



ViPNet Client 5 for Android

Руководство администратора

Версия продукта: 5.3.0

© АО «ИнфоТеКС», 2025

ФРКЕ.00405-01 32 01

Версия продукта 5.3.0

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

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

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

Все условия эксплуатации и ограничения на использование ViPNet Client 5 приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Client 5.

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.....	5
О документе.....	6
Соглашения документа.....	6
О программе	7
Различия форматов ключей.....	7
Рекомендации по безопасности	8
Системные требования	10
Требования к корпоративной сети	10
Протестированные на совместимость устройства	11
Что нового в версии 5.3.0	12
Комплект поставки	13
Обратная связь.....	14
 Глава 1. Установка и обновление ViPNet Client 5	15
Порядок установки ViPNet Client 5.....	16
Обновление из управляющего ПО	17
Рекомендации по повышению производительности.....	20
 Глава 2. Администрирование ViPNet Client 5	21
Многофакторная аутентификация.....	22
Назначение многофакторной аутентификации	22
Включение видимости туннелируемых узлов по виртуальным IP-адресам	24
Рекомендации по настройке работы с DNS	25
Способ выбора координатора	26
Координаторы в группе серверов	27
Подключение к узлам напрямую.....	28
Изменение портов для прикладных протоколов	29
Управление настройками ViPNet Client 5	30
Параметры ViPNet Client 5	31
Секция secured	31
Секция policies	31
Секция dns	32
Секция network.....	32
Секция settings	33
Секция firewall.....	33

Секция nodes.....	35
Секция features.....	37
Секция updates.....	37
Пример настроек.....	38
Загрузка файла обновлений справочников и ключей.....	40
Глава 3. Отладка ViPNet Client 5.....	41
Переход в режим отладки.....	42
Инструменты отладки.....	44
Настройки журналирования.....	44
Настройки защищённого соединения.....	45
Диагностика.....	51
Инструменты тестирования.....	54
Приложение А. Возможные неполадки и способы их устранения.....	55
Файл *.vrnconfig не применён.....	55
Не удаётся установить дистрибутив ключей на устройство.....	55
Нет соединения с координатором.....	56
Нет доступа к узлам по доменным именам.....	56
Увеличился расход заряда батареи устройства.....	56
Приложение В. Термины и сокращения.....	57



Введение

О документе	6
О программе	7
Системные требования	10
Что нового в версии 5.3.0	12
Комплект поставки	13
Обратная связь	14

О документе

Документ предназначен для администраторов [сети ViPNet](#), которые управляют приложением ViPNet Client 5 for Android (далее — ViPNet Client 5), установленным на мобильные устройства с операционной системой Android.

В документе содержится информация об администрировании приложения ViPNet Client 5.

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.

О программе

ViPNet Client 5 защищает IP-трафик на мобильных устройствах с Android (далее — устройства) путём шифрования IP-пакетов.

С помощью ViPNet Client 5 ваше устройство станет [узлом сети ViPNet](#) (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 приложение ViPNet CSS Connect.

Различия форматов ключей

В ViPNet Client 5 вы можете установить ключи в формате DST и DS5. Клиенты с ключами *.ds5 могут быть частью сетей пятого поколения.

	DST	DS5
Поколение сети	4	5
Управляющее ПО	ViPNet Administrator, ViPNet Prime	ViPNet Prime
Лицензия в ViPNet Prime	Client for Android	Client for Android v.5, Universal Client v.5
Транспорт	MFTP	UT
Управление портами для прикладных протоколов и настройками межсетевого экрана из управляющего ПО	+	-



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

Рекомендации по безопасности

Чтобы обеспечивать безопасность 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».

- В 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 и выше:
`$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

- Операционная система:
 - Android 8.0 и выше;
 - HarmonyOS 2.0.0 и выше;
 - kvadraOS 1.0.0 и выше;
 - РЕД ОС М 12.

Для операционной системы должны быть установлены актуальные обновления безопасности.

- Архитектура процессора и Android: ARM64.

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.

Протестированные на совместимость устройства

Модель	ОС
Samsung Galaxy S7	Samsung Experience 9.0 (Android 8)
Samsung Galaxy S25	Android 16
Samsung Galaxy S25 FE	Android 16
Samsung Galaxy S25 Ultra	Android 16
Samsung Galaxy A36 5G	Android 16
Samsung Galaxy Z Fold 7	Android 16
Redmi Note 7 Pro	Android 9
Pixel 3a	Android 11
Pixel 3aXL	Android 12
Pixel 4	Android 10
Pixel 5a	Android 12
Pixel 5	Android 12, 13, 14
Pixel 6 Pro	Android 16
Pixel 7	Android 15
Pixel 8	Android 16
Pixel 8 Pro	Android 16
Pixel 9	Android 16
Lenovo Tab P11	Android 11
Huawei P60 Pro	EMUI 14.2 (Android 12)
Xiaomi Redmi Note 13 Pro	Hyper OS 2 (Android 14)
Realme 12+	realme UI 6.0 (Android 15)
Honor 200 Lite	Magic OS 9 (Android 15)
Samsung Galaxy Tab S6 Lite	OneUI 6.1 (Android 14)
Samsung Galaxy Tab S10 FE	Android 16
Samsung Galaxy Tab S11 5G	Android 16
Huawei Pura 70 Pro	EMUI 14.2 (Android 12)
KVADRA_T	kvadraOS 1.23 (Android 12)
БайтЭрг MBK-T2101	Ред ОС М 12 (Android 12)
Huawei MatePad 11.5"S	HarmonyOS 4.2 (Android 12)

Что нового в версии 5.3.0

- **Возможность запретить менять расширенные настройки локально**

Теперь в управляющем ПО вы можете запретить пользователям изменять [расширенные настройки](#) на устройстве. Задайте эти настройки в секции `secured`, и они будут иметь приоритет над настройками, заданными по умолчанию и вручную. Эти настройки можно будет изменить только из управляющего ПО.

- **Исключения из блокировки пользовательского трафика**

Из управляющего ПО вы можете задать узлы, на которых будет разрешён пользовательский трафик, даже если не пройдена многофакторная аутентификация. Перечислите эти узлы [в секции policies](#) в расширенных настройках.

- **Дополнительная проверка служебных конвертов**

Теперь ViPNet Client 5 проводит больше проверок, чтобы подтвердить подлинность служебных конвертов. Некорректные конверты не обрабатываются и не применяются. Клиент блокирует их и отправляет уведомление о таких конвертах на узел с ViPNet ЦУС или с центром управления ViPNet Prime. [Вы можете посмотреть эту информацию в журнале клиента](#), установленного на этом узле. Рекомендуется регулярно отслеживать попытки доставить подозрительные служебные конверты на защищённые узлы.

- **Изменения в контроле защищённого трафика**

Клиент проверяет целостность входящих пакетов и их актуальность, чтобы поддерживать уровень безопасности в защищённой сети. Если какой-то узел отправляет пакеты, целостность которых нарушена, клиент временно блокирует трафик от этого узла. Если пакет устарел, клиент не принимает его. Теперь [в расширенных настройках клиента](#) администратор может управлять блокировкой трафика от отправителя некорректных пакетов и задавать допустимый интервал времени между отправлением и получением пакета.

- **Поддержка Android 16**

Комплект поставки

- Установочный файл ViPNet Client 5 в формате APK.
- Файлы для централизованного обновления клиентов с ключами *.dst в формате LZH.
- Файлы для централизованного обновления клиентов с ключами *.ds5 в формате ZIP.
- Документы в формате PDF:
 - Быстрый старт.
 - Руководство пользователя.
 - Руководство администратора.
 - Руководство по настройке работы сторонних приложений в сети ViPNet.
 - ViPNet Client 5 SDK API. Справочник разработчика.
 - ViPNet Client 5 SDK. Справочник разработчика.

Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ViPNet Client 5, см. в ZIP-архиве «ViPNet Client 5 for Android. 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 и обновление ViPNet Client 5

Порядок установки ViPNet Client 5	16
Обновление из управляющего ПО	17
Рекомендации по повышению производительности	20

Порядок установки ViPNet Client 5

Действие	Ссылка на документ
☐ В ViPNet ЦУС создайте узлы пользователей и назначьте им роль «VPN Client для мобильных устройств» или в ViPNet Prime создайте клиенты и выберите для них платформу Android	• «ViPNet Центр управления сетью. Руководство администратора», раздел «Добавление клиента» • «ViPNet Prime. Руководство администратора», раздел «Создание клиента»
☐ На координаторы, которые являются сервером соединений для добавленных узлов, отправьте обновление справочников и ключей с информацией о новых узлах. Иначе у ViPNet Client 5 не будет связи с защищённой сетью	• «ViPNet Центр управления сетью. Руководство администратора», раздел «Отправка обновлений на сетевые узлы»
☐ Установите ViPNet Client 5 на устройства пользователей с помощью файла *.apk или из магазина приложений	• «ViPNet Client 5 for Android. Руководство пользователя», раздел «Установка, обновление и удаление ViPNet Client 5»
☐ В ViPNet УКЦ или в ViPNet Prime создайте дистрибутивы ключей . Пользователям, которым хотите назначить многофакторную аутентификацию, добавьте связь с узлом Client Auth Server. Передайте пользователям дистрибутив ключей и пароль доверенным способом. Длина пароля не должна превышать 31 символ.	• «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Создание дистрибутивов ключей» • «ViPNet Prime. Руководство администратора», раздел «Создание дистрибутивов ключей»
☐ Убедитесь, что пользователи ViPNet Client 5 установили ключи и запустили приложение	• «ViPNet Client 5 for Android. Руководство пользователя», раздел «Установка ключей»

При выходе новой версии ViPNet Client 5 вы можете:

- Обновить ViPNet Client 5 на устройствах с помощью нового файла *.apk или из магазина приложений.
- Отправить обновление ViPNet Client 5 централизованно на все устройства вашей сети из управляющего ПО. При этом пользователям необходимо подтвердить установку обновления на устройствах.

Подробнее см. руководство пользователя, раздел «Установка, обновление и удаление ViPNet Client 5».



Внимание! На устройствах Samsung KNOX Enterprise при работе контейнера KNOX (внутри замкнутой программной среды) поддерживается только обновление с помощью файла *.apk.

Обновляйте ViPNet Client 4U сразу до актуальной версии ViPNet Client 5.

Обновление из управляющего ПО

Администратор сети ViPNet может отправлять обновление клиентов из управляющего ПО. Обновления применяются автоматически.

Обновление клиентов с ключами *.dst

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

Обновление клиентов с ключами *.ds5

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

Порядок обновления:

- 1 Загрузите архив с обновлением на HTTP-сервер внутри защищённой сети.
- 2 Укажите параметры обновления в расширенных настройках клиентов в ViPNet Prime в секции updates.

Вы можете задать параметры обновления вручную или получить их автоматически из ZIP-архива.

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

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


class MyDumper(yaml.Dumper):

    def increase_indent(self, flow=False, indentless=False):
        return super(MyDumper, self).increase_indent(flow, False)


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

```

```

        return update_info

if __name__ == "__main__":
    if len(sys.argv) < 2:
        print(f"usage: {sys.argv[0]} <update_file1.zip> [<update_file2.zip> ...] ")
        exit(1)

    update_root = {'updates': []}

    for _zip in sys.argv[1:]:
        print(f"# {_zip}")

        update_info = make_update_yaml_from_zip(_zip)

        update_root['updates'].append(update_info)

    print(yaml.dump(update_root, Dumper=MyDumper, default_flow_style=None,
sort_keys=False))

```

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 Android. В таблицу маршрутизации Android можно добавить только 1024 записи, поэтому 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 Android.
- 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 Android.

Из-за этого при переносе списка туннелируемых IP-адресов в таблицу маршрутизации Android могут записаться не все IP-адреса, заданные в справочнике. IP-адреса, которые не войдут в 1024 записи, будут игнорироваться, и клиент не сможет подключаться к ним.

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

Сокращение количества записей

Чтобы уменьшить количество записей в дистрибутиве ключей и в таблице маршрутизации Android, 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.

2

Администрирование ViPNet Client 5

Многофакторная аутентификация	22
Включение видимости туннелируемых узлов по виртуальным IP-адресам	24
Рекомендации по настройке работы с DNS	25
Способ выбора координатора	26
Координаторы в группе серверов	27
Подключение к узлам напрямую	28
Изменение портов для прикладных протоколов	29
Управление настройками ViPNet Client 5	30
Загрузка файла обновлений справочников и ключей	40

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. 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».

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.

Рекомендации по настройке работы с DNS

Для обеспечения корректной и безопасной работы пользователей с ресурсами корпоративной сети по доменным именам:

- В корпоративной сети выделите отдельные DNS-серверы для обработки защищённого трафика и для обработки трафика открытой сети.
- В ViPNet ЦУС добавьте DNS-серверы для защищённого трафика в список защищённых DNS-серверов и укажите их в настройках узла ViPNet Client 5, см. «ViPNet Центр управления сетью. Руководство администратора», раздел «Настройка защищённых DNS-серверов».
- В ViPNet Prime добавьте DNS-серверы для отправки запросов на разрешение доменных имён на защищённых DNS-серверах в профили DNS, см. «ViPNet Prime. Руководство администратора», раздел «Создание профилей DNS».
- Направьте защищённый трафик на обработку защищёнными DNS-серверами, открытый трафик — на обработку DNS-серверами для открытой сети. Для этого в ViPNet ЦУС в настройках защищённых DNS-серверов:
 - Укажите корпоративные DNS-зоны, которые будут обрабатываться этими серверами.
 - Снимите флажок **DNS-серверы поддерживают разрешение имен публичных ресурсов**.

В Android существуют ограничения:

- Указанное выше разграничение выполняется только для пользовательского DNS-трафика, служебный DNS-трафик будет обрабатываться DNS-серверами для открытой сети.
- Не все приложения поддерживают работу и отправку DNS-трафика через VPN. Вы можете просмотреть и настроить список приложений, работающих в защищённой сети, в [режиме отладки ViPNet Client 5](#).
- Включение опции **Использовать защищенные DNS-серверы для обработки доменов открытой сети** в режиме отладки ViPNet Client 5 замедляет работу с открытой сетью, а также увеличивает энергопотребление. Включать эту опцию не рекомендуется.
- Не включайте использование частных DNS-серверов в настройках Android. При включении этой опции в ViPNet Client 5 отобразится уведомление с рекомендацией отключить опцию.

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"
```

Изменение портов для прикладных протоколов

По умолчанию в клиенте для обработки прикладных протоколов используются стандартные порты:

- 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 программ требуется обработка трафика по другим портам, вы можете передать настройки на компьютеры пользователей одним из способов:

- 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. Во время активной работы пользователей настройки протоколов применяются с задержкой. Отправляйте настройки на компьютеры пользователей в нерабочие часы, тогда 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).

Управление настройками ViPNet Client 5

Вы можете задать настройки ViPNet Client 5 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. Настройки передаются в ViPNet Client 5 в составе справочников. Размер справочника должен быть до 1 Мбайта. Подробнее см. руководство администратора управляющего ПО.

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`.
- 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`
- `restrictedTrafficModeExclusions`

Секция policies

- `restrictedTrafficModeExclusions` — узлы, на которых будет разрешён пользовательский трафик, даже если 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 по умолчанию — `77.88.8.88, 77.88.8.2`.

- `searchDomain` — включение поиска коротких доменных имён в указанном домене.

Значение в ViPNet Client 5 по умолчанию отсутствует.

Секция network

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

По умолчанию в ViPNet Client 5 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 автоматически.

