ViPNet Terminal 4

Общее описание

infotecs

© 1991 – 2019 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00154-01 90 01

Версия продукта 4.1.8

Этот документ входит в комплект поставки ViPNet Terminal, 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 ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

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

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: https://infotecs.ru/

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение ... **6**
О документе ... 7
Для кого предназначен документ ... 7
Соглашения документа ... 7
Комплект поставки ... 9
Новые возможности версии 4.1.7 ... 10
Обратная связь ... 11
Навигатор по документации ... 12

Глава 1. Общая информация ... **14**
Защищенная сеть ViPNet ... 15
Назначение ViPNet Terminal ... 16
Состав программного обеспечения ... 17
Режимы подключения ViPNet Terminal к внешней сети через межсетевой экран ... 18

Глава 2. Варианты исполнения и лицензирование ... **20**
Варианты исполнения ViPNet Terminal ... 21
Системные требования для варианта исполнения Live USB ... 21
Аппаратная платформа Kraftway Credo VV18 ... 22
Аппаратная платформа TONK TN1902 ... 23
Лицензирование ViPNet Terminal ... 25

Глава 3. Подготовка к развертыванию сети с узлами ViPNet Terminal ... **26**
Порядок развертывания сети с узлами ViPNet Terminal ... 27
Создание сетевых узлов ViPNet Terminal ... 29
Создание сетевых узлов в ЦУСе версии ниже 4.x ... 29
Создание сетевых узлов в ЦУСе версии 4.x ... 33
Особенности работы с терминальным сервером ... 35

Приложение А. Возможные неполадки и способы их устранения ... **36**
При загрузке компьютера возникает ошибка ... 36
При каждой загрузке на сертифицированной платформе возникает предложение восстановить параметры BIOS ... 36
Потеря подключения устройства аутентификации ... 37
Не удается выполнить аутентификацию с помощью eToken PRO Java 72K ... 37

Не удается установить справочники и ключи из-за предложения восстановить BIOS 37
Не удается использовать съемные носители в терминальной сессии 38
Дефекты изображения на экране компьютера 38
Не работают подключенные к компьютеру USB-устройства 38
Не удается включить 3G/LTE-модем 39
Не определяется 3G-модем 40
Не удается подключиться к терминальному серверу Citrix по протоколу ICA 40
При подключении к терминальному серверу Citrix окно с терминальной сессией выходит за рамки экрана 40
Не удается подключиться по протоколу RDP к терминальному серверу, использующему SSL-сертификаты 41
Составное устройство хранения данных перенаправляется некорректно 41
Не удается перенаправить принтер HP Laserjet Professional p1102/p1102w 42
Не удается возобновить печать на принтере HP LaserJet Professional p1102/p1102w 43

Приложение B. Список поддерживаемого оборудования 44
Поддерживаемые 3G/4G-модемы 44
Поддерживаемые сетевые карты Wi-Fi 45
Поддерживаемые графические адаптеры 45
Поддерживаемые принтеры 45
Поддерживаемые USB-гарнитуры 46
Поддерживаемые криптотокены и смарт-карты 46
Поддерживаемые считыватели смарт-карт 46
Поддерживаемые сканеры штрих-кодов 46

Приложение C. История версий 47
Версия 4.1.6 47
Версия 4.1.5 48
Версия 4.1.4 49
Версия 4.1.3 49
Версия 4.1.2 50
Версия 4.1.1 51
Версия 4.1.0 52
Версия 3.4.0 55
Версия 3.3.0 55
Версия 3.2.0 57
Версия 3.1.0 58
Версия 3.0.0 59

Версия 2.2.0 59
Версия 2.1.0 59
Версия 2.0.0 60

Приложение D. Глоссарий 61

Введение

О документе 7

Комплект поставки 9

Новые возможности версии 4.1.6 10

Обратная связь 11

Навигатор по документации 12

О документе

В документе описывается назначение и применение программного обеспечения ViPNet Terminal в составе защищенных сетей ViPNet. В нем приведены варианты исполнения ViPNet Terminal, указан список поддерживаемого оборудования, описаны возможные неполадки и способы их устранения. Также в документе содержится навигатор по остальным документам из комплекта поставки (см. Комплект поставки на стр. 9).

Для кого предназначен документ

Документ предназначен для администраторов, отвечающих за настройку и эксплуатацию ViPNet Terminal.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.

Обозначение	Описание
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

Комплект поставки

ViPNet Terminal поставляется либо в виде образа ПО, либо в одном из вариантов с предустановленным ПО:

- Образ загрузочного диска `terminal_vipnet_base_i386_x.x.x-xxxx.usb.img`.
- Образ установочного диска `terminal_vipnet_base_i386_x.x.x-xxxx.img`.
- USB Flash.
- Компактный компьютер Kraftway Credo VV18.
- Компактный компьютер TONK TN1902.

