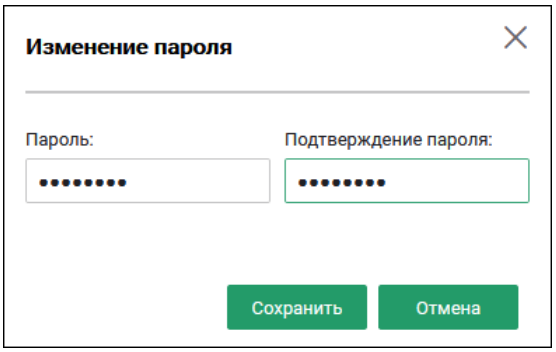


Рисунок 109. Установка пароля

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**.

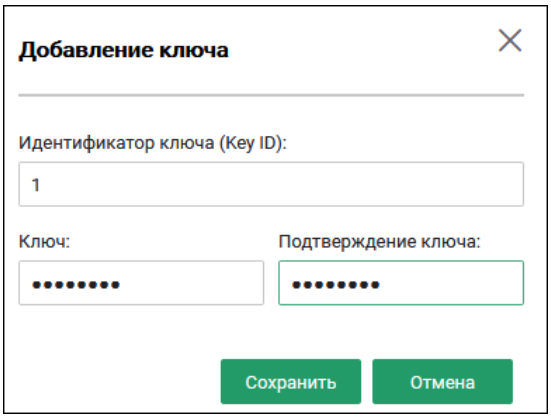


Рисунок 110. Добавление ключа

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

5 Создайте сетевые фильтры открытой сети:

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

Таблица 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 HW.

5.2 Фильтр, разрешающий исходящий IP-трафик ViPNet Coordinator HW 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

Одна распределенная сеть может состоять из нескольких автономных систем, в каждой из которых используется своя политика маршрутизации: Static, DHCP или OSPF. Чтобы автономные системы могли обмениваться маршрутами, на маршрутизаторе, расположенном на их границе необходимо настроить перераспределение маршрутов. Вы можете использовать ViPNet Coordinator HW как граничный маршрутизатор, который может перераспределять статические маршруты и маршруты, полученные по DHCP, в протокол OSPF.

Например, чтобы HW-2 HW-3 могли получать маршруты, используемые на R-4 и R-5, настройте перераспределение маршрутов на HW-1.

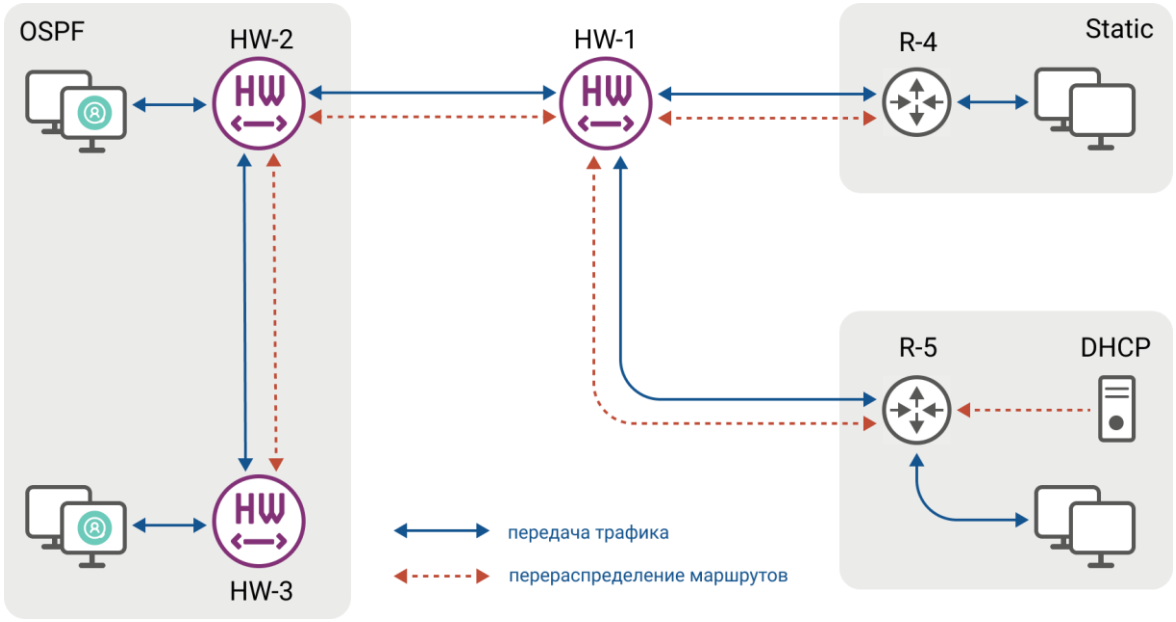


Рисунок 111. Перераспределение маршрутов между автономными системами

Включите перераспределение маршрутов:

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

2 Включите **Служба OSPF**.

3 Перейдите в **Настройки службы**.

4 Установите флажок в группе **Типы распространяемых маршрутов**:

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

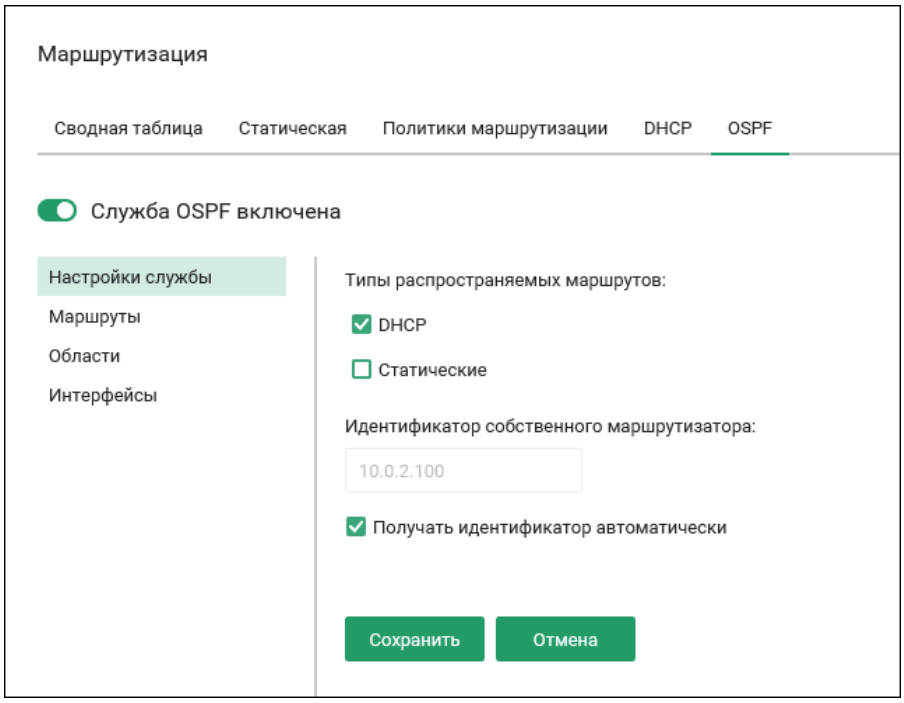


Рисунок 112. Включение перераспределения маршрутов DHCP-сервера

5 Чтобы выключить перераспределение маршрутов, снимите соответствующие флажки.

6 Нажмите **Сохранить**.

Настройка BGP

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 HW 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).

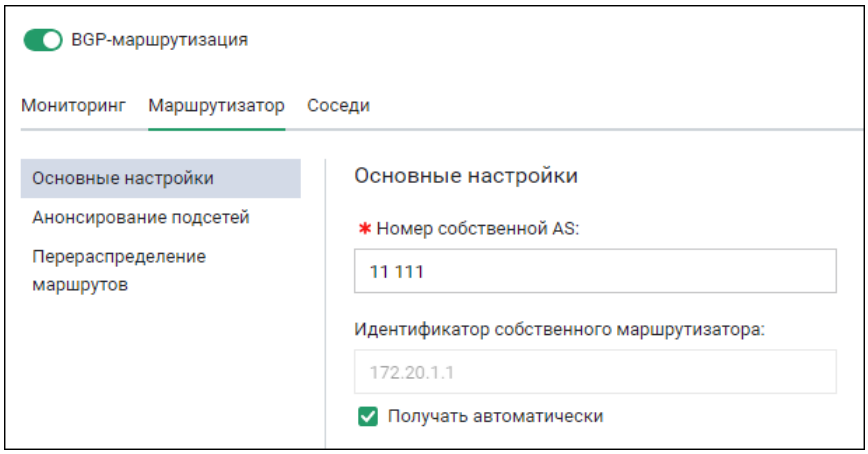


Рисунок 113. Основные настройки маршрутизатора

6 Нажмите **Сохранить**.

Настройка соседей

Добавление соседа

Внимание! Текущая версия ViPNet Coordinator HW 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

Имя фильтра	Источник	Назначение	Транспортный протокол	Расписание
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.

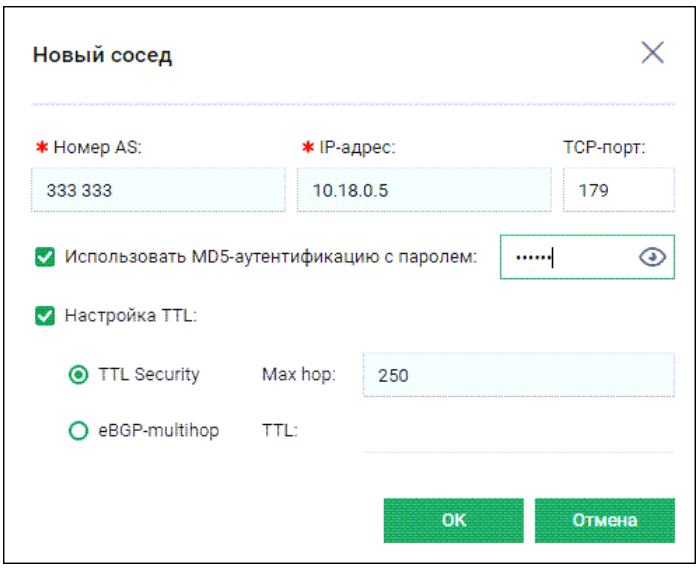


Рисунок 114. Добавление соседа

2.4 Нажмите **OK**.

Просмотр списка соседей

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

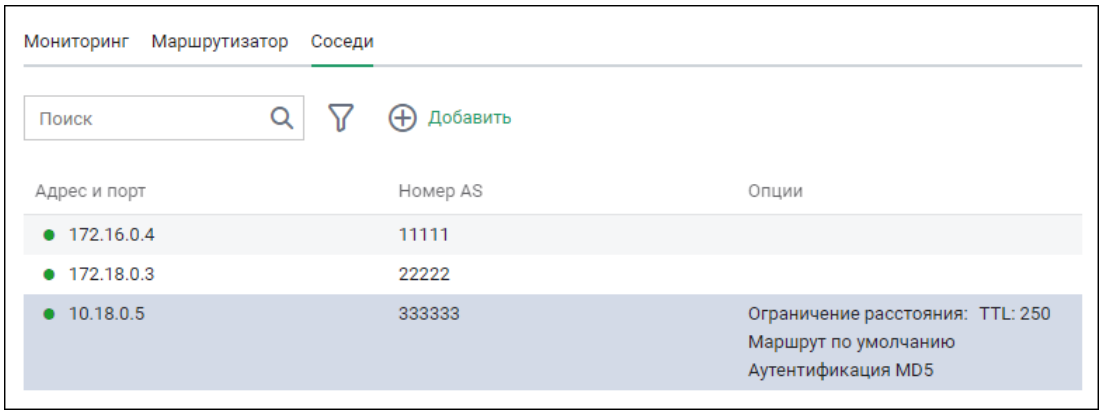


Рисунок 115. Список соседей

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.

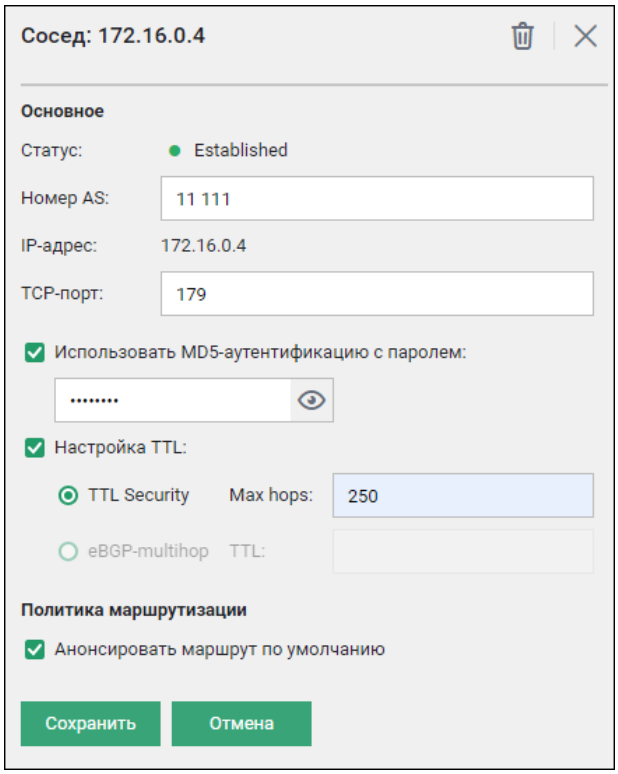


Рисунок 116. Изменение настроек соседа

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**.

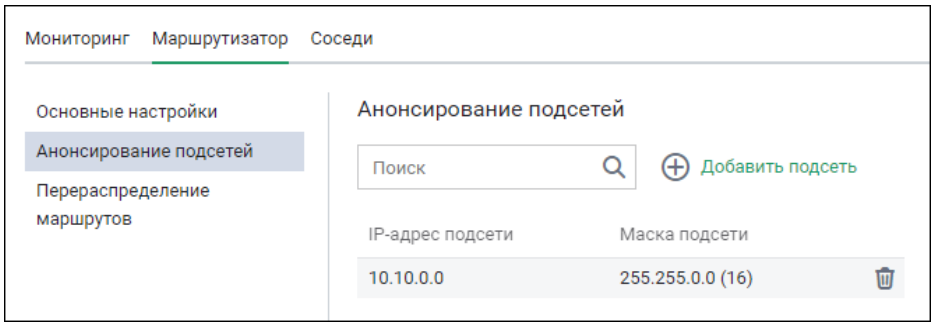


Рисунок 117. Добавление анонсируемой подсети

Перераспределение маршрутов

Внимание! Текущая версия ViPNet Coordinator HW 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**.

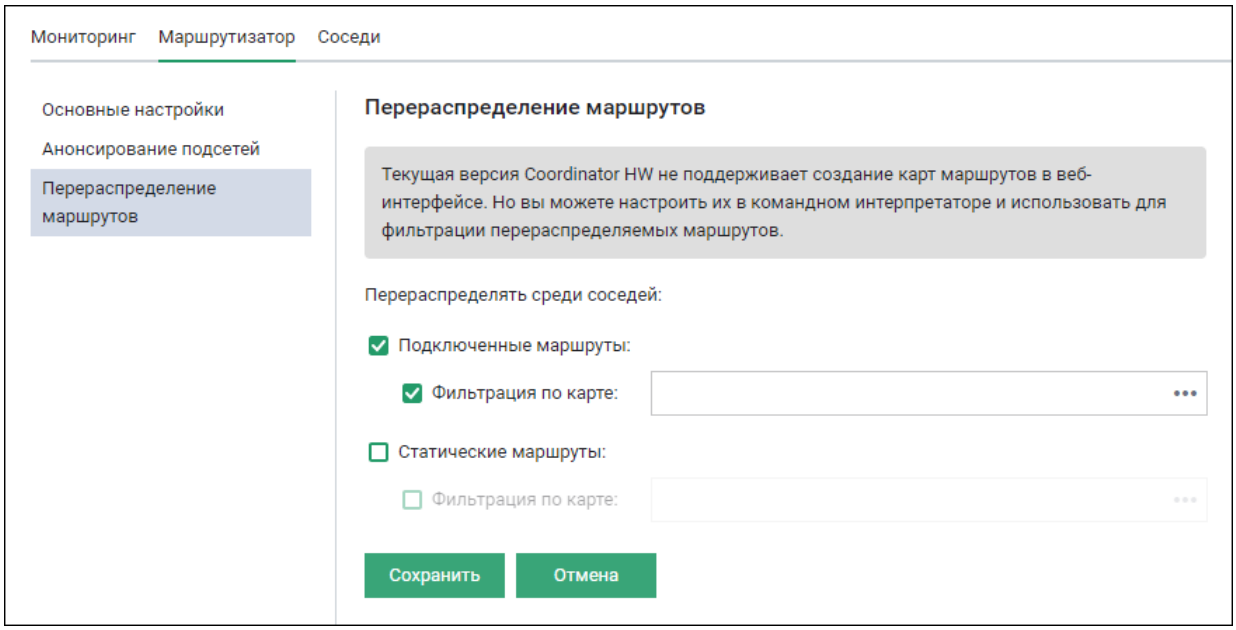


Рисунок 118. Выбор типа перераспределяемых маршрутов и фильтрации по картам маршрутов

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.

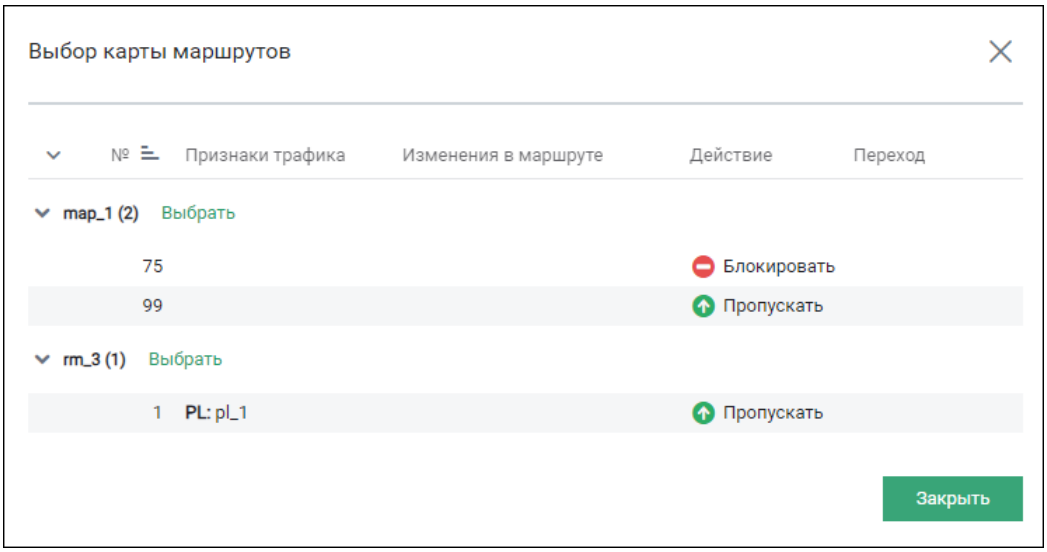


Рисунок 119. Выбор карты маршрутов

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 120. BGP-таблица

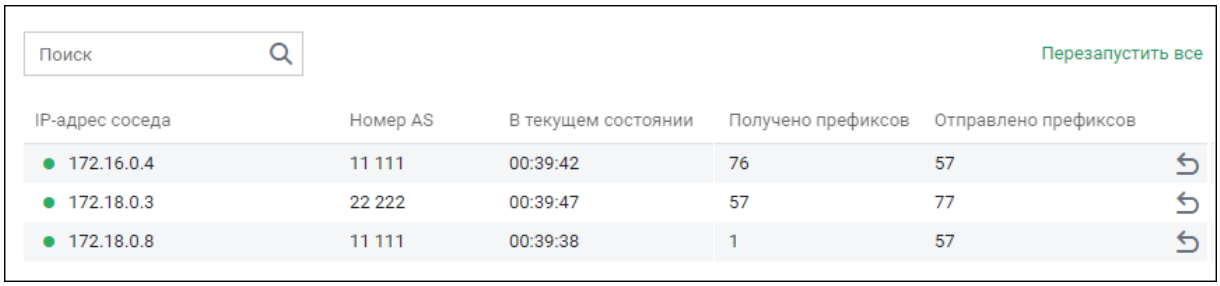
В списке по каждому маршруту отображаются:

- 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 121. 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 MultiWAN

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

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

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

Особенности настройки

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

- После добавления проверки шлюза DGD по протоколу TCP и портам 80 и 443 необходимо создать соответствующий разрешающий сетевой фильтр: источник — **Мой узел ViPNet**, назначение — IP-адрес шлюза, порты назначения 80 и 443.

Настройка политик маршрутизации

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

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

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

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

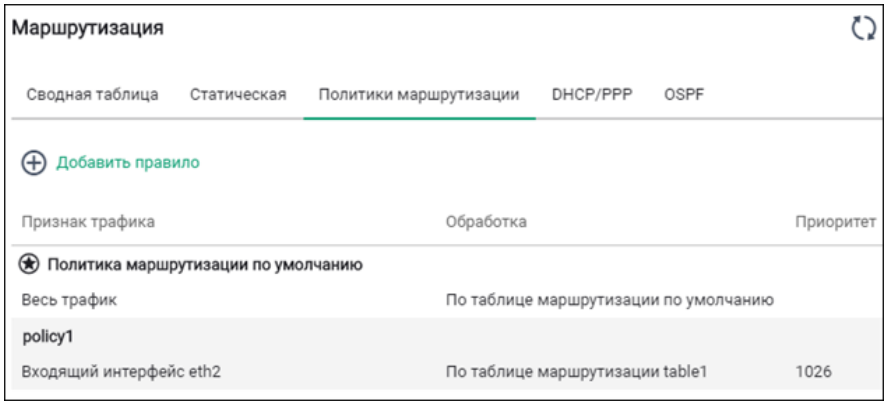


Рисунок 122. Настройка политик маршрутизации

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

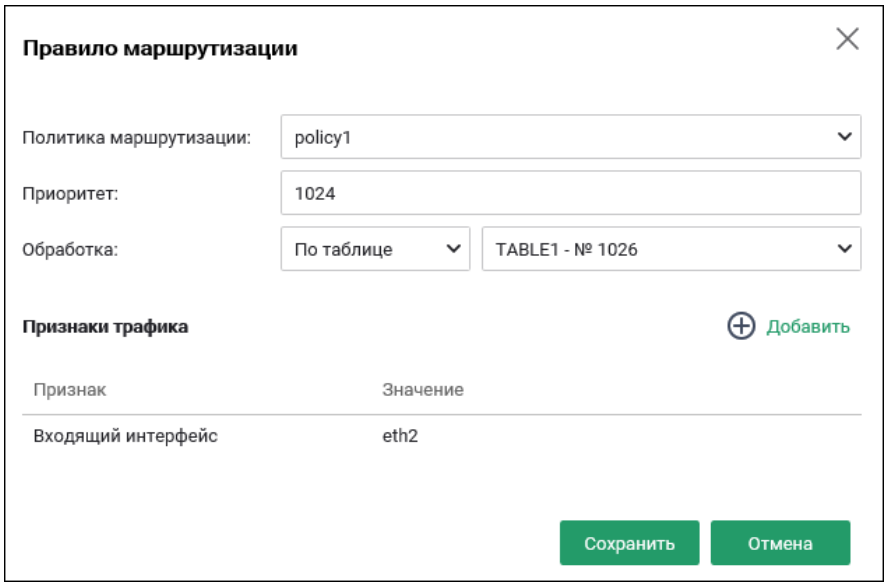


Рисунок 123. Добавление правила маршрутизации

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

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

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

---

5 Выберите метод обработки IP-пакетов для правила маршрутизации:

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

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

6.1 Нажмите ⊕ **Добавить**.

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

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

6.4 Нажмите **Сохранить**.

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

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

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

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

Настройка проверки состояния шлюзов (DGD)

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

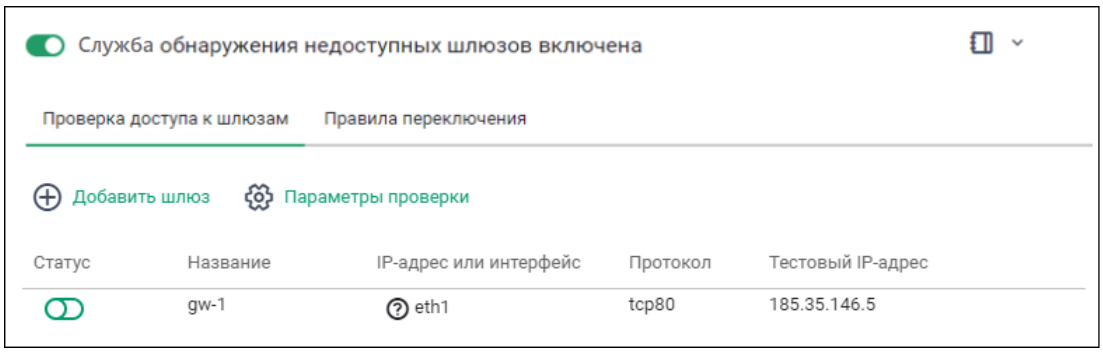


Рисунок 124. Настройка проверки состояния шлюзов

2 Включите **Служба обнаружения недоступных шлюзов**.

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

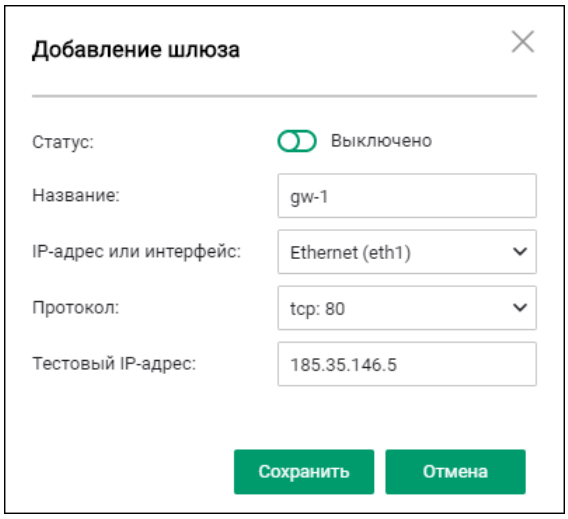


Рисунок 125. Добавление проверки доступности шлюза

- произвольное название шлюза;
- IP-адрес шлюза (если IP-адрес назначен статически) или сетевой интерфейс ViPNet Coordinator HW (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.

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:

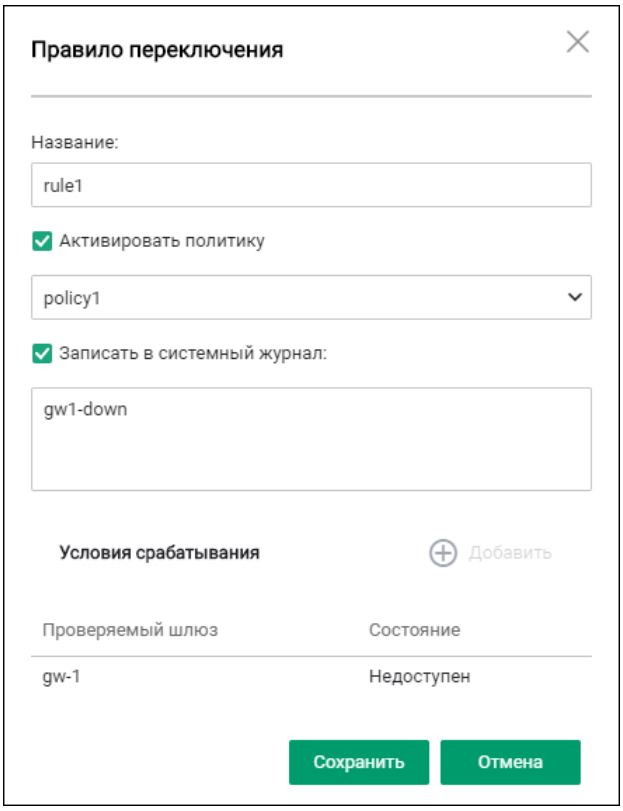


Рисунок 126. Добавление правила проверки состояния шлюза

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

6.4 Нажмите **Сохранить**.

7 Чтобы сбросить параметры проверки доступности к значениям по умолчанию:

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

7.2 Нажмите **Параметры проверки**.

7.3 Нажмите **Сброс настроек**.

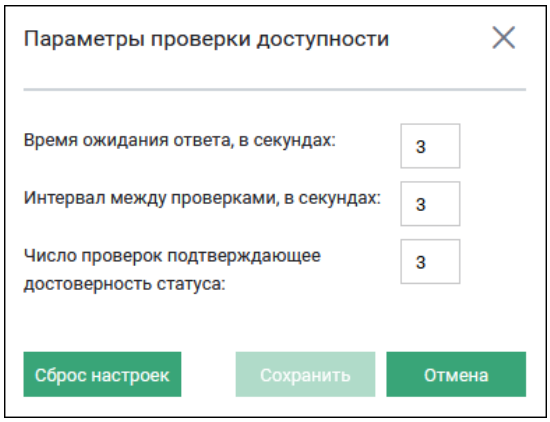


Рисунок 127. Окно настроек проверки доступности шлюза



8

Настройка параметров безопасности

Управление локальными учетными записями 207

Управление ключами локального SSH-сервера 212

Настройка подключения к веб-интерфейсу 213

Обновление ключей по истечении срока их действия 215

Управление локальными учетными записями

Параметры учетных записей

Таблица 10. Параметры локальных учетных записей

Параметр	Обозначение	Значения
Имя *	`Login`	• допустимые символы: буквы (`A–Z`, `a–z`), цифры (`0–9`), символы `-._()` • длина: 1–63 символа
Пароль *	`Password`	• допустимые символы: буквы (`A–Z`, `a–z`), цифры (`0–9`), символы `(!@#$%^&*()-_+=;:'",.<>/?|\`~[]{})` • длина: 8–31 символ • пароль не имеет ограничения по сроку действия. Напоминание о необходимости смены пароля выводится через 150 дней после его установки или смены, а предупреждение — через 180 дней
Роль *	`Role`	• `Superadmin` — суперадминистратор • `Administrator` — администратор • `Netadmin` — сетевой администратор • `Auditor` — аудитор
Полное имя	`Full name`	• строка символов UTF-8 • длина строки: не более 128 символов
Описание	`Description`	• строка символов UTF-8 • длина строки: не более 128 символов • `Built-in account` — описание суперадминистратора (неизменяемое)
Состояние *	`Status`	• `active` — учетная запись активна • `blocked` — учетная запись заблокирована

* — обязательный параметр учетной записи.

Полномочия ролей по управлению учетными записями

Роль учетной записи определяет полномочия пользователя по настройке учетных записей, а именно:

- создание учетных записей;
- удаление учетных записей;
- изменение параметров учетных записей;
- просмотр учетных записей и завершение сессий пользователей.

Таблица 11. Полномочия ролей по созданию учетных записей

	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Создание учетных записей	Да	Да	Нет	Нет
Доступные роли учетной записи при создании новой или изменении существующей	• Administrator • Netadmin • Auditor	• Administrator • Netadmin • Auditor		

Таблица 12. Полномочия ролей по удалению учетных записей

	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Удаление учетных записей	Да	Да	Нет	Нет
Роли удаляемых учетных записей	• Administrator • Netadmin • Auditor	• Administrator • Netadmin • Auditor		

Таблица 13. Полномочия ролей по изменению параметров учетных записей

Параметр	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Имя	Да	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator
Роль	Нет	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator
Полное имя	Да	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator
Описание	Нет	Superadmin	Superadmin	• Superadmin • Administrator
Пароль	Да	• Superadmin • Administrator	• Superadmin • Administrator • Netadmin (свой пароль)	• Superadmin • Administrator • Auditor (свой пароль)

Параметр	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Состояние	Нет	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator

Таблица 14. Полномочия ролей по просмотру учетных записей и завершению сессий

	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Просмотр списка локальных пользователей и параметров их учетных записей	Да	Да	Да	Нет
Завершение сессий локальных пользователей	• свои сессии • Administrator • Netadmin • Auditor	• свои сессии • Administrator • Netadmin • Auditor	свои сессии	свои сессии

Управление учетными записями

После инициализации на ViPNet Coordinator HW есть только локальная учетная запись `admin` с ролью суперадминистратора. Пароль для этой учетной записи вы задали в ходе инициализации.

В соответствии с политиками безопасности вашей организации создайте учетные записи с ролями администратора, сетевого администратора и аудитора. Для этого выберите **Пользователи Coordinator HW** > **Локальные учетные записи**.

Чтобы добавить учетную запись:

1. Нажмите **Добавление учетной записи**.
2. Введите имя учетной записи.
3. Выберите роль пользователя.
4. Введите и подтвердите пароль.
5. При необходимости задайте полное имя пользователя и описание учетной записи.
6. Нажмите **Сохранить**.

Чтобы изменить параметры или задать новый пароль учетной записи:

1. В строке пользователя справа выберите > **Изменить**.
2. Измените необходимые параметры.
3. Для изменения пароля нажмите **Изменить**, введите и подтвердите новый пароль.

4 Нажмите **Сохранить**.

Чтобы заблокировать учетную запись, в строке пользователя справа выберите  > **Заблокировать**. При блокировке учетной записи пользователя все его сессии завершаются.

Чтобы удалить учетную запись:

1 В строке пользователя справа выберите  > **Удалить**.

2 Подтвердите выполнение операции.

Для поиска учетных записей вы можете использовать:

1 Поиск по имени учетной записи, полному имени пользователя и описанию: начните вводить текст в поле  **Поиск**.

2 Фильтр для отображения заблокированных учетных записей.

2.1 Нажмите  .

2.2 Выберите состояния для отображения:

- **Активна** — пользователь может подключаться к ViPNet Coordinator HW.
- **Заблокирована** — учетная запись заблокирована администратором.
- **Временно заблокирована** — учетная запись автоматически заблокирована для предотвращения подбора пароля.

Предотвращение подбора пароля учетных записей

Для предотвращения подбора пароля локальных учетных записей используется прогрессивная задержка ввода пароля, временная блокировка учетных записей и оповещение о попытках подбора пароля:

- Если имя пользователя указано верно, то каждая неудачная попытка ввода пароля, в том числе совершаемая им в разных сессиях, увеличивает счетчик ошибок аутентификации учетной записи на единицу.
- Если пароль учетной записи введен правильно, счетчик ошибок аутентификации учетной записи сбрасывается. Иначе, после 10-ой неудачной попытки учетная запись пользователя временно блокируется, по умолчанию на 10 минут. По истечении времени блокировки учетная запись автоматически разблокируется. Настроить другое время блокировки (от 10 до 1440 минут), одинаковое для всех локальных пользователей, вы можете в командном интерпретаторе.
- После трех неудачных попыток ввод пароля станет доступен через 3 секунды. Каждая последующая неудачная попытка ввода пароля увеличивает задержку в два раза по сравнению с предыдущей и считается попыткой подбора пароля. При этом значение счетчика попыток подбора пароля, общего для всех локальных учетных записей, увеличивается на

единицу. Уведомление о попытках подбора пароля с указанием значения счетчика отображается при каждой успешной аутентификации любого пользователя в окне **Зафиксированы попытки подбора пароля** центра оповещения.

- Неудачные попытки аутентификации пользователей и попытки подбора пароля регистрируются в журнале СКЗИ. Чтобы просмотреть попытки подбора пароля:

  2.1 Нажмите .

