



ViPNet Client 5 для ОС Аврора

Руководство администратора

Версия продукта: 5.1.0

© АО «ИнфоТеКС», 2025

ФРКЕ.00441-01 32 01

Версия продукта 5.1.0

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

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

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

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

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.....	4
О документе.....	4
Соглашения документа.....	4
О программе	4
Различия форматов ключей.....	5
Рекомендации по безопасности	5
Системные требования	7
Требования к корпоративной сети	7
Протестированные на совместимость устройства	7
Комплект поставки	7
Обратная связь.....	8
 Установка, обновление и удаление	9
Установка	9
Установка ключей	10
Обновление ключей	10
Удаление.....	11
 Администрирование	11
Рекомендации по работе с DNS	11
Рекомендации по защите мобильного устройства.....	12
Настройка протокола mDNS	13
Расширенные настройки	14
Использование нескольких VPN-соединений.....	15
Настройка пользовательских маршрутов трафика	16
Выключение режима шлюзового координатора	17
Работа с журналом критически важных событий	17
Способ выбора координатора	19
Координаторы в группе серверов	20
Управление настройками ViPNet Client 5	21
Параметры ViPNet Client 5	21
Пример настроек.....	25
 Термины и сокращения	27

Введение

О документе

В документе содержится информация о назначении, установке и администрировании программы ViPNet Client 5 для ОС Аврора (далее — ViPNet Client 5).

Документ предназначен для администраторов сети ViPNet, которые устанавливают ViPNet Client 5 на устройства с операционной системой Аврора.

Соглашения документа

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



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

О программе

ViPNet Client 5 защищает IP-трафик на устройствах с ОС Аврора путём шифрования IP-пакетов.

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

Приложение ViPNet Client 5 устанавливает администратор с помощью установочного файла, Аврора Маркет или RuStore.

В процессе установки приложение ViPNet Client 5 для ОС Аврора встраивается в текущую прошивку устройства в качестве набора дополнительных плагинов, ОС при этом не затрагивается.

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 1.9.8 и выше	Client for Aurora	Client for Aurora v.5 Universal Client v.5
Лицензия в ViPNet Prime 1.9.5-1.9.7	Client for Android	Client for Aurora v.5 Universal Client v.5
Лицензия в ViPNet Prime версии ниже 1.9.5	Client for Android	Client for Android v.5
Транспорт	MFTP	UT

Рекомендации по безопасности

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

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

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

Просмотр информации о подозрительных конвертах

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

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

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

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

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

- журнале транспортных конвертов.

Чтобы просмотреть журнал:

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

В ViPNet Client for Windows на узле с ViPNet ЦУС:

- В ViPNet Client > Приложения > ViPNet Транспортный модуль.

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

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

По умолчанию подозрительные конверты помещаются в папку `invalid`:

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

Очищайте папку `invalid` вручную.

Системные требования

ОС Аврора 5.1.5 «Петропавловск-Камчатский» RC 5 (номер сборки: 5.1.5.105).

Расширение списка ОС возможно с помощью привлечения экспертной организации.

Требования к корпоративной сети

- [ViPNet Administrator](#) версии 4.6.11 и выше.
- [ViPNet Prime](#) версии 1.7.2 и выше.

Протестированные на совместимость устройства

Архитектура процессора ARMv7 x32:

- FPLUS T1100,
- БайтЭрг MBK-T2101,
- Масштаб TrustPhone T1,
- Aquarius NS M21,
- FPLUS R570E.

Архитектура процессора ARMv8 x64:

- KVADRA_T.
- Масштаб TrustPhone T1.

Комплект поставки

- Установочный файл в формате RPM.
- Документация в формате PDF:
 - Руководство пользователя.
 - Руководство администратора.

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

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Telegram-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](#).

Установка, обновление и удаление

Установка



Внимание! Если на устройстве уже установлен ViPNet Client другой версии, сначала [удалите его](#). Иначе ViPNet Client 5 не установится.

Способы установки

- [Аврора Маркет](#).
 - RuStore.
 - Установочный файл *.rpm.
Передайте установочный файл на устройство. Нажмите на него и выберите **Установить**.
 - По протоколу SSH на устройства с включённым режимом разработчика.
 - С помощью ПО «Аврора Центр» на устройства с выключенным режимом разработчика.
- Подробнее см. в [документации ОС Аврора](#).

Установка по протоколу SSH

Для установки ViPNet Client 5 вам понадобятся:

- Устройство с ОС Аврора с включённым режимом разработчика.
- Компьютер для подключения по протоколу SSH.
- Не менее 5 Гбайт свободного места на жёстком диске компьютера.
- Кабель Type-C.