В комплект поставки также входит документация в формате PDF:

- «ViPNet Terminal. Быстрый старт».
- «ViPNet Terminal. Общее описание».
- «ViPNet Terminal. Установка и обновление».
- «ViPNet Terminal. Руководство пользователя».
- «ViPNet Terminal. Руководство администратора».
- «Справочное руководство по командному интерпретатору. Приложение к руководству администратора ViPNet Terminal».
- «Справочное руководство по конфигурационным файлам. Приложение к руководству администратора ViPNet Terminal».
- «ViPNet Terminal. API ЭП в браузере Firefox. Руководство разработчика».

Новые возможности версии 4.1.8

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Terminal версии 4.1.8 по сравнению с версией 4.1.7.

Информация об изменениях в предыдущих версиях содержится в приложении История версий (на стр. 47).

- **Поддержка нескольких микрофонов**

  Начиная с версии 4.1.8, ViPNet Terminal поддерживает подключение несколько микрофонов. Подробнее см. в документе «ViPNet Terminal. Справочное руководство по командному интерпретатору», описание команд `machine show microphone` и `machine set microphone`.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Информация о продуктах ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Часто задаваемые вопросы https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт https://infotecs.ru/support/request/.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения https://infotecs.ru/disclosure.php.

Навигатор по документации

Данный раздел поможет вам сориентироваться в комплекте документации ViPNet Terminal версии 4.1. В таблице ниже указаны документы и основные сведения и настройки ViPNet Terminal, которые в них описаны.

Таблица 3. Навигатор по документации

Документ	Сведения и настройки
«ViPNet Terminal. Общее описание»	Общие сведения о сети ViPNet. Назначение и состав ViPNet Terminal. Варианты исполнения ViPNet Terminal. Подготовка к развертыванию сети с узлами ViPNet Terminal. Возможные неполадки и способы их устранения. Список поддерживаемого оборудования.
«ViPNet Terminal. Установка и обновление»	Запись образа ПО ViPNet Terminal на USB-носитель. Установка ПО ViPNet Terminal на компьютер. Обновление ПО ViPNet Terminal. Установка справочников и ключей сетевого узла ViPNet.
«ViPNet Terminal. Руководство пользователя»	Запуск ViPNet Terminal. Настройка системных параметров. Настройка подключения к сети. Изменение списка доступных терминальных серверов. Просмотр списка узлов защищенной сети. Просмотр сетевых фильтров. Смена конфигурации сетевого экрана. Сценарии работы в терминальной сессии.
«ViPNet Terminal. Руководство администратора»	Настройка системных параметров с помощью командного интерпретатора. Настройка подключения к сети с помощью командного интерпретатора.

Документ	Сведения и настройки
	Настройка списка доступных терминальных серверов с помощью командного интерпретатора. Создание и изменение сетевых фильтров с помощью командного интерпретатора. Настройка транспортного модуля ViPNet. Работа с конфигурациями ViPNet. Экспорт и импорт справочников, ключей и настроек. Просмотр журналов событий.
«Справочное руководство по командному интерпретатору. Приложение к руководству администратора ViPNet Terminal»	Описание команд ViPNet Terminal.
«Справочное руководство по конфигурационным файлам. Приложение к руководству администратора ViPNet Terminal»	Описание конфигурационных файлов управляющего демона.
«ViPNet Terminal. API ЭП в браузере Firefox. Руководство разработчика»	Описание функций электронной подписи и сопряженных функций, реализованных в плагине для браузера Firefox.
«ViPNet Terminal. Быстрый старт»	Краткое описание работы с ViPNet Terminal.

1

Общая информация

Защищенная сеть ViPNet 15

Назначение ViPNet Terminal 16

Состав программного обеспечения 17

Режимы подключения ViPNet Terminal к внешней сети через межсетевой экран 18

Защищенная сеть ViPNet

Программное обеспечение ViPNet Terminal предназначено для использования в защищенной сети ViPNet, построенной на основе комплекса программных продуктов ViPNet.

Сеть ViPNet представляет собой виртуальную защищенную сеть, которая может быть развернута поверх локальных или глобальных сетей любой структуры. В отличие от многих популярных VPN-решений, технология ViPNet обеспечивает защищенное взаимодействие между сетевыми узлами (см. глоссарий, стр. 64) по схеме «клиент-клиент».

Защита информации в сети ViPNet осуществляется с помощью специального программного обеспечения, которое выполняет две основные функции:

- Фильтрация всего IP-трафика сетевых узлов. Фильтрация трафика осуществляется в соответствии с заданными на узле правилами.
- Шифрование соединений между узлами сети ViPNet. Для шифрования трафика используются симметричные ключи, которые создаются и распределяются централизованно.

Для управления защищенной сетью ViPNet предназначена программа ViPNet Центр управление сетью (ЦУС) (см. глоссарий, стр. 62). С помощью этой программы осуществляется создание сетевых узлов и связей между ними, настройка параметров отдельных узлов, создание дистрибутивов ключей (см. глоссарий, стр. 62) для каждого узла, централизованное обновление справочников, ключей и программного обеспечения на узлах.