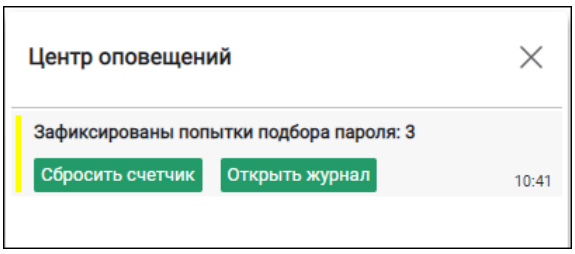
  

  Рисунок 128. Оповещение о попытках подбора пароля

  2.2 Для просмотра подробных сведения о попытках подбора пароля в журнале СКЗИ, нажмите **Открыть журнал**.

  2.3 Для сброса попыток подбора пароля (при наличии прав суперадминистратора, локального или централизованного администратора), нажмите **Сбросить счетчик**.

- Неверное указание имени пользователя также вызывает прогрессивную задержку ввода пароля. После 10-ой попытки аутентификации с неверным именем пользователя прогрессивная задержка сбрасывается.

Управление ключами локального SSH-сервера

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

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

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



Рисунок 129. Ключи локального SSH-сервера

2 Нажмите **Перевыпустить ключи**.

3 Нажмите **Продолжить**.

Настройка подключения к веб-интерфейсу

Чтобы перевыпустить самоподписанный сертификат:

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**:

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

3 Нажмите **Сохранить**.

4 Заново выполните аутентификацию на ViPNet Coordinator HW.

Вместо самоподписанного сертификата вы можете использовать сертификат, выданный УЦ:

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

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

2.1 В разделе **Владелец сертификата** — параметры в соответствии с требованиями УЦ.

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

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

3 Нажмите **Сохранить**.

4 Перешлите файл запроса в УЦ.

5 Получите сертификат из УЦ.

6 Импортируйте сертификат в локальное хранилище сертификатов ViPNet Coordinator HW:

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

6.2 Нажмите **Импортировать**.

6.3 Вставьте текст сертификата или загрузите файл сертификата.

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**.

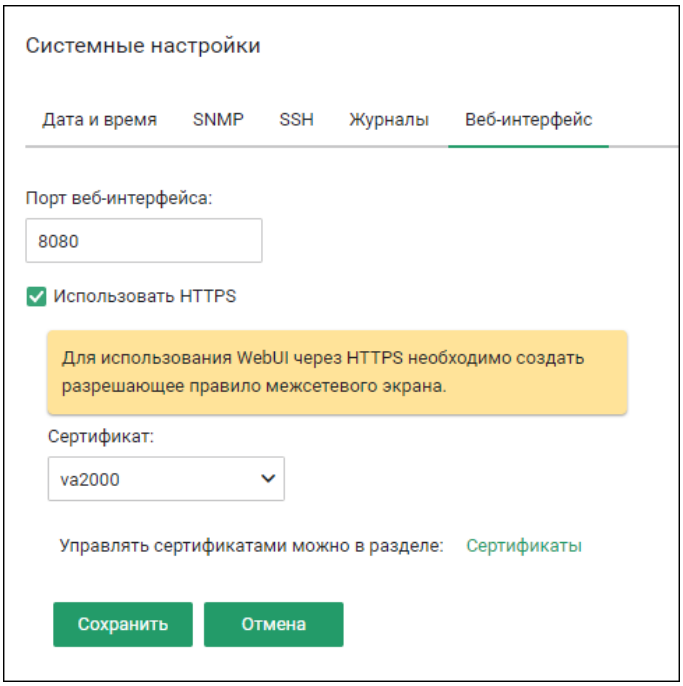


Рисунок 130. Параметры подключения к веб-интерфейсу

8 Заново выполните аутентификацию на ViPNet Coordinator HW.

При необходимости измените TCP-порт 8080:

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

2 Нажмите **Сохранить**.

3 Измените номер TCP-порта в фильтре защищенной сети **Allow ViPNet WebGUI**.

4 Заново выполните аутентификацию на ViPNet Coordinator HW.

Чтобы для подключения использовать HTTP:

1 Снимите флажок **Использовать HTTPS**.

2 Нажмите **Сохранить**.

3 Заново выполните аутентификацию на ViPNet Coordinator HW.

Обновление ключей по истечении срока их действия

Ключи обмена, ключи защиты обновлений узла и закрытый ключ сертификата пользователя имеют ограниченный срок действия — 15, 15 и 12 месяцев соответственно. Истечение срока действия любого из ключей не накладывает ограничений на работу ViPNet Coordinator HW. Но мы рекомендуем обновить ключи, чтобы гарантировать защиту трафика между узлами сети ViPNet.

При скором истечении срока действия (по умолчанию за 30 дней) или истечении срока действия любого из ключей в командном интерпретаторе и веб-интерфейсе выводится оповещение. Кроме этого, в системном журнале регистрируется событие об оповещении. Администратор сети ViPNet должен сформировать новые ключи и выслать их на ViPNet Coordinator HW.



Внимание! После обновления ключей создайте новую резервную копию конфигурации, так как использовать ранее созданные резервные копии будет невозможно.



9

Настройка системных параметров

Настройка даты и времени 217

Перезагрузка ViPNet Coordinator HW 218

Выбор профиля производительности 219

Установка серийного номера 221

Просмотр лицензии 222

Настройка даты и времени

Внимание! Если системные дата и время заданы неверно, защищённые соединения с другими узлами защищённой сети могут блокироваться. Рекомендуем настраивать синхронизацию системного времени по протоколу NTP (см. Настройка NTP-сервера).

Чтобы настроить дату и время:

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

2 Укажите часовой пояс, дату и время.

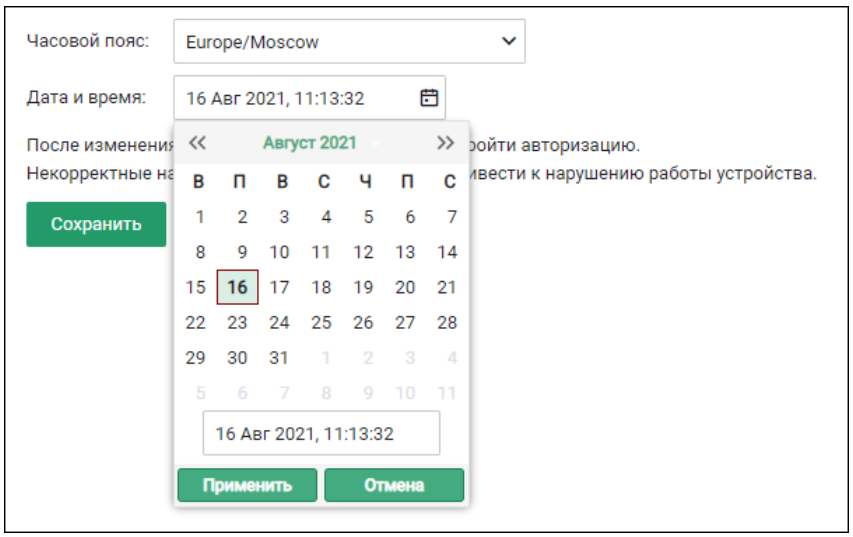


Рисунок 131. Настройка даты и времени

3 Нажмите **Сохранить**.

Перезагрузка ViPNet Coordinator HW

Чтобы удаленно перезагрузить ViPNet Coordinator HW:

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

2 Нажмите **Перезагрузить**.

3 Нажмите **ОК** для подтверждения.

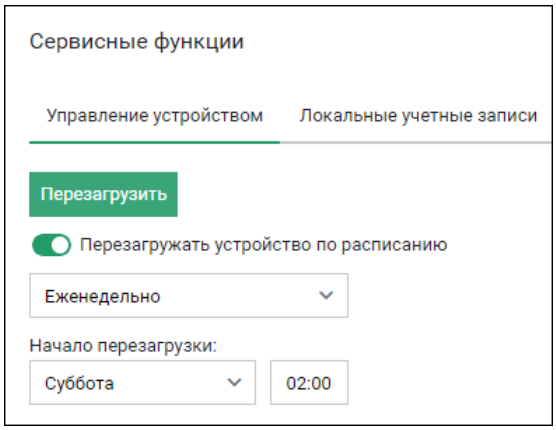


Рисунок 132. Перезагрузка ViPNet Coordinator HW

Чтобы настроить перезагрузку по расписанию:

3.1 Включите **Перезагружать устройство по расписанию**.

3.2 Настройте расписание.

Выбор профиля производительности

Для исполнений ViPNet Coordinator HW на аппаратных платформах HW100 N1, N2, N3, Q1, Q2, HW2000 Q4, Q5, HW5000 Q1, Q2 вы можете выбрать профиль производительности обработки трафика сетевых соединений. По умолчанию установлен профиль стандартного распределения ресурсов, обеспечивающий быструю обработку трафика нескольких сетевых соединений.

При выборе профиля высокой производительности для обработки трафика одного соединения происходит перераспределение ресурсов: все аппаратные прерывания от сетевых адаптеров обрабатываются одним ядром процессора, а шифрование выполняется оставшимися ядрами.

Внимание! Если выбран профиль высокой производительности, а фактическое количество сетевых соединений, обрабатываемых ViPNet Coordinator HW, больше одного, то скорость обработки и передачи защищенного трафика будет снижена.

Чтобы выбрать профиль высокой производительности для одного сетевого соединения:

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

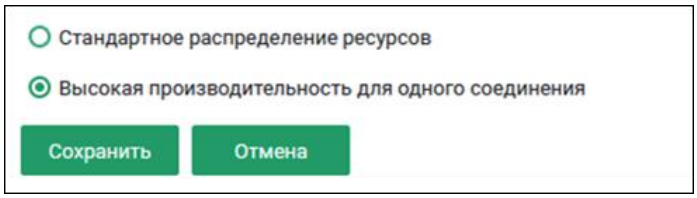


Рисунок 133. Выбор профиля производительности

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

3 Нажмите **Сохранить**.

4 В окне **Применение профиля производительности** выберите:

- **Перезагрузить сейчас.**
- **Применить при следующей перезагрузке**.

5 Нажмите **OK**.

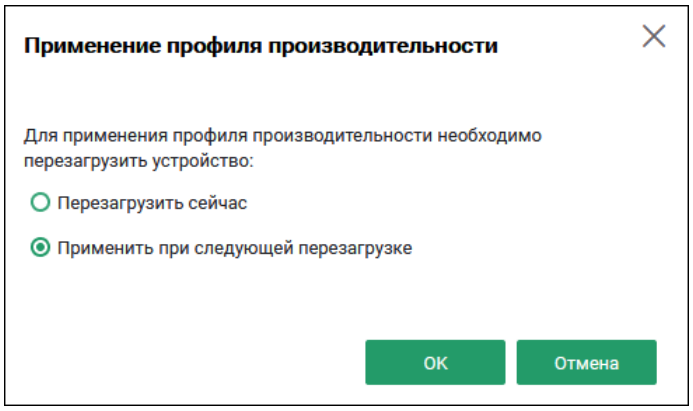


Рисунок 134. Применение профиля производительности

Установка серийного номера

Начиная с версии 5.2.0 ПО ViPNet Coordinator HW поддерживает серийный номер устройства для исполнений на аппаратных платформах. Для новых устройств номер устанавливается на производстве и не может быть изменен. Для устройств с ПО, обновленных пользователем, номер рекомендуется установить вручную в соответствии с указанным на этикетке устройства.

Внимание! Если серийный номер не отображается после обновления ПО, необходимо установить его вручную в соответствии с указанным на этикетке устройства.

Длина серийного номера: 4–18 символов. Допустимые символы:

- Прописные и строчные буквы латинского алфавита: `A–Z`, `a–z`.
- Арабские цифры: `0–9`.
- Специальный символ `-` .

Используйте серийный номер:

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

1 В правой верхней части страницы нажмите .



Рисунок 135. Серийный номер не задан

2 Если номера нет, вы можете установить его:

2.1 Нажмите .

2.2 Укажите серийный номер.

2.3 Нажмите .

Просмотр лицензии

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

1. В правой верхней части страницы нажмите .
2. Нажмите **Лицензионное соглашение**, чтобы ознакомиться с ним.
3. Чтобы посмотреть сведения о лицензиях, перейдите на вкладку **Лицензия**. В окне отобразятся сведения об основном и дополнительных объектах лицензирования, в т.ч. идентификаторы подписок.

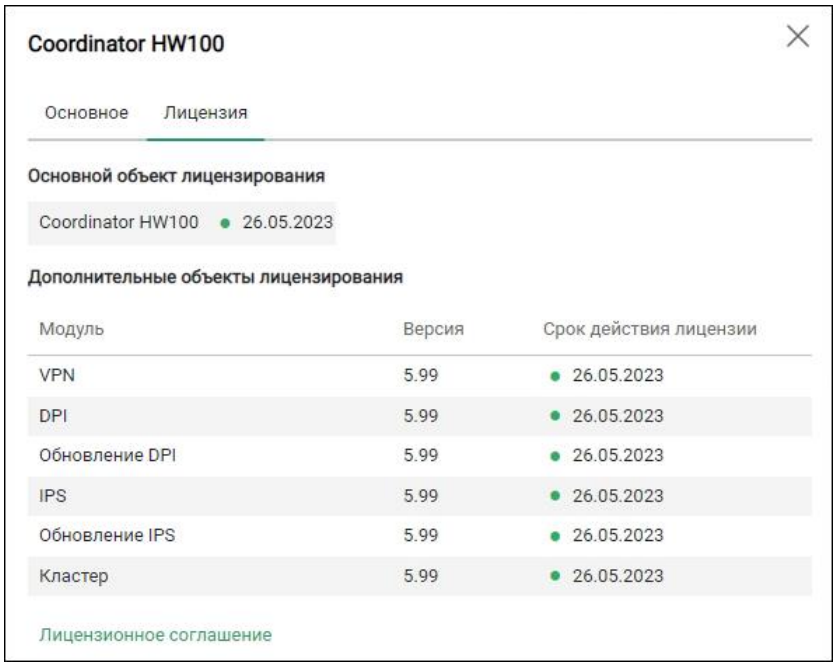


Рисунок 136. Сведения о лицензиях ViPNet Coordinator HW

10

Резервное копирование и восстановление настроек

Управление индивидуальной конфигурацией 224

Управление универсальной конфигурацией 228

Управление индивидуальной конфигурацией

Индивидуальная конфигурация позволяет осуществлять возврат настроек ViPNet Coordinator HW к состоянию, которое было на момент её создания. Файл индивидуальной конфигурации имеет расширение `ecf` и зашифрован на ключе обмена, который используется для защиты соединения ViPNet Coordinator HW с ViPNet Prime. Чтобы восстановить настройки из файла индивидуальной конфигурации, на ViPNet Coordinator HW должен быть установлен тот же ключ обмена, который использовался при экспорте конфигурации. Если ключ обмена был обновлён на ViPNet Coordinator HW, создайте новую резервную копию индивидуальной конфигурации.

Вы можете использовать копии индивидуальных конфигураций:

- Для восстановления настроек ViPNet Coordinator HW в случае сбоя или некорректного обновления ПО.
- При замене неисправного ViPNet Coordinator HW, в том числе и в кластере.

Индивидуальная конфигурация содержит:

- настройки защищенной сети;
- настройки сетевых интерфейсов;
- настройки маршрутизации и статические маршруты, если такие созданы;
- сетевые фильтры и правила трансляции адресов;
- настройки параметров обработки прикладных протоколов;
- настройки системы защиты от сбоев;
- настройки транспортного сервера MFTP;
- журналы и настройки протоколирования;
- настройки дополнительных служб (DHCP-сервера и других);
- настройки взаимодействия с ИБП;
- настройки туннелирования;
- текущие ключи для соединений по протоколу SSH2.

Резервное копирование индивидуальной конфигурации

Резервное копирование индивидуальной конфигурации может быть выполнено:

- В автоматическом режиме — на сервер ViPNet Prime по расписанию.

- В ручном режиме — на сервер ViPNet Prime или папку компьютера, с которого вы подключились к ViPNet Coordinator HW.

Примечание. На время резервного копирования создается сетевой фильтр, разрешающий подключение к серверу ViPNet Prime и останавливаются службы `vpn` и `mftp`.

По завершении копирования фильтр будет удален, а службы будут запущены заново.

В автоматическом режиме копия индивидуальной конфигурации создается один раз в сутки в соответствии с расписанием. При этом на сервере ViPNet Prime хранится только последняя копия конфигурации — каждая последующая копия заменяет предыдущую. По умолчанию резервное копирование включено в автоматическом режиме и выполняется по расписанию в случайное время из интервала 21.00–23.00.

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

Чтобы настроить время резервного копирования индивидуальной конфигурации в автоматическом режиме:

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

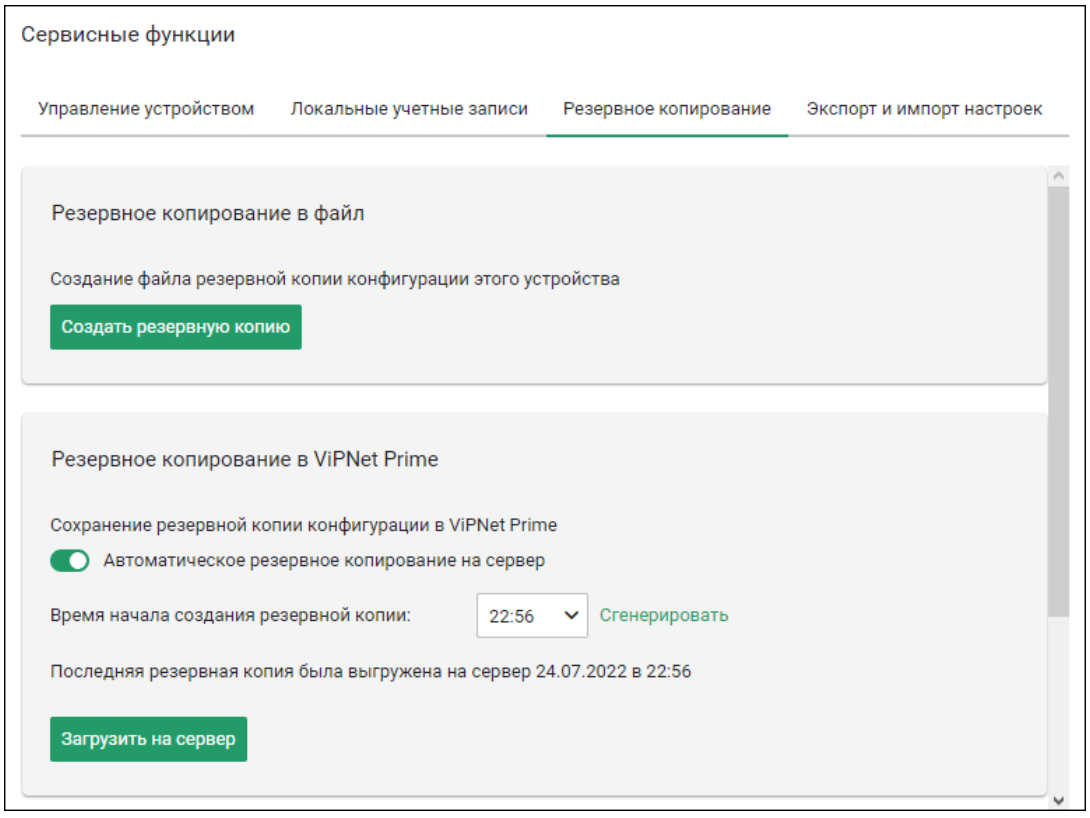


Рисунок 137. Настройка резервного копирования индивидуальной конфигурации

2 В разделе **Резервное копирование в ViPNet Prime** задайте время создания резервной копии:

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

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

2.2.1 Нажмите **Сгенерировать**.

2.2.2 Выберите из списков начало и окончание интервала времени.

2.2.3 Нажмите **Сгенерировать**.

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

Чтобы однократно создать копию конфигурации на сервере ViPNet Prime, независимо от настройки резервного копирования в автоматическом режиме, нажмите **Загрузить на сервер**. Дождитесь завершения операции; в случае успеха в строке **Последняя резервная копия была загружена на сервер в** будет указано время окончания загрузки.

Чтобы создать резервную копию индивидуальной конфигурации и сохранить ее в папке компьютера, с которого вы подключились к ViPNet Coordinator HW:

1. В разделе **Резервное копирование в файл** нажмите **Создать резервную копию**.
2. Дождитесь завершения операции. Файл индивидуальной конфигурации будет сохранен в папке **Загрузки**. 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.

Восстановление из резервной копии индивидуальной конфигурации

1. Выберите **Системные настройки** > **Сервисные функции** > **Резервное копирование**.
2. В разделе **Восстановление** нажмите **Восстановить**.
3. Выберите файл резервной копии и нажмите **Далее**.
4. Просмотрите параметры подключения к ViPNet Coordinator HW, которые будут восстановлены из резервной копии.

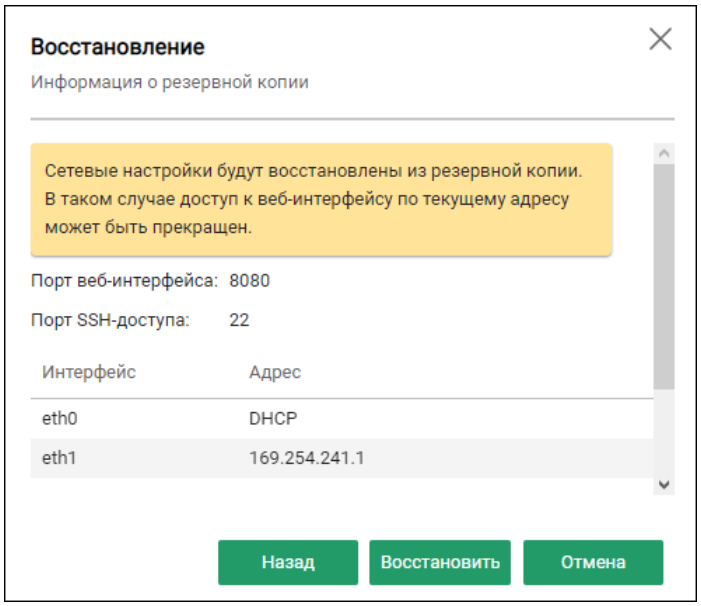


Рисунок 138. Параметры подключения к ViPNet Coordinator HW после восстановления настроек

5 Нажмите **Восстановить**.

6 Дождитесь восстановления настроек из резервной копии и перезагрузки ViPNet Coordinator HW.

Управление универсальной конфигурацией

Универсальная конфигурация включает три группы настроек ViPNet Coordinator HW:

- Настройки межсетевого экрана:
  - Сетевые фильтры.
  - Правила трансляции адресов (NAT).
  - Группы объектов.
- Настройки сетевых интерфейсов:
  - Состояние интерфейса (`on`/`off`).
  - Класс интерфейса (`access`, `trunk`, `slave`).
  - IP-адрес и маска сети, или настройки получения IP-адреса и других параметров по DHCP.
  - Дополнительные IP-адреса (`alias`).
  - Режим работы агрегированного интерфейса (`balance-rr`, `balance-xor`, `balance-tlb`, `802.3ad`, `active-backup`, `broadcast`).
  - Настроенные VLAN.
- Настройки маршрутизации:
  - Маршрут по умолчанию.
  - Статические маршруты.
  - Административная дистанция и вес маршрута.
  - Административная дистанция и вес маршрутов, полученных по DHCP.
  - Настройка метрики для маршрутов PPP-протокола.
  - Настройки маршрутизации по протоколу OSPF (состояние службы, области маршрутизации и подсети, приоритет интерфейсов, настройка перераспределения статических маршрутов и динамических маршрутов, полученных по DHCP, идентификатор маршрутизатора, настройки аутентификации).
  - Настройки DGD (состояние, перечень шлюзов и метод проверки доступности, правила переключения политик маршрутизации).
  - Настройки Policy Routing (политики маршрутизации и активная на момент обновления политика).

Кроме этого, универсальная конфигурация содержит сведения о продукте, платформе и версии ПО, например: HW-VA, VA, 5.1.0. Универсальная конфигурация позволяет переносить настройки с ViPNet Coordinator HW различных исполнений и версий ПО (4.3.2 и 4.5.x), а также ViPNet xFirewall

5.x. Файл универсальной конфигурации имеет расширение `vbe` и зашифровывается на пароле при экспорте конфигурации.

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: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

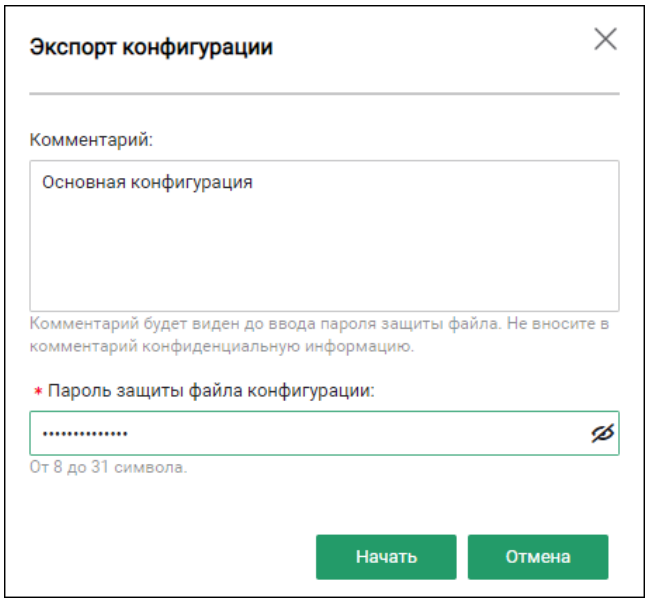


Рисунок 139. Экспорт универсальной конфигурации

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

Чтобы импортировать настройки универсальной конфигурации:

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

2 В разделе **Импорт настроек** нажмите **Импорт**.

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

4 Введите пароль защиты файла конфигурации.

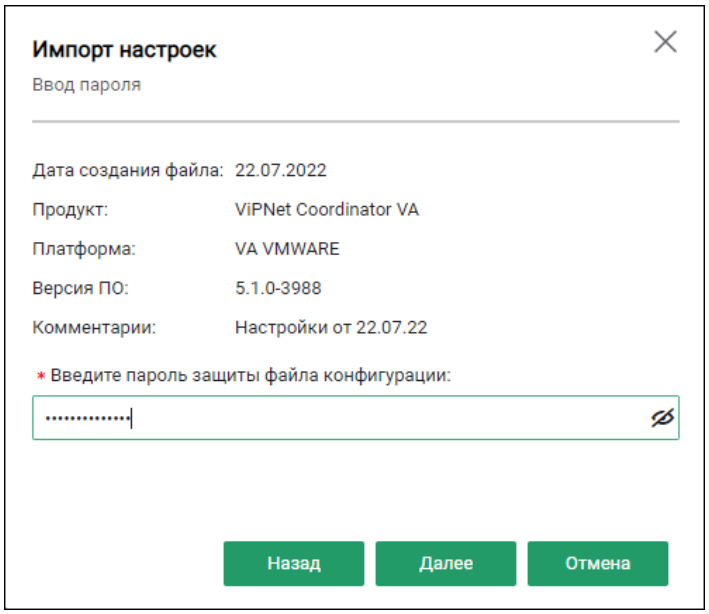


Рисунок 140. Ввод пароля защиты файла конфигурации

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

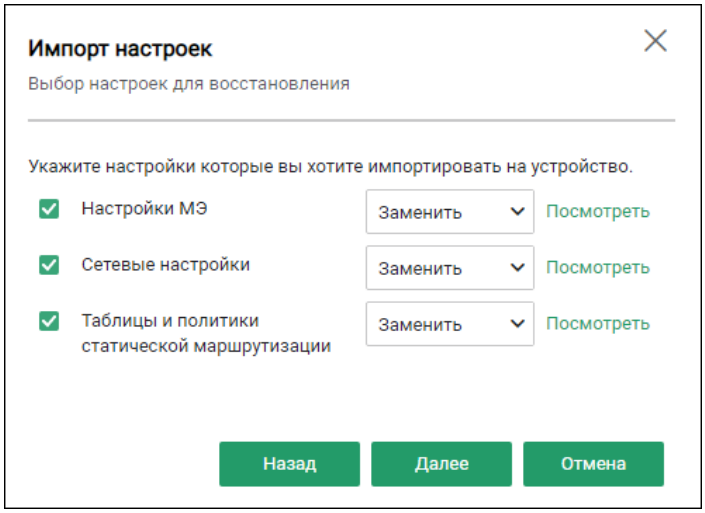


Рисунок 141. Выбор групп настроек и способа импорта

Для просмотра состава импортируемой группы настроек нажмите **Просмотреть**.

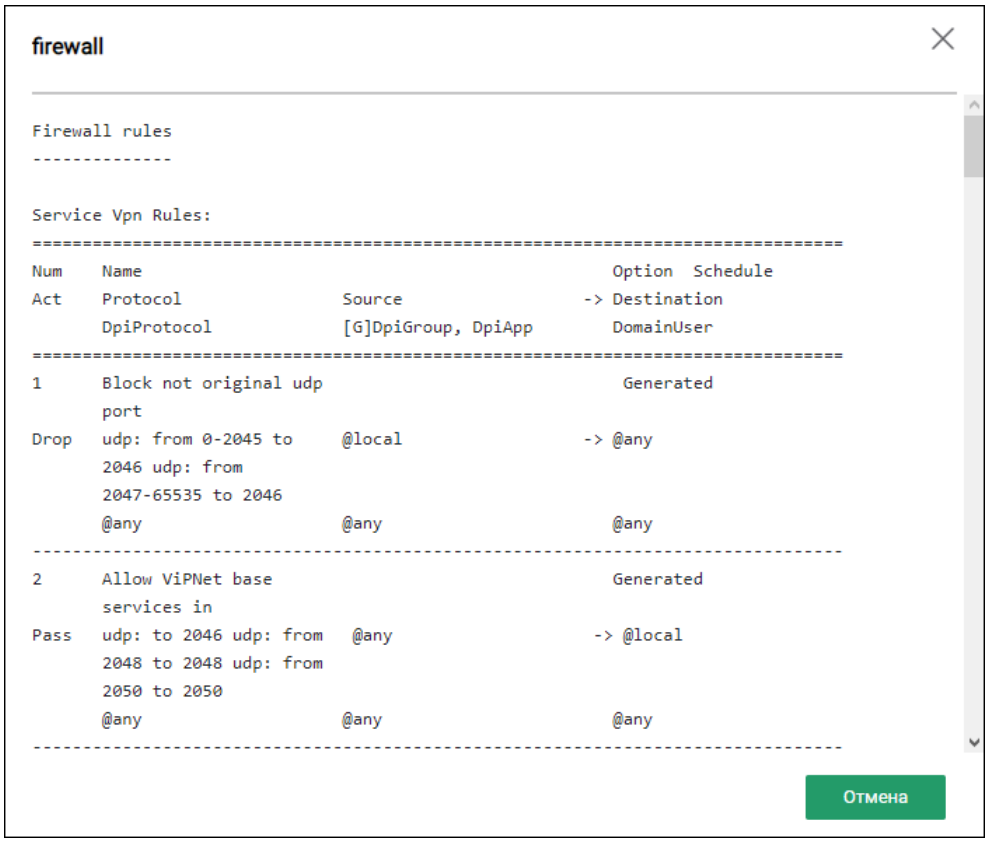


Рисунок 142. Просмотр импортируемых настроек группы firewall

6 Просмотрите параметры подключения к ViPNet Coordinator HW после завершения импорта настроек и нажмите **Продолжить**.

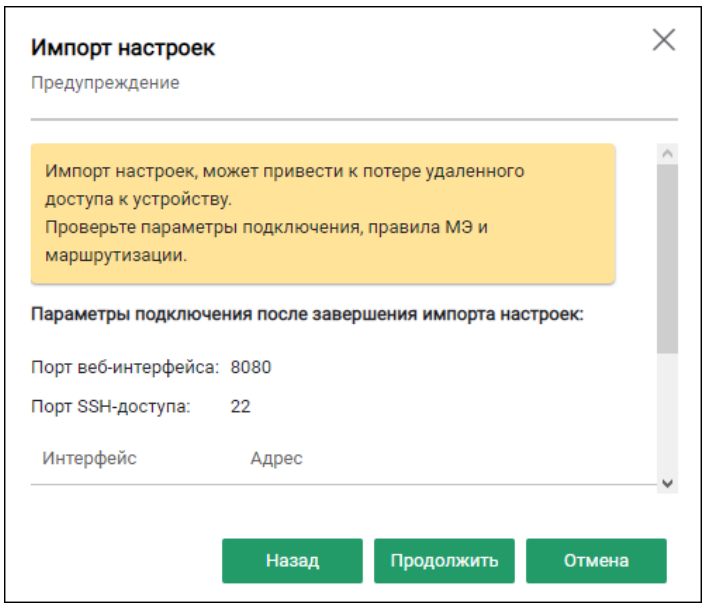


Рисунок 143. Параметры подключения к ViPNet Coordinator HW после импорта настроек

7 Дождитесь завершения импорта выбранных настроек универсальной конфигурации и нажмите **ОК**.

11

Работа с журналами

Настройка журналов 233

Журнал IP-пакетов 237

Журнал сессий 242

Журнал аудита 246

Журнал СКЗИ 248

Журнал MFTP 250

Журнал DNS-запросов 252

Системный журнал 254

Настройка журналов

Чтобы настроить параметры ведения журналов:

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

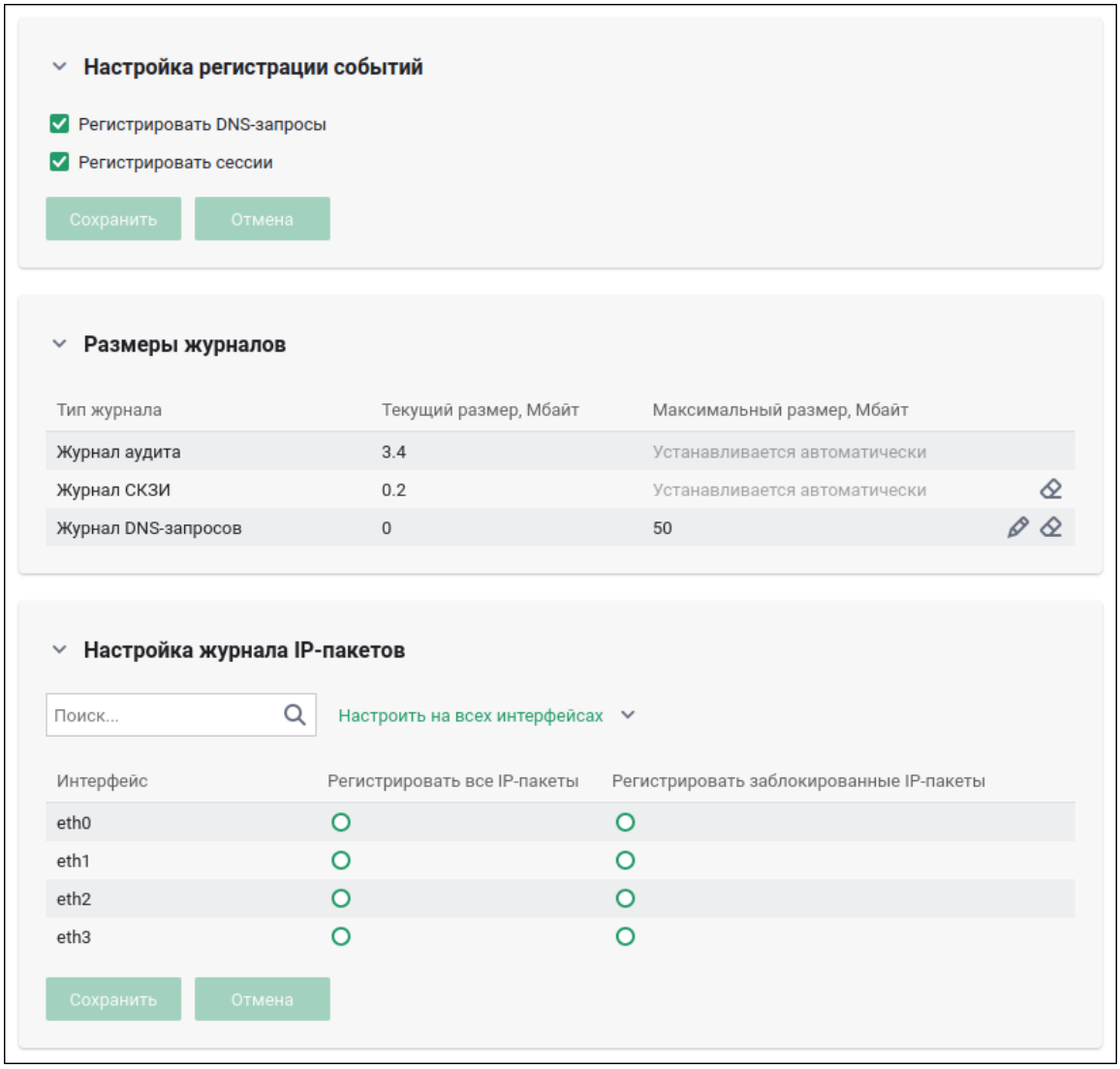


Рисунок 144. Настройка журналов

2 Чтобы настроить регистрацию событий:

2.1 Откройте раздел **Настройка регистрации событий**.

