



ViPNet Client 5 for Windows

Руководство администратора

Версия продукта: 5.5

© АО «ИнфоТеКС», 2025

ФРКЕ.00403-01 32 01

Версия продукта 5.5

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

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	11
Протестированные на совместимость внешние устройства.....	12
Комплект поставки.....	13
Связанные документы.....	13
Обратная связь.....	14
 Глава 1. Подготовка к работе	15
Порядок установки.....	16
Установка на компьютере с ViPNet ЦУС.....	17
Установка на компьютере с ViPNet Policy Manager	18
Переход с ViPNet Client 4.5	19
Рекомендации по повышению производительности.....	20
Способы аутентификации в ViPNet Client 5.....	21
Подготовка к работе с внешними устройствами.....	22
Обновление из управляющего ПО	24
 Глава 2. Настройка ViPNet Client 5	27
Блокировка ОС при отключении внешнего устройства.....	28
Обмен межсетевой информацией с доверенными сетями	29
Многофакторная аутентификация.....	30
Назначение многофакторной аутентификации	30
Рекомендации по работе с DNS.....	32
Поиск DNS.....	33
Режимы доступа в ViPNet Client 5.....	35
Совместная работа с ViPNet EPP Агент	36
Способ выбора координатора	38
Координаторы в группе серверов	39

Подключение к узлам напрямую.....	40
Изменение портов для прикладных протоколов	41
Настройка адресации узлов	42
Управление настройками ViPNet Client 5	43
Параметры ViPNet Client 5	44
Секция secured	44
Секция policies	44
Секция dns	45
Секция network.....	45
Секция settings	46
Секция firewall.....	47
Секция logging.....	48
Секция nodes.....	49
Секция features.....	51
Секция updates.....	51
Пример настроек.....	52
Настройки на компьютерах пользователей.....	53
Глава 3. Работа в командной строке	55
Включение видимости туннелируемых узлов по виртуальным IP-адресам	56
Переинициализация внутренних конфигурационных файлов	57
Работа с транспортным модулем.....	58
Просмотр журнала IP-пакетов	59
Регламентный контроль целостности ViPNet Client 5.....	60
Работа с журналом критически важных событий	61
Настройка фильтрации трафика.....	63
Просмотр информации о работе VPN-драйвера	65
Приложение А. Создание файла с сетевыми фильтрами.....	72
Группы объектов	78
Источник и назначение	81
Протокол	84
Расписание	86
Приложение В. Общие и индивидуальные настройки профилей	88
Приложение С. Возможные неполадки и способы их устранения.....	90
Не устанавливается ViPNet Client 5 из файла *.msi.....	90
Не устанавливается дистрибутив ключей	91

Особенности обновления справочников и ключей	91
После обновления на узле с ViPNet ЦУС в сети не принимаются обновления справочников из доверенной сети	92
Защищённая сеть определяется как общедоступная	92
Ошибка установки конфигурационного файла *.vpnconfig	93
Нет соединения с координатором	93
Проблемы после перезапуска клиента	93
Нет соединения в Microsoft Outlook и неправильный статус подключения к сети	94
Медленная загрузка корпоративных ресурсов	94
Корпоративные ресурсы недоступны	95
Нарушена целостность компонентов программы ViPNet Client 5 или связанных системных библиотек	96
Проблемы со справочниками или ключами в ViPNet Деловая почта	97
Приложение D. Термины и сокращения	98



Введение

О документе	7
О программе	8
Обратная связь	14

О документе

Документ поможет администратору сети ViPNet установить и настроить ViPNet Client 5 for Windows (далее — ViPNet Client 5, клиент).

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 только в режиме администратора, выделены красным цветом:
`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]`
- Если можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:
`команда {вариант-1 | вариант-2}`

О программе

ViPNet Client 5 — клиент для работы в защищённой сети. Он защищает трафик на компьютерах с Windows путём шифрования IP-пакетов.

С помощью ViPNet Client 5 ваш компьютер 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 компьютер с ViPNet Client 5 программу ViPNet CSS Connect и ViPNet Деловая почта.

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 Windows	Client for Windows v.5, Universal Client v.5
Роль в ViPNet Administrator	VPN-клиент	-
Транспорт	MFTP	UT
Аутентификация по внешнему устройству	+	-
Совместимость с ViPNet Деловая почта	+	-



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

- Архитектура процессора — x86, x86-64 или ARMv8 x64.
- Количество ядер — 2 и более.
- Объём оперативной памяти — не менее 1 Гбайт для 32-разрядных систем или 2 Гбайт для 64-разрядных систем.
- Свободное место на жёстком диске — не менее 500 Мбайт (рекомендуется 1 Гбайт).
- Операционная система для x86 и x86-64:
 - Windows 10 LTSC 1809 (64-разрядная);
 - Windows 10 LTSC 21H2 (64-разрядная);
 - Windows 11 23H2;
 - Windows 11 24H2;
 - Windows 11 LTSC 24H2;
 - Windows Server 2019;
 - Windows Server 2022;
 - Windows Server 2025.
- Операционная система для ARMv8 x64 — Windows 11 24H2.

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.

Протестированные на совместимость внешние устройства



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

Производитель	Устройство
«Аладдин Р.Д.»	• JaCarta ГОСТ • JaCarta-2 ГОСТ • JaCarta PKI/Flash • JaCarta PKI/ГОСТ • JaCarta-2 PKI/ГОСТ • JaCarta SF/ГОСТ • JaCarta LT • JaCarta Pro
«Актив»	• Рутокен ЭЦП 2.0 (2000, 2100, 3000) • Рутокен ЭЦП 3.0 (3120, 3220) • Рутокена ЭЦП 3.0 NFC (3100) • 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

- Установочный файл в формате EXE или MSI.
- Файлы для централизованного обновления клиентов с ключами *.dst в формате LZH.
- Файлы для централизованного обновления клиентов с ключами *.ds5 в формате ZIP.
- Библиотека для работы через VPN API в формате DLL.
- Документация в формате PDF:
 - Быстрый старт.
 - Руководство пользователя.
 - Руководство администратора.
 - Справочник разработчика.

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

Связанные документы

- ViPNet Сервер многофакторной аутентификации. Руководство администратора.

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

Подготовка к работе

Порядок установки	16
Рекомендации по повышению производительности	20
Способы аутентификации в ViPNet Client 5	21
Подготовка к работе с внешними устройствами	22
Обновление из управляющего ПО	24

Порядок установки

Действие	Ссылка на документ
☐ В управляющем ПО создайте клиенты	• «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 будет отсутствовать связь клиента с защищённой сетью	• «ViPNet Центр управления сетью. Руководство администратора», раздел «Отправка обновлений на сетевые узлы»
☐ Установите ViPNet Client 5 for Windows0	• «ViPNet Client 5 for Windows. Руководство пользователя», раздел «Установка, обновление и удаление»
☐ Для пользователей, которые будут проходить аутентификацию с помощью персонального ключа на внешнем устройстве, подготовьте компьютеры для работы с внешними устройствами	• «ViPNet Client 5 for Windows. Руководство администратора», раздел «Подготовка к работе с внешними устройствами»
☐ В ViPNet Administrator или в ViPNet Prime создайте дистрибутивы ключей и передайте их пользователям доверенным способом (файл *.dst или *.ds5 и пароль. Длина пароля не должна превышать 31 символ). Пользователям, которым хотите назначить многофакторную аутентификацию, добавьте связь с узлом Client Auth Server. Передайте внешние устройства с персональным ключом и PIN-коды к ним пользователям, для которых выбран соответствующий способ аутентификации	• «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Создание дистрибутивов ключей» • «ViPNet Prime. Руководство администратора», раздел «Создание дистрибутивов ключей»
☐ Поручите пользователям установить ключи	• «ViPNet Client 5 for Windows. Руководство пользователя», раздел «Установка ключей»

Установка на компьютере с ViPNet ЦУС

- 1 Установите ViPNet Administrator версии 4.6.11 и выше.