Сетевые узлы ViPNet делятся на два типа:

- Клиент (ViPNet-клиент) (см. глоссарий, стр. 63) — предназначен для работы пользователей сети ViPNet. Сетевой узел ViPNet Terminal является клиентом.
- Координатор (ViPNet-координатор) (см. глоссарий, стр. 63) — сервер сети ViPNet.

Также сеть ViPNet может включать компьютеры без программного обеспечения ViPNet, защищенные с помощью технологии туннелирования (см. глоссарий, стр. 65). Эти узлы называются «туннелируемыми», их трафик защищают ViPNet-координаторы.

Назначение ViPNet Terminal

Программное обеспечение ViPNet Terminal предназначено для организации защищенного рабочего места пользователя сети ViPNet и выполняет функцию тонкого клиента (см. глоссарий, стр. 64). ViPNet Terminal позволяет организовать следующие виды защищенного удаленного доступа:

- Доступ к удаленному рабочему столу на терминальном сервере (см. глоссарий, стр. 64) Citrix (по протоколу ICA) или Windows Server 2003/2008/2008 R2/2012/2012 R2 (по протоколу RDP).
- Доступ к опубликованным приложениям на сервере Citrix (по протоколам ICA, HTTP).
- Доступ к службам, реализованным по технологии Web Access (по протоколам HTTP и HTTPS).
- Доступ к виртуальным рабочим столам, реализованным по технологии VMware Horizon View (по протоколам RDP и PCoIP).
- Доступ к виртуальным рабочим столам, реализованным по технологии IBS Parallels VDI.
- Доступ к видеоконференциям TrueConf и Vinteo.

Преимущество работы в режиме терминального клиента заключается в снижении расходов на программное и аппаратное обеспечение, уменьшении затрат времени на администрирование, повышении уровня защиты от внутренних злоумышленников.

С точки зрения технологии ViPNet, узел с ПО ViPNet Terminal является клиентом сети ViPNet. ПО ViPNet Terminal осуществляет шифрование IP-трафика и выполняет функции персонального сетевого экрана. Терминальный сервер может быть расположен на защищенном узле ViPNet или на узле, который туннелируется координатором ViPNet. Тем самым обеспечивается защита ViPNet Terminal от сетевых атак и вмешательства в терминальную сессию пользователя.

Состав программного обеспечения

Программное обеспечение ViPNet Terminal содержит следующие основные функциональные модули:

- **Низкоуровневый драйвер сетевой защиты iplir**, взаимодействующий непосредственно с драйверами сетевых интерфейсов и контролирующий весь обмен трафиком данного компьютера с внешней сетью.
- **Управляющий демон iplircfg**, который осуществляет загрузку необходимых параметров в драйвер iplir, рассылку и прием информации об IP-адресах клиентов, ведение журнала трафика и так далее. Рекомендуется, чтобы этот демон всегда был запущен, но при его остановке драйвер iplir продолжает работать и обмен трафиком не прерывается.
- **Криптографический драйвер**, выполняющий криптографические операции по запросу драйвера iplir.
- **Демон mftpd (транспортный модуль MFTP)**, который обеспечивает прием и передачу транспортных конвертов между узлами сети ViPNet.
- **Демон algd**, который осуществляет обработку прикладных протоколов.
- **SNMP-демон**, который позволяет получать статистику работы ПО ViPNet с удаленных узлов по протоколу SNMP.
- **Командный интерпретатор**, с помощью которого осуществляется тонкая настройка ViPNet Terminal.
- **Графический интерфейс пользователя**, который обеспечивает запуск терминальных сессий и настройку основных параметров ViPNet Terminal.

Режимы подключения ViPNet Terminal к внешней сети через межсетевой экран

Чтобы обеспечить возможность подключения ViPNet Terminal к внешней сети при использовании различных типов межсетевого экрана, в программном обеспечении ViPNet предусмотрено четыре режима работы через межсетевой экран:

1. **Без использования межсетевого экрана** — ViPNet Terminal имеет прямое подключение к внешней сети.
2. **Координатор** – в качестве межсетевого экрана используется координатор.
3. **Со статической трансляцией адресов** — подключение через внешний межсетевой экран (устройство) с трансляцией адресов (NAT), на котором возможна настройка статических правил трансляции адресов.
4. **С динамической трансляцией адресов** — подключение через внешний межсетевой экран (устройство), на котором осуществляется динамическая трансляция адресов (наиболее распространенный способ подключения к WAN).

Если ViPNet Terminal имеет непосредственное подключение к внешней сети, то есть может быть доступен напрямую со стороны любых других сетевых узлов (например, имеет публичный адрес), то для него следует выбрать режим **Без использования межсетевого экрана**.

Если ViPNet Terminal имеет частный IP-адрес, который может быть недоступен для других сетевых узлов в соответствии с общими правилами маршрутизации (то есть на выходе во внешнюю сеть установлен межсетевой экран или иное устройство, выполняющее преобразование адресов), то необходимо выбрать один из режимов подключения к сети через межсетевой экран.