2.2 По умолчанию ведение журнала сессий выключено. Чтобы включить ведение журнала, выберите **Регистрировать сессии**.

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

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.

3.3 Максимальный размер журнала DNS-запросов вы можете задать в диапазоне:

- 1–50 Мбайт: для исполнений с одним дисковым накопителем;
- 1–200 Мбайт: для исполнений с двумя дисковыми накопителями.



Внимание! 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»).

3.4 Чтобы очистить журналы, нажмите  .

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

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

4 В разделе **Настройка журнала IP-пакетов** вы можете выбрать, какие пакеты (заблокированные или все) будут регистрироваться в журнале для каждого или для всех интерфейсов.



Примечание. Если для любого из сетевых интерфейсов выбрать, какие пакеты будут регистрироваться в журнале, то на таком интерфейсе выключится регистрация IP-пакетов по сетевым фильтрам и включится регистрация по интерфейсам. Это значит, что параметры каждого фильтра, отвечающие за регистрацию IP-пакетов, будут 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».

---

5 Чтобы настроить экспорт журнала IP-пакетов или журнала сессий по сети в формате CEF:

5.1 Откройте раздел **Отправка CEF-сообщений на удалённый сервер**.

5.2 Чтобы добавить сервер, на который будут отправляться сообщения в формате CEF, нажмите  **Добавить сервер** и задайте параметры:

- имя сервера;
- IP-адрес сервера и порт;
- выберите журнал для отправки CEF-сообщений.

Нажмите **Сохранить**.

Примечание. Чтобы экспортировать оба журнала на один сервер, добавьте новый сервер с такими же параметрами, но задайте другое имя сервера, как на рисунке ниже.

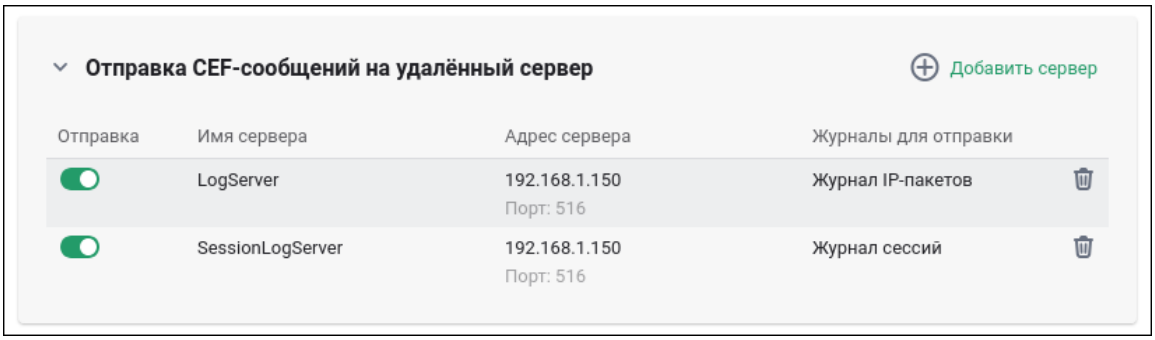


Рисунок 145. Настройка экспорта журнала IP-пакетов и журнала сессий на один сервер

5.3 Включите отправку CEF-сообщений на сервер.

5.4 Чтобы изменить параметры сервера или выбрать другой журнал для отправки, удалите сервер с помощью кнопки и добавьте новый.

5.5 Если удалённый сервер расположен в открытой сети, создайте транзитный фильтр, разрешающий исходящее соединение. При этом задайте параметры фильтра:

- **Состояние** – Включено.
- **Действие** – Пропускать трафик.
- **Источники** – Мой узел.
- **Назначения** – IP-адрес сервера.
- **Транспортные протоколы** – TCP или UDP, назначение – порт сервера.

Пример настройки показан на рисунке ниже.

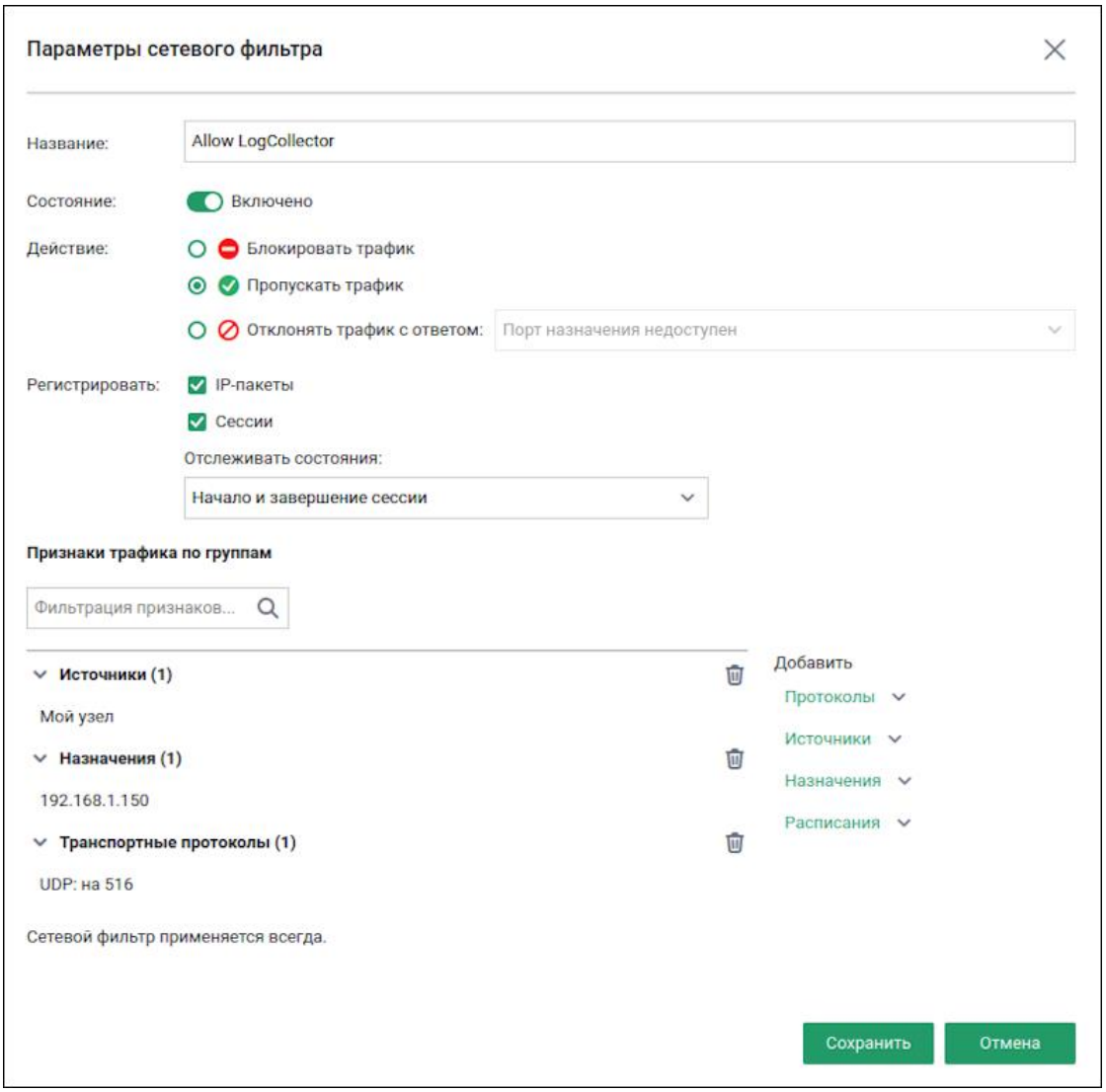


Рисунок 146. Добавление транзитного фильтра открытой сети для отправки CEF-сообщений

Журнал IP-пакетов

ViPNet Coordinator HW 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 HW.

- 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 HW версий ниже 5.3.0 и будет по умолчанию использоваться после обновления ПО с этих версий до версии 5.4.0. При этом параметр регистрации IP-пакетов в сетевых фильтрах игнорируется.

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

- Чтобы включить регистрацию IP-пакетов по фильтрам после обновления ПО ViPNet Coordinator HW с версий ниже 5.3.0 до версии 5.4.0 и выше, см. документ «Настройка с помощью командного интерпретатора», раздел «Журнал IP-пакетов».
- Чтобы включить регистрацию IP-пакетов по интерфейсам, см. Настройка журналов.

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

Примечание. Просмотр журнала IP-пакетов в кластере доступен 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, прошедших через сетевые интерфейсы за последний час.

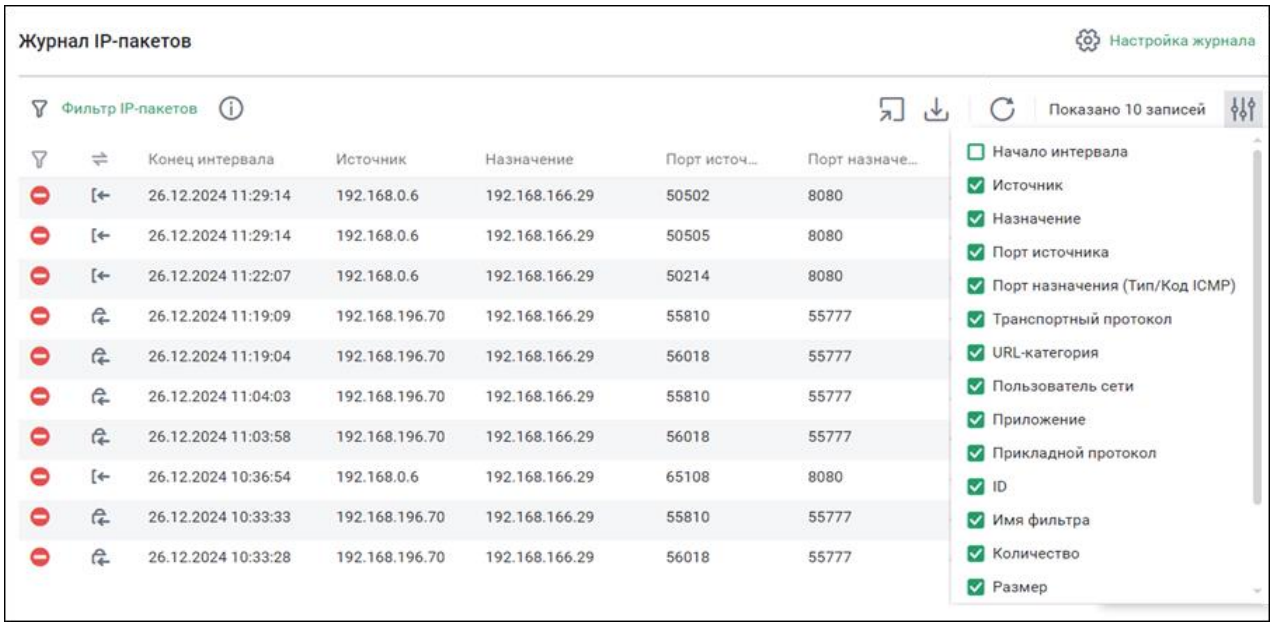


Рисунок 147. Просмотр журнала IP-пакетов

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

Примечание. Чтобы просмотреть фильтры МЭ или правила IPS, сработавшие для тех или иных событий, выберите флажок **Имя фильтра**. Если фильтр МЭ или правило IPS, сработавшее на событие, было удалено, то в столбце **Имя фильтра** вместо названия будет выведено предупреждение. При этом информация о зарегистрированном событии останется в журнале.

3 Чтобы выбрать определённые записи журнала, используйте фильтр:

3.1 Нажмите **Фильтр IP-пакетов**.

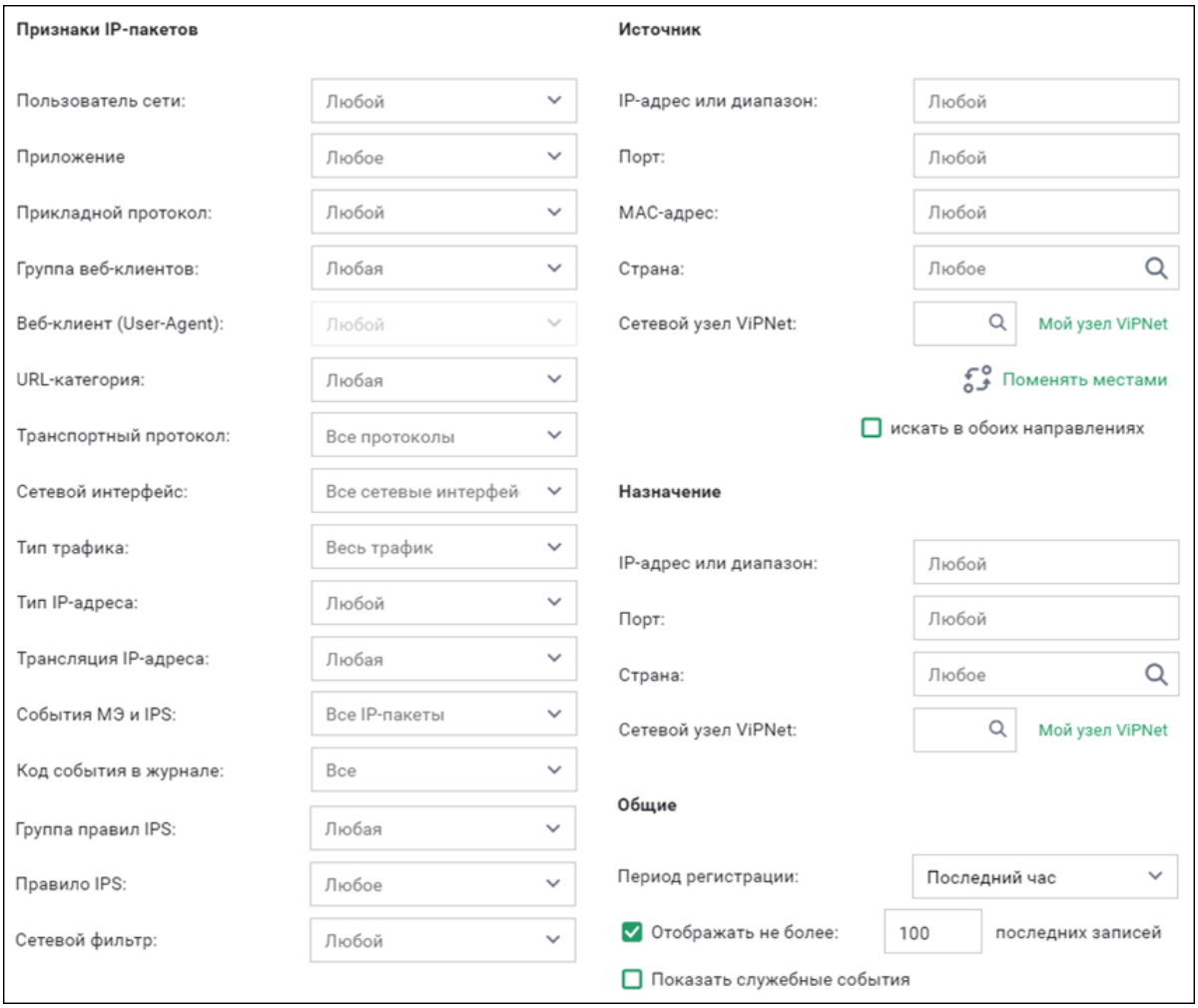


Рисунок 148. Фильтр журнала IP-пакетов

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

- пользователя Active Directory или Captive portal;
- приложение, для которого передаются IP-пакеты;
- прикладной протокол, с использованием которого передаются IP-пакеты;

> **Примечание.** Тип прикладного протокола или приложения не всегда определяется по первому IP-пакету (в зависимости от сочетания транспортного и прикладного протоколов). Например, вы создали разрешающее правило для прикладного протокола HTTP. В этом случае для разрешённого HTTP-соединения в журнале IP-пакетов будут отображаться несколько записей о пакетах с транспортным протоколом TCP и неизвестным прикладным протоколом, так как прикладной протокол еще не определён. После того, как прикладной протокол будет определён, в журнале будут отображаться записи о пакетах с транспортным протоколом TCP и прикладным протоколом HTTP.
>
> При обновлении DPI некоторые прикладные протоколы, приложения и группы приложений могут быть удалены из списка поддерживаемых. Записи в журнале IP-пакетов с такими протоколами или приложениями будут отображать в качестве имени протокола или приложения «Неизвестно/Неизвестен (ID=номер протокола или приложения)».

- группу веб-клиентов;

- для выбранной группы веб-клиентов — конкретного веб-клиента;
- URL-категорию;
- транспортный протокол, с использованием которого передаются IP-пакеты (TCP, UDP, ICMP или другой);
- сетевой интерфейс, через который проходят IP-пакеты (`eth0`, `eth1` и так далее);
- тип трафика, к которому относятся IP-пакеты (весь трафик, транзитный управляющий, транзитный открытый, локальный управляющий или локальный открытый);
- тип IP-адреса (одноадресный, широковещательный или групповой);
- трансляцию IP-адреса (выполнена, не выполнена);
- события МЭ и IPS, к которым относятся IP-пакеты (заблокированные IPS, предупреждение IPS, заблокированные МЭ, пропущенные МЭ или служебные и пр.);
- код события в журнале;
- группа правил IPS, которая срабатывает на IP-пакеты;
- правило IPS или фильтр МЭ, которые срабатывают на IP-пакеты.

3.3 В разделе **Источник** (**Назначение**) укажите:

- IP-адрес отправителя (получателя) или диапазон IP-адресов отправителей (получателей);
- номер порта отправителя (получателя);
- MAC-адрес отправителя;
- страну отправителя (получателя);
- сетевой узел ViPNet.

3.4 В разделе **Общие**:

- в поле **Период регистрации** укажите диапазон времени, за который вы хотите просмотреть информацию об IP-пакетах;
- чтобы ограничить число записей об IP-пакетах, отображаемое в результате поиска, выберите соответствующий флажок и укажите это число (максимальное число выводимых записей ограничено 1000).

3.5 Нажмите **Найти**.

4 Выполните одно из действий со списком выбранных записей:

- Щёлкните запись в списке, чтобы просмотреть подробные сведения об IP-пакете.

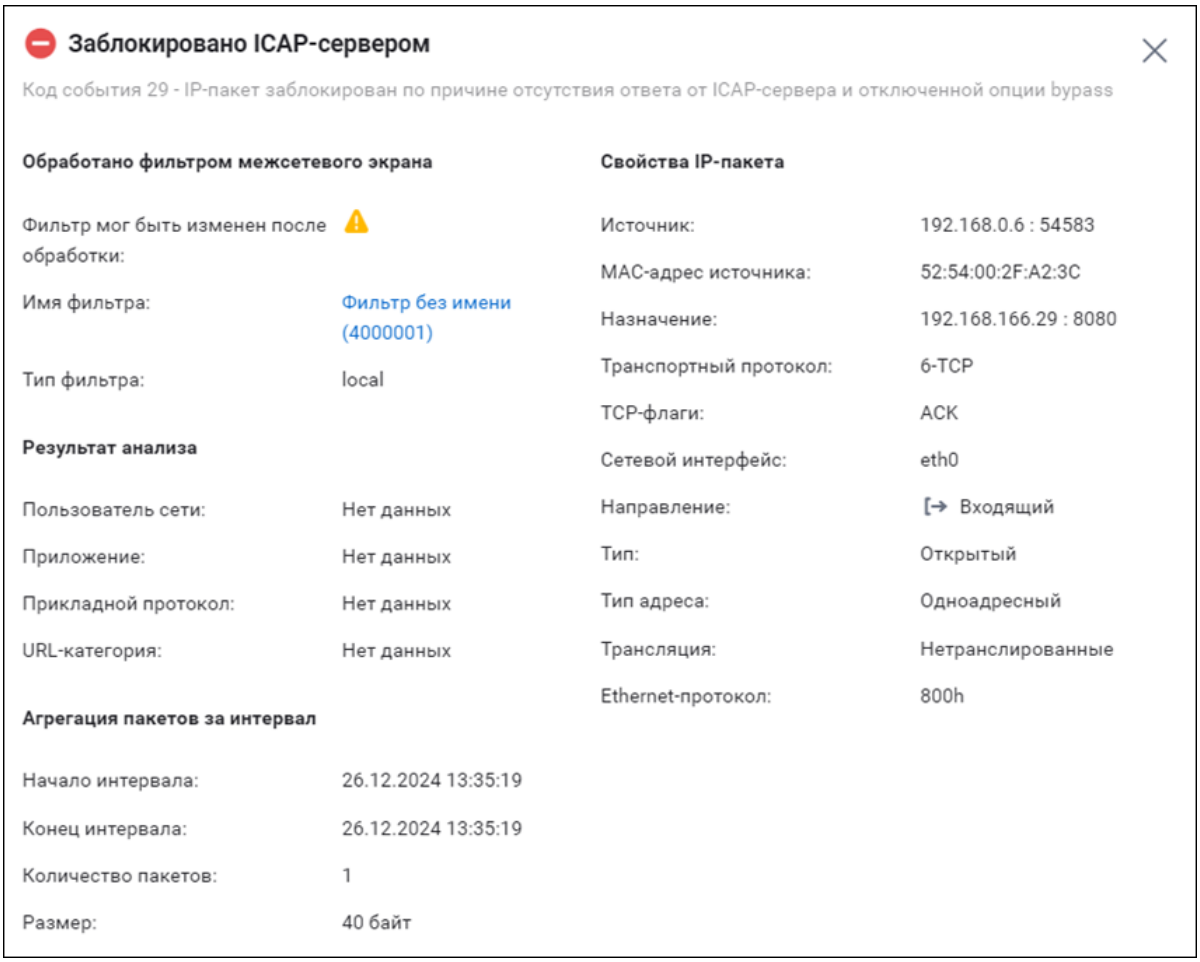


Рисунок 149. Подробные сведения об IP-пакете

Примечание. Для событий 3, 11, 30-32, 34-37, 41 60-63 в поле **Имя фильтра** указывается имя сработавшего фильтра. Для события 40 имя фильтра может отсутствовать (**Нет данных**), если причина события не связана с МЭ, например, при декапсуляции входящего зашифрованного IPlir-пакета. Для остальных событий в поле **Имя фильтра** указывается **Нет данных**.

- Нажмите , чтобы скачать файл формата *.`xls`, который содержит выбранные записи.
- Нажмите , чтобы просмотреть выбранные записи в новой вкладке браузера.

Журнал сессий

В журнале регистрируются сетевые сессии. Каждая сессия — непрерывный поток IP-пакетов между двумя сетевыми узлами, который определяется параметрами:

- адрес и порт узла–источника;
- адрес и порт узла–приемника;
- протокол уровня 3–4 OSI;
- дата и время начала сессии;
- дата и время окончания сессии (для активной сессии — не определено).

По умолчанию ведение журнала отключено. Чтобы включить его, см. Настройка журналов.

Чтобы посмотреть журнал сессий:

1 Выберите **Журналы** > **Журнал сессий**.

По умолчанию отобразятся не более 1000 записей обо всех сессиях.

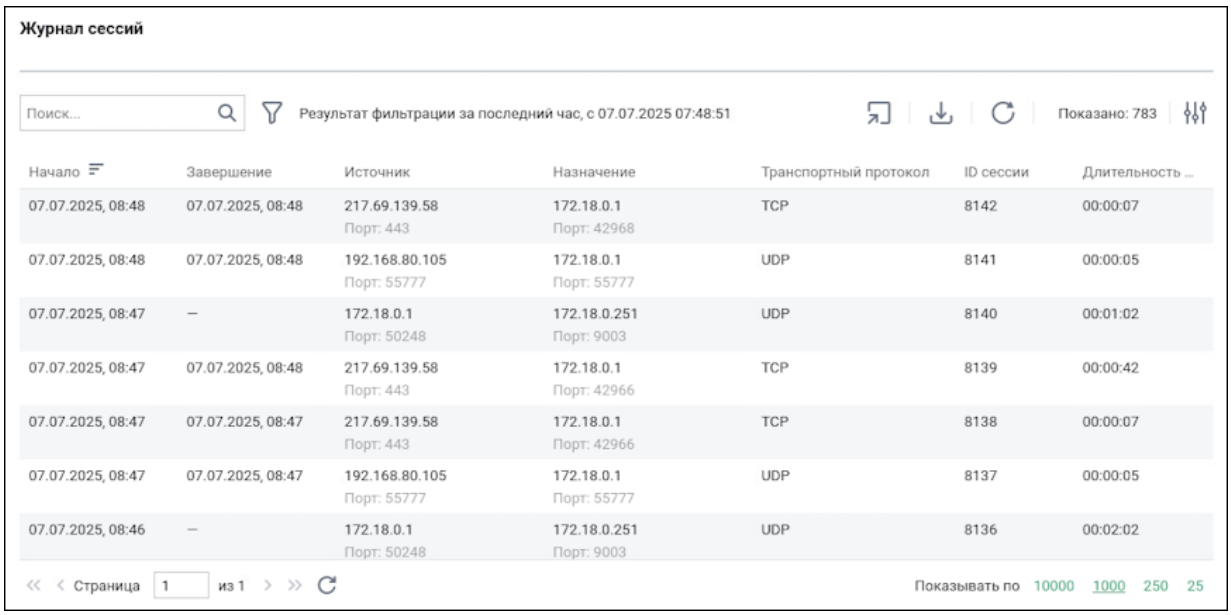


Рисунок 150. Просмотр журнала сессий

Примечание.

- В связи с особенностями реализации, в ViPNet Coordinator HW версии 5.4.2 в журнале могут дублироваться записи с одинаковым идентификатором сессии.
- Если соединение заблокировано без обработки МЭ (например, по событию 18), в столбце **Сетевой фильтр** указывается **Не применён**.

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

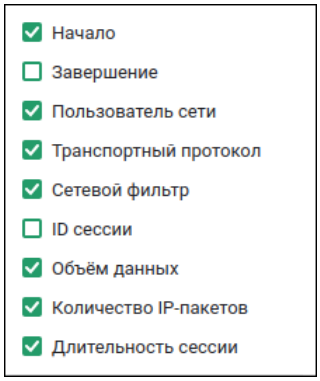


Рисунок 151. Настройка вида таблицы журнала регистрации сессий

3 Чтобы выбрать определённые записи журнала, используйте фильтр:

3.1 Нажмите **Фильтр сессий**.

3.2 В разделе **Признаки сессий** укажите:

- идентификатор сессии;
- пользователя Active Directory или Captive portal;
- транспортный протокол;
- идентификатор сетевого фильтра, срабатывание которого привело к регистрации сессии;
- событие сессии;
- признак трансляции IP-адреса;
- объём отправленных и полученных данных в рамках сессии (в мегабайтах);
- количество отправленных и полученных IP-пакетов.

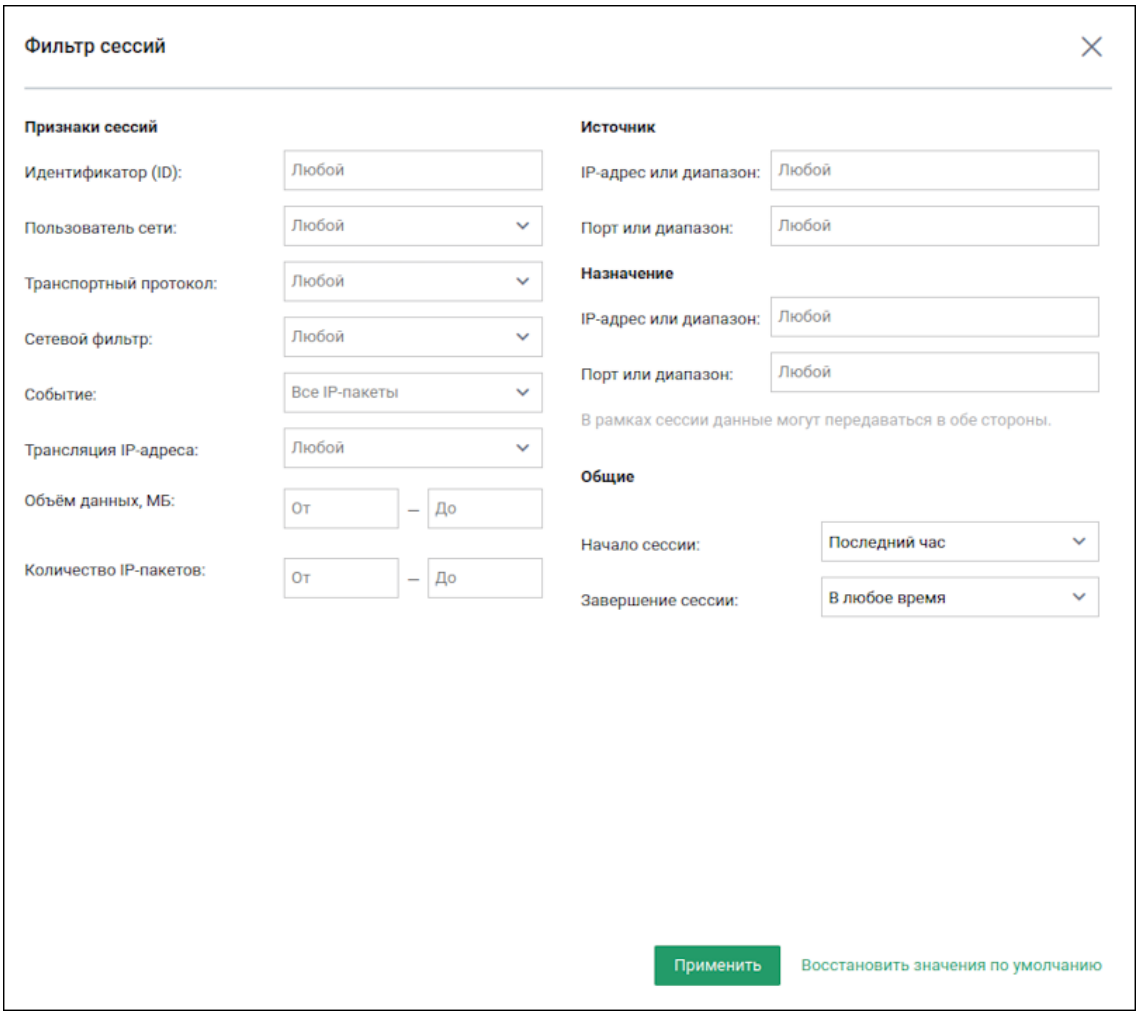


Рисунок 152. Настройка фильтра журнала сессий

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

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

В рамках сессии данные могут передаваться в обе стороны. Адрес и порт инициатора сессии указывайте в разделе **Источник**.

3.4 В разделе **Общие** укажите время начала и завершения сессии.

3.5 Нажмите **Применить**.

4 Вы можете ограничить количество отображаемых на странице записей. Для этого выберите количество в разделе **Показывать по** справа снизу.

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 или журнала сессий по сети в формате CEF».

---

5 Выполните одно из действий со списком выбранных записей:

5.1 Для просмотра подробной информации о сессии выберите запись в списке.



Примечание. При анализе записей журнала важно учитывать, что если в сетевом фильтре, срабатывание которого привело к регистрации сессии, не включена регистрация завершения сессии, фактическая её длительность не может быть установлена.

5.2 Для скачивания списка выбранных записей в формате `*.csv` нажмите  .

5.3 Для просмотра списка выбранных записей в новой вкладке браузера нажмите  .

Журнал аудита

В журнале аудита регистрируются события, связанные с выполнением запросов пользователей, в том числе от ViPNet Prime и служебных запросов ViPNet Coordinator HW. 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.

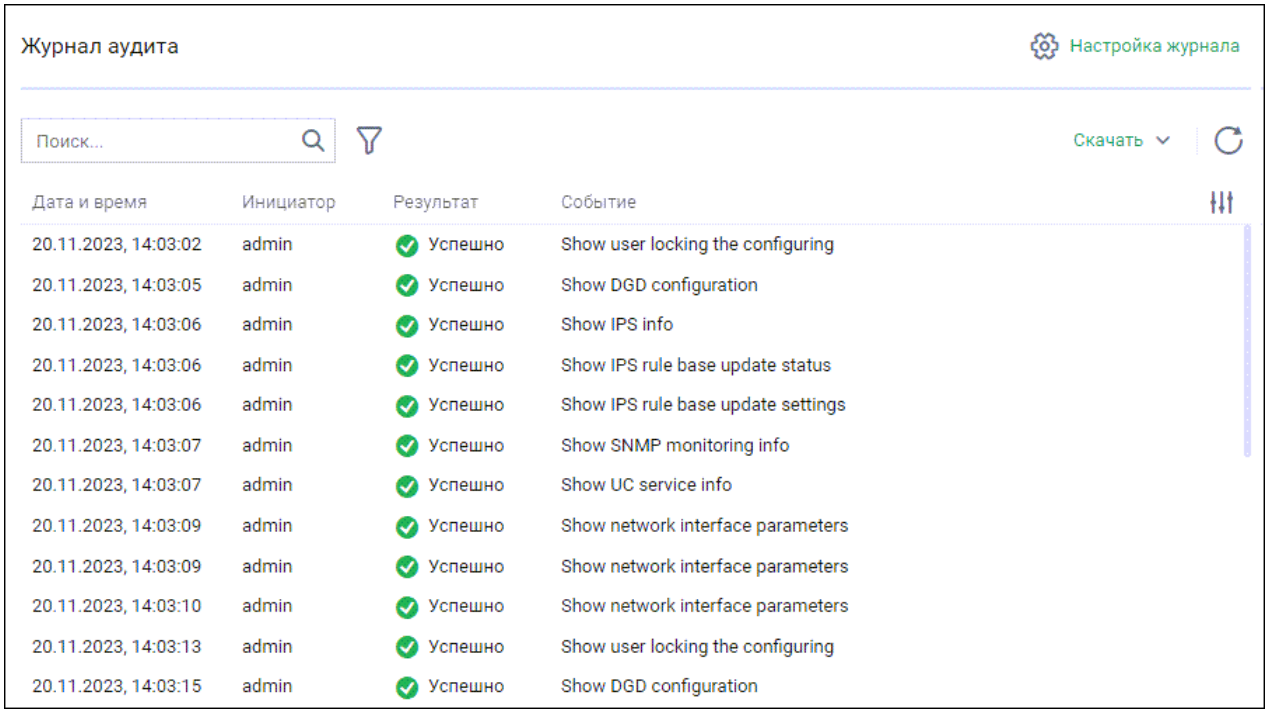


Рисунок 153. Просмотр журнала аудита

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.

