infotecs®

ViPNet **Coordinator** 4.2

Быстрый старт

Компьютеры с программным обеспечением ViPNet Coordinator называются координаторами сети ViPNet. Они играют роль VPN-серверов и межсетевых экранов. Обычно координаторы устанавливают на границе локальной сети, в которой требуется обеспечить защиту трафика.

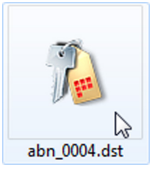
Этот документ поможет вам узнать о возможностях ViPNet Coordinator и начать работу с программой.

Установка программы

Перед установкой ViPNet Coordinator 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 Coordinator может быть несовместима с антивирусами, которые имеют функцию сетевого экрана.

Для установки программы ViPNet Coordinator запустите установочный файл. Затем примите условия лицензионного соглашения и нажмите кнопку **Установить сейчас**. Если потребуется, после окончания установки перезагрузите компьютер.

Установка ключей



Для работы программного обеспечения ViPNet Coordinator требуются ключи ViPNet. Обратитесь к администратору вашей сети ViPNet, чтобы получить файл DST, необходимый для установки ключей, и пароль либо устройство аутентификации для входа в программу.

Чтобы установить ключи, дважды щелкните файл DST и в открывшемся окне нажмите кнопку **Установить ключи**.

Запуск программы

Чтобы запустить программу ViPNet Coordinator после установки ключей, дважды щелкните ярлык программы на рабочем столе. В дальнейшем программа ViPNet Coordinator будет запускаться автоматически. Аутентификацию в ViPNet Coordinator необходимо выполнить перед входом в операционную систему.

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

Если вы хотите администрировать координатор удаленно, вы можете настроить автоматический вход в программу ViPNet Coordinator. Подробную информацию вы найдете в справке программы.

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 проверить соединение с узлом ViPNet, начать чат с пользователем узла или отправить файл, щелкните узел правой кнопкой мыши и в меню выберите действие.

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.

Вы можете настроить сетевые фильтры для защищенного трафика и для следующих типов открытого (незашифрованного) трафика:

- Локального, отправителем или получателем которого является ваш координатор.
- Транзитного, проходящего через координатор из одной сети в другую.

Например, чтобы обеспечить пользователям локальной сети доступ к веб-сайтам в Интернете, необходимо настроить правило трансляции адресов (см. раздел **Настройка правил трансляции адресов**) и разрешить транзитный трафик из локальной сети во внешнюю по протоколу HTTP (TCP порт 80).

Чтобы настроить транзитный сетевой фильтр:

1. В разделе **Транзитные фильтры открытой сети** нажмите кнопку **Создать**.
2. В окне фильтра в разделе **Основные параметры** выберите действие фильтра: **Пропускать трафик**.
3. В разделе **Источники** укажите диапазон IP-адресов вашей локальной сети.
4. В разделе **Назначения** укажите группу IP-адресов **Публичные IP-адреса**.
5. В разделе **Протоколы** добавьте протокол TCP, порт назначения 80.
6. Чтобы сохранить фильтр, нажмите кнопку **ОК**.

Транзитные фильтры открытой сети

Вкл.	Действие	Имя	Источник	Назначение	Протокол	Расписание
Настраиваемые фильтры						
☑	Разрешить	Пропускать HTTP	192.168.1.0/255....	Публичны...	TCP: 80	Все
Фильтры по умолчанию						
☑	Блокировать	Прочий трафик	Все	Все	Все	Все

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

8 Нажмите кнопку **Применить все**.

Аналогичным образом в разделе **Локальные фильтры открытой сети** вы можете настроить сетевые фильтры для локального открытого трафика, а в разделе **Фильтры защищенной сети** — для защищенного трафика.

Настройка правил трансляции адресов

С помощью трансляции адресов (NAT) вы можете обеспечить доступ компьютеров локальной сети в Интернет или открыть доступ из внешней сети к серверу, находящемуся в локальной сети.

Чтобы обеспечить пользователям локальной сети доступ к веб-сайтам в Интернете, помимо транзитного фильтра (см. раздел **Настройка сетевых фильтров**) необходимо настроить трансляцию адреса источника для HTTP-трафика (TCP порт 80). Для этого:

1 В разделе **Трансляция адресов** нажмите кнопку **Создать**.

2 В окне правила в разделе **Источники** укажите диапазон IP-адресов локальной сети.

3 В разделе **Назначения** укажите группу IP-адресов **Публичные IP-адреса**.

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

Трансляция адресов

Вкл.	Имя	Источник	Назначение	Протокол	Трансляция
Настраиваемые фильтры					
☑	Доступ к веб-...	192.168.1.0/255.255.255.0	Публичные IP-ад...	TCP: 80	Источник (Адрес исходя...

5 В разделе **Трансляция адресов** установите флажок **Заменять адрес источника на** и выберите пункт **Адрес исходящего интерфейса (определяется автоматически)**.

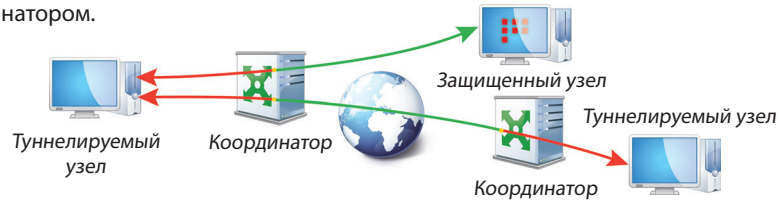
6 Чтобы сохранить правило, нажмите кнопку **ОК**.

7 Задайте приоритет правила, поместив его на нужную позицию в списке.

8 В разделе **Трансляция адресов** нажмите кнопку **Применить все**.

Туннелирование

Координатор может осуществлять тунелирование соединений с компьютерами, на которых не установлено программное обеспечение ViPNet (открытыми узлами), чтобы защитить трафик при передаче через Интернет. Доступ к туннелируемым узлам можно получить с любого узла ViPNet или с компьютера, который туннелируется другим координатором.



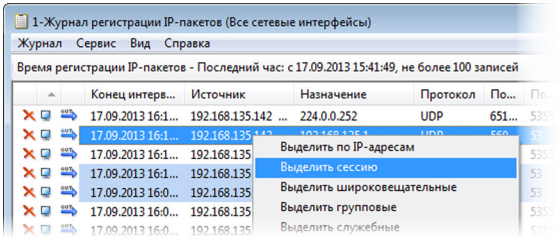
IP-адреса узлов, которые туннелирует координатор, а также максимальное число одновременно туннелируемых соединений рекомендуется задать в Центре управления сетью. На туннелируемых узлах в качестве шлюза по умолчанию должен быть указан IP-адрес координатора.

Чтобы ограничить трафик между туннелируемыми узлами вашего координатора и защищенными узлами ViPNet, вы можете создать сетевые фильтры в разделе **Фильтры для туннелируемых узлов**. Настройка этих фильтров аналогична созданию фильтров открытой сети (см. **Настройка сетевых фильтров**).

Просмотр журнала IP-пакетов

Для просмотра истории пропущенных и заблокированных пакетов вы можете использовать журнал IP-пакетов. Чтобы просмотреть журнал IP-пакетов:

1. В разделе **Журнал IP-пакетов** задайте параметры поиска IP-пакетов в журнале.
2. Нажмите кнопку **Поиск**.
3. В окне **Журнал регистрации IP-пакетов** просмотрите результат поиска.



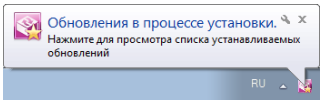
4. Если требуется создать сетевой фильтр на основе записи в журнале, в контекстном меню выберите пункт **Создать фильтр**. Затем задайте параметры нового фильтра, как описано в разделе **Настройка сетевых фильтров**.

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 открыть окно программы ViPNet Контроль приложений, в программе ViPNet Монитор в меню **Приложения** выберите пункт **Контроль 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, в области уведомлений появляется соответствующее сообщение.



Документация для продуктов ViPNet:	http://docs.infotecs.ru/
Видеоруководства и презентации:	http://www.youtube.com/user/InfotecsDoc
Электронный адрес службы поддержки:	hotline@infotecs.ru
Телефон горячей линии (бесплатный звонок с территории России, кроме Москвы):	8–800–250–0–260