Режим **Координатор** выбирается в случае, если на выходе во внешнюю сеть установлен координатор, выполняющий функции межсетевого экрана. В этом случае установленный координатор выбирается в качестве межсетевого экрана для ViPNet Terminal.

Режим **Со статической трансляцией адресов** выбирается в случае, если на выходе во внешнюю сеть установлен межсетевой экран или иное NAT-устройство, на котором можно настроить статические правила трансляции адресов, обеспечивающие взаимодействие с определенным внутренним адресом сети по протоколу UDP с заданным портом. Данный режим используется по умолчанию в ViPNet Terminal версии 4.1 и выше.

Режим **С динамической трансляцией адресов** выбирается в случае, если на выходе во внешнюю сеть установлен межсетевой экран или иное NAT-устройство, на котором затруднительно настроить статические правила трансляции адресов. Следует отметить, что данный режим наиболее универсален и ViPNet Terminal в этом режиме будет работоспособен и при других способах подключения к сети.

Примечание. Если узлы находятся в одной локальной сети и могут обмениваться широковещательными пакетами, то независимо от выбранного типа межсетевого экрана взаимодействие между ними всегда осуществляется напрямую по IP-адресу узла.

2

Варианты исполнения и лицензирование

Варианты исполнения ViPNet Terminal 21

Лицензирование ViPNet Terminal 25

Варианты исполнения ViPNet Terminal

ViPNet Terminal имеет три варианта исполнения. Эти варианты отличаются носителем, который используется в качестве загрузочного:

- Исполнение Live USB — в качестве загрузочного используется USB-носитель.
- Исполнение K — исполнение на базе компактного компьютера Kraftway Credo VV18 (см. «Аппаратная платформа Kraftway Credo VV18» на стр. 22). В этом варианте в качестве загрузочного носителя используется встроенная карта CompactFlash.
- Исполнение T — исполнение на базе компактного компьютера TONK TN1902 (см. «Аппаратная платформа TONK TN1902» на стр. 23). В этом варианте в качестве загрузочного носителя используется встроенный SSD-диск.

Примечание. ПО ViPNet Terminal может поставляться в базовом и минимальном вариантах. В минимальном варианте доступны все функции, кроме доступа к виртуальным рабочим столам, реализованным по технологиям IBS Parallels VDI и Fusion Access, доступа к видеоконференциям TrueConf и Vinteo.

Программное обеспечение ViPNet Terminal функционирует под управлением операционной системы Linux. В качестве консоли используются монитор и клавиатура.

Системные требования для варианта исполнения Live USB

В варианте исполнения Live USB в качестве загрузочного должен использоваться USB-носитель объемом не менее 4 Гбайт. Для операции удаленного обновления ПО необходим USB-носитель объемом не менее 8 Гбайт.

ViPNet Terminal в варианте исполнения Live USB рекомендуется использовать на IBM-совместимых компьютерах (стационарных или портативных) следующей конфигурации:

- Процессор — не менее Intel Pentium III.
- Оперативная память — не менее 2 Гбайт.
- Сетевые интерфейсы — один интерфейс Ethernet 10/100/1000 (Ethernet 10/100).
- Разъемы USB 2.0 — не менее трех.
- Графический адаптер — карта VGA.

Аппаратная платформа Kraftway Credo VV18

В варианте исполнения K в качестве аппаратной платформы для программного обеспечения ViPNet Terminal используется компактный компьютер Kraftway Credo VV18. Компьютер представляет собой вычислительную платформу на базе процессора Intel Atom с частотой 1,66 ГГц. Компьютер выполнен в прочном корпусе, устойчив к пыли и вибрациям, обладает низким уровнем энергопотребления и тепловыделения, имеет миниатюрные размеры и малый вес. Он может устанавливаться на столе или крепиться по стандарту VESA 100 на любую поверхность, в том числе на заднюю стенку монитора.

На передней панели компьютера Kraftway Credo VV18 расположены два разъема USB, два аудиоразъема и кнопка питания. Остальные коммуникационные разъемы находятся на задней панели компьютера.

Рисунок 1. Задняя панель компьютера Kraftway Credo VV18

Компьютер Kraftway Credo VV18 имеет следующие технические характеристики:

Таблица 4. Характеристики компактного компьютера Kraftway Credo VV18

Описание	Характеристика
Процессор	Intel Atom N450, FSB 667; 1,66 ГГц
Оперативная память	2 Гбайт
Сетевые интерфейсы	1 интерфейс Ethernet 10/100/1000 Мбит/с Адаптер Wi-Fi 802.11b/g
Графический адаптер	VGA, максимальное разрешение 2048x1536
Накопитель	CompactFlash от 4 Гбайт
Разъемы ввода-вывода	6 разъемов USB 2.0 1 разъем VGA (D-Sub) 1 разъем RJ-45
Мощность источника питания	36 Вт (внешний адаптер AC-DC)

Аппаратная платформа TONK TN1902

В варианте исполнения Т в качестве аппаратной платформы для программного обеспечения ViPNet Terminal используется компактный компьютер TONK TN1902. Компьютер представляет собой вычислительную платформу на базе 4-ядерного процессора INTEL Baytrail-D J1900 с частотой 2,41 ГГц. Компьютер выполнен в компактном корпусе, обладает высоким уровнем производительности, имеет миниатюрные размеры и малый вес. Он может устанавливаться на столе или крепиться по стандарту VESA 100 на любую поверхность, в том числе на заднюю стенку монитора.

