ViPNet Client

Быстрый старт

ViPNet Client — программное обеспечение для защиты трафика на рабочих местах пользователей. ViPNet Client фильтрует весь входящий и исходящий трафик компьютера и позволяет обмениваться данными с другими узлами ViPNet по защищенному VPN-каналу.

Этот документ поможет вам узнать о возможностях ViPNet Client и начать работу с программой.

Установка программы

Перед установкой ViPNet Client убедитесь, что на вашем компьютере правильно заданы системное время и региональные настройки. Если у вас установлен сторонний сетевой экран (firewall), удалите его. Также программа ViPNet Client может быть несовместима с антивирусами, которые имеют функцию сетевого экрана.

Для установки программы ViPNet Client запустите установочный файл и следуйте указаниям мастера. После окончания установки может потребоваться перезагрузка компьютера.

Установка ключей

Для работы программного обеспечения ViPNet Client требуются ключи ViPNet. Обратитесь к администратору вашей сети ViPNet, чтобы получить файл `.dst` (`.enc`), необходимый для установки ключей, и пароль либо устройство аутентификации для входа в программу.

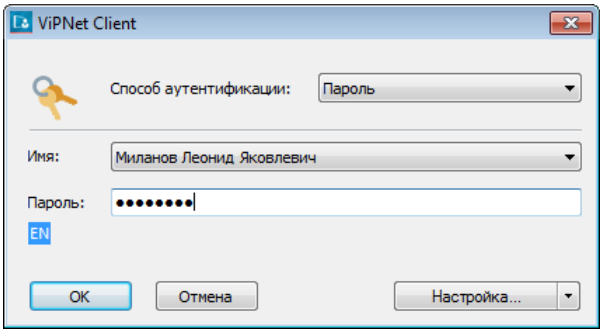
Чтобы установить ключи выполните одно из действий:

- дважды щелкните файл `.dst` и в открывшемся окне нажмите кнопку **Установить ключи**.
- запустите ViPNet Client и в окне входа в программу щелкните значок  справа от кнопки **Настройка**, затем выберите пункт **Установить ключи**. На странице мастера установки укажите путь к файлу дистрибутива ключей `.dst` или `.enc`.

Запуск программы

После установки ключей запустите программу ViPNet Client. В дальнейшем программа будет запускаться автоматически, аутентификацию в ViPNet Client необходимо выполнять перед входом в операционную систему.

Для входа в программу введите ваш пароль либо подключите устройство аутентификации и введите ПИН-код.



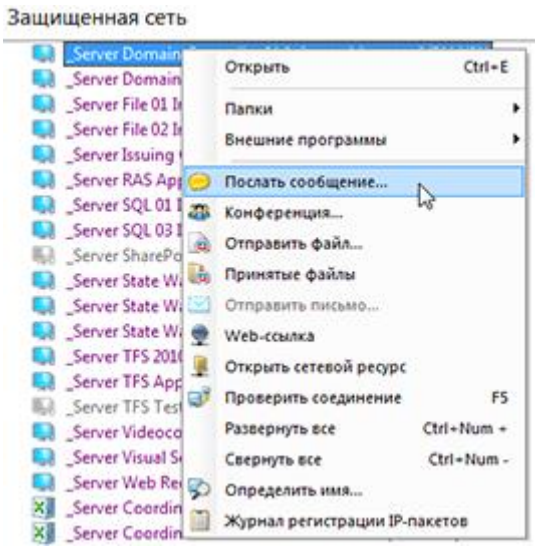
Откроется окно программы ViPNet Монитор.

Работа в защищенной сети

Список узлов ViPNet, с которыми вы можете обмениваться данными по защищенному VPN-каналу, отображается в программе ViPNet Монитор в разделе **Защищенная сеть**.

Чтобы использовать возможности работы в защищенной сети, щелкните нужный узел правой кнопкой мыши и выберите в меню один из пунктов:

- Чтобы проверить доступность узла, выберите пункт **Проверить соединение**.
- Чтобы начать чат с пользователем узла, выберите пункт **Послать сообщение**.
- Чтобы отправить пользователю узла сообщение электронной почты, выберите пункт **Отправить письмо** (см. раздел «ViPNet Деловая почта»).
- Чтобы отправить пользователю узла файл любого размера, выберите пункт **Отправить файл**.
- Чтобы вызвать приложение для удаленного доступа к сетевому узлу (например, Remote Desktop Connection), выберите пункт **Внешние программы**, затем щелкните название нужной программы.
- Для обзора общих папок на сетевом узле, выберите пункт **Открыть сетевой ресурс**.



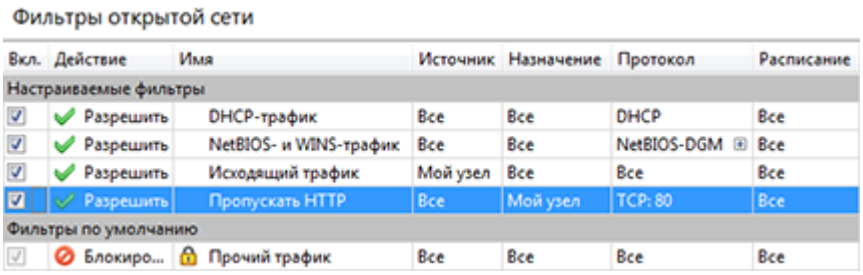
Настройка сетевых фильтров

Сетевые фильтры используются, чтобы пропускать или блокировать трафик по определенным признакам. Сетевые фильтры, настроенные по умолчанию, блокируют входящий открытый (незашифрованный) трафик за исключением протоколов DHCP, NetBIOS, WINS. При необходимости вы можете настроить собственные сетевые фильтры для открытого и зашифрованного трафика.