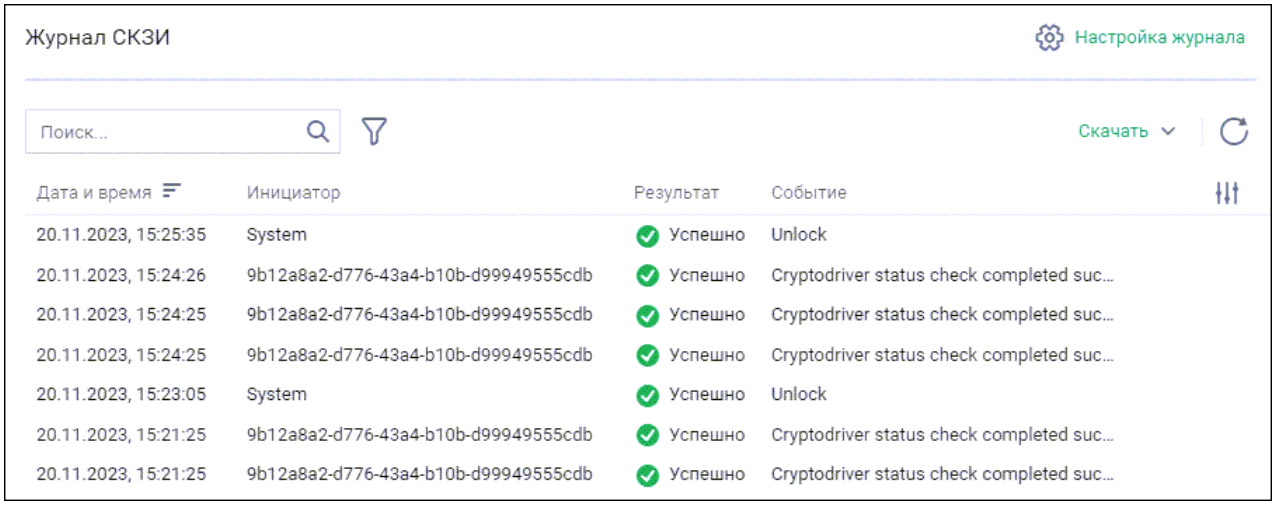


Рисунок 154. Просмотр журнала СКЗИ

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 HW, выберите **Скачать** > **Скачать с очисткой журнала**.

Файл журнала будет сохранён в папке загрузки вашего компьютера, а все записи журнала на ViPNet Coordinator HW 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:

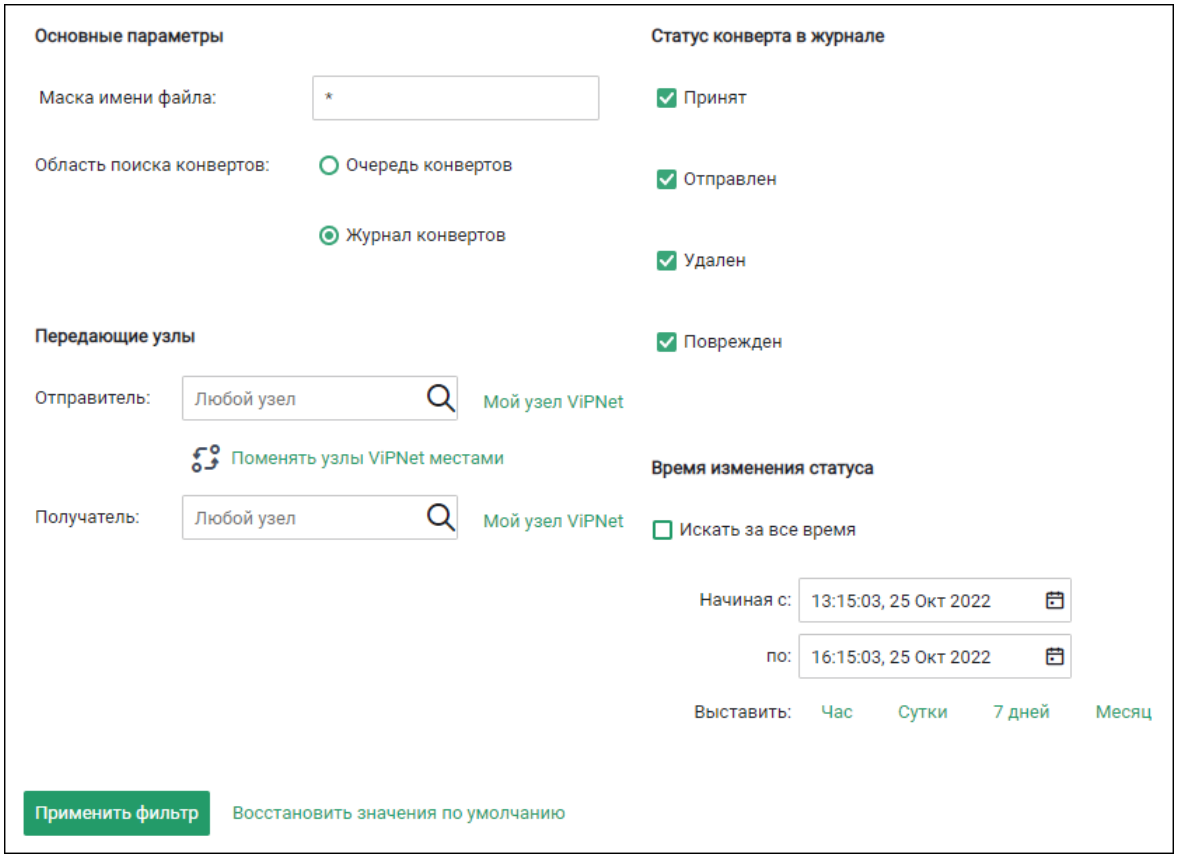


Рисунок 155. Настройка параметров журнала MFTP

- Настройте **Основные параметры**:
  - Область поиска конвертов — очередь конвертов или журнал конвертов.
  - Маску имени файла. По умолчанию задана маска `*` для поиска всех файлов.
- В разделе **Передающие узлы** укажите сетевые узлы ViPNet в качестве отправителя и получателя транспортных конвертов.

- Укажите сетевой узел ViPNet Coordinator HW в качестве отправителя, либо в качестве получателя транспортных конвертов.

Совет. В разделе **Передающие узлы**:

- Чтобы указать идентификатор сетевого узла, нажмите  , и выберите нужный узел в списке. Чтобы указать собственный сетевой узел, нажмите **Мой узел ViPNet**.
- Вы можете поменять местами сетевые узлы отправителей и получателей.

- В разделе **Состояние конверта в очереди** или **Статус конверта в журнале** (в зависимости от выбранной области поиска конвертов) выберите состояния транспортных конвертов, информацию о которых вы хотите просмотреть.
- 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 HW:

- 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.

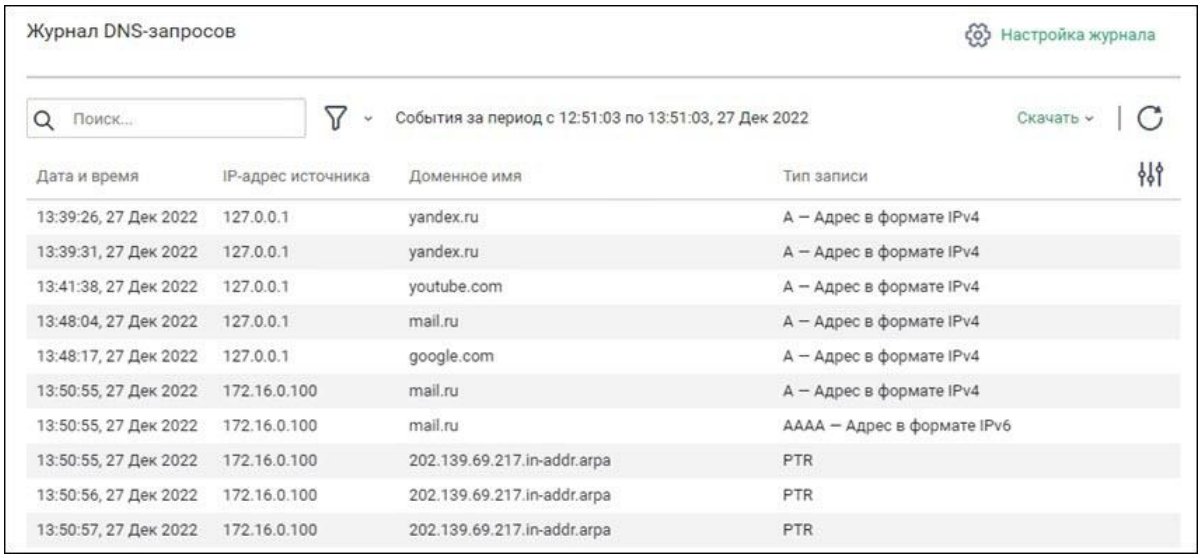


Рисунок 156. Просмотр журнала DNS-запросов

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 ведется локально или удаленно, файлы журнала ротируются.

Чтобы просмотреть системный журнал:

1 Выберите **Журналы** > **Системный журнал**.

По умолчанию заданы параметры для просмотра записей всех служб.

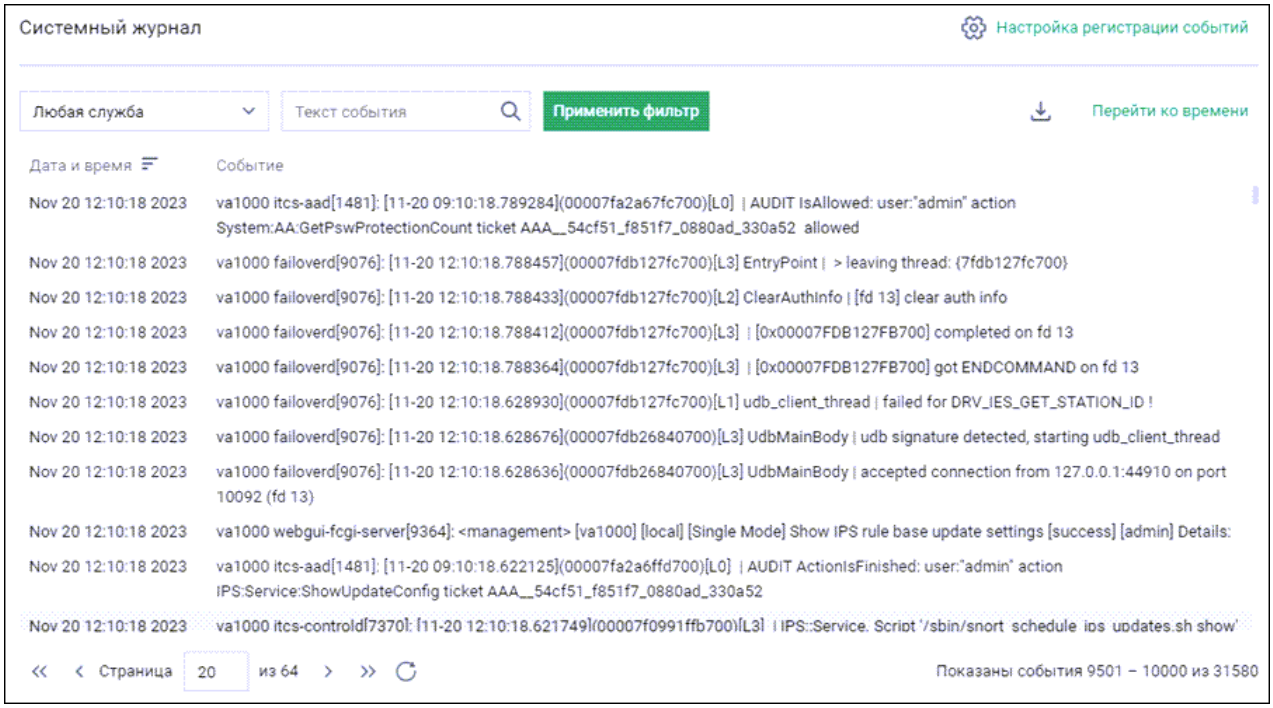


Рисунок 157. Просмотр системного журнала

2 Чтобы просмотреть записи определенной службы, выберите ее из списка и нажмите **Применить фильтр**.

3 Чтобы просмотреть записи с определенным текстом, введите его в поле **Текст события** и нажмите **Применить фильтр**.

4 Чтобы просмотреть записи с определенного момента времени, нажмите **Перейти ко времени**, выберите дату и время в календаре, затем нажмите **Перейти**.

5 Для служб IPS, идентификации пользователей, DGD и SNMP вы можете изменить уровень важности событий, регистрируемых в журнале:

5.1 Нажмите **Настройка регистрации событий**.

5.2 Выберите уровни важности.

5.3 Нажмите **Сохранить**.

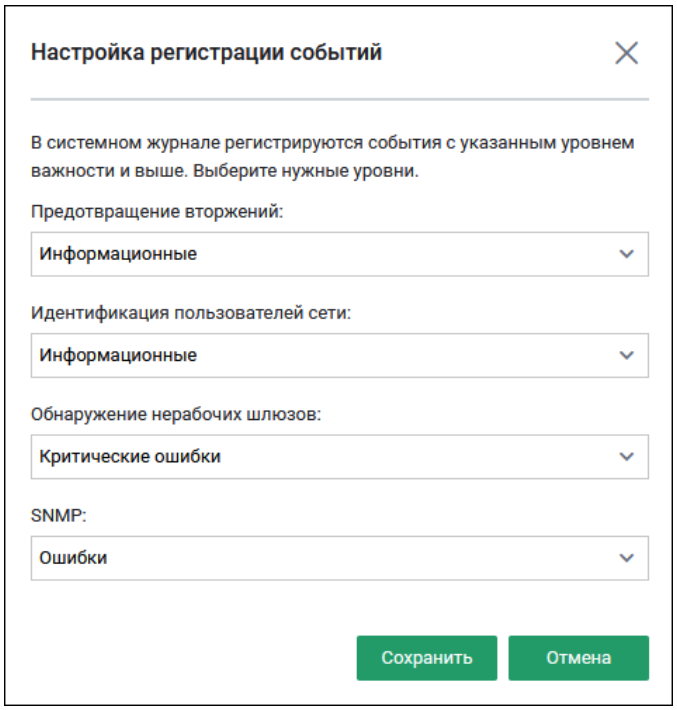


Рисунок 158. Настройка регистрации событий

6 Чтобы скачать файл архива системного журнала:

6.1 Нажмите .

6.2 Выберите степень сжатия архива: без сжатия, минимальное, среднее или максимальное.

6.3 По умолчанию, в архив добавляются ротированные файлы журнала. Если добавлять файлы не нужно, снимите флажок **Включить в архив ротированные файлы журнала**.

6.4 Нажмите **Скачать**.

Файл архива журнала в формате `<имя узла>-logs_DD-MM-YYYYTHH_MM.zip` будет сохранен в папке вашего компьютера.

12

Мониторинг работы

Просмотр состояния 257

Мониторинг по SNMP 258

Просмотр статистики передачи данных 271

Просмотр статистики IP-пакетов 272

Просмотр состояния

Вы можете следить за состоянием ViPNet Coordinator HW в режиме реального времени: состоянием служб, загрузкой процессора, использованием оперативной памяти и дискового пространства.

Чтобы просмотреть информацию о текущем состоянии ViPNet Coordinator HW, выберите **Состояние системы**.

Примечание. При остановленной службе системы защиты от сбоев **Failover** информация о состоянии системы не отображается.

Графики загрузки процессора и использования оперативной памяти в кластере отображаются только для активного узла.

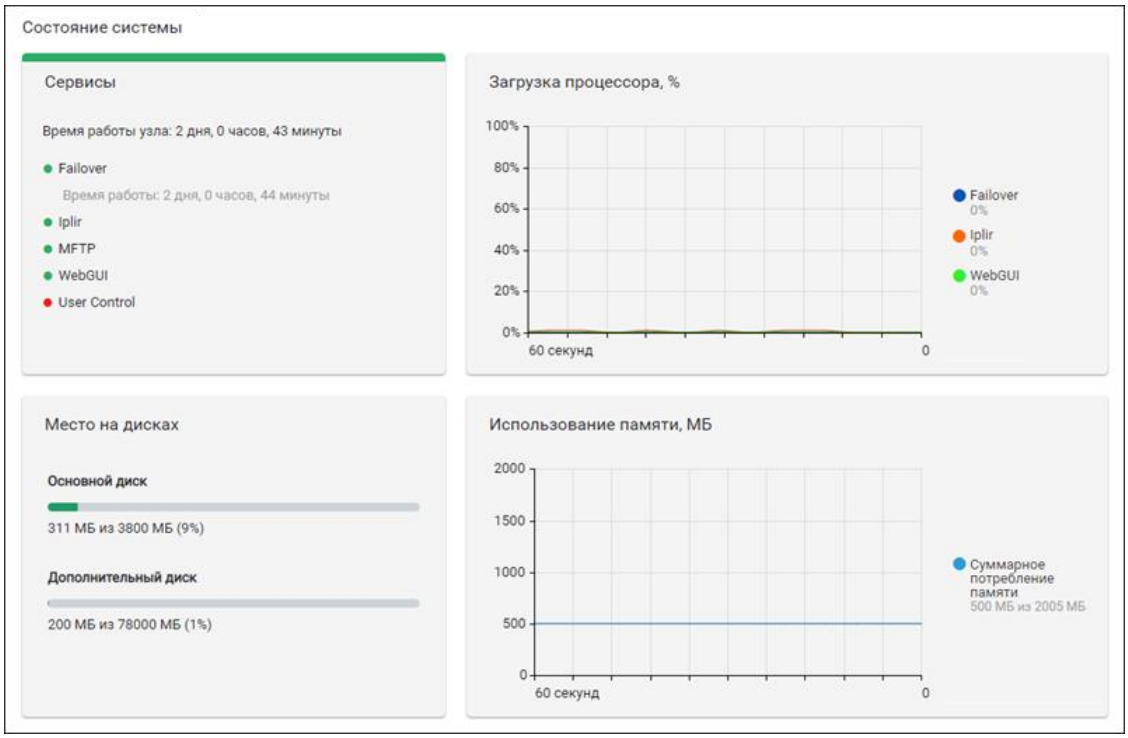


Рисунок 159. Просмотр состояния ViPNet Coordinator HW

Мониторинг по SNMP

С помощью SNMP-агента, входящего в состав ПО ViPNet Coordinator HW, вы можете удалённо получать информацию о работе ViPNet Coordinator HW, 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 HW вы можете просмотреть в приложении Базы управляющей информации (MIB) для протокола SNMP. Все SNMP-параметры доступны только для чтения.

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

- ViPNet 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 узел защищённой сети или туннелируемый узел. Если вы будете использовать открытый узел, добавьте сетевые фильтры, разрешающие локальный SNMP-трафик:

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

Протокол SNMP поддерживает следующие способы получения информации:

- Передача параметров по запросу — сервер мониторинга посылает SNMP-запрос на ViPNet Coordinator HW и получает в ответ значения необходимых параметров.
- Передача уведомлений — SNMP-агент ViPNet Coordinator HW 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 HW, который доступен с сервера мониторинга по кратчайшему маршруту.

Если вы включили передачу SNMP-уведомлений, то после включения или перезагрузки ViPNet Coordinator HW 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 систему мониторинга MIB-файлы, поддерживаемые ViPNet Coordinator HW, вы сможете:

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

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

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

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

  Для получения SNMP-уведомлений сервером мониторинга в настройках его SNMP-менеджера, а также в настройках ViPNet Coordinator HW, необходимо задать community для уведомлений.
- В SNMPv3 создаются учётные записи пользователей SNMP. ViPNet Coordinator HW ответит на SNMP-запрос, если данные пользователя в запросе совпадают с данными любого из пользователей, заданных на ViPNet Coordinator HW:
  - имя пользователя;
  - пароль пользователя и алгоритм хэширования пароля;
  - 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 HW. 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



Внимание! Рекомендуется настраивать SNMP-агент в выключенном состоянии, иначе при задании большого количества параметров увеличится время перезапуска службы SNMP-агента.

По умолчанию SNMP-агент выключен.

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

На странице отображаются текущие настройки SNMP-агента.

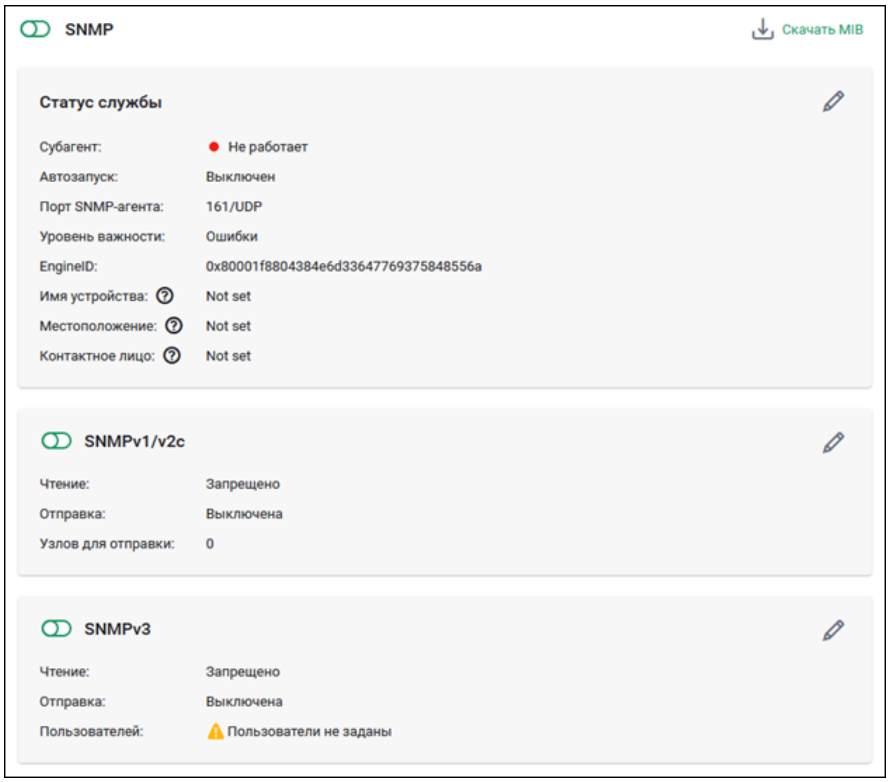


Рисунок 160. Настройка мониторинга по протоколу SNMP

2 Чтобы настроить основные параметры SNMP-агента, нажмите  в разделе **Статус службы**.

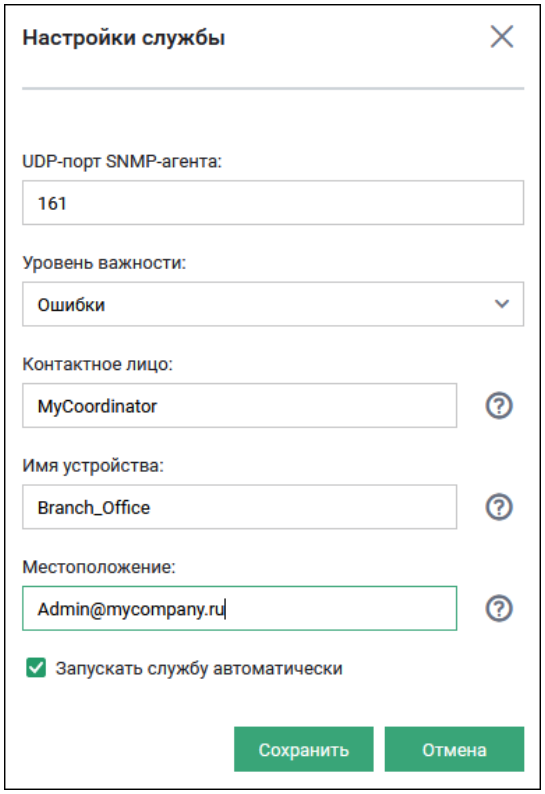


Рисунок 161. Настройка службы SNMP

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 HW, 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 HW, выберите **Запускать службу автоматически**.

3 Для настройки параметров протоколов SNMPv1 и SNMPv2c нажмите  в разделе **SNMPv1/v2c**.

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

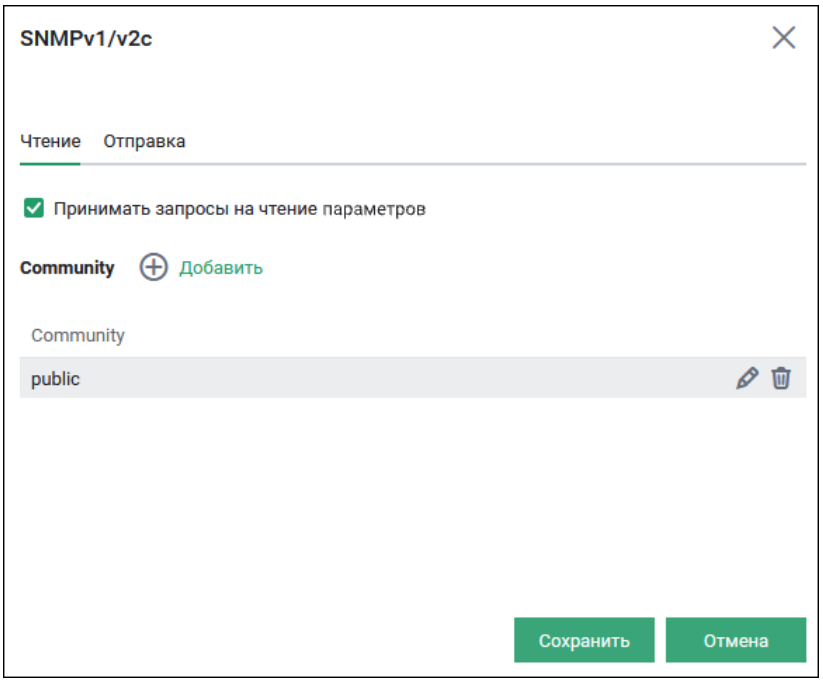


Рисунок 162. Настройка чтения SNMP-параметров

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, 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.

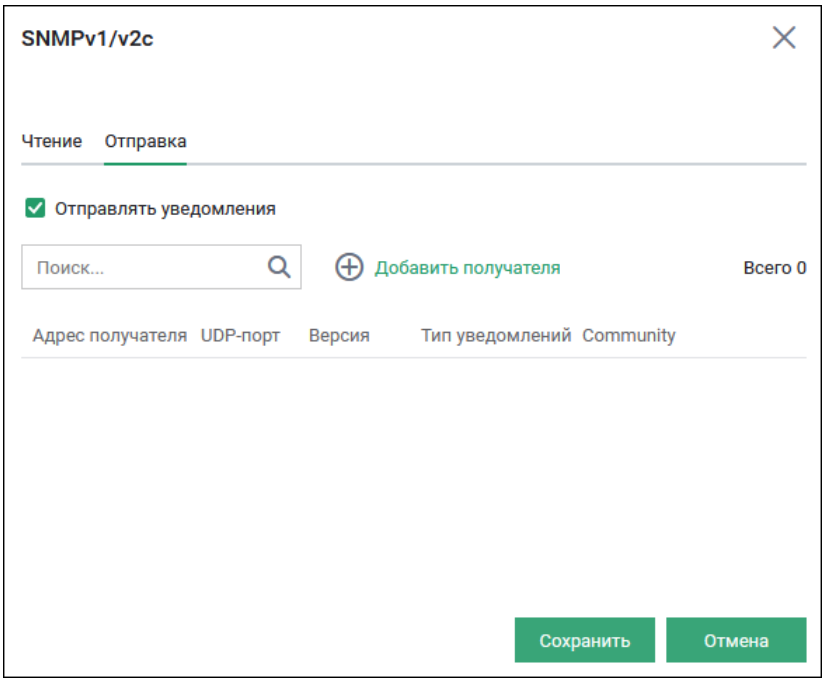


Рисунок 163. Настройка отправки SNMP-уведомлений

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.

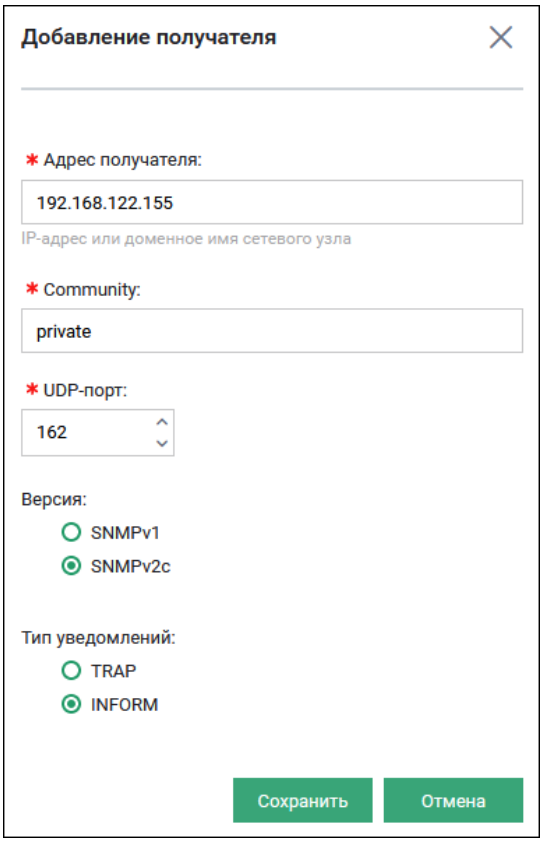


Рисунок 164. Добавление узла для отправки уведомлений в SNMP v1 и v2c

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 **SNMPv1/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:

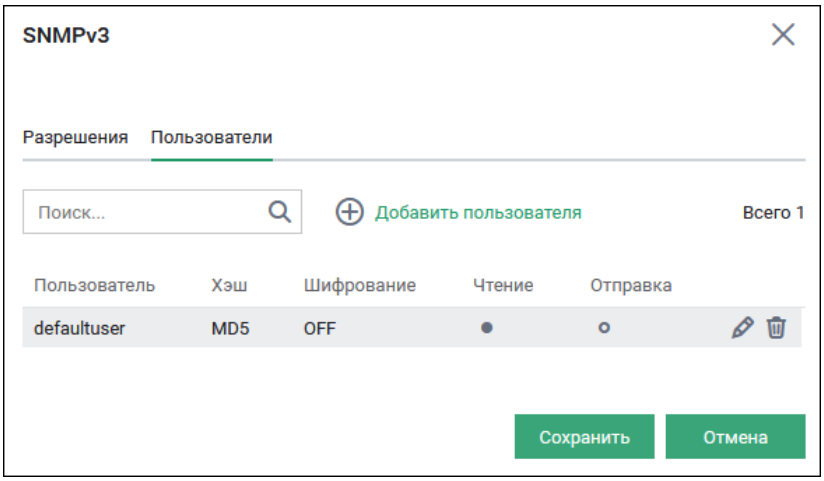


Рисунок 165. Настройка протокола SNMPv3

- Чтобы добавить пользователя для чтения SNMP-параметров, 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:

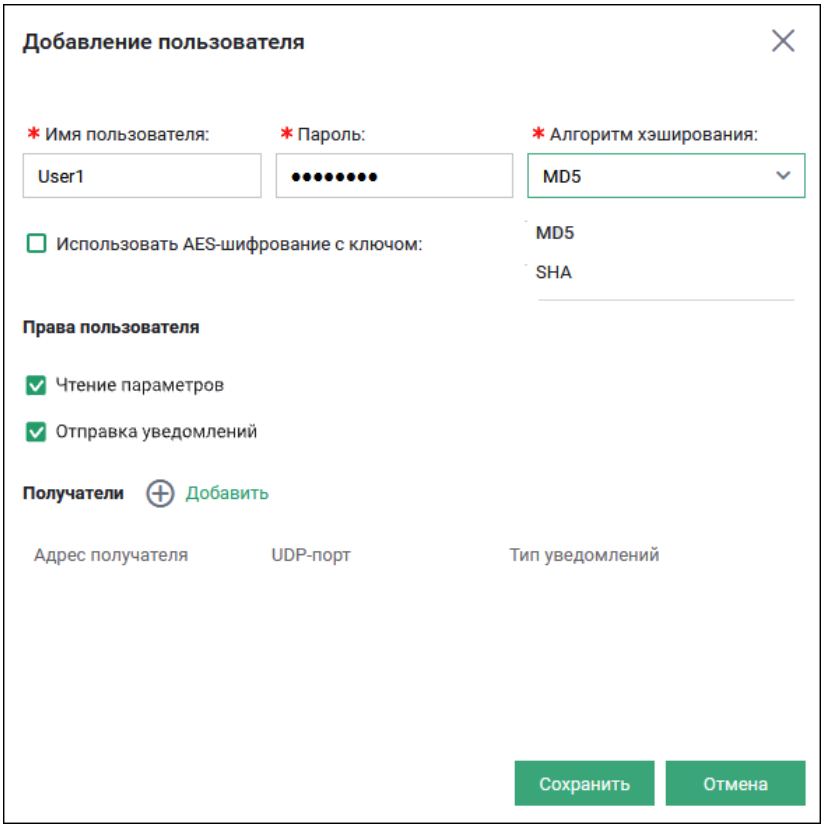


Рисунок 166. Добавление пользователя для чтения SNMP-параметров

- 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 HW, 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:

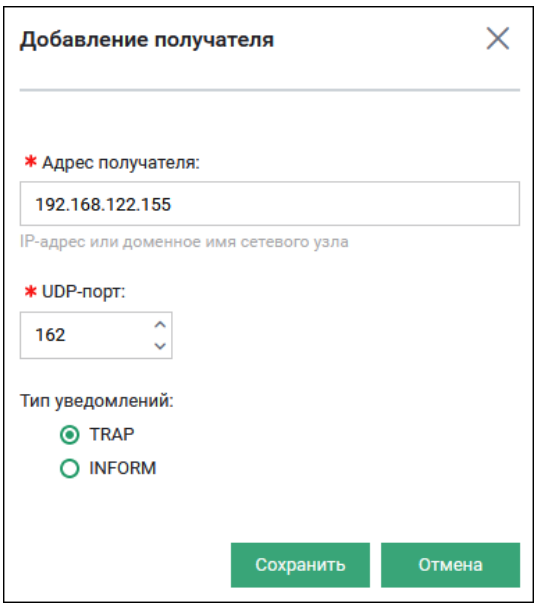


Рисунок 167. Добавление узла для отправки уведомлений в SNMP3

- 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.

Для уведомлений типа INFORM сервер мониторинга должен быть доступен при каждом запуске службы SNMP-агента, иначе SNMP-агент будет недоступен около минуты после каждой отправки оповещения.