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.

-
- `enableDnsSD` — поиск VPN-устройств в локальной сети по протоколу DNS Service Discovery для взаимодействия с ними напрямую (без участия координатора) по протоколам IPv4 и IPv6.

Функция работает только с устройствами со значением `enableDnsSD: true` при включённом VPN-соединении.

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

Секция settings

- `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 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 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. Вы можете указать одно из значений:
 - `true` — открытый трафик блокируется.
 - `false` — открытый трафик разрешён.

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

- `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 `udp: []`.

Значение в ViPNet Client 5 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.

- `appsVpnAccessMode` — режим доступа приложений на устройстве в защищённую сеть. Вы можете указать один из трёх режимов:
 - `all` — доступ в защищённую сеть разрешён всем приложениям. Этот режим включается автоматически, если в параметре `blockOpenNetwork` указано значение `true`.
 - `allowList` — доступ в защищённую сеть запрещён всем приложениям, кроме исключений, указанных в параметре `appsAllowList`.
 - `blockList` — доступ в защищённую сеть разрешён всем приложениям, кроме исключений, указанных в параметре `appsBlockList`.

Значение в ViPNet Client 5 по умолчанию — `blockList`.

- `appsAllowList` — список идентификаторов приложений, которым разрешён доступ в защищённую сеть.



Внимание! ViPNet CSS Connect всегда имеет доступ в защищённую сеть и не отображается в списке `appsAllowList`. Если приложение ViPNet CSS Connect было установлено после выбора режима `allowList`, перезапустите VPN-соединение.

- `appsBlockList` — список идентификаторов приложений, которым запрещён доступ в защищённую сеть.

Примечание. Чтобы узнать идентификатор приложения:



- в веб-версии [Google Play](#) найдите приложение, на странице информации о приложении идентификатор отобразится в адресной строке в параметре `id`. Например: `https://play.google.com/store/apps/details?id=com.google.chrome`.
 - в веб-версии RuStore найдите приложение, на странице информации о приложении идентификатор отобразится в конце адресной строки. Например: `https://apps.rustore.ru/app/com.google.chrome`.
-

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 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 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 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 имя файла обновления.
- `product: vpn-client`.
- `brand: vipnet`.
- `version` — версия обновления.
- `platform: android`.
- `arch` — архитектура процессора: `armv8`.
- `edition` — список особенностей.

Криптография:

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

Страна: `ru`.

Дистрибутив: `apk`.

Магазин приложений: `other`.

- `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
  - features
  - policies.restrictedTrafficModeExclusions
dns:
  trustedServers:
    - 77.88.8.88
    - 77.88.8.2
  searchDomain: infotecs-nt

settings:
  macSpoofingProtection: true
  allowedPacketTimeDiff: 7200
network:
  privateSubnet: 192.168.0.0
  tcpMssDecrease: 20
  mtuOnTun: 2000
  enableDnsSD: false
firewall:
  blockOpenNetwork: false
  appsVpnAccessMode: allowList
  appsAllowList:
    - com.google.chrome
    - ru.yandex.browser
  appsBlockList:
    - com.google.vending
  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
nodes:
  privateAddressAssignment:
    strategy: BUNCHES_4x16K
    bunchesGatewaysList:
      - 12340000
      - 12340000
      - 12340000
      - 12340000
  flags:
    0004008A:
      forceStaticAccessPoints: false
  staticAccessPoints:
    0004008A:
      - "192.168.1.71:55778"
      - "192.168.1.71:55779"
      - "192.168.1.71:55780"
features:
  - name: tunnel_priority
    mode: active_coordinator
updates:
  - url: "путь к ZIP-архиву с обновлением на HTTP-сервере"
    name: client-andriod_armv8_update_5.3.0.zip
    product: vpn-client
    brand: vipnet
    version: 5.3.0
    platform: android
    arch: armv8
    edition: [gost, ru, apk, other]
    retry_timeout: 300

```

Загрузка файла обновлений справочников и ключей



Внимание! Выполняйте описанные ниже действия только по рекомендации технических специалистов ИнфоТеКС.

Если обновление справочников или ключей невозможно передать на устройства пользователей из управляющего ПО, вы можете вручную загрузить в ViPNet Client 5 файл *.ctl или *.bin с обновлением справочников или ключей. Для этого:

- 1 Передайте файл на устройство с ViPNet Client 5 доверенным способом.
- 2 Откройте файл. Если появится окно выбора приложения для открытия файла, нажмите ViPNet Client 5.

Обновление установится, если файл:

- проходит проверки целостности и подлинности;
- содержит обновление справочников или ключей для того узла, на котором применяется;
- дата создания файла позже, чем дата создания обновлений справочников или ключей, установленных ранее.



3

Отладка ViPNet Client 5

Переход в режим отладки	42
Инструменты отладки	44

Переход в режим отладки

Для доступа к расширенным настройкам и инструментам проверки работоспособности ViPNet Client 5 перейдите в режим отладки:

- 1 Выберите  > О приложении.
- 2 Трижды нажмите надпись **ViPNet Client** в течение 1 секунды.
- 3 Включите  **Режим разработчика**.

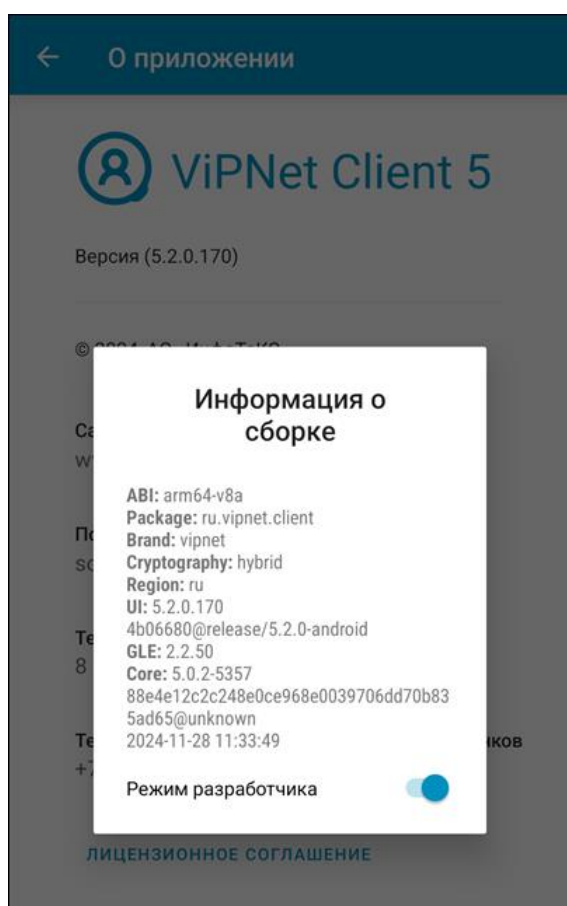


Рисунок 1. Включение режима разработчика

ViPNet Client 5 переключится в режим отладки:

- На главном экране приложения отобразится разница времени с сервером соединений и кнопки для перехода к списку связанных узлов, настройкам ViPNet Client 5 и инструментам его отладки (см. [Инструменты отладки](#)).
- В меню приложения появится пункт **Отладка** для перехода к инструментам отладки ViPNet Client 5.
- На экране свойств узлов из списка связанных узлов появятся кнопки проверки соединения (ping)  и просмотра сетевых настроек защищённого узла .

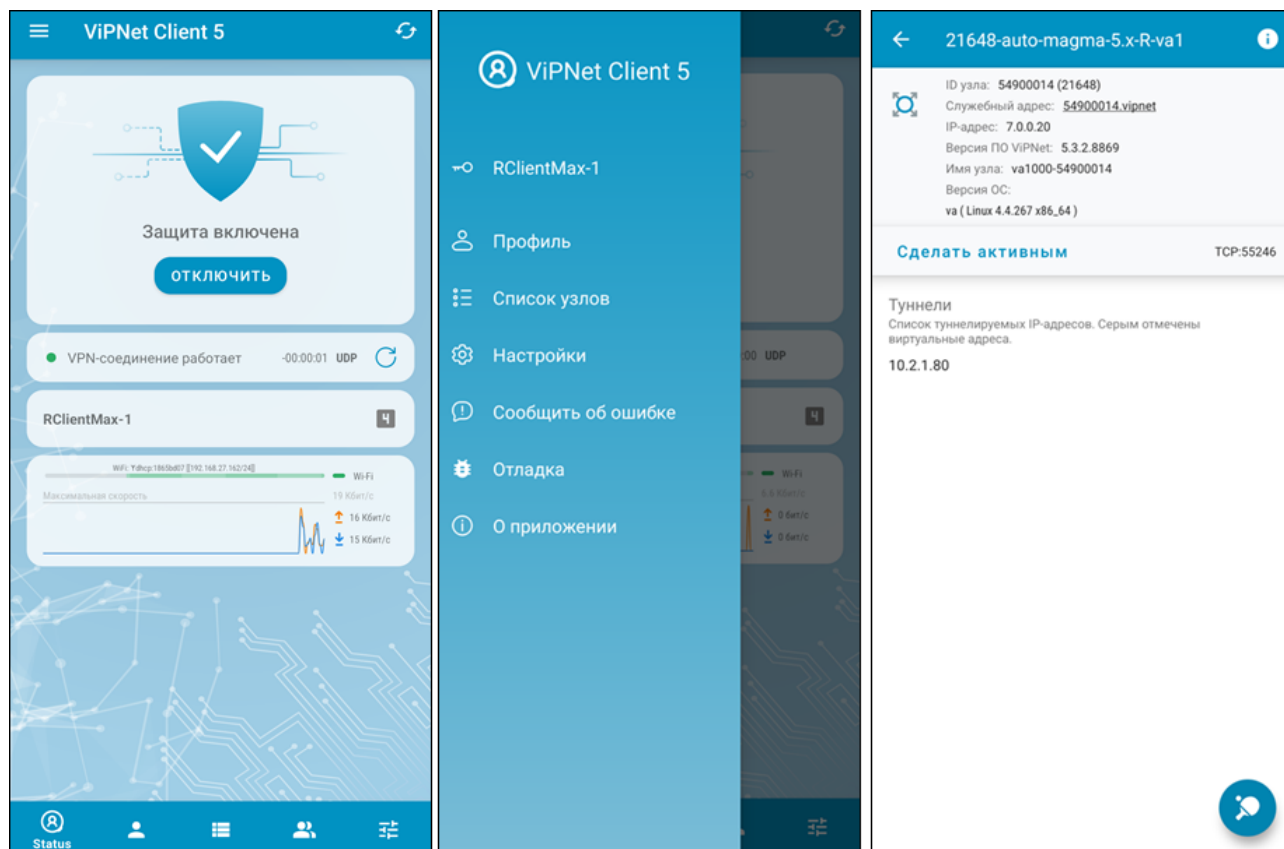


Рисунок 2. Интерфейс приложения ViPNet Client 5 в режиме отладки

Для выхода из режима отладки выполните одно из действий:

- Выберите  > **Настройки** и нажмите **Отключить режим разработчика**.
- Выберите  > **О приложении**, трижды нажмите надпись **ViPNet Client** в течение 1 секунды и выключите  **Режим разработчика**.

Инструменты отладки

Настройки журналирования

- **Уровень детализации в журнале.** Доступны 11 уровней. Значение по умолчанию — 3. Если включён режим отладки или расширенное протоколирование, значение по умолчанию — 5. Чтобы получить отладочную информацию, установите значение 5.

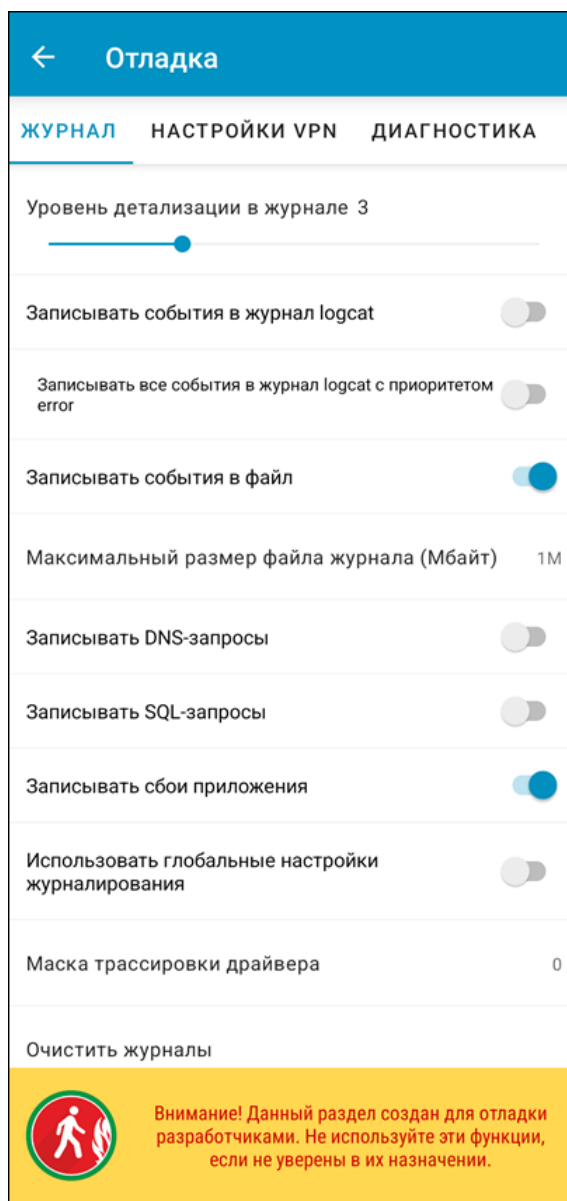


Рисунок 3. Настройки журналирования ViPNet Client 5

- **Записывать события в журнал logcat** (системный журнал). По умолчанию — выключена.

- **Записывать все события в журнал logcat с приоритетом error** — журналировать все события ViPNet Client 5 на устройствах, которые записывают в системный журнал только события с приоритетами fatal и error. По умолчанию — выключена.
- **Записывать события в файл**. По умолчанию — включена.
- **Максимальный размер файла журнала (Мбайт)**. По умолчанию — 1 Мбайт.
- **Записывать DNS-запросы** — дополнительно журналировать все DNS-запросы, проходящие через ViPNet Client 5. По умолчанию — выключена. Включать настройку рекомендуется только разработчикам ViPNet Client 5.
- **Записывать SQL-запросы**. По умолчанию — выключена.
- **Записывать сбои приложения** — журналировать сбои приложения. Эту настройку можно выключать при работе с ViPNet Client 5 в режиме отладки, чтобы тестовые сбои не учитывались в журнале. По умолчанию — включена.
- **Использовать глобальные настройки журналирования** — сохранять для всех профилей настройки журналирования, заданные последними. Если настройка выключена, то для каждого профиля можно задать собственные настройки журналирования. По умолчанию — выключена.
- **Маска трассировки драйвера** — типы событий в драйвере, которые необходимо записывать в журнал. Задается при помощи побитовой маски, например 128, 256. Значение по умолчанию — 0. Изменять значение параметра рекомендуется только разработчикам ViPNet Client 5.
- **Очистить журналы** — удаление файлов журнала ViPNet Client 5. После очистки запись событий продолжится в уже начатые файлы журнала.

Настройки защищённого соединения

- **Доступ приложений в VPN** — управление доступом приложений в защищённую сеть. Сокращение списка приложений, которым разрешён доступ в защищённую сеть, помогает экономить заряд батареи. Вы можете использовать один из трёх вариантов настройки:
 - Доступ разрешён всем приложениям. Эта настройка применяется автоматически, если включена блокировка открытого IP-трафика.
 - Доступ разрешён всем приложениям, кроме исключений (чёрный список). При выборе этого варианта нажмите **Приложения-исключения** и запретите конкретным приложениям доступ к защищённой сети  (запретить).
 - Доступ запрещён всем приложениям, кроме исключений (белый список). При выборе этого варианта нажмите **Приложения-исключения** и разрешите конкретным приложениям доступ к защищённой сети  (разрешить).

Белый и чёрный списки приложений ведутся независимо. При необходимости вы можете переключаться между этими настройками и не настраивать каждый раз новый список. По умолчанию используется чёрный список.

Если вы получили значение этого параметра из ViPNet ЦУС, а затем изменили его в режиме отладки, приоритетным будет значение, заданное в режиме отладки, а значение из ViPNet ЦУС будет игнорироваться. Чтобы вернуть приоритет настройке из ЦУС, нажмите и удерживайте заголовок **Доступ приложений в VPN**, при этом исчезнет жёлтая окраска этой области.



Внимание! После изменения настройки **Доступ приложений в VPN**, в том числе изменений в белом или чёрном списке приложений, перезапустите VPN-соединение.

ViPNet CSS Connect всегда имеет доступ в защищённую сеть и не отображается в списке **Приложения-исключения**. Если приложение ViPNet CSS Connect было установлено после выбора режима **Запрещен всем, кроме исключений**, перезапустите VPN-соединение.

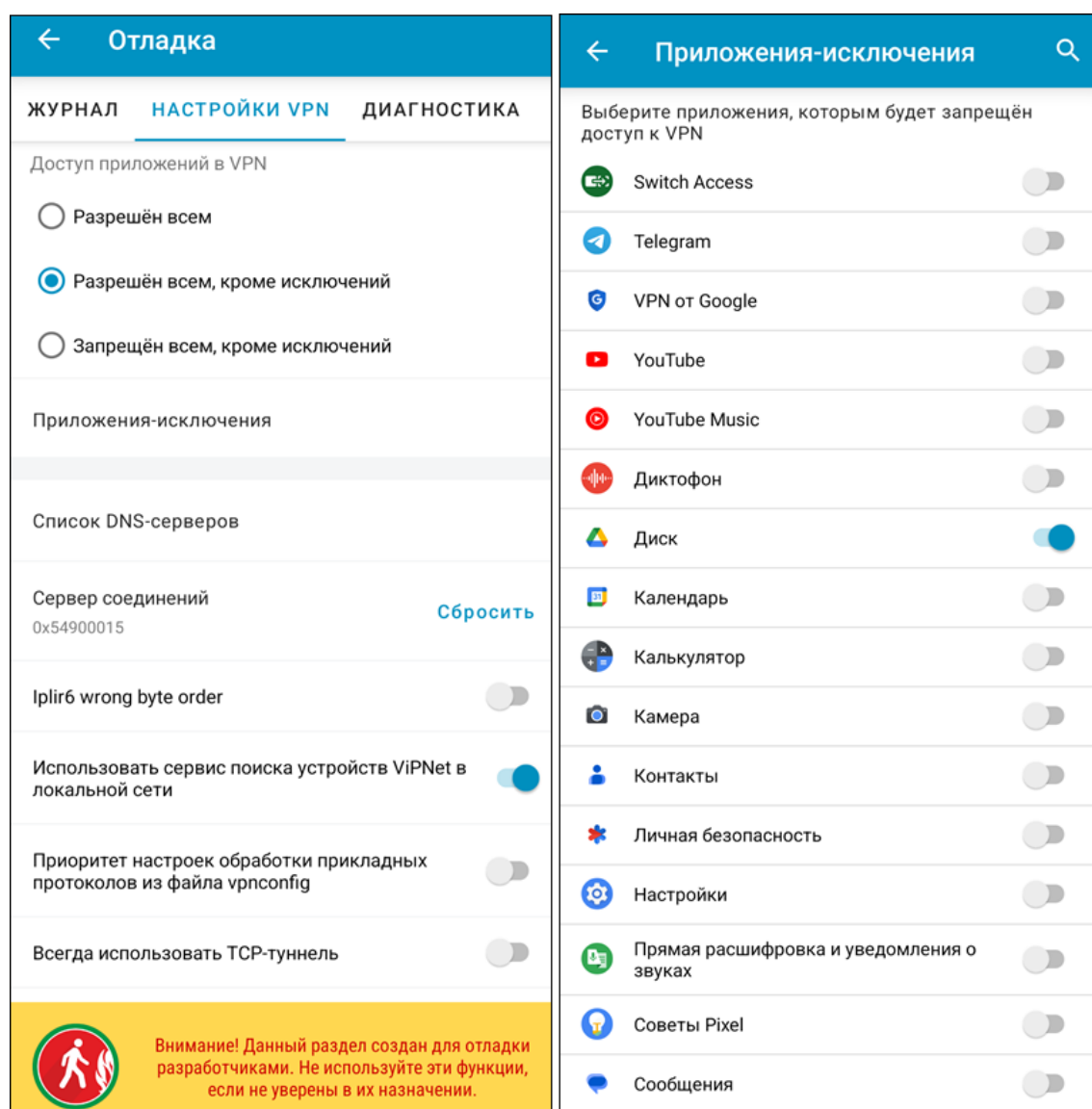


Рисунок 4. Запрет доступа приложений в сеть ViPNet

- **Список DNS-серверов** — разрешение работы с заданными на устройстве DNS-серверами.



Рисунок 5. Список DNS-серверов, заданных на устройстве

- **Сервер соединений** — ViPNet-идентификатор текущего сервера соединений. Нажмите **Сбросить**, чтобы вернуть сервер соединений по умолчанию (выбранный в управляющем ПО ViPNet). При этом автоматически выключится экспериментальная настройка **Сохранять выбор сервера**.
- **Использовать сервис поиска устройств ViPNet в локальной сети** — поиск устройств ViPNet в сети Wi-Fi по протоколу DNS Service Discovery для последующего взаимодействия с ними напрямую (без участия координатора) по протоколам IPv4 и IPv6. По умолчанию — выключена. Функция для разработчиков ViPNet Client 5.

Чтобы значение этого параметра, заданное в режиме отладки, было приоритетнее значения, [полученного из ViPNet ЦУС](#), нажмите и удерживайте строку **Использовать сервис поиска устройств ViPNet в локальной сети**, при этом она окрасится в жёлтый цвет. Чтобы вернуть приоритет настройке из ЦУС, повторите действия.

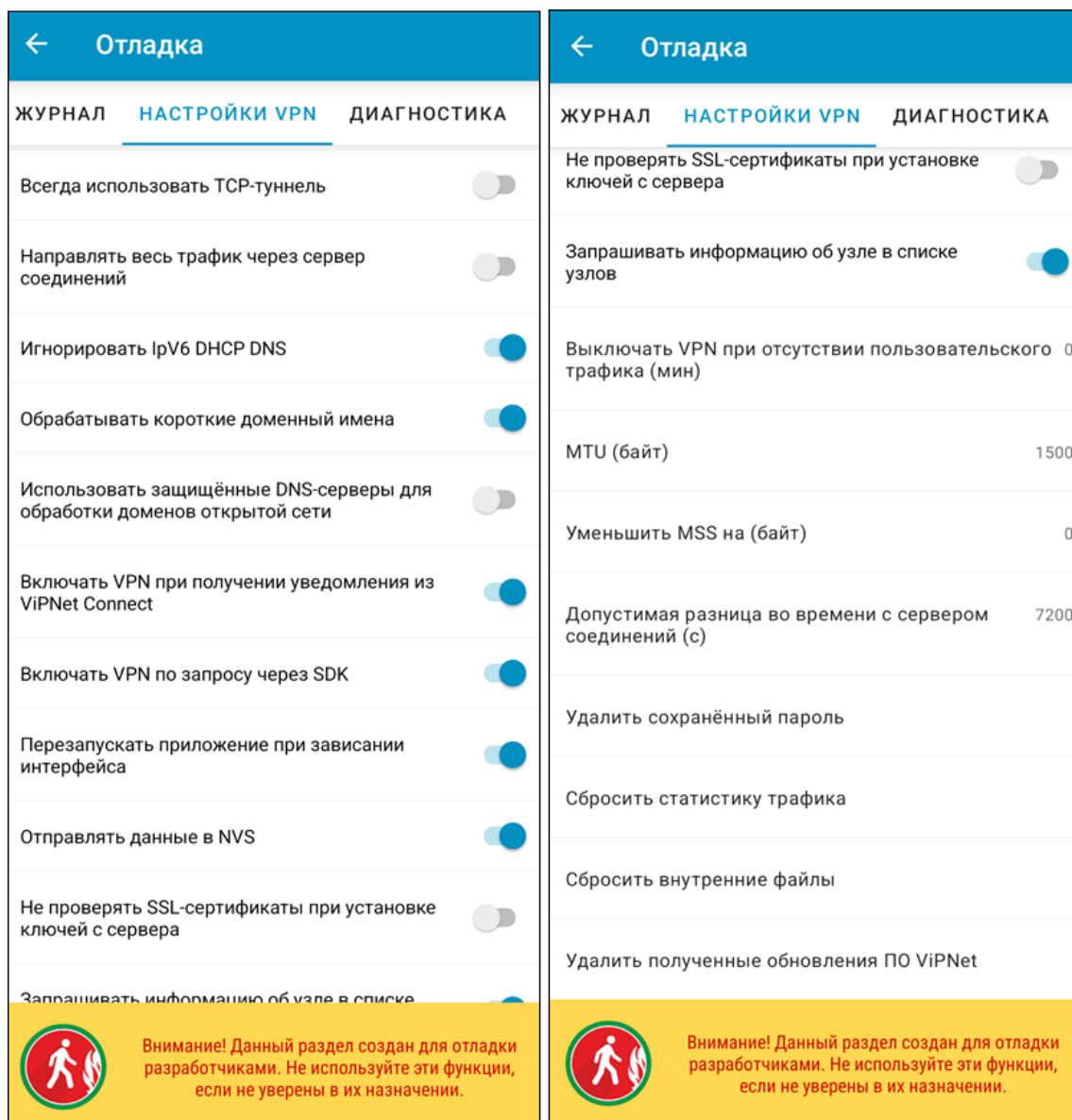


Рисунок 6. Настройка защищённого соединения

- **Приоритет настроек обработки прикладных протоколов из файла `vpnconfig`** — локальная настройка обработки прикладных протоколов. При включении этой функции будут использоваться только настройки из файла `*.vpnconfig`, а настройки, полученные из программы ViPNet Policy Manager, не будут приниматься на узле. По умолчанию локальная настройка выключена (настройки из программы ViPNet Policy Manager принимаются на узле).
- **Всегда использовать TCP-туннель** — всегда использовать протокол TCP для передачи данных. По умолчанию — выключена.
- **Направлять весь трафик через сервер соединений** — направлять весь VPN-трафик через сервер соединений. По умолчанию — выключена.
- **Игнорировать IPv6 DHCP DNS** — адреса IPv6 не будут обрабатываться ViPNet Client 5. По умолчанию — включена. Функция для разработчиков ViPNet Client 5.

- **Обрабатывать короткие доменные имена:**
 - Если настройка включена, то разрешение доменного имени будет выполняться по всем возможным доменам, пока не будет получен ответ.
 - Если настройка выключена, то будет выполнено разрешение только самого доменного имени.

По умолчанию настройка включена. Выключение настройки помогает экономить заряд батареи.

- **Использовать защищённые DNS-серверы для обработки доменов открытой сети.** По умолчанию — выключена. Выключение настройки помогает экономить заряд батареи.
- **Включать VPN при получении уведомления из ViPNet Connect.** По умолчанию — включена.
- **Перезапускать приложение при зависании интерфейса.** По умолчанию — выключена.
- **Отправлять данные в NVS** — отправка данных о работе устройства и ViPNet Client 5 в систему мониторинга ViPNet NVS. По умолчанию — включена. Функция для разработчиков ViPNet Client 5.
- **Не проверять SSL-сертификаты при установке ключей с сервера.** По умолчанию — выключена. Функция для разработчиков ViPNet Client 5.
- **Выключать VPN при отсутствии пользовательского трафика (мин)** — автоматическое отключение VPN-соединения при отсутствии пользовательского и DNS-трафика в течение заданного времени в минутах. По умолчанию — 0 (выключена).

Если сторонние приложения (например, почтовые клиенты) настроены на периодический опрос серверов, VPN-соединение не отключится.

- **MTU (байт)** — максимальный размер исходящего пакета на TUN-интерфейсе устройства. Значение по умолчанию — 1500 байт. Чтобы оптимизировать передачу данных через TUN-интерфейс, вы можете изменить размер MTU в диапазоне 1280–9000 байт.

Чтобы значение этого параметра, заданное в режиме отладки, было приоритетнее значения, [полученного из ViPNet ЦУС](#), нажмите и удерживайте строку **MTU (байт)**, при этом она окрасится в жёлтый цвет. Чтобы вернуть приоритет настройке из ЦУС, повторите действия.

- **Уменьшить MSS на (байт)** — число байт, на которое будет уменьшен параметр MSS (максимальный размер сегмента) протокола TCP. Значение по умолчанию — 0. 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 рекомендуется установить значение MSS от 20 до 40 байт. Чтобы уменьшить размер исходящих пакетов узла, значение параметра MSS следует изменить на узле получателя пакетов. Функция для разработчиков ViPNet Client 5.

Чтобы значение этого параметра, заданное в режиме отладки, было приоритетнее значения, [полученного из ViPNet ЦУС](#), нажмите и удерживайте строку **Уменьшить MSS на (байт)**, при этом она окрасится в жёлтый цвет. Чтобы вернуть приоритет настройке из ЦУС, повторите действия.

- **Допустимая разница во времени с сервером соединений (с).** Если предельное значение превышено, пакеты отклоняются. Значение по умолчанию — 7200 секунд. Изменять значение данного параметра рекомендуется только разработчикам ViPNet Client 5.
- **Удалить сохранённый пароль** — удаление пароля к дистрибутиву ключей, если пароль был сохранен пользователем.
- **Сбросить статистику трафика** — очистка статистики трафика, отображаемой в ViPNet Client 5.
- **Сбросить внутренние файлы** — создание новых конфигурационных файлов ViPNet Client 5 на основе последних актуальных справочников. Сброс может потребоваться в случае повреждения конфигурационных файлов при сбое ОС, неудачном обновлении справочников и ключей или в других нештатных ситуациях. Перед переинициализацией отключите VPN-соединение.



Примечание. Если вы изменяли активный координатор, то после сброса внутренних конфигурационных файлов клиента активным снова станет координатор, заданный в управляющем ПО.

- **Удалить полученные обновления ПО ViPNet** — удаление обновления ViPNet Client и ViPNet CSS Connect. Может потребоваться, если по ошибке было получено некорректное обновление.

Диагностика

- Просмотр содержимого системных файлов, примененных на устройстве: `iplir.conf`, `nodeinfo.txt`, `dns.txt`, `user.vpnconfig`, `user_info.json`, `custom.yaml`, `custom_user.yaml`, `custom_user_import.yaml`.

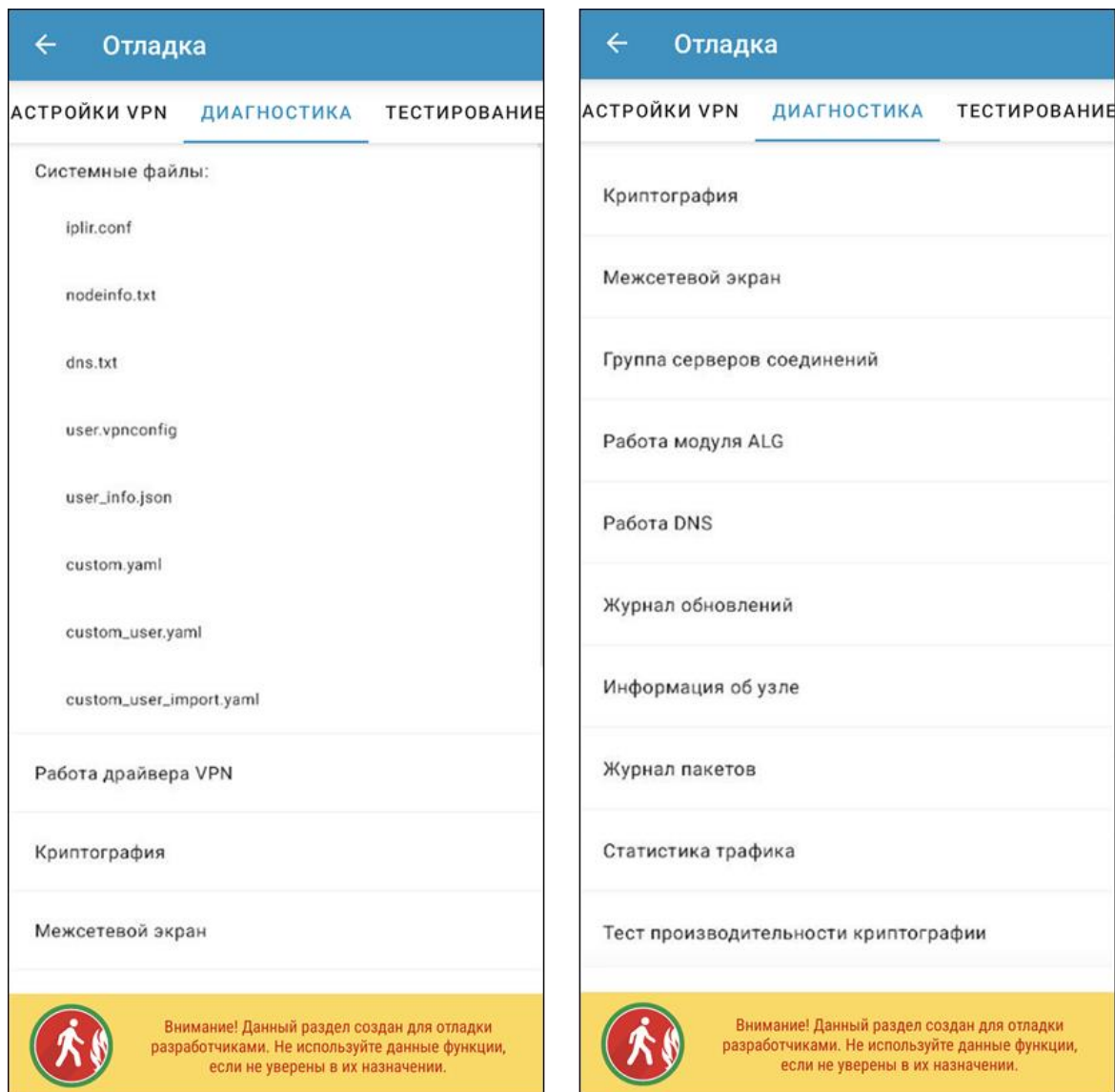


Рисунок 7. Диагностика работы ViPNet Client 5

- Работа драйвера VPN** — выполнение команд для получения информации об актуальном состоянии драйвера VPN и вывод результата на экран:

```
ipilirdiag -s adapters --info
ipilirdiag -s adapters --stats
ipilirdiag -s ipsettings --stats
ipilirdiag -s ipsettings --v-table
ipilirdiag -s ipsettings --v-tun-table
```

Функция для разработчиков ViPNet Client 5.

- **Криптография** — выполнение команды для получения списка доступных криптографических алгоритмов и вывод результата на экран:

```
ipilirdiag -s cipher -info
```

Функция для разработчиков ViPNet Client 5.

- **Межсетевой экран** — выполнение команды для получения информации о правилах межсетевого экрана и вывод результата на экран:

```
ipilirdiag -s firewall --stats
```

Функция для разработчиков ViPNet Client 5.

- **Группа серверов соединений** — выполнение команды для получения списка доступных серверов соединений и информации об активном сервере и вывод результата на экран:

```
ipilirdiag -s groupserver --info
```

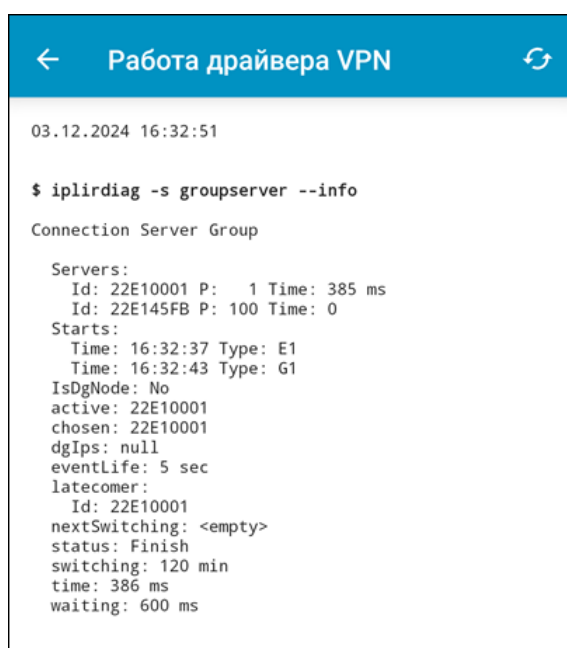


Рисунок 8. Просмотр информации о группе серверов соединений

Функция для разработчиков ViPNet Client 5.

- **Работа модуля ALG** — выполнение команд для получения информации о состоянии модуля ALG и вывод результата на экран:

```
ipilirdiag -s firewall --natal-bindings
```

```
ipilirdiag -s firewall --wait-rule
```

Функция для разработчиков ViPNet Client 5.

- **Работа DNS** — выполнение команды для диагностики работы DNS.

```
ipilirdiag -s dnsproxy --info
```

Функция для разработчиков ViPNet Client 5.

- **Журнал обновлений** — выполнение команды для получения информации о полученных обновлениях ViPNet Client 5 и вывод результата на экран:

```
iplirdiag -s updates --info
```

- **Информация об узле** — выполнение команды для просмотра сетевых настроек своего узла и вывод результата на экран:

```
ipilirdiag -s ipsettings --node-info
```

Функция для разработчиков ViPNet Client 5.

- **Журнал пакетов** — вывод на экран 1000 последних записей журнала IP-пакетов.

←

Журнал пакетов

03.12.2024 16:34:19

Time begin	Time end	Dev	Eth	Flags	Prot	Source IP	Port	Destination IP	Port	Size	Cnt	Src Node	DestNode	Event		
03.12.2024 16:33:37	03.12.2024 16:33:37	tun	800h	>-C---	6			7.0.0.20	8081					7.0.114.33 52634	64	
03.12.2024 16:33:37	03.12.2024 16:33:37	tun	800h	>-C---	6			7.0.0.20	8081					7.0.114.33 52634	64	
03.12.2024 16:33:37	03.12.2024 16:33:37	tun	800h	<-C---	6			7.0.114.33	52634					7.0.0.20 8081	169	
03.12.2024 16:33:37	03.12.2024 16:33:37	tun	800h	>-C---	6			7.0.0.20	8081					7.0.114.33 52634	571	
03.12.2024 16:33:47	03.12.2024 16:33:47	tun	800h	<D-----	58	fe80::b9d5:7162:8dd3:6585	0							ff02::2	0	48
03.12.2024 16:33:47	03.12.2024 16:33:47	tun	800h	<D-----	0	fe80::b9d5:7162:8dd3:6585	0							ff02::16	0	172
03.12.2024 16:33:47	03.12.2024 16:33:47	tun	800h	<-C---	17			7.0.114.148	2046					81.30.192.133 2049	72	
03.12.2024 16:33:47	03.12.2024 16:33:47	tun	800h	<-C---	17			7.0.114.148	2046					10.10.88.91 2049	72	
03.12.2024 16:33:47	03.12.2024 16:33:47	tun	800h	<-C---	17			7.0.114.148	2046					7.0.69.251 2046	29	
03.12.2024 16:33:47	03.12.2024 16:33:47	tun	800h	<-C---	17			7.0.114.148	2046					7.0.69.251 2046	29	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	58	fe80::b985:e22d:2315:3fb4	0							ff02::2	0	48
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	0	fe80::b985:e22d:2315:3fb4	0							ff02::16	0	172
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	17			7.0.114.148	2046					7.0.69.251 2046	299	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	17			7.0.114.148	2046					10.10.88.91 2049	72	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	17			7.0.114.148	2046					81.30.192.133 2049	72	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	6	192.168.27.162	48032							81.30.192.133 22281	52	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	6	192.168.27.162	48032							81.30.192.133 22281	197	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	17			7.0.114.148	2046					7.0.69.251 2046	29	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	17			7.0.114.148	2046					7.0.69.251 2046	299	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	6	192.168.27.162	37606							149.154.167.41 443	52	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	6	192.168.27.162	37606							149.154.167.41 443	397	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	6	192.168.27.162	48032							81.30.192.133 22281	64	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	17			7.0.114.148	2046					7.0.69.251 2046	299	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	6			7.0.114.148	35504					7.0.1.26 8088	60	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<-C---	17			7.0.114.148	2046					7.0.69.251 2046	299	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	6	192.168.27.162	48032							81.30.192.133 22281	52	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	6	192.168.27.162	37606							149.154.167.41 443	397	
03.12.2024 16:33:48	03.12.2024 16:33:48	tun	800h	<D-----	0	fe80::b985:e22d:2315:3fb4	0							ff02::16	0	192

Рисунок 9. Просмотр журнала пакетов

- **Статистика трафика** — просмотр информации о переданных и принятых на устройстве IP-пакетах.
- **Тест производительности криптографии** — проверка производительности криптодрайвера ViPNet Client 5 при заданном размере тестового буфера информации. Функция для разработчиков ViPNet Client 5.

Инструменты тестирования

- Симулировать сбой интерфейса приложения. Функция для разработчиков ViPNet Client 5.

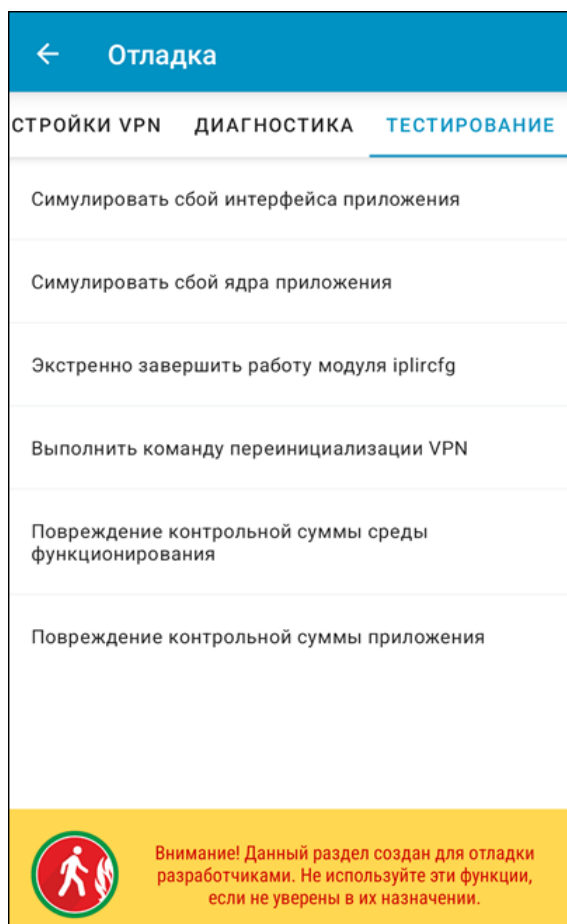


Рисунок 10. Тестирование работы ViPNet Client 5

- Симулировать сбой ядра приложения. Функция для разработчиков ViPNet Client 5.
- Экстренно завершить работу модуля iplircfg. Функция для разработчиков ViPNet Client 5.
- Выполнить команду переинициализации VPN — отправить сообщение type 3 на сервер соединений, чтобы получить статус подключения к защищённой сети.
- Повреждение контрольной суммы среды функционирования. Функция для разработчиков ViPNet Client 5.
- Повреждение контрольной суммы приложения. Функция для разработчиков ViPNet Client 5.



Возможные неполадки и способы их устранения

Файл *.vpnconfig не применён

Убедитесь, что конфигурационный файл:

- содержит записи,
- сохранен в кодировке UTF-8 (без BOM),
- не превышает 5 Кбайт.

Не удаётся установить дистрибутив ключей на устройство

Если пользователь ViPNet Client 5 не может установить дистрибутив ключей на устройство, удостоверьтесь:

- что пользователь вводит правильный пароль;
- в организации соблюдаются требования к корпоративной сети;
- в ViPNet Administrator на клиент добавлена роль «VPN Client для мобильных устройств», и для этого клиента настроено подключение через межсетевой экран с динамической трансляцией адресов с направлением трафика через координатор;
- в дистрибутиве ключей содержится действительная лицензия на использование ViPNet Client 5.

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.

Нет доступа к узлам по доменным именам

Если к защищённым или туннелируемым узлам в корпоративной сети не удаётся обратиться по доменным именам, убедитесь, что в ViPNet ЦУС были выполнены следующие действия:

- Если DNS-сервер является защищённым узлом сети ViPNet, на этот узел добавлена [роль](#) «DNS-сервер».
- Если DNS-сервер туннелируется координатором, на этот координатор добавлена роль «DNS-сервер», указан IP-адрес DNS-сервера.

Подробнее о добавлении роли «DNS-сервер» на узлы см. документ «ViPNet Центр управления сетью. Руководство администратора», разделы «Добавление ролей «DNS-Сервер» и «WINS-Сервер»».

- Заданы DNS-зоны, обслуживаемые защищёнными DNS-серверами.

Подробнее о настройке DNS-зон см. документ «ViPNet Центр управления сетью. Руководство администратора», раздел «Настройка списка защищённых DNS-серверов и доменных зон».

Если в ViPNet Client 5 отображается уведомление «Нет подключения к защищённым DNS-серверам», выключите использование частных DNS-серверов в настройках Android.

Увеличился расход заряда батареи устройства

Если на устройстве увеличился расход заряда батареи при работе ViPNet Client 5:

- 1 В программе ViPNet ЦУС проверьте списки защищённых DNS-серверов и корпоративных DNS-зон на избыточность и удалите лишнее. Затем отправьте на устройство обновление справочников и ключей.
- 2 Если в настройках защищённых DNS-серверов включена функция **DNS-серверы поддерживают разрешение имен публичных ресурсов**, то на устройстве в режиме отладки ViPNet Client 5 переключите функцию **Доступ приложений в VPN** в значение **Запрещен всем, кроме исключений** и удалите все лишние приложения из списка исключений.
- 3 Удалите ViPNet Client 5 из списка исключений политик экономии заряда батареи.
- 4 Перезагрузите устройство.



Термины и сокращения

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 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.

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.

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.

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 Prime.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищённых узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Шлюз

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