Порядок установки:

- 1 Передайте на устройство установочный файл.
- 2 Подключитесь к устройству с компьютера по протоколу SSH. Для подключения используйте имя, IP-адрес и пароль, заданные при настройке режима разработчика устройства (**Настройки > Средства разработчика**). Например, `ssh defaultuser@192.168.2.1`
- 3 Чтобы установить ViPNet Client 5, получите права суперпользователя:

```
$ devel-su
```

4 Выполните:

```
# gdbus call -y -d ru.omp.APM -o /ru/omp/APM -m ru.omp.APM.Install  
/home/defaultuser/Downloads/ru.infotecs.ViPNetClient-X.X.X-XXXX.ARCH.rpm "{}"
```

5 Перезагрузите устройство.



Примечание. При возникновении проблем с установкой [обратитесь в ИнфоТеКС](#).

Установка ключей

В управляющем ПО создайте дистрибутивы ключей и передайте их пользователям доверенным способом.

В ViPNet Administrator:

- 1 Назначьте узлу с ключами *.dst роль «VPN-клиент для мобильных устройств».
- 2 Отправьте обновление справочников и ключей с информацией о новом клиенте на координатор, за которым будет зарегистрирован клиент. Иначе будет отсутствовать связь клиента с защищённой сетью.

В ViPNet Prime назначьте узлу лицензию [в зависимости от формата ключей](#).

Поручите пользователям установить ключи, см. руководство пользователя, раздел «Установка ключей».

Обновление ключей

При смене в сети мастер-ключа ключей обмена:

- 1 Для узлов с ключами *.ds5 создайте новые дистрибутивы ключей.
- 2 Передайте их пользователям.
- 3 Поручите пользователям установить ключи, см. руководство пользователя, раздел «Установка ключей».

Удаление

- 1 Удалите ключи, см. руководство пользователя, раздел «Удаление ключей».
- 2 Выполните одно из действий:
 - Откройте на устройстве приложение Terminal.
 - Подключите устройство к USB-разъёму компьютера. Подключитесь к устройству по протоколу SSH с использованием имени учётной записи `defaultuser` и IP-адреса и пароля, заданных ранее.

- 3 Удалите ViPNet Client 5 для ОС Аврора, получите права суперпользователя:

```
$ devel-su
```

- 4 Выполните:

```
# gdbus call -y -d ru.omp.APM -o /ru/omp/APM -m ru.omp.APM.Remove  
ru.infotecs.ViPNetClient {}
```

Администрирование

Рекомендации по работе с DNS

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

- В корпоративной сети выделите отдельные DNS-серверы для обработки защищённого трафика и трафика открытой сети.
- В ViPNet ЦУС добавьте DNS-серверы для защищённого трафика в список защищённых DNS-серверов и укажите их в настройках узла ViPNet Client 5, см. руководство администратора ViPNet ЦУС, раздел «Настройка защищённых DNS-серверов».
- В ViPNet Prime добавьте DNS-серверы для отправки запросов на разрешение доменных имён на защищённых DNS-серверах в профили DNS, см. руководство администратора ViPNet Prime, раздел «Создание профилей DNS».

Рекомендации по защите мобильного устройства

Недостаточная защита мобильного устройства, которое используется для доступа в корпоративную сеть, ставит под угрозу не только личные данные пользователя этого устройства, но и коммерческие сведения всей компании.

Чтобы защитить данные, хранящиеся на устройстве с ViPNet Client 5, и параметры доступа в корпоративную сеть:

- Задайте пароль для подключения к устройству по протоколу SSH. Используйте надёжный пароль, состоящий более чем из шести символов, строчных и заглавных букв, цифр и знаков подчёркивания.
- Отключите режим разработчика после установки или обновления ViPNet Client 5.
- Не устанавливайте на устройство программное обеспечение из неизвестных источников и отключите возможность установки программного обеспечения из неизвестных источников.

Настройка протокола mDNS

С помощью протокола MulticastDNS вы можете искать узлы ViPNet в локальной сети и взаимодействовать с ними напрямую без участия координатора. Функция экспериментальная. Чтобы её включить:

- 1 [Перейдите в расширенные настройки.](#)
- 2 Нажмите **Настройки протокола mDNS**.
- 3 Нажмите **Использовать протокол mDNS**.
- 4 Чтобы записывать события mDNS в журнал, включите **Журналировать работу mDNS**.

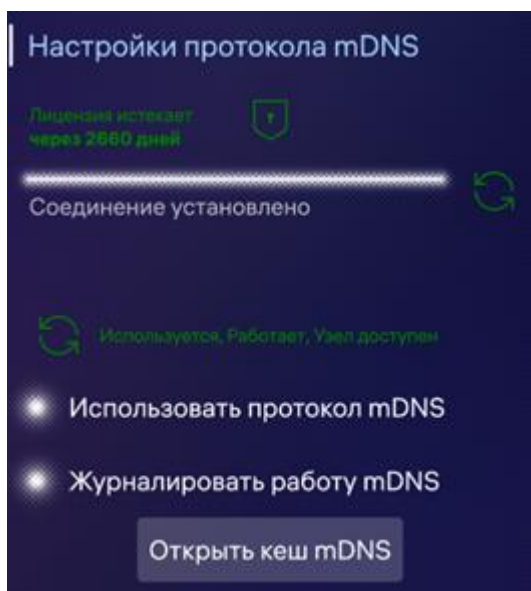


Рисунок 1. Настройки протокола mDNS

Статусы работы протокола mDNS

- **Используется/Не используется** — включено ли использование протокола mDNS в настройках.
- **Работает/Не работает** — работает ли поиск узлов в локальной сети.
- **Узел доступен/Узел недоступен** — доступен ли ваш узел другим узлам для взаимодействия по протоколу mDNS.

Просмотр кеша mDNS

- 1 [Перейдите в расширенные настройки.](#)
- 2 Нажмите **Настройки протокола mDNS**.
- 3 Нажмите **Открыть кеш mDNS**.

Расширенные настройки

- 1 В настройках устройства в разделе **Управление соединениями** выберите **VPN**.
- 2 Нажмите и удерживайте имя VPN.
- 3 В появившемся меню выберите **Редактировать**.
- 4 На экране **Изменить настройки VPN** нажмите **Расширенные настройки**.

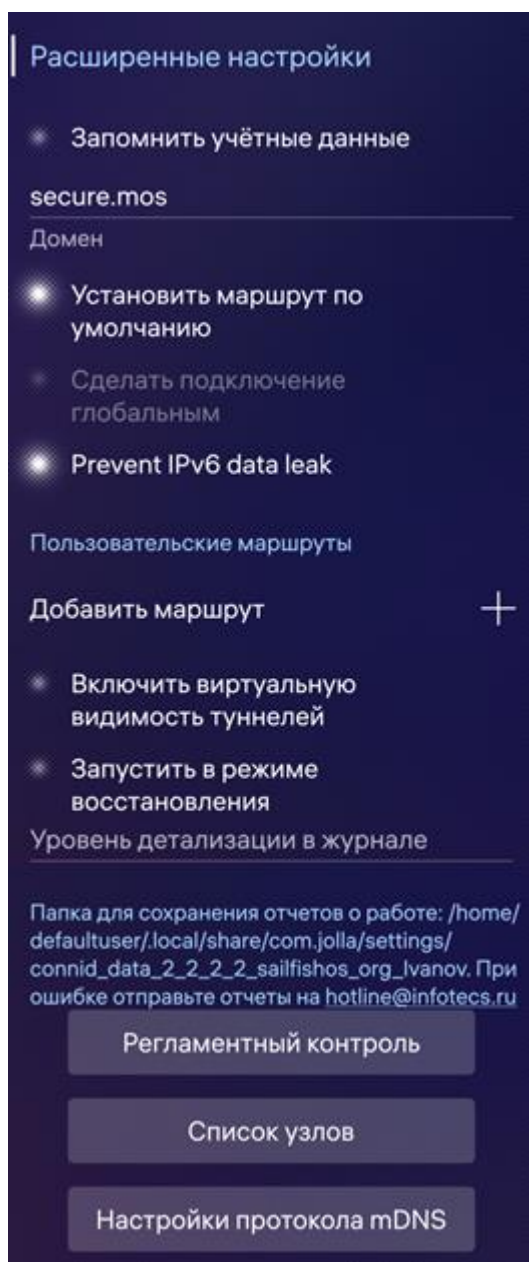


Рисунок 2. Расширенные настройки ViPNet Client 5

Использование нескольких VPN-соединений



Внимание! Настраивать эту функцию рекомендуется только опытным администраторам.

Вы можете добавить на устройство с ViPNet Client 5 сразу несколько VPN-соединений и переключаться между ними в процессе работы. Это может потребоваться, например, когда одно устройство используют несколько человек с различным уровнем полномочий, чтобы создать для них отдельные VPN-соединения с разными связями и доступными ресурсами.

Чтобы использовать несколько VPN-соединений, установите все дистрибутивы ключей.

Чтобы VPN-соединением могли пользоваться другие пользователи устройства, установите ключи под учётной записью администратора устройства.

Чтобы переключить VPN-соединение:

- 1 Отключите текущее VPN-соединение.
 - 2 Включите нужное VPN-соединение.
-



Примечание. Вы можете переключаться между VPN-соединениями без отключения текущего соединения, но возможны задержки в подключении.

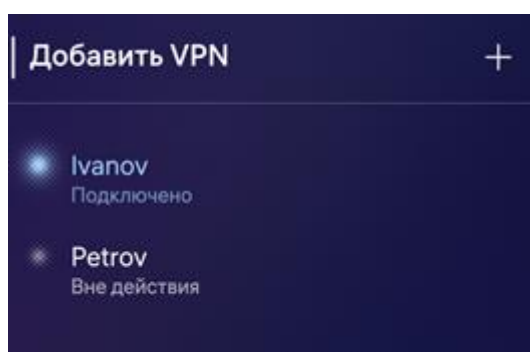


Рисунок 3. Переключение между VPN-соединениями

Настройка пользовательских маршрутов трафика



Внимание! Настраивать эту функцию рекомендуется только опытным администраторам.

Чтобы указать дополнительные сетевые маршруты для передачи IP-трафика через VPN-соединение:

- 1 [Перейдите в расширенные настройки.](#)
- 2 Нажмите **Добавить маршрут**.
- 3 Укажите IP-адрес назначения, [маску подсети](#) и [шлюз](#) по умолчанию.
- 4 Сохраните изменения.

Рисунок 4. Добавление пользовательского маршрута трафика

- 5 Вернитесь на предыдущий экран.
- 6 Нажмите **Подтвердить**.
- 7 Перезапустите VPN-соединение.

Выключение режима шлюзового координатора



Внимание! Настраивать эту функцию рекомендуется только опытным администраторам.

После установки ключей в ViPNet Client 5 автоматически включается режим шлюзового координатора. В этом режиме пользователь может подключаться только к корпоративным ресурсам.

Чтобы выключить режим шлюзового координатора:

- 1 [Перейдите в расширенные настройки.](#)
- 2 Выключите **Установить маршрут по умолчанию.**
- 3 Вернитесь на предыдущий экран.
- 4 Нажмите **Подтвердить.**
- 5 Перезапустите VPN-соединение.

Работа с журналом критически важных событий

ViPNet Client 5 записывает в системный журнал ОС Аврора информацию о критически важных событиях:

- об удалении ключей,
- смене пароля,
- результате ввода пароля,
- результате проверки криптографических функций,
- результате проверки целостности ViPNet Client 5.

Ограничение доступа пользователя

В целях безопасности запретите пользователю сохранять журнал администратора.

- 1 На устройстве войдите в учётную запись администратора: **Настройки > Пользователи > Администратор устройства.**
- 2 Откройте **Настройки > Политики безопасности.**
- 3 Заблокируйте  **Экспорт пользовательских отчетов.**

Пользователи смогут просмотреть журнал, но не смогут сохранить его на устройство.

Просмотр и экспорт журнала

Убедитесь, что вы используете учётную запись администратора устройства. При разблокировке устройства на странице ввода пароля должно быть написано **Владелец устройства**. В настройках устройства в разделе **Пользователи** под названием вашей учётной записи — **Администратор устройства**.

В графическом интерфейсе:

- 1 На устройстве откройте **Журнал**.
- 2 Нажмите  > **Экспортировать системный отчет**.
- 3 Выберите папку, в которую нужно сохранить архив с журналом.
- 4 Нажмите **Экспорт**.

Архив *.tar.bz2 будет сохранён в выбранную папку.

В командной строке:

- 1 Подключитесь к устройству с компьютера по протоколу SSH. Для подключения используйте имя, IP-адрес и пароль, заданные при настройке режима разработчика устройства (**Настройки** > **Средства разработчика**). Например, `ssh defaultuser@192.168.2.1`

- 2 Чтобы открыть системный журнал:

```
# journalctl -a
```

Чтобы сохранить файл с журналом:

```
# journalctl -a > log.txt
```

Файл *.txt будет сохранён в домашнюю папку пользователя. Например, в `/home/defaultuser`.

Настройка журнала

- 1 Подключитесь к устройству с компьютера по протоколу SSH. Для подключения используйте имя, IP-адрес и пароль, заданные при настройке режима разработчика устройства (**Настройки** > **Средства разработчика**). Например, `ssh defaultuser@192.168.2.1`

- 2 Откройте конфигурационный файл:

```
# vi /etc/systemd/journald.conf
```

- 3 Настройте место хранения и максимальный размер журнала.:

- o **Storage** — место хранения журнала.

По умолчанию: `volatile`, журнал хранится в оперативной памяти и очищается при перезагрузке устройства. Чтобы журнал сохранялся в постоянной памяти устройства, задайте значение `persistent`.

- o **SystemMaxUse** — максимальный размер журнала при хранении в постоянной памяти в `/var/log/journal`.

По умолчанию: 50 Мбайт.

- `RuntimeMaxUse` — максимальный размер журнала при хранении в оперативной памяти в `/run/log/journal`.

По умолчанию: 1 Мбайт.

- 4 Перезагрузите устройство, чтобы сохранить изменения.

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 управляющем ПО в расширенных настройках [задайте параметры в секции features](#):

`features:`

```
- name: tunnel_priority
  mode: active_server
```

Координаторы в группе 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.

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.

Управление настройками ViPNet Client 5

Вы можете задать настройки ViPNet Client 5 для ОС Аврора централизованно в управляющем 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.

Укажите параметры в формате YAML в управляющем ПО в расширенных настройках клиентов с ViPNet Client 5. Настройки передаются в ViPNet Client 5 в составе справочников. Подробнее см. руководство администратора управляющего ПО.

Параметры ViPNet Client 5

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

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

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

Значение в ViPNet Client 5 по умолчанию — `150`.

Секция settings

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

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

Этот параметр можно задать только из управляющего ПО.

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

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

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

Этот параметр можно задать только из управляющего ПО.

Секция 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 firewall

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

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

Значение в ViPNet Client 5 по умолчанию:

```
dns:
  udp:
    - 53
ftp:
  tcp:
```

```

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

```



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

Секция nodes

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.

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"
```

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.
 - o `mode: min_id` — выбирается координатор с меньшим идентификатором узла.
 - o `mode: active_coordinator` — выбирается текущий активный координатор из группы серверов.

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

Пример настроек

dns:

trustedServers:

- 77.88.8.8
- 77.88.8.1

settings:

macSpoofingProtection: true
allowedPacketTimeDiff: 7200

features:

- name: tunnel_priority
mode: active_coordinator

network:

tcpMssDecrease: 20

firewall:

applicationLevelGateway:

dns:

udp:

- 53

ftp:

tcp:

- 21

h.323:

tcp:

- 1720

udp:

- 1719

sccp:

tcp:

- 2000

sip:

tcp:

- 5065
- 5068

```
- 5080
udp:
  - 5060
  - 5068
  - 5080
logging:
  level: 3
nodes:
  flags:
    0004008A:
      forceStaticAccessPoints: true
staticAccessPoints:
  0004008A:
    - "192.168.1.71:55778"
```

Термины и сокращения

ViPNet Administrator

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

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задаёт связи между ними.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в неё устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

Дистрибутив ключей

Файл с расширением *.dst или *.ds5 для каждого пользователя узла ViPNet. Создаётся в управляющем ПО ViPNet. Содержит справочники, ключи и файл лицензии для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Маска подсети

Битовая маска, определяющая, какая часть IP-адреса сетевого узла относится к адресу самой сети, а какая часть — к адресу узла в этой сети.

Мастер-ключ

Ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена;
- мастер-ключ ключей защиты ключей обмена;
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Роль

Функциональность сетевого узла, которая решает целевые и служебные задачи сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Набор ролей для каждого сетевого узла задаёт администратор сети ViPNet в программе ViPNet Administrator.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сетевой узел ViPNet

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

Сеть ViPNet

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

Симметричный ключ

Последовательность битов заданной длины (для алгоритма ГОСТ 28147-89 — 256 бит), используемая как для зашифрования, так и для расшифрования информации.

В программном обеспечении ViPNet симметричные ключи используются для зашифрования и расшифрования IP-трафика, информации приложений (в том числе почтовой), служебных и прикладных конвертов.

Суперпользователь (root)

Учётная запись в UNIX-системах, пользователь которой наделён специальными полномочиями, позволяющими осуществлять полный контроль над системой, изменять системные файлы, запускать специальные приложения, выполнять резервное копирование системы. Полномочия пользователя, работающего в системе с правами root, ничем не ограничены.

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Шлюз

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