На передней панели компьютера TONK TN1902 расположен разъем USB 3.0, два аудиоразъема и кнопка питания. Остальные коммуникационные разъемы находятся на задней панели компьютера.

Рисунок 2. Передняя и задняя панели компьютера TONK TN1902

Компьютер TONK TN1902 имеет следующие технические характеристики:

Таблица 5. Характеристики компактного компьютера TONK TN1902

Описание	Характеристика
Процессор	INTEL Baytrail-D J1900 Quad-Core; 2.42GHz

Описание	Характеристика
Оперативная память	4 Гбайт
Сетевые интерфейсы	1 интерфейс Ethernet 10/100/1000 Мбит/с Адаптер Wi-Fi 802.11b/g
Графический адаптер	Intel® Graphics Media Accelerator 3600, максимальное разрешение 1920x1200 (DVI), 2560x1600 (Display Port)
Накопитель	SSD 16 Гбайт
Разъемы ввода-вывода	5 разъемов USB 2.0 1 разъем USB 3.0 1 разъем Display Port 1 разъем DVI 1 разъем RJ-45
Мощность источника питания	10 Вт (внешний адаптер AC-DC)

Лицензирование ViPNet Terminal

Лицензирование ViPNet Terminal осуществляется с помощью назначения сетевому узлу соответствующей роли в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 62).

В программе ViPNet Центр управления сетью администратор сети ViPNet может ограничить следующие параметры ViPNet Terminal:

- Возможность использования токена.
- Возможность подключения USB-накопителей.
- Возможность локальной печати.
- Возможность воспроизведения звука.
- Уровень полномочий при работе с веб-интерфейсом.
- Использование энергосбережения.
- Возможность использования многооконного режима работы.
- Разрешение экрана.

3

Подготовка к развертыванию сети с узлами ViPNet Terminal

Порядок развертывания сети с узлами ViPNet Terminal 27

Создание сетевых узлов ViPNet Terminal 29

Особенности работы с терминальным сервером 35

Порядок развертывания сети с узлами ViPNet Terminal

Рассмотрим пример сети, состоящей из терминального сервера (см. глоссарий, стр. 64) и нескольких клиентов (см. глоссарий, стр. 64). На сервере установлена операционная система Windows Server 2003/2008/2008 R2/2012/2012 R2 со службой терминалов, в качестве клиентов используются ViPNet Terminal.

ViPNet Terminal могут находиться в сетях Ethernet или Wi-Fi либо подключаться к Интернету с помощью USB-модема Yota или 3G-модемов сотовых операторов.

Примечание. ViPNet Terminal в варианте исполнения Live USB можно запустить на любом компьютере, загрузившись с USB-носителя, на котором записано ПО ViPNet Terminal.

При создании сетевых узлов для ViPNet Terminal необходимо наличие в ViPNet-сети координатора, на котором будут зарегистрированы эти узлы. Координатор должен быть доступен из Интернета по публичному IP-адресу или через межсетевой экран со статической трансляцией адресов. В частном случае координатор может быть терминальным сервером либо туннелировать терминальный сервер (см. глоссарий, стр. 65).

Если координатор сам является терминальным сервером, при создании сетевых узлов для ViPNet Terminal (см. Создание сетевых узлов ViPNet Terminal на стр. 29) в качестве IP-адреса терминального сервера нужно указать IP-адрес доступа к координатору (89.173.28.15 на схеме ниже).

Рисунок 3. Координатор является терминальным сервером

Если координатор туннелирует терминальный сервер либо сетевые узлы ViPNet Terminal зарегистрированы на каком-либо другом координаторе, то в настройках ViPNet Terminal нужно указать реальный IP-адрес терминального сервера (10.0.0.2 на схеме ниже).