- Тип уведомлений.

4.6 Включите **SNMPv3**.

5 Включите **SNMP**.

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

Мониторинг кластера

Вы можете следить за состоянием обоих узлов кластера по протоколу SNMP. При этом только активный узел кластера принимает SNMP-запросы и отправляет SNMP-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 HW кластера создаётся community для режима кластера. SNMP-запрос с таким community будет адресован конкретному ViPNet Coordinator HW независимо от его текущего режима работы в кластере (активный или пассивный). При переключении системы защиты от сбоев в одиночный режим, community для режима кластера автоматически удаляется.
- При использовании SNMPv3 каждому узлу кластера назначается свой контекст (строка, идентифицирующая ViPNet Coordinator HW в кластере). Контексты создаются автоматически на активном узле в формате `Node<порядковый номер>`, где `<порядковый номер>` — число от 1, которое выбирается по возрастанию в соответствии с IP-адресом интерфейса синхронизации.

Для мониторинга кластера по протоколу SNMP:

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

Настройки будут переданы на пассивный узел при последующей синхронизации.

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

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

2.1 Выберите вкладку **Мониторинг узлов кластера**.

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

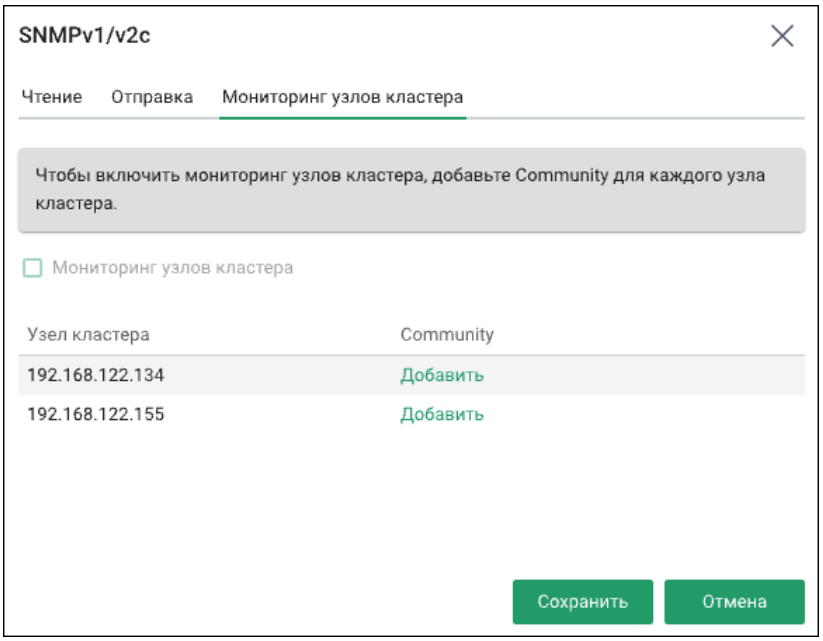


Рисунок 168. Настройка чтения SNMP-параметров в кластере

2.3 Введите community, отличное от других.

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

2.4 Чтобы разрешить чтение SNMP-параметров узлов кластера, выберите **Мониторинг узлов кластера**.

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

3.1 Выберите вкладку **Контексты кластера**.

3.2 Если требуется изменить контексты узлов кластера, наведите 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.

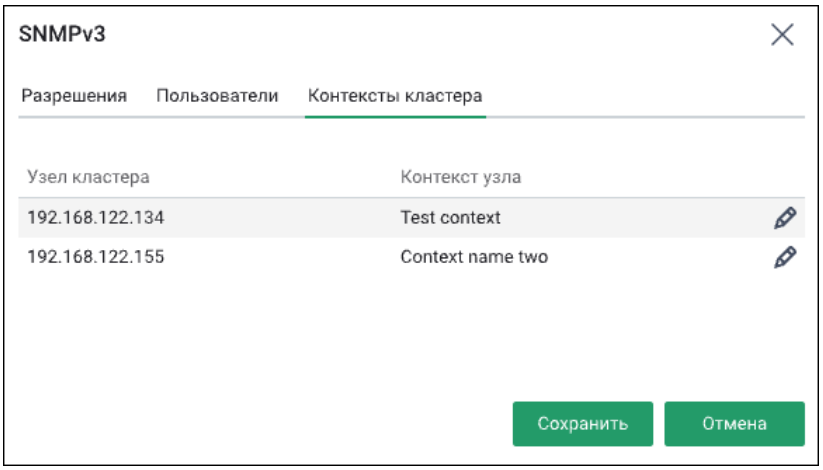


Рисунок 169. Просмотр контекстов для узлов кластера

4 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.

Мониторинг ViPNet-узлов

Чтобы обнаруживать потерю связи ViPNet Coordinator HW с другими узлами ViPNet, настройте автоматическую отправку SNMP-оповещений о доступности узлов ViPNet на сервер мониторинга:

1 Настройте SNMP-агент (см. Настройка SNMP-агента).

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

3 Щелкните нужный узел в списке.

4 В разделе **Общая информация** включите **Мониторинг по SNMP**.

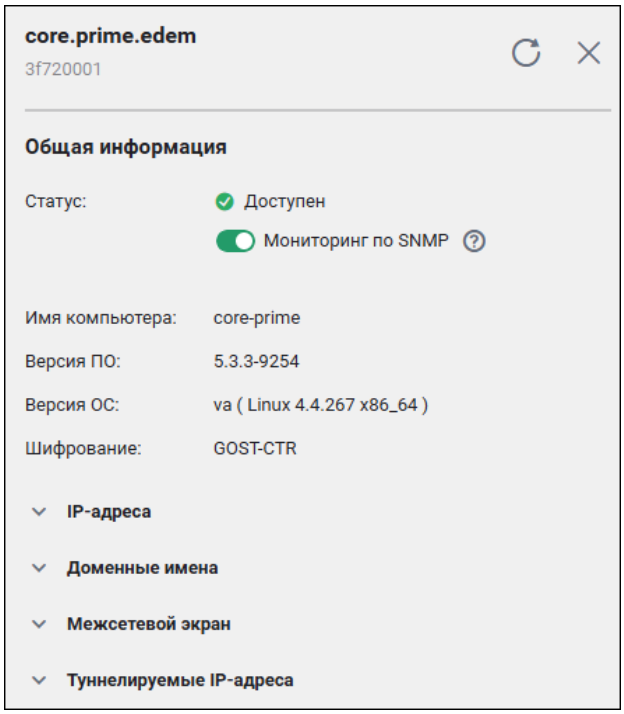


Рисунок 170. Настройка мониторинга узла

Чтобы включить автоматическую отправку SNMP-оповещений сразу для нескольких узлов:

1 Выберите эти узлы с помощью флажков.

2 Выберите **Мониторинг по SNMP** > **Включить**.

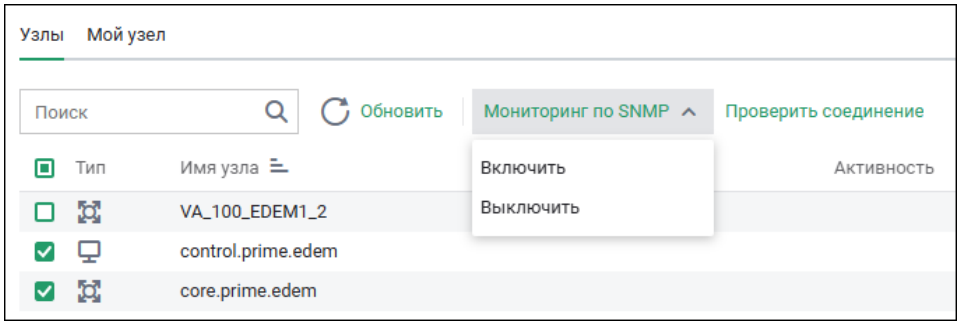


Рисунок 171. Настройка мониторинга группы узлов

Просмотр статистики передачи данных

Статистика передачи данных ведется раздельно по всем интерфейсам с момента включения ViPNet Coordinator HW. Статистика учитывает текущую скорость интерфейсов и объем трафика. Данные статистики отображаются в виде графика скорости и диаграммы объема трафика с заданным интервалом обновления (по умолчанию — 3 сек.). Значения скорости отображаются в диапазоне 600 сек. от начала просмотра статистики. Для кластера отображается статистика интерфейсов активного узла. После перезагрузки ViPNet Coordinator HW или удаления интерфейса данные статистики сбрасываются. Для ViPNet Coordinator VA статистика может быть сброшена после перезапуска интерфейса.

Чтобы просмотреть статистику передачи данных:

1 Выберите **Статистика**.

По умолчанию в разделе **Передача данных** отображается статистика интерфейса `eth0`.

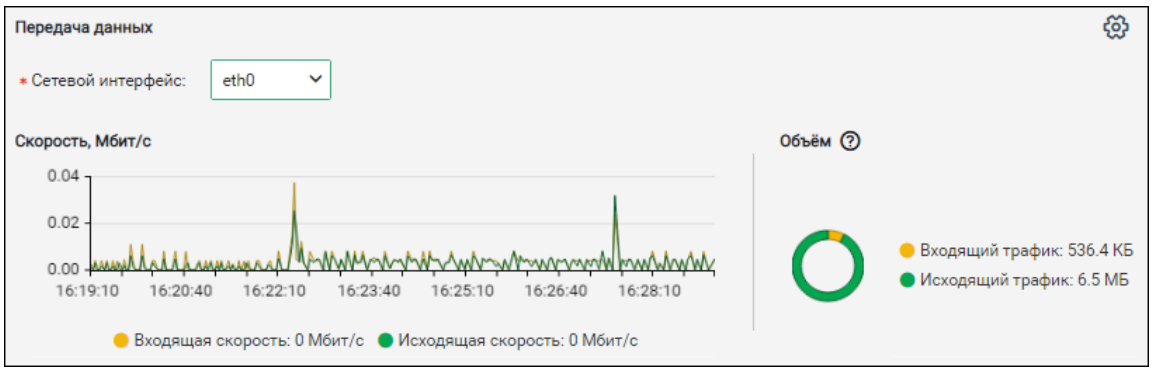


Рисунок 172. Статистика передачи данных сетевого интерфейса eth0

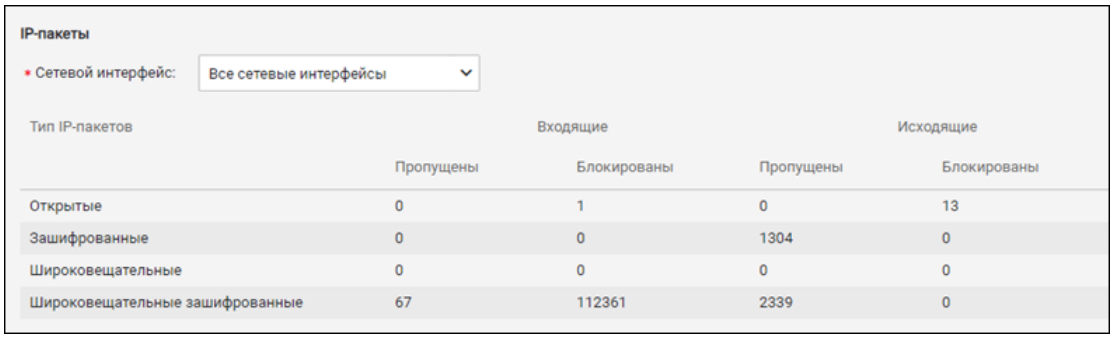
2 Вы можете переключаться между интерфейсами, выбирая нужный из списка **Сетевой интерфейс**.

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.



Тип IP-пакетов	Входящие		Исходящие	
	Пропущены	Блокированы	Пропущены	Блокированы
Открытые	0	1	0	13
Зашифрованные	0	0	1304	0
Широковещательные	0	0	0	0
Широковещательные зашифрованные	67	112361	2339	0

Рисунок 173. Просмотр информации о количестве IP-пакетов, прошедших через все сетевые интерфейсы ViPNet Coordinator HW

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

A

Сетевые фильтры по умолчанию

Таблица 15. Фильтры защищенной сети (vpn)

Название	Источник	Назначение	Протокол	Действие
Служебные фильтры в режиме кластера				
ViPNet Service in	@any	@local	udp: from 2060 to 2060	pass
ViPNet Service out	@local	@any	udp: from 2060 to 2060	pass
Служебные фильтры				
Block not original udp port	@local	@any	udp: from 0-2045, 2047-63536 to 2046	drop
Allow ViPNet base services in	@any	@local	udp: to 2046, from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet base services out	@local	@any	udp: to 2046, from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet MFTP in	@any	@local	tcp: from 5000-5003	pass
Allow ViPNet MFTP out	@local	@any	tcp: from 5000-5003	pass
Allow ViPNet Control services in	ViPNet ID Prime	@local	@any	pass
Allow ViPNet Control services out	@local	ViPNet ID Prime	@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: from 2047	pass
Allow ViPNet DBViewer out	@local	@any	tcp: from 2047	pass
Allow DNS client	@local	@any	tcp/udp: from 53	pass
Allow DNS server	@any	@local	tcp/udp: from 53	pass
Allow NTP client	@local	@any	udp: from 123	pass
Allow NTP server	@any	@local	udp: from 123	pass
Allow DHCP client req	@local	@any	udp: to 68 from 67	pass
Allow DHCP client resp	@any	@local	udp: to 67 from 68	pass
Allow DHCP server req	@local	@any	udp: to 67 from 68	pass
Allow DHCP server resp	@any	@local	udp: to 68 from 67	pass
Allow DHCP-Relay service in	@any	@local	udp: to 67 from 67	pass
Allow DHCP-Relay service out	@local	@any	udp: to 67 from 67	pass
Allow SSH client	@local	@any	tcp: from 22	pass
Allow syslog outgoing	@local	@any	udp: from 514	pass
Allow cef outgoing	@local	@any	udp: from 5001	pass
Allow SNMP	@any	@local	udp: from 161	pass
Allow SNMP traps	@local	@any	udp: from 162	pass
Allow UPS service in (только для аппаратных платформ)	@any	@local	tcp: from 3493	pass
Allow UPS service out (только для аппаратных платформ)	@local	@any	tcp: from 3493	pass
Служебный фильтр по умолчанию				
Default VPN rule	@any	@any	@any	drop

Таблица 16. 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
Служебный фильтр по умолчанию				
Default tunnel rule	@any	@any	@any	drop

Таблица 17. Локальные фильтры открытой сети (`local`)

Название	Источник	Назначение	Протокол	Действие
Служебные фильтры в режиме кластера				
Failover test IP	@local	<список значений параметров `testip` из `failover.ini`>	icmp	pass
Failover Channel	@local	interface <имя интерфейса синхронизации>	@any	pass
Failover Channel	<IP-адрес интерфейса синхронизации второго узла кластера>	interface <имя интерфейса синхронизации>	@any	pass
Служебные фильтры				
ViPNet Service Common In	@any	@local	tcp/udp: to 2046, 2047, 10096, 5100, 10092	drop
ViPNet Service Common Out	@local	@any	tcp/udp: from 2046	drop
Настраиваемые фильтры				
ICMP redirect in	@any	@local	icmp:5	drop
ICMP redirect out	@local	@any	icmp:5	drop
Block ICMP timestamp response	@local	@any	icmp:14	drop
Allow ICMP Ping	@local	@any	icmp: 8	pass

Allow DNS	@local	@any	tcp/udp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Allow DHCP service req	@any	@local	udp: from 67 to 68	pass
Allow DHCP service resp	@local	@any	udp: from 68 to 67	pass
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 ICMP blackhole response	@local	@any	icmp type 3 code 4	pass
Служебный фильтр по умолчанию				
Default local rule	@any	@any	@any	drop

Таблица 18. Транзитные фильтры открытой сети (`forward`)

Название	Источник	Назначение	Протокол	Действие
Служебный фильтр по умолчанию				
Default transit rule	@any	@any	@any	drop

B

Группы объектов «Протоколы» по умолчанию

Таблица 19. Состав групп объектов «Протоколы»

Имя группы протоколов	Состав группы протоколов
DHCP	UDP:from 67-68 to 67-68
CITRIX	TCP:to 1494
DNS	UDP:to 53
FTP	TCP:to 21
GRE	IP:47
H323	TCP:to 1720
HTTP	TCP:to 80, TCP:to 8080
HTTP-Proxy	TCP:to 3128
HTTPS	TCP:to 443
IGMP	IP:2
IKE	UDP:to 500
IMAP	TCP:to 143
IPSecESP	IP:50
Kerberos	TCP:to 88, TCP:to 749, UDP:to 88, UDP:to 749
L2TP	UDP:to 1701
LDAP	TCP:to 389, UDP:to 389

LotusNotes	TCP:to 1352
MS-SQL	TCP:to 1433-1434, UDP:to 1433-1434
MySQL	TCP:to 3306
NetBIOS-DGM	UDP:from 138 to 138
NetBIOS-NC	UDP:from 137 to 137
NetMeeting	TCP:to 1503
NTP	UDP:to 123
PING	ICMP:8
POP3	TCP:to 110
Postgres	TCP:to 5432
PPTP	TCP:to 1723
RADIUS	UDP:to 1812-1813
RDP	TCP:to 3389
RTSP	TCP:to 554
SCCP	TCP:to 2000
SIP	TCP:to 5060, UDP:to 5060
SMTP	TCP:to 25
SNMP	UDP:to 161
SNMP-Traps	UDP:to 162
SSH	TCP:to 22
Syslog	UDP:to 514
Telnet	TCP:to 23
TFTP	UDP:to 69
UPnP	TCP:to 1900, TCP:to 2869, UDP:to 1900, UDP:to 2869
MFTP	TCP:to 5000-5003
SMCMonitoring	TCP:to 2047, TCP:to 5100, TCP:to 10092
VPNBase	UDP:to 2046, UDP:from 2048 to 2048, UDP:from 2050 to 2050
Cluster	UDP:from 2060 to 2060
ClusterMonitoring	UDP:from 2060 to 2065, UDP:from 2065 to 2060
VNC	TCP:to 5900
OSPF	IP:89

C

База URL-категорий

Таблица 20. Описание URL-категорий

Обозначение	Название	Описание
Advertisements and Pop-Ups	Реклама и всплывающие окна	Сайты, содержащие графическую рекламу (баннеры, всплывающие окна и прочее).
Alcohol and Tobacco	Алкоголь и табак	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции.
Anonymizers	Анонимайзеры	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхода средств веб-фильтрации и т.д.
Arts	Искусство	Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т.д.
Botnets	Ботнеты	Сайты, которые управляют сетями ботов через командно-контрольные центры.
Business	Бизнес	К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах, необходимых предприятиям любого размера для успешной деятельности.
Chat	Чаты	Сайты, позволяющие осуществлять общение в режиме реального времени.

Обозначение	Название	Описание
Child Abuse Images	Жестокое обращение с детьми	Сайты, содержащие фотографии, иллюстрирующие случаи жестокого обращения с детьми.
Compromised	Заражённые сайты	Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ без ведома владельцев. В категорию также входят ресурсы из группы высокого риска заражения.
Computers and Technology	Компьютеры и технологии	Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах.
Criminal Activity	Преступная деятельность	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения.
Cryptocurrency Mining	Криптомайнеры	Сайты, которые используют технологии майнинга криптовалют без разрешения пользователя.
Cults	Религиозные культы	Сайты, связанные с нетрадиционной религиозной практикой, обычно называемой культами. Подобные движения считаются ложными, неортодоксальными, экстремистскими. Члены культов зачастую живут под руководством харизматического лидера.
Dating and Personals	Сайты знакомств	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств, ресурсы, предлагающие эскорт-услуги.
Download Sites	Download-архивы	Сайты, которые содержат доступное для скачивания программное обеспечение. Эта категория также включает в себя некоторые Peer-to-Peer сайты.

Обозначение	Название	Описание
Education	Образование	Сайты, поддерживаемые учебными заведениями и школами всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы.
Entertainment	Развлечения	Сайты, предлагающие пользователю телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости.
Fashion and Beauty	Мода и красота	Сайты о моде, ювелирных изделиях, гламуре, красоте, модельном бизнесе, косметике или связанных со всем перечисленным товарах или услугах. Включает отзывы, сравнения, а также общую информацию, полезную потребителю.
Finance	Финансы	Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний, порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д.
Forums and Newsgroups	Форумы и новостные ленты	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги.
Gambling	Азартные игры	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами.
Games	Игры	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах.
Gay, Lesbian or Bisexual	Нетрадиционная сексуальная ориентация	Сайты, содержащие материалы о геях, лесбиянках, трансгендерах.
General	Общие	Сайты, которые не попадают в другие категории, например, пустые веб-страницы.

Обозначение	Название	Описание
Government	Правительство	Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц.
Greeting cards	Поздравительные открытки	Сайты, которые позволяют людям получать и отправлять поздравительные открытки.
Hacking	Хакерство	Сайты, которые способствуют или содержат рекомендации о том, как получить несанкционированный доступ к компьютерным системам с целью кражи информации, совершения мошеннических действий, советы по созданию вирусов или совершению других видов незаконной деятельности, связанной с кражей цифровой информации.
Hate and Intolerance	Ненависть и нетерпение	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
Health and Medicine	Здоровье и медицина	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной, рецептами лекарств, и т.д.
Illegal Drug	Наркотики	Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами.
Illegal Software	Нелегальное ПО	Сайты, которые незаконно распространяют программное обеспечение или защищенные авторским правом материалы, такие как фильмы, музыка, незаконные серийные номера, генераторы ключей.
Image Sharing	Обмен картинками	Порталы для размещения цифровых фотографий и изображений, фотоальбомы и фотообменники.

Обозначение	Название	Описание
Instant Messaging	Сервисы мгновенных сообщений	Сайты, которые позволяют создавать и использовать аккаунт в службах обмена мгновенными сообщениями, таких как ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, и т.п.
Job Search	Поиск работы	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний.
Kids sites	Детские сайты	Сайты, ориентированные на детскую аудиторию.
Legal	Юриспруденция	Сайты юридических фирм, обсуждение и анализ юридических вопросов.
Leisure and Recreation	Отдых и оздоровление	Сайты, связанные с рекреационной деятельностью и увлечениями, включая ресурсы, посвященные зоопаркам, центрам общественного отдыха, бассейнам, паркам развлечениям и хобби, таким как садоводство, литература, искусства и ремесла, домашний декор и т.д.
Literature and Books	Литература и книги	Сайты, содержащие опубликованные книги, новеллы, рассказы, включая фантастику, биографии.
Local Information	Местные достопримечательности	Путеводители и информация для туристов, в том числе о ресторанах и местные достопримечательности.
Malware	Вредоносное ПО	Сайты, содержащие нежелательные программы, автоматически загружающиеся и устанавливающиеся на ПК пользователей. Вирусы вносят изменения в систему и позволяют злоумышленникам получить данные с компьютера без ведома и согласия его владельца.
Military	Военные сайты	Информация о военных организациях, военной истории.
Nudity	Нудизм	Ресурсы, содержащие изображение частичной или полной наготы. Категория включает в себя сайты, рекламирующие или продающие нижнее белье, интимную одежду или купальные костюмы.
Nutrition and Diet	Здоровое питание и диеты	Сайты, посвященные правильному питанию, снижению веса, диетам.

Обозначение	Название	Описание
Online training and tools	Онлайн обучение	Дистанционное образование, онлайн-курсы, профессиональное обучение, программы обучения, повышения квалификации.
Parked Domains	Припаркованные домены	К припаркованным доменам относятся URL-адреса с ограниченным контентом, конечные точки перехода с рекламных объявлений. Подобные ресурсы могут приносить прибыль, но, как правило, не несут в себе полезной для пользователя информации. Категория также включает в себя сайты, находящиеся на реконструкции, папки и базовые страницы веб-серверов.
Peer-to-Peer	Пиринговые сети	Сайты, которые позволяют осуществлять прямой обмен файлами между пользователями вне зависимости от центрального сервера.
Personal Sites	Персональные сайты	Персональные сайты, созданные отдельными людьми или группами лиц, блоги.
Personal Storage	Персональные хранилища	Сайты, которые позволяют загружать файлы и резервные копии для удаленного хранения данных.
Pets and Animals	Домашние животные	Сайты, посвященные продуктам и сервисам для домашних и других животных.
Phishing and Fraud	Фишинг и мошенничество	Сайты, которые используются для обмана или в мошеннических целях (например, фишинг), такие как кражи финансовой или другой информации посредством учетной записи пользователя. Эти сайты чаще всего являются искусно выполненной подделкой популярных законных ресурсов, что вводит в заблуждение пользователей.
Politics	Политика	Сайты, посвященные политическим партиям или занимающиеся политической пропагандой, а также предоставляющие информацию о группах интересов, выборах, законодательстве или вопросе лоббирования. Категория включает в себя сайты, которые предлагают сведения о правах и их защите.

Обозначение	Название	Описание
Pornography/Sexually Explicit	Порнография и насилие	Сайты, которые содержат контент сексуального содержания. Категория включает в себя продукцию для взрослых, такую как секс-игрушки, компакт-диски и видео. Сайты из данной группы позволяют заказывать эскорт-услуги, получить сведения о стриптиз-клубах, почитать эротические рассказы и текстовые описания половых актов.
Profanity	Нецензурная лексика	Сайты, содержащие нецензурную лексику
Professional social networks	Профессиональные социальные сети	Подмножество веб-сайтов социальных сетей, которое включает в себя контент, предназначенный исключительно для бизнеса и профессионалов.
Real Estate	Недвижимость	Информация об аренде, покупке или продаже недвижимости или земельных участков. Рекомендации по покупке или продаже жилых помещений. Агентства недвижимости, услуги по аренде, переезду, улучшению жилищных условий.
Reference and Research	Справочная информация	Профессиональные или образовательные справочные материалы, в том числе онлайн-словари, карты, переписи, альманахи, каталоги библиотек, генеалогии, и научной информации.
Religion	Религия	Сайты, посвященные вопросу веры, человеческой духовности и религиозным убеждениям, в том числе сайты церквей, синагог, мечетей и других молитвенных домов.
Restaurants and Dining	Рестораны и еда	Сайты, содержащие списки, обзоры заведений общественного питания. Категория включает в себя сайты с рецептами, инструкциями и советами, продуктами питания и советами по выбору вина.
School Cheating	Школьные мошенничества	Сайты с ответами на различные школьные тесты, написанными эссе, рефератами, исследовательскими или курсовыми работами.
Search Engines and Portals	Поисковые системы и порталы	Сайты, позволяющие осуществлять поиск в интернете по новостям, изображениям, каталогам и другим видам онлайн-контента. Категория включает в себя порталы и каталоги сайтов, такие как белые/желтые страницы.

Обозначение	Название	Описание
Sex Education	Половое воспитание	Сайты, связанные с сексуальным образованием, включая такие темы, как уважение к партнеру, аборты, бисексуальный образ жизни, противозачаточные средства, заболевания, передаваемые половым путем и беременность.
Shopping	Покупки	Интернет-магазины, каталоги, аукционы, рекламные объявления. Категория не включает в себя ресурсы, посвященные товарам и услугам из более узких категорий, таких как здравоохранение и медицина.
Social Networking	Социальные сети	Сайты социальных сетей, пользователи которых могут общаться, взаимодействовать, обмениваться сообщениями, файлами.
Spam Sites	Спам-сайты	Сайты, продвижение которых основано на использовании спам-рассылок.
Sports	Спорт	Сайты команд или спортивных ассоциаций, международные и национальные, спортивные колледжи. Ресурсы, содержащие результаты и расписания игр, спортивные журналы и газеты, виртуальный спорт и спортивные лиги.
Stock trading	Фондовый рынок	Сайты по торговле ценными бумагами и управления инвестиционными активами. Также включает информацию о финансово-инвестиционной стратегии, котировкам и новостям.
Streaming Media and Downloads	Потоковое мультимедиа и загрузки	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.
Tasteless	Сайты сомнительного содержания	Сайты с оскорбительным контентом, такого рода как юмор "ниже пояса", ужасный или даже пугающий контент, шокирующие изображения крови, ран или жестокого обращения с животными.
Technical information and documentation	Техническая информация	Сайты, которые предоставляют информацию к технической документации и информации.
Translators	Переводчики	Сайты, на которых возможен онлайн-перевод веб-страниц на другие языки. Данные ресурсы могут использоваться для обхода заданных ограничений, так как просмотр сайтов осуществляется с URL сайта онлайн-переводчика.

Обозначение	Название	Описание
Transportation	Транспорт	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами, сообщества, клубы автолюбителей и т.д.
Travel	Путешествия	Авиакомпании, агентства по бронированию авиабилетов, планирование поездок, предварительные заказы, аренда транспортных средств, описания мест назначения, реклама гостиниц и казино.
Unknown	Неизвестная тематика	Сайты без принадлежности к какой-либо категории.
Updates	Обновления	Сайты обновлений программного обеспечения, обновлений операционных систем, обновлений
Violence	Насилие	Сайты, содержащие изображения, текстовые описания и пропаганду физического насилия против людей, животных или организаций\сообществ. Категория включает в себя ресурсы с иллюстрациями ужасов природы, а также сайты, содержащие ненормативную лексику.
Weapons	Оружие	Сайты, содержащие изображения, обзоры и описания оружия. В категории также входят интернет-магазины орудий и оружия, в том числе для занятия спортом.
Web-based Email	Веб-почта	Порталы, позволяющие завести собственные почтовые аккаунты для написания, чтения, отправки и получения электронных писем.

D

Типы событий журнала IP-пакетов

Таблица 21. События блокирования IP-пакетов фильтрами защищенной сети

Номер	Описание события
1	Не найден ключ для передачи IP-пакета сетевому узлу с идентификатором, указанным в IP-пакете
3	Входящий зашифрованный или предназначенный для шифрования исходящий открытый IP-пакет заблокирован фильтром защищенной сети
4	Слишком большой тайм-аут IP-пакета, то есть время его отправки отличается от времени его получения на величину, большую указанной в соответствующей настройке
7	Метод шифрования, код которого указан во входящем IP-пакете, не поддерживается
8	IP-пакет поврежден
9	Неизвестный идентификатор сетевого узла
11	IP-пакет заблокирован фильтром защищенной сети с ICMP- или TCP RST-ответом
13	Превышено максимальное время пребывания IP-пакета в сети
14	Неверный адрес получателя IP-пакета
16	Исчерпана лицензия на количество туннелируемых узлов
17	Неверный IP-адрес получателя
18	Неизвестный IP-адрес получателя
26	Узел с данного координатора недоступен

Таблица 22. События блокирования IP-пакетов локальными фильтрами открытой сети

Номер	Описание события
22	От защищенного узла получен открытый IP-пакет
23	От защищенного узла получен открытый широковещательный IP-пакет
24	На порт, используемый одной из служб ViPNet, получен открытый IP-пакет
30	Локальный IP-пакет заблокирован фильтром открытой сети
31	Транзитный IP-пакет заблокирован фильтром открытой сети
32	Широковещательный IP-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

Таблица 23. События блокирования IP-пакетов по другим причинам

Номер	Описание события
28	IP-пакет заблокирован ICAP-сервером
29	IP-пакет заблокирован по причине: включена блокировка трафика, если ICAP-сервер не отвечает
81	Недопустимая версия протокола IP (поддерживается только IPv4)
82	Длина заголовка IP-пакета меньше допустимой
83	Длина IP-пакета меньше указанной в IP-заголовке
84	Значение контрольной суммы в заголовке IP-пакета отличается от ее значения в IP-пакете
85	Размер TCP-заголовка меньше допустимого
86	Размер UDP-заголовка меньше допустимого
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
94	Недостаточно памяти
99	Заблокирован фрагментированный IP-пакет
115	Не удалось найти маршрут для IP-пакета в таблице маршрутизации
116	Не найден сетевой адаптер

118	Ошибка при шифровании исходящего IP-пакета для защищенного узла
119	Получен зашифрованный IP-пакет неизвестного формата, который не может быть расшифрован
131	Ошибка обработки прикладных протоколов: не удалось построить маршрут
135	Ошибка обработки модуля ALG
136	Недостаточно памяти для выполнения трансляции адреса (NAT)
139	Отсутствуют лицензии для туннелирования на узле назначения
142	IP-пакет заблокирован правилом IPS

Таблица 24. 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 25. 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
67	IP-пакет пропущен с предупреждением IPS

E

Базы управляющей информации (MIB) для протокола SNMP

MIB-II System

MIB-II System (.1.3.6.1.2.1.1) включает в себя объекты, предназначенные для получения информации о системных параметрах сетевого узла (например, имя узла, ОС, количество и параметры сетевых интерфейсов, статистика по SNMP-сообщениям). Подробнее см. в RFC 1213.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator HW могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать имена интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 26. 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.
.1.3.6.1.2.1.1.7.0	Число, означающее наличие сетевых служб на определённых уровнях модели OSI. Для каждого уровня, для которого на узле есть службы, число 2 возводится в степень (L-1) и добавляется к общей сумме. Пример для координатора: 2^(4-1)+2^(7-1)=72 – узел работает на транспортном и прикладном уровне.
.1.3.6.1.2.1.1.8.0	Значение sysUpTime с момента последнего изменения состояния или значения столбца .1.3.6.1.2.1.1.9.1.2.A из таблицы .1.3.6.1.2.1.1.9.1.
Таблица поддерживаемых MIB (.1.3.6.1.2.1.1.9.1):	
A — индекс таблицы	
.1.3.6.1.2.1.1.9.1.1.A	Индекс таблицы.
.1.3.6.1.2.1.1.9.1.2.A	OID для MIB, с которыми работает SNMP-агент.
.1.3.6.1.2.1.1.9.1.3.A	Текстовое описание MIB.
.1.3.6.1.2.1.1.9.1.4.A	Время с момента подключения MIB.
ARP-таблица (.1.3.6.1.2.1.3.1.1):	
B — индекс интерфейса, присвоенный сетевым узлом	
E — IP-адрес сетевого узла	
.1.3.6.1.2.1.3.1.1.1.B.1.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.3.1.1.2.B.1.E	MAC-адрес.
.1.3.6.1.2.1.3.1.1.3.B.1.E	IP-адрес, соответствующий MAC-адресу.
Таблица описания маршрутов (.1.3.6.1.2.1.4.21.1):	
E — IP-адрес сетевого узла или сети	
.1.3.6.1.2.1.4.21.1.1.E	IP-адрес назначения маршрутов (маршрут по умолчанию 0.0.0.0).
.1.3.6.1.2.1.4.21.1.2.E	Индекс интерфейса (1.3.6.1.2.1.2.2.1.1), через который будет производится маршрутизация.
.1.3.6.1.2.1.4.21.1.3.E	Основная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.4.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).