Рассмотрим создание фильтра, разрешающего входящие соединения от любых адресов по протоколу HTTP (TCP порт 80):

1 В разделе **Фильтры открытой сети** нажмите кнопку **Создать**.

2 В окне фильтра в разделе **Основные параметры** выберите действие фильтра: **Пропускать трафик**.



3 В разделе **Источники** оставьте список источников пустым. Тогда фильтр будет действовать для трафика, отправленного с любых адресов.

4 В разделе **Назначения** добавьте в список объект **Мой узел**.

5 В разделе **Протоколы** добавьте протокол TCP, порт назначения 80.

6 Чтобы сохранить фильтр, нажмите кнопку **OK**.

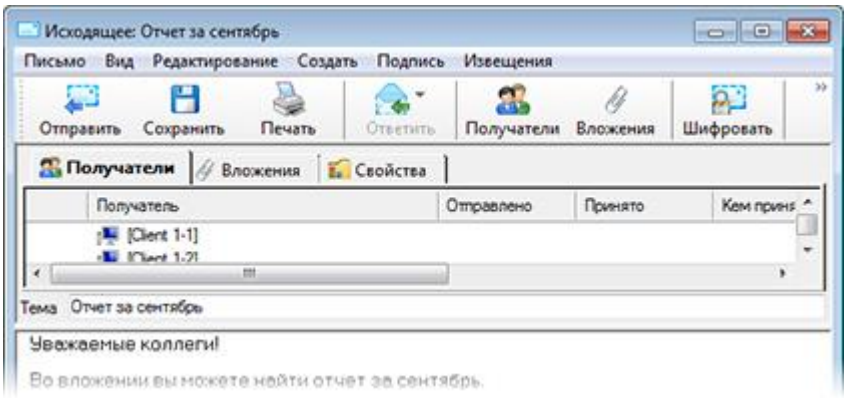
7 При необходимости переместите ваш фильтр на нужную позицию в списке. Чем выше фильтр в списке, тем выше его приоритет.

8 Нажмите кнопку **Применить**.

Примечание. Аналогичным образом вы можете настроить сетевые фильтры для защищенного трафика в разделе **Фильтры защищенной сети**.

ViPNet Деловая почта

С помощью программы ViPNet Деловая почта вы можете отправлять сообщения электронной почты и вложения пользователям других узлов ViPNet. По умолчанию сообщения зашифрованы и подписаны электронной подписью.



Чтобы отправить сообщение электронной почты:

1 Запустите программу ViPNet Деловая почта с помощью ярлыка.

2 Введите пароль либо подключите устройство аутентификации и введите ПИН-код.

3 Нажмите кнопку **Письмо**, в открывшемся окне введите тему и текст письма.

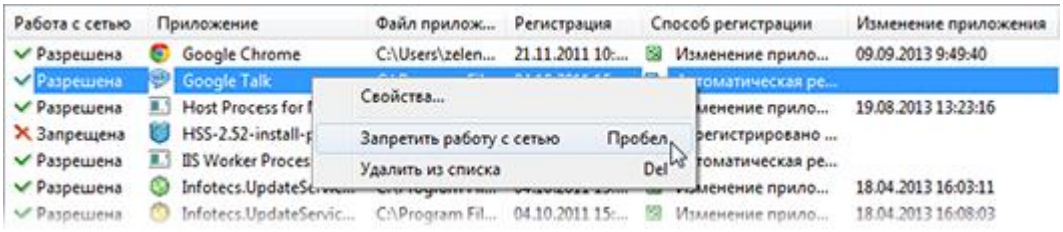
4 Если нужно добавить вложение, на панели инструментов нажмите кнопку **Вложения**.

5 Нажмите кнопку **Получатели** и укажите получателей письма.

6 Нажмите кнопку **Отправить**.

ViPNet Контроль приложений

Программа ViPNet Контроль приложений обеспечивает контроль над сетевой активностью приложений, установленных на компьютере. Если какая-либо программа пытается получить доступ к сети, на экране появляется предупреждение. В окне предупреждения вы можете выбрать, разрешить программе доступ к сети или запретить.



Чтобы просмотреть список приложений, которым разрешен или запрещен доступ к сети, в программе ViPNet Монитор в меню **Приложения** выберите пункт **Контроль приложений**. При необходимости вы можете добавить приложения в список или изменить разрешения для добавленных ранее приложений.

Прием обновлений

Администратор сети ViPNet может присылать на ваш сетевой узел обновления ключей, программного обеспечения и политик безопасности. По умолчанию система обновления ViPNet на вашем компьютере автоматически устанавливает полученные обновления.

При необходимости вы можете изменить настройки системы обновления. Для этого в меню **Пуск** выберите **ViPNet** > **ViPNet Система обновления**.

АО «ИнфоТеКС», 127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29
Телефон: +7 (495) 737-6162, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)
Веб-сайт: https://infotecs.ru
Служба технической поддержки: hotline@infotecs.ru
ФРКЕ.00116-05 34 05, версия продукта 4.5.3