Подробнее см. руководство по установке ViPNet Administrator.

- 2 Установите ViPNet Client 5 без графического интерфейса из файла *.msi одним из способов:

- Выполните:

```
msiexec /q /i <путь до файла *.msi> ADDLOCAL="Applications"
```

- Запустите установочный файл *.msi и следуйте указаниям мастера. На шаге **Custom Setup** для **ViPNet Client UI** выберите **Entire feature will be unavailable**.

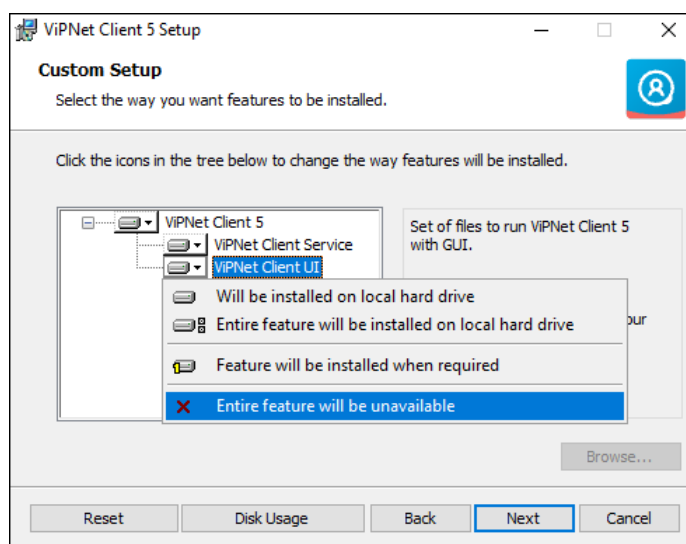


Рисунок 1. Установка ViPNet Client 5 без графического интерфейса

- 3 Установите ключи в формате DST одним из способов:

- Установите новые ключи.

Подробнее см. руководство пользователя, раздел «Работа в командной строке» > «Установка ключей».

- Перенесите ключи из ViPNet Client 4.5.

Подробнее см. руководство пользователя, раздел «Работа в командной строке» > «Переход с ViPNet Client 4.5».

- 4 Перезагрузите компьютер.

Установка на компьютере с ViPNet Policy Manager

1 Установите ViPNet Client 5.

Подробнее см. руководство пользователя.

Если вы хотите установить ViPNet Client 5, ViPNet Policy Manager и ViPNet Центр управления сетью на одном компьютере, [устанавливайте ViPNet Client 5 без графического интерфейса](#).

2 Установите ключи в формате DST с ролью «Policy Manager» одним из способов:

- Установите новые ключи.

Подробнее см. руководство администратора ViPNet Центр управления сетью, раздел «Изменение списка ролей сетевого узла» и руководство пользователя ViPNet Client 5, раздел «Установка ключей».

- Перенесите ключи из ViPNet Client 4.5.

Подробнее см. руководство администратора ViPNet Центр управления сетью, раздел «Изменение списка ролей сетевого узла» и руководство пользователя ViPNet Client 5, раздел «Переход с ViPNet Client 4.5».

3 Установите ViPNet Policy Manager версии 4.5.5 и выше на компьютер с ViPNet Client 5.

Подробнее см. руководство администратора ViPNet Policy Manager, раздел «Установка ViPNet Policy Manager».

4 Если ViPNet Policy Manager устанавливается отдельно от ViPNet Центр управления сетью, установите ViPNet CSP версии 4.4 и выше.

5 Перезагрузите компьютер.



Внимание! Если вы добавили, удалили или переименовали узлы из связей клиента с ролью «Policy Manager», перезапустите Policy Manager. Иначе изменения применятся только в клиенте. Перезапускайте Policy Manager после каждого изменения связей узла.

Переход с ViPNet Client 4.5

Действие	Ссылка
1 На узлах с ViPNet Client 4.5 для пользователя, которого хотите перевести в ViPNet Client 5 for Windows, установите способ аутентификации Пароль или Персональный ключ на устройстве	«ViPNet Client 4. Руководство пользователя», раздел «Изменение способа аутентификации пользователя»
2 В ViPNet Client 5 перенесите ключи из ViPNet Client 4.5 или поручите пользователям сделать это самостоятельно. Чтобы перенести актуальные настройки DNS, переносите ключи с помощью командной строки	«ViPNet Client 5 for Windows. Руководство пользователя», раздел «Переход с ViPNet Client 4.5»
3 В управляющем ПО отправьте на узлы актуальные настройки DNS, если ключи переносились из графического интерфейса	«ViPNet ЦУС 4. Руководство администратора», раздел «Отправка справочников и ключей». «ViPNet Prime. Руководство администратора», раздел «Обновление справочников и ключей вручную»
4 На узлах удалите компонент ViPNet Монитор или поручите пользователям сделать это самостоятельно	«ViPNet Client 4. Руководство пользователя», раздел «Добавление, удаление и восстановление компонентов»
5 Настройте доступ в ViPNet Деловая почта или поручите пользователям сделать это самостоятельно	«ViPNet Client 5 for Windows. Руководство пользователя», раздел «Доступ в ViPNet Деловая почта»



Примечание. ViPNet Client 5 поддерживает два уровня полномочий: минимальные и максимальные. Если в ViPNet Client 4.5 у пользователя были средние или специальные полномочия, в ViPNet Client 5 ему будут назначены максимальные полномочия.

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.

Способы аутентификации в ViPNet Client 5

Способ аутентификации	Описание	Требования
Пароль	однофакторная аутентификация, требуется ввести только пароль	• дистрибутив ключей *.dst или *.ds5; • пароль от дистрибутива ключей
Персональный ключ на внешнем устройстве	двухфакторная аутентификация, требуется подключить к компьютеру внешнее устройство с персональным ключом и ввести PIN-код. При отключении внешнего устройства VPN-соединение автоматически прерывается	• дистрибутив ключей *.dst; • пароль от дистрибутива ключей; • внешнее устройство; • PIN-код к внешнему устройству

Администратор задаёт способ аутентификации и может дополнительно [назначить пользователям многофакторную аутентификацию](#) для доступа к корпоративным ресурсам.

Пользователь может сменить способ аутентификации.

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 процессора x86-64 и x86.

1 Установите драйверы для работы с внешним устройством:

- Для устройств Rutoken.
 - Для устройств JaCarta.
-



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

2 Проверьте, корректно ли установлены драйверы и определяется ли внешнее устройство при подключении к компьютеру. Это можно сделать с помощью ПО производителя.

3 В ViPNet УКЦ:

3.1 Включите **Выбор способа аутентификации в мастере выдачи дистрибутива ключей**.

3.2 Создайте **дистрибутивы ключей**. Выберите способ аутентификации **Устройство (персональный ключ)** и задайте PIN-код для внешнего устройства.