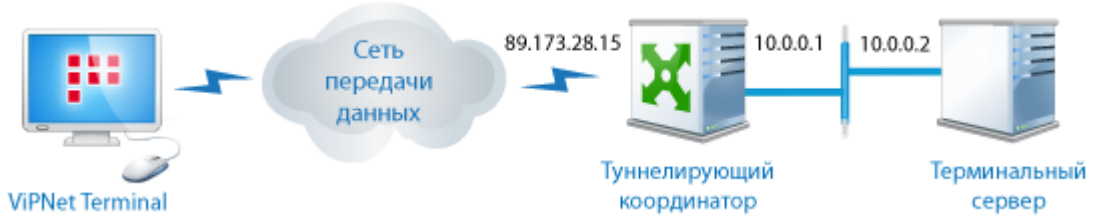

Рисунок 4. Терминальный сервер туннелируется координатором

Для развертывания сети с узлами ViPNet Terminal выполните следующие действия:

1. В программе ViPNet Центр управления сетью создайте сетевые узлы, из которых будет состоять сеть (см. Создание сетевых узлов ViPNet Terminal на стр. 29).
2. Создайте дистрибутивы ключей и перенесите их на съемные USB-носители.
3. Запишите образы программного обеспечения ViPNet Terminal на съемные USB-носители.
4. Если в сети используются ViPNet Terminal в варианте исполнения K или T (см. Варианты исполнения ViPNet Terminal на стр. 21), установите ПО ViPNet Terminal на каждый компактный компьютер.
5. На каждом узле ViPNet Terminal установите справочники и ключи.

   Установка ПО ViPNet Terminal, а также установка справочников и ключей подробно описаны в документе «ViPNet Terminal. Установка и обновление».
6. Перед началом работы настройте каждый узел ViPNet Terminal.

   Сведения о настройке ViPNet Terminal содержатся в документе «ViPNet Terminal. Руководство пользователя».

Создание сетевых узлов ViPNet Terminal

Для развертывания сети, состоящей из терминального сервера и клиентских узлов ViPNet Terminal, требуется создать сетевые узлы в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 62).

Порядок создания сетевых узлов зависит от версии программы ViPNet Центр управления сетью, которую вы используете, — версия ниже 4.x (см. Создание сетевых узлов в ЦУСе версии ниже 4.x на стр. 29) или версия 4.x и выше (см. Создание сетевых узлов в ЦУСе версии 4.x на стр. 33).

После создания сетевых узлов сохраните дистрибутивы ключей и передайте их пользователям ViPNet Terminal.

В программе ViPNet Центр управления сетью при создании сетевых узлов вы можете задать их параметры. Состав параметров также зависит от версии программы ViPNet Центр управления сетью:

- В версии ниже 4.x вы можете задать список терминальных серверов, операторов сети 3G и настройки прокси-сервера веб-браузера Firefox.
- В версии 4.x вы можете задать только список терминальных серверов. Настройки прокси-сервера вы должны выполнить непосредственно на сетевом узле ViPNet Terminal.

В дальнейшем в программе ViPNet Центр управления сетью вы можете изменить параметры сетевых узлов ViPNet Terminal, заданные при их создании. Чтобы применить изменения, отправьте на эти узлы справочники и ключи.

Подробная информация о работе в программе ViPNet Центр управления сетью содержится в документе «ViPNet Центр управления сетью. Руководство администратора».

Создание сетевых узлов в ЦУСе версии ниже 4.x

Если вы используете программу ViPNet Центр управления сетью версии ниже 4.x, для создания сетевых узлов выполните следующие действия:

1 Зарегистрируйте абонентские пункты, которые будут использоваться в качестве терминальных клиентов, на каком-либо координаторе.

Примечание. Не используйте в имени сетевого узла символ '№'. При использовании этого символа имя сетевого узла некорректно отображается при установке ключей на ViPNet Terminal.

2 На созданных сетевых узлах зарегистрируйте типы коллективов и пользователей.

3 В окне групповой регистрации узлов в прикладных задачах выберите задачу «ViPNet Terminal». Откроется окно **Регистрация в задаче ViPNet Terminal**.

4 С помощью кнопки **Добавить** зарегистрируйте в данной прикладной задаче абонентские пункты, на которых будет использоваться ПО ViPNet Terminal.

5 Для каждого абонентского пункта задайте полномочия пользователей и параметры перенаправления устройств на терминальный сервер. Для этого нажмите кнопку **Полномочия** и установите или снимите соответствующие флажки.

6 Задайте связь типов коллективов абонентских пунктов с типом коллективов терминального сервера или координатора, который туннелирует терминальный сервер. Если требуется, свяжите абонентские пункты с несколькими терминальными серверами.

7 Для каждого абонентского пункта задайте список терминальных серверов. Для этого нажмите кнопку **IP-адреса**. В списке IP-адресов задайте параметры терминальных серверов, которые должны быть доступны на абонентском пункте. Для каждого терминального сервера добавьте в список строку следующего вида:

```
T:<протокол>:<адрес> [<параметр 1>=<значение 1>] ... [<параметр n>=<значение n>]
```

Для каждого терминального сервера вы можете задать следующие параметры:

- `протокол` — протокол доступа к терминальному серверу. Допустимые значения: `rdp`, `citrix`, `http`, `https`, `vmware-vdi`, `ibs-vdi`.
- `адрес` — адрес терминального сервера. Может быть задан в виде IP-адреса или DNS-имени, если сервер является открытым или туннелируемым узлом. Если сервер является защищенным узлом ViPNet, может быть указан его шестнадцатеричный идентификатор в формате `0xAAAAAAAA`.
- `параметр n, значение n` — необязательные параметры и их значения. Допустимые необязательные параметры перечислены ниже:
  - `application` — имя приложения, опубликованного на сервере Citrix.
  - `citrix-type` — тип подключения к терминальному серверу Citrix. Используется только вместе с параметром `application`. Допустимые значения: `farm` (подключение к ферме серверов) или `server` (подключение к отдельному серверу). По умолчанию используется подключение к отдельному серверу.
  - `reserve-address` — адрес резервного сервера при подключении к опубликованному приложению фермы серверов Citrix. Используется только вместе с параметром `application` и параметром `citrix-type=farm`. Задается в формате: `<тип адреса>:<адрес>`. Допустимые значения типа адреса: `ip` (IP-адрес), `dns` (DNS-имя) или `id` (ID узла). Например: `ip:10.0.2.196`.
  - `autoconnect` — признак, указывающий на необходимость запуска приложения при загрузке графической сессии. Допустимые значения: `on` (включить автоматический запуск) или `off` (отключить автоматический запуск). По умолчанию автоматический запуск отключен.

- `path` — относительный URL-адрес страницы или веб-приложения на сервере (без адреса самого сервера). Используется только для протоколов HTTP и HTTPS. Например, если для сервера с адресом `address` задан протокол доступа `http`, то абсолютный URL-адрес будет иметь вид `http://address/path`.
- `port` — номер порта для подключения к серверу. Если порт не задан, то используется стандартное значение для используемого протокола.
- `windowgeometry` — размер окна терминальной сессии. Может быть задан в пикселях (например, `800x600`) или в процентах от размера рабочего стола абонентского пункта (например, `80%`). Используется для протоколов RDP и ICA.
- `title` — название терминального сервера в меню. Может включать пробелы, заданные как последовательность символов `%20`.
- `user` — имя пользователя для авторизации на терминальном сервере.
- `password` — пароль пользователя для авторизации на терминальном сервере.
- `domain` — имя домена. Используется только для протоколов RDP и ICA.
- `default` — признак использования в качестве сервера по умолчанию для полноэкранного режима работы. Допустимые значения: `on` (использовать сервер по умолчанию) или `off` (не использовать сервер). Значение `on` должно быть указано только для одного сервера.
- `rdp-client` — RDP-клиент для подключения к серверу. Используется только для протокола RDP. Допустимые значения: `freerdp` или `rdesktop`. По умолчанию используется клиент FreeRDP.
- `vmware-conn-proto` — протокол для организации подключения по технологии VMware Horizon View. Допустимые значения: `pcoip` или `rdp`.
- `vmware-pool` — имя пула виртуальных рабочих столов, используемого по умолчанию при подключении по технологии VMware Horizon View.
- `ssl-verification-mode` — режим проверки подлинности SSL-сертификата при подключении по технологии VMware Horizon View. Допустимые значения: `default`, `reject-untrusted`, `warn-untrusted`, `ignore-untrusted`.
- `usb-export-technology` — технология перенаправления USB-устройств на сервер. Допустимые значения: `default`, `rdp8`, `ctxusb`, `usbredir`, `pcoip`.
- `usb-export-classes` — классы USB-устройств, разрешенные для перенаправления на сервер. Класс задается шестнадцатеричным двухсимвольным номером. Можно указать один класс или список классов через запятую.
- `usb-export-devices` — отдельные USB-устройства, разрешенные для перенаправления на сервер. Устройство задается двумя четырехсимвольными шестнадцатеричными номерами, разделенными двоеточием (например, 0000:ffff). Можно указать одно устройство или список устройств через запятую.

Примеры строк, задающих параметры терминального сервера:

- Подключение по протоколу RDP к терминальному серверу, который находится на узле ViPNet с идентификатором 15E8000A. Размер окна терминальной сессии 1024x768, название терминального сервера в меню абонентского пункта — «Main server».

  `T:rdp:0x15E8000A windowgeometry=1024x768 title=Main%20Server`

- Подключение по протоколу HTTP к серверу по адресу `http://webserver`, номер порта 8080. Для аутентификации используется имя пользователя `Smith` и пароль `qwerty`.

  `T:http:webserver port=8080 user=Smith password=qwerty`

- Подключение по протоколу RDP к пулу виртуальных рабочих столов с именем `pool1`, который находится на сервере с адресом `10.0.0.1`.

  `T:vmware-vdi:10.0.0.1 vmware-conn-proto=rdp vmware-pool=pool1`

8 Для каждого абонентского пункта задайте параметры прокси-сервера веб-браузера Firefox. Для этого нажмите кнопку IP-адреса и добавьте в список строку следующего вида:

```
:webproxy: [<параметр 1>=<значение 1>] ... [<параметр n>=<значение n>]
```

Вы можете задать следующие параметры:

- `параметр n, значение n` — необязательные параметры и их значения, перечисленные ниже:

  - `mode` — режим использования и настройки прокси-сервера. Допустимые значения: `off` (не использовать прокси-сервер) или `manual` (использовать прокси-сервер с заданными параметрами). По умолчанию прокси-сервер не используется.

  - `server_address` — протокол и параметры прокси-сервера для этого протокола. Задается в формате `<протокол>:<адрес>:<порт>` либо `<протокол>:noproxy` (равносильно заданию `mode=off`). Можно указать несколько значений через запятую. Допустимые значения протокола: `ftp`, `http`, `socks`, `ssl`, `all`.

  - `exclusion` — адрес, для которого не нужно использовать прокси-сервер. Можно указать несколько значений через запятую. В качестве адреса можно указать отдельный IP-адрес или DNS-имя, подсеть в формате CIDR или домен.

  Несколько значений, заданных в параметрах `server_address` и `exclusion`, будут применяться по порядку слева направо.

Пример строки, задающей параметры прокси-сервера для всех протоколов (`all`) и для протокола SSL (`ssl`), а также список исключений:

```
:webproxy: mode=manual server_address=all:10.0.4.10:1111,ssl:10.0.4.20:2222
exclusion=10.0.0.0/8,192.168.0.0/16,mail.infotecs.ru
```

Примечание. Вы можете задать настройки прокси-сервера сразу для всех абонентских пунктов. Для этого добавьте указанную строку в список IP-адресов координатора. Если для отдельных абонентских пунктов нужно задать индивидуальные настройки, добавьте соответствующие строки в список IP-адресов этих абонентских пунктов. Настройки, заданные для абонентского пункта, имеют приоритет над настройками, заданными для его координатора.

---

9 Для тех абонентских пунктов, которые будут подключаться к Интернету через 3G-модем, задайте оператора сети 3G, если он отсутствует в стандартном списке ПО ViPNet Terminal

(Билайн, Мегафон, МТС, Скай Линк, Verizon, Vodafone). Для этого нажмите кнопку **IP-адреса**. В списке IP-адресов задайте имена операторов сети 3G (провайдеров), услугами которых вы пользуетесь, и параметры соединения с ними. Для каждого провайдера добавьте в список строку следующего вида:

```
:P3G: name=<имя провайдера> [<параметр 1>=<значение 1>] ... [<параметр
n>=<значение n>]
```

Для каждого провайдера вы можете задать следующие параметры:

- `name` — имя провайдера (обязательный параметр).
- `параметр n, значение n` — необязательные параметры и их значения. Допустимые необязательные параметры перечислены ниже:
  - `phone` — телефон для дозвона.
  - `apn` — адрес сервера, используемого для соединения.
  - `user` — имя пользователя для авторизации при дозвоне.
  - `password` — пароль пользователя для авторизации при дозвоне.

Пример строки для оператора МТС:

```
:P3G: name=mts phone=*99***1# apn=internet.mts.ru user=mts password=mts
```

Примечание. Вы можете задать дополнительных провайдеров сразу для всех абонентских пунктов. Для этого добавьте указанную строку для каждого провайдера в список IP-адресов координатора. Если для отдельных абонентских пунктов нужно задать индивидуальные настройки, добавьте соответствующие строки в список IP-адресов этих абонентских пунктов. Настройки, заданные для абонентского пункта, имеют приоритет над настройками, заданными для его координатора.

10 Выполнив необходимые настройки сетевых узлов, в программе ViPNet Центр управления сетью в меню **Службы** выберите команду **Сформировать все справочники**. По этой команде будут сформированы и переданы в УКЦ справочники, предназначенные для создания дистрибутивов ключей сетевых узлов. При создании дистрибутивов ключи пользователя могут быть сохранены в составе дистрибутива либо перенесены на внешнее устройство.

11 Созданные дистрибутивы ключей перенесите на USB-носитель и установите справочники и ключи на сетевых узлах ViPNet Terminal.

Создание сетевых узлов в ЦУСе версии 4.x

Для создания сетевых узлов в программе ViPNet Центр управления сетью версии 4.x выполните следующие действия:

1 Создайте клиентские узлы, на которых будет использоваться ПО ViPNet Terminal. При создании зарегистрируйте клиенты на каком-либо координаторе.

Примечание. Не используйте в имени сетевого узла символ '№'. При использовании этого символа имя сетевого узла некорректно отображается при установке ключей на ViPNet Terminal.

2 На каждый клиент добавьте роль «ViPNet Terminal» или «ViPNet ThinClient» (названия одной и той же роли в разных версиях ViPNet Administrator) и настройте параметры роли. Вы можете задать параметры двумя способами:

- Централизованно для всех или для группы клиентов с ролью «ViPNet Terminal» или «ViPNet ThinClient».
- Индивидуально для каждого клиента с ролью «ViPNet Terminal» или «ViPNet ThinClient».

Также вы можете сначала настроить параметры централизованно, а затем задать индивидуальные настройки для отдельных клиентов.

3 Чтобы задать параметры роли «ViPNet Terminal» или «ViPNet ThinClient» