



ViPNet Client 5 for Linux

Руководство администратора

Версия продукта: 5.1.4

© АО «ИнфоТеКС», 2025

ФРКЕ.00380-01 32 01

Версия продукта 5.1.4

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 Client 5 for Linux приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Client 5 for Linux.

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.....	6
О документе.....	7
Соглашения документа.....	7
О программе	8
Технология обработки трафика в ViPNet Client 5.....	8
Различия форматов ключей.....	9
Рекомендации по безопасности	9
Системные требования	11
Требования к корпоративной сети	12
Поддерживаемые архитектуры процессоров и дистрибутивы Linux	13
Протестированные на совместимость внешние устройства	15
Комплект поставки.....	16
Обратная связь.....	17
 Глава 1. Установка, обновление и удаление	18
Порядок установки.....	19
Установка и обновление	21
Создание репозитория для установки и обновления в домене ALD Pro.....	24
Обновление из управляющего ПО.....	25
Изменение рабочего каталога клиента	26
Автоматическое получение параметров обновления	27
Рекомендации по повышению производительности	29
Запуск VPN-соединения до аутентификации пользователя в ОС	30
Подготовка к работе с внешними устройствами.....	31
Удаление.....	32
 Глава 2. Администрирование.....	33
Управление автозапуском ViPNet Client 5	35
Обмен межсетевой информацией с доверенными сетями	36
Многофакторная аутентификация.....	37
Назначение многофакторной аутентификации	37
Включение видимости туннелируемых узлов по виртуальным IP-адресам.....	39
Настройка количества потоков обработки IP-трафика	40
Изменение используемых портов для прикладных протоколов.....	41
Настройки в файле vipnet.conf	42

Рекомендации по настройке работы с DNS	44
Порядок настройки	44
Обработка DNS-трафика при включённом VPN-соединении.....	45
Обработка DNS-трафика при отключённом VPN-соединении.....	48
Настройка DNS в ОС	48
Поиск DNS	52
Способ выбора координатора	53
Координаторы в группе серверов	54
Подключение к узлам напрямую.....	55
Управление настройками ViPNet Client 5 for Linux	56
Параметры ViPNet Client 5	57
Секция secured	57
Секция policies	57
Секция dns	58
Секция network.....	58
Секция settings	59
Секция firewall.....	59
Секция logging.....	61
Секция nodes.....	61
Секция features	63
Секция updates	63
Пример настроек.....	65
Переинициализация внутренних конфигурационных файлов	67
Работа с транспортным модулем.....	68
Настройка журнала событий.....	69
Просмотр журнала IP-пакетов	70
Настройка передачи данных по протоколу TCP	71
Регламентный контроль целостности.....	72
Работа с журналом критически важных событий	73
Настройка фильтрации трафика.....	75
Особенности работы с ViPNet EPP	77
Глава 3. Отладка ViPNet Client 5.....	79
Команды отладки	80
Просмотр информации о работе VPN-драйвера	82
Приложение А. Создание файла с сетевыми фильтрами.....	96
Группы объектов	102
Источник и назначение	105

Протокол	108
Расписание	110
Приложение В. Общие и индивидуальные настройки профилей	112
Приложение С. Возможные неполадки и способы их устранения	114
Особенности ViPNet Client 5	114
Не удаётся установить ViPNet Client 5	114
Не удаётся обновить ViPNet Client 5 с помощью QApt	115
После обновления на узле с центром управления ViPNet Prime в сети не принимаются обновления справочников из доверенной сети	115
После установки ViPNet Client 5 не отображаются иконки программ	116
Не отображается информация о применении обновлений справочников и ключей в журнале транспортных конвертов в ViPNet Prime	116
Бесконечное обновление ViPNet Client 5 через opkg	116
Не запускается VPN-соединение после обновления	117
Изменился сервер соединений	117
Проблемы с отображением графического интерфейса ViPNet Client 5 в ОС Ubuntu 22.04 LTS	117
Не работает передача данных в ViPNet NVS по открытому каналу	118
Нет соединения с координатором	119
Сетевой экран firewalld блокирует работу ViPNet Client 5	119
Совместная работа ViPNet Client 5 и службы SELinux	120
Не работает служба systemd-resolver	120
Не удаётся установить дистрибутив ключей на компьютер	121
Нарушена работа ViPNet Client 5 с DNS	121
Нарушена целостность компонентов программы ViPNet Client 5 или связанных системных библиотек	122
ViPNet Client 5 не определяет подключённое внешнее устройство	123
Проблемы с определением внешнего устройства из-за пакета OpenCT	123
Не удаётся выполнить смену способа аутентификации при использовании внешнего устройства JaCarta	124
Корпоративные ресурсы недоступны	124
Уведомление «Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG) /bpfilter_umh»	126
ViPNet Client 5 не отвечает и отображается непредвиденная ошибка	126
Приложение D. Термины и сокращения	128



Введение

О документе	7
О программе	8
Системные требования	11
Комплект поставки	16
Обратная связь	17

О документе

В документе содержится информация о назначении и установке программы ViPNet Client 5 for Linux (далее — ViPNet Client 5).

Документ предназначен для администраторов сети ViPNet, которые устанавливают ViPNet Client 5 на компьютеры с операционной системой GNU/Linux (далее — Linux).

Предполагается, что читатель этого документа обладает знаниями и опытом в области администрирования Linux.

Соглашения документа

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



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

Обозначения при описании команд в документе:

- Команды, которые могут быть выполнены пользователем Linux, содержат приглашение:
`user@host:~$ команда`
- Команды, которые могут быть выполнены администратором Linux, содержат приглашение:
`root@host:~# команда`
- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки:
`команда <параметр>`
- Необязательные параметры или ключевые слова заключены в квадратные скобки:
`команда <обязательный параметр> [необязательный параметр]`
- Допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:
`команда {вариант-1 | вариант-2}`

О программе

ViPNet Client 5 защищает трафик на компьютерах с Linux путём шифрования IP-пакетов.

С помощью ViPNet Client 5 ваше устройство станет [узлом защищённой сети](#) (далее — узел). Вы сможете подключаться к другим узлам или [туннелируемым узлам](#) по защищённому каналу через координатор и получать доступ к размещённым на этих узлах ресурсам: корпоративным веб-порталам, электронной почте, системе IP-телефонии и другим корпоративным сервисам. К открытым ресурсам интернета вы будете подключаться напрямую по незащищённому каналу.

Чтобы общаться с пользователями сети ViPNet по защищённому каналу, установите на устройство с ViPNet Client 5 программы ViPNet CSS Connect и ViPNet Деловая почта.

ViPNet Client 5 поставляется в одном из вариантов:

- Консольная версия, с которой можно работать только из командной строки.
- Графическая версия, с которой можно работать в командной строке и в графическом интерфейсе.

Технология обработки трафика в ViPNet Client 5

ViPNet Client 5 использует для маршрутизации трафика виртуальный сетевой интерфейс TUN. IP-адреса и диапазоны IP-адресов защищённой сети добавляются в таблицу маршрутизации ОС, обеспечивая передачу трафика от программ на интерфейс TUN, а затем трафик обрабатывается в ViPNet Client 5.

По умолчанию IP-адрес TUN-интерфейса назначается в виде `7.0.XX.YY`, где:

- `XX` — старший байт идентификатора узла ViPNet, переведённый в десятичную систему.
- `YY` — младший байт идентификатора узла ViPNet, переведённый в десятичную систему.

Например, шестнадцатеричный идентификатор узла в защищённой сети: `0x04D2162E`, где:

- `04D2` — идентификатор сети ViPNet.
- `162E` — идентификатор узла в сети ViPNet.

В шестнадцатеричной системе `XX` — это `16`, `YY` — `2E`. После перевода в десятичную `XX` — это `22`, `YY` — `46`. Результирующий IP-адрес TUN-интерфейса — `7.0.22.46`. Назначение IP-адресов по такому алгоритму обеспечивает уникальность виртуальных IP-адресов внутри защищённой сети.

Различия форматов ключей

В ViPNet Client 5 вы можете установить ключи в формате DST и DS5. Клиенты с ключами *.ds5 относятся к поколению продуктов ViPNet 5.

	DST	DS5
Поколение сети	4	5
Управляющее ПО	ViPNet Administrator, ViPNet Prime	ViPNet Prime
Лицензия в ViPNet Prime	Client for Linux	Client for Linux v.5, Universal Client v.5
Роль в ViPNet Administrator	Client for Linux (0091)	-
Транспорт	MFTP	UT
Аутентификация с помощью внешнего устройства	На устройствах с архитектурой процессора x86-64	-
Смена пароля	-	+
Использование функции туннелирования	+	-
Совместимость с ViPNet Деловая почта	+	-
Установка на 4G роутер TELEOFIS LT50-M	+	-



Примечание. Про совместимость с ViPNet CSS Connect см. документацию вашей версии ViPNet CSS Connect.

Рекомендации по безопасности

Чтобы обеспечивать безопасности в корпоративной сети, рекомендуется регулярно отслеживать попытки доставить подозрительные служебные конверты на узлы с ViPNet Client. Если в вашей сети обнаружены подозрительные служебные конверты, [сообщите в службу технического сопровождения ИнфоТеКС](#).

Некорректные служебные конверты не обрабатываются и не применяются на узлах. Клиент блокирует подозрительные конверты и отправляет уведомление об этом на узел с ViPNet ЦУС или с центром управления ViPNet Prime.

Имя конверта (транспортной квитанции), отправленного после получения подозрительного служебного конверта, будет начинаться с символа !.

Просмотр информации о подозрительных конвертах

В ViPNet Client 5 for Linux на узле с центром управления ViPNet Prime и в ViPNet Client 5 for Windows на узле с ViPNet ЦУС:

- в журнале из ZIP-архива с отчётом о работе клиента.
 - В ViPNet Client 5 for Linux: `mftpenv.journal` в версии 5.0.0, `tpv4env.journal` в версии 5.1.3 и выше.

Также вы можете просмотреть этот журнал в каталоге с журналами ViPNet Client 5. Путь по умолчанию — `$HOME/.vipnet-vpn/var/log` или `$HOME/.vipnet/var/log`.

- В ViPNet Client 5 for Windows: `tpv4env.journal` в `/var/log/ID_Узла`.

О создании отчёта о работе клиента см. руководство пользователя ViPNet Client 5, раздел «Обращение в службу поддержки».

- [журнале транспортных конвертов](#).

Чтобы просмотреть журнал:

- в ViPNet Client 5 for Linux выполните:
`user@host:~$ vipnetclient transport events`
- в ViPNet Client 5 for Windows выполните:
`vipnetclient transport events`

В ViPNet Client for Windows на узле с ViPNet ЦУС:

- В ViPNet Client > Приложения > ViPNet Транспортный модуль.

На вкладке **Конверты** найдите конверты с именем `!*.ctl`.

- В журнале `mftpenv.log` в транспортном каталоге (по умолчанию `C:\ProgramData\InfoTeCS\ID_Узла`).

По умолчанию подозрительные конверты помещаются в папку `invalid`:

- ViPNet Client 5 for Linux 5.0.0: `$HOME/.vipnet-vpn/profiles/ID_Узла/mftp/in/invalid/`
- ViPNet Client 5 for Linux 5.1.3: `$HOME/.vipnet-vpn/profiles/ID_Узла/tpv4/in/invalid/`
- ViPNet Client 5 for Windows:
`C:\ProgramData\InfoTeCS\.vipnet\WorkDir\profiles\ID_Узла\tpv4\in\invalid`
- ViPNet Client for Windows: `C:\ProgramData\Infotecs\ID_Узла\invalid`

Очищайте папку `invalid` вручную.

Системные требования

Параметры	Минимальные	Рекомендуемые
Частота процессора	500 МГц	2 ГГц
Архитектура процессора	x86_64	x86_64
	ARMv5	ARMv5
	ARMv7	ARMv7
	ARMv8	ARMv8
	Байкал-М	Байкал-М
	MIPS	MIPS
Количество ядер	1	4
Объём свободной оперативной памяти	128 Мбайт	512 Мбайт
Свободное место на жёстком диске	128 Мбайт	512 Мбайт
Требования к ОС	Версия ядра 3.10 и выше TUN-интерфейс libxkbcommon-x11 или libxkbcommon-x11-0 (для графической версии)	Версия ядра 3.10 и выше TUN-интерфейс Пакетный менеджер для deb, rpm или ipk-пакета libxkbcommon-x11 или libxkbcommon-x11-0 (для графической версии) iptables , systemd



Примечание. ViPNet Client 5 может работать и на менее производительных устройствах. При необходимости гарантированной поддержки менее производительного устройства [обратитесь в ИнфоТекС](#).

На устройствах со слабыми процессорами работа с ViPNet Client 5 может быть замедлена.

Допускается работа в виртуальных средах:

- VMware Workstation Pro версии 15.0 и выше,
- VirtualBox версии 6.0 и выше,
- Proxmox Virtual Environment версии 8.0 и выше.

Вы можете использовать другие виртуальные среды и версии, но они не тестировались и их работа не гарантирована.

Требования к корпоративной сети

Для клиентов с ключами *.dst

Управляющее ПО:

- [ViPNet Administrator](#) версии 4.6.11 и выше.
- [ViPNet Prime](#) версии 1.7.0 и выше.

Координатор:

- ViPNet Coordinator HW 4 версии 4.3.x (версии 4.3.2 и выше).
- ViPNet Coordinator HW 4 версии 4.5.x (версии 4.5.2 и выше).
- ViPNet Coordinator HW 5 версии 5.1.2 и выше.

Для клиентов с ключами *.ds5

- [ViPNet Prime](#) версии 1.9.5 и выше.
- ViPNet Coordinator HW 5 версии 5.3.1 и выше.

Поддерживаемые архитектуры процессоров и дистрибутивы Linux

Таблица 1. x86-64

Дистрибутив Linux	Протестированные на совместимость версии
Операционная система специального назначения «Astra Linux Special Edition»	РУСБ.10015-01, очередное обновление 1.7 РУСБ.10015-01, очередное обновление 1.7 в мобильном режиме РУСБ.10015-01, очередное обновление 1.8 РУСБ.10015-10 РУСБ.10015-16 (исп.1) РУСБ.10015-17
Альт СП релиз 10	Рабочая станция Сервер
РЕД ОС	7.3, сертифицированная редакция 8, стандартная редакция
EMIAS OS	1.0
РОСА «ХРОМ» ФСТЭК 12	Рабочая станция Сервер
AlterOS	7.5, сертифицированная редакция
СинтезМ	8.0
Операционная система общего назначения «ОСнова» ДВНБ.10001-01	2.13
Атлант Alcione	Alcione
Ubuntu	22.04 LTS 24.04 LTS
Debian	11 12

Таблица 2. ARMv5

Дистрибутив Linux	Протестированные на совместимость устройства
OpenWrt-based	4G роутер TELEOFIS RTU1068 V4

Таблица 3. ARMv7

Дистрибутив Linux	Протестированные на совместимость устройства
OpenEmbedded-based	Сервер доступа к данным (контроллер) TOPAZ IEC DAS MX240 E2R4 (2Gtx-4R) Сервер доступа к данным (контроллер) TOPAZ IEC DAS MX681 E3R2 (3Gtx-2R)
Ubuntu 22.04 LTS	Raspberry Pi 4
OpenWrt-based	4G роутер TELEOFIS LT50-M
Debian 11	Контроллер Многофункциональный ЭНТЕК E2R2(G)-1 v.6

Таблица 4. ARMv8

Дистрибутив Linux	Протестированные на совместимость устройства
Ubuntu 22.04 LTS	Raspberry Pi 4
Ubuntu 24.04 LTS	Raspberry Pi 4
Debian 11	Raspberry Pi 4
Debian 12	Raspberry Pi 4
Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10152-02	Очередное обновление 4.7 в мобильном режиме Очередное обновление 4.7 на Байкал-М
Альт СП релиз 10	Рабочая станция на Байкал-М Сервер на Байкал-М
РЕД ОС 7.3	Сертифицированная редакция на Байкал-М

Таблица 5. MIPS

Дистрибутив Linux	Протестированные на совместимость устройства
OpenWrt-based	Многофункциональный роутер iRZ RL21w (серия R2)

Протестированные на совместимость внешние устройства



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами *.dst на устройствах с архитектурой x86_64.

Производитель	Устройство
«Аладдин Р.Д.»	JaCarta-2 ГОСТ
	JaCarta PKI/Flash
	JaCarta PRO
	JaCarta PKI/ГОСТ
	JaCarta ГОСТ
	JaCarta-2 PKI/ГОСТ
	JaCarta SF/ГОСТ
	JaCarta LT
«Актив»	Рутокен ЭЦП
	Рутокен ЭЦП 2.0 (2000, 2100, 3000)
	Рутокен ЭЦП 3.0 (3120, 3100, 3220)
	Рутокен PKI (1800)
	Рутокен Lite (1000, 1010)



Примечание. Вы можете использовать другие внешние устройства производителей «Аладдин Р.Д.» и «Актив», но они не тестировались и их работа не гарантирована.

Комплект поставки

- Пакеты установки в форматах DEB, RPM и IPK.
- Файлы в формате LZN для централизованного обновления клиентов с ключами *.dst.
- Файлы в формате ZIP для централизованного обновления клиентов с ключами *.ds5.
- Документы в формате PDF:
 - Руководство администратора.
 - Руководство пользователя.
 - Соответствие пакетов установки поддерживаемым платформам.
 - Установка на промышленные контроллеры.
 - Использование функции туннелирования.
 - Справочник разработчика.

Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ViPNet Client 5, см. в ZIP-архиве «ViPNet Client 5 for Linux. Руководство администратора (Приложение)».

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21.
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

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

1

Установка, обновление и удаление

Порядок установки	19
Установка и обновление	21
Запуск VPN-соединения до аутентификации пользователя в ОС	30
Подготовка к работе с внешними устройствами	31
Удаление	32

Порядок установки



Внимание! Для установки ViPNet Client 5 необходимо, чтобы каталоги `/var`, `/lib`, `/usr` и `/etc` были доступны для записи.

1 В управляющем ПО создайте клиенты.

- В ViPNet Administrator назначьте клиентам роль «Client for Linux» (0091).

См. «ViPNet Центр управления сетью. Руководство администратора», раздел «Добавление клиента».

- В ViPNet Prime для клиентов четвертого поколения с ключами в формате DST выберите платформу Linux и лицензию Client for Linux.

Для клиентов пятого поколения с ключами в формате DS5 выберите платформу Linux и лицензию Client for Linux v.5 или Universal Client v.5.

См. «ViPNet Prime. Руководство администратора», раздел «Создание клиента».



Внимание! На [узле](#) должен быть зарегистрирован только один пользователь.

2 В ViPNet Administrator включите настройку **Выбор способа аутентификации в мастере выдачи дистрибутива ключей**.

См. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Настройка параметров создания дистрибутивов ключей».

3 Установите ViPNet Client 5 на компьютеры пользователей.

Об установке на промышленные контроллеры см. документ «Установка на промышленные контроллеры».

4 Для пользователей, которые будут проходить аутентификацию с помощью персонального ключа на внешнем устройстве, [подготовьте компьютеры для работы с внешними устройствами](#).



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами `*.dst` на устройствах с архитектурой `x86_64`.

5 Создайте дистрибутивы ключей в управляющем ПО ViPNet, при этом выберите способ аутентификации пользователей в ViPNet Client 5. Длина пароля не должна превышать 31 символ.

См. «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Создание дистрибутивов ключей»; «ViPNet Prime. Руководство администратора», раздел «Создание дистрибутивов ключей».

Если вы устанавливаете ViPNet Client 5 на сервисные или серверные узлы, например, центр управления ViPNet Prime, ViPNet CSS Hub, ViPNet CSS FileExchange, ViPNet CSS CPNS, ViPNet CSS Bot Server или Client Auth Server, используйте только один дистрибутив ключей в одном ViPNet Client 5. Использование нескольких дистрибутивов ключей в одном ViPNet Client 5 — экспериментальная функция, и её работа на таких узлах может быть ограничена. Подробнее см. руководство пользователя, раздел «Несколько профилей на устройстве».

Примечание. Если предполагается установка дистрибутива ключей на маломощное устройство, для файла дистрибутива ключей должны выполняться ограничения:



- Максимальный размер файла *.dst или *.ds5 — 5 Мбайт.
- Максимальное количество туннелей — 3000.
- Максимальное количество связей с узлами — 500.

-
- 6 Передайте дистрибутивы ключей вместе с паролями пользователям ViPNet Client 5 доверенным способом. Передайте также внешние устройства с персональным ключом и PIN-коды к ним пользователям, для которых выбран соответствующий способ аутентификации.

Если вы планируете в дальнейшем [обновлять ViPNet Client 5 из управляющего ПО](#) на устройстве с ОС Astra Linux Special Edition, устанавливайте ключи под пользователем с высоким уровнем целостности или настройте для пользователей и низкий, и высокий уровни целостности. Это нужно, потому что принять обновление из управляющего ПО можно только под пользователем с высоким уровнем целостности, под которым устанавливали ключи.

- 7 Убедитесь, что пользователи ViPNet Client 5 установили ключи и запустили программу.

См. руководство пользователя, раздел «Установка ключей».

Установка и обновление

В разделе описаны установка и обновление ViPNet Client 5. Особенности обновления ключей и смены мастер-ключей см. в руководстве администратора ViPNet Prime.



Примечание. Не рекомендуется обновлять ViPNet Client 5 на более ранние версии, иначе программа может работать нестабильно.

Название и формат пакета установки ViPNet Client 5 зависят от архитектуры процессора и используемой ОС. Полный список названий и форматов см. в документе «ViPNet Client 5 for Linux. Соответствие пакетов установки поддерживаемым платформам».

На устройствах без пакетного менеджера установить и обновить ViPNet Client 5 можно только вручную. Подробнее см. документ «Установка на промышленные контроллеры».

Перед обновлением ViPNet Client 5 через пакетный менеджер `opkg` проверьте статус установленного пакета:

- 1 Выполните:

```
root@host:~# opkg info vipnetclient
```

- 2 Если в строке `Status` отображается статус `install ok half-installed`:

- 2.1 Перейдите в режим редактирования файла `/var/lib/opkg/status`.

- 2.2 Удалите записи о недоустановленном пакете ViPNet Client 5.

- 3 Обновите ViPNet Client 5.

Чтобы установить или обновить ViPNet Client 5:



Внимание! Если в ОС включён мандатный контроль и другие средства защиты информации, установка ViPNet Client 5 должна выполняться администратором с высоким уровнем целостности в ОС.

- 1 Войдите в консоль ОС Linux с правами суперпользователя (`root`).

- 2 Если вы планируете устанавливать DEB-пакет на компьютер с недавно развёрнутой ОС Linux, установите все зависимости:

```
root@host:~# apt -f install
```

- 3 Для ОСна выключите режим замкнутой программной среды:

```
user@host:~$ sudo rm /etc/ima/policy
```

```
user@host:~$ sudo ln -s /etc/ima/policy.d/empty /etc/ima/policy
```

```
user@host:~$ sudo update-initramfs -u -k all
```

```
user@host:~$ sudo reboot
```

- 4 Чтобы установить или обновить ViPNet Client 5 из репозитория ALD Pro, [создайте репозиторий](#).

5 В зависимости от типа пакета выполните команды:

- Для установки из репозитория ALD Pro:

```
root@host:~# apt install {vipnetclient | vipnetclient-gui}
```
- Для обновления из репозитория ALD Pro:

```
root@host:~# apt install --only-upgrade {vipnetclient | vipnetclient-gui}
```
- Для установки и обновления DEB-пакета (в том числе подписанного DEB-пакета для ОС Astra Linux Special Edition и ОСнова):

```
root@host:~# dpkg -i <название_пакета>.deb
```
- Для установки RPM-пакета:

```
root@host:~# rpm -i <название_пакета>.rpm
```
- Для обновления RPM-пакета:

```
root@host:~# rpm -U <название_пакета>.rpm
```
- Для установки и обновления IPK-пакета:

```
root@host:~# opkg install <название_пакета>.ipk
```

Примечание. Чтобы при установке автоматически принять лицензионное соглашение:



- Для DEB-пакета выполните:

```
root@host:~# ACCEPT_EULA=true dpkg -i *.deb
```
- Для RPM-пакета выполните:

```
root@host:~# ACCEPT_EULA=Y rpm -i *.rpm
```

Для IPK-пакета дополнительных действий не требуется.

6 Чтобы установить ViPNet Client 5, примите лицензионное соглашение.

7 Если в обновлении находится новая версия файла `vipnet.conf`:

- Для DEB-пакета во время обновления появится предложение установить новую версию файла `vipnet.conf`, введите один из символов:
 - **Y** или **I** — установить новую версию файла `vipnet.conf` из установочного пакета ViPNet Client 5. При этом все ранее выполненные в этом файле настройки будут утеряны, после обновления ViPNet Client 5 в файле будут содержаться новые настройки.
 - **N** или **O** — оставить текущую версию файла `vipnet.conf`. Все ранее выполненные в этом файле настройки будут сохранены после обновления ViPNet Client 5.
 - **D** — показать различия между текущей версией файла `vipnet.conf` и версией из установочного пакета ViPNet Client 5. После просмотра различий выберите один из перечисленных выше вариантов.
 - **Z** — запустить командную оболочку для просмотра файла `vipnet.conf`. Выход из командной оболочки по команде `exit`. После просмотра настроек выберите один из перечисленных выше вариантов.

Вариант по умолчанию — N. Также вы можете запустить обновление DEB-пакета с опцией `--force-confnew`, чтобы новая версия файла `vipnet.conf` была установлена автоматически.

- Для RPM-пакета в процессе обновления создаётся новый файл `vipnet.conf.rpmnew`. Выполните одно из действий:
 - Чтобы оставить текущую версию файла `vipnet.conf` со всеми выполненными ранее настройками, удалите новый файл:

```
root@host:~# rm /etc/vipnet.conf.rpmnew
```
 - Чтобы обновить файл `vipnet.conf`:
 - Выключите VPN-соединение:

```
user@host:~$ vipnetclient stop
```
 - Удалите текущую версию файла:

```
root@host:~# rm /etc/vipnet.conf
```
 - Замените файл новым:

```
root@host:~# mv /etc/vipnet.conf.rpmnew /etc/vipnet.conf
```
 - Включите VPN-соединение:

```
user@host:~$ vipnetclient start
```
- Для IPK-пакета выполните одно из действий:
 - Чтобы оставить текущую версию файла `vipnet.conf` со всеми выполненными ранее настройками, запустите обновление ViPNet Client 5, как описано в шаге 3.
При этом будет создан новый файл `vipnet.conf-opkg`, удалите его:

```
root@host:~# rm /etc/vipnet.conf-opkg
```
 - Чтобы установить новую версию файла `vipnet.conf` из установочного пакета ViPNet Client 5, запустите обновление ViPNet Client 5 с дополнительной опцией `--force-maintainer`.

- 8 Если вы обновляете ViPNet Client 5 при выключенном VPN-соединении, после обновления оно может остаться выключенным. В таком случае включите VPN-соединение вручную:

```
user@host:~$ vipnetclient start
```

Возможно обновление с консольной версии ViPNet Client 5 на графическую или с графической версии на консольную. При этом в результате обновления первоначально установленная версия ViPNet Client 5 будет удалена.

Примечание. При обновлении до последней версии ViPNet Client 5:



- ViPNet Client 4U со сменой исполнения,
- ViPNet Client 4U версии 4.15 и ниже

может выключиться VPN-соединение. После обновления включите VPN-соединение вручную или перезагрузите компьютер.

Создание репозиториев для установки и обновления в домене ALD Pro

- 1 Проверьте, что в ALD Pro установлен сервер подсистемы сетевого репозитория.

Подробнее см. руководство администратора ALD Pro, раздел «Установка сервера репозиториев».

- 2 В ALD Pro создайте репозиторий с установочным пакетом ViPNet Client 5 .

Если вы впервые создаёте репозиторий, задайте:

- o Имя репозитория:

`vipnetclient` — для консольной версии ViPNet Client 5,

`vipnetclient-gui` — для графической версии ViPNet Client 5.

- o Относительный путь публикации репозитория:

`/vipnetclient` — для консольной версии ViPNet Client 5,

`/vipnetclient-gui` — для графической версии ViPNet Client 5.

Если вы создаёте новую версию существующего репозитория, задайте:

- o Тип источника: Пакеты,

- o Источник: `infotecs`,

- o Метка: `vpnclient`,

- o Номер версии: <начиная с 1, по порядку: 1, 2, 3...>

При обновлении используйте следующий порядковый номер.

- o Кодовое имя дистрибутива: `latest`,

- o Архитектура: `amd64`.

Подробнее см. руководство администратора ALD Pro, раздел «Создание репозитория из загруженных пакетов deb».

- 3 В Astra Linux Special Edition в домене ALD Pro в файл `/etc/apt/sources.list` добавьте:

```
deb [trusted=yes] <абсолютный путь до созданного репозитория с установочным пакетом ViPNet Client 5> latest main
```

Абсолютный путь можно посмотреть в карточке репозитория в ALD Pro.

- 4 Обновите список пакетов:

```
root@host:~# apt update
```

Обновление из управляющего ПО

Администратор сети ViPNet может отправлять обновление клиентов из управляющего ПО (см. документацию управляющего ПО). Обновления применяются автоматически.

Если на защищённый узел пришли некорректные обновления, которые не проходят проверки целостности и подлинности, они не применяются. Клиент блокирует подозрительные служебные конверты и [отправляет уведомление об этом](#) на узел с ViPNet ЦУС или с центром управления ViPNet Prime.

Внимание!



- На устройстве с ОС Astra Linux Special Edition перед отправкой обновления из управляющего ПО выполните аутентификацию в ОС под пользователем, под которым выполнялась установка ключей. При этом выберите атрибут безопасности **Уровень целостности — Высокий**. Иначе обновление не выполнится.
 - На промышленные контроллеры с ViPNet Client 4U версий 4.8–4.13 сначала отправьте обновление до версии 4.15, а потом до 5.1.4.
 - На устройствах без пакетного менеджера обновить ViPNet Client 5 можно только вручную. Подробнее см. документ «Установка на промышленные контроллеры».
-

Обновление клиентов с ключами *.dst

Вы можете обновить клиенты с ключами *.dst из ViPNet Administrator и ViPNet Prime. Для этого используйте LZN-архив:

- с DEB-пакетом,
- с RPM-пакетом,
- с IPK-пакетом,
- с DEB, RPM и IPK пакетами.

Для обновления:

- ViPNet Client 4U версий 4.8–4.12 используйте LZN-архив с одним установочным пакетом.
- ViPNet Client 4U версий 4.13 и выше используйте любой LZN-архив без слова `_update` в названии.
- ViPNet Client 5 версий 5.0.0 и 5.1.3 и выше:
 - проверьте, чтобы на узлах был установлен пакет стандартных корневых сертификатов `ca-certificates`. Сертификаты должны быть действительны.
 - используйте LZN-архив с электронной подписью (в названии такого архива есть слово `_update`).

Для ОСнова используйте LZN-архив, в названии которого есть слово `generic`.

- Проверьте, чтобы в рабочем каталоге клиента (по умолчанию — `$HOME/.vipnet-vpn/var/log` или `$HOME/.vipnet/var/log`) было свободно в три раза

больше места, чем занимает архив с обновлением. Если места недостаточно, [измените рабочий каталог](#).

Обновление клиентов с ключами *.ds5

Вы можете обновить клиенты с ключами *.ds5 из ViPNet Prime. Для этого используйте ZIP-архив:

- с DEB-пакетом,
- с RPM-пакетом,
- с IPK-пакетом.

Для обновления ViPNet Client 5 версий 5.0.x для ОСноа используйте ZIP-архив, в названии которого есть слово generic.

Порядок обновления:

- 1 Проверьте, чтобы в рабочем каталоге клиента (по умолчанию — `$HOME/.vipnet-vpn/var/log` или `$HOME/.vipnet/var/log`) было свободно в три раза больше места, чем занимает архив с обновлением. Если места недостаточно, [измените рабочий каталог](#).
- 2 Загрузите архив с обновлением на HTTP-сервер внутри защищённой сети.
- 3 [Укажите параметры обновления в расширенных настройках клиентов в ViPNet Prime](#) в секции updates.
- 4 После отправки обновления из управляющего ПО, перезапустите на узлах VPN-соединение или поручите это сделать пользователям. Подробнее см. руководство пользователя, раздел «Запуск и завершение работы».

Вы можете задать параметры обновления вручную или [получить их автоматически](#) из ZIP-архива.

Также вы можете [применить обновление вручную на компьютере пользователя](#).

Изменение рабочего каталога клиента

При обновлении:

- из ZIP-архива,
- LZH-архива с электронной подписью

клиент создаёт временные файлы. Они в два раза больше, чем архив с обновлением. После обновления эти файлы автоматически удаляются.

Проверьте, чтобы в рабочем каталоге клиента (по умолчанию — `$HOME/.vipnet-vpn/var/log` или `$HOME/.vipnet/var/log`) было свободно в три раза больше места, чем занимает архив с обновлением. Если места недостаточно:

- 1 Удалите ключи:

```
user@host:~$ vipnetclient deletekeys
```

Подробнее см. руководство пользователя, раздел «Удаление ключей».

- 2 В файле `vipnet.conf` задайте путь к рабочему каталогу ViPNet Client 5, в котором достаточно места.
- 3 Установите ключи:

```
user@host:~$ vipnetclient installkeys <путь к дистрибутиву ключей>
```

Подробнее см. руководство пользователя, раздел «Установка ключей».
- 4 Обновите ViPNet Client 5.

Автоматическое получение параметров обновления

Порядок действий:

- 1 Загрузите архив с обновлением на устройство.
- 2 Создайте файл `*.py` и скопируйте туда код для получения параметров.
- 3 Запустите файл `*.py`:

```
root@host:~# python3 <путь к файлу *.py> <путь к ZIP-архиву с обновлением на устройстве>
```

Отобразятся параметры обновления.

 - 3.1 Скопируйте параметры в [расширенные настройки клиентов в ViPNet Prime](#) в секцию `updates`.
 - 3.2 В поле `url` укажите путь к ZIP-архиву с обновлением на HTTP-сервере.
- 4 Повторите шаг 3 для каждого ZIP-архива с обновлением.

Код для получения параметров:

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import json
import os
import yaml # python3 -m pip install pyyaml
import sys
import tempfile
import zipfile

# create custom.yaml part from update.zip's info.json
def make_update_yaml_from_zip(file_path):
    zf = zipfile.ZipFile(file_path)
```

```

# extract shell zip

with tempfile.TemporaryDirectory() as temp_dir:

    zf.extractall(temp_dir)

    zf.close()


# extract info.json from update.zip

zfu = zipfile.ZipFile(os.path.join(temp_dir, 'update.zip'))

with tempfile.TemporaryDirectory() as temp_dir2:

    info_json_file = os.path.join(temp_dir2, 'info.json')

    zfu.extract(os.path.basename(info_json_file), temp_dir2)

    zfu.close()


# convert info.json to yaml

with open(info_json_file, 'r') as fp:

    json_data = json.load(fp)

    update_info = json_data['update']

    update_info['url'] = '<путь к ZIP-архиву с обновлением на HTTP-сервере>'

    update_root = {'updates': [update_info]}

    print(yaml.dump (update_root))


if __name__ == "__main__":

    if len(sys.argv) < 2:

        print(f"usage: {sys.argv[0]} <update_file.zip> ")

        exit(1)

    file_path = sys.argv[1]

    make_update_yaml_from_zip(file_path)

```

Рекомендации по повышению производительности

При создании дистрибутива ключей в управляющем ПО вы можете добавить в справочник до 3000 записей туннелируемых IP-адресов диапазонами или одиночными записями. При установке дистрибутива ключей туннелируемые IP-адреса переносятся из справочника в таблицу маршрутизации ОС.

При переносе IP-адресов из справочника клиент разделяет и объединяет некоторые IP-адреса с помощью подсетей. Например:

- IP-адреса 10.10.0.0 и 10.10.0.1 из справочника будут одной записью 10.10.0.1/31 в таблице маршрутизации ОС.
- Диапазон IP-адресов 10.0.3.200–10.0.3.219 из справочника разобьётся на записи 10.0.3.200/29, 10.0.3.208/29, 10.0.3.216/30 в таблице маршрутизации ОС.

Чем больше записей в таблице маршрутизации, тем дольше проверяются адреса IP-пакетов. Чтобы ускорить проверку и повысить производительность, сократите количество записей в справочнике.

Сокращение количества записей

Чтобы уменьшить количество записей в дистрибутиве ключей и в таблице маршрутизации ОС, задавайте туннелируемые IP-адреса в справочнике через подсети.

Например, вместо записей:

10.10.0.1
10.10.0.2
10.10.0.3
10.10.0.4
10.10.0.5–10

добавьте запись:

10.10.0.0–10.10.0.15

Это уменьшит количество записей, но дополнительно будут туннелироваться адреса 10.10.0.0 и 10.10.11–10.10.0.15.

Запуск VPN-соединения до аутентификации пользователя в ОС

Если в вашей организации:

- используются доменные учётные записи пользователей и компьютер контроллера домена доступен только по сети ViPNet;
- пользователи подключаются к рабочему столу компьютера с установленным ViPNet Client 5 удалённо по сети ViPNet;

настройте запуск VPN-соединения в ViPNet Client 5 до аутентификации пользователя в ОС.

Если пользователю назначены не минимальные полномочия, то для настройки запуска VPN-соединения до аутентификации пользователя в ОС:

- 1 Войдите в консоль ОС Linux с правами суперпользователя (root).
- 2 Установите ключи, как описано в руководстве пользователя в разделе «Установка ключей».



Примечание. Если не работает запуск VPN-соединения до аутентификации пользователя в ОС, в которой включена служба SELinux, [создайте для службы SELinux модуль локальной политики](#).

Если:

- пользователю ViPNet назначены минимальные полномочия;
- пользователю ViPNet назначены не минимальные полномочия и требуется обеспечить ввод изменённого PIN-кода от устройства в ViPNet Client 5 до аутентификации пользователя в ОС;

включите отображение окна аутентификации в ViPNet Client 5 до аутентификации пользователя в ОС. Для этого [включите параметр](#) `authBeforeOsLogon`.



Примечание. Отображение окна аутентификации в ViPNet Client 5 до аутентификации пользователя в ОС возможно только для версий ViPNet Client 5 с графическим интерфейсом. В ОС должен быть установлен пакет `libxkbcommon-x11` или `libxkbcommon-x11-0`.

Окно аутентификации в ViPNet Client 5 не появляется автоматически при выходе компьютера из спящего режима. Если в вашей организации используется доменная аутентификация и не настроено кэширование входа в ОС, то для появления окна аутентификации в ViPNet Client 5 и включения VPN-соединения перезагрузите компьютер.

Подготовка к работе с внешними устройствами



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами *.dst на устройствах с архитектурой x86_64.

Для аутентификации пользователя в ViPNet Client 5 с помощью персонального ключа на внешнем устройстве подготовьте компьютер для работы с внешними устройствами:

- 1 Войдите в консоль ОС Linux с правами суперпользователя (root).
- 2 Установите драйверы, поддерживающие работу интерфейса PC/SC:
 - Для ОС на основе менеджера пакетов DEB:

```
root@host:~# apt-get install libccid pcscd libpcsclite1
```
 - Для ОС на основе менеджера пакетов RPM:

```
root@host:~# yum install ccid pcsc-lite
```
 - Для ОС Альт Linux:

```
root@host:~# apt-get install pcsc-lite-ccid libpcsclite
```
- 3 Установите драйверы, поддерживающие работу интерфейса PKCS#11:
 - [Для устройств Rutoken.](#)
 - [Для устройств JaCarta PKI.](#)



Внимание! Для корректной работы с внешними устройствами используйте версии драйверов, которые поддерживает ваша ОС.

- 4 Перезагрузите компьютер или выполните команду:

```
user@host:~$ vipnetclient debug --reload
```
- 5 Убедитесь, что ViPNet Client 5 определяет установленные библиотеки:
 - 5.1 Проверьте, что ViPNet Client 5 включён.
 - 5.2 Введите `user@host:~$ vipnetclient debug --tokens.`Если нужные библиотеки не обнаружены, в консоли отобразится сообщение об ошибке.
- 6 Подключите внешнее устройство к компьютеру и проверьте, определяют ли его ОС и ViPNet Client 5:

```
user@host:~$ lsusb
```

```
user@host:~$ vipnetclient list --tokens
```



Примечание. Вы можете изменить PIN-код от внешнего устройства средствами производителя. После этого при первом подключении внешнего устройства потребуется ввести новый PIN-код.

Удаление



Примечание. Программы ViPNet CSS Connect for Linux и ViPNet Деловая почта для Linux зависят от ViPNet Client 5. Удалите их до удаления ViPNet Client 5.

Об удалении ViPNet Client 5 на устройствах без пакетного менеджера см. документ «Установка на промышленные контроллеры».

1 Войдите в консоль ОС Linux с правами суперпользователя (root).

2 Для ОС на базе Linux выключите режим замкнутой программной среды:

```
user@host:~$ sudo rm /etc/ima/policy
user@host:~$ sudo ln -s /etc/ima/policy.d/empty /etc/ima/policy
user@host:~$ sudo update-initramfs -u -k all
user@host:~$ sudo reboot
```

3 В зависимости от типа пакета, который был установлен, выполните команды:

○ Для DEB-пакета, установленного из репозитория ALD Pro:

- Консольная версия ViPNet Client 5:

```
root@host:~# apt remove vipnetclient
```

- Графическая версия ViPNet Client 5:

```
root@host:~# apt remove vipnetclient-gui
```

○ Для DEB-пакета:

- Консольная версия ViPNet Client 5:

```
root@host:~# dpkg -r vipnetclient
```

- Графическая версия ViPNet Client 5:

```
root@host:~# dpkg -r vipnetclient-gui
```

○ Для RPM-пакета:

- Консольная версия ViPNet Client 5:

```
root@host:~# rpm -e vipnetclient
```

- Графическая версия ViPNet Client 5:

```
root@host:~# rpm -e vipnetclient-gui
```

○ Для IPK-пакета:

```
root@host:~# opkg remove vipnetclient
```



Внимание! При удалении ViPNet Client 5 ключи не удаляются автоматически. Про удаление ключей см. руководство пользователя.

2

Администрирование

Управление автозапуском ViPNet Client 5	35
Обмен межсетевой информацией с доверенными сетями	36
Многофакторная аутентификация	37
Включение видимости туннелируемых узлов по виртуальным IP-адресам	39
Настройка количества потоков обработки IP-трафика	40
Изменение используемых портов для прикладных протоколов	41
Настройки в файле vipnet.conf	42
Рекомендации по настройке работы с DNS	44
Способ выбора координатора	53
Координаторы в группе серверов	54
Подключение к узлам напрямую	55
Управление настройками ViPNet Client 5 for Linux	56
Переинициализация внутренних конфигурационных файлов	67
Работа с транспортным модулем	68
Настройка журнала событий	69
Просмотр журнала IP-пакетов	70
Настройка передачи данных по протоколу TCP	71

Регламентный контроль целостности	72
Работа с журналом критически важных событий	73
Настройка фильтрации трафика	75

Управление автозапуском ViPNet Client 5

По умолчанию при установке ключей включается автоматический запуск ViPNet Client 5 (при не минимальном уровне полномочий пользователя) и подключение к защищённой сети после аутентификации пользователя в ОС. Если пользователю назначена многофакторная аутентификация, её нужно будет пройти для доступа к корпоративным ресурсам.

При установке ключей пользователь может указать параметр `--no-autostart`, чтобы отключить автоматический запуск.



Примечание. Если в ОС Astra Linux SE у пользователя с низким уровнем целостности не работает автоматический запуск ViPNet Client 5 и подключение к защищённой сети после аутентификации в ОС, выдайте пользователю полный доступ к папке `.config/autostart/`.

Чтобы включить автоматический запуск:

```
user@host:~$ vipnetclient debug --autostart
```

Чтобы выключить автоматический запуск:

```
user@host:~$ vipnetclient debug --no-autostart
```



Примечание. Если ключи устанавливались под учётной записью `root`, то автоматический запуск ViPNet Client 5 и подключение к защищённой сети после аутентификации пользователя в ОС отключить невозможно.

Обмен межсетевой информацией с доверенными сетями

Доверенные сети могут обмениваться межсетевой информацией по защищённому VPN-каналу. Это происходит автоматически.



Внимание! Если есть несколько доверенных сетей, в которых на компьютер с центром управления ViPNet Prime установлен клиент с ключами *.ds5, для межсетевого взаимодействия должно использоваться шифрование по алгоритму ГОСТ 28147-89. Иначе передать межсетевую информацию между этими сетями можно будет только вручную. Подробнее см. руководство администратора ViPNet Prime, раздел «Отправка межсетевой информации».

Чтобы автоматически принимались обновления справочников из доверенной сети, в доверенных сетях на узлах с ViPNet ЦУС и с центром управления ViPNet Prime должен быть установлен один из клиентов:

- ViPNet Client for Windows 4.5.3 hotfix 7 и выше
или ViPNet Client for Windows 4.5.5 hotfix 9 и выше,
- ViPNet Client 5 for Windows 5.1 и выше,
- ViPNet Client 5 for Linux 5.0.0 или 5.1.3 и выше.

До установки актуальной версии в доверенной сети вы можете установить обновления вручную. Для этого получите от администратора доверенной сети обновления доверенным способом.

Многофакторная аутентификация

Для доступа к корпоративным ресурсам вы можете настроить многофакторную аутентификацию. Это увеличит уровень безопасности защищённой сети с помощью дополнительной проверки пользователя при подключении к ней. Пользователю потребуется ввести данные доменной учётной записи и использовать специальное приложение для аутентификации.

Чтобы настроить многофакторную аутентификацию:

- 1 Установите систему многофакторной аутентификации, см. документацию конкретной системы.
- 2 Разверните сервер аутентификации, см. «ViPNet Сервер многофакторной аутентификации. Руководство администратора».
- 3 Назначьте многофакторную аутентификацию пользователям.

Клиент поддерживает несколько приложений для аутентификации. В зависимости от настроек, в приложении нужно:

- Нажать кнопку в уведомлении о попытке входа, чтобы подтвердить, что это вы проходите аутентификацию. Уведомление приходит при каждой попытке входа.
- Получить одноразовый код и ввести его в ViPNet Client 5 for Linux. Одноразовый код действителен ограниченное время и уникален при каждом входе.

Если аутентификация не пройдена, пользовательский трафик будет заблокирован, но будут передаваться служебный и DNS-трафик: пользователь подключится к защищённой сети, но не сможет работать с корпоративными ресурсами.

Клиент поддерживает несколько способов многофакторной аутентификации. Подробнее см. руководство пользователя.

Назначение многофакторной аутентификации

- 1 Проверьте, что длина пароля доменной учётной записи пользователя не превышает 31 символ.
- 2 В управляющем ПО:
 - 2.1 Добавьте узлу пользователя связь с узлом `Client Auth Server`.



Внимание! В связях узла может быть только один узел, в имени которого есть слова `Client Auth Server`, иначе ключи не установятся.

- 2.2 Отправьте обновление справочников и ключей.

3 На компьютерах пользователей ViPNet Client 5 for Windows отключите быстрый запуск:

3.1 Откройте **Параметры > Система > Питание и спящий режим > Дополнительные параметры питания > Действия кнопок питания**.

3.2 В параметрах завершения работы отключите **Включить быстрый запуск (рекомендуется)**.

Отключать быстрый запуск необходимо, чтобы многофакторная аутентификация запрашивалась при каждом включении компьютера.

Про настройку системы многофакторной аутентификации см. в документации к конкретной системе.

В системах многофакторной аутентификации Multifactor и Аладдин JAS вы можете:

- разрешить пользователю выбирать способ аутентификации при каждом подключении к защищённой сети,
- назначить пользователю единственный способ аутентификации.

В Indeed AM вы можете назначить пользователю единственный способ аутентификации.

Пользователи, которым назначена многофакторная аутентификация, получают уведомления об этом. Подробнее см. руководство пользователя, раздел «Многофакторная аутентификация».

Для корректной работы многофакторной аутентификации пользователи не должны использовать режим гибернации.

Включение видимости туннелируемых узлов по виртуальным IP-адресам

Если IP-адреса туннелируемых узлов и IP-адреса локальной сети пересекаются, то могут возникать проблемы с подключением к туннелируемым ресурсам. Чтобы это исправить, включите видимость туннелируемых узлов по виртуальным IP-адресам.

Предварительные действия

Настройте корпоративные DNS-серверы, чтобы использовать видимость туннелируемых ресурсов по виртуальным IP-адресам. Если туннелируются все IP-адреса внешней сети, для этих DNS-серверов в управляющем ПО:

- ViPNet Prime включите настройку **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах**.
- ViPNet Administrator включите настройку **Использовать для разрешения имен публичных ресурсов только заданные DNS-серверы**.

Иначе при включении видимости по виртуальным IP-адресам не будет доступа к туннелируемым ресурсам.



Внимание! Для координатора, который туннелирует DNS-сервер или является DNS-сервером, нельзя выключать прикладные протоколы DNS.

Настройка на устройстве

Выполните:

```
user@host:~$ vipnetclient debug --tunnel-visibility {0 | 1}
```

где:

- 0 — видимость туннелируемых узлов по реальным IP-адресам.
- 1 — видимость туннелируемых узлов по виртуальным IP-адресам.

Значение по умолчанию — 0.

Настройка количества потоков обработки IP-трафика

По умолчанию драйверная часть ViPNet Client 5 использует четыре потока для обработки IP-трафика. Вы можете изменять количество потоков, чтобы регулировать скорость обработки IP-трафика. На скорость также влияют характеристики устройства: модель, тактовая частота и количество ядер процессора, операционная система. Поэтому на некоторых устройствах при увеличении количества потоков скорость обработки IP-трафика может не повышаться, а понижаться. Подбирайте оптимальное значение количества потоков индивидуально для каждого клиента.

1 В переменной окружения `ITCS_THREADS_COUNT` укажите количество потоков (от 1 до 1024):

- Если на устройстве используется `systemd` и выполнена интеграция ViPNet Client 5 с `systemd`:

```
user@host:~$ sudo systemctl set-environment ITCS_THREADS_COUNT=<количество потоков>
```

Чтобы проверить интеграцию ViPNet Client 5 с `systemd`:

```
user@host:~$ systemctl status vipnet <имя пользователя, под которым устанавливались ключи>.service
```

Если на устройстве со службой SELinux и `systemd` не выполнена интеграция ViPNet Client 5 с `systemd`, [создайте модуль локальной политики для службы SELinux](#).

- Если на устройстве нет `systemd`:

```
user@host:~$ ITCS_THREADS_COUNT=<количество потоков>
```

2 Завершите работу службы ViPNet Client:

```
user@host:~$ sudo killall vipnetclient
```

3 Убедитесь, что нет запущенных процессов ViPNet Client:

```
user@host:~$ ps -ef | grep vipnetclient
```

4 Включите VPN-соединение:

```
user@host:~$ vipnetclient start
```

Изменение используемых портов для прикладных протоколов

По умолчанию в ViPNet Client 5 for Linux для обработки прикладных протоколов используются стандартные значения портов:

- FTP (TCP) — 21.
- DNS (UDP) — 53.
- H.323 (UDP) — 1719, (TCP) — 1720.
- SCCP (TCP) — 2000.
- SIP (UDP, TCP) — 5060, 5068, 5080.

Если для каких-то приложений требуется обработка трафика по другим портам, вы можете передать настройки на устройства пользователей одним из способов:

- В [составе справочников из программы ViPNet ЦУС](#). В этом случае настройки применяются на устройствах пользователей автоматически. Подробнее см. в руководстве администратора ViPNet ЦУС.
- В виде политики безопасности из программы ViPNet Policy Manager или ViPNet Prime Policy Management по защищённой сети. В этом случае настройки применяются на устройствах пользователей автоматически. Подробнее о настройках политики и совместимости с ViPNet Client 5 см. в руководстве администратора ViPNet Policy Manager или ViPNet Prime Policy Management.



Примечание. Рекомендуется отправлять настройки на устройства пользователей в нерабочие часы, так как во время активной работы пользователей настройки протоколов применяются с задержкой. Если настройки отправлены в нерабочие часы, они будут применены незаметно для пользователей.

-
- В составе [расширенных настроек](#). В этом случае задайте значения портов в секции `firewall` в настройке `applicationLevelGateway`.

На устройствах пользователей будут использоваться настройки портов для обработки прикладных протоколов, применённые последними (вне зависимости от способа получения этих настроек).

Настройки в файле vipnet.conf

Вы можете задать дополнительные настройки ViPNet Client 5 с помощью файла `/etc/vipnet.conf`. Этот конфигурационный файл создаётся автоматически при установке ViPNet Client 5. Не удаляйте этот файл, иначе будет нарушена работа с DNS.

В файле `vipnet.conf` вы можете задать значения параметров:

- Секция `[global]`:
 - `config_dir` — путь к рабочему каталогу ViPNet, в котором хранятся конфигурационные файлы, справочники и ключи ViPNet, а также файлы аудита. По умолчанию эти файлы хранятся в каталоге `$HOME/.vipnet-vpn` (или `$HOME/.vipnet`). Если указать путь к рабочему каталогу ViPNet в файле `/etc/vipnet.conf`, то использовать установленные на компьютере справочники и ключи смогут все пользователи ОС.

Задайте этот параметр для установки ключей под учётной записью `root`. Это нужно для работы с ViPNet CSS Connect и ViPNet Деловая почта. Чтобы задать этот параметр, раскомментируйте строку с ним: сотрите символ `;` в начале строки.



Примечание. Если путь к рабочему каталогу ViPNet указан в файле `/etc/vipnet.conf`, то запустить графический интерфейс ViPNet Client 5 можно только с правами суперпользователя (`root`).

- `log_dir` — путь к каталогу с журналами ViPNet Client 5. Путь по умолчанию — `$HOME/.vipnet-vpn/var/log` (или `$HOME/.vipnet/var/log`). Чтобы задать этот параметр, раскомментируйте строку с ним: сотрите символ `;` в начале строки.
- `root-certificates` — путь к корневому сертификату из пакета корневых сертификатов `ca-certificates`. По умолчанию сертификаты хранятся в `/etc/ssl/certs`. Если на устройстве сертификаты хранятся в другом месте, задайте параметр одним из способов:
 - `root-certificates=<полный путь до каталога с корневым сертификатом>` — чтобы использовать сертификат из каталога.
 - `root-certificates=<полный путь до файла с корневым сертификатом>` — чтобы использовать сертификат из файла `ca-bundle` со всеми сертификатами.

Не используйте в этом параметре символические ссылки.

- Секция `[dns]`:
 - `iptables` — использовать утилиту `iptables` для перехвата всего DNS-трафика. Чтобы задать этот параметр, раскомментируйте строку с ним: сотрите символ `;` в начале строки. Вы можете установить следующие [способы обработки трафика](#):
 - `iptables=domain` — DNS-трафик на корпоративные DNS-зоны, настроенные в управляющем ПО, перехватывается `iptables` и направляется в ViPNet Client 5, а затем на защищённые DNS-серверы.

Направление DNS-трафика открытой сети зависит от того, установлен ли в управляющем ПО флажок **DNS-серверы поддерживают разрешение имен публичных ресурсов** или **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах**. Если флажок не установлен, DNS-трафик открытой сети передаёт DNS-клиент операционной системы на открытые DNS-серверы, указанные в настройках ОС. ViPNet Client 5 не участвует в передаче DNS-трафика открытой сети. Если флажок установлен, DNS-трафик открытой сети отправляется на DNS-серверы защищённой сети. При этом, если нет ответа от DNS-серверов защищённой сети, DNS-трафик открытой сети перенаправляется на доверенные открытые DNS-серверы, указанные в файле `/etc/vipnet.conf`.

- `iptables=on` — весь DNS-трафик перехватывается `iptables` и направляется в ViPNet Client 5. Затем ViPNet Client 5 отправляет DNS-трафик защищённой сети на защищённые DNS-серверы.

Направление DNS-трафика открытой сети зависит от того, установлен ли в управляющем ПО флажок **DNS-серверы поддерживают разрешение имен публичных ресурсов** или **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах**. Если флажок не установлен, DNS-трафик открытой сети отправляется на открытые DNS-серверы, указанные в файле `/etc/vipnet.conf`. Если флажок установлен, DNS-трафик открытой сети отправляется на DNS-серверы защищённой сети. При этом, если нет ответа от DNS-серверов защищённой сети, DNS-трафик открытой сети перенаправляется на доверенные открытые DNS-серверы, указанные в файле `/etc/vipnet.conf`.

- `iptables=off` — открытый DNS-трафик обрабатывается в соответствии с настройками ОС, а защищённый DNS-трафик для обработки передаётся через IP-адрес `11.254.254.254` в ViPNet Client 5. DNS-трафик открытой сети отправляется на открытые DNS-серверы, указанные в файле `/etc/vipnet.conf`.

Для корректной работы в список IP-адресов DNS-серверов в настройках ОС добавьте IP-адрес `11.254.254.254`.

По умолчанию `iptables=on`.

- о `trusted` — IP-адрес доверенного DNS-сервера для открытой сети. По умолчанию — `77.88.8.88, 77.88.8.2`. Задайте этот параметр, если `iptables=on` или в управляющем ПО установлен флажок **DNS-серверы поддерживают разрешение имен публичных ресурсов** или **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах**.

Пример содержимого файла `vipnet.conf`:

```
[global]
config_dir=/opt/vipnet
log_dir=/var/log
[dns]
trusted=77.88.8.88,77.88.8.2
iptables=on
```

Рекомендации по настройке работы с DNS

Порядок настройки

- 1 В корпоративной сети выделите DNS-серверы для обработки защищённого трафика. Эти DNS-серверы должны быть развёрнуты на узле, которому назначена роль DNS-сервер, или туннелироваться координаторами, которым назначена роль DNS-сервер.
- 2 В управляющем ПО:
 - 2.1 Добавьте в сеть ViPNet защищённые DNS-серверы.
 - 2.2 Укажите **корпоративные DNS-зоны** для защищённых DNS-серверов. Имена корпоративных DNS-зон должны быть до 126 символов.



Внимание! Задавайте корпоративные DNS-зоны для каждого защищённого DNS-сервера, иначе справочники и ключи не установятся и пользователи не смогут работать с ViPNet Client 5.

- 2.3 Чтобы DNS-трафик открытой сети отправлялся на DNS-серверы защищённой сети, включите:
 - в ViPNet ЦУС: **DNS-серверы поддерживают разрешение имен публичных ресурсов;**
 - в ViPNet Prime: **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах.**

При этом весь DNS-трафик будет передаваться в ViPNet Client 5, а потом на защищённые DNS-серверы. Это повысит уровень безопасности при работе с DNS.

- 2.4 Задайте DNS-серверы в настройках клиентов с ViPNet Client 5.

Если DNS-серверы не заданы, то DNS-трафик будет обрабатываться так же, как при включённых настройках **DNS-серверы поддерживают разрешение имен публичных ресурсов** или **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах.**

- 2.5 Отправьте справочники на узлы.

Подробнее см. документацию управляющего ПО.

- 3 На устройстве с ViPNet Client 5:
 - 3.1 В **настройках ОС** задайте доверенные DNS-серверы для обработки трафика открытой сети.
 - 3.2 В файле `vipnet.conf`:
 - Задайте **способ перехвата DNS-трафика** в параметре `iptables`.

- Если в управляющем ПО включено **DNS-серверы поддерживают разрешение имен публичных ресурсов** или **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах**, задайте доверенные DNS-серверы в параметре `trusted`.
 - Если `iptables={on|off}`, задайте доверенные DNS-серверы в параметре `trusted`.
- 3.3** Если на устройстве не используется утилита `iptables` и `iptables=off`, в список IP-адресов DNS-серверов в [настройках ОС](#) добавьте IP-адрес `11.254.254.254`.
- Если этого адреса не будет в списке DNS-серверов, то весь DNS-трафик будет обрабатываться ОС: не будет доступа к корпоративным ресурсам по доменным именам и к узлам по доменной зоне `.vipnet`.

Обработка DNS-трафика при включённом VPN-соединении

При включённом VPN-соединении DNS-трафик защищённой сети передаётся в ViPNet Client 5, а затем обрабатывается на защищённых DNS-серверах. DNS-трафик открытой сети может передаваться:

- в ViPNet Client 5, а затем на защищённые DNS-серверы;
- в ViPNet Client 5, а затем на DNS-серверы, заданные в файле `vipnet.conf`;
- на DNS-серверы, заданные в настройках ОС.

Передача всего DNS-трафика в ViPNet Client 5, а затем на защищённые DNS-серверы

При этом способе весь DNS-трафик передаётся в ViPNet Client 5, а затем отправляется на защищённые DNS-серверы. Если DNS-запросы открытой сети не удалось разрешить на защищённых DNS-серверах, то они передаются на доверенные DNS-серверы, указанные в [файле `vipnet.conf`](#).

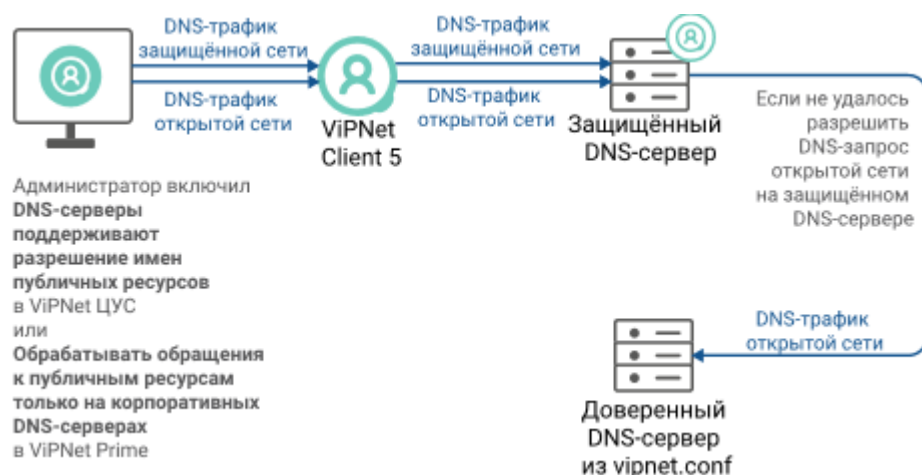


Рисунок 1: Обработка DNS-трафика на защищённых DNS-серверах

Чтобы использовать этот способ:

- Для защищённых DNS-серверов включите настройку в управляющем ПО:
 - в ViPNet ЦУС: **DNS-серверы поддерживают разрешение имен публичных ресурсов;**
 - ViPNet Prime: **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах.**



Примечание. Если на компьютере используется TCP DNS и в ViPNet Client 5 настроена видимость туннелей по виртуальным IP-адресам, доступ к защищённым узлам по доменным именам может не работать.

На трафик TCP DNS не распространяются настройки **DNS-серверы поддерживают разрешение имен публичных ресурсов** и **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах** из управляющего ПО.

- Если на устройстве используется утилита iptables, правило добавится в неё автоматически. Задайте в файле `vipnet.conf` доверенные DNS-серверы в параметре `trusted`.
- Если на устройстве не используется утилита iptables, задайте:
 - в файле `vipnet.conf`: `iptables=off` и доверенные DNS-серверы в параметре `trusted`;
 - **настройках ОС**: передачу всего DNS-трафика в ViPNet Client 5 через IP-адрес 11.254.254.254.

Этот же способ используется, если в управляющем ПО для клиентов с ViPNet Client 5 не настроены DNS-серверы.

Если в управляющем ПО для защищённых DNS-серверов отключено:

- **DNS-серверы поддерживают разрешение имен публичных ресурсов** в ViPNet ЦУС,
- **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах** в ViPNet Prime,

DNS-трафик защищённой сети обрабатывается на защищённых DNS-серверах, а обработка DNS-трафика открытой сети зависит от параметра `iptables` в файле `vipnet.conf`.

Передача DNS-трафика открытой сети в ViPNet Client 5, а затем на DNS-серверы из `vipnet.conf`

При этом способе весь DNS-трафик передаётся в ViPNet Client 5. Затем ViPNet Client 5 отправляет DNS-трафик защищённой сети на защищённые DNS-серверы, а DNS-трафик открытой сети — на доверенные DNS-серверы, указанные в файле `vipnet.conf` (по умолчанию: 77.88.8.88, 77.88.8.2).

Если на устройстве используется утилита iptables, в файле `vipnet.conf` задайте:

- `iptables=on` (задано по умолчанию);
- доверенные DNS-серверы в параметре `trusted`.

Правило обработки DNS-трафика добавится в утилиту iptables автоматически.

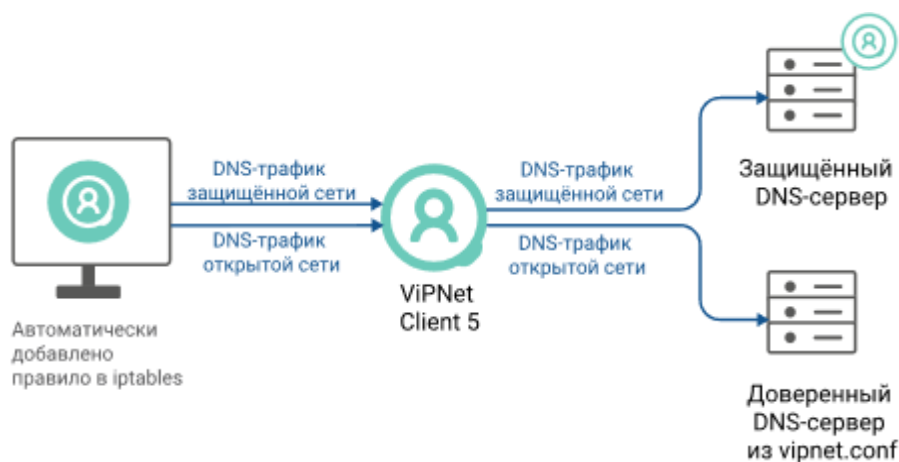


Рисунок 2. Обработка DNS-трафика, если `iptables=on`

Если на устройстве не используется утилита `iptables`, задайте:

- в файле `vipnet.conf`: `iptables=off` и доверенные DNS-серверы в параметре `trusted`;
- настройках ОС: передачу всего DNS-трафика в ViPNet Client 5 через IP-адрес `11.254.254.254`.

Как правило, DNS настраивается в графических инструментах настройки сети или в конфигурационных файлах ОС, подробнее см. документацию ОС. После настройки в ОС DNS-трафик защищённой сети отправляется на защищённые DNS-серверы. DNS-трафик открытой сети отправляется на доверенные DNS-серверы, указанные в файле `vipnet.conf`.

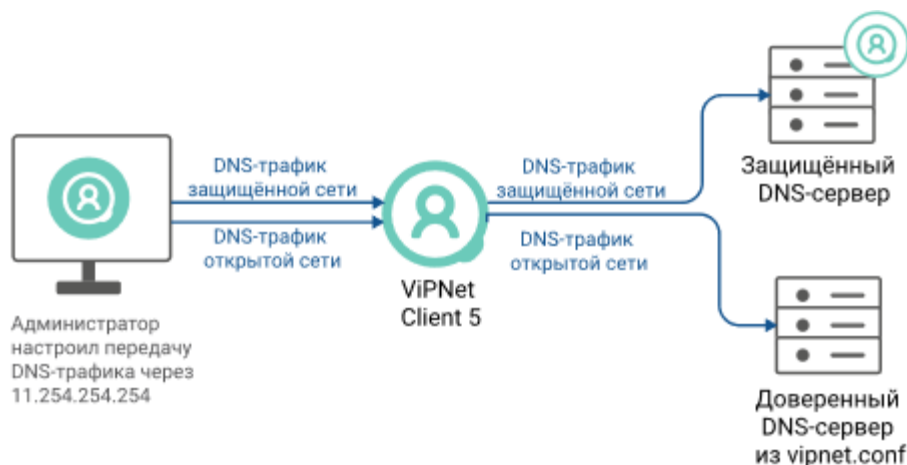


Рисунок 3. Обработка DNS-трафика, если на устройстве нет `iptables`

Передача DNS-трафика открытой сети на DNS-серверы из настроек ОС

При этом способе только DNS-трафик защищённой сети передаётся в ViPNet Client 5, а затем отправляется на защищённые DNS-серверы. DNS-трафик открытой сети отправляется на доверенные DNS-серверы, указанные в настройках ОС. Этот способ можно настроить, если на устройстве используется `iptables`.

Задайте:

- в файле `vipnet.conf`: `iptables=domain`.

- [настройках ОС](#): доверенные DNS-серверы.

Правило обработки DNS-трафика добавится в утилиту iptables автоматически.

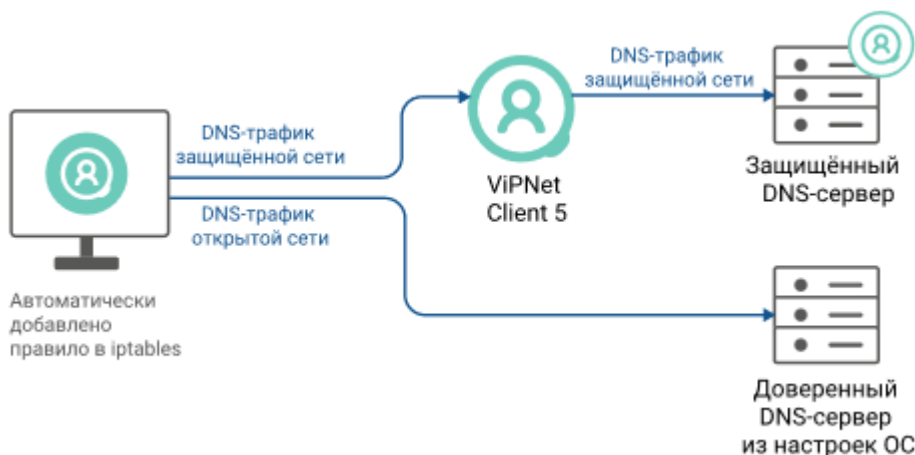


Рисунок 4. Обработка DNS-трафика, если `iptables=domain`

Обработка DNS-трафика при отключённом VPN-соединении

Если на устройстве отключено VPN-соединение, ViPNet Client 5 не перехватывает DNS-трафик, и он передаётся на доверенные DNS-серверы из настроек ОС. Задайте доверенные DNS-серверы в [настройках ОС](#).

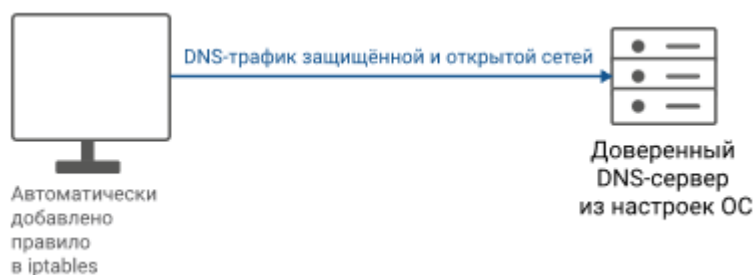


Рисунок 5. Обработка DNS-трафика, если отключено VPN-соединение

Настройка DNS в ОС

DNS настраивается разными утилитами в зависимости от ОС. Вы можете посмотреть, какая утилита управляет настройками DNS на вашем устройстве в `/etc/resolv.conf`.

В этом разделе собраны примеры настройки с помощью:

- NetworkManager;
- resolv.conf;

- systemd-resolved;
- Центра управления системой.

Внешний вид и расположение настроек могут отличаться в зависимости от версии и ОС.

Если в ОС управление системным DNS осуществляется через иные сервисы, обратитесь к документации данного сервиса и добавьте адрес DNS-сервера 11.254.254.254 и доменные имена защищённых ресурсов, которые были заданы администратором сети.

Если в ОС не заданы настройки системного DNS (например, IP-адрес, маска подсети, шлюз по умолчанию были заданы вручную), добавьте адрес DNS-сервера 11.254.254.254 в системные настройки DNS. Это нужно для доступа к корпоративным ресурсам по доменным именам и для доступности доменной зоны .vipnet.

NetworkManager

- 1 Перейдите в NetworkManager.
- 2 Откройте параметры IPv4.
- 3 Добавьте DNS-сервер 11.254.254.254.



Примечание. Если в настройках задано несколько DNS-серверов, 11.254.254.254 должен быть первым в списке.

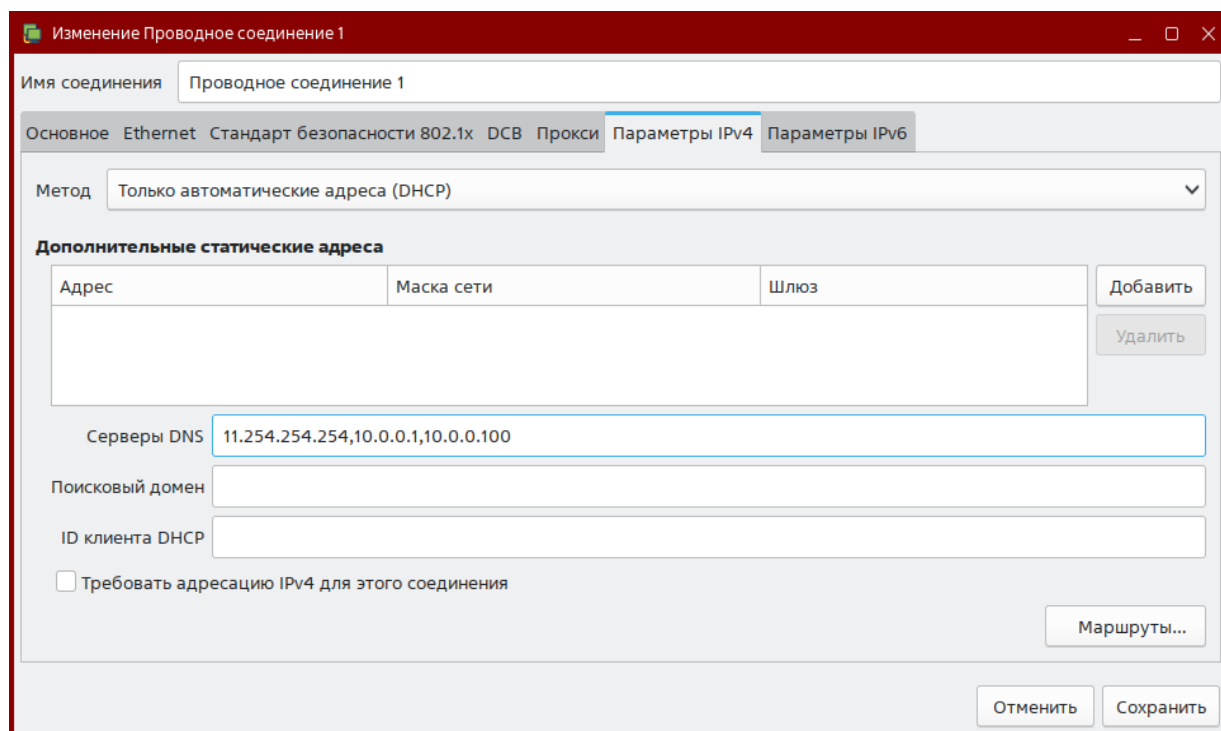


Рисунок 6. Настройка DNS через NetworkManager

resolv.conf

- 1 Откройте для редактирования конфигурационный файл `/etc/resolv.conf`.

- 2 Добавьте адрес DNS-сервера:

```
nameserver 11.254.254.254
```



Примечание. Если в файле задано несколько DNS-серверов, строка `nameserver 11.254.254.254` должна быть первой в списке заданных DNS-серверов.

```
nameserver 11.254.254.254
nameserver 10.0.0.1
nameserver 10.0.0.100
```

Рисунок 7. Настройка DNS через `resolv.conf`

systemd-resolved

- 1 Перейдите в режим редактирования конфигурационного файла

`/etc/systemd/resolved.conf`.

- 2 Раскомментируйте строку `DNS=` и укажите адрес DNS-сервера `11.254.254.254`:

```
DNS=11.254.254.254
```



Примечание. Если в строке `DNS` задано несколько DNS-серверов, `11.254.254.254` должен быть первым в списке.

- 3 Раскомментируйте строку `Domains=` и через пробел без запятых запишите `vipnet` и доменные имена защищённых ресурсов, которые были заданы администратором сети.

```
[Resolve]
# Some examples of DNS servers which may be used for DNS= and FallbackDNS=:
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com 2606:4700:4700::1111#cloudflare-dns.com 2606:4700:4700::1001#cloudflare-dns.com
# Google: 8.8.8.8#dns.google 8.8.4.4#dns.google 2001:4860:4860::8888#dns.google 2001:4860:4860::8844#dns.google
# Quad9: 9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net 2620:fe::fe#dns.quad9.net 2620:fe::9#dns.quad9.net
DNS=11.254.254.254 10.0.0.1 10.0.0.100
#FallbackDNS=
Domains=example.ru vipnet
#DNSSEC=no
#DNSOverTLS=no
#MulticastDNS=no
#LLMNR=no
#Cache=no-negative
#CacheFromLocalhost=no
#DNSStubListener=yes
#DNSStubListenerExtra=
#ReadEtcHosts=yes
#ResolveUnicastSingleLabel=no
#StaleRetentionSec=0
```

Рисунок 8. Настройка DNS через `systemd-resolved`

- 4 Перезапустите `systemd-resolved`:

```
root@host:~# systemctl restart systemd-resolved
```

- 5 Очистите DNS-кэш:

```
root@host:~# systemd-resolve --flush-caches
```

или

```
root@host:~# resolvectl flush-caches
```

Центр управления системой

- 1 Откройте Центр управления системой.
- 2 В настройках сети найдите Ethernet-интерфейсы
- 3 Добавьте DNS-сервер 11.254.254.254.



Примечание. Если в настройках задано несколько DNS-серверов, 11.254.254.254 должен быть первым в списке.

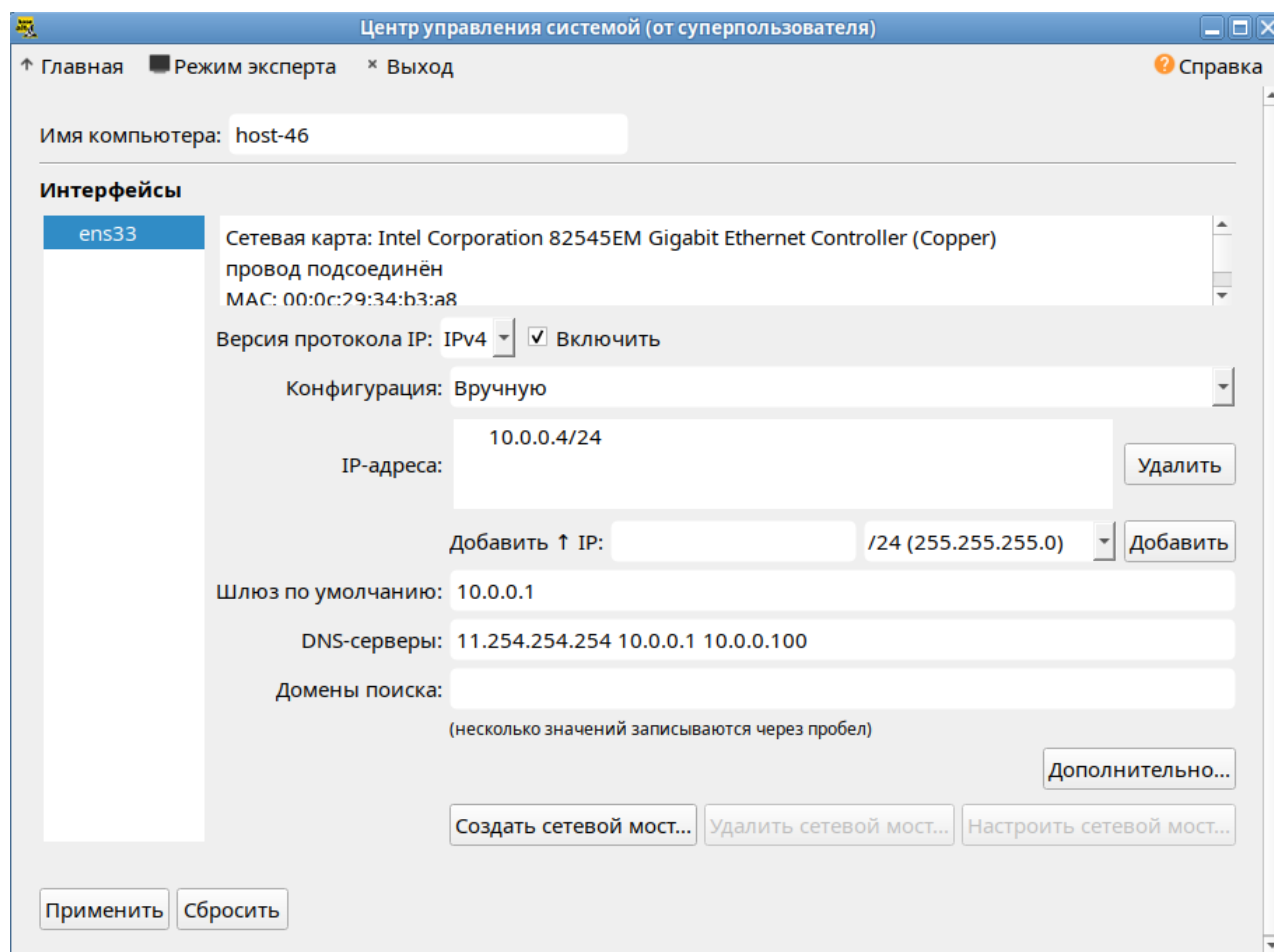


Рисунок 9. Настройка DNS через Центр управления системой

Поиск DNS

В ViPNet Client 5 реализованы служебные DNS-зоны `.vipnet` и `.in-addr.arpa`. DNS-запросы с именами `<идентификатор_узла_ViPNet>.vipnet` и `<IP-адрес_туннеля>.<идентификатор_туннелирующего_координатора>.vipnet` разрешаются внутри ViPNet Client 5 в IP-адреса видимости этих узлов.

Для проверки доступности ресурсов командой `ping` используйте флаг `-n`. Например:

```
ping -n <ID узла>.vipnet
```

```
ping -n ya.ru
```

ViPNet Client 5 перехватывает все запросы на [обратный поиск DNS](#) и отправляет их на защищённые DNS-серверы. Для обратного поиска доменных имён из зоны `.vipnet` в запросах на обратный поиск DNS в качестве IP-адреса назначения укажите `11.254.254.253`.

Пример прямого поиска DNS:

```
nslookup 00040009.vipnet
```

Пример обратного поиска DNS:

```
nslookup 7.4.0.9 11.254.254.253
```

Если в ОС не заданы настройки системного DNS (например, IP-адрес, маска подсети, шлюз по умолчанию были заданы вручную), [добавьте адрес DNS-сервера](#) `11.254.254.254` в системные настройки DNS. Это нужно для доступа к корпоративным ресурсам по доменным именам и работы DNS-зоны `vipnet`. В этом случае для прямого поиска добавьте к запросу `11.254.254.254`, например:

```
nslookup 00040009.vipnet 11.254.254.254
```

Способ выбора координатора

Если:

- несколько координаторов из связей клиента туннелируют одинаковые IP-адреса,
- связь с одним из координаторов пропадает,

клиент определяет, какие IP-адреса стали недоступны, и подключается к другому координатору, который туннелирует эти IP-адреса. По умолчанию клиент выбирает координатор с меньшим идентификатором узла.

Чтобы клиент выбирал текущий активный координатор из группы серверов:

- 1 Добавьте связи между координаторами, которые туннелируют одинаковые IP-адреса.
- 2 На координаторах задайте разные диапазоны виртуальных IP-адресов. Подробнее см. документацию координаторов.
- 3 На общих туннелируемых ресурсах настройте статическую маршрутизацию до адресов координаторов, заданных на шаге 2.

Например, если:

- на координаторе А заданы адреса 11.0.0.0/8,
- на координаторе В заданы адреса 13.0.0.0/8,

то на туннелируемом ресурсе нужно создать статические маршруты:

- на адреса 11.0.0.0/8 через координатор А,
- на адреса 13.0.0.0/8 через координатор В.

- 4 В клиентах с ключами `*.dst` включите настройку **Группа серверов**, см. руководство пользователя, раздел «Экспериментальные настройки».
- 5 В расширенных настройках [задайте параметры в секции features](#):

`features:`

```
- name: tunnel_priority
  mode: active_coordinator
```

Координаторы в группе серверов

Если включена настройка **Группа серверов**, ViPNet Client 5 автоматически переключается на другой сервер соединений, когда активный координатор недоступен. Вы можете [просмотреть информацию о настройке](#).

Новый сервер соединений выбирается из группы серверов. В группу серверов для клиента с ключами *.dst входят все координаторы своей сети, с которыми у узла есть связь.

Для клиентов с ключами *.ds5 состав группы серверов зависит от настроек в ViPNet Prime. Если для координатора, на котором зарегистрирован клиент, задан способ подключения к внешней сети:

- **Координатор доступен напрямую**, то в группу входит только координатор, на котором зарегистрирован клиент.
- **Координатор доступен с использованием сервера соединений**, то в группу входят:
 - координатор, на котором зарегистрирован клиент,
 - координатор с вершины цепочки координаторов, для которого задан способ подключения к внешней сети **Координатор доступен напрямую**.

При потере работоспособности этого координатора будут недоступны все координаторы цепочки, и на узле не будет работать VPN-соединение.

Пример 1:

- Клиент зарегистрирован на координаторе А.
- Координатор А доступен с использованием сервера соединений.
- Сервер соединений координатора А — координатор Б.
- Координатор Б доступен напрямую.

В группе серверов соединений клиента будут координаторы А и Б.

Пример 2:

- Клиент зарегистрирован на координаторе А.
- Координатор А доступен с использованием сервера соединений.
- Сервер соединений координатора А — координатор Б.
- Координатор Б доступен с использованием сервера соединений.
- Сервер соединений координатора Б — координатор С.
- Координатор С доступен напрямую.

В группе серверов соединений клиента будут только координаторы А и С.

Подключение к узлам напрямую

Вы можете задать узлы, с которыми клиент будет взаимодействовать напрямую, в режиме «точка-точка», чтобы:

- гибко организовывать топологию сети и оптимизировать маршруты между узлами.
- снизить нагрузку на координаторы, к которым регулярно подключается большое количество узлов в сети.

Например, чтобы снизить нагрузку на координатор, который используется для подключения к серверу ViPNet CSS FileExchange, вы можете настроить подключение клиентов к серверу ViPNet CSS FileExchange напрямую.

Это экспериментальная функция, доступно два режима:

- По возможности подключаться к узлам напрямую.

При появлении пользовательского защищённого трафика клиент попытается подключиться к узлу. Если клиент подключится к одному из доступных портов узла, то между узлами установится соединение в режиме «точка-точка». При отсутствии трафика между узлами более 75 секунд или после приёма обновлений справочников и ключей режим «точка-точка» отменится: когда трафик снова появится, клиент будет заново проверять доступность портов и пробовать установить соединение напрямую. Если все порты недоступны, соединение установится через активный координатор.

- Подключаться к узлам только напрямую.

Клиент будет устанавливать соединение с узлом только в режиме «точка-точка». Если порт узла недоступен, не будет соединения между узлами.

Чтобы выбрать режим и настроить соединение между узлами, [задайте для этих узлов параметры в секции nodes:](#)

```
nodes:
  flags:
    идентификатор узла:
      forceStaticAccessPoints: {false | true}
      useStaticKeepAlive: {false | true}
  staticAccessPoints:
    идентификатор узла:
      - "IP-адрес:порт"
```

Управление настройками ViPNet Client 5 for Linux

Вы можете задать настройки ViPNet Client 5 for Linux централизованно в управляющем ПО или вручную на устройстве пользователя.

Если в управляющем ПО настройки заданы в [секции secured](#), они будут иметь приоритет над настройками, заданными по умолчанию и вручную. Эти настройки нельзя будет изменить локально.

Настройка из управляющего ПО



Внимание! В ViPNet Administrator вы можете задать индивидуальные настройки всем клиентам.

В ViPNet Prime версии 1.9.5 и выше вы можете задать одинаковые настройки всем клиентам. Индивидуальные настройки для отдельных клиентов задавайте вручную на устройствах пользователей.

[Укажите параметры](#) в формате YAML в расширенных настройках клиентов с ViPNet Client 5 for Linux. Настройки передаются в ViPNet Client 5 for Linux в составе справочников. Размер справочника должен быть до 1 Мбайта. Подробнее см. руководство администратора управляющего ПО.

Расширенные настройки в управляющем ПО нельзя задать для туннелирующего клиента.

Настройка на устройстве пользователя.

- 1 Создайте файл `<имя_файла>.vpnconfig`.

Размер файла должен быть до 1 Мбайта.

- 2 [Укажите параметры](#) в формате YAML в кодировке UTF-8 (без BOM).

- 3 Выключите VPN-соединение.

- 4 Примените файл `<имя_файла>.vpnconfig`.

```
user@host:~$ vipnetclient debug --user-vpnconfig <имя_файла>.vpnconfig
```

- 5 Включите VPN-соединение.

Параметры ViPNet Client 5

Секция secured

Параметры, которые можно изменить только из управляющего ПО.

Чтобы запретить изменять какие-либо параметры локально на устройстве пользователя, задайте их в этой секции. Если параметры не будут заданы в секции `secured`, их можно будет изменить, применив файл `*.vpnconfig` на устройстве пользователя.

Некоторые параметры можно изменить только из управляющего ПО, даже если они не заданы в этой секции:

- `macSpoofingProtection`
- `allowedPacketTimeDiff`

Секция policies

- `restrictedTrafficModeExclusions` — узлы, на которых будет разрешён пользовательский трафик, даже если его блокирует сторонний процесс или не пройдена многофакторная аутентификация.

Если в сети один координатор туннелирует все ресурсы, то при добавлении этого координатора в `restrictedTrafficModeExclusions` будет разрешён весь трафик, который проходит через этот координатор.

Этот параметр можно задать только из управляющего ПО. Его значение имеет приоритет над значением, полученным из ViPNet Policy Manager или ViPNet Prime Policy Management.

`policies:`

```
restrictedTrafficModeExclusions:  
  - 0x<идентификатор узла>  
  - 0x<идентификатор узла>
```

Чтобы снова блокировать пользовательский трафик на узле, удалите узел из списка и отправьте обновление расширенных настроек.

Чтобы удалить из списка все узлы, отправьте обновление расширенных настроек без параметра или с пустым параметром:

`policies:`

```
restrictedTrafficModeExclusions: []
```

Если вы удалите из списка все узлы, и для этих узлов задавались правила фильтрации трафика в ViPNet Policy Manager или ViPNet Prime Policy Management, эти правила начнут действовать на этих узлах.

Секция dns

- `trustedServers` — IP-адреса доверенных DNS-серверов для открытой сети. Вы можете задать до двух IP-адресов.

Значения, заданные в `trustedServers`, имеют приоритет над настройками из файла `vipnet.conf`.

Значение в ViPNet Client 5 for Linux по умолчанию — `77.88.8.88, 77.88.8.2`.

Секция network

- `privateSubnet` — диапазон уникальных частных IP-адресов, который будет использоваться в сети ViPNet.

По умолчанию в ViPNet Client 5 for Linux IP-адрес назначается в виде `7.0.id.id`, где `id.id` — уникальный идентификатор узла в сети ViPNet. С помощью параметра `privateSubnet` вы можете задать первые два октета IP-адреса. Вместо вторых двух октетов укажите `0.0`, они будут сформированы ViPNet Client 5 for Linux автоматически (см. [Технология обработки трафика в ViPNet Client 5](#)).

Например, чтобы изменить IP-адрес узла с `7.0.35.223` на `172.17.35.223`, укажите `privateSubnet: 172.17.0.0`.

После изменения параметра `privateSubnet` перезапустите на устройстве все сервисы, которые использовали сеть ViPNet и виртуальный сетевой интерфейс TUN. Также измените адрес сетевого интерфейса TUN во всех конфигурационных файлах сервисов, где он указан.

Примечание.



- Настройка `privateSubnet` меняет только IP-адреса узлов своей сети ViPNet. Для узлов других сетей адресация не изменится.
- Адреса на интерфейсе TUN должны отличаться от адресов физических интерфейсов в ОС.

- `tcpMssDecrease` — уменьшение параметра MSS (максимальный размер сегмента) для протокола TCP на указанное число байт. Вы можете указать число из диапазона `0–1024`. Изменять значение параметра MSS рекомендуется, только если между собственным и другими защищёнными или туннелируемыми узлами успешно проходит проверка соединения (`ping`), но не устанавливается TCP-соединение из-за фрагментации пакетов на устройствах, стоящих на пути от отправителя к получателю.

Во избежание фрагментации входящих пакетов рекомендуется установить значение MSS от 20 до 40 байт. Чтобы уменьшить размер исходящих пакетов, значение параметра MSS следует изменить на узле получателя пакетов.

Значение в ViPNet Client 5 for Linux по умолчанию — `0`.

- `mtuOnTun` — максимальный размер исходящего пакета на TUN-интерфейсе устройства в байтах. Чтобы оптимизировать передачу данных через TUN-интерфейс, вы можете изменить размер MTU в диапазоне `1280–9000` байт.

Значение в ViPNet Client 5 for Linux по умолчанию — `1500`.

Секция settings

- `authBeforeOsLogon` — отображение окна аутентификации ViPNet Client 5 for Linux до аутентификации пользователя в ОС. Вы можете указать одно из значений:
 - `true` — окно аутентификации ViPNet Client 5 for Linux отображается до аутентификации пользователя в ОС.
 - `false` — окно аутентификации ViPNet Client 5 for Linux не отображается до аутентификации пользователя в ОС.

Значение в ViPNet Client 5 for Linux по умолчанию — `false`.



Примечание. Отображение окна аутентификации в ViPNet Client 5 до аутентификации пользователя в ОС возможно только для версий ViPNet Client 5 с графическим интерфейсом и если [ключи были установлены под учётной записью root](#).

- `macSpoofingProtection` — блокировка трафика от отправителя некорректных пакетов в защищённой сети. При взаимодействии с узлами клиент проверяет целостность пакетов, которые приходят от этих узлов. Если какой-то узел отправляет пакеты, целостность которых нарушена, клиент может временно заблокировать трафик от этого узла.
 - `true` — при получении 20 некорректных пакетов за 5 секунд клиент блокирует трафик от отправителя этих пакетов на 20 секунд.
 - `false` — клиент не блокирует трафик от отправителя некорректных пакетов.

Значение в ViPNet Client 5 for Linux по умолчанию — `true`.

Этот параметр можно задать только из управляющего ПО.

- `allowedPacketTimeDiff` — допустимый интервал времени между отправкой и получением пакета в защищённой сети. Устаревшие пакеты могут содержать неактуальную информацию и негативно влиять на работу защищённой сети. Если с момента отправки пакета прошло больше времени, чем задано в этом параметре, клиент не примет такой пакет.

Вы можете задать интервал от 0 до 7200 секунд. При настройке учитывайте разницу во времени между узлами (по UTC): если она больше, чем значение параметра, узлы не будут принимать пакеты. Подбирайте оптимальное значение параметра индивидуально для каждой сети.

Значение в ViPNet Client 5 for Linux по умолчанию — 7200 (2 часа).

Этот параметр можно задать только из управляющего ПО.

Секция firewall

- `blockOpenNetwork` — блокировка всего открытого IP-трафика устройства при включённом VPN-соединении, кроме открытого трафика, необходимого для работы ОС и ViPNet Client 5 for Linux. Вы можете указать одно из значений:
 - `true` — открытый трафик блокируется.

- `false` — открытый трафик разрешён.
- Значение в ViPNet Client 5 for Linux по умолчанию — `false`.



Примечание. Если параметр `blockOpenNetwork` не задан в секции `secured`, вы можете изменить его из консоли. Тогда значение, заданное из консоли, будет приоритетнее заданного вручную или полученного из управляющего ПО. Если параметр `blockOpenNetwork` задан в секции `secured`, его можно изменить только из управляющего ПО.

- `applicationLevelGateway` — порты для обработки прикладных протоколов. Укажите номера портов для каждого протокола. Если нужно задать несколько портов, каждый порт указывайте с новой строки.

Чтобы не использовать протокол, задайте `<название протокола>: []`. Например `udr: []`.

Значение в ViPNet Client 5 for Linux по умолчанию:

```
dns:
  udp:
    - 53
ftp:
  tcp:
    - 21
h.323:
  tcp:
    - 1720
  udp:
    - 1719
sccp:
  tcp:
    - 2000
sip:
  tcp:
    - 5060
    - 5068
    - 5080
  udp:
    - 5060
    - 5068
    - 5080
```



Внимание! Если вы задаёте настройку `applicationLevelGateway`, указывайте значения портов для каждого прикладного протокола, иначе будут использоваться значения по умолчанию.

Секция logging

- `level` — уровень детализации в журнале. Доступно 11 уровней. Чтобы получить отладочную информацию, установите значение 5. Если этот параметр задан в секции `secured`, то для новых профилей будет использоваться значение, которое задал администратор при создании ключей или значение по умолчанию. Если этот параметр не задан в секции `secured`, то для новых профилей будет использоваться то значение, которое устанавливали на устройстве последним. Значение в ViPNet Client 5 по умолчанию — 3.

Секция nodes

Секция `privateAddressAssignment`:

- `strategy` — алгоритм назначения IP-адресов для узла. В одной сети должны использоваться одинаковые алгоритмы.
 - `default` — стандартный алгоритм назначения IP-адресов.
 - `BUNCHES_8x8K` — альтернативный алгоритм назначения IP-адресов в сетях, в которых до 8 координаторов и до 8 тысяч узлов за каждым координатором.
 - `BUNCHES_4x16K` — альтернативный алгоритм назначения IP-адресов в сетях, в которых до 4 координаторов и до 16 тысяч узлов за каждым координатором.

Описание альтернативных алгоритмов см. в «ViPNet Administrator 4. Настройка алгоритма назначения сетевых адресов».

Значение в ViPNet Client 5 for Linux по умолчанию — `default`.

- `bunchesGatewaysList` — список сетевых адресов координаторов, на основе которых формируется порядковый номер координатора в правилах `BUNCHES_8x8K` и `BUNCHES_4x16K`. Если не задан или содержит пустой список, то в правилах назначения IP-адресов используется адрес узла из справочника.

Секция `flags`:

- `forceStaticAccessPoints` — режим взаимодействия между клиентами без участия координатора. Задайте эту настройку на каждом из узлов, между которыми нужно настроить взаимодействие напрямую.

Укажите значение параметра для каждого узла, к которому надо подключаться напрямую, в формате:

`flags:`

идентификатор узла:

`forceStaticAccessPoints: {false | true}`

Узлы, к которым надо подключаться напрямую, перечислите в секции `staticAccessPoints`.

- `false` — по возможности подключаться к узлам напрямую.

В этом режиме можно задать до десяти IP-адресов с портами для каждого узла, к которому нужно подключаться напрямую. При появлении пользовательского защищённого трафика

клиент попытается подключиться к узлу. Если клиент подключится к одному из доступных портов узла, то между узлами установится соединение в режиме «точка-точка». При отсутствии трафика между узлами более 75 секунд или после приёма обновления справочников и ключей режим «точка-точка» отменится: когда трафик снова появится, клиент будет заново проверять доступность портов и пробовать установить соединение напрямую. Если все порты недоступны, соединение установится через активный координатор.

- `true` — подключаться к узлам только напрямую.

В этом режиме можно задать только один IP-адрес и порт для каждого узла, к которому нужно подключаться напрямую. Если задано несколько IP-адресов с портами, будет использоваться только первый из списка. Если порт доступен, между узлами установится соединение в режиме «точка-точка». Если порт недоступен, не будет соединения между узлами.

- `useStaticKeepAlive` — периодически отправлять служебные сообщения, чтобы поддерживать соединение между узлами. Если соединение устанавливается через промежуточное сетевое оборудование, включите этот параметр. Если клиенты расположены в одной подсети и могут подключаться друг к другу без промежуточного оборудования, или сети ограничены в скорости, вы можете выключить этот параметр.

- `true` — отправляются служебные сообщения. Периодичность отправки зависит от периода опроса координатора, заданного в управляющем ПО (по умолчанию — 25 секунд).

- `false` — не отправляются служебные сообщения.

Значение в ViPNet Client 5 for Linux по умолчанию — `true`. Чтобы выключить эту настройку, задайте значение `false` для каждого узла, для которого не нужно отправлять служебные сообщения:

flags:

идентификатор узла:

```
forceStaticAccessPoints: {false | true}
```

```
useStaticKeepAlive: {false | true}
```

Секция `staticAccessPoints`: список узлов, их IP-адресов и портов, к которым клиент будет подключаться напрямую. Задайте эту настройку на каждом из узлов, между которыми нужно настроить взаимодействие напрямую. Вы можете задать до 10 узлов.

Укажите значение параметра для каждого узла, к которому надо подключаться напрямую, в формате:

`staticAccessPoints:`

идентификатор узла:

– "IP-адрес:порт"

Чтобы задать порт для собственного узла:

```
staticAccessPoints:

    идентификатор узла:

        - "0.0.0.0:порт"
```

Секция features

- `name: tunnel_priority` — способ выбора координатора, если несколько координаторов из связей клиента туннелируют один IP-адрес и связь с одним из координаторов пропадает. Клиент определяет, какие IP-адреса стали недоступны, и подключается к другому координатору, который туннелирует эти IP-адреса.
 - `mode: min_id` — выбирается координатор с меньшим идентификатором узла.
 - `mode: active_coordinator` — выбирается текущий активный координатор из группы серверов.

Чтобы использовать этот способ для клиентов с ключами `*.dst`, включите настройку **Группа серверов** (см. руководство пользователя, раздел «Экспериментальные настройки»).

Значение в ViPNet Client 5 for Linux по умолчанию — `min_id`.

Секция updates

Параметры для обновления клиентов с ключами `*.ds5` из ViPNet Prime:

- `url` — путь к ZIP-архиву с обновлением на HTTP-сервере.
- `name` — произвольное наименование файла обновления.
- `product: vpn-client`.
- `brand: vipnet`.
- `version` — версия обновления.
- `platform: linux`.
- `arch` — архитектура процессора: `x86_64`, `armv5el`, `armv7hf`, `armv8`, `mips`.
- `edition` — список особенностей.

Криптография:

- `gost` — ГОСТ, Магма, Кузнечик,
- `hybrid` — ГОСТ, Магма, Кузнечик, AES, FIPS.

Установочный пакет: `deb`, `rpm`, `ipk`.

Дистрибутив Linux:

- `astra_se` — Astra Linux Special Edition,
- `osnova` — Основа,

- o `generic` — остальные дистрибутивы.

Исполнение:

- o `cli` — консольная версия,
- o `gui` — графическая версия.
- `retry_timeout` — время повторного запроса на HTTP-сервер в случае ошибки в секундах. Необязательный параметр. Вы можете указать значение от 30 до 86400 (24 часа). Значение по умолчанию — 300 (5 минут).

Укажите все параметры для каждого ZIP-архива с обновлением. Тогда каждый клиент сможет установить обновление, которое ему подходит.

Пример настроек

secured:

- network.privateSubnet
- firewall.blockOpenNetwork

policies:

restrictedTrafficModeExclusions:

- 0x12340005
- 0x12340006
- 0x12340007

dns:

trustedServers:

- 77.88.8.8
- 77.88.8.1

settings:

authBeforeOsLogon: true
macSpoofingProtection: true
allowedPacketTimeDiff: 7200

features:

- name: tunnel_priority
mode: active_coordinator

network:

privateSubnet: 10.136.0.0
tcpMssDecrease: 20
mtuOnTun: 1300

firewall:

blockOpenNetwork: true
applicationLevelGateway:

dns:

udp:
- 53

ftp:

tcp:
- 21

h.323:

tcp:
- 1720

udp:
- 1719

sccp:

tcp:
- 2000

sip:

tcp:

```

        - 5065
        - 5068
        - 5080
    udp:
        - 5060
        - 5068
        - 5080
logging:
    level: 3
nodes:
    privateAddressAssignment:
        strategy: BUNCHES_4x16K
        bunchesGatewaysList:
            - 12340000
            - 12340000
            - 12340000
            - 12340000
    flags:
        0004008A:
            forceStaticAccessPoints: true
            useStaticKeepAlive: true
    staticAccessPoints:
        0004008A:
            - "192.168.1.71:55778"
updates:
    - url: "путь к ZIP-архиву с обновлением на HTTP-сервере"
      name: client-linux-cli_gost_x86_64_update_5.1.4.zip
      product: vpn-client
      brand: vipnet
      version: 5.1.4
      platform: linux
      arch: x86_64
      edition: [gost, cli, deb, generic]
      retry_timeout: 300

```

Переинициализация внутренних конфигурационных файлов

В случае повреждения внутренних конфигурационных файлов ViPNet Client 5 при сбое ОС, неудачном обновлении справочников и ключей или других нештатных ситуациях, вы можете создать эти файлы заново на основе последних актуальных справочников:

- 1 Выключите VPN-соединение:

```
user@host:~$ vipnetclient stop
```

- 2 Выполните:

```
user@host:~$ vipnetclient reconfigure
```



Примечание. Переинициализация не затрагивает `vipnet.conf` и `vipnet_token.conf`, а также настройки, заданные через команды `vipnetclient`.

Если вы изменяли активный координатор, то после сброса внутренних конфигурационных файлов клиента активным снова станет координатор, заданный в управляющем ПО. Чтобы активным оставался координатор, выбранный вручную в ViPNet Client 5 for Linux, включите настройку **Сохранять выбор сервера**. См. руководство пользователя, раздел «Экспериментальные настройки».

Работа с транспортным модулем

По умолчанию транспортный модуль MFTP или UT из состава ViPNet Client 5 проверяет наличие обновлений справочников и ключей раз в 5 минут. Вы можете проверить обновления вручную, например в диагностических целях, или если хотите получить обновления быстрее.

- Проверить обновления справочников и ключей:

```
user@host:~$ vipnetclient transport peep
```

- Применить обновления справочников и ключей:

```
user@host:~$ vipnetclient transport cms <путь к файлу обновления *.ctl или *.bin>
```

Вы можете просмотреть журнал транспортных конвертов:

```
user@host:~$ vipnetclient transport events
```

Чтобы просмотреть информацию о команде:

```
user@host:~$ vipnetclient transport --help
```

Настройка журнала событий

Информация о событиях ViPNet Client 5 записывается в журнал. По умолчанию файл журнала располагается в `<рабочий_каталог_ViPNet>/var/log` или

`<домашний_каталог>/.vipnet-vpn/var/log` (или `<домашний_каталог>/.vipnet/var/log`).

Расположение файла журнала можно изменить с помощью файла `vipnet.conf`. Когда размер файла журнала достигает 10 Мбайт, выполняется автоматическая ротация файлов.

Чтобы настроить уровень детализации событий ViPNet Client 5, записываемых в журнал:

- выполните:

```
user@host:~$ vipnetclient debug --loglevel <уровень_детализации>
```
- выберите уровень детализации на вкладке **Настройки** в интерфейсе ViPNet Client 5,
- задайте параметр `level` в расширенных настройках клиентов в управляющем ПО или на компьютере пользователя.

Если этот параметр задан в секции `secured`, то для новых профилей будет использоваться значение, которое задал администратор при создании ключей или значение по умолчанию.

Если этот параметр не задан в секции `secured`, то для новых профилей будет использоваться то значение, которое устанавливали на устройстве последним.

Возможные значения уровня детализации:

- 0 — в журнал записываются только критичные ошибки.
- 1 — в журнал записываются события уровня 0 и некритичные ошибки.
- 2 — в журнал записываются события уровней 0, 1 и уведомления.
- 3 — в журнал записываются события уровней 0, 1, 2 и информационные события.
- 4 — в журнал записываются события уровней 0, 1, 2, 3 и события режима отладки.
- 5 — в журнал записываются события уровней 0, 1, 2, 3, 4 и детальные события работы приложения.

По умолчанию используется уровень 3.

Просмотр журнала IP-пакетов

В ViPNet Client 5 ведётся журнал регистрации IP-пакетов, в который записывается информация обо всех IP-пакетах, передаваемых или получаемых через сеть ViPNet. На основе информации из журнала IP-пакетов вы можете анализировать и контролировать взаимодействие компьютера с ViPNet Client 5 с другими узлами сети ViPNet.

Чтобы просмотреть журнал IP-пакетов:

- 1 Выполните:

```
user@host:~$ vipnetclient dbviewer
```

- 2 Подождите завершения выполнения команды. Это может занять некоторое время.

В результате в консоли отобразится информация о переданных и полученных IP-пакетах за последние 7 дней (не более 65536 записей).

```
user@host:~$ vipnetclient dbviewer
```

Time begin	Time end	Dev	Eth	Flags	Prot	Source IP	Port	Destination IP	Port	Size	Cnt	Src Node
14.04.2025 10:06:03	14.04.2025 10:06:03	tun	800h	<D----	tcp	7.0.23.56	55740	185.125.190.17	80	60	1	00000000
00000000 22 - Non-encrypted IP Packet from network node												
14.04.2025 10:06:03	14.04.2025 10:06:03	tun	800h	<D----	tcp	7.0.23.56	36574	91.189.91.96	80	60	1	00000000
00000000 22 - Non-encrypted IP Packet from network node												
14.04.2025 10:06:03	14.04.2025 10:06:03	tun	800h	<D----	tcp	7.0.23.56	45212	185.125.190.97	80	60	1	00000000
00000000 22 - Non-encrypted IP Packet from network node												
14.04.2025 10:06:03	14.04.2025 10:06:03	tun	800h	<-C---	udp	7.0.23.56	2046	10.10.88.67	2049	72	1	22E11738
22E11732 40 - Encrypted IP packet allowed												
14.04.2025 10:06:03	14.04.2025 10:06:03	tun	800h	<-C---	udp	7.0.23.56	2046	81.30.192.133	2049	72	1	22E11738
22E11732 40 - Encrypted IP packet allowed												
14.04.2025 10:06:03	14.04.2025 10:06:03	tun	800h	<-C---	udp	7.0.23.56	2046	7.0.23.50	2046	29	1	22E11738
22E11732 40 - Encrypted IP packet allowed												
14.04.2025 10:06:04	14.04.2025 10:06:04	tun	800h	<-C---	udp	7.0.23.56	2046	7.0.23.50	2046	245	1	22E11738
22E11732 40 - Encrypted IP packet allowed												
14.04.2025 10:06:04	14.04.2025 10:06:04	tun	800h	<-C---	udp	7.0.23.56	2046	10.10.88.67	2049	72	1	22E11738
22E11732 40 - Encrypted IP packet allowed												

Рисунок 10. Просмотр журнала IP-пакетов

Настройка передачи данных по протоколу TCP

Если пользователь наблюдает нестабильное подключение к защищённой сети, это может быть вызвано тем, что провайдер блокирует передачу трафика по протоколу UDP. В таких условиях вы можете переключить ViPNet Client 5 на передачу трафика по протоколу TCP, чтобы восстановить стабильную связь с координатором и защищённой сетью. Для этого выполните:

```
user@host:~$ vipnetclient debug --tcp-tunnel-mode {on | auto | off}
```

Возможные значения:

- `on` — всегда использовать протокол TCP для соединения с защищённой сетью.
- `auto` — соединение с защищённой сетью по протоколу TCP будет устанавливаться автоматически, если не работает соединение по протоколу UDP. Значение по умолчанию.
- `off` — не использовать протокол TCP для соединения с защищённой сетью.

Соединение по протоколу TCP не работает с локальными IP-адресами координаторов:

- 10.0.0.0–10.255.255.255,
- 172.16.0.0–172.31.255.255,
- 192.168.0.0–192.168.255.255.

Регламентный контроль целостности

В рамках эксплуатации ViPNet Client 5 системному администратору или администратору безопасности рекомендуется выполнять следующие регламентные проверки программы:

- Проверка целостности программного обеспечения ViPNet Client 5 и среды функционирования.
- Проверка работоспособности датчиков случайных чисел и криптографических алгоритмов.

Чтобы запустить регламентную проверку из командной строки:

- 1 Если VPN-соединение выключено, включите его:

```
user@host:~$ vipnetclient start
```

- 2 Выполните:

```
user@host:~$ vipnetclient info --regulations [--psw <пароль_администратора_узла>]
```

где `psw` — пароль администратора узла, задаётся в управляющем ПО. Чтобы снизить риск компрометации пароля, применять параметр `--psw` не рекомендуется, так как при этом пароль отображается в консоли в явном виде. Вводите пароль по запросу во время выполнения команды.



Примечание. Если пароль указывается с помощью параметров и содержит спецсимволы, используйте экранирование спецсимволов. Подробнее см. в справочных материалах используемого командного интерпретатора (например, `man bash`).

- 3 Если пароль не был указан в команде, введите пароль администратора узла и нажмите **Enter**.

Результаты регламентных проверок отобразятся в консоли.

Чтобы запустить регламентную проверку в интерфейсе ViPNet Client 5 на вкладке **Безопасность** нажмите **Начать проверку**.

В случае нарушения целостности или при неработоспособности какого-либо из проверяемых компонентов появится информация об этом, и подключение к защищённой сети будет прервано (см. рекомендации раздела [Нарушена целостность компонентов программы ViPNet Client 5 или связанных системных библиотек](#)).

```
user@host:~$ vipnetclient info --regulations
Type VPN administrator password:
Checking the license for integrity ... succeeded
Checking the host links for integrity ... succeeded
Checking the configuration files for integrity ... succeeded
Checking the firewall rules for integrity ... succeeded
Checking the executables for integrity ... succeeded
Checking the environment for integrity ... succeeded
Checking the key system ... succeeded
user@host:~$
```

Рисунок 11. Просмотр результатов регламентного контроля функционирования

Работа с журналом критически важных событий

В ViPNet Client 5 ведётся журнал критически важных событий программы, в который записывается:

- информация о добавлении, смене и удалении ключей (установка и удаление дистрибутива ключей, обновление справочников и ключей, проверка срока действия лицензии);
- информация о неудачных попытках добавления и смены ключей (ошибки установки дистрибутива ключей, ошибки обновления справочников и ключей);
- информация о включении и выключении межсетевого экрана, изменении режима межсетевого экрана, применении и сбросе сетевых фильтров, событиях межсетевого экрана;
- результаты проверки целостности компонентов ViPNet Client 5;
- результаты проверки целостности среды функционирования ViPNet Client 5;
- результаты проверки работоспособности ViPNet Client 5;
- результат аутентификации пользователя и администратора узла;
- информация о проведении регламентных работ (результаты выполнения регламентной проверки, информация о выгрузке и очистке журнала критически важных событий).

Для доступа к журналу критически важных событий требуется пароль администратора узла. Получите этот пароль у администратора сети ViPNet.

Чтобы экспортировать информацию из журнала критически важных событий в файл:

- 1 Если VPN-соединение выключено, включите его:

```
user@host:~$ vipnetclient start
```

- 2 Выполните:

```
user@host:~$ vipnetclient eventlog [--psw <пароль_администратора_сетевого_узла>]  
[--output <каталог_сохранения_файла_журнала>] [--delete  
<каталог_сохранения_файла_журнала>]
```

где:

- `--psw` — параметр для указания пароля администратора узла. Чтобы снизить риск компрометации пароля, применять параметр `--psw` не рекомендуется, так как при этом пароль отображается в консоли в явном виде. Вводите пароль по запросу во время выполнения команды.



Примечание. Если пароль указывается с помощью параметров и содержит спецсимволы, используйте экранирование спецсимволов. Подробнее см. в справочных материалах используемого командного интерпретатора (например, `man bash`).

- `--output` — параметр для указания каталога, в который будет сохранен файл журнала. Если этот параметр не будет указан, файл журнала будет сохранён в каталог, в котором запущена команда.
- `--delete` — параметр для экспорта файла журнала с последующим удалением записей старше 72 часов из журнала.

3 Если пароль не был указан в команде, введите пароль администратора узла и нажмите клавишу **Enter**.

В результате архив `*.zip`, содержащий файл журнала критически важных событий, будет сохранен в указанный каталог или каталог, в котором была запущена команда.

Настройка фильтрации трафика

В ViPNet Client 5 вы можете настроить фильтрацию защищённого трафика одним из способов:

- С помощью локальных сетевых фильтров (режим сетевого экрана LOCAL). В этом случае администратор ViPNet Client 5 задаёт в файле *.xml сетевые фильтры для защищённого трафика и загружает файл в ViPNet Client 5, а сетевые фильтры из ViPNet Policy Manager и ViPNet Prime Policy Management игнорируются.

Этот способ используется, например, если закончилась лицензия ViPNet Policy Manager или в вашей организации администратор узла приоритетнее администратора ViPNet Policy Manager.

- [Персонального межсетевого экрана из программы ViPNet EPP.](#)
- С помощью политик безопасности из программы ViPNet Policy Manager и модуля ViPNet Prime Policy Management (режим сетевого экрана POLICY). В этом случае сетевые фильтры для защищённого трафика создаёт администратор ViPNet Policy Manager или ViPNet Prime Policy Management и передаёт на узлы по сети ViPNet, при этом локальные сетевые фильтры в ViPNet Client 5 игнорируются. Подробнее о настройках политик и совместимости с ViPNet Client 5 см. в руководстве администратора ViPNet Policy Manager или ViPNet Prime Policy Management.

Внимание!

Особенности обработки правил из модуля ViPNet Prime Policy Management:



- Чтобы задать правило с расписанием по дню недели или периоду, задайте время действия 00:00–23:59, чтобы в расписание вошли все полные сутки. Если оставить время действия по умолчанию 00:00–00:00, правило не будет работать.
- Сетевые фильтры с действием «Отклонять и отправлять сообщение» преобразуются в фильтры с действием «Блокировать» в ViPNet Client 5.

Особенности обработки правил из модуля ViPNet Policy Manager:

- Чтобы задать ежедневное правило, задайте время выполнения фильтра 00:00–23:59, чтобы в расписание вошли все полные сутки. Если оставить время действия 00:00–00:00, правило не будет работать.
-

Для открытого трафика вы можете включить правило «Блокировать весь исходящий и входящий открытый трафик». В этом случае на компьютере при включённом VPN-соединении будет разрешён только защищённый IP-трафик с узлами сети ViPNet и туннелируемыми ресурсами, а также открытый трафик, необходимый для работы ОС и ViPNet Client 5 (трафик интерфейсов loopback, TUN, серверов DHCP, NTP).

Блокировка открытого трафика работает только на устройствах с модулями ядра для утилиты iptables.

По умолчанию в ViPNet Client 5 разрешён любой защищённый и открытый трафик. Чтобы настроить фильтрацию трафика:



Примечание. При выполнении перечисленных ниже команд потребуется ввести пароль администратора узла.

1 Выберите режим работы сетевого экрана ViPNet Client 5:

- Режим POLICY:

```
user@host:~$ vipnetclient {firewall | fw} protected --policy
```

- Режим LOCAL:

```
user@host:~$ vipnetclient {firewall | fw} protected --no-policy
```

2 Загрузите в ViPNet Client 5 локальные сетевые фильтры для защищённого трафика:

2.1 Создайте файл *.xml с сетевыми фильтрами.

2.2 Загрузите файл в ViPNet Client 5:

```
user@host:~$ vipnetclient {firewall | fw} protected --user-xml <путь к файлу>
```

Эти сетевые фильтры будут применяться при переключении сетевого экрана в режим LOCAL.

3 Чтобы блокировать весь открытый трафик:

```
user@host:~$ vipnetclient {firewall | fw} public --block
```

Чтобы отменить блокировку открытого трафика:

```
user@host:~$ vipnetclient {firewall | fw} public --no-block
```

4 Чтобы экспортировать действующие локальные сетевые фильтры в файл *.xml:

```
user@host:~$ vipnetclient {firewall | fw} protected --save-user-xml <путь для  
сохранения файла>
```

5 Чтобы удалить все действующие локальные сетевые фильтры:

```
user@host:~$ vipnetclient {firewall | fw} protected --erase-user-xml
```

Также вы можете просмотреть список действующих сетевых фильтров (пароль администратора узла не требуется). Для этого при включённом VPN-соединении выполните:

```
user@host:~$ vipnetclient iplirdiag -s firewall --static
```

Чтобы просмотреть информацию о сетевом экране ViPNet Client 5 (пароль администратора узла не требуется):

```
user@host:~$ vipnetclient {firewall | fw} info
```

Особенности работы с ViPNet EPP

Информацию о настройках и совместимости с ViPNet Client 5 см. в документации ViPNet EPP.

Режим работы [персонального межсетевого экрана](#) устанавливается через ViPNet EPP Агент Linux или централизованно с ViPNet EPP Сервер при назначении на группу защищаемых узлов [базы правил](#). См. руководство администратора ViPNet EPP, пункт «Просмотр и выбор режима работы».

Чтобы посмотреть текущий режим работы персонального межсетевого экрана ViPNet EPP Агент Linux, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора, аудитора или пользователя агента> pfw get-mode
```

Список режимов персонального межсетевого экрана ViPNet EPP Агент Linux:

- **private** — частная сеть. По умолчанию пропускаются все исходящие соединения и блокируются все входящие соединения. В этом режиме недоступны защищённые ресурсы сети ViPNet. Чтобы защищённые ресурсы были доступны, добавьте разрешающее правило:
 - Централизованно через политику ViPNet EPP Сервер.
См. руководство администратора ViPNet EPP, раздел «Настройка фильтров политик безопасности».
 - Локально через пользовательский фильтр ViPNet EPP Агент Linux. Пример команды:

```
/opt/epp-agent/bin/epp_mc_cli --login=admin --password=admin pfw rules add --name=<название фильтра> --action=accept --mode=private
```


См. руководство администратора ViPNet EPP, раздел «Настройка пользовательских фильтров».
- **public** — публичная сеть. По умолчанию блокируются все входящие и исходящие соединения. В этом режиме недоступны защищённые ресурсы сети ViPNet. Чтобы защищённые ресурсы были доступны, добавьте разрешающее правило централизованно через политику ViPNet EPP Сервер.
См. руководство администратора ViPNet EPP, раздел «Настройка фильтров политик безопасности».
- **protected** — защищённая сеть. По умолчанию пропускаются все исходящие и входящие соединения, кроме соединений, запрещённых пользовательскими фильтрами.
- **block** — полная блокировка трафика. По умолчанию блокируются все входящие и исходящие соединения. В этом режиме недоступны защищённые ресурсы сети ViPNet, узел полностью отключён от сети. Сделать защищённые ресурсы доступными невозможно.
- **off** — отключён. Персональный межсетевой экран отключён и не влияет на сетевой трафик.

Внимание! Запрещающие правила имеют приоритет:



- Правило ViPNet Client 5 для блокировки трафика будет работать, даже если в ViPNet EPP Агент Linux весь трафик разрешён.
- Правило ViPNet EPP Агент Linux для блокировки трафика будет работать, даже если в ViPNet Client 5 весь трафик разрешён.

В режимах `private` и `protected` при обнаружении подозрительной сетевой активности приложений вы можете заблокировать исходящий трафик этих приложений через ViPNet EPP Агент Linux. При блокировке защищённые ресурсы сети ViPNet становятся недоступными. Разблокировать защищённые ресурсы можно только через ViPNet EPP Агент Linux.

Подробнее см. руководство администратора ViPNet EPP, глава «Настройка ViPNet EPP Агент Linux», пункт «Просмотр активных соединений».

3

Отладка ViPNet Client 5

Команды отладки	80
Просмотр информации о работе VPN-драйвера	82

Команды отладки



Внимание! Данный раздел предназначен для разработчиков.

Чтобы посмотреть список доступных опций для отладки работы ViPNet Client 5 выполните:

```
user@host:~$ vipnetclient debug --help
```

Вы можете воспользоваться следующими опциями команды `vipnetclient debug`:

- `--get-client-param <название параметра>` — просмотр внутренних параметров. Подробнее см. справочник разработчика.
- `--nvs-debug` — задать интервал отправки событий в систему мониторинга ViPNet NVS длительностью 60 секунд в целях отладки.
- `--no-nvs-debug` — выключить настройку `--nvs-debug` и использовать интервал, полученный из системы мониторинга ViPNet NVS. В ViPNet NVS можно настроить интервал 5 минут и более. Если задать интервал менее 5 минут, будет использоваться 5 минут.

Подробную информацию о настройках и совместимости с ViPNet Client 5 см. в документации ViPNet NVS.

- `--benchmark <размер буфера в байтах>` — проверка производительности криптодрайвера ViPNet Client 5 при заданном размере тестового буфера информации.
- `--reload` — перезагрузка службы ViPNet Client 5.
- `--mdns` — включить поиск узлов ViPNet в локальной сети по протоколам MulticastDNS и DNS Service Discovery для последующего взаимодействия с ними напрямую (без участия координатора) по протоколу IPv6. При этом используется режим шифрования, заданный в управляющем ПО. Функция работает только при включённом VPN-соединении. По умолчанию поиск узлов ViPNet выключен.

При включении опции в вывод команды `vipnetclient info` добавляется строка статуса модуля `mdns`, которая может принимать одно из значений:

- Multicast DNS Announcing and Discovering — модуль `mdns` включён, сервис анонсируется, поиск узлов ViPNet работает.
- Multicast DNS Off — опция `mdns` включена, но модуль `mdns` выключен или не работает.
- Multicast DNS Announcing — работает только анонсирование сервиса, поиск узлов ViPNet не работает (по причине сбоя).
- Multicast DNS Discovering — работает только поиск узлов ViPNet, анонсирование сервиса не работает (по причине сбоя).
- Multicast DNS (Re-)registering and Discovering — выполняется перерегистрация сервиса, поиск узлов ViPNet работает.

- o Multicast DNS (Re-)registering — выполняется перерегистрация сервиса, поиск узлов ViPNet не работает (по причине сбоя).
- o Multicast DNS Switching off — выполняется выключение модуля mdns.

Если включена блокировка IP-трафика открытой сети, IP-пакеты mdns будут заблокированы.

- `--no-mdns` — выключить поиск узлов ViPNet в локальной сети.
- `--mdns-debug` — включить запись событий модуля mdns в системный журнал. Если опция включена, то строка статуса модуля mdns в выводе команды `vipnetclient info` будет дополнена сообщением `with debug`.
- `--no-mdns-debug` — выключить запись событий модуля mdns в системный журнал.
- `--mdns-cache` — просмотр кэша модуля mdns.

Просмотр информации о работе VPN-драйвера



Внимание! В этом разделе представлены функции для разработчиков.

Чтобы посмотреть список доступных опций для отладки работы ViPNet Client 5 выполните:

```
user@host:~$ vipnetclient vpndiag --help
```

- Информация для диагностики работы адаптеров:

```
user@host:~$ vipnetclient vpndiag -s adapters --info | --stats | --routes
```

- `--info` — информация об адаптерах.

```
user@host:~$ vipnetclient vpndiag -s adapters --info
Calling the "vpndiag" with the following parameters: -s adapters --info ... Success

Information about adapters

  adapterName: tun
  firstIpAddress: 7.0.23.56
  logOverflow: 0
```

Рисунок 12. Информация об адаптерах

- `--stats` — статистика подсистемы adapters.

```

user@host:~$ vipnetclient vpndiag -s adapters --stats
Calling the "vpndiag" with the following parameters: -s adapters --stats ... Success

Subsystem statistics

blockOtherProtocols: 0
decreaseMSSValue: 0
filterDisableDriver: 0
filterInitDrop: 0
filterProtectedNetEnable: 0
ioThreadsCount: 2
maxHeadAddInfoSize: 0
maxIpPacketDataSize: 65535
maxTailAddInfoSize: 0
numAdapterContext: 1
timeDifferenceInSecond: 7200
traffic:
  dns:
    inBytes: 6510
    inPackets: 32
    outBytes: 1446
    outPackets: 32
  port2046:
    inBytes: 1847
    inPackets: 10

```

Рисунок 13. Статистика подсистемы adapters

- o `--routes` — таблица маршрутизации.

```

user@host:~$ vipnetclient vpndiag -s adapters --routes
Calling the "vpndiag" with the following parameters: -s adapters --routes ... Success

Routes map

Subnet/Mask          Gateway             Interface
default             10.70.0.1           ens33
7.0.0.0/16           7.0.23.56           tun0
10.70.0.0/16         0.0.0.0             ens33
11.0.0.0/8           7.0.23.56           tun0
172.16.0.10/32       7.0.23.56           tun0
172.16.0.20/32       7.0.23.56           tun0
172.16.0.30/31       7.0.23.56           tun0
172.16.0.32/29       7.0.23.56           tun0
172.16.0.40/32       7.0.23.56           tun0
::a472:2a3:e1d9:51fd/64 0.0.0.0             tun0
::80fe/64            0.0.0.0             ens33
::80fe/64            0.0.0.0             tun0

```

Рисунок 14. Таблица маршрутизации

- Информация о криптографии:

```

user@host:~$ vipnetclient vpndiag -s cipher --info

```

```

user@host:~$ vipnetclient vpndiag -s cipher --info
Calling the "vpndiag" with the following parameters: -s cipher --info ... Success

Cryptography information

supportedCipherSuites:
  0
  2
  4
  5
 257
 258
 259
 260
 385
 388
 390

```

Рисунок 15. Информация о криптографии

- Информация для диагностики работы DNS:

```

user@host:~$ vipnetclient vpndiag -s dnsproxy --info | --query-logging arg {on | off }

```

- o --info — информация о работе DNS.

```

user@host:~$ vipnetclient vpndiag -s dnsproxy --info
Calling the "vpndiag" with the following parameters: -s dnsproxy --info ... Success

DNS proxy information

dnsProxyIp: 11.254.254.254
enabled: true
ipv4Socket: 45
ipv6Resolving: false
ipv6Socket: 0
nativeIp: 7.0.23.56
openResolveHostList:
  <empty>
privateDomains:
  <empty>
resolveInternetWithPrivateDns: true
servers:
  dhcp:
    <empty>
  disabled:
    <empty>
  private:
    <empty>
  trusted:
    77.88.8.2
    77.88.8.88
  user:
    <empty>

```

Рисунок 16. Информация о работе DNS

- o `--query-logging arg {on | off }` — включение или выключение журналирования DNS-запросов. По умолчанию выключено.

```
user@host:~$ vipnetclient vpndiag -s dnsproxy --query-logging on
Calling the "vpndiag" with the following parameters: -s dnsproxy --query-logging on ... Success
```

Рисунок 17. Журналирования DNS-запросов

- Информация о межсетевом экране:

```
user@host:~$ vipnetclient vpndiag -s firewall --static --stats | --static | --ip | --tcp
| --udp | --udp-bcast | --icmp | --icmp-bcast | --icmp-tcp | --icmp-udp | --icmp-icmp
| --wait-rule | --nat-al-bindings | --bcast-id | --params | --counters | --used-ports
| --drv-alg-trace arg | --dnsnamedump | --store | --unknownips
```

- o `--stats` — статистика подсистемы firewall,

```
user@host:~$ vipnetclient vpndiag -s firewall --stats
Calling the "vpndiag" with the following parameters: -s firewall --stats ... Success

Subsystem statistics

counters:
  Connection table size: 1 (max = 150000)
  DNS connection count: 0
  FTP connection count: 0
  H323 TCP connection count: 0
  H323 UDP connection count: 0
  ICMP connections count: 0
  Other TCP connection count: 0
  Other UDP connection count: 0
  Protected connections count: 1
  Public connections count: 0
  SCCP connection count: 0
  SIP TCP connection count: 0
  SIP UDP connection count: 0
  TCP connections count: 0
  TCP public connections count: 0
  Total alg connections count: 0
  Total connections count: 1
  Transit connections count: 0
  Tunnel connections count: 0
  UDP connections count: 1
  VPN connections count: 1
icmp:
  <empty>
icmp-bcast:
  <empty>
icmp-icmp:
  <empty>
```

Рисунок 18. Статистика подсистемы firewall

- o `--static` — список загруженных правил для фильтрации защищённого трафика,

```
user@host:~$ vipnetclient vpndiag -s firewall --static
Calling the "vpndiag" with the following parameters: -s firewall --static ... Success

Protected network rules:
0: StaticRule
  action= DROP
  condition=
    AND(
      Direction(OUT),
      DestinationNodeRole(CLIENT),
    )
1: StaticRule
  action= PASS
  condition= TRUE
```

Рисунок 19. Правила для фильтрации защищённого трафика

- o `--ip` — список правил для протокола IP,

```
user@host:~$ vipnetclient vpndiag -s firewall --ip
Calling the "vpndiag" with the following parameters: -s firewall --ip ... Success
ip:
  <empty>
```

Рисунок 20. Правила для протокола IP

- o `--tcp` — список правил для протокола TCP,

```
user@host:~$ vipnetclient vpndiag -s firewall --tcp
Calling the "vpndiag" with the following parameters: -s firewall --tcp ... Success
tcp:
  <empty>
```

Рисунок 21. Правила для протокола TCP

- o `--udp` — список правил для протокола UDP,

```
user@host:~$ vipnetclient vpndiag -s firewall --udp
Calling the "vpndiag" with the following parameters: -s firewall --udp ... Success
udp:
  IN 7.0.23.50:2046 -> 7.0.23.56:2046
  OUT 7.0.23.56:2046 -> 7.0.23.50:2046
```

Рисунок 22. Правила для протокола UDP

- o `--udp-bcast` — список правил для широковещательных запросов протокола UDP,

```
user@host:~$ vipnetclient vpndiag -s firewall --udp-bcast
Calling the "vpndiag" with the following parameters: -s firewall --udp-bcast ... Success
udp-bcast:
  <empty>
```

Рисунок 23. Правила для широковещательных запросов протокола UDP

- o `--icmp` — список правил для протокола ICMP,

```
user@host:~$ vipnetclient vpndiag -s firewall --icmp
Calling the "vpndiag" with the following parameters: -s firewall --icmp ... Success
icmp:
<empty>
```

Рисунок 24. Правила для протокола ICMP

- o `--icmp-bcast` — список правил для широковещательных запросов протокола ICMP,

```
user@host:~$ vipnetclient vpndiag -s firewall --icmp-bcast
Calling the "vpndiag" with the following parameters: -s firewall --icmp-bcast ... Success
icmp-bcast:
<empty>
```

Рисунок 25. Правила для широковещательных запросов протокола ICMP

- o `--icmp-tcp` — список правил для протокола ICMP (TCP),

```
user@host:~$ vipnetclient vpndiag -s firewall --icmp-tcp
Calling the "vpndiag" with the following parameters: -s firewall --icmp-tcp ... Success
icmp-tcp:
<empty>
```

Рисунок 26. Правила для протокола ICMP (TCP)

- o `--icmp-udp` — список правил для протокола ICMP (UDP),

```
user@host:~$ vipnetclient vpndiag -s firewall --icmp-udp
Calling the "vpndiag" with the following parameters: -s firewall --icmp-udp ... Success
icmp-udp:
  OUT 7.0.23.50 7.0.23.50:2046 -> 7.0.23.56:2046
  IN 7.0.23.56 7.0.23.56:2046 -> 7.0.23.50:2046
```

Рисунок 27. Правила для протокола ICMP (UDP)

- o `--icmp-icmp` — список правил для протокола ICMP (ICMP),

```
user@host:~$ vipnetclient vpndiag -s firewall --icmp-icmp
Calling the "vpndiag" with the following parameters: -s firewall --icmp-icmp ... Success
icmp-icmp:
<empty>
```

Рисунок 28. Правила для протокола ICMP (ICMP)

- o `--wait-rule` — список правил в ожидании,

```
user@host:~$ vipnetclient vpndiag -s firewall --wait-rule
Calling the "vpndiag" with the following parameters: -s firewall --wait-rule ... Success
wait-rule:
<empty>
```

Рисунок 29. Правила в ожидании

- o `--natal-bindings` — настройки прикладных протоколов (ALG),

```
user@host:~$ vipnetclient vpndiag -s firewall --natal-bindings
Calling the "vpndiag" with the following parameters: -s firewall --natal-bindings ... Success

Natal bindings:
TCP 0.0.0.0:0-0 -- 0.0.0.0:21-21 (21) 0 2025-04-14T10:06:03
TCP 0.0.0.0:0-0 -- 0.0.0.0:1720-1720 (1720) 0 2025-04-14T10:06:03
TCP 0.0.0.0:0-0 -- 0.0.0.0:2000-2000 (2000) 0 2025-04-14T10:06:03
TCP 0.0.0.0:0-0 -- 0.0.0.0:5060-5060 (5060) 0 2025-04-14T10:06:03
TCP 0.0.0.0:0-0 -- 0.0.0.0:5068-5068 (5060) 0 2025-04-14T10:06:03
TCP 0.0.0.0:0-0 -- 0.0.0.0:5080-5080 (5060) 0 2025-04-14T10:06:03
UDP 0.0.0.0:0-0 -- 0.0.0.0:53-53 (53) 0 2025-04-14T10:06:03
UDP 0.0.0.0:0-0 -- 0.0.0.0:1719-1719 (1720) 0 2025-04-14T10:06:03
UDP 0.0.0.0:0-0 -- 0.0.0.0:5060-5060 (5060) 0 2025-04-14T10:06:03
UDP 0.0.0.0:0-0 -- 0.0.0.0:5068-5068 (5060) 0 2025-04-14T10:06:03
UDP 0.0.0.0:0-0 -- 0.0.0.0:5080-5080 (5060) 0 2025-04-14T10:06:03
```

Рисунок 30. Настройки прикладных протоколов

- o `--bcast-id` — идентификаторы широковещательных запросов,

```
user@host:~$ vipnetclient vpndiag -s firewall --bcast-id
Calling the "vpndiag" with the following parameters: -s firewall --bcast-id ... Success
null
```

Рисунок 31. Идентификаторы широковещательных запросов

- o `--params` — параметры подсистемы firewall,

```
user@host:~$ vipnetclient vpndiag -s firewall --params
Calling the "vpndiag" with the following parameters: -s firewall --params ... Success
params:
Cleanup interval: 20
Connection ttl IP: 30
Connection ttl TCP: 30
Connection ttl UDP: 30
Default connection timeout: 30
Dynamic ports:
  dynamicport_max: 65535
  dynamicport_min: 1024
Dynamic timeouts: 0
ICMP timeout: 10
License:
  license_ip_timeout: 900
  license_max_ips: -1
Listen timeout: 30
Max connections: 150000
Max dynamic rules: 20000000
Static rule soft erase: 1
TCP SYN timeout: 10
```

Рисунок 32. Параметры подсистемы firewall

- o `--counters` — счётчик соединений межсетевого экрана,

```
user@host:~$ vipnetclient vpndiag -s firewall --counters
Calling the "vpndiag" with the following parameters: -s firewall --counters ... Success
counters:
  Connection table size: 1 (max = 150000)
  DNS connection count: 0
  FTP connection count: 0
  H323 TCP connection count: 0
  H323 UDP connection count: 0
  ICMP connections count: 0
  Other TCP connection count: 0
  Other UDP connection count: 0
  Protected connections count: 1
  Public connections count: 0
  SCCP connection count: 0
  SIP TCP connection count: 0
  SIP UDP connection count: 0
  TCP connections count: 0
  TCP public connections count: 0
  Total alg connections count: 0
  Total connections count: 1
  Transit connections count: 0
  Tunnel connections count: 0
  UDP connections count: 1
  VPN connections count: 1
```

Рисунок 33. Соединения межсетевого экрана

- o `--used-ports` — список используемых портов,

```
user@host:~$ vipnetclient vpndiag -s firewall --used-ports
Calling the "vpndiag" with the following parameters: -s firewall --used-ports ... Success
used-ports:
  Free TCP ports: 65535
  Free UDP ports: 65535
  Used TCP ports: 0
  Used UDP ports: 0
```

Рисунок 34. Используемые порты

- Информация о настройке **Группа серверов**:

```
user@host:~$ vipnetclient vpndiag -s groupserver --info
```

```
user@host:~$ vipnetclient vpndiag -s groupserver --info
Calling the "vpndiag" with the following parameters: -s groupserver --info ... Success

Connection Server Group

Servers:
  Id: 15FD000A P: 1 Time: 129 ms
  Id: 15FD002E P: 100 Time: 0
  Id: 15FD09FD P: 100 Time: 0
  Id: 15FD28F0 P: 100 Time: 0
  Id: 15FD2A99 P: 100 Time: 0
  Id: 15FD2A9B P: 100 Time: 0
  Id: 15FD2A9C P: 100 Time: 0
  Id: 15FD2AA4 P: 100 Time: 0
  Id: 15FD2C1A P: 100 Time: 0
Starts:
  Time: 10:41:36 Type: E1
  Time: 10:41:50 Type: G1
IsDgNode: No
active: 15FD000A
chosen: 15FD000A
dgIps: null
eventLife: 5 sec
latecomer:
  Id: 15FD000A
nextSwitching: <empty>
status: Finish
switching: 120 min
time: 130 ms
waiting: 600 ms
```

Рисунок 35. Информация о настройке **Группа серверов**

Информация о настройке **Группа серверов** в формате JSON:

```
user@host:~$ vipnetclient vpndiag -s groupserver --info --json
```

```
user@host:~$ vipnetclient vpndiag -s groupserver --info --json
{
  "groupserver": {
    "info": {
      "IsDgNode": "No",
      "active": "15FD000A",
      "chosen": "15FD000A",
      "dgIps": null,
      "eventLife": "5 sec",
      "latecomer": {
        "Id": "15FD000A"
      },
      "nextSwitching": "<empty>",
      "servers": [
        {
          "Id": "15FD000A",
          "priority": 1,
          "time": "129 ms"
        },
        {
          "Id": "15FD002E",
          "priority": 100,
          "time": "0"
        },
        {
          "Id": "15FD09FD",
          "priority": 100,
          "time": "0"
        },
        {
          "Id": "15FD28F0",
          "priority": 100,
          "time": "0"
        }
      ]
    }
  }
}
```

Рисунок 36: Информация о настройке **Группа серверов** в формате JSON

Результат выполнения команды:

- o Servers — информация о **координаторах, которые клиент может использовать в качестве сервера соединений**:
 - Id — идентификатор,
 - P — приоритет,

Примечание. Приоритет определяет порядок выбора другого сервера соединений для клиента, когда активный координатор недоступен. Чем меньше значение P, тем выше приоритет координатора.



Приоритет активного координатора по умолчанию равен одному. Приоритет других координаторов из группы серверов зависит от формата ключей клиента:

- в клиентах с ключами *.dst — приоритет равен 100;
 - с ключами *.ds5 — двум.
-

- `Time` — время отклика (0 — координатор недоступен).
- `Starts` — десять последних записей о запуске настройки **Группа серверов**:
 - `Time` — время запуска,
 - `Type` — причина запуска.

Таблица 6. Описание причин запуска настройки

Причина	Описание
A1	Периодическая отправка сервисного сообщения «Hello/Wassup» на активный координатор
A2	Изменение сетевых интерфейсов или перевод времени
B1	Переключение на сервер соединений с более высоким приоритетом
C1	Проверка соединения с активным координатором
D1	Событие от подсистемы доступности сетевого узла при появлении пользовательского трафика на координаторе
E1	Запуск межузловой рассылки при запуске VPN-соединения
G1	Запуск пользователем настройки Группа серверов

- `IsDgNode` — использование в качестве сервера соединений координатора с адресом шлюза по умолчанию. Значение по умолчанию — `No`.
- `dgIps` — IP-адрес шлюза по умолчанию. Значение по умолчанию — `Null`.
- `active` — идентификатор активного координатора по умолчанию, заданного в управляющем ПО или вручную в ViPNet Client 5.
- `chosen` — идентификатор текущего активного координатора из группы серверов.
- `eventLife` — время ожидания ответа от координатора, после которого координатор считается недоступным, и запускается настройка **Группа серверов**.
- `latecomer` — идентификатор координатора, который первый ответил после запуска настройки **Группа серверов**.
- `nextSwitching` — время переключения клиента к координатору с более высоким приоритетом.
- `status` — статус настройки **Группа серверов**:
 - `Run` — настройка запущена, выполняется поиск доступного координатора из группы серверов;
 - `Finish` — поиск координатора завершён.

Если в группе серверов есть доступный координатор, клиент подключится к нему.

Если доступного координатора нет, у клиента не будет связи с корпоративными ресурсами. Настройте подключение к узлам напрямую, см. разделы [«Подключение к узлам напрямую»](#) и [«Команды отладки»](#).

- o `switching` — продолжительность перепоключения клиента к координатору с более высоким приоритетом. По умолчанию 120 минут.
- o `time` — время выполнения настройки **Группа серверов**.
- o `waiting` — время между запросами на координаторы с разным приоритетом. По умолчанию 600 миллисекунд.

Запросы отправляются на координаторы в порядке уменьшения их приоритета. В результате координаторы с более высоким приоритетом получают больше времени на обработку запроса и ответ.

- Информация о сетевых настройках:

```
user@host:~$ vipnetclient vpndiag -s ipsettings --stats | --v-table | --v-tun-table | --node-info arg
```

- o `--stats` — статистика подсистемы `ipsettings`.

```
user@host:~$ vipnetclient vpndiag -s ipsettings --stats
Calling the "vpndiag" with the following parameters: -s ipsettings --stats ... Success

Subsystem statistics

  coordinatorMode: 0
  limitNativeTunnelingIp: 0
  nativeId: 15FD2584
  numNodesRow: 20
  numUsedTunnelingIp: 0
  numVisibilityIp: 50
  numVisibilityTunnelingIp: 41
```

Рисунок 37. Статистика подсистемы `ipsettings`

- o `--v-table` — список всех связей в формате <идентификатор туннелируемого узла> — <IP-адрес>.

```
user@host:~$ vipnetclient vpndiag -s ipsettings --v-table
Calling the "vpndiag" with the following parameters: -s ipsettings --v-table ... Success

Nodes addresses

  22E11732: 7.0.23.50
  22E11738: 7.0.23.56
  22E11732: 11.1.0.1
  22E11732: fd51:d9e1:a302:72a4::22e1:1732
  22E11738: fd51:d9e1:a302:72a4::22e1:1738
```

Рисунок 38. Список связей

- o `--v-tun-table` — список всех туннелируемых адресов в формате <идентификатор координатора, туннелирующего IP-адрес> — <IP-адрес туннелируемого ресурса>.

```
user@host:~$ vipnetclient vpndiag -s ipsettings --v-tun-table
Calling the "vpndiag" with the following parameters: -s ipsettings --v-tun-table ... Success

Virtual tunnels addresses

22E11732: 172.16.0.10 - 172.16.0.10
22E11732: 172.16.0.20 - 172.16.0.20
22E11732: 172.16.0.30 - 172.16.0.40
```

Рисунок 39. Список туннелируемых адресов

- o `--node-info` <идентификатор узла> — подробная информация об узле (идентификатор и имя узла, его IP-адрес видимости и другая информация). Для координаторов отображаются также туннелируемые ими IP-адреса открытых узлов.

```
user@host:~$ vipnetclient vpndiag -s ipsettings --node-info 22E11732
Calling the "vpndiag" with the following parameters: -s ipsettings
--node-info 22E11732 ... Success

Node IP settings

accessPoint:
  Encapsulation: Udp
  Type: Direct
  ip: 81.30.192.133
  node: 22E11732
  port: 58867
accessPoints:
  default:
    Id: 22E11732
    Ip: 81.30.192.133
    Port: 58867
  endpoints:
    81.30.192.133:58867
    10.10.88.67:58867
    10.2.0.67:58867
  firewall:
    Id: 22E11732
    Ip: 81.30.192.133
    Port: 58867
  multicast:
    <empty>
  proxy:
    Id: FFFFFFFE
baseVirtualIp: 11.0.0.1
cipher: 0
ips:
```

Рисунок 40. Просмотр подробной информации об узле

- Информация о состоянии модуля политик пользовательского трафика:

```
user@host:~$ vipnetclient vpndiag -s tpm --info
```

Если пользовательский трафик заблокирован, отображается [причина блокировки](#) и список узлов [из параметра restrictedTrafficModeExclusions](#), для которых пользовательский трафик разрешён.

```
user@host:~$ vipnetclient vpndiag -s tpm --info
Calling the "vpndiag" with the following parameters: -s tpm --info ... Success

Traffic Policy Module information

exclusions:
  15FD000A
  15FD00D6
  15FD00D9
reasons:
  sdk
restricted: true
```

Рисунок 41. Информация о состоянии модуля политик пользовательского трафика

- Информация об [обновлении из управляющего ПО](#) клиентов с ключами *.ds5:

```
vipnetclient vpndiag -s updates --info
```

Отображается информация об архиве с обновлением и установлено ли обновление. Если обновление не установлено, отображается причина.

```
user@host:~$ vipnetclient vpndiag -s updates --info
Calling the "vpndiag" with the following parameters: -s updates --info ... Success

Updates manager information

error:
filename: client-linux-gui_x86_64_update_5.1.3-7182_deb.zip
id: 1
info:
  arch: x86_64
  brand: vipnet
  edition:
    deb
    generic
    gui
    hybrid
  name: client-linux-gui_x86_64_update_5.1.3-7182_deb.zip
  platform: linux
  product: vpn-client
  retry_timeout: 300
  url: http://10.10.88.16:9090/bombova/client-linux-gui_x86_64_update_5.1.3-7182_deb.zip
  version: 5.1.3-7182
status: installed
```

Рисунок 42. Информация об обновлении



Создание файла с сетевыми фильтрами

- 1 Создайте файл *.xml.
- 2 Добавьте в файл следующее содержимое:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>  
  
<vn:Policy xmlns:vn="http://www.infotecs.ru/2007/ViPNet"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="http://www.infotecs.ru/2007/ViPNet rules.xsd">
```

```
  <NamedObjects>  
    <ServiceObject>  
      <Name>Protocol 1</Name>  
      <Id>1</Id>  
      <CreationType>Policy</CreationType>  
      <Inclusion xsi:type="vn:TcpCondition">  
        <DestinationPort xsi:type="vn:PortRange">  
          <Begin>  
            <Value>1</Value>  
          </Begin>  
          <End>  
            <Value>443</Value>  
          </End>  
        </DestinationPort>  
        <Protocol>6</Protocol>
```

```

</Inclusion>
<Exclusion xsi:type="vn:TcpCondition">
  <Protocol>6</Protocol>
</Exclusion>
<Exclusion xsi:type="vn:TcpCondition">
  <DestinationPort xsi:type="vn:Port">
    <Value>21</Value>
  </DestinationPort>
  <Protocol>6</Protocol>
</Exclusion>
</ServiceObject>

<VpnObject>
  <Name>ViPNet Nodes 1</Name>
  <Id>3</Id>
  <CreationType>Policy</CreationType>
  <Exclusion xsi:type="vn:VpnNameTemplate">
    <Template>ARM-ADMIN-VPN1722-*</Template>
  </Exclusion>
  <Inclusion xsi:type="vn:VpnSystemObjectRef">
    <Name>AllClients</Name>
  </Inclusion>
</VpnObject>
</NamedObjects>

<Rules>
  <Rule IsActive="true" xsi:type="vn:VpnRule">
    <RuleId>200001</RuleId>
    <OrderId>2</OrderId>
    <Name>Filter 1</Name>
    <CreationType>Policy</CreationType>
    <ConditionSet>
      <Source xsi:type="vn:PrivateNetwork">
        <VpnHostCondition xsi:type="vn:VpnObjectRef">
          <Id>3</Id>
        </VpnHostCondition>
      </Source>
      <ServiceCondition xsi:type="vn:ServiceObjectRef">
        <Id>1</Id>
      </ServiceCondition>
    </ConditionSet>
  </Rule>
</Rules>

```

```

</ServiceCondition>
<Destination xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnSystemObjectRef">
    <Name>LocalHost</Name>
  </VpnHostCondition>
</Destination>
</ConditionSet>
<Action IsBidirectional="false"
  IsConnectionLoggingEnabled="true"
  IsConnectionStateless="false"
  IsPacketLoggingEnabled="true"
  xsi:type="vn:Filter">
  <FilteringAction>Drop</FilteringAction>
</Action>
<Section>VpnSection</Section>
</Rule>
<Rule IsActive="true" xsi:type="vn:VpnRule">
  <RuleId>200002</RuleId>
  <OrderId>1</OrderId>
  <Name>Filter 2</Name>
  <CreationType>Policy</CreationType>
  <ConditionSet>
    <ScheduleCondition xsi:type="vn:Calendar">
      <StartTime>00:00:00</StartTime>
      <EndTime>23:59:00</EndTime>
      <StartDate>2023-03-13</StartDate>
      <EndDate>2024-03-13</EndDate>
    </ScheduleCondition>
    <Source xsi:type="vn:PrivateNetwork">
      <VpnHostCondition xsi:type="vn:VpnSystemObjectRef">
        <Name>OtherHost</Name>
      </VpnHostCondition>
    </Source>
    <ServiceCondition xsi:type="vn:UdpCondition">
      <DestinationPort xsi:type="vn:PortRange">
        <Begin>
          <Value>25000</Value>
        </Begin>
        <End>
          <Value>30000</Value>
        </End>
      </DestinationPort>
    </ServiceCondition>
  </ConditionSet>
</Rule>

```

```

        </End>
    </DestinationPort>
    <Protocol>17</Protocol>
</ServiceCondition>
<Destination xsi:type="vn:PrivateNetwork">
    <VpnHostCondition xsi:type="vn:VpnSystemObjectRef">
        <Name>LocalHost</Name>
    </VpnHostCondition>
</Destination>
</ConditionSet>
<Action IsBidirectional="false"
        IsConnectionLoggingEnabled="true"
        IsConnectionStateless="false"
        IsPacketLoggingEnabled="true"
        xsi:type="vn:Filter">
    <FilteringAction>Pass</FilteringAction>
</Action>
<Section>VpnSection</Section>
</Rule>
<Rule IsActive="true" xsi:type="vn:VpnRule">
    <RuleId>200003</RuleId>
    <OrderId>3</OrderId>
    <Name>Filter 1</Name>
    <CreationType>Policy</CreationType>
    <ConditionSet>
        <Destination xsi:type="vn:PrivateNetwork">
            <VpnHostCondition xsi:type="vn:VpnSystemObjectRef">
                <Name>OtherHost</Name>
            </VpnHostCondition>
        </Destination>
    </ConditionSet>
    <Action IsBidirectional="false"
            IsConnectionLoggingEnabled="true"
            IsConnectionStateless="false"
            IsPacketLoggingEnabled="true"
            xsi:type="vn:Filter">
        <FilteringAction>Drop</FilteringAction>
    </Action>
    <Section>VpnSection</Section>
</Rule>

```

```
</Rules>
```

```
<Properties>
```

```
<Version>1.0</Version>
```

```
<IssueDateTime>2023-03-13T09:08:30</IssueDateTime>
```

```
<RollbackPeriod>3000</RollbackPeriod>
```

```
</Properties>
```

```
</vn:Policy>
```



Внимание! Не меняйте последовательность секций в файле, иначе сетевые фильтры не будут работать.

Не создавайте в файле *.xml блоки, которые включают одновременно все источники, назначения, номера портов и протоколов. Такие блоки дублируют правила по умолчанию, поэтому сетевые фильтры не применяются.

- 3 В секции `<NamedObjects>` при необходимости задайте группы объектов для сетевых фильтров (см. [Группы объектов](#)).
- 4 В секции `<Rules>` перечислите сетевые фильтры. Если вы хотите создать несколько сетевых фильтров, скопируйте структуру `<Rule>` нужное количество раз.
- 5 Для каждого сетевого фильтра в структуре `<Rule>` укажите значения следующих параметров:
 - o `isActive` — включён сетевой фильтр (`true`) или нет (`false`).
 - o `RuleId` — идентификатор сетевого фильтра (число 200001 и выше).
 - o `OrderId` — порядковый номер, определяющий приоритет применения сетевого фильтра.
 - o `Name` — имя сетевого фильтра (текст не более 255 символов).
- 6 Для каждого сетевого фильтра задайте сетевые условия в структуре `<ConditionSet>`:
 - o В структурах `<Source>` и `<Destination>` укажите отправителя и получателя IP-пакетов (см. [Источник и назначение](#)), к которым будет применяться сетевой фильтр.
 - o При необходимости добавьте структуру `<ServiceCondition>` и укажите в ней протокол и порты (см. [Протокол](#)), к которым будет применяться сетевой фильтр.
 - o При необходимости добавьте структуру `<ScheduleCondition>` и укажите в ней расписание (см. [Расписание](#)), по которому будет применяться сетевой фильтр.



Внимание! Сетевые фильтры будут применяться по расписанию в соответствии с локальным временем на устройстве.

7 Для каждого сетевого фильтра в структуре `<Action>`:

- В параметре `IsBidirectional` укажите одно из значений:
 - `true` — применять сетевой фильтр к трафику в двух направлениях. В этом случае в ViPNet Client 5 будет загружен текущий сетевой фильтр и еще один сетевой фильтр, созданный на его основе. В дополнительном сетевом фильтре источник и назначение из основного фильтра поменяются местами.
 - `false` — применять сетевой фильтр к трафику в одном направлении. В этом случае в ViPNet Client 5 будет загружен текущий сетевой фильтр, дополнительный сетевой фильтр создан не будет.

Значение по умолчанию `false`.

- В параметре `FilteringAction` укажите действие фильтра: пропустить (PASS) или заблокировать (DROP) IP-пакет.

8 Остальные структуры и параметры из примера в пункте 2 не изменяйте и не удаляйте.

Группы объектов

Чтобы упростить процесс описания сетевых фильтров в файле *.xml, вы можете задать в структуре <NamedObjects> группы объектов, а затем указывать только номера этих групп в составе сетевых фильтров:



Внимание! Не меняйте последовательность секций в структуре <NamedObjects>, иначе сетевые фильтры не будут работать.

1 Чтобы создать группу протоколов и портов:

1.1 Скопируйте структуру:

```
<ServiceObject>
  <Name>Protocol 1</Name>
  <Id>1</Id>
  <CreationType>Policy</CreationType>
  <Inclusion xsi:type="vn:TcpCondition">
    <DestinationPort xsi:type="vn:PortRange">
      <Begin>
        <Value>1</Value>
      </Begin>
      <End>
        <Value>443</Value>
      </End>
    </DestinationPort>
    <Protocol>6</Protocol>
  </Inclusion>
  <Exclusion xsi:type="vn:TcpCondition">
    <Protocol>6</Protocol>
  </Exclusion>
  <Exclusion xsi:type="vn:TcpCondition">
    <DestinationPort xsi:type="vn:Port">
      <Value>21</Value>
    </DestinationPort>
    <Protocol>6</Protocol>
  </Exclusion>
</ServiceObject>
```

1.2 В параметре Name укажите имя группы объектов (текст не более 255 символов).

1.3 В параметре Id укажите номер группы объектов.

- 1.4 В структуре `<Inclusion>` укажите состав группы. Вы можете указать номер протокола, порт или диапазон портов источника и назначения или системную группу объектов. Используйте синтаксис, аналогичный структуре `<ServiceCondition>` (см. [Протокол](#)).
 - 1.5 В структуре `<Exclusion>` укажите исключения из состава группы. Вы можете указать номер протокола, порт или диапазон портов источника и назначения. Используйте синтаксис, аналогичный структуре `<ServiceCondition>` (см. [Протокол](#)).
 - 1.6 Остальные структуры и параметры из примера в пункте 1.1 не изменяйте и не удаляйте.
- 2 Чтобы создать группу узлов сети ViPNet:

2.1 Скопируйте структуру:

```
<VpnObject>
  <Name>ViPNet Nodes 1</Name>
  <Id>3</Id>
  <CreationType>Policy</CreationType>
  <Exclusion xsi:type="vn:VpnNameTemplate">
    <Template>ARM-ADMIN-VPN1722-*</Template>
  </Exclusion>
  <Inclusion xsi:type="vn:VpnSystemObjectRef">
    <Name>AllClients</Name>
  </Inclusion>
</VpnObject>
```

- 2.2 В параметре `Name` укажите имя группы объектов (текст не более 255 символов).
 - 2.3 В параметре `Id` укажите номер группы объектов.
 - 2.4 В структуре `<Exclusion>` укажите исключения из состава группы. Вы можете указать ViPNet-идентификатор, переведённый в десятичную систему, шаблон имени защищённого узла, номер сети ViPNet или одну из системных групп объектов. Используйте синтаксис, аналогичный структуре `<VpnHostCondition>` (см. [Источник и назначение](#)).
 - 2.5 В структуре `<Inclusion>` укажите состав группы. Вы можете указать ViPNet-идентификатор, переведённый в десятичную систему, шаблон имени защищённого узла, номер сети ViPNet или одну из системных групп объектов. Используйте синтаксис, аналогичный структуре `<VpnHostCondition>` (см. [Источник и назначение](#)).
 - 2.6 Остальные структуры и параметры из примера в пункте 2.1 не изменяйте и не удаляйте.
- 3 Чтобы создать группу расписаний:

3.1 Скопируйте структуру:

```
<ScheduleObject>
  <Name>Schedule 1</Name>
  <Id>3</Id>
  <CreationType>Policy</CreationType>
  <Exclusion xsi:type="vn:Daily">
    <StartTime>09:30:00</StartTime>
  </Exclusion>
</ScheduleObject>
```

```
<EndTime>10:00:00</EndTime>
</Exclusion>
<Inclusion xsi:type="vn:Daily">
  <StartTime>09:00:00</StartTime>
  <EndTime>17:00:00</EndTime>
</Inclusion>
</ScheduleObject>
```

- 3.2 В параметре `Name` укажите имя группы объектов (текст не более 255 символов).
- 3.3 В параметре `Id` укажите номер группы объектов.
- 3.4 В структуре `<Exclusion>` укажите исключения из состава группы. Вы можете указать время для ежедневного применения, определённый период или определённые дни недели. Используйте синтаксис, аналогичный структуре `<ScheduleCondition>` (см. [Расписание](#)).
- 3.5 В структуре `<Inclusion>` укажите состав группы. Вы можете указать время для ежедневного применения, определённый период или дни недели. Используйте синтаксис, аналогичный структуре `<ScheduleCondition>` (см. [Расписание](#)).
- 3.6 Остальные структуры и параметры из примера в пункте 3.1 не изменяйте и не удаляйте.

Источник и назначение

В структурах `<Source>` и `<Destination>` во вложенной структуре `<VpnHostCondition>` укажите отправителя и получателя IP-пакетов, к которым будет применяться сетевой фильтр. Если нужно указать несколько источников или назначений, скопируйте структуру `<VpnHostCondition>` нужное количество раз.

В качестве источника или назначения могут быть указаны:

- `xsi:type="vn:VpnNodeId"` — ViPNet-идентификатор защищённого узла, переведённый в десятичную систему, например 2DBF001D -> 767492125. В этом случае структура должна выглядеть следующим образом:

```
<Source xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnNodeId">
    <Value>767492125</Value>
  </VpnHostCondition>
</Source>
```

Или:

```
<Destination xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnNodeId">
    <Value>767492125</Value>
  </VpnHostCondition>
</Destination>
```

- `xsi:type="vn:VpnNetworkId"` — номер сети ViPNet. В этом случае структура должна выглядеть следующим образом:

```
<Source xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnNetworkId">
    <Value>4000</Value>
  </VpnHostCondition>
</Source>
```

Или:

```
<Destination xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnNetworkId">
    <Value>4000</Value>
  </VpnHostCondition>
</Destination>
```

- `xsi:type="vn:VpnNameTemplate"` — шаблон имени защищённого узла, заданный с помощью регулярных выражений. При этом в регулярных выражениях можно использовать только операции `?` (замена одного символа) и `*` (замена любого числа символов). В этом случае структура должна выглядеть следующим образом:

```
<Source xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnNameTemplate">
    <Template>Ivanov*</Template>
  </VpnHostCondition>
</Source>
```

Или:

```
<Destination xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnNameTemplate">
    <Template>Ivanov*</Template>
  </VpnHostCondition>
</Destination>
```

- `xsi:type="vn:VpnObjectRef"` — группа узлов (см. [Группы объектов](#)), описанная в структуре `<NamedObjects>`. В этом случае укажите только номер группы:

```
<Source xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnObjectRef">
    <Id>1</Id>
  </VpnHostCondition>
</Source>
```

Или:

```
<Destination xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnObjectRef">
    <Id>2</Id>
  </VpnHostCondition>
</Destination>
```

- `xsi:type="vn:VpnSystemObjectRef"` — системная группа объектов. В этом случае укажите только имя системной группы:
 - `AllClients` — все клиенты сети ViPNet, с которыми у узла есть связь.
 - `AllCoordinators` — все координаторы сети ViPNet, с которыми у узла есть связь.
 - `LocalHost` — собственный узел.
 - `OtherHost` — все узлы сети ViPNet, кроме собственного.



Внимание! Чтобы задать структуре `<Source>` или `<Destination>` значение «Все» (All), не указывайте её в `.xml`-файле. В ViPNet Client 5 по умолчанию задаётся значение «Все» (All), если структура не указана.

В этом случае структура должна выглядеть следующим образом:

```
<Source xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnSystemObjectRef">
    <Name>AllClients</Name>
```

```
    </VpnHostCondition>
</Source>
```

Или:

```
<Destination xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnSystemObjectRef">
    <Name>AllClients</Name>
  </VpnHostCondition>
</Destination>
```

Пример указания источника и назначения:

```
<Source xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnNodeId">
    <Value>767492125</Value>
  </VpnHostCondition>
  <VpnHostCondition xsi:type="vn:VpnNodeId">
    <Value>368902358</Value>
  </VpnHostCondition>
</Source>

<Destination xsi:type="vn:PrivateNetwork">
  <VpnHostCondition xsi:type="vn:VpnSystemObjectRef">
    <Name>LocalHost</Name>
  </VpnHostCondition>
</Destination>
```

Протокол

В структуре `<ServiceCondition>` укажите протокол и порты, к которым будет применяться сетевой фильтр.

- `xsi:type` — тип протокола, к которому будет применяться сетевой фильтр:
 - `xsi:type="vn:TcpCondition"` — TCP.
 - `xsi:type="vn:UdpCondition"` — UDP.
 - `xsi:type="vn:IcmpCondition"` — ICMP-сообщение.
 - `xsi:type="vn:ProtocolCondition"` — другие протоколы, инкапсулируемые в IP.
 - `xsi:type="vn:ServiceObjectRef"` — группа протоколов (см. [Группы объектов](#)), описанная в структуре `<NamedObject>`. В этом случае укажите только номер группы:

```
<ServiceCondition xsi:type="vn:ServiceObjectRef">
  <Id>2</Id>
</ServiceCondition>
```



Внимание! Чтобы задать структуре `<ServiceCondition>` значение «Все» (All), не указывайте её в `.xml`-файле. В ViPNet Client 5 по умолчанию задаётся значение «Все» (All), если структура не указана.

- `Type` — тип ICMP-сообщения. Например, `<ServiceCondition Type="8" xsi:type="vn:IcmpCondition">`.
- `<SourcePort>` — порт или диапазон портов источника. Например:

```
<SourcePort xsi:type="vn:PortRange">
  <Begin>
    <Value>1</Value>
  </Begin>
  <End>
    <Value>443</Value>
  </End>
</SourcePort>
```
- `<DestinationPort>` — порт или диапазон портов назначения. Например:

```
<DestinationPort xsi:type="vn:Port">
  <Value>10001</Value>
</DestinationPort>
```
- `Protocol` — номер протокола (см. [список на сайте](#)).

Пример структуры <ServiceCondition>:

```
<ServiceCondition xsi:type="vn:TcpCondition">
  <DestinationPort xsi:type="vn:Port">
    <Value>80</Value>
  </DestinationPort>
  <Protocol>6</Protocol>
</ServiceCondition>
```

Или:

```
<ServiceCondition xsi:type="vn:UdpCondition">
  <SourcePort xsi:type="vn:Port">
    <Value>1024</Value>
  </SourcePort>
  <DestinationPort xsi:type="vn:PortRange">
    <Begin>
      <Value>1024</Value>
    </Begin>
    <End>
      <Value>1030</Value>
    </End>
  </DestinationPort>
  <Protocol>17</Protocol>
</ServiceCondition>
```

Или:

```
<ServiceCondition Type="8" xsi:type="vn:IcmpCondition">
  <Protocol>1</Protocol>
</ServiceCondition>
```

Или:

```
<ServiceCondition xsi:type="vn:ProtocolCondition">
  <Protocol>4</Protocol>
</ServiceCondition>
```

Расписание



Внимание! Сетевые фильтры будут применяться по расписанию в соответствии с локальным временем на устройстве.

В структуре `<ScheduleCondition>` укажите расписание, по которому будет применяться сетевой фильтр:

- `xsi:type` — тип расписания, по которому будет применяться сетевой фильтр:
 - `xsi:type="vn:Daily"` — каждый день в заданное время.
 - `xsi:type="vn:Calendar"` — в течение выбранного периода.
 - `xsi:type="vn:Weekly"` — в выбранные дни недели.
 - `xsi:type="vn:ScheduleObjectRef"` — группа расписаний (см. [Группы объектов](#)), описанная в структуре `<NamedObject>`. В этом случае укажите только номер группы:

```
<ScheduleCondition xsi:type="vn:ScheduleObjectRef">
  <Id>3</Id>
</ScheduleCondition>
```



Внимание! Чтобы задать структуре `<ScheduleCondition>` значение «Постоянно» (All), не указывайте её в `.xml`-файле. В ViPNet Client 5 по умолчанию задаётся значение «Постоянно» (All), если структура не указана.

- В параметрах `StartTime` и `EndTime` укажите время начала и конца действия сетевого фильтра в формате `hh:mm:ss`. Время окончания действия фильтра включает в себя последнюю минуту из указанного значения (например, если указано `18:00:00`, то фильтр перестанет действовать в `18:01:00`). Эти параметры указываются для любого типа расписания.
- В параметрах `StartDate` и `EndDate` укажите дату начала и конца действия сетевого фильтра в формате `yyyy-mm-dd`. Эти параметры указываются, если выбран тип расписания `Calendar`.
- В параметре `<WeekDays>` укажите, в какие дни недели будет применяться сетевой фильтр (значение `true` или `false`). Этот параметр указывается, если выбран тип расписания `Weekly`:

```
<WeekDays>
  <Monday>true</Monday>
  <Tuesday>false</Tuesday>
  <Wednesday>true</Wednesday>
  <Thursday>true</Thursday>
  <Friday>false</Friday>
  <Saturday>true</Saturday>
  <Sunday>true</Sunday>
</WeekDays>
```

Пример структуры <ScheduleCondition>:

```
<ScheduleCondition xsi:type="vn:Calendar">
  <StartTime>09:00:00</StartTime>
  <EndTime>18:00:00</EndTime>
  <StartDate>2022-02-03</StartDate>
  <EndDate>2022-02-10</EndDate>
</ScheduleCondition>
```

Или:

```
<ScheduleCondition xsi:type="vn:Weekly">
  <StartTime>09:00:00</StartTime>
  <EndTime>18:00:00</EndTime>
  <WeekDays>
    <Monday>true</Monday>
    <Tuesday>true</Tuesday>
    <Wednesday>true</Wednesday>
    <Thursday>true</Thursday>
    <Friday>true</Friday>
    <Saturday>false</Saturday>
    <Sunday>false</Sunday>
  </WeekDays>
</ScheduleCondition>
```

В

Общие и индивидуальные настройки профилей

Настройки и функции для всех профилей:

- [Уровень детализации в журнале.](#)
- [Настройки в файле vipnet.conf.](#)
- [Блокировка пользовательского трафика сторонним приложением.](#)
- [Контроль целостности программного обеспечения ViPNet Client 5 и среды функционирования.](#)

Настройки и функции, индивидуальные для каждого профиля:

- [Уровень детализации в журнале.](#)
- [Видимость туннелируемых узлов по виртуальным IP-адресам.](#)
- [Передача данных по протоколу TCP.](#)
- [Автоматический выбор сервера соединений и сохранение выбора сервера соединений.](#)

Подробнее см. руководство пользователя, раздел «Экспериментальные настройки».

- [Управление автозапуском ViPNet Client 5.](#)
- [Опции отладки:](#)
 - `--mdns`
 - `--no-mdns`
 - `--mdns-debug`
 - `--no-mdns-debug`
 - `--nvs-debug`
 - `--no-nvs-debug`

- [Настройки из секции firewall.](#)
- [Блокировка пользовательского трафика при проблемах с лицензией, многофакторной аутентификацией или политиками ZTNA.](#)
- [Расширенные настройки.](#)
- [Настройки прикладных протоколов.](#)
- [Смена пароля.](#)
Подробнее см. руководство пользователя, раздел «Смена пароля».
- [Многофакторная аутентификация.](#)
Подробнее см. руководство пользователя, раздел «Многофакторная аутентификация».
- [Переинициализация внутренних конфигурационных файлов](#)

Для каждого профиля проверяется разница во времени с координатором.

С

Возможные неполадки и способы их устранения

Особенности ViPNet Client 5

Условия	Возможные неполадки	Метод решения
- Координатор с ПО ViPNet Coordinator for Linux версии 4.3.x и координатор с ПО ViPNet Coordinator for Windows версии 4.3.x. - Клиент с программой ViPNet Client 5.	Если настроена видимость туннелируемых узлов по реальным IP-адресам и за двумя разными координаторами находятся туннелируемые узлы с одним и тем же реальным IP-адресом, на клиенте ViPNet Client 5 один из туннелируемых узлов становится недоступен.	Включите видимость туннелируемых узлов по виртуальным IP-адресам.

Не удаётся установить ViPNet Client 5

Убедитесь, что:

- на компьютере установлена поддерживаемая ОС (см. [Системные требования](#));
- установлены все зависимости — [связанные с компонентами ViPNet Client 5 библиотеки](#).

Не удаётся обновить ViPNet Client 5 с помощью QApt

Если обновление ViPNet Client 5 с помощью установщика пакетов QApt не завершается в течение длительного времени и при принудительном прерывании обновления появляется сообщение об ошибке:

- 1 Прервите обновление ViPNet Client 5.
- 2 Удалите конфигурационный файл `/etc/vipnet.conf`.
- 3 Повторно запустите обновление ViPNet Client 5.

После обновления на узле с центром управления ViPNet Prime в сети не принимаются обновления справочников из доверенной сети

Если на узле с ViPNet ЦУС или с центром управления ViPNet Prime:

- в вашей сети установлена актуальная версия ViPNet Client,
- в доверенной сети установлена прошлая версия ViPNet Client,

то в вашей сети не будут автоматически приниматься обновления справочников из этой доверенной сети. Остальное межсетевое взаимодействие не нарушится.

Чтобы обновления справочников автоматически принимались, попросите администраторов доверенной сети установить на узле с ViPNet ЦУС или с центром управления ViPNet Prime актуальную версию ViPNet Client:

- ViPNet Client for Windows 4.5.3 hotfix 7 и выше или ViPNet Client for Windows 4.5.5 hotfix 9 и выше,
- ViPNet Client 5 for Windows 5.1 и выше,
- ViPNet Client 5 for Linux 5.0.0 или 5.1.3 и выше.

До установки актуальной версии в доверенной сети вы можете установить обновления вручную. Для этого получите от администратора доверенной сети обновления доверенным способом.

После установки ViPNet Client 5 не отображаются иконки программ

- 1 Завершите текущий сеанс пользователя Linux.
- 2 Повторно войдите в ОС.

Не отображается информация о применении обновлений справочников и ключей в журнале транспортных конвертов в ViPNet Prime

Если в сети:

- на узле с центром управления ViPNet Prime установлены ключи *.ds5,
- есть узлы с ключами *.dst,

то для узлов с ключами *.dst в журнале транспортных конвертов в ViPNet Prime будет отображаться только информация о доставке обновлений справочников и ключей. Информация о применении обновлений на этих узлах отображаться не будет, даже если обновления применены.

Способы устранения

- Установите ключи *.dst на узле с центром управления ViPNet Prime или ключи *.ds5 на всех узлах сети.
- Отслеживайте применение обновлений справочников и ключей в журнале событий ViPNet Prime Network Visibility System.

Бесконечное обновление ViPNet Client 5 через opkg

После обновления ViPNet Client 5 через пакетный менеджер opkg при вызове других команд может отображаться бесконечный процесс обновления: `Software upgrage is in progress. Try again later.`

Способ устранения

Перезапустите службу ViPNet Client 5 одним из способов:

- `root@host:~# sudo pkill -9 vipnetclient`
- `root@host:~# sudo killall -USR1 vipnetclient`

Не запускается VPN-соединение после обновления

1 Выполните:

```
user@host:~$ vipnetclient reconfigure
```

2 Включите VPN-соединение:

```
user@host:~$ vipnetclient start
```

Изменился сервер соединений

При обновлении или в случае внутренних ошибок клиент может удалять информацию о взаимодействии узлов из внутренних конфигурационных файлов. Вместе с этим может сброситься выбор сервера соединений: активным снова станет координатор, заданный в управляющем ПО.

Способ устранения

Для клиентов с ключами *.dst включите настройку **Сохранять выбор сервера** или выполните:

```
user@host:~$ vipnetclient debug --active-server <идентификатор координатора> --insist
```

Тогда после обновления клиента или сброса внутренних конфигурационных файлов сервером соединений останется координатор, выбранный вручную.



Примечание. Чтобы проверить, какой координатор используется в качестве сервера соединений, включите VPN-соединение и выполните:

```
user@host:~$ vipnetclient info
```

Сервер соединений отобразится в строке **Active coordinator**.

Проблемы с отображением графического интерфейса ViPNet Client 5 в ОС Ubuntu 22.04 LTS

Если в ОС Ubuntu 22.04 LTS с оконным интерфейсом Wayland некорректно отображается ViPNet Client 5:

1 Убедитесь, что в ОС включён оконный интерфейс Wayland.

Для этого перейдите в настройки ОС во вкладку **О системе**. В строке **Оконный интерфейс** должен быть указан "Wayland".

2 Переключите оконный интерфейс на Xorg|X11.

Для этого в конфигурационном файле `/etc/gdm3/custom.conf` раскомментируйте строку `#WaylandEnable = false` и перезагрузите ОС.

или:

2.1 Завершите текущий сеанс пользователя Linux.

2.2 В окне аутентификации выберите пользователя и введите пароль.

2.3 В правом нижнем углу нажмите  и выберите **Ubuntu on Xorg**.

2.4 Выполните аутентификацию в ОС.

Не работает передача данных в ViPNet NVS по открытому каналу

ViPNet Client 5 проверяет безопасность сертификата, по которому устанавливается соединение с ViPNet NVS по открытому каналу. Если сертификат подписан корневым сертификатом сервера NVS, соединение устанавливается, и передача данных работает. По умолчанию ViPNet Client 5 получает корневой сертификат сервера NVS из параметра `certificate.root` из справочника `nvs.info`.

Если администратор NVS выключил параметр `certificate.root`, ViPNet Client 5 не сможет получить корневой сертификат сервера NVS. Тогда сертификат, по которому устанавливается соединение, будет проверяться по списку корневых доверенных сертификатов ОС. Если в списке нет корневого сертификата сервера NVS, передача данных не будет работать.

Способы устранения

- Добавьте корневой сертификат сервера NVS в корневые доверенные сертификаты ОС.
- На устройстве с сервером NVS включите отправку корневого сертификата NVS на конечные устройства:
 - Откройте для редактирования файл `/usr/share/infotecs/nvs/config.env`.
 - Включите параметр `certificate.root`, добавив строку:
`NVS_Core_CertificateOptions__SendRootCertificate=true`
 - Перезапустите сервер NVS. См. «ViPNet Prime Network Visibility System. Руководство администратора».
 - Перезагрузите компьютер с сервером NVS.

Нет соединения с координатором

Если не работает соединение с координатором версии 4.2.0 и ниже:

- 1 Проверьте, что реальный IP-адрес координатора отличается от IP-адреса узла.
- 2 Если IP-адреса совпадают, измените настройки координатора. Реальный IP-адрес координатора не должен пересекаться с адресами туннелируемых узлов. См. документацию управляющего ПО.

Сетевой экран firewalld блокирует работу ViPNet Client 5

Ниже приведены способы устранения возможных неполадок в ОС с сетевым экраном firewalld и установленной программой ViPNet Client 5.

Не работают прикладные протоколы

- 1 Добавьте интерфейс tun0 в зону trusted:

```
root@host:~# firewall-cmd --permanent --zone=trusted --change-interface=tun0
```

- 2 Переинициализируйте сетевой экран:

```
root@host:~# firewall-cmd --reload
```

Если добавление интерфейса tun0 в зону trusted не помогло:

- 1 Добавьте интерфейс tun0 в зону public:

```
root@host:~# firewall-cmd --permanent --zone=public --change-interface=tun0
```

- 2 Переинициализируйте сетевой экран:

```
root@host:~# firewall-cmd --reload
```

Не работает модуль mDNS:

- 1 Разрешите соединение на порт 5353 по протоколу UDP:

```
root@host:~# firewall-cmd --permanent --add-port=5353/udp
```

- 2 Переинициализируйте сетевой экран:

```
root@host:~# firewall-cmd --reload
```

- 3 Перезапустите модуль mDNS:

```
user@host:~$ vipnetclient debug --no-mdns
```

```
user@host:~$ vipnetclient debug --mdns
```

Совместная работа ViPNet Client 5 и службы SELinux

Если в ОС со службой SELinux и установленной программой ViPNet Client 5:

- блокируется создание unit ViPNet Client 5,
- не работает запуск VPN-соединения до аутентификации пользователя в ОС,
- появляется сообщение об отказе AVS,

создайте модуль локальной политики для службы SELinux:

1 Выполните:

```
root@host:~# ausearch -c '(etclient)' --raw | audit2allow -M my-etclient
root@host:~# semodule -i my-etclient.pp
```

2 Узнайте идентификатор процесса для службы vipnetclient:

```
user@host:~$ vipnetclient info
```

Идентификатор процесса отображается в поле **Process ID**.

3 Перезапустите службу ViPNet Client 5:

```
root@host:~# kill -9 <идентификатор_процесса>
```

Если блокируется запуск пользовательского интерфейса ViPNet Client 5:

1 Создайте модуль локальной политики для службы SELinux:

```
root@host:~# ausearch -c 'vipnetclient-gu' --raw | audit2allow -M my-vipnetclientgu
root@host:~# semodule -i my-vipnetclientgu.pp
```

2 Узнайте идентификатор процесса для службы vipnetclient:

```
user@host:~$ vipnetclient info
```

Идентификатор процесса отображается в поле **Process ID**.

3 Перезапустите службу ViPNet Client 5:

```
root@host:~# kill -9 <идентификатор_процесса>
```

Не работает служба systemd-resolver

При работе сторонних VPN, может не работать служба systemd-resolved.

Способ устранения

Перезапустите службу systemd-resolved:

```
user@host:~$ sudo systemctl restart systemd-resolved.service
```

Не удаётся установить дистрибутив ключей на компьютер

Если пользователь ViPNet Client 5 не может установить дистрибутив ключей на компьютер, удостоверьтесь, что пользователь вводит правильный пароль и дистрибутив ключей соответствует требованиям:

- Дистрибутив ключей создан в ViPNet Administrator версии 4.6.11 и выше или в ViPNet Prime версии 1.7.0 и выше.
- В ViPNet Administrator на клиент добавлена роль «Client for Linux» (0091) или в ViPNet Prime выбрана платформа Linux и лицензия Client for Linux (для ключей *.dst), Client for Linux v.5 или Universal Client v.5 (для ключей *.ds5).
- В дистрибутиве ключей содержится действительная лицензия на использование ViPNet Client 5.

В случае ошибки в процессе установки ключей обратитесь к администратору для выпуска нового дистрибутива ключей.

Нарушена работа ViPNet Client 5 с DNS

В ОС отсутствует доступ до корпоративных ресурсов по DNS-именам или не работает доменная зона .vipnet.

Способ устранения

Проверьте настройки в файле `vipnet.conf`. Возможно, в файле `vipnet.conf` выключено использование `iptables` либо произошла ошибка при загрузке правил `iptables`.

В случае ошибки загрузки правил `iptables`, если в ОС управление системным DNS осуществляется через `systemd-resolved`:

- 1 Перейдите в режим редактирования конфигурационного файла `/etc/systemd/resolved.conf`.
- 2 Раскомментируйте строку `DNS=` и укажите адрес DNS-сервера `11.254.254.254`:
`DNS=11.254.254.254`
- 3 Раскомментируйте строку `Domains=` и через пробел без запятых укажите доменные имена защищённых ресурсов, которые были заданы администратором сети.
- 4 Перезапустите `systemd-resolved`:
`root@host:~# systemctl restart systemd-resolved`

5 Очистите DNS-кэш:

```
root@host:~# systemd-resolve --flush-caches
```

или

```
root@host:~# resolvectl flush-caches
```

Если в ОС управление системным DNS осуществляется через `/etc/resolv.conf`:

1 Измените конфигурационный файл `/etc/resolv.conf`.

2 Добавьте адрес DNS-сервера:

```
nameserver 11.254.254.254
```



Примечание. Если в файле задано несколько DNS-серверов, строка `nameserver 11.254.254.254` должна быть первой и в списке заданных DNS-серверов.

Если в ОС управление системным DNS осуществляется через иные сервисы, обратитесь к документации данного сервиса и добавьте адрес DNS-сервера `11.254.254.254` и доменные имена защищённых ресурсов, которые были заданы администратором сети.

Если в ОС не заданы настройки системного DNS (например, IP-адрес, маска подсети, шлюз по умолчанию были заданы вручную), добавьте адрес DNS-сервера `11.254.254.254` в системные настройки DNS. Это нужно для доступа к корпоративным ресурсам по доменным именам и для доступности доменной зоны `.vipnet`.

Нарушена целостность компонентов программы ViPNet Client 5 или связанных системных библиотек

Если нарушена:

- целостность исполняемых файлов или библиотек ViPNet Client 5,
- работа датчиков случайных чисел или криптографических алгоритмов,

переустановите ViPNet Client 5:

1 [Удалите ViPNet Client 5.](#)

2 [Установите ViPNet Client 5.](#)

Если нарушена целостность справочников:

- 1 Удалите ключи.
- 2 Установите ключи. См. руководство пользователя.

Если одновременно нарушена целостность исполняемых файлов или библиотек ViPNet Client 5, целостность справочников и работа датчиков случайных чисел или криптографических алгоритмов:

- 1 Удалите ключи.
- 2 [Удалите ViPNet Client 5.](#)
- 3 [Установите ViPNet Client 5.](#)
- 4 Установите ключи в командной строке.

ViPNet Client 5 не определяет подключённое внешнее устройство

- 1 Перезапустите службу pcsd:

```
root@host:~# systemctl restart pcsd.service
```

- 2 Убедитесь, что ViPNet Client 5 for Linux определяет подключённое внешнее устройство:

```
user@host:~$ vipnetclient list --tokens
```

Проблемы с определением внешнего устройства из-за пакета OpenCT

- 1 Убедитесь, что пакет OpenCT установлен:

- Для DEB-пакета:

```
user@host:~$ dpkg -s openct
```

- Для RPM-пакета:

```
user@host:~$ rpm -q openct
```

- 2 Удалите пакет OpenCT:

- Для DEB-пакета:

```
root@host:~# dpkg -r openct
```

- Для RPM-пакета:

```
root@host:~# rpm -e openct
```

- 3 Перезапустите сервис pcsd:

```
root@host:~# systemctl restart pcsd.service
```

Не удаётся выполнить смену способа аутентификации при использовании внешнего устройства JaCarta

Если не удаётся выполнить смену способа аутентификации при использовании внешнего устройства JaCarta с версией ПК «Единый Клиент JaCarta» 3.0:

1 Убедитесь, что установлены пакеты jacartauc и jcpkcs11-2:

○ Для DEB-пакета:

```
user@host:~$ dpkg -s jacartauc
user@host:~$ dpkg -s jcpkcs11-2
```

○ Для RPM-пакета:

```
user@host:~$ rpm -q jacartauc
user@host:~$ rpm -q jcpkcs11-2
```

2 Удалите пакеты jacartauc и jcpkcs11-2:

○ Для DEB-пакета:

```
root@host:~# dpkg --purge jacartauc
root@host:~# dpkg --purge jcpkcs11-2
```

○ Для RPM-пакета:

```
root@host:~# rpm -e jacartauc
root@host:~# rpm -e jcpkcs11-2
```

3 Установите ПК «Единый Клиент JaCarta» версии 2.13.

4 Перезагрузите службу ViPNet Client 5:

```
user@host:~$ vipnetclient debug --reload
```

5 Отформатируйте внешнее устройство JaCarta.

Корпоративные ресурсы недоступны

Если пользовательский трафик заблокирован, пользователь сможет подключиться к защищённой сети, но не сможет работать с корпоративными ресурсами.

Чтобы просмотреть причину блокировки пользовательского трафика, выполните:

```
user@host:~$ vipnetclient info
```

В строке `User traffic status` отобразится статус `Blocked`.

Причина блокировки	Описание	Решение
by <путь_к_процессу>	Блокировка сторонним процессом.	Исправить причину блокировки в указанном стороннем процессе.
due to unfinished multi-factor authentication	Не пройдена многофакторная аутентификация.	- Пройти многофакторную аутентификацию. - Подробнее см. руководство пользователя.
due to license expiry	Лицензия истекла.	Обновить лицензию. Подробнее см. документацию управляющего ПО.
due to invalid license	Неподходящая лицензия.	- Проверить дату и другие поля лицензии, - проверить, что в ViPNet Administrator на клиент добавлена роль «Client for Linux» (0091) или в ViPNet Prime выбрана платформа Linux и лицензия Client for Linux (для ключей *.dst), Client for Linux v.5 или Universal Client v.5 (для ключей *.ds5), - отправить новую лицензию. Подробнее см. документацию управляющего ПО.
due to invalid license file	Лицензия имеет некорректный формат или повреждена.	Отправить новую лицензию. Подробнее см. документацию управляющего ПО.
due to zero-trust access feature	Не пройдена проверка политики ZTNA в программе ViPNet EPP Агент.	Выключить для клиента параметр Блокировка VPN без ViPNet EPP. Подробнее см. документацию ViPNet Prime

Уведомление «Загрузка неподписанного файла заблокирована C3 ОС (DIGSIG) /bpfilter_umh»

Уведомление появляется в Asrta Linux Special Edition 1.7 с включенной замкнутой программной средой. Это может происходить при установке и обновлении ключей, потому что модуль ядра bpfilter нельзя подписать цифровой подписью для работы в режиме замкнутой программной среды.

Способ устранения

Отключите модуль ядра bpfilter:

1 Запустите терминал Fly:

- Меню Пуск > Системные > Терминал Fly.
- «Alt» + «Т».

2 Выполните:

```
user@host:~$ sudo su
root@host:~$ echo "blacklist bpfilter" >> /etc/modprobe.d/blacklist-astra.conf
root@host:~$ echo "install bpfilter /bin/false" >> /etc/modprobe.d/blacklist-astra.conf
root@host:~$ depmod -a
root@host:~$ update-initramfs -uk all
```

3 Перезагрузите компьютер.

ViPNet Client 5 не отвечает и отображается непредвиденная ошибка

- При выполнении любой команды появляется ошибка «ViPNet Client does not respond. Try again later».
- При включении VPN-соединения в интерфейсе ViPNet Client 5 появляется ошибка «Непредвиденная ошибка. Возникла непредвиденная ошибка».

Способ устранения

1 Если вы используете Astra Linux Special Edition:

- #### 1.1
- Проверьте, что в ОС подключены базовый и расширенный репозитории. Если они не подключены, добавьте зафиксированные ветки базового и расширенного репозитория для вашей версии Astra Linux Special Edition в файл `/etc/apt/sources.list`.

1.2 Включите сохранение дампов памяти процессов:

```
user@host:~$ sudo apt install systemd-coredump
```

Подробнее см. документацию Astra Linux Special Edition.

2 Создайте дамп памяти ViPNet Client 5:

```
user@host:~$ sudo pkill -11 vipnetclient
```

3 Создайте отчёт об ошибке ViPNet Client 5 и отправьте его в ИнфоТеКС. Подробнее см. руководство пользователя.

Если вы используете Astra Linux Special Edition, приложите к письму с отчётом об ошибке созданный дамп памяти. По умолчанию он сохраняется в `/var/lib/systemd/coredump`.



Термины и сокращения

Iptables

Утилита для управления работой межсетевого экрана с помощью набора правил. Для использования утилиты iptables требуются права суперпользователя (root).

Personal Firewall

Модуль, реализующий функции персонального межсетевого экрана; объект лицензирования ViPNet EPP.

ViPNet Administrator

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

ViPNet Policy Manager

Программа для централизованного управления политиками безопасности узлов защищённой сети ViPNet.

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и 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.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

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

База правил

Набор предустановленных параметров и правил работы средств защиты ViPNet Client 5 for Linux: персонального межсетевого экрана, контроля приложений, обнаружения и предотвращения вторжений, ZTNA. Обновления базы правил регулярно публикуются на сервере обновлений.

Дистрибутив ключей

Файл с расширением *.dst или *.ds5 для каждого пользователя узла ViPNet. Создаётся в управляющем ПО ViPNet. Содержит справочники, ключи и файл лицензии для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Защищённый DNS-сервер

DNS-сервер, развёрнутый на ViPNet-узле, которому назначена роль DNS-сервер, или DNS-сервер, туннелируемый ViPNet-координатором, которому назначена роль DNS-сервер.

Зона .vipnet

Пространство доменных имён вида <идентификатор_узла_ViPNet>.vipnet и <IP-адрес_туннеля>.<идентификатор_туннелирующего_координатора>.vipnet. Внутри ViPNet Client 5 разрешаются в IP-адреса видимости этих узлов.

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.

Корпоративная DNS-зона

Пространство доменных имён корпоративных ресурсов, развёрнутых в защищённой сети.

Модуль ViPNet Network Visibility System

Модуль системы управления ViPNet Prime для мониторинга состояния устройств.

Обратный поиск DNS (reverse DNS lookup)

Обращение к DNS-зоне .in-addr.arpa для определения DNS-имени узла по его IP-адресу.

Персональный межсетевой экран

Средство защиты ViPNet Client 5 for Linux Агент. Выполняет фильтрацию IP-пакетов сетевого трафика защищаемого узла с помощью сетевых фильтров; реализовано модулем PFW.

Роль

Функциональность сетевого узла, которая решает целевые и служебные задачи сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Набор ролей для каждого сетевого узла задаёт администратор сети ViPNet в программе ViPNet Administrator.

Сервер соединений

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

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Суперпользователь (root)

Учётная запись в UNIX-системах, пользователь которой наделён специальными полномочиями, позволяющими осуществлять полный контроль над системой, изменять системные файлы, запускать специальные приложения, выполнять резервное копирование системы. Полномочия пользователя, работающего в системе с правами root, ничем не ограничены.

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами сети ViPNet.

Транспортный сервер UT

Серверная часть транспортного компонента UT ViPNet Administrator. Обеспечивает передачу транспортных сообщений по протоколу HTTP от ViPNet Administrator к транспортному клиенту UT устройств сети ViPNet, поддерживающих работу с дистрибутивом ключей *.ds5.

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.