

ViPNet Client 5 for Linux

Использование функции туннелирования

Версия продукта 5.1.4

Для туннелирования трафика таких устройств, как видеорекамеры и датчики, и создания защищённой сети в случаях, когда нельзя использовать программно-аппаратные решения, вы можете использовать ViPNet Client 5 for Linux в качестве туннелирующего клиента.

Вы можете настроить туннелирование трафика через ViPNet Client 5 for Linux в управляющем ПО ViPNet.

Ограничения ViPNet Client 5 for Linux:

- Работает только с ключами в формате DST.
- Одновременно поддерживает туннелирование не более пяти соединений.
- Не может быть сервером соединений для других сетевых узлов.
- Не может выполнять роль защищённого интернет-шлюза для других сетевых узлов.
- Не может использоваться в качестве межсетевого шлюза.
- Не может использоваться в качестве межсетевого экрана для других сетевых узлов.
- Не гарантирует корректное туннелирование прикладного трафика (DNS, FTP, SIP, H.323). Нельзя изменять настройки прикладных протоколов клиента, включать и выключать трансляцию адресов.
- Не предназначен для туннелирования всех адресов сети интернет. Не указывайте для туннелирования диапазон адресов 0.0.0.0–255.255.255.255.



Внимание! Чтобы программа работала корректно, не изменяйте вручную конфигурационные файлы туннелирующего клиента в ViPNet Client 5 for Linux.

Предварительные действия

В ОС Astra Linux SE пользователям с низким уровнем целостности выдайте привилегию PARSEC_CAP_PROCFS, битовая маска 0x80000 (см. Astra Linux SE. Эксплуатационная и дополнительная документация). Она позволяет игнорировать ограничения мандатного управления доступом и мандатного контроля целостности на файловой системе `/proc`.

В IRZ R2 RL21w выполните [предварительную настройку](#).

Создание туннелирующего клиента в ViPNet Prime

Чтобы добавить туннелирующий клиент в защищённую сеть, в ViPNet Prime создайте:

- 1 Координатор с лицензией **Coordinator for Windows**.
- 2 Ресурсы, которые будут туннелироваться созданным координатором.
- 3 Дистрибутив ключей для созданного координатора.

Подробнее см. в документации ViPNet Prime.

Создание координатора

- 1 Выберите организацию и подразделение.
- 2 Выберите ViPNet VPN  > Управление защищенной сетью > Координаторы.
- 3 Нажмите  **Добавить**. Следуйте указаниям мастера.
 - 3.1 На шаге 1 нажмите  **Создать**.
 - 3.2 На шаге 2 укажите:
 - имя устройства;
 - лицензию **Coordinator for Windows**;
 - 3.3 Нажмите **Готово**. Будет создан координатор.
- 4 Нажмите **Настройки координатора**.
- 5 На вкладке **Параметры подключения** выберите тип подключения координатора к внешней сети **Координатор доступен с использованием сервера соединений**.
- 6 В поле **Сервер соединений** выберите координатор, который доступен напрямую.
- 7 Нажмите **Сохранить**.

Создание ресурсов

- 1 Выберите ViPNet VPN  > Управление защищенной сетью > Ресурсы.
- 2 Нажмите  **Добавить** и в меню выберите один из пунктов:
 - **Создать новый ресурс** — чтобы создать новое устройство ресурса для туннелирования координатором нескольких IP-адресов, в том числе диапазона IP-адресов. Откроется мастер создания нового ресурса, следуйте его указаниям.

Введите имя ресурса и укажите созданный координатор для туннелирования IP-адресов.
 - **Добавить существующий ресурс** — чтобы выбрать созданное ранее устройство в качестве ресурса для туннелирования его IP-адреса.

Выберите устройство и созданный координатор. В списке для выбора ресурса отображаются все устройства организации, которые не задействованы в модуле VPN.

- 3 В поле **Добавление IP-адресов ресурса** введите IP-адрес или диапазон IP-адресов ресурса для туннелирования и нажмите **Добавить**.

Диапазон IP-адресов укажите через дефис (например, 1.2.2.–0-1.2.2.100) или с использованием маски в префиксном формате (например, 11.2.2.0/28).

Не дублируйте адреса туннелируемых узлов в сети ViPNet с туннелирующим клиентом, иначе возникнут сложности с настройкой корректной работы: туннелирование будет назначено узлу с наименьшим значением ViPNet-идентификатора.

- 4 Нажмите **Сохранить**.

Создание дистрибутива ключей

- 1 Выберите созданный координатор и нажмите **Создать сейчас**. Загрузка начнётся автоматически.
- 2 Установите ключи на узле с туннелирующим клиентом.

Создание туннелирующего клиента в ViPNet Administrator

Чтобы добавить туннелирующий клиент в защищённую сеть, в ViPNet Administrator:

- 1 Создайте координатор с ролью **Client+**.
- 2 Отправьте обновления справочников и ключей на узлы.
- 3 Создайте дистрибутив ключей для туннелирующего клиента.

Подробнее см. в документации ViPNet Administrator.

Создание координатора

- 1 В ViPNet ЦУС добавьте координатор.

См. раздел «Добавление координатора» в «ViPNet Центр управления сетью 4. Руководство администратора».

1.1 Выберите **ViPNet ЦУС > Координаторы**.

1.2 Выберите режим **Выполняет функции VPN-сервера**.

1.3 Выберите **Настроить после создания** и нажмите **Создать**.

Будет создан новый координатор и откроется окно с настройками.

- 2 Выберите **Роли узла** и удалите все автоматически назначенные роли. Нажмите **Добавить**.

- 3 В списке доступных ролей выберите **Client+**.

Туннелирующему клиенту запрещено назначать любые роли, кроме Client+.

- 4 Задайте сервер соединений.

4.1 Выберите **Межсетевой экран**.

4.2 В списке **Межсетевой экран** выберите **С динамической трансляцией адресов**.

4.3 В списке **Координатор для организации соединений с внешними узлами** выберите координатор.

Сервер соединений должен быть в той же локальной сети, что и туннелирующий клиент.

- 5 На вкладке **Межсерверные каналы** задайте координатор, с которым требуется образовать межсерверный канал.
- 6 Выберите **Туннелирование** и укажите IP-адрес или диапазон IP-адресов, для которых требуется туннелирование трафика.

Не дублируйте адреса туннелируемых узлов в сети ViPNet с туннелирующим клиентом, иначе возникнут сложности с настройкой корректной работы: туннелирование будет назначено узлу с наименьшим значением ViPNet-идентификатора.

- 7 Нажмите **ОК**.

Обновление справочников и ключей

Отправьте обновлённые справочники и ключи на узлы, на которые повлияли изменения сети.

См. «ViPNet Центр управления сетью 4. Руководство администратора», разделы «Создание справочников» и «Отправка справочников и ключей».

Создание дистрибутива ключей

- 1 В УКЦ создайте дистрибутив ключей для туннелирующего клиента.

См. «ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора», глава «Управление ключевой структурой ViPNet».

- 2 Установите ключи на узле с туннелирующим клиентом.

Обновление ПО на туннелирующем клиенте



Примечание. В ViPNet Prime обновить туннелирующий клиент можно только локально.

- 1 В ЦУСе загрузите архив *.lzh.
- 2 В списке **Программное обеспечение** выберите **Client+**.
- 3 Подтвердите загрузку обновления.
- 4 Отправьте обновление на туннелирующий клиент.

Подробнее про обновление ПО см. раздел «Обновление программного обеспечения» в «ViPNet Центр управления сетью 4. Руководство администратора».

Настройка IRZ R2 RL21w в роли туннелирующего клиента

В инструкции описана настройка для моделей с Ethernet-портом в качестве внешнего интерфейса.

Порядок настройки

- 1 Подготовьте роутер.
- 2 Установите на роутер ViPNet Client 5.
См. «Установка на промышленные контроллеры».
- 3 Установите ключи.
См. руководство пользователя, в разделе «Установка ключей».
- 4 Настройте конфигурацию сети роутера.
- 5 Настройте межсетевой экран роутера.

Подготовка роутера

- 1 Сбросьте роутер до заводских настроек. Для этого нажмите и удерживайте кнопку **RESET** более 20 секунд.
- 2 Определитесь с тем, какие сетевые порты будут отвечать за внутреннюю и внешнюю сеть соответственно.
- 3 Откройте веб-интерфейс роутера. Адрес по умолчанию: 192.168.1.1.
- 4 Выберите **Network > Local Network**, освободите любой порт локальной сети и примените настройки.
- 5 Выберите **Network > Wired Internet** и добавьте новое проводное соединение:
 - 5.1 Выберите порт, который освободили на предыдущем шаге.
 - 5.2 Выберите для него тип соединения:
 - Static — статический адрес,
 - DHCP — адрес, получаемый по DHCP.
 - 5.3 Примените настройки.

Настройка конфигурации сети

- 1 Подключитесь к роутеру по протоколу SSH.
- 2 Добавьте в файл конфигурации сети `/etc/config/network` строки:

```
config interface 'vipnet'
    option auto '1'
    option ifname 'tun0'
    option proto 'static'
```

- 3 Перезапустите сетевую службу:

```
root@host:~# /etc/init.d/network restart
```

Настройка межсетевого экрана

- 1 Откройте веб-интерфейс роутера. Адрес по умолчанию: 192.168.1.1.
- 2 Выберите **Services > Firewall**.
- 3 В **Zones list**:
 - 3.1 В lan-зоне выберите lan и vipnet интерфейсы.
 - 3.2 Выберите **АССЕПТ** для всех типов трафика.
 - 3.3 В wan-зоне выберите wan<любое число> и vipnet интерфейсы.
 - 3.4 Выберите **АССЕПТ** для всех типов трафика.
- 4 В **Allowed forwards** задайте:
 - 4.1 Source: lan, Destination: wan.
 - 4.2 Source: wan, Destination: lan.
- 5 В **Default Actions** выберите **DROP** для всех типов трафика.
- 6 Примените настройки.



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, телеграм-канал поддержки: t.me/vhd21

ФРКЕ.00380-01 90 01, версия продукта 5.1.4

© АО «ИнфоТеКС», 2025. ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, являющиеся зарегистрированными товарными знаками, принадлежат соответствующим владельцам.