OID	Описание
.1.3.6.1.2.1.4.21.1.5.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.6.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.7.E	IP-адрес следующего маршрутизатора по маршруту (Next Hop).
.1.3.6.1.2.1.4.21.1.8.E	Тип маршрута: • 1 (other) — другое, не может быть причислено к другим категориям; • 2 (invalid) — некорректный; • 3 (direct) — маршрут к подключённой сети; • 4 (indirect) — маршрут к удалённой сети.
.1.3.6.1.2.1.4.21.1.9.E	Механизм маршрутизации, через который был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам; • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP; • 4 (icmp) — протокол ICMP (Redirect); • 5 (egp) — протокол EGP; • 6 (ggp) — протокол GGP; • 7 (hello) — протокол Hello; • 8 (rip) — протокол RIP; • 9 (is-is) — протокол IS-IS; • 10 (es-is) — протокол ES-IS; • 11 (ciscoIgrp) — протокол cisco IGRP; • 12 (bbnSpfIgp) — протокол BBNSPFIGP; • 13 (ospf) — протокол OSPF; • 14 (bgp) — протокол BGP.
.1.3.6.1.2.1.4.21.1.10.E	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.21.1.11.E	Маска маршрута.
.1.3.6.1.2.1.4.21.1.12.E	Дополнительная метрика протокола маршрутизации.
.1.3.6.1.2.1.4.21.1.13.E	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.11.1.0	Количество полученных сообщений SNMP.
.1.3.6.1.2.1.11.2.0	Количество отправленных сообщений SNMP.
.1.3.6.1.2.1.11.3.0	Количество полученных сообщений SNMP неподдерживаемой версии.

OID	Описание
.1.3.6.1.2.1.11.4.0	Количество полученных сообщений SNMP, адресованных неизвестному сообществу.
.1.3.6.1.2.1.11.5.0	Количество полученных сообщений SNMP, содержащих операцию, не разрешенную на сетевом узле для сообщества.
.1.3.6.1.2.1.11.6.0	Количество ошибок ASN.1 или BER при разборе SNMP-сообщений.
.1.3.6.1.2.1.11.8.0	Количество входящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.9.0	Количество входящих SNMP PDU, для которых значение поля error-status – «noSuchName».
1.3.6.1.2.1.11.10.0	Количество входящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.11.0	Количество входящих SNMP PDU, для которых значение поля error-status – «readOnly».
.1.3.6.1.2.1.11.12.0	Количество входящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.13.0	Количество успешно полученных MIB объектов с использованием Get-Request и Get-Next.
.1.3.6.1.2.1.11.14.0	Количество успешно записанных MIB объектов с использованием Set-Request.
.1.3.6.1.2.1.11.15.0	Количество успешно обработанных SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.16.0	Количество успешно обработанных SNMP Get-Next PDUs.
.1.3.6.1.2.1.11.17.0	Количество успешно обработанных SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.18.0	Количество успешно обработанных SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.19.0	Количество успешно обработанных SNMP Trap PDUs.
.1.3.6.1.2.1.11.20.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.21.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «noSuchName».
.1.3.6.1.2.1.11.22.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.24.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.25.0	Количество успешно сгенерированных исходящих SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.26.0	Количество успешно сгенерированных исходящих SNMP Get-Next PDUs.

OID	Описание
.1.3.6.1.2.1.11.27.0	Количество успешно сгенерированных исходящих SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.28.0	Количество успешно сгенерированных исходящих SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.29.0	Количество успешно сгенерированных исходящих SNMP Trap PDUs.
.1.3.6.1.2.1.11.30.0	Возможность отправки authenticationFailure traps: • 1 — разрешено; • 2 — запрещено.
.1.3.6.1.2.1.11.31.0	Количество параметров отброшенных SNMP без уведомлений в связи с несоответствием параметров агента и сервера.
.1.3.6.1.2.1.11.32.0	Количество параметров отброшенных SNMP без уведомлений в связи с проблемами proxy.

IF-MIB

IF-MIB (.1.3.6.1.2.1.2) включает в себя объекты, предназначенные для получения информации о параметрах сетевых интерфейсов сетевого узла (например, тип сетевого интерфейса, физический адрес, пропускная способность). Подробнее см. в RFC 2863.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator HW могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP вместо индексов используйте названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 27. SNMP-параметры. IF-MIB

OID	Описание
.1.3.6.1.2.1.2.1.0	Количество сетевых интерфейсов (физических, виртуальных, включая loopback).
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.2.1.2.2.1):	
A — индекс интерфейса	
.1.3.6.1.2.1.2.2.1.1.A	Индекс сетевого интерфейса (A).
.1.3.6.1.2.1.2.2.1.2.A	Описание интерфейса (производитель, название и версия оборудования или ПО).

OID	Описание
.1.3.6.1.2.1.2.2.1.3.A	Тип сетевого интерфейса: • 6 — ethernet; • 24 — localhost. Остальные значения можно посмотреть здесь.
.1.3.6.1.2.1.2.2.1.4.A	MTU (в байтах).
.1.3.6.1.2.1.2.2.1.5.A	Максимальная пропускная способность (бит/сек).
.1.3.6.1.2.1.2.2.1.6.A	MAC-адрес.
.1.3.6.1.2.1.2.2.1.7.A	Назначенное состояние интерфейса: • 1 (up) — включен; • 2 (down) — выключен; • 3 (testing) — состояние тестирования, указывает, что никакие рабочие пакеты не могут быть переданы.
.1.3.6.1.2.1.2.2.1.8.A	Текущее рабочее состояние интерфейса: • 1 (up) — включен; • 2 (down) — выключен; • 3 (testing) — состояние тестирования. Никакие рабочие пакеты не могут быть переданы; • 4 (unknown) — неизвестно; • 5 (dormant) — интерфейс ожидает внешних действий (таких как последовательная линия, ожидающая входящее соединение); • 6 (notPresent) — в интерфейсе отсутствуют компоненты (обычно аппаратные); • 7 (lowerLayerDown) — не работает из-за состояния интерфейса нижнего уровня.
.1.3.6.1.2.1.2.2.1.9.A	Время работы SNMP-агента с начала его запуска (sysUpTime) до момента перехода интерфейса в его текущее состояние.
.1.3.6.1.2.1.2.2.1.10.A	Количество полученных байт (октетов).
.1.3.6.1.2.1.2.2.1.11.A	Количество полученных одноадресных (unicast) пакетов.
.1.3.6.1.2.1.2.2.1.12.A	Количество полученных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.13.A	Количество отклоненных пакетов.
.1.3.6.1.2.1.2.2.1.14.A	Количество пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.15.A	Количество пакетов, которые были отклонены из-за неизвестного или не поддерживаемого протокола.
.1.3.6.1.2.1.2.2.1.16.A	Количество отправленных байт (октетов).
.1.3.6.1.2.1.2.2.1.17.A	Количество отправленных одноадресных (unicast) пакетов.

OID	Описание
.1.3.6.1.2.1.2.2.1.18.A	Количество отправленных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.19.A	Количество отклоненных отправленных пакетов.
.1.3.6.1.2.1.2.2.1.20.A	Количество отправленных пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.21.A	Количество исходящих пакетов в очереди на отправку.
Таблица статистики дополнительных параметров сетевых интерфейсов (.1.3.6.1.2.1.31.1.1.1):	
A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1	
.1.3.6.1.2.1.31.1.1.1.1.A	Имя интерфейса.
.1.3.6.1.2.1.31.1.1.1.2.A	Количество входящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.3.A	Количество входящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.4.A	Количество исходящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.5.A	Количество исходящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.6.A	Количество байт (октетов), принятых интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.7.A	Количество входящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.8.A	Количество входящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.9.A	Количество входящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.10.A	Количество байт (октетов), отправленных интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.11.A	Количество исходящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.12.A	Количество исходящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.13.A	Количество исходящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.14.A	Необходимость отправки trap на события linkUp/linkDown: • 1 — отправлять trap; • 2 — не отправлять trap.
.1.3.6.1.2.1.31.1.1.1.15.A	Максимальная скорость интерфейса (Мегабит/сек).
.1.3.6.1.2.1.31.1.1.1.16.A	Режим работы интерфейса: • 1 (true) — принимает все пакеты; • 2 (false) — принимает только пакеты, адресованные сетевому узлу.

OID	Описание
.1.3.6.1.2.1.31.1.1.1.17.A	Наличие физического коннектора у интерфейса: • 1 (true) — есть коннектор (для ethernet); • 2 (false) — нет коннектора (для localhost).
.1.3.6.1.2.1.31.1.1.1.18.A	Имя интерфейса, заданное администратором. Для координатора всегда равно 0.
.1.3.6.1.2.1.31.1.1.1.19.A	Время работы SNMP-агента с последнего запуска (sysUpTime) до появления разрыва в подсчете счетчиков на интерфейсе.
.1.3.6.1.2.1.31.1.5.0	Время работы SNMP-агента с последнего запуска (sysUpTime) до последнего добавления или удаления записи в таблице статистики дополнительных параметров сетевых интерфейсов.

IP-MIB

IP-MIB (.1.3.6.1.2.1.4) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу IP (например, параметры сетевых интерфейсов, статистика для IP-трафика, таблица IP-адресов). Подробнее см. в RFC 4293.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 28. SNMP-параметры. IP-MIB

OID	Описание
.1.3.6.1.2.1.4.1.0	Указывает, является ли сетевой узел маршрутизатором: • 1 — является (координатор всегда работает в данном режиме); • 2 — не является.
.1.3.6.1.2.1.4.2.0	TTL по умолчанию для IP-пакетов.
.1.3.6.1.2.1.4.3.0	Общее количество IP-пакетов, принятых сетевым узлом, включая пакеты с ошибками.
.1.3.6.1.2.1.4.4.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в заголовке пакета.
.1.3.6.1.2.1.4.5.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в адресе.
.1.3.6.1.2.1.4.6.0	Количество IP-пакетов, переданных на следующий шлюз.
.1.3.6.1.2.1.4.7.0	Количество IP-пакетов, отклонённых по причине неизвестного или неподдерживаемого протокола.
1.3.6.1.2.1.4.8.0	Количество отклоненных пакетов по причине недостатка буфера.
.1.3.6.1.2.1.4.9.0	Количество успешно доставленных IP-пакетов.

OID	Описание
.1.3.6.1.2.1.4.10.0	Количество IP-пакетов, отправленных сетевым узлом (не включая .1.3.6.1.2.1.4.6.0).
.1.3.6.1.2.1.4.11.0	Количество IP-пакетов, отклонённых по причине недостатка буфера.
.1.3.6.1.2.1.4.12.0	Количество IP-пакетов, отклоненных к дальнейшей передаче по причине отсутствия маршрута.
.1.3.6.1.2.1.4.13.0	Максимальное количество секунд ожидания сборки фрагментов.
.1.3.6.1.2.1.4.14.0	Количество принятых IP-фрагментов.
.1.3.6.1.2.1.4.15.0	Количество успешных сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.16.0	Количество ошибок сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.17.0	Количество успешно фрагментированных исходящих IP-пакетов.
.1.3.6.1.2.1.4.18.0	Количество ошибок при фрагментации исходящих IP-пакетов.
.1.3.6.1.2.1.4.19.0	Количество фрагментов IP-пакетов, сгенерированных данным сетевым узлом.
Таблица IP-адресов сетевого узла для протокола IPv4 (.1.3.6.1.2.1.4.20.1.):	
E — IP-адрес	
.1.3.6.1.2.1.4.20.1.1.E	IP-адрес.
.1.3.6.1.2.1.4.20.1.2.E	Указатель на интерфейс, которому присвоен этот IP-адрес (A - из таблицы .1.3.6.1.2.1.2.2.1).
.1.3.6.1.2.1.4.20.1.3.E	Маска сети.
.1.3.6.1.2.1.4.20.1.4.E	Значение наименее значимого бита в широковещательном (broadcast) IP-адресе.
Таблица разрешения IP-адресов в физические адреса (ARP-таблица) (.1.3.6.1.2.1.4.22.1.):	
A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB	
E — IP-адрес	
.1.3.6.1.2.1.4.22.1.1.A.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.4.22.1.2.A.E	MAC-адрес.
.1.3.6.1.2.1.4.22.1.3.A.E	IP-адрес.
.1.3.6.1.2.1.4.22.1.4.A.E	Тип маппинга: • 1 — другое; • 2 — некорректный; • 3 — динамический; • 4 — статический.
.1.3.6.1.2.1.4.23.0	Количество отклоненных маршрутов.

OID	Описание
.1.3.6.1.2.1.4.31.1.1.	Таблица, содержащая статистику (счетчики) IP-трафика различных версий на сетевом узле для всех интерфейсов.
.1.3.6.1.2.1.4.31.2.0	Значение sysUpTime в момент добавления/удаления столбцов в таблицу .1.3.6.1.2.1.4.31.1.1.

Таблица префиксов IP-адресов (.1.3.6.1.2.1.4.32.1.):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

B — тип адреса:

- **значение 0 — неизвестно;**
- **значение 1 — ipv4;**
- **значение 2 — ipv6;**
- **значение 3 — ipv4z;**
- **значение 4 — ipv6z;**
- **значение 16 — dns.**

C — префикс (адрес сети)

D — длина префикса

.1.3.6.1.2.1.4.32.1.5.A.B.C.D	Источник префикса: • 1 — другое; • 2 — вручную; • 3 — общеизвестный префикс; • 4 — dhcp; • 3 — routeradv (значение получено от роутера).
.1.3.6.1.2.1.4.32.1.6.A.B.C.D	Указывает, может ли префикс использоваться как маршрут: • 1 — может; • 2 — не может.
.1.3.6.1.2.1.4.32.1.7.A.B.C.D	Указывает, может ли префикс использоваться для автоматической конфигурации адреса: • 1 — может; • 2 — не может.
.1.3.6.1.2.1.4.32.1.8.A.B.C.D	Время (в секундах), в течение которого префикс будет оставаться предпочтительным. Значение 4294967295 означает бесконечность.
.1.3.6.1.2.1.4.32.1.9.A.B.C.D	Время (в секундах), в течение которого префикс будет существовать. Значение 4294967295 означает бесконечность.

OID	Описание
Таблица адресной информации по интерфейсам (.1.3.6.1.2.1.4.34.1):	
B — тип адреса: • **значение 0 — неизвестно;** • **значение 1 — ipv4;** • **значение 2 — ipv6;** • **значение 3 — ipv4z;** • **значение 4 — ipv6z;** • **значение 16 — dns.**	
E — IP-адрес	
.1.3.6.1.2.1.4.34.1.3.B.E	Индекс сетевого интерфейса.
.1.3.6.1.2.1.4.34.1.4.B.E	Тип адреса: • 1 (unicast) — одноадресный; • 2 (anycast) — к ближайшему узлу; • 3 (broadcast) — широковещательный.
.1.3.6.1.2.1.4.34.1.5.B.E	Ссылка на строку таблицы префиксов.
.1.3.6.1.2.1.4.34.1.6.B.E	Происхождение адреса: • 1 (other) — другое; • 2 (manual) — назначен вручную; • 4 (dhcp) — назначен по dhcp; • 5 (linklayer) — назначен механизмом автоконфигурации протокола IPv6 (SLAAC); • 6 (random) — назначен случайным образом.
.1.3.6.1.2.1.4.34.1.7.B.E	Статус адреса: • 1 (preferred) — предпочтительный; • 2 (deprecated) — устарел; • 3 (invalid) — недействителен; • 4 (inaccessible) — недоступен; • 5 (unknown)— неизвестен; • 6 (tentative) — предварительный; • 7 (duplicate) — дублированный; • 8 (optimistic) — оптимистичный.
.1.3.6.1.2.1.4.34.1.8.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента создания записи.
.1.3.6.1.2.1.4.34.1.9.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента изменения записи.

OID	Описание
.1.3.6.1.2.1.4.34.1.10.B.E	Статус строки: • 1 (active) — строка доступна для использования; • 2 (notInService) — строка недоступна для использования; • 3 (notReady) — отсутствует информация для использования; • 4 (createAndGo) — создание строки и перевод ее в статус active; • 5 (createAndWait) — создание строки и перевод ее в статус notInService; • 6 (destroy) — удаление.
.1.3.6.1.2.1.4.34.1.11.B.E	Механизм хранения строки: • 1 (other) — другое; • 2 (volatile) — изменяемая; • 3 (nonvolatile) — энергонезависимая; • 4 (permanent) — постоянная; • 5 (readOnly) — только для чтения.

Таблица трансляции MAC IP (.1.3.6.1.2.1.4.35.1):

A — индекс интерфейса из таблицы .1.3.6.1.2.1.2.2.1.1 MIB-II

B — тип адреса:

- **0 — неизвестно;**
- **1 — ipv4;**
- **2 — ipv6;**
- **3 — ipv4z;**
- **4 — ipv6z;**
- **16 — dns.**

E — IP-адрес

.1.3.6.1.2.1.4.35.1.4.A.B.E	Транслируемый MAC-адрес.
.1.3.6.1.2.1.4.35.1.5.A.B.E	Время работы SNMP-агента с момента последнего запуска (sysUpTime) до момента изменения MAC-адреса.
.1.3.6.1.2.1.4.35.1.6.A.B.E	Тип маппинга: • 1 (other) — другое; • 2 (invalid) — недопустимое значение; • 3 (dynamic) — динамическое; • 4 (static) — статическое; • 5 (local) — предоставляется для собственного адреса интерфейса объекта.

OID	Описание
.1.3.6.1.2.1.4.35.1.7.A.B.E	Статус маппинга: • 1(reachable) — подтвержден; • 2 (stale) — не подтвержден; • 3 (delay) — ожидание; • 4 (probeprobe) — активное; • 5 (invalid) — недействителен; • 6 (unknown) — не определен; • 7 (incomplete) — выполняется разрешение адреса.
.1.3.6.1.2.1.4.35.1.8.A.B.E	Статус строки: • 1 (active) — строка доступна для использования; • 2 (notInService) — строка недоступна для использования; • 3 (notReady) — отсутствует информация для использования; • 4 (createAndGo) — создание строки и перевод ее в статус active; • 5 (createAndWait) — создание строки и перевод ее в статус notInService; • 6 (destroy) — удаление.
.1.3.6.1.2.1.5.1.0	Общее число ICMP-запросов, полученных сетевым узлом.
.1.3.6.1.2.1.5.2.0	Число ICMP-запросов с ошибкой, полученных сетевым узлом.
.1.3.6.1.2.1.5.3.0	Количество сообщений о недоступности заданного сетевого узла, полученных данным сетевым узлом.
.1.3.6.1.2.1.5.4.0	Количество сообщений об истечении времени ожидания ответа, полученных сетевым узлом.
.1.3.6.1.2.1.5.5.0	Количество полученных сообщений ICMP Parameter Problem.
.1.3.6.1.2.1.5.6.0	Количество полученных сообщений ICMP Source Quench.
.1.3.6.1.2.1.5.7.0	Количество полученных сообщений ICMP Redirect messages.
.1.3.6.1.2.1.5.8.0	Количество полученных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.9.0	Количество полученных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.10.0	Количество полученных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.11.0	Количество полученных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.12.0	Количество полученных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.13.0	Количество полученных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.14.0	Количество ICMP сообщений, отправленных сетевым узлом.
.1.3.6.1.2.1.5.15.0	Количество ICMP сообщений, которые сетевой узел не смог отправить из-за проблем с ICMP.
.1.3.6.1.2.1.5.16.0	Количество отправленных сообщений ICMP Destination Unreachable.

OID	Описание
.1.3.6.1.2.1.5.17.0	Количество отправленных сообщений ICMP Time Exceeded.
.1.3.6.1.2.1.5.18.0	Количество отправленных сообщений ICMP Parameter Problem.
1.3.6.1.2.1.5.19.0	Количество отправленных сообщений ICMP Source Quench.
1.3.6.1.2.1.5.20.0	Количество отправленных сообщений ICMP Redirect.
1.3.6.1.2.1.5.21.0	Количество отправленных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.22.0	Количество отправленных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.23.0	Количество отправленных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.24.0	Количество отправленных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.25.0	Количество отправленных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.26.0	Количество отправленных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.29.1	Таблица счетчиков ICMP сообщений с указанием версии протокола IP.
.1.3.6.1.2.1.5.30.1	Таблица счетчиков входящих-исходящих ICMP пакетов с указанием версии протокола IP.

IP-FORWARD-MIB

IP-FORWARD-MIB (.1.3.6.1.2.1.4.24) включает в себя объекты, предназначенные для получения информации о параметрах маршрутизации сетевого узла. Подробнее см. в RFC 4292.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 29. SNMP-параметры. IP-FORWARD-MIB

OID	Описание
Таблица маршрутизации сетевого узла (.1.3.6.1.2.1.4.24.4.1):	
.1.3.6.1.2.1.4.24.4.1.1.A.B.C.D	Адрес назначения маршрута (A).
.1.3.6.1.2.1.4.24.4.1.2.A.B.C.D	Маска адреса назначения маршрута (B).
.1.3.6.1.2.1.4.24.4.1.3.A.B.C.D	Параметр, обозначающий значение поля IP TOS Field (C).
.1.3.6.1.2.1.4.24.4.1.4.A.B.C.D	Адрес следующего маршрутизатора в маршруте (D).
.1.3.6.1.2.1.4.24.4.1.5.A.B.C.D	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2.1 IF-MIB.

OID	Описание
.1.3.6.1.2.1.4.24.4.1.6.A.B.C.D	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения.
.1.3.6.1.2.1.4.24.4.1.7.A.B.C.D	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.4.1.8.A.B.C.D	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.24.4.1.9.A.B.C.D	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.4.24.4.1.10.A.B.C.D	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.4.1.11.A.B.C.D	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.12.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.13.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.4.24.4.1.14.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.15.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.16.A.B.C.D	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление
1.3.6.1.2.1.4.24.6.0	Количество текущих корректных маршрутов из таблицы .1.3.6.1.2.1.4.24.7.1
Таблица маршрутизации сетевого узла с указанием версии протокола IP (.1.3.6.1.2.1.4.24.7.1):	
.1.3.6.1.2.1.4.24.7.1.7	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2 IF-MIB.
.1.3.6.1.2.1.4.24.7.1.8	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения, • 5 (blackhole) — маршрут, по которому пакеты теряются без сообщений об ошибках.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.9	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.7.1.10	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.24.7.1.11	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.7.1.12	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.13	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.14	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.15	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.16	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.17	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

Ethernet-Like MIB

Ethernet-Like MIB (1.3.6.1.2.1.10) включает в себя объекты, предназначенные для получения статистической информации о работе интерфейсов сетевого узла. Подробнее см. в RFC 3635.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 30. 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 31. 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 - удалённый IP-адрес

D - удалённый 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 удалённого адреса,

C — удалённый IP-адрес,

D — удалённый 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 32. 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 удалённого адреса,** **C — IP-адрес удалённого порта,** **D — номер удалённого 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 33. SNMP-параметры. HOST-RESOURCES-MIB

OID	Описание
.1.3.6.1.2.1.25.1.1.0	Время работы системы с момента 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 оперативной памяти (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 — процессор (ядра), • 4 — сетевой интерфейс, • 5 — принтер, • 6 — жесткий диск (HDD, SSD), • 10 — видеоустройство, • 11 — аудиоустройство, • 12 — сопроцессор, • 13 — клавиатура, • 14 — модем, • 15 — параллельный порт, • 16 — манипулятор типа мышь, • 17 — последовательный порт, • 18 — ленточное хранилище, • 19 — часы, • 20 — энергозависимая память, • 21 — энергонезависимая память.
.1.3.6.1.2.1.25.3.2.1.3.B	Описание устройства.
.1.3.6.1.2.1.25.3.2.1.4.B	ID продукта.

OID	Описание
.1.3.6.1.2.1.25.3.2.1.5.B	Текущий статус устройства: • 1 — статус неизвестен (unknown), • 2 — работает (running), • 3 — предупреждение (warning), • 4 — проверка (testing), • 5 — не работает (down).
.1.3.6.1.2.1.25.3.2.1.6.B	Счетчик количества ошибок на устройстве.

Таблица загрузки процессоров сетевого узла (.1.3.6.1.2.1.25.3.3.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.3.1.1.B	ID продукта.
.1.3.6.1.2.1.25.3.3.1.2.B	Средняя нагрузка на ядро за последнюю минуту.

Таблица сетевых устройств (.1.3.6.1.2.1.25.3.4.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.4.1.1.B	Индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB.

Таблица дисков сетевого узла (.1.3.6.1.2.1.25.3.6.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.6.1.1.B	Доступ к диску: • 1 — чтение и запись, • 2 — чтение.
.1.3.6.1.2.1.25.3.6.1.2.B	Тип устройства: • 1 — применяется, если не может быть отнесено к другой группе, • 2 — неизвестен, • 3 — жесткий диск, • 4 — дискета, • 5 — оптический диск ROM, • 6 — оптический диск WORM, • 10 — оптический диск RW, • 11 — RAM диск.
.1.3.6.1.2.1.25.3.6.1.3.B	Возможность извлечения диска: • 1 — Разрешено, • 2 — Запрещено.
.1.3.6.1.2.1.25.3.6.1.4.B	Размер диска (в килобайтах). Если диск извлекаемый и он извлечен, параметр равен 0.

Таблица разделов сетевого узла (.1.3.6.1.2.1.25.3.7.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

D — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

OID	Описание
.1.3.6.1.2.1.25.3.7.1.1.B.D	Индекс устройства (D).
.1.3.6.1.2.1.25.3.7.1.2.B.D	Описание раздела.
.1.3.6.1.2.1.25.3.7.1.3.B.D	ID раздела в операционной системе — октетная строка.
.1.3.6.1.2.1.25.3.7.1.4.B.D	Размер раздела (в килобайтах).
.1.3.6.1.2.1.25.3.7.1.5.B.D	Файловая система, используемая в разделе. Если файловой системы нет, параметр равен 0.

Таблица файловых систем сетевого узла (.1.3.6.1.2.1.25.3.8.1):

E — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

.1.3.6.1.2.1.25.3.8.1.1.E	Индекс устройства (E).
.1.3.6.1.2.1.25.3.8.1.2.E	Корневая папка файловой системы (точка монтирования).
.1.3.6.1.2.1.25.3.8.1.3.E	Описание удалённого сервера, с которого смонтирована файловая система. Может включать корневую папку файловой системы (точка монтирования) на удалённом сервере. Для локальных файловых систем параметр содержит пустую строку.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.4.E	OID, присвоенный данному типу файловой системы: 1.3.6.1.2.1.25.3.9 + • 1 — Применяется, если не может быть отнесена к другой группе, • 2 — Если тип файловой системы неизвестен, • 3 — BFFS, • 4 — System V, • 5 — DOS FAT, • 6 — OS/2 HPFS, • 7 — MHFS, • 8 — MFS, • 9 — NTFS, • 10 — VNode File System, • 11 — Journaled File System, • 12 — ISO 9660 File System for CD, • 13 — RockRidge File System for CD, • 14 — NFS File System, • 15 — Netware File System, • 16 — Andrew File System, • 17 — OSF DCE Distributed File System, • 18 — AppleShare File System, • 19 — RFS File System, • 20 — Data General DGCFS, • 21 — SVR4 Boot File System, • 22 — Windows FAT32, • 23 — Linux EXT2 File System.
.1.3.6.1.2.1.25.3.8.1.5.E	Права доступа к файловой системе: • 1 — запись, чтение, • 2 — чтение.
.1.3.6.1.2.1.25.3.8.1.6.E	Возможность запуска с файловой системы: • 1 — возможно, • 2 — невозможно.
.1.3.6.1.2.1.25.3.8.1.7.E	Указывает на связь файловой системы и хранилищ.
.1.3.6.1.2.1.25.3.8.1.8.E	Дата последнего полного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.9.E	Дата последнего частичного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.
Таблица ПО, запущенного на сетевом узле (.1.3.6.1.2.1.25.4.2.1):	
F — индекс ПО	
.1.3.6.1.2.1.25.4.2.1.1.F	Индекс запущенного ПО (F).
.1.3.6.1.2.1.25.4.2.1.2.F	Наименование запущенного ПО.
.1.3.6.1.2.1.25.4.2.1.3.F	ID ПО производителя.
.1.3.6.1.2.1.25.4.2.1.4.F	Папка, из которой запущено ПО.
.1.3.6.1.2.1.25.4.2.1.5.F	Параметры, с которыми запущено ПО.
.1.3.6.1.2.1.25.4.2.1.6.F	Тип программного обеспечения: • 1 — неизвестно, • 2 — ОС, • 3 — драйвер устройства, • 4 — приложение.
.1.3.6.1.2.1.25.4.2.1.7.F	Текущее состояние ПО: • 1 — запущено (running), • 2 — работоспособно (runnable), • 3 — неработоспособно (notRunnable), • 4 — работает некорректно (invalid).
Таблица с потреблением каждого ПО ЦПУ и ОЗУ (.1.3.6.1.2.1.25.5.1.1):	
F — индекс ПО из таблицы .1.3.6.1.2.1.25.4.2.1	
.1.3.6.1.2.1.25.5.1.1.1.F	Количество процессорного времени, выделенного ПО, в сантисекундах (0,01 с).
.1.3.6.1.2.1.25.5.1.1.2.F	Количество занимаемой оперативной памяти (в килобайтах).

LM-SENSORS-MIB

LM-SENSORS-MIB (.1.3.6.1.4.1.2021) включает в себя объекты, предназначенные для получения информации от различных датчиков, которые установлены в оборудовании сетевого узла.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 34. SNMP-параметры. LM-SENSORS-MIB

OID	Описание
Таблица температурных датчиков сетевого узла (.1.3.6.1.4.1.2021.13.16.2.1):	
A — индекс температурного датчика	
.1.3.6.1.4.1.2021.13.16.2.1.1.A	Индекс температурного датчика (A).
.1.3.6.1.4.1.2021.13.16.2.1.2.A	Имя температурного датчика.
.1.3.6.1.4.1.2021.13.16.2.1.3.A	Температура (в м°C).
Таблица датчиков скорости вращения вентиляторов (.1.3.6.1.4.1.2021.13.16.3.1):	
B — индекс датчика скорости вращения вентилятора	
.3.6.1.4.1.2021.13.16.3.1.1.B	Индекс датчика скорости вращения вентилятора (B).
.3.6.1.4.1.2021.13.16.3.1.2.B	Имя датчика скорости вращения вентилятора.
.3.6.1.4.1.2021.13.16.3.1.3.B	Скорость вращения вентилятора (в оборотах в минуту). Если вентилятор не подключен, параметр равен 0.

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 35. SNMP-параметры. NOTIFICATION-LOG-MIB

OID	Описание
.1.3.6.1.2.1.92.1.1.1.0	Максимальное количество записей, которое может хранить таблица журналов .1.3.6.1.2.1.92.1.3.1.1 (таблица не поддерживается в ViPNet Coordinator HW). Если ограничений нет, параметр равен 0.
.1.3.6.1.2.1.92.1.1.2.0	Время, в течение которого SNMP-агент должен хранить уведомления (в минутах). Если время не ограничено, параметр равен 0.
.1.3.6.1.2.1.92.1.2.1.0	Количество записей в таблице журналов .1.3.6.1.2.1.92.1.3.1.1 (таблица не поддерживается ViPNet Coordinator HW).
.1.3.6.1.2.1.92.1.2.2.0	Количество записей, отброшенных из-за необходимости освобождения места под новые, или по причине превышения значений параметров .1.3.6.1.2.1.92.1.1.1.0 или 1.3.6.1.2.1.92.1.1.3.1.3. Не включает в себя количество записей, удалённых 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 36. SNMP-параметры. UCD-SNMP-MIB

OID	Описание
.1.3.6.1.4.1.2021.4.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.4.2.0	Фиктивное имя, всегда равно объему виртуальной памяти.
.1.3.6.1.4.1.2021.4.3.0	Объем виртуальной памяти (swap) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.4.0	Объем доступной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.5.0	Объем физической памяти (RAM) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.6.0	Объем доступной физической памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.7.0	Объем виртуальной памяти, выделенный для текстовых страниц (в кибибайтах).
.1.3.6.1.4.1.2021.4.9.0	Объем физической памяти (RAM), выделенный для текстовых страниц (в кибибайтах). Не выводится, если операционная система не выделяет текстовые страницы от других используемых в RAM.
.1.3.6.1.4.1.2021.4.11.0	Общий объем доступной памяти (RAM + swap) (в кибибайтах).
.1.3.6.1.4.1.2021.4.12.0	Минимальный объем свободной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.13.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory).
.1.3.6.1.4.1.2021.4.14.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена.
.1.3.6.1.4.1.2021.4.15.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кешированной памяти.
.1.3.6.1.4.1.2021.4.16.0	Объем виртуальной памяти, занятый текстовыми страницами (в кибибайтах).
.1.3.6.1.4.1.2021.4.17.0	Объем физической памяти (RAM), занятый текстовыми страницами (в кибибайтах). Не выводится если операционная система не выделяет текстовые страницы от других используемых в RAM.
.1.3.6.1.4.1.2021.4.18.0	Объем виртуальной памяти на сетевом узле (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.3.0.

OID	Описание
.1.3.6.1.4.1.2021.4.19.0	Объем доступной виртуальной памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.4.0.
.1.3.6.1.4.1.2021.4.20.0	Объем физической памяти на сетевом узле (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.5.0.
.1.3.6.1.4.1.2021.4.21.0	Объем свободной физической памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.6.0.
.1.3.6.1.4.1.2021.4.22.0	Общий объем доступной памяти (RAM + swap) (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.11.0.
.1.3.6.1.4.1.2021.4.23.0	Минимальный объем свободной виртуальной памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.12.0.
.1.3.6.1.4.1.2021.4.24.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory). 64-битный аналог .1.3.6.1.4.1.2021.4.13.0.
.1.3.6.1.4.1.2021.4.25.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена. 64-битный аналог .1.3.6.1.4.1.2021.4.14.0.
.1.3.6.1.4.1.2021.4.26.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кешированной памяти. 64-битный аналог .1.3.6.1.4.1.2021.4.15.0.
.1.3.6.1.4.1.2021.4.27.0	Объем доступной памяти (в кибибайтах), доступный для запуска новых приложений без вымещения данных в swap.
.1.3.6.1.4.1.2021.4.100.0	Признак, что объем виртуальной памяти меньше минимально установленного значения.
.1.3.6.1.4.1.2021.4.101.0	Сообщение о том, что доступный объем виртуальной памяти меньше минимально установленного значения.

Таблица сведений о разделах (.1.3.6.1.4.1.2021.9.1)

B — индекс диска, присвоенный сетевым узлом

.1.3.6.1.4.1.2021.9.1.1.B	Индекс раздела (B).
.1.3.6.1.4.1.2021.9.1.2.B	Точка монтирования раздела.
.1.3.6.1.4.1.2021.9.1.3.B	Устройство (или tmpfs), на котором находится раздел.
.1.3.6.1.4.1.2021.9.1.4.B	Минимальный объем свободного места на разделе (в килобайтах) до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.5.B	Минимальный объем свободного места на разделе (в процентах) от общего до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.6.B	Общий объём раздела (в килобайтах).
.1.3.6.1.4.1.2021.9.1.7.B	Свободное место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.8.B	Занятое место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.9.B	Занятое место в разделе (в процентах).

OID	Описание
.1.3.6.1.4.1.2021.9.1.10.B	Процент использования инодов в разделе.
.1.3.6.1.4.1.2021.9.1.100.B	Флаг ошибки, сигнализирующий о том, что свободного места в разделе осталось меньше заданного значения .1.3.6.1.4.1.2021.9.1.4.B или .1.3.6.1.4.1.2021.9.1.5.B: • 0 — нет ошибки, • 1 — есть ошибка.
.1.3.6.1.4.1.2021.9.1.101.B	Сообщение об ошибке. Если параметр .1.3.6.1.4.1.2021.9.1.10.B равен 0, сообщение пустое.
.1.3.6.1.4.1.2021.9.1.11.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если раздел менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.6.B.
.1.3.6.1.4.1.2021.9.1.12.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если раздел менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.13.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если свободно менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.7.B.
.1.3.6.1.4.1.2021.9.1.14.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если свободно менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.15.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если занято менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.8.B.
.1.3.6.1.4.1.2021.9.1.16.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если занято менее 2ТБайт, параметр равен 0.

Таблица информации о средней загрузке системы за 1, 5, 15 минут (1.3.6.1.4.1.2021.10.1)

C — индекс, присвоенный сетевым узлом (постоянный):

- **1 — значение для 1 минуты,**
- **2 — значение для 5 минут,**
- **3 — значение для 15 минут**

.1.3.6.1.4.1.2021.10.1.1.C	Индекс значения средней загрузки: • 1 — 1 минута, • 2 — 5 минут, • 3 — 15 минут
.1.3.6.1.4.1.2021.10.1.2.C	Имя загрузки (по умолчанию: Load-1, Load-5, Load-15).
.1.3.6.1.4.1.2021.10.1.3.C	Средняя загрузка системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.4.C	Пороговое значение загрузки системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.5.C	Загрузка системы в процентах (в виде целого числа).

OID	Описание
.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.
.1.3.6.1.4.1.2021.10.1.0	Фиктивный индекс, всегда равен 1.
.1.3.6.1.4.1.2021.10.2.0	Фиктивное имя, всегда равно systemStats.
.1.3.6.1.4.1.2021.11.3.0	Среднее количество информации (в килобайтах), записанное на диск за минуту.
.1.3.6.1.4.1.2021.11.4.0	Среднее количество информации (в килобайтах), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.5.0	Среднее количество информации (в блоках данных), записанное на диск за минуту.
.1.3.6.1.4.1.2021.11.6.0	Среднее количество информации (в блоках данных), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.7.0	Среднее количество системных прерываний за минуту.
.1.3.6.1.4.1.2021.11.8.0	Среднее количество переключений контекста за минуту.
.1.3.6.1.4.1.2021.11.9.0	Процент времени, занятого пользовательскими процессами (за минуту).
.1.3.6.1.4.1.2021.11.10.0	Процент времени, когда процессор занят системными процессами (за минуту).
.1.3.6.1.4.1.2021.11.11.0	Процент времени, когда процессор не занят процессами (за минуту).
.1.3.6.1.4.1.2021.11.50.0	Количество тиков процессорного времени, затраченного на исполнения user-level code.
.1.3.6.1.4.1.2021.11.51.0	Количество тиков процессорного времени, затраченного на исполнение reduced-priority code.
.1.3.6.1.4.1.2021.11.52.0	Количество тиков процессорного времени, затраченного на исполнение system-level code.
.1.3.6.1.4.1.2021.11.53.0	Количество тиков процессорного времени, проведенного в состоянии idle.
.1.3.6.1.4.1.2021.11.54.0	Количество тиков процессорного времени, затраченного на исполнение ожидания ввода-вывода.
.1.3.6.1.4.1.2021.11.55.0	Количество тиков процессорного времени, затраченного на исполнение kernel-level code.
.1.3.6.1.4.1.2021.11.56.0	Количество тиков процессорного времени, затраченного на исполнение аппаратных прерываний.
.1.3.6.1.4.1.2021.11.57.0	Количество блоков, отправленное блочному устройству (диску).

OID	Описание
.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.
.1.3.6.1.4.1.2021.11.62.0	Количество блоков, помещенных в виртуальную память.
.1.3.6.1.4.1.2021.11.63.0	Количество блоков, извлеченных из виртуальной памяти.
.1.3.6.1.4.1.2021.11.64.0	Количество тиков процессорного времени, затраченного кодом гипервизора (если узел работает в виртуальной среде).
.1.3.6.1.4.1.2021.11.65.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре.
.1.3.6.1.4.1.2021.11.66.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре с пониженным приоритетом.
.1.3.6.1.4.1.2021.11.67.0	Количество ядер процессоров.
.1.3.6.1.4.1.2021.100.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.100.2.0	Ключевое слово CVS.
.1.3.6.1.4.1.2021.100.3.0	Строка времени из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.4.0	Строка времени из ctime.
.1.3.6.1.4.1.2021.100.5.0	Идентификатор из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.6.0	Опции конфигурации SNMP-агента.
.1.3.6.1.4.1.2021.101.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.101.2.0	Фиктивная строка, всегда равная snmp.
.1.3.6.1.4.1.2021.101.100.0	Признак ошибки SNMP-агента.
.1.3.6.1.4.1.2021.101.101.0	Описание ошибки SNMP-агента.

UCD-DISKIO-MIB

UCD-DISKIO-MIB (.1.3.6.1.4.1.2021.13.15) включает в себя объекты, предназначенные для получения информации о состоянии памяти и дискового пространства сетевого узла. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 37. SNMP-параметры. UCD-DISKIO-MIB

OID	Описание
Таблица значений текущих параметров оперативной памяти, виртуальной памяти, дискового пространства и их загрузки (.1.3.6.1.4.1.2021.13.15.1.1.)	
A — индекс таблицы	
.1.3.6.1.4.1.2021.13.15.1.1.1.A	Индекс таблицы (A).
.1.3.6.1.4.1.2021.13.15.1.1.2.A	Описание устройства, полученное от ОС. Для координатора принимает значения: ram0-ram15 loop0-loop7 sda, sda1, sda2, sdb1, sdb2, sdb3
.1.3.6.1.4.1.2021.13.15.1.1.3.A	Количество байт, считанных с устройства с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.4.A	Количество байт, записанных на устройство с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.5.A	Количество операций доступа к устройству на чтение.
.1.3.6.1.4.1.2021.13.15.1.1.6.A	Количество операций доступа к устройству на запись.
.1.3.6.1.4.1.2021.13.15.1.1.9.A	Средняя загрузка устройства за 1 минуту (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.10.A	Средняя загрузка устройства за 5 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.11.A	Средняя загрузка устройства за 15 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.12.A	Количество операций доступа к устройству на чтение. 64-разрядный параметр.
.1.3.6.1.4.1.2021.13.15.1.1.13.A	Количество байт, записанных на устройство с момента запуска. 64-разрядный параметр.
.1.3.6.1.4.1.2021.13.15.1.1.14.A	Время использования диска с момента запуска (в микросекундах).

NET-SNMP-MIB

NET-SNMP-MIB (1.3.6.1.4.1.8072) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 38. SNMP-параметры. NET-SNMP-MIB

OID	Описание
Таблица, содержащая все OID, зарегистрированные MIB-модулями в SNMP-агенте (.1.3.6.1.4.1.8072.1.2.1.1):	

OID	Описание
A – имя MIB-модуля	
B – OID MIB-модуля	
C – приоритет MIB-модуля	
.1.3.6.1.4.1.8072.1.2.1.1.4.A.B.C	Имя модуля, который зарегистрировал OID.
.1.3.6.1.4.1.8072.1.2.1.1.5.A.B.C	Биты, означающие режим работы OID.
.1.3.6.1.4.1.8072.1.2.1.1.6.A.B.C	Таймаут для модуля.
Таблица заскриптованных расширений (.1.3.6.1.4.1.8072.1.3.2.2.1):	
D – идентификатор расширения	
.1.3.6.1.4.1.8072.1.3.2.2.1.2.D	Путь к бинарному файлу или скрипту для запуска.
.1.3.6.1.4.1.8072.1.3.2.2.1.3.D	Аргументы для команды.
.1.3.6.1.4.1.8072.1.3.2.2.1.4.D	Стандартные вводные для команды.
.1.3.6.1.4.1.8072.1.3.2.2.1.5.D	Продолжительность времени, в течение которого результат выполнения команды кешируется (секунд).
.1.3.6.1.4.1.8072.1.3.2.2.1.6.D	Механизм запуска команды: • 1 — fork-and-exec, • 2 — run via a sub-shell.
.1.3.6.1.4.1.8072.1.3.2.2.1.7.D	Механизм исполнения команды: • 1 — run-on-read, • 2 — run-on-set, • 3 — run-command.
.1.3.6.1.4.1.8072.1.3.2.2.1.20.D	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.4.1.8072.1.3.2.2.1.21.D	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

OID	Описание
Таблица результатов выполнения скриптов (.1.3.6.1.4.1.8072.1.3.2.3.1):	
D – идентификатор расширения	
.1.3.6.1.4.1.8072.1.3.2.3.1.1.D	Первая строка в результате запуска команды.
.1.3.6.1.4.1.8072.1.3.2.3.1.2.D	Полный результат запуска команды одной строки.
.1.3.6.1.4.1.8072.1.3.2.3.1.3.D	Количество строк в результате запуска команды.
.1.3.6.1.4.1.8072.1.3.2.3.1.4.D	Значение, возвращенное командой.
Таблица результатов выполнения команды построчно (.1.3.6.1.4.1.8072.1.3.2.4.1):	
D – идентификатор расширения	
E – номер строки (с единицы)	
.1.3.6.1.4.1.8072.1.3.2.4.1.D.E	Единичная строка вывода команды.
.1.3.6.1.4.1.8072.1.5.1.0	Время, на которое кешируется значение OID по умолчанию (в секундах), если оно не задано в параметре .1.3.6.1.4.1.8072.1.5.3.1.2.F.
.1.3.6.1.4.1.8072.1.5.2.0	Статус кеширования: • 1 — включено, • 2 — выключено.
Таблица кешированных OID (.1.3.6.1.4.1.8072.1.5.3.1):	
F – OID, значение которого кешировано	
.1.3.6.1.4.1.8072.1.5.3.1.2.F	Время, на которое кешируется значение OID (в секундах).
.1.3.6.1.4.1.8072.1.5.3.1.3.F	Статус записи: • 1 (enabled) — включена, • 2 (disabled) — выключена, • 3 (empty) — пустая, • 4 (cached) — кешированная, • 5 (expired) — истекла.
1.3.6.1.4.1.8072.1.7.1.1.0	Статус режима debug SNMP-агента: • 1 — включен, • 2 — выключен.
.1.3.6.1.4.1.8072.1.7.1.2.0	Переключатель вывода для debug: • 1 — вывод всех значений, • 2 — фильтрация вывода. Для работы переключателя параметр .1.3.6.1.4.1.8072.1.7.1.1.0 должен быть равен 1.
.1.3.6.1.4.1.8072.1.7.1.3.0	Переключатель вывода сырого дампа пакетов: • 1 — включен, • 2 — выключен.

OID	Описание
Таблица результатов debug (.1.3.6.1.4.1.8072.1.7.1.4.1):	
G – префикс идентификатора	
.1.3.6.1.4.1.8072.1.7.1.4.4.G	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
Таблица форм вывода сообщений SNMP-агента (.1.3.6.1.4.1.8072.1.7.2.1.1):	
H – уровень важности событий:	
0 – emergency	
1 – alert	
2 – critical	
3 – error	
4 – warning	
5 – notice	
6 – info	
7 – debug	
I – идентификатор журнала	
.1.3.6.1.4.1.8072.1.7.2.1.1.3.H.I	Форма вывода сообщений для данной строки: • 1 — stdout, • 2 — stderr, • 3 — file, • 4 — syslog, • 5 — callback.
.1.3.6.1.4.1.8072.1.7.2.1.1.4.H.I	Максимальное значение, для которого применима данная строка: • 0 — emergency, • 1 — alert, • 2 — critical, • 3 — error, • 4 — warning, • 5 — notice, • 7 — debug.

OID	Описание
.1.3.6.1.4.1.8072.1.7.2.1.1.5.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
VACM таблица доступа сетевого узла (.1.3.6.1.4.1.8072.1.9.1.1.): **J – имя группы:** **K – префикс контекста доступа** **L – модель безопасности доступа** **M – уровень безопасности доступа** **N – способ аутентификации**	
.1.3.6.1.4.1.8072.1.9.1.1.2.J.K.L.M.N	Механизм выбора совпадений в VACM: • 1 — exact (полное совпадение), • 2 — prefix (совпадает префикс).
.1.3.6.1.4.1.8072.1.9.1.1.3.J.K.L.M.N	Значение секции ViewName.
.1.3.6.1.4.1.8072.1.9.1.1.4.J.K.L.M.N	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.4.1.8072.1.9.1.1.5.J.K.L.M.N	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-MPD-MIB

SNMP-MPD-MIB (.1.3.6.1.6.3.11) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 39. SNMP-параметры. SNMP-MPD-MIB

OID	Описание
.1.3.6.1.6.3.11.2.1.1.0	Количество полученных SNMP-пакетов, заблокированных по причине неподдерживаемой или неизвестной модели безопасности.
.1.3.6.1.6.3.11.2.1.2.0	Количество полученных SNMP-пакетов, заблокированных по причине ошибок в SNMP-сообщении.
.1.3.6.1.6.3.11.2.1.3.0	Количество полученных SNMP-пакетов, заблокированных по причине несоответствия pduType.

SNMP-TARGET-MIB

SNMP-TARGET-MIB (.1.3.6.1.6.3.12) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 40. 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 41. SNMP-параметры. SNMP-USER-BASED-SM-MIB

OID	Описание
.1.3.6.1.6.3.15.1.1.1.0	Количество заблокированных SNMP-пакетов по причине запроса неизвестного или недоступного уровня безопасности.
.1.3.6.1.6.3.15.1.1.2.0	Количество заблокированных SNMP-пакетов по причине появления вне определённого (доверенного) SNMP-агентом окна.
.1.3.6.1.6.3.15.1.1.3.0	Количество заблокированных SNMP-пакетов по причине использования неизвестного SNMP-агенту имени пользователя.
.1.3.6.1.6.3.15.1.1.4.0	Количество заблокированных SNMP-пакетов по причине обращения к неизвестному SNMP-агенту snmpEngineID.
.1.3.6.1.6.3.15.1.1.5.0	Количество заблокированных SNMP-пакетов по причине отсутствия ожидаемого значения digest value.
.1.3.6.1.6.3.15.1.1.6.0	Количество заблокированных SNMP-пакетов по причине невозможности их расшифровки.
.1.3.6.1.6.3.15.1.2.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицей .1.3.6.1.6.3.15.1.2.2.1.
Таблица параметров безопасности пользователя (.1.3.6.1.6.3.15.1.2.2.1):	
A – EngineID пользователя	
B – имя пользователя	
.1.3.6.1.6.3.15.1.2.2.1.3.A.B	Имя пользователя в формате модели безопасности.
.1.3.6.1.6.3.15.1.2.2.1.4.A.B	Ссылка на другую строку таблицы, в которой создана копия пользователя из текущей строки.
.1.3.6.1.6.3.15.1.2.2.1.5.A.B	Тип протокола аутентификации пользователя.
.1.3.6.1.6.3.15.1.2.2.1.8.A.B	Тип протокола конфиденциальности пользователя.
.1.3.6.1.6.3.15.1.2.2.1.11.A.B	Параметр для определения факта смены ключей пользователя.
.1.3.6.1.6.3.15.1.2.2.1.12.A.B	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.6.3.15.1.2.2.1.13.A.B	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-VIEW-BASED-ACM-MIB

SNMP-VIEW-BASED-ACM-MIB (.1.3.6.1.6.3.16) включает в себя объекты, предназначенные для получения информации о правах доступа к SNMP-параметрам.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 42. SNMP-параметры. SNMP-VIEW-BASED-ACM-MIB

OID	Описание
Таблица доступных контекстов сетевого узла (.1.3.6.1.6.3.16.1.1): **A – строка контекста**	
.1.3.6.1.6.3.16.1.1.1.A	Строка контекста.
Таблица групп доступа (.1.3.6.1.6.3.16.1.2.1): **B – модель безопасности** **C – имя безопасности**	
.1.3.6.1.6.3.16.1.2.1.3.B.C	Имя группы
.1.3.6.1.6.3.16.1.2.1.4.B.C	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.6.3.16.1.2.1.5.B.C	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
Таблица прав доступа к группам (.1.3.6.1.6.3.16.1.4.1): **D – имя группы** **E – контекст доступа** **F – модель безопасности** **G – уровень безопасности**	
.1.3.6.1.6.3.16.1.4.1.4.D.E.F.G	Формат совпадения: • 1 (exact) — полное совпадение, • 2 (prefix) — совпадает префикс.
.1.3.6.1.6.3.16.1.4.1.5.D.E.F.G	Имя view на просмотр.
.1.3.6.1.6.3.16.1.4.1.6.D.E.F.G	Имя view на запись.
.1.3.6.1.6.3.16.1.4.1.7.D.E.F.G	Имя view для уведомлений.
.1.3.6.1.6.3.16.1.4.1.8.D.E.F.G	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.4.1.9.D.E.F.G	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.6.3.16.1.5.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицами данного MIB.

OID	Описание
Таблица с параметрами view для семей поддеревьев (.1.3.6.1.6.3.16.1.5.2.1.):	
H – имя view	
I – поддерево	
.1.3.6.1.6.3.16.1.5.2.1.3.H.I	Маска, заданная для view.
.1.3.6.1.6.3.16.1.5.2.1.4.H.I	Тип view: • 1 — included, • 2 — excluded.
.1.3.6.1.6.3.16.1.5.2.1.5.H.I	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.5.2.1.6.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-FRAMEWORK-MIB

SNMP-FRAMEWORK-MIB (.1.3.6.1.6.3.10) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 43. SNMP-параметры. SNMP-FRAMEWORK-MIB

OID	Описание
.1.3.6.1.6.3.10.2.1.1.0	Идентификатор SNMP-engine.
.1.3.6.1.6.3.10.2.1.2.0	Количество инициализаций SNMP-engine после создания идентификатора.
.1.3.6.1.6.3.10.2.1.3.0	Время, прошедшее с последнего изменения количества инициализаций SNMP-engine (в секундах).

OID	Описание
.1.3.6.1.6.3.10.2.1.4.0	Максимальная длина входящего и исходящего SNMP-сообщения (в байтах).

VIPNET-MIB

VIPNET-MIB (.1.3.6.1.4.1.10812) включает в себя объекты, предназначенные для получения информации о параметрах сетевых узлов ViPNet. Для получения этой информации используется ветвь: `.iso.org.dod.internet.private.enterprises.infotecs.vipnet` (.1.3.6.1.4.1.10812.1).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 44. 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 HW (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.
.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.

OID	Описание
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.
.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 HW (.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.

OID	Описание
.1.3.6.1.4.1.10812.1.10.1.1.3.X	Значение параметра Serial number.

SNMP-агент ViPNet Coordinator HW может отправлять уведомления:

Таблица 45. 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.

VIPNETHW-MIB

VIPNETHW-MIB (.1.3.6.1.4.1.10812.13) включает в себя объекты, предназначенные для получения информации о службе внешнего управления remote_management. Для получения этой информации используется ветвь:
`.iso.org.dod.internet.private.enterprises.infotecs.infvipnetPolicy` (.1.3.6.1.4.1.10812.13).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 46. SNMP-параметры. VIPNETHW-MIB

OID	Описание
.1.3.6.1.4.1.10812.13.1	Последовательность объектов, описывающих политики в очереди.
.1.3.6.1.4.1.10812.13.1.1	Объекты, описывающие политики.
.1.3.6.1.4.1.10812.13.1.1.1.X	SNMP-индекс политики.

.1.3.6.1.4.1.10812.13.1.1.2.X	Тип политики: • Software; • License; • Firewall; • VPN; • DPI; • Services.
.1.3.6.1.4.1.10812.13.1.1.3.X	Время формирования политики в ViPNet Prime.
.1.3.6.1.4.1.10812.13.1.1.4.X	Время планового применения политики.

VIPNETFWLOAD-MIB

VIPNETFWLOAD-MIB (.1.3.6.1.4.1.10812.16) содержит объекты, предназначенные для мониторинга нагрузки ViPNet Coordinator HW.

SNMP-агент ViPNet Coordinator HW может отправлять оповещения типа TRAP:

Таблица 47. SNMP-оповещения. VIPNETFWLOAD-MIB

OID	Описание
.1.3.6.1.4.1.10812.16.0.1	Нагрузка на ЦП — повышенная
.1.3.6.1.4.1.10812.16.0.2	Нагрузка на ЦП — критическая
.1.3.6.1.4.1.10812.16.0.3	Нагрузка на ЦП — норма
.1.3.6.1.4.1.10812.16.0.4	Использование ОП — повышенное
.1.3.6.1.4.1.10812.16.0.5	Использование ОП — критическое
.1.3.6.1.4.1.10812.16.0.6	Использование ОП — норма
.1.3.6.1.4.1.10812.16.0.7	Количество активных сессий — повышенное
.1.3.6.1.4.1.10812.16.0.8	Количество активных сессий — критическое
.1.3.6.1.4.1.10812.16.0.9	Количество активных сессий — норма
.1.3.6.1.4.1.10812.16.0.10	Количество новых сессий в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.11	Количество новых сессий в секунду — критическое
.1.3.6.1.4.1.10812.16.0.12	Количество новых сессий в секунду — норма
.1.3.6.1.4.1.10812.16.0.13	Количество IP-пакетов в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.14	Количество IP-пакетов в секунду — критическое
.1.3.6.1.4.1.10812.16.0.15	Количество IP-пакетов в секунду — норма

OID	Описание
.1.3.6.1.4.1.10812.16.0.16	Объем трафика через МЭ — повышенный
.1.3.6.1.4.1.10812.16.0.17	Объем трафика через МЭ — критический
.1.3.6.1.4.1.10812.16.0.18	Объем трафика через МЭ — норма
.1.3.6.1.4.1.10812.16.0.19	Отношение объема трафика через МЭ к количеству IP-пакетов в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.20	Отношение объема трафика через МЭ к количеству IP-пакетов в секунду — критическое
.1.3.6.1.4.1.10812.16.0.21	Отношение объема трафика через МЭ к количеству IP-пакетов в секунду — норма
.1.3.6.1.4.1.10812.16.0.22	Количество SYN-запросов TCP в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.23	Количество SYN-запросов TCP в секунду — критическое
.1.3.6.1.4.1.10812.16.0.24	Количество SYN-запросов TCP в секунду — норма
.1.3.6.1.4.1.10812.16.0.25	Количество ICMP-запросов — повышенное
.1.3.6.1.4.1.10812.16.0.26	Количество ICMP-запросов — критическое
.1.3.6.1.4.1.10812.16.0.27	Количество ICMP-запросов — норма
.1.3.6.1.4.1.10812.16.0.28	Количество UDP-соединений со статусом UNREPLIED — повышенное
.1.3.6.1.4.1.10812.16.0.29	Количество UDP-соединений со статусом UNREPLIED — критическое
.1.3.6.1.4.1.10812.16.0.30	Количество UDP-соединений со статусом UNREPLIED — норма
.1.3.6.1.4.1.10812.16.0.31	Количество ошибок приема/передачи IP-пакетов — повышенное
.1.3.6.1.4.1.10812.16.0.32	Количество ошибок приема/передачи IP-пакетов — критическое
.1.3.6.1.4.1.10812.16.0.33	Количество ошибок приема/передачи IP-пакетов — норма
.1.3.6.1.4.1.10812.16.0.34	Количество отброшенных IP-пакетов — повышенное
.1.3.6.1.4.1.10812.16.0.35	Количество отброшенных IP-пакетов — критическое
.1.3.6.1.4.1.10812.16.0.36	Количество отброшенных IP-пакетов — норма
.1.3.6.1.4.1.10812.16.0.37	Нагрузка на HDD/SSD —повышенная
.1.3.6.1.4.1.10812.16.0.38	Нагрузка на HDD/SSD —критическая
.1.3.6.1.4.1.10812.16.0.39	Нагрузка на HDD/SSD —норма
.1.3.6.1.4.1.10812.16.0.40	Средняя нагрузка на ЦП (loadavg) — повышенная
.1.3.6.1.4.1.10812.16.0.41	Средняя нагрузка на ЦП (loadavg) — критическая
.1.3.6.1.4.1.10812.16.0.42	Средняя нагрузка на ЦП (loadavg) — норма
.1.3.6.1.4.1.10812.16.0.43	Загрузка свободной ОП — повышенная
.1.3.6.1.4.1.10812.16.0.44	Загрузка свободной ОП — критическая

OID	Описание
.1.3.6.1.4.1.10812.16.0.45	Загрузка свободной ОП — норма
.1.3.6.1.4.1.10812.16.0.46	Уровень доступной ОП — повышенный
.1.3.6.1.4.1.10812.16.0.47	Уровень доступной ОП — критический
.1.3.6.1.4.1.10812.16.0.48	Уровень доступной ОП — норма
.1.3.6.1.4.1.10812.16.0.52	Обнаружен источник повышенной сетевой нагрузки

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 48. 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 49. 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

Службы ПО ViPNet Coordinator HW

Службы ViPNet:

- `aad` — скрипт управления службой аутентификации и авторизации;
- `bonding` — скрипт управления модулем агрегирования сетевых интерфейсов;
- `conntrackd_tracker` — служба синхронизации сессий межсетевого экрана;
- `itcs_controld` — служба обработки запросов;
- `dgd` — скрипт управления службой `dgdd`;
- `drviplir` — драйвер перехвата сетевого трафика;
- `frr` — скрипт управления службой динамической маршрутизации `zebra`;
- `itcs-external-controld` — служба взаимодействия с ViPNet Prime;
- `failover` — скрипт управления службой `failoverd`;
- `failoverd` — служба системы защиты от сбоев;
- `healthmond` — служба мониторинга нагрузки;
- `l2overip` — драйвер прозрачного соединения сегментов сети на уровне L2;
- `iplircfg` — служба настройки драйвера перехвата сетевого трафика, ведения журнала IP-пакетов, обновления справочно-ключевой информации;
- `iplirpasswd` — утилита проверки паролей аудитора и администратора;
- `itcscrpt` — драйвер шифрования IP-пакетов;
- `itcskrniface` — драйвер перехвата сетевого трафика;
- `itcswd` — драйвер службы мониторинга системы;

- `mftp` — скрипт управления службой `mftpd`;
- `mftpd` — служба транспортного сервера MFTP;
- `network_journald` — служба работы с журналами IP-пакетов и сессий;
- `ntp_service` — скрипт управления службой NTP;
- `rvpn_shell` — командный интерпретатор ViPNet;
- `session_watcher` — служба, отслеживающая сессии пользователей ViPNet;
- `uc` — служба идентификации пользователей сети;
- `unmerge` — утилита распаковки дистрибутива справочников и ключей;
- `urlcatd` — служба управления URL-категориями;
- `vipnetsnmp` — служба SNMP;
- `vupgrade` — утилита обновления ПО ViPNet Coordinator HW;
- `webgui` (`webgui_captive_portal`, `webgui-fcgi-server`, `webgui_php`, `webgui_frontend`) — служба веб-интерфейса.

Службы Linux:

- `acpid` — служба обработки ACPI-событий;
- `crond` — служба запуска задач по расписанию;
- `conntrackd` — служба работы с сессиями межсетевого экрана;
- `dgdd` — служба проверки состояния удаленных шлюзов (DGD);
- `dhcpd` — служба DHCP-сервера;
- `dhcrelay` — служба агента-ретранслятора DHCP-запросов;
- `icap` — служба работы с ICAP-серверами;
- `licd` — служба лицензирования;
- `login` — служба аутентификации и открытия сессий;
- `named` — служба DNS;
- `ntpd` — служба NTP;
- `pcscd` — служба работы с токенами;
- `pppd` — службы управления соединениями точка-точка (только в исполнениях HW50 и HW100);
- `snmpd` — служба SNMP;
- `snort` — служба IPS/DPI;
- `sshd` — служба SSH;
- `sslsplit` — служба SSL/TLS-инспекции;
- `syslogd` — служба системного журнала;
- `ospfd` — служба OSPF-маршрутизации;

- `udhcpc` — служба DHCP-клиента;
- `upslog`, `upssched` — службы мониторинга и управления ИБП;
- `watchfrr` — служба управления службой динамической маршрутизации `frr`;
- `watchquagga` — служба управления службой динамической маршрутизации `quagga`;
- `vmunix` — ядро Linux;
- `xinetd` — служба запуска сетевых серверных процессов;
- `zebra` — динамической маршрутизации;
- `zdhcpd` — служба протокола DHCP для динамической маршрутизации.

G

Поддерживаемые приложения

Эти приложения вы можете указать в параметре `dpiapp <название приложения>` транзитного фильтра.

1 - 9

123VPN, 1kxun

A

AccuWeather, Activision Blizzard, AdobeConnect, Adult Content, Advertisement, Analytics and Tracking, AI Search, AirBnB, Akamai Cloud, Alibaba, AliExpress, AliPay, Amazon, Amazon Alexa, Amazon API Gateway, Amazon Cloud, Amazon Cloudfront, Amazon EC2, Amazon Prime Video, Amazon S3, Among Us, Ankama, AnyDesk, APNS, Apple Music, Apple Services, Apple Siri, Apple TV, Apteka.ru, Atlassian, Avast DNS, Avira Phantom VPN, Avito

B

Badoo, Blacknut, Bloomberg, Bluesky, Boosteroid, Brightcove, Browsec VPN, Bumble

C

CacheFly, CactusVPN, Canonical, CDNetworks, CDNvideo, Channel One, character.ai, ChatGPT, Citilink, Citrix, Claude, ClickHouse, Cloud Mail / VK WorkDisk, Cloudera Platform, Cloudflare, Cloudflare WARP, Cloudinary, CNN, CopyMonkey, Crashlytics, Criteo, CrossFire, Cybersec

D

Dailymotion, DashScope, DataSaver, DAZN, DeepSeek, Deezer, DigitalOcean, DingTalk, DirecTV, Discord, Disney Plus, DNS Shop, DNSCrypt, DoH/DoT, Dota 2, DotVPN, Dropbox

E

EA Games, eBay, Edgecast CDN, Elastic Search Cloud, Epic Games, Erstream, ESPN, ETM, Evernote

F

Facebook, Facebook Reels and Stories, Facebook VoIP, Fastly, Fortinet, FusionBrain, Fuze Meeting

G

GearUp Booster, Gemini, Genprokuratura, Gerwin, GigaChat, GigaCode, GitHub, GitLab, Gold Apple, Google, Google AI Studio, Google Analytics, Google Chat, Google Classroom, Google Cloud, Google Docs, Google Drive, Google Mail, Google Maps, Google Meet, Google Photos, Google Play, Google Shared Services, Google Trust Services, GoToMeeting, Guild Wars 2

H

HBO Now, Huawei Mobile Cloud, Huawei Services, Hugging Face, Hulu

I

iCloud, iFlix, iHeartRadio, Instagram, iOS App Store, Iqiyi, iTunes, Ivi-Ru

J

Jasper, Joom

K

Kakaotalk, Kaspersky Services, KeyCDN, Kick, Kinopoisk, Kontur Talk, Kuper

L

LagoFast, Lamoda, Last-fm, Leonardo.Ai, Life-Ru, Line, LinkedIn, LitRes-Ru, Livestream, LoL Wild Rift, Lumen Technologies, Lustre

M

M.Video-Eldorado, Maestro, Magnit Market, Mail-Ru, Mastodon, MAX, MCHS, MediaNova CDN, Megamarket, Messenger, Meta AI, Microsoft Azure, Microsoft Outlook, Microsoft Services, Microsoft Teams, MidJourney, Minimax Chat, Mining, mos.ru, Mozilla, MTS Link, MTS Services, MTS TV, Mudfish, Mullvad VPN, Mumble, MyOffice

N

Naver, NBC News, NBC Sports, Nest, NetEase Games, NetFlix, Nexon, NGenix, Nintendo Network, NoMachine, NordVPN, NotebookLM, Notion, Ntop, Nvidia GeForce NOW, Nvidia Services

O

OCS, Odnoklassniki, Office 365, Ollama, OneDrive, Ookla, OpenAI, OpenDNS, Opera VPN, Oracle Cloud Infrastructure (OCI), Oracle Services, Ozon

P

Paltalk, Pandora, Paramount Plus, Pastebin, Path of Exile, Pay-Rw, Perplexity, Petrovich, Pinterest, PlayStation Network, Pluralsight, Pochta Rossii, POPS, Private Internet Access, Proton VPN

Q

QQ, Qwen Chat

R

Rackspace Cloud, Radmin, reddit, Roblox, RoboGPT, Rockstar Games, Rudalle, Rumble, RUTUBE

S

Salesforce, Samokat, Samsung Max Privacy VPN, SberDisk, SecureVPN, SecureVPN-Pro, Shedevrum, Shein, Showtime, Signal, Signal VoIP, Sima-Land, Sina, Sina Weibo, SiriusXM, Slack, SMTPS, Snapchat, Snapchat Call, SoftEther, Sonos, SoundCloud, Speakchat, Spotify, Stability AI, Steam, Surfshark

T

Tailscale, Taobao, TeamViewer, Telegram, Temu, Tencent, Tencent Games, Tencent Video, Tesla Services, The Elder Scrolls Online, Threads, Tidal, TikTok, TOR, TrueConf Online, Tumblr, TuneIn Radio, TunnelBear, TurboText, Twitch

U

Ubiquity, unknown

V

Viber, Vimeo, ViPNet, Visper, Vivox, VK, VK Messenger, VK Teams, VK Video, VkusVill, Vse Instrumenty, Vudu

W

Wangsu CDN, Waze, Webex, WeChat, WhatsApp, WhatsApp Call, WhatsApp Files, Wikipedia, Wildberries, Windows Update, Windscribe, World of Warcraft

X

X (Twitter), X5 Services, XBOX, Xiaomi Services

Y

Yahoo Services, Yandex Alice, Yandex Browser Telemetry, Yandex Cloud, Yandex Direct, Yandex Disk, Yandex Docs, Yandex Eda-Delivery, Yandex Foundation Models, Yandex Lavka, Yandex Mail, Yandex Market, Yandex Messenger, Yandex Metrika, Yandex Music, Yandex Services, Yandex Telemost, Yandex Tracker, Youla, YouTube, YouTube Upload

Z

Zattoo, ZOOGVPN, Zoom



Поддерживаемые прикладные протоколы

Эти протоколы вы можете указать в параметре `dpiprotocol <название протокола>` транзитного фильтра.

A

AFP, Agora, AH IPSec, AliCloud Server, AMQP, Apache JServ, Apache Kafka, Armagetron, ATG, Avast Services

B

BACNET, Beckhoff ADS, BFCP, BFD, BGP, Bitcoin, BitTorrent, BJNP

C

Call of Duty Mobile, CAN, CAPWAP, Cassandra, Ceph, Check_MK, CNP over IP, CoAP, Collectd, Common Industrial Protocol, Corba, CPHA, CryNetwork

D

DCE RPC, DHCP, DHCPv6, Diameter, DICOM, DLEP, DNP3, DNS, DRDA, DTLS

E

EAQ, EasyWeather, eDonkey, EGD, EGP, Elasticsearch, ERSPAN, ESP IPSec, Ether-S-Bus, Ethereum, EtherNetIP, EtherSIO

F

FastCGI, FINS, FIX, FLUTE, FTP, FTP Data, FTPS

G

Gaijin Entertainment, Gearman, Geneve, Genshin Impact, Git, GLBP, Gnutella, Google Call, GRE, GTP

H

H323, Hamachi, HAProxy, HART-IP, HCL Notes, Heroes of the Storm, HiSLIP, HL7, HLS, HP VM Group Management, HSRP, HTTP, HTTP Connect, HTTP Proxy, HTTP/2

I

i3D, IAX, ICMP, ICMPv6, IEC 62056 (DLMS/COSEM), IEEE 1703, IEEE C37.118 Synchrophasor Protocol, IGMP, IMAP, IMAPS, IP in IP, IPlir4, IPlir6, IPP, IPsec, IRC, ISO 9506-1-2003 MMS

J

Jabber, Java RMI, JSON-RPC

K

KakaoTalk Voice, KCP, Kerberos, Kismet, KNXnet IP

L

LDAP, LDP, Line Call, Link-Local Multicast, LISP

M

Megaco, MELSEC, Memcached, Meraki Cloud, MGCP, Microsoft Delivery Optimization, Microsoft Teams Call, MikroTik NDP, Modbus, Monero, MongoDB, MPEG, MPEG-DASH, MPLS, MQTT, MS SQL TDS, MS-RPCH, MulticastDNS, Munin, MySQL

N

Nano, NAT-PMP, NATS, NetBIOS, NetFlow, New Office Environment, NFS, NTP

O

OCSP, OICQ, OPC UA, OpenFlow, OpenVPN, OpenWire, Oracle Database, OSPF

P

PFCP, PGM, PIM, POP, PostgreSQL, PPTP, Protocol Buffers, PTPv2

Q

QUIC

R

RADIUS, RAFT, RakNet, RDP, RESP, Riot Games, RIPE Atlas, RMCP, Roughtime, RSH, Rsync, RTCP, RTMP, RTP, RTPS, RTSP, Rx

S

S7comm, S7comm Plus, Samsung SDP, SCADA, SCTP, sFlow, SIP, Skinny, SLP, SMB v2/3, SMB/CIFS, SMPP, SMTP, SNMP, SOAP, Socks, SOME/IP, Source Engine, SSDP, SSH, SSL, STOMP, STUN, Syncthing, Syslog

T

TeamSpeak, Telegram Call, Telnet, Teredo, TFTP, Threema, Thrift, Tinc, TivoConnect, Toca Boca, TP-Link SHP, TRDP, TriStation, TrueConf, Tuya LAN, TZSP

U

UBNTAC2, UFTP, UMAS, unknown, Usenet

V

Valve SDR, Viber Call, VNC, VPN Kontinent, VRRP, VXLAN

W

Warcraft 3, WebDAV, WebSocket, WHOIS, WireGuard, WS-Discovery

X

XDMCP

Y

Yojimbo

Z

Z39.50, Zabbix, Zug

Поддерживаемые группы приложений

Эти группы приложений вы можете указать в параметре `dpigroup <группа приложений>` транзитного фильтра (см. Создание и изменение сетевых фильтров).

Advertisement and Analytic Services

Приложения в группе:

`Advertisement, Analytics And Tracking, Criteo, Google Analytics, Yandex Browser Telemetry, Yandex Direct, Yandex Metrika`

App-Stores and OS Updates

Приложения в группе:

`Google Play, iOS App Store, Windows Update`

Связанные протоколы:

`Microsoft Delivery Optimization`

Artificial Intelligence

Приложения в группе:

`AI Search, Amazon Alexa, Apple Siri, character.ai, ChatGPT, Claude, CopyMonkey, DashScope, DeepSeek, FusionBrain, Gemini, Gerwin, GigaChat, GigaCode, Google AI Studio, Hugging Face, Jasper, Leonardo.Ai, Maestro, Meta AI, MidJourney, Minimax Chat, NotebookLM, Ollama, OpenAI, Perplexity, Qwen Chat, RoboGPT, Rudalle, Shedevrum, Stability AI, TurboText, Visper, Yandex Alice, Yandex Foundation Models`

Audio Entertainment

Приложения в группе:

Apple Music, Deezer, iHeartRadio, Last-fm, Pandora, SiriusXM, Sonos, SoundCloud, Spotify, Tidal, TuneIn Radio, Yandex Music

Books and Magazines

Приложения в группе:

LitRes-Ru

Browsers

Приложения в группе:

Mozilla

Business

Приложения в группе:

Atlassian, Evernote, Google Docs, Google Trust Services, MyOffice, Notion, Nvidia Services, Office 365, Yandex Docs, Yandex Tracker

Связанные протоколы:

DICOM, HL7, Zug

Cloud and CDN Services

Приложения в группе:

Akamai Cloud, Amazon API Gateway, Amazon Cloud, Amazon Cloudfront, Amazon EC2, Amazon S3, Brightcove, CacheFly, Canonical, CDNetworks, CDNvideo, Cloudera Platform, Cloudflare, Cloudinary, DigitalOcean, Edgecast CDN, Erstream, Fastly, Google Cloud, Huawei Mobile Cloud, KeyCDN, Lumen Technologies, MediaNova CDN, Microsoft Azure, NGenix, Oracle Cloud Infrastructure (OCI), Oracle Services, Rackspace Cloud, Wangsu CDN, Yandex Cloud

Связанные протоколы:

Ceph

Conference

Приложения в группе:

AdobeConnect, Discord, Fuze Meeting, Google Meet, GoToMeeting, Kontur Talk, Microsoft Teams, MTS Link, Slack, Speakchat, TrueConf Online, Webex, Yandex Telemost, Zoom

Связанные протоколы:

BFCP, HCL Notes, TrueConf

Cryptocurrency

Приложения в группе:

Mining

Связанные протоколы:

Bitcoin, Ethereum, Monero, Nano

Database

Приложения в группе:

ClickHouse, Elastic Search Cloud

Связанные протоколы:

Cassandra, DRDA, Elasticsearch, Memcached, MongoDB, MS SQL TDS, MySQL, Oracle Database, PostgreSQL

Development Tools and Services

Приложения в группе:

Crashlytics, GitHub, GitLab, Salesforce

Связанные протоколы:

Apache Kafka

Device Security

Приложения в группе:

Avast DNS, Cybersec, Kaspersky Services

Связанные протоколы:

Avast Services

E-Commerce

Приложения в группе:

AliExpress, Amazon, Apteka.ru, Avito, Citilink, DNS Shop, eBay, ETM, Gold Apple, Joom, Kuper, Lamoda, M.Video-Eldorado, Magnit Market, Megamarket, Ozon, Petrovich, Samokat, Shein, Sima-Land, Taobao, Temu, VkusVill, Vse Instrumenty, Wildberries, X5 Services, Yandex Eda-Delivery, Yandex Lavka, Yandex Market, Youla

Education

Приложения в группе:

Google Classroom, Pluralsight, Wikipedia

Encrypted

Связанные протоколы:

DTLS, QUIC, SSL

Enterprise Services

Приложения в группе:

Alibaba, Apple Services, Citrix, Google Shared Services, Huawei Services, Microsoft Services, MTS Services, Tesla Services, Xiaomi Services, Yandex Services

Filetransfer

Приложения в группе:

Cloud Mail / VK WorkDisk, Dropbox, Google Drive, Google Photos, iCloud, Lustre, OneDrive, Pastebin, SberDisk, WhatsApp Files, Yandex Disk

Связанные протоколы:

AFP, FLUTE, FTP, FTP Data, FTPS, NFS, Rsync, SMB v2/3, SMB/CIFS, Syncthing, TFTP, UFTP, WebDAV

Finance

Приложения в группе:

Pay-Rw

Связанные протоколы:

FIX

Gaming

Приложения в группе:

Activision Blizzard, Among Us, Ankama, Blacknut, Boosteroid, CrossFire, Dota 2, EA Games, Epic Games, GearUp Booster, Guild Wars 2, LagoFast, LoL Wild Rift, NetEase Games, Nexon, Nintendo Network, Nvidia GeForce NOW, Path of Exile, PlayStation Network, Roblox, Rockstar Games, Steam, Tencent Games, The Elder Scrolls Online, World of Warcraft, XBOX

Связанные протоколы:

Armagetron, Call of Duty Mobile, CryNetwork, Gaijin Entertainment, Genshin Impact, Heroes of the Storm, i3D, RakNet, Riot Games, Source Engine, Toca Boca, Valve SDR, Warcraft 3, Yojimbo

Generic

Приложения в группе:

unknown

Связанные протоколы:

unknown

Government

Приложения в группе:

Genprokuratura, MCHS, mos.ru, Pochta Rossii

Industrial

Связанные протоколы:

BACNET, Beckhoff ADS, CAN, CNP over IP, Common Industrial Protocol, DNP3, EGD, Ether-S-Bus, EtherNetIP, EtherSIO, FINS, HART-IP, IEC 62056 (DLMS/COSEM), IEEE 1703, IEEE C37.118 Synchrophasor Protocol, ISO 9506-1-2003 MMS, KNXnet IP, Modbus, RTPS, S7comm, S7comm Plus, SCADA, UMAS

M2M and IoT

Приложения в группе:

Nest

Связанные протоколы:

AMQP, ATG, CoAP, EasyWeather, MELSEC, MQTT, NATS, OPC UA, OpenWire, TP-Link SHP, TRDP, TriStation, Tuya LAN

Mail

Приложения в группе:

Google Mail, Mail-Ru, Microsoft Outlook, POPS, SMTPS, Yandex Mail

Связанные протоколы:

IMAP, IMAPS, POP, SMTP

Messaging

Приложения в группе:

APNS, DingTalk, Google Chat, Kakaotalk, Line, MAX, Messenger, Paltalk, QQ, Signal, Snapchat, Telegram, Viber, VK Messenger, VK Teams, WeChat, WhatsApp, Yandex Messenger

Связанные протоколы:

IRC, Jabber, OICQ, SMPP, STOMP, Threema, Usenet

Navigation

Приложения в группе:

2Gis, Google Maps, Waze

Network Management

Приложения в группе:

DNSCrypt, DoH/DoT, Ntop, Ookla, OpenDNS, Ubiquity

Связанные протоколы:

AliCloud Server, Apache JServ, BFD, BGP, BJNP, CAPWAP, Check_MK, Collectd, Corba, CPHA, DHCP, DHCPv6, Diameter, DLEP, DNS, EGP, FastCGI, Git, GLBP, HP VM Group Management, HSRP, ICMP, ICMPv6, IGMP, IPP, KCP, Kerberos, Kismet, LDAP, LDP, Link-Local Multicast, LISP, Megaco, Meraki Cloud, MikroTik NDP, MulticastDNS, Munin, NAT-PMP, NetBIOS, NetFlow, NTP, OCSP, OpenFlow, OSPF, PFCP, PGM, PIM, Protocol Buffers, PTPv2, RADIUS, RAFT, RESP, RIPE Atlas, Roughtime, RSH, Rx, Samsung SDP, SCTP, sFlow, SLP, SNMP, SOME/IP, SSDP, Syslog, Thrift, Tinc, TivoConnect, UBNTAC2, VRRP, VXLAN, WHOIS, WS-Discovery, Z39.50, Zabbix

News

Приложения в группе:

AccuWeather, Bloomberg, CNN, Life-Ru, NBC News

Peer to Peer

Связанные протоколы:

BitTorrent, eDonkey, Gnutella

Pornography

Приложения в группе:

Adult Content

Remote Control

Приложения в группе:

AnyDesk, NoMachine, Radmin, TeamViewer

Связанные протоколы:

DCE RPC, Gearman, HiSLIP, Java RMI, JSON-RPC, MS-RPCH, RDP, RMCP, SOAP, SSH, Telnet, VNC, XDMCP

Social

Приложения в группе:

Badoo, Bluesky, Bumble, Facebook, Facebook Reels and Stories, Instagram, LinkedIn, Mastodon, Odnoklassniki, Pinterest, reddit, Sina, Sina Weibo, Threads, TikTok, Tumblr, VK, X (Twitter)

Streaming

Приложения в группе:

1kxun, Amazon Prime Video, Apple TV, Channel One, Dailymotion, DAZN, DirecTV, Disney Plus, ESPN, HBO Now, Hulu, iFlix, Iqiyi, iTunes, Ivi-Ru, Kick, Kinopoisk, Livestream, MTS TV, NBC Sports, NetFlix, OCS, Paramount Plus, Rumble, RUTUBE, Showtime, Tencent Video, Twitch, Vimeo, VK Video, Vudu, YouTube, YouTube Upload, Zattoo

Связанные протоколы:

Agora, HLS, MPEG, MPEG-DASH, RTCP, RTMP, RTP, RTSP

Travel and Transportation

Приложения в группе:

AirBnB

Tunnel

Приложения в группе:

123VPN, Avira Phantom VPN, Browsec VPN, CactusVPN, Cloudflare WARP, DotVPN, Fortinet, Mudfish, Mullvad VPN, NordVPN, Opera VPN, Private Internet Access, Proton VPN, Samsung Max Privacy VPN, SecureVPN, SecureVPN-Pro, SoftEther, Surfshark, Tailscale, TOR, TunnelBear, ViPNet, Windscribe, ZOOGVPN

Связанные протоколы:

AH IPSec, ERSPAN, ESP IPSec, Geneve, GRE, GTP, Hamachi, HTTP Connect, HTTP Proxy, IP in IP, IPlir4, IPlir6, IPsec, MPLS, OpenVPN, PPTP, Socks, Teredo, TZSP, VPN Kontinent, WireGuard

Voice over IP

Приложения в группе:

Facebook VoIP, Mumble, Signal VoIP, Snapchat Call, Vivox, WhatsApp Call

Связанные протоколы:

EAQ, Google Call, H323, IAX, KakaoTalk Voice, Line Call, MGCP, Microsoft Teams Call, New Office Environment, SIP, Skinny, STUN, TeamSpeak, Telegram Call, Viber Call

Wallet

Приложения в группе:

AliPay

Web

Приложения в группе:

DataSaver, Google, Naver, Tencent, Yahoo Services

Связанные протоколы:

HAProxy, HTTP, HTTP/2, WebSocket

J

Особенности фильтрации по приложениям и прикладным протоколам

Для ряда приложений и прикладных протоколов, которые вы можете задать при создании транзитных фильтров, существуют следующие особенности:

- Фильтр с заданным протоколом MySQL обрабатывает трафик для версии MySQL 5.6 и выше.
- Чтобы разрешить трафик Aliexpress, создайте разрешающий фильтр с указанием приложений Aliexpress и Alibaba.
- Запрещающий фильтр по приложению Alibaba также будет блокировать трафик сайта Aliexpress.
- Приложение Kontur Talk использует в своей работе Yandex Services. Поэтому в разрешающий фильтр для приложения Kontur Talk также добавляйте приложение Yandex Services.

  Если вы хотите разрешить трафик Kontur Talk и запретить трафик одного из приложений Яндекс, создайте:

  - разрешающий фильтр для приложения Kontur Talk;
  - запрещающий фильтр для приложения Яндекс;
  - разрешающий фильтр для Yandex Services.
- Чтобы разрешить трафик любого из приложений Яндекс, создайте разрешающий фильтр для самого приложения Яндекс и для приложения Yandex Services.
- Чтобы разрешить трафик любого из приложений Google, создайте разрешающий фильтр для самого приложения Google и для приложения Google Services.

- Для корректной работы программ и сервисов из группы приложений Gaming, создайте разрешающий фильтр для этой группы и для группы Cloud and CDN Services.
- Чтобы разрешить трафик VK Video, создайте разрешающий фильтр для приложений VK Video, VK и Odnoklassniki.
- Чтобы разрешить трафик VK Messenger, создайте разрешающий фильтр для приложений VK Messenger и VK.
- Чтобы разрешить трафик Cloud Mail / VK WorkDisk, создайте разрешающий фильтр для приложений Cloud Mail / VK WorkDisk, VK и Mail-Ru.
- Чтобы разрешить трафик VK Teams, создайте разрешающий фильтр для приложений VK Teams, VK и Mail-Ru.

K

Поддерживаемые MIME-типы

- **Application — Внутренний формат прикладной программы**
  - application/atom+xml: Atom
  - application/EDI-X12: EDI X12 (RFC 1767)
  - application/EDIFACT: EDI EDIFACT (RFC 1767)
  - application/json: JavaScript Object Notation JSON (RFC 4627)
  - application/javascript: JavaScript (RFC 4329)
  - application/octet-stream: двоичный файл без указания формата (RFC 2046)
  - application/ogg: Ogg (RFC 5334)
  - application/pdf: Portable Document Format, PDF (RFC 3778)
  - application/postscript: PostScript (RFC 2046)
  - application/soap+xml: SOAP (RFC 3902)
  - application/font-woff: Web Open Font Format
  - application/xhtml+xml: XHTML (RFC 3236)
  - application/xml-dtd: DTD (RFC 3023)
  - application/xop+xml: XOP
  - application/zip: ZIP
  - application/gzip: Gzip
  - application/x-bittorrent: BitTorrent

- application/x-tex: TeX

- **audio — Аудио**
  - audio/basic: mulaw аудио, 8 кГц, 1 канал (RFC 2046)
  - audio/L24: 24-bit Linear PCM аудио, 8-48 кГц, 1-N каналов (RFC 3190)
  - audio/mp4: MP4
  - audio/aac: AAC
  - audio/mpeg: MP3 или др. MPEG (RFC 3003)
  - audio/ogg: Ogg Vorbis, Speex, Flac или др. аудио (RFC 5334)
  - audio/vorbis: Vorbis (RFC 5215)
  - audio/x-ms-wma: Windows Media Audio
  - audio/x-ms-wax: Windows Media Audio перенаправление
  - audio/vnd.rn-realaudio: RealAudio
  - audio/vnd.wave: WAV (RFC 2361)
  - audio/webm: WebM
- **image — Изображение**
  - image/gif: GIF (RFC 2045 и RFC 2046)
  - image/jpeg: JPEG (RFC 2045 и RFC 2046)
  - image/pjpeg: JPEG
  - image/png: Portable Network Graphics (RFC 2083)
  - image/svg+xml: SVG
  - image/tiff: TIFF (RFC 3302)
  - image/vnd.microsoft.icon: ICO
  - image/vnd.wap.wbmp: WBMP
- **message — Сообщение**
  - message/http: (RFC 2616)
  - message/imdn+xml: IMDN (RFC 5438)
  - message/partial: E-mail (RFC 2045 и RFC 2046)
  - message/rfc822: E-mail; EML файлы, MIME файлы, MHT файлы, MHTML файлы (RFC 2045 и RFC 2046)
- **model — Для 3D моделей**
  - model/example: (RFC 4735)
  - model/iges: IGS файлы, IGES файлы (RFC 2077)
  - model/mesh: MSH файлы, MESH файлы (RFC 2077), SILO файлы

- model/vrml: WRL файлы, VRML файлы (RFC 2077)
- model/x3d+binary: X3D ISO стандарт для 3D компьютерной графики, X3DB файлы
- model/x3d+vrml: X3D ISO стандарт для 3D компьютерной графики, X3DV VRML файлы
- model/x3d+xml: X3D ISO стандарт для 3D компьютерной графики, X3D XML файлы

- **multipart — Составные файлы**
  - multipart/form-data: MIME Webform (RFC 2388)
  - multipart/signed: (RFC 1847)
  - multipart/encrypted: (RFC 1847)
  - multipart/mixed: MIME E-mail (RFC 2045 и RFC 2046)
  - multipart/alternative: MIME E-mail (RFC 2045 и RFC 2046)
  - multipart/related: MIME E-mail (RFC 2387 и используемое MHTML (HTML mail))
- **text — Текст**
  - text/cmd: команды
  - text/css: Cascading Style Sheets (RFC 2318)
  - text/csv: CSV (RFC 4180)
  - text/html: HTML (RFC 2854)
  - text/javascript (Obsolete): JavaScript (RFC 4329)
  - text/plain: текстовые данные (RFC 2046 и RFC 3676)
  - text/php: Скрипт языка PHP
  - text/xml: Extensible Markup Language (RFC 3023)
- **video — Видео**
  - video/mpeg: MPEG-1 (RFC 2045 и RFC 2046)
  - video/mp4: MP4 (RFC 4337)
  - video/ogg: Ogg Theora или другое видео (RFC 5334)
  - video/quicktime: QuickTime
  - video/webm: WebM
  - video/x-ms-wmv: Windows Media Video
  - video/x-flv: FLV
  - video/3gpp: .3gpp .3gp
  - video/3gpp2: .3gpp2 .3g2
- **vnd — Вендорные файлы**
  - application/vnd.oasis.opendocument.text: OpenDocument
  - application/vnd.oasis.opendocument.spreadsheet: OpenDocument

- application/vnd.oasis.opendocument.presentation: OpenDocument
- application/vnd.oasis.opendocument.graphics: OpenDocument
- application/vnd.ms-excel: Microsoft Excel файлы
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet: Microsoft Excel 2007 файлы
- application/vnd.ms-powerpoint: Microsoft Powerpoint файлы
- application/vnd.openxmlformats-officedocument.presentationml.presentation: Microsoft Powerpoint 2007 файлы
- application/msword: Microsoft Word файлы
- application/vnd.openxmlformats-officedocument.wordprocessingml.document: Microsoft Word 2007 файлы
- application/vnd.mozilla.xul+xml: Mozilla XUL файлы
- application/vnd.google-earth.kml+xml: KML файлы (например, для Google Earth)

- **x — Нестандартные файлы**
  - application/x-www-form-urlencoded: Form Encoded Data
  - application/x-dvi: DVI
  - application/x-latex: LaTeX файлы
  - application/x-font-ttf: TrueType (незарегистрированный MIME-тип, но наиболее часто используемый)
  - application/x-shockwave-flash: Adobe Flash
  - application/x-stuffit: StuffIt
  - application/x-rar-compressed: RAR
  - application/x-tar: Tarball
  - text/x-jquery-tmpl: jQuery
  - application/x-javascript
- **x-pkcs — PKCS**
  - application/x-pkcs12: p12 файлы
  - application/x-pkcs12: pfx файлы
  - application/x-pkcs7-certificates: p7b файлы
  - application/x-pkcs7-certificates: spc файлы
  - application/x-pkcs7-certreqresp: p7r файлы
  - application/x-pkcs7-mime: p7c файлы
  - application/x-pkcs7-mime: p7m файлы
  - application/x-pkcs7-signature: p7s файлы



Формат указания IP-адресов и портов в правилах IPS

Диапазон IPv4-адресов в правилах IPS задается указанием маски подсети в формате CIDR.

Примеры:

- `172.16.0.2/16`
- `192.168.0.0/8`

Особенности указания IP-адресов при настройке параметров правил и работе с ними:

- Для указания IP-адресов могут быть использованы переменные.

  Примеры:

  - `$HOME_NET` — IP-адреса защищаемой сети.
  - `$EXTERNAL_NET` — IP-адреса внешних сетей.

  Перечень всех доступных переменных с указанием присвоенных по умолчанию значений см. в приложении Параметры правил IPS по умолчанию.

- Для указания IP-адресов, которые необходимо исключить из указанного диапазона, применяется восклицательный знак.

  Примеры:

  - `!$HOME_NET`
  - `!192.168.0.100`

- Для указания нескольких диапазонов и/или одиночных IP-адресов разделяйте их запятыми.

  Пример: `10.10.20.0/24,!10.10.20.1`

Внимание! При указании нескольких диапазонов и/или одиночных IP-адресов не используйте противоречивые выражения:



- логические противоречия, например: `1.1.1.1,!1.1.1.1`;
- бессмысленные отрицания, например: `1.1.1.0,!1.1.0.0/16`.

Правила IPS не будут применены до исправления всех противоречий. О наличии противоречий свидетельствует появление сообщения «Ошибка валидации базы IPS перед применением обновлений» при попытке применить правила.

Особенности указания портов при настройке параметров правил и работе с правилами:

- Для указания диапазона портов разделяйте начальное и конечное значение двоеточием.

  Пример: `20:27`

- Для указания диапазона портов от начального значения до порта 65535 поставьте двоеточие после начального значения.

  Пример: `20:`

- Для указания диапазона портов от порта 0 до конечного значения поставьте двоеточие перед конечным значением.

  Пример: `:20`

- Для указания портов могут быть использованы переменные.

  Пример:

  - `$SSH_PORTS` — открытые (доступные) порты SSH-серверов.

  Перечень всех доступных переменных с указанием присвоенных по умолчанию значений см. в приложении Параметры правил IPS по умолчанию.

- Для указания портов, которые необходимо исключить из указанного диапазона, применяется восклицательный знак.

  Пример: `!22`

- Для указания нескольких портов и/или диапазонов портов разделяйте их запятыми.

  Пример: `40:60,!50,80,81,593:`

Внимание! При указании нескольких диапазонов и/или одиночных портов, не используйте противоречивые выражения, такие как:



- логические противоречия, например: `80,!80`
- номера портов (или переменные, задающие номера), используемые как IP-адрес.

Правила IPS не будут применены до исправления всех противоречий. О наличии противоречий свидетельствует появление сообщения "Ошибка валидации базы IPS перед применением обновлений" при попытке применить правила.

M

Параметры правил IPS по умолчанию

Для параметров $HTTP_PORTS и $AIM_SERVERS допустимое количество значений 1–100. Для остальных параметров правил IPS допустимое количество значений 1–10.

Ниже в таблицах приведены значения по умолчанию для параметров сетей и доверенных ресурсов защищаемой сети.

Таблица 50. Параметры сетей

Параметр	Переменная	Допустимые значения	Значение по умолчанию
Список защищаемых сетей	$HOME_NET	**IP адрес/префикс**, например: 10.0.0.0/16	192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12
Список внешних сетей	$EXTERNAL_NET	**IP адрес/префикс**, например: 10.0.0.0/16 **Переменные:** $HOME_NET	!$HOME_NET

Таблица 51. Параметры доверенных ресурсов защищаемой сети (IP-адреса и (или) номера портов)

Параметр	Переменная	Допустимые значения	Значение по умолчанию
Перечень IP-адресов доверенных SSH-серверов	$SSH_SERVERS	**IP-адрес**, например: 10.10.10.1	$HOME_NET

Параметр	Переменная	Допустимые значения	Значение по умолчанию
		Диапазон адресов: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET	
Перечень доступных (открытых) портов SSH-серверов	$SSH_PORTS	**Номер порта**, например: 22 **Диапазон портов**: например: 8080:8088	22
Перечень IP-адресов доверенных веб-серверов	$HTTP_SERVERS	**IP-адрес**, например: 10.10.10.1 **Диапазон адресов**: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET, $SSH_SERVERS	$HOME_NET
Перечень портов, используемых при передаче данных по протоколу HTTP	$HTTP_PORTS	**Номер порта**, например: 80 **Диапазон портов**: например: 8080:8088	80, 81, 311, 383, 591, 593, 901, 1220, 1414, 1741, 1830, 2301, 2381, 2809, 3128, 3702, 4343, 4848, 5250, 7001, 7145, 7510, 7777, 7779, 8000, 8008, 8014, 8028, 8080, 8088, 8090, 8118, 8123, 8180, 8181, 8243, 8280, 8300, 8800, 8888, 8899, 9000, 9060, 9080, 9090, 9091, 9443, 9999, 11371, 50002, 55555
Перечень IP-адресов доверенных FTP-серверов	$FTP_SERVERS	**IP-адрес**, например: 10.10.10.1 **Диапазон адресов**: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET, $SSH_SERVERS	$HOME_NET
Перечень доступных (открытых) портов FTP-серверов	$FTP_PORTS	**Номер порта**, например: 21 **Диапазон портов**, например: 8080:8088	20, 21, 2100, 3535
Перечень IP-адресов доверенных SIP-серверов	$SIP_SERVERS	**IP-адрес**, например: 10.10.10.1 **Диапазон адресов**: <IP-адрес	$HOME_NET

Параметр	Переменная	Допустимые значения	Значение по умолчанию
		1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET	
Перечень доступных (открытых) портов SIP-серверов	$SIP_PORTS	**Номер порта**, например: 5060 **Диапазон портов**, например: 8080:8088	5060, 5061, 5600
Перечень IP-адресов доверенных DNS-серверов	$DNS_SERVERS	**IP-адрес**, например: 10.10.10.1 **Диапазон адресов**: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET	$HOME_NET
Перечень IP-адресов доверенных SMTP-серверов	$SMTP_SERVERS	**IP-адрес**, например: 10.10.10.1 **Диапазон адресов**: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET	$HOME_NET
Перечень IP-адресов доверенных SQL-серверов	$SQL_SERVERS	**IP-адрес**, например: 10.10.10.1 **Диапазон адресов**: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET	$HOME_NET
Перечень IP-адресов доверенных TELNET-серверов	$TELNET_SERVERS	**IP-адрес**, например: 10.10.10.1 **Диапазон адресов**: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET, $EXTERNAL_NET, $SSH_SERVERS, $HTTP_SERVERS, $FTP_SERVERS	$HOME_NET
Перечень доверенных AOL Instant Messenger (AIM)-серверов	$AIM_SERVERS	**IP-адрес**, например: 10.10.10.1 **Ip адрес/префикс**, например: 10.0.0.0/16 **Диапазон адресов**: <IP-адрес 1>-<IP-адрес 2> **Переменные:** $HOME_NET,	64.12.24.0/23, 64.12.28.0/23, 64.12.161.0/24, 64.12.163.0/24, 64.12.200.0/24, 205.188.3.0/24, 205.188.5.0/24, 205.188.7.0/24,

Параметр	Переменная	Допустимые значения	Значение по умолчанию
		$EXTERNAL_NET, $SSH_SERVERS	205.188.9.0/24, 205.188.153.0/24, 205.188.179.0/24, 205.188.248.0/24
Перечень портов для передачи произвольного кода	$SHELLCODE_PORTS	**Номер порта**, например: 22 **Диапазон портов**, например: 8080:8088 **Переменные:** $SSH_PORTS, $HTTP_PORTS, $FTP_PORTS, $SIP_PORTS	!80
Перечень доступных (открытых) портов баз данных ORACLE	$ORACLE_PORTS	**Номер порта**, например: 1024 **Диапазон портов**, например: 8080:8088	1024
Перечень портов для передачи файловых данных	$FILE_DATA_PORTS	**Номер порта**, например: 110 **Диапазон портов**, например: 8080:8088 **Переменные:** $HTTP_PORTS, $FTP_PORTS	$HTTP_PORTS, 110, 143
Перечень GTP-портов для GTP-препроцессора	$GTP_PORTS	**Номер порта**, например: 22 **Диапазон портов**, например: 8080:8088	2123, 2152, 3386

N

Группы правил IPS

Таблица 52. Группы правил предупреждения вторжений

Название группы	Что выявляет группа правил
activex	Вызов функции ActiveX
attack_response	Ответ сетевого узла, который выглядит как ответ узла, подверженного вторжению
current_events	Сигнатуры с малым сроком действия обнаруживают угрозы, актуальные на данный момент. Теряют актуальность в течение 14–90 дней.
decoder	Аномалии в заголовках пакетов при их первичном декодировании (например, несоответствие минимальной длины заголовка пакета)
dns	Вторжения на DNS-серверы
dos	Вторжения, направленные на отказ в обслуживании
drop	Сигнатуры обнаруживают соединения с подсетями, зафиксированными в Spamhaus
exploit	Попытки эксплуатации уязвимостей в программном обеспечении
ftp	Вторжения на FTP-серверы
info	Сигнатуры указывают на подозрительную активность, но сами не классифицируются как вредоносные
malware	Трафик вредоносного программного обеспечения
netbios	Атаки или подозрительная активность по протоколу Netbios
p2p	Трафик пиринговых программ (например, торрент-трекеров)
policy	Вторжения, направленные на нарушение политики информационной безопасности (например, анонимный вход по FTP, запуск java-апплетов для воспроизведения видео, доступ к Gmail)

Название группы	Что выявляет группа правил
preprocessor	Аномалии в процессе предварительной обработки пакетов
scada	Вторжения в SCADA-системы
scan	Попытки сканирования сети
sensitive-data	Конфиденциальная информация (например, номера банковских карт, адреса электронной почты и прочее)
shellcode	Двоичный исполняемый код (шелл-код)
smtp	Потенциальные вторжения в почтовую службу SMTP
snmp	Активность протокола SNMP (удаленное управление сетевым оборудованием)
sql	Вторжения в SQL-серверы
telnet	Вторжения в ходе выполнения telnet-сессии
tftp	Вторжения в TFTP-службы и TFTP-клиенты
trojan	Трафик вредоносного программного обеспечения
user_agents	HTTP-пакеты, в заголовках которых фигурируют User Agents, замеченные в использовании подозрительным или вредоносным ПО
web_client	Потенциально опасный трафик со стороны клиентских веб-приложений
web_server	Вторжения, направленные на веб-серверы
web_specific_apps	Вторжения в различные веб-службы (например FrontPage, IIS) и веб-приложения (например реализованные на языке ColdFusion)
worm	Трафик вредоносного программного обеспечения

О

Номера правил анализа трафика эвристическим методом

Таблица 53. Номера правил IPS эвристического метода анализа трафика

Номер правила gid.sid	Метод обнаружения	Тип события
112.1-112.4	Анализ служебных заголовков пакетов	Аномалия ARP
145.1-145.6	Анализ служебных заголовков пакетов	Аномалия DNP3
106.1-106.5	Анализ служебных заголовков пакетов	Аномалия RPC
119.1-119.32	Анализ служебных заголовков пакетов	Аномалия HTTP на стороне клиента
120.1-120.11	Анализ служебных заголовков пакетов	Аномалия HTTP на стороне сервера
124.1-124.13	Анализ служебных заголовков пакетов	Аномалия SMTP
125.1-125.9	Анализ служебных заголовков пакетов	Аномалия FTP
126.1-126.3	Анализ служебных заголовков пакетов	Аномалия Telnet

128.1-128.7	Анализ служебных заголовков пакетов	Аномалия SSH
129.1-129.19	Анализ служебных заголовков пакетов	Аномалия TCP
131.1-131.3	Анализ служебных заголовков пакетов	Аномалия DNS
133.1-133.56	Анализ служебных заголовков пакетов	Аномалия DCE
137.1-137.2	Анализ служебных заголовков пакетов	Аномалия SSL
140.1-140.27	Анализ служебных заголовков пакетов	Аномалия SIP
141.1-141.7	Анализ служебных заголовков пакетов	Аномалия IMAP
142.1-142.7	Анализ служебных заголовков пакетов	Аномалия POP
143.1-143.3	Анализ служебных заголовков пакетов	Аномалия GTP
138.2-138.6, 139.1	Поиск конфиденциальных данных	Обнаружены конфиденциальные данные
105.1-105.4	Отслеживание попыток удаленного выполнения произвольного кода	Аномалия Back Orifice
116.1-116.456	Поиск аномалий при декодировании пакетов	Аномалия декодера пакетов
123.1-123.13	Поиск аномалий фрагментации пакетов	Аномалия фрагментации пакетов
122.1-122.27	Отслеживание попыток сканирования портов	Сканирование портов
134.1-134.2	Мониторинг производительности пакетов	Аномалия PPM

P

Термины и сокращения

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 задаёт связи между ними.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в неё 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.

Дистрибутив ключей

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

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

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

Защищенный 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.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Открытый 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.

Сетевой узел ViPNet

Сетевой узел с ПО ViPNet, зарегистрированный в ViPNet Prime VPN.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищённых узлов ViPNet. Сеть ViPNet имеет наложенную

маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Справочники и ключи

Настройки узла ViPNet, ключи защиты обновлений, ключи обмена и ключи пользователя.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки транспортного конверта MFTP.

Транспортный конверт

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

Транспортный сервер MFTP

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

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

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.

Туннелирующий координатор

Координатор, который осуществляет туннелирование.

Шлюзовой координатор

Координатор, через который происходит обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ViPNet Prime каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

Электронная подпись (ЭП)

Откреплённая CMS-подпись, сформированная по Р 1323565.1.025–2019 и ГОСТ 34.10-2012 (512 бит).