Если для аутентификации пользователя в ViPNet Client 5 используется внешнее устройство JaCarta PRO производителя «Аладдин Р.Д.»:

3.2.1 Отформатируйте внешнее устройство. Для этого используйте Единый Клиент JaCarta.

3.2.2 Создайте дистрибутивы ключей. Если появится окно **ViPNet CSP — инициализация контейнера ключей**, задайте имя контейнера **cur_pers**, выберите устройство JaCarta PRO и введите PIN-код от него.

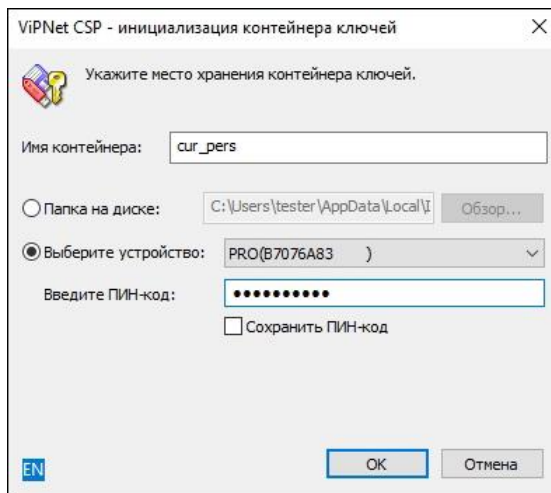


Рисунок 2. Окно «ViPNet CSP — инициализация контейнера ключей»

3.3 Передайте пользователям:

- дистрибутив ключей (*.dst);
- пароль от дистрибутива ключей;
- внешнее устройство с персональным ключом и PIN-код к нему.

Подробнее см. «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Обновление из управляющего ПО

Администратор 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.

Обновление клиентов с ключами *.dst

Вы можете обновить ViPNet Client 5 с ключами *.dst из ViPNet Administrator и из ViPNet Prime. Для этого используйте LZH-архив.

Обновление клиентов с ключами *.ds5

Вы можете обновить ViPNet Client 5 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 компьютере пользователя](#).

При обновлении клиентов с ключами *.ds5 выполняется [переинициализация внутренних конфигурационных файлов](#) на основе актуальных справочников. Из-за этого могут измениться виртуальные IP-адреса узлов и устареть настройки клиента, которые используют эти адреса. Проверьте корректность таких настроек после обновления.

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:

```
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)
```

2

Настройка ViPNet Client 5

Блокировка ОС при отключении внешнего устройства	28
Обмен межсетевой информацией с доверенными сетями	29
Многофакторная аутентификация	30
Рекомендации по работе с DNS	32
Режимы доступа в ViPNet Client 5	35
Совместная работа с ViPNet EPP Агент	36
Способ выбора координатора	38
Координаторы в группе серверов	39
Подключение к узлам напрямую	40
Изменение портов для прикладных протоколов	41
Настройка адресации узлов	42
Управление настройками ViPNet Client 5	43

Блокировка ОС при отключении внешнего устройства

Вы сможете настроить автоматическую блокировку Windows при отключении внешнего устройства, если соблюдаются все условия:

- в сети используется Active Directory,
- пользователи авторизуются в Windows с помощью сертификатов типа **Пользователь со смарт-картой** или **Вход со смарт-картой**.



Примечание. В этом разделе описаны действия на примере Windows Server 2019, в других ОС названия элементов интерфейса могут отличаться.

- 1 На контроллере домена откройте **Панель управления > Система и безопасность > Администрирование > Управление групповой политикой > Объекты групповой политики**.
- 2 Щёлкните правой кнопкой мыши объект **Default Domain Policy** и выберите **Изменить**.
- 3 В окне **Редактор управления групповыми политиками** выберите **Конфигурация Windows > Параметры безопасности > Локальные политики > Параметры безопасности**.
- 4 Щёлкните правой кнопкой мыши политику **Интерактивный вход в систему: поведение при извлечении смарт-карты** и выберите **Свойства**.
- 5 Выберите **Определить следующий параметр политики**.
- 6 В списке выберите **Блокировка рабочей станции**.
- 7 Нажмите **ОК**.

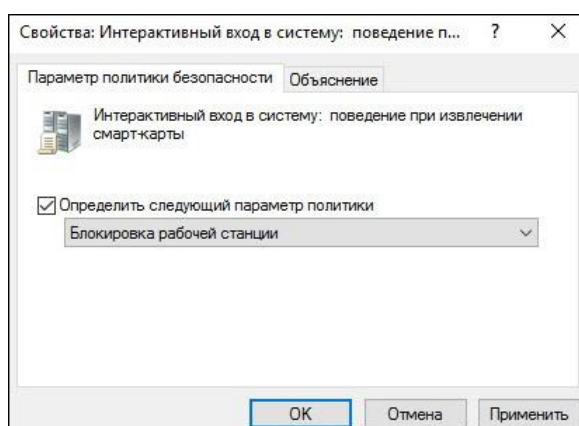


Рисунок 3. Блокировка рабочей станции

- 8 Перезагрузите сервер.
- 9 Если клиентские компьютеры были загружены во время настройки сервера, перезагрузите их.
- 10 На клиентских компьютерах установите автоматический запуск службы **Политика удаления смарт-карт/Smart Card Removal Policy**.

Обмен межсетевой информацией с доверенными сетями

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



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. 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».

Рекомендации по работе с DNS

Чтобы удалённые пользователи могли безопасно подключаться к ресурсам корпоративной сети:

- 1 Выделите отдельные **DNS-серверы** для ресурсов корпоративной сети и отдельные DNS-серверы для обработки доменных имён ресурсов открытой сети.
- 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 параметре **trustedServers** в расширенных настройках 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.

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



Внимание! Если на DNS-сервере разрешены только безопасные динамические обновления, то на координаторе, туннелирующем DNS-сервер, **настройте видимость клиентов по реальным IP-адресам**. Иначе обновления записей на DNS-сервере не будут считаться безопасными и клиенты не зарегистрируются на туннелируемом DNS-сервере.

Для примера рассмотрим схему сети, в которой корпоративный DNS-сервер туннелируется координатором, при этом:

- есть узлы без ViPNet Client 5, которые находятся в туннеле;
- есть узлы с ViPNet Client 5, которые подключаются к корпоративной сети через интернет;
- с внутренних туннелируемых узлов (1) надо обращаться к узлам с ViPNet Client 5 в интернете (2) по доменным именам.

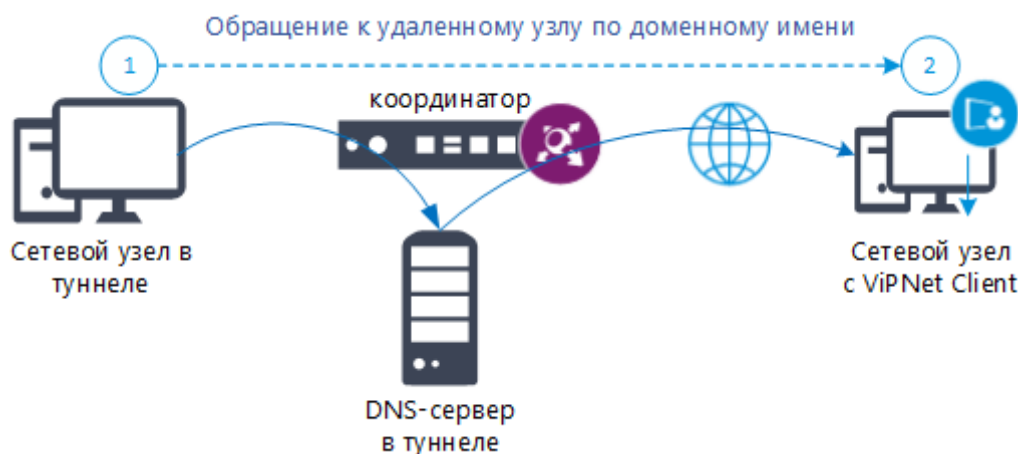


Рисунок 4. Схема расположения сетевых узлов и DNS-сервера

Чтобы в этой схеме доменные имена разрешались правильно:

- На DNS-сервере настройте поддержку динамического изменения DNS-записей. Обычно DNS-серверы не поддерживают эту настройку по умолчанию.
- Для клиентов, к которым будут обращаться по доменному имени:
 - в управляющем ПО задайте корпоративный DNS-сервер;
 - проверьте, чтобы на клиентах была настроена автоматическая регистрация на DNS-сервере.
- На всех туннелирующих координаторах, участвующих в схеме, включите обработку прикладного протокола DNS.

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.

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
```

Примечание. Обращайтесь к узлам защищённой сети по служебным адресам ViPNet:

- <идентификатор узла>.vipnet — для обращения к узлам. Например, 2DBF001D.vipnet.
- <IP-адрес туннеля>.<идентификатор туннелирующего координатора>.vipnet — для обращения к ресурсам, туннелируемым координатором. Например, 10.0.2.26.2DBF000A.vipnet.



Это самый надёжный способ обращения к узлам, потому что служебный адрес ViPNet не изменяется, а IP-адрес и доменное имя могут меняться.

Режимы доступа в ViPNet Client 5

В ViPNet Client 5 вы можете настроить режим доступа, если на компьютере работают несколько пользователей. По умолчанию включён режим общего доступа: управлять ViPNet Client 5 может только один пользователь Windows. Если он включил VPN-соединение, остальные пользователи смогут работать в защищённой сети, но не смогут выключить VPN-соединение или изменить настройки ViPNet Client 5. В режиме раздельного доступа управлять ViPNet Client 5 могут все пользователи.

Общий доступ

- Только один пользователь Windows может управлять ViPNet Client 5.
Управляет ViPNet Client 5 тот пользователь, у которого установлены ключи и включено VPN-соединение. Если этот пользователь выключит VPN-соединение, управлять ViPNet Client 5 сможет другой пользователь, у которого установлены ключи.
- Только пользователь, который управляет ViPNet Client 5, может работать с ViPNet CSS Connect.
- Другие пользователи могут работать в защищённой сети, но не могут выключить VPN-соединение.
- Другим пользователям недоступны разделы ViPNet Client 5:
 - Настройки,
 - Сетевые узлы,
 - Профиль.
- Все пользователи могут создать отчёт об ошибке, но в него сохраняются данные о работе пользователя, который управляет ViPNet Client 5.
- Настройки из управляющего ПО применяются для всех пользователей.

Раздельный доступ

- Все пользователи Windows могут:
 - установить ключи,
 - управлять ViPNet Client 5.
- При выходе пользователя из учётной записи выключается VPN.
- Включение VPN до авторизации пользователя в ОС доступно только для пользователя, который последним вышел из учётной записи.

Например, компьютер используют два пользователя. Сначала первый пользователь вышел из своей учётной записи, а затем второй пользователь вышел из своей учётной записи. Тогда включение VPN до авторизации пользователя в ОС будет доступно только второму пользователю.

Совместная работа с ViPNet EPP Агент

О ViPNet EPP

Чтобы повысить безопасность сети, используйте ViPNet EndPoint Protection версии 1.8.0 (далее — ViPNet EPP). Это программный комплекс для защиты персональных компьютеров пользователей и корпоративных серверов организаций от угроз безопасности информации. Он идентифицирует события информационной безопасности и реагирует на угрозы на основе анализа событий.

ViPNet EPP включает клиентский компонент ViPNet EPP Агент и серверный компонент ViPNet EPP Сервер. Подробнее см. документацию ViPNet EPP.

Защита компьютеров пользователей

Вы можете настроить блокировку пользовательского трафика на узле до тех пор, пока не будут выполнены проверки безопасности ViPNet EPP Агент:

- 1 Установите на компьютеры пользователей ViPNet EPP Агент.

Подробнее см. руководство администратора ViPNet EPP, раздел «Установка ViPNet EPP Агент».

- 2 В ViPNet EPP Сервер включите и настройте политику ZTNA.

Подробнее см. руководство администратора ViPNet EPP, раздел «Управление политиками ZTNA»

- 3 В ViPNet Prime включите для узлов **Блокировка VPN без ViPNet EPP**.

Подробнее см. руководство администратора ViPNet Prime, раздел «Блокировка VPN без ViPNet EPP».

После этого на компьютерах будут доступны корпоративные ресурсы, только когда:

- установлен и запущен ViPNet EPP Агент;
- в ViPNet EPP Агент включена политика ZTNA;
- выполняется политика ZTNA.

При этом служебный, DNS-трафик и трафик между ViPNet EPP Агент и ViPNet EPP Сервер будут передаваться. Подробнее см. руководство администратора ViPNet EPP, раздел «Сетевой доступ с нулевым доверием (ZTNA)».

Если для узла в ViPNet Prime включена **Блокировка VPN без ViPNet EPP**, но на компьютере не установлен ViPNet EPP Агент или не выполняется политика ZTNA, в ViPNet Client 5 заблокируется пользовательский трафик и отобразится уведомление об этом. Чтобы разблокировать пользовательский трафик, потребуется:

- установить ViPNet EPP Агент;
- включить политику ZTNA;
- выполнить рекомендации ViPNet EPP Агент по выполнению политики ZTNA.

Подробнее см. руководство пользователя ViPNet EPP, раздел «Просмотр статуса выполнения политики ZTNA».

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 компьютерах пользователей автоматически. Подробнее см. руководство 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 виде [расширенных настроек](#) параметра `applicationLevelGateway` [секции firewall](#).
 - В виде настроек в секции `[ALG]` [в конфигурационном файле](#), который нужно применить на компьютере.



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

Настройка адресации узлов

По умолчанию в защищённой сети используются [виртуальные IP-адреса](#) из диапазона 7.0.x.x. Если узлы из доверенных сетей имеют одинаковый внутрисетевой ViPNet-идентификатор узла, при межсетевом взаимодействии может возникнуть совпадение IP-адресов. Чтобы этого избежать, назначьте узлам с ViPNet Client 5 адреса из нового диапазона одним из способов:

- В виде [расширенных настроек](#) параметра `privateSubnet` [секции network](#).
- В виде настроек в секции `[IP_SETTINGS]` [в конфигурационном файле](#), который нужно применить на компьютере.

Внимание!



- Адреса из выбранного диапазона должны быть назначены всем узлам защищённой сети, иначе соединения между узлами по виртуальным адресам будут невозможны.
 - Виртуальный адрес клиента должен отличаться от реального адреса на TUN-интерфейсе.
-

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`.

```
vipnetclient debug --user-vpnconfig <имя_файла>.vpnconfig
```

Или левой кнопкой мыши дважды щёлкните файл и подтвердите загрузку в ViPNet Client 5.

- 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 его блокирует сторонний процесс или не пройдена многофакторная аутентификация или проверка политики ZTNA.

Если в сети используется ViPNet EPP Сервер, который доступен только по сети ViPNet:

- и установлен на узле ViPNet — задайте в параметре идентификатор этого узла;
- туннелируется координатором — идентификатор этого координатора.

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.

Значение в ViPNet Client 5 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 Windows 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 Windows 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 защищенными 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 Windows 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 Windows по умолчанию — 1500.

Секция settings

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

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

- `shareVpn` — [режим доступа в ViPNet Client 5 for Windows](#).
 - `true` — общий доступ. Управлять ViPNet Client 5 for Windows может только один пользователь Windows.
 - `false` — отдельный доступ. Управлять ViPNet Client 5 for Windows могут все пользователи Windows.

Чтобы настроить режим отдельного доступа, `shareVpn` нужно выключать отдельно для каждого пользователя. Иначе пользователь, у которого останется включена настройка `shareVpn`, вернёт ViPNet Client 5 for Windows в режим общего доступа, и остальные пользователи не смогут управлять ViPNet Client 5 for Windows.

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

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

Значение в ViPNet Client 5 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.

- `blockUserTrafficOnSystemLock` — блокировка пользовательского VPN-трафика при блокировке ОС, выходе или смене пользователя, переходе компьютера в спящий режим.
 - `true` — блокировка пользовательского VPN-трафика включена;
Если включить эту настройку в режиме общего доступа, пользователи, которые не управляют ViPNet Client 5, не смогут работать в защищённой сети.
 - `false` — блокировка пользовательского VPN-трафика отключена.

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 for Windows 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.

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 Windows 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.

- o `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.

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

- o `false` — не отправляются служебные сообщения.

Значение в `VipNet Client 5 for Windows` 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 наименование файла обновления.
- `product: vpn-client`.
- `brand: vipnet`.
- `version` — версия обновления в формате `x.x.xxxx`.
- `platform: windows`.
- `arch: x86,x86_64`.
- `edition: [ru, hybrid]`.
- `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.

При обновлении клиентов с ключами `*.ds5` выполняется **переинициализация внутренних конфигурационных файлов** на основе актуальных справочников. Из-за этого могут измениться виртуальные IP-адреса узлов и устареть настройки клиента, которые используют эти адреса. Проверьте корректность таких настроек после обновления.

Пример настроек

```
dns:
  trustedServers:
    - 77.88.8.8
    - 77.88.8.1

network:
  privateSubnet: 10.136.0.0
  tcpMssDecrease: 20

settings:
  authBeforeOsLogon: true
  shareVpn: true

features:
  - name: tunnel_priority
    mode: active_coordinator

firewall:
  blockOpenNetwork: true
  blockUserTrafficOnSystemLock: true
  applicationLevelGateway:
    dns:
      udp:
        - 53
    ftp:
      tcp:
        - 21
    h.323:
      tcp:
        - 1720
      udp:
        - 1719
    sccp:
      tcp:
        - 2000
    sip:
      tcp:
        - 5060
        - 5068
        - 5080
      udp:
        - 5060
        - 5068
        - 5080

logging:
  level: 3

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"
updates:
  - url: "путь к ZIP-архиву с обновлением на HTTP-сервере"
    name: client-windows_x86_64_update_5.5.zip
    product: vpn-client
    brand: vipnet
    version: 5.5.1234
    platform: windows
    arch: x86,x86_64
    edition: [ru, hybrid]
    retry_timeout: 300

```

Настройки на компьютерах пользователей



Примечание. Этот способ отличается от описанного в разделе «[Параметры ViPNet Client 5](#)» только форматированием файла *.vpnconfig.

Некоторые настройки вы можете задать локально, в отдельном конфигурационном файле *.vpnconfig, и применить на компьютерах пользователей:

- Порты для обработки прикладных протоколов.
- Диапазон виртуальных IP-адресов узлов.

Чтобы задать эти настройки:

- 1 Создайте файл <имя_файла>.vpnconfig.

Размер файла должен быть до 1 Мбайта.

- 2 Чтобы изменить порты для обработки прикладных протоколов, создайте в файле секцию [ALG] и задайте в ней значения портов:

```

FTPTCP={<номер_порта> | off}
DNSUDP=<номер_порта>
H323UDP={<номер_порта> | off}
H323TCP={<номер_порта> | off}

```

```
SIPUDP={<номер_порта> | off}  
SCCPTCP={<номер_порта> | off}  
SIPTCP={<номер_порта> | off}
```

Параметры могут принимать следующие значения:

- о <номер_порта> — порт или список портов, разделённых точкой с запятой.
- о off — использование прикладного протокола отключено.

Если в секции [ALG] будут заданы значения не для всех протоколов, то после применения настроек из конфигурационного файла для отсутствующих прикладных протоколов будут использоваться значения по умолчанию.

- 3 Чтобы изменить диапазон виртуальных IP-адресов узлов, создайте секцию [IP_SETTINGS] и задайте в ней параметр SUBNET=X.X.0.0.

В параметре SUBNET первые два октета новых адресов узлов. Вместо вторых двух октетов укажите 0.0, они будут сформированы программой ViPNet Client 5 автоматически на основе идентификатора узла.

- 4 Сохраните файл.
- 5 Передайте файл пользователям и попросите применить настройки на устройстве, см. руководство пользователя, раздел «Применение настроек из файла *.vpnconfig».

Пример конфигурационного файла

```
[ALG]  
FTP_TCP=21  
DNS_UDP=53;5353  
H323_TCP=1720  
SCCP_TCP=2000  
SIP_TCP=5060;5061  
SIP_UDP=off  
[IP_SETTINGS]  
SUBNET=7.0.0.0
```

3

Работа в командной строке



Совет. Чтобы посмотреть список доступных команд для работы в командной строке, выполните:

```
vipnetclient --help
```

Включение видимости туннелируемых узлов по виртуальным IP-адресам	56
Переинициализация внутренних конфигурационных файлов	57
Работа с транспортным модулем	58
Просмотр журнала IP-пакетов	59
Регламентный контроль целостности ViPNet Client 5	60
Работа с журналом критически важных событий	61
Настройка фильтрации трафика	63
Просмотр информации о работе VPN-драйвера	65

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

1 Отключите VPN-соединение.

2 Выполните:

```
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.

3 Включите VPN-соединение.

Переинициализация внутренних конфигурационных файлов

В случае повреждения внутренних конфигурационных файлов клиента при сбое ОС, неудачном обновлении справочников и ключей или других нештатных ситуациях, создайте эти файлы заново на основе последних актуальных справочников:

- 1 Выключите VPN-соединение:

```
vipnetclient stop
```

- 2 Выполните:

```
vipnetclient reconfigure
```



Примечание. Переинициализация не затрагивает `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.

Переинициализация автоматически выполняется при обновлении клиентов с ключами `*.ds5` из управляющего ПО.

Работа с транспортным модулем

По умолчанию [модуль MFTP](#) или [UT](#) из состава ViPNet Client 5 for Windows 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:

```
vipnetclient transport peep
```

- Применить обновления справочников и ключей, в случае, если их не удаётся отправить из управляющего ПО:

```
vipnetclient transport cms <путь к файлу обновления *.ctl или *.bin>
```

Или левой кнопкой мыши дважды щёлкнуть файл *.ctl или *.bin.

Обновление будет применено, если:

- файл содержит обновление справочников или ключей для того узла, на котором применяется;
- дата создания файла позже, чем дата создания обновлений справочников или ключей, применённых в клиенте ранее.

Чтобы просмотреть журнал транспортных конвертов для клиента с ключами *.dst:

```
vipnetclient transport events
```

Чтобы просмотреть информацию о команде:

```
vipnetclient transport --help
```

Просмотр журнала IP-пакетов

Журнал регистрации IP-пакетов содержит информацию обо всех IP-пакетах, передаваемых или получаемых через защищённую сеть. На основе этой информации вы можете анализировать взаимодействие компьютера с клиентом с другими узлами.

Чтобы просмотреть журнал IP-пакетов, выполните:

```
vipnetclient dbviewer
```

В результате в консоли отобразится информация об IP-пакетах, переданных и полученных через защищённую сеть за последние 7 дней (не более 65536 записей).

Регламентный контроль целостности ViPNet Client 5

Контроль целостности ViPNet Client 5 автоматически выполняется:

- при каждом запуске VPN-соединения,
- при каждом запуске службы ViPNet Client Service,
- каждые 8 часов.

Также контроль целостности ViPNet Client 5 выполняется при регламентной проверке по команде пользователя или администратора.

При [нарушении целостности](#) подключение к сети ViPNet невозможно.

Регламентная проверка

При эксплуатации ViPNet Client 5 системному администратору или администратору безопасности рекомендуется выполнять регламентные проверки программы:

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

Во время выполнения регламентных проверок требуется ввести пароль администратора узла. Получите этот пароль у администратора сети ViPNet.

Чтобы провести регламентные проверки:

- 1 Если VPN-соединение выключено, включите его:

```
vipnetclient start
```

- 2 Выполните:

```
vipnetclient info --regulations [--psw <пароль_администратора_узла>]
```

где:

--psw — параметр для указания пароля администратора сетевого 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.

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

Результаты регламентных проверок отобразятся в консоли. В случае [нарушения целостности](#) или при неработоспособности какого-либо из проверяемых компонентов появится информация об этом, и подключение к сети ViPNet будет прервано.

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:

```
vipnetclient start
```

- 2 Выполните:

```
vipnetclient eventlog [--psw <пароль_администратора_сетевого_узла>] [--output  
<каталог_сохранения_файла_журнала>] [--delete <каталог_сохранения_файла_журнала>]
```

где:

- `--psw` — параметр для 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.
- `--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 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.

- 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).

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:

```
vipnetclient {firewall | fw} protected --policy
```

- Режим LOCAL:

```
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:

```
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:

```
vipnetclient {firewall | fw} public --block
```

Чтобы отменить блокировку открытого трафика:

```
vipnetclient {firewall | fw} public --no-block
```

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

```
vipnetclient {firewall | fw} protected --save-user-xml <путь для сохранения файла>
```

5 Чтобы удалить все действующие локальные сетевые фильтры:

```
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:

```
vipnetclient iplirdiag -s firewall --static
```

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

```
vipnetclient {firewall | fw} info
```

Просмотр информации о работе VPN-драйвера



Внимание! В этом разделе представлены функции для разработчиков.

- Информация для диагностики работы адаптеров:

```
vipnetclient iplirdiag -s adapters --info | --stats
```

где:

- --info — информация об адаптерах.

```
C:\Users\vipnetclient>vipnetclient iplirdiag -s adapters --info
Calling the "iplirdiag" with the following parameters: -s adapters --info ... Success

Adapters info rows 1.

adapterNumber: 0
adapterName: tun
firstIpAddress: 7.0.5.189
logOverflow: 0
```

Рисунок 5. Информация об адаптерах

- --stats — статистика подсистемы.

```
C:\Users\vipnetclient>vipnetclient iplirdiag -s adapters --stats
Calling the "iplirdiag" with the following parameters: -s adapters --stats ... Success

Subsystem statistics:
cipher: 0
keySize: 32
timeDifferenceInSecond: 7200
decreaseMSSValue: 0
Block other protocols: 0
filterDisableDriver: 0
filterInitDrop: 0
filterProtectedNetEnable: 1
maxHeadAddInfoSize: 8
maxTailAddInfoSize: 197
maxIpPacketDataSize: 65535
numAdapterContext: 1
ioThreadsCount: 1
```

Рисунок 6. Статистика подсистемы

- Информация о криптографии:

```
vipnetclient iplirdiag -s cipher --info
```

```
C:\Users\vipnetclient>vipnetclient iplirdiag -s cipher --info
Calling the "iplirdiag" with the following parameters: -s cipher --info ... Success

Supported 9 cipher suites:
0
1
2
4
5
6
7
14
132
```

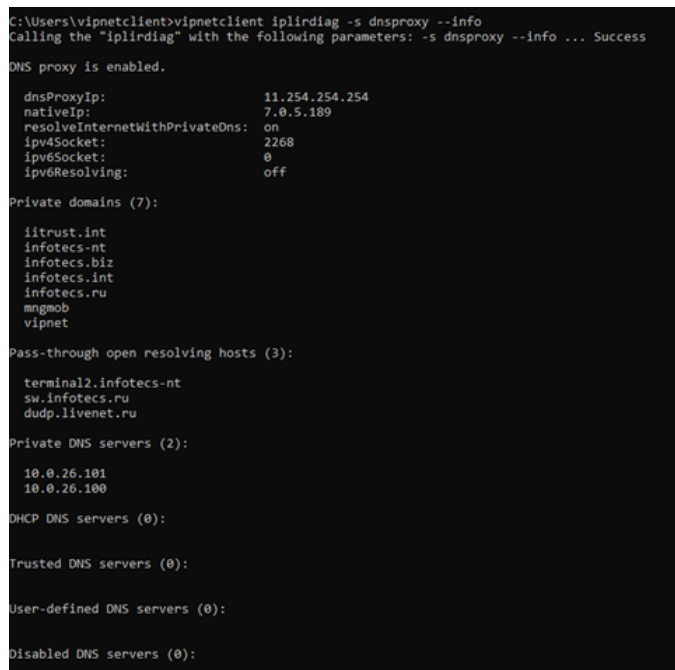
Рисунок 7. Информация о криптографии

- Информация для диагностики работы DNS:

```
vipnetclient iplirdiag -s dnsproxy --info | --query-logging arg {on | off }
```

где:

- `--info` — информация о работе DNS.



```
C:\Users\vipnetclient>vipnetclient iplirdiag -s dnsproxy --info
Calling the "iplirdiag" with the following parameters: -s dnsproxy --info ... Success

DNS proxy is enabled.

dnsProxyIp:          11.254.254.254
nativeIp:            7.0.5.189
resolveInternetWithPrivateDns: on
ipv4Socket:          2268
ipv6Socket:          0
ipv6Resolving:       off

Private domains (7):
iitrust.int
infotecs-nt
infotecs.biz
infotecs.int
infotecs.ru
mngmob
vipnet

Pass-through open resolving hosts (3):
terminal2.infotecs-nt
sw.infotecs.ru
dudp.livenet.ru

Private DNS servers (2):
10.0.26.101
10.0.26.100

DHCP DNS servers (0):

Trusted DNS servers (0):

User-defined DNS servers (0):

Disabled DNS servers (0):
```

Рисунок 8. Информация о работе DNS

- `--query-logging arg {on | off }` — включение или выключение журналирования DNS-запросов. По умолчанию выключено.
- Информация о межсетевом экране:


```
vipnetclient iplirdiag -s firewall --static | --bcast-id
```

 - `--static` — список загруженных правил для фильтрации защищённого трафика.
 - `--bcast-id` — идентификаторы широковещательных запросов.

- Информация о настройке **Группа серверов**:

```
vipnetclient iplirdiag -s groupserver --info
```

```
C:\Windows\system32>vipnetclient iplirdiag -s groupserver --info
Calling the "iplirdiag" with the following parameters: -s groupserver --info ... Success

Connection Server Group

Servers:
Id: 22E10001 P: 1 Time: 0
Id: 22E10010 P: 100 Time: 0
Id: 22E10011 P: 100 Time: 0
Id: 22E1003F P: 100 Time: 0
Id: 22E10040 P: 100 Time: 0
Id: 22E10041 P: 100 Time: 0
Id: 22E10042 P: 100 Time: 0
Id: 22E10079 P: 100 Time: 0
Id: 22E1007E P: 100 Time: 0
Id: 22E1010F P: 100 Time: 0
Id: 22E10E2A P: 100 Time: 0
Id: 22E1128A P: 100 Time: 0
Id: 22E112BC P: 100 Time: 0
Id: 22E112BD P: 100 Time: 0
Id: 22E112BE P: 100 Time: 0
Id: 22E112BF P: 100 Time: 0
Id: 22E112C0 P: 100 Time: 0
Id: 22E112C1 P: 100 Time: 0
Id: 22E112D3 P: 100 Time: 0
Id: 22E11742 P: 100 Time: 0
Id: 22E11766 P: 100 Time: 0
Id: 22E11768 P: 100 Time: 0
Id: 22E117A7 P: 100 Time: 0
Id: 22E117B7 P: 100 Time: 0
Id: 22E11C74 P: 100 Time: 0
Id: 22E11C77 P: 100 Time: 0
Id: 22E11C84 P: 100 Time: 0
Id: 22E1328B P: 100 Time: 0
Id: 22E13299 P: 100 Time: 0
Id: 22E1329A P: 100 Time: 0
Id: 22E13AA3 P: 100 Time: 0
Id: 22E13ACA P: 100 Time: 0
Id: 22E14167 P: 100 Time: 0
Id: 22E1435F P: 100 Time: 0
Id: 22E14589 P: 100 Time: 0
Id: 22E145FB P: 100 Time: 0
Id: 22E14668 P: 100 Time: 0

Starts:
Time: 12:05:00 Type: E1
Time: 12:06:43 Type: G1
IsDgNode: No
active: 22E10001
chosen: null
dgIps: null
eventLife: 5 sec
nextSwitching: <empty>
status: Run
switching: 120 min
waiting: 600 ms
```

Рисунок 9. Информация о настройке **Группа серверов**

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

```
vipnetclient iplirdiag -s groupserver --info --json
```

```
C:\Windows\system32>vipnetclient iplirdiag -s groupserver --info --json
{
  "groupserver": {
    "info": {
      "IsDgNode": "No",
      "active": "22E10001",
      "chosen": "22E10001",
      "dgIps": null,
      "eventLife": "5 sec",
      "latecomer": {
        "Id": "22E10001"
      }
    },
    "nextSwitching": "<empty>",
    "servers": [
      {
        "Id": "22E10001",
        "priority": 1,
        "time": "76 ms"
      },
      {
        "Id": "22E10010",
        "priority": 100,
        "time": "0"
      },
      {
        "Id": "22E10011",
        "priority": 100,
        "time": "0"
      },
      {
        "Id": "22E1003F",
        "priority": 100,
        "time": "0"
      },
      {
        "Id": "22E10040",
        "priority": 100,
        "time": "0"
      },
      {
        "Id": "22E10041",
        "priority": 100,
        "time": "0"
      }
    ]
  }
}
```

Рисунок 10. Информация о настройке **Группа серверов** в формате JSON

Результат выполнения команды:

- 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 1. 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

- o IsDgNode — использование в качестве сервера соединений координатора с адресом шлюза по умолчанию. Значение по умолчанию — No.
- o dgIps — IP-адрес шлюза по умолчанию. Значение по умолчанию — Null.
- o active — идентификатор активного координатора по умолчанию, заданного в управляющем ПО или вручную в ViPNet Client 5.
- o chosen — идентификатор текущего активного координатора из группы серверов.
- o eventLife — время ожидания ответа от координатора, после которого координатор считается недоступным, и запускается настройка **Группа серверов**.
- o latecomer — идентификатор координатора, который первый ответил после запуска настройки **Группа серверов**.
- o nextSwitching — время переключения клиента к координатору с более высоким приоритетом.
- o 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. раздел [«Подключение к узлам напрямую»](#).
- o switching — продолжительность переключения 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:

vipnetclient iplirdiag -s ipsettings --stats | --v-table | --v-tun-table | --node-info arg

- o --stats — статистика подсистемы.

```
C:\Users\vipnetclient>vipnetclient iplirdiag -s ipsettings --stats
Calling the "iplirdiag" with the following parameters: -s ipsettings --stats ... Success

Subsystem statistics:
  nativeId:                270E05BD
  openGateId:              00000000
  coordinatorMode:         0
  packetFormat:            0x401
  numUsedTunnelingIp:      0
  limitativeTunnelingIp:   4294967295
  numNodesRow:             1384
  numVisibilityIp:         2117
  numVisibilityTunnelingIp: 248

Context for adapterNumber '0':
  outsideInterface:        0
```

Рисунок 11. Статистика подсистемы

- o --v-table — список всех связей в формате IP-адрес – ID узла.

```
C:\Users\vipnetclient>vipnetclient iplirdiag -s ipsettings --v-table
Calling the "iplirdiag" with the following parameters: -s ipsettings --v-table ... Success

The visibility table (rows 2148):
Ip address      Node id
7.0.0.10        270E000A
7.0.0.36        270E0024
7.0.0.203       270E00CB
7.0.0.228       270E00E4
7.0.0.237       270E00ED
7.0.1.12        270E010C
```

Рисунок 12. Таблица видимости

- o --v-tun-table — список всех туннелируемых адресов в формате IP-адреса – ID туннелируемого узла.

```
C:\Users\vipnetclient>vipnetclient iplirdiag -s ipsettings --v-tun-table
Calling the "iplirdiag" with the following parameters: -s ipsettings --v-tun-table ... Success

The visibility tunneling table (rows 248):
Begin ip address  End ip address  Node id
1.0.0.2          1.0.0.2        270E00C8
10.0.2.7         10.0.2.7       00010008
10.0.2.26        10.0.2.26      0001027D
10.0.2.244       10.0.2.244     0001027D
10.0.3.2         10.0.3.149     000103A4
10.0.3.200       10.0.3.219     000103A4
```

Рисунок 13. Таблица видимости туннелей

- 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.

- Информация о состоянии модуля политик пользовательского трафика:

```
vipnetclient iplirdiag -s tpm --info
```

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

```
C:\Windows\System32>vipnetclient iplirdiag -s tpm --info
Calling the "iplirdiag" with the following parameters: -s tpm --info ... Success

Traffic Policy Module information

exclusions:
  57100001
  57100002
reasons:
  ztna
restricted: true
```

Рисунок 14. Состояние модуля политик пользовательского трафика

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

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

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

```
C:\Windows\System32>vipnetclient iplirdiag -s updates --info
Calling the "iplirdiag" with the following parameters: -s updates --info ... Success

Updates manager information

error: uncompress
filename: vipnetclient_x86_x86_64_update_5.5.4491.zip
id: 1
info:
  arch: x86,x86_64
  brand: vipnet
  edition:
    hybrid
    ru
  name: vipnetclient_x86_x86_64_update_5.5.4491.zip
  platform: windows
  product: vpn-client
  retry_timeout: 300
  url: http://192.168.43.199:9090/bombova/vipnetclient_x86_x86_64_update_5.5.4491.zip
  version: 5.5.4491
status: fatal_error
error:
filename: vipnetclient_x86_x86_64_update_5.5.4490.zip
id: 2
info:
  arch: x86,x86_64
  brand: vipnet
  edition:
    hybrid
    ru
  name: vipnetclient_x86_x86_64_update_5.5.4490.zip
  platform: windows
  product: vpn-client
  retry_timeout: 300
  url: http://192.168.43.199:9090/bombova/vipnetclient_x86_x86_64_update_5.5.4490.zip
  version: 5.5.4490
status: installed
```

Рисунок 15. 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 ещё 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 файле `*.xml`. 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.
- [Блокировка пользовательского трафика сторонним приложением.](#)
- Контроль целостности программного обеспечения ViPNet Client 5.

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.
- [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.



Возможные неполадки и способы их устранения

Не устанавливается ViPNet Client 5 из файла *.msi

Возможные ошибки:

- Error 0x80070643: Failed to execute MSI package.
- Для установки этого приложения требуется лицензия разработчика для магазина Windows или система с возможностью загрузки неопубликованных приложений.

Способ устранения

- 1 Запустите редактор локальной групповой политики `gpedit.msc`.
- 2 Выберите **Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Развертывание пакета приложения**.
- 3 Включите:
 - Разрешить установку всех доверенных приложений.
 - Разрешить разработку приложений Магазина Windows и их установку из интегрированной среды разработки (IDE).
- 4 Нажмите **Применить**.

Не устанавливается дистрибутив ключей

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 VPN-клиент или в ViPNet Prime выбрана платформа Windows и лицензия Client for Windows (для ключей *.dst), Client for Windows 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.

Особенности обновления справочников и ключей

Обновление справочников и ключей необходимо, если изменилась структура защищённой сети или свойства узлов, а также в случае смены мастер-ключей.

- В ViPNet ЦУС отправьте обновления вручную.
- В ViPNet Prime обновления отправятся автоматически.

Подробнее см. руководство администратора ViPNet ЦУС или ViPNet Prime.

Обновления устанавливаются на устройствах пользователей автоматически. При некоторых изменениях в справочниках и ключах у клиентов могут возникнуть неполадки.

Способы устранения

Условие	Возможные неполадки	Решение
Добавление или удаление туннелей	Пропадает удалённое подключение к компьютеру с ViPNet Client 5	Повторите подключение вручную

После обновления на узле с ViPNet ЦУС 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.

Защищённая сеть определяется как общедоступная

В Windows защищённая сеть может отображаться как общедоступная, даже если домен входит в защищённые DNS-зоны. Это происходит, если категорию сети не получилось определить с первого раза.

Способ устранения

Чтобы категория сети определялась правильно:

- 1 В разделе реестра
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters` **создайте** параметр `DWORD` с именем `AlwaysExpectDomainController`.
- 2 Установите параметру `AlwaysExpectDomainController` значение 1.

Ошибка установки конфигурационного файла *.vpnconfig

- **Ошибка применения настроек протоколов.**

Неверный формат записей в секции [ALG]. Убедитесь, что значения портов для обработки прикладных протоколов указаны в секции [ALG] в соответствии с синтаксисом.

- **Файл *.vpnconfig не применен.**

Убедитесь, что конфигурационный файл был сохранён в кодировке UTF-8 (без BOM) и не превышает 5 Кбайт.

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.

Проблемы после перезапуска клиента

Если после перезагрузки компьютера или перезапуска службы клиента не работают:

- удалённое подключение к компьютеру по протоколу RDP,
- подключение с других узлов, например, по протоколам RDP, SSH, ICMP,
- личные чаты в ViPNet CSS Connect,

это может происходить, если в разделе реестра

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters параметру ArpRetryCount установлено значение 0.

Способ устранения

- 1 В разделе реестра HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters установите параметру ArpRetryCount значение 1.
- 2 Перезагрузите компьютер.

Нет соединения в Microsoft Outlook и неправильный статус подключения к сети

Если на компьютере отображается статус  **Без доступа к интернету** и при этом:

- доступен интернет,
- недоступны программы Microsoft (Outlook, Office365, Skype, OneDrive),

используйте глобальную службу DNS для проверки подключения к сети.

Настройка через редактор локальной групповой политики

- 1 Запустите редактор локальной групповой политики `gpedit.msc`.
- 2 Выберите **Конфигурация компьютера > Административные шаблоны > Сеть > Индикатор состояния сетевого подключения**.
- 3 Включите **Укажите глобальную службу DNS** и выберите **Использовать глобальную службу DNS**.
- 4 Нажмите **Применить**.

Настройка через редактор реестра

- 1 В командной строке от имени администратора выполните:

```
reg add  
"HKEY_LOCAL_MACHINE\SOFTWARE\POLICIES\MICROSOFT\Windows\NetworkConnectivityStatusI  
ndicator" /v UseGlobalDNS /t REG_DWORD /d 1 /f
```

- 2 Перезагрузите компьютер или выполните:

```
gpupdate /force
```

Медленная загрузка корпоративных ресурсов

Если на узле используются незащищённые DNS-серверы, которые доступны по протоколу IPv6, то могут долго загружаться ресурсы защищённой сети.

Способ устранения

- 1 На компьютере пользователя откройте свойства основного сетевого интерфейса.
- 2 Отключите компонент **IP версии 6 (TCP/IPv6)**.

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:

```
vipnetclient info
```

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

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

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.

Если нарушена целостность справочников:

- 1 Удалите ключи.
- 2 Установите новые ключи.

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

- 1 Удалите ViPNet Client 5.
- 2 Установите ViPNet Client 5.
- 3 Установите новые ключи.

Проблемы со справочниками или ключами в ViPNet Деловая почта

Если в ViPNet Деловая почта возникают ошибки, связанные со справочниками или ключами, и при этом в ViPNet Client 5:

- установлены ключи,
- предоставлен доступ к ключам для ViPNet Деловая почта,

проблема может быть во внутренних конфигурационных файлах. Они могут повредиться при сбое ОС, неудачном обновлении справочников и ключей и других нештатных ситуациях.

Способ устранения

Создайте внутренние конфигурационные файлы заново на основе последних актуальных справочников:

- 1 Выключите VPN-соединение:

```
vipnetclient stop
```

- 2 Выполните:

```
vipnetclient reconfigure --bm
```



Термины и сокращения

DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса DNS- и WINS-серверов.

DNS-сервер

Хранит информацию о соответствии доменных имён интернет-узлов их IP-адресам и предоставляет эту информацию по запросам.

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.

Аутентификация

Процесс односторонней или двусторонней (взаимной) проверки подлинности между клиентом (пользователем) и системой (сервером), например, с использованием учётных данных или сертификатов ключей проверки электронной подписи.

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удалённых узлов в приложениях ViPNet.

Дистрибутив ключей

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.

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.

Сетевой узел ViPNet

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

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами сети ViPNet.

Транспортный сервер UT

Серверная часть транспортного компонента UT ViPNet Prime. Обеспечивает передачу транспортных сообщений по протоколу HTTP от ViPNet Prime к транспортному клиенту UT устройств сети ViPNet, поддерживающих работу с дистрибутивом ключей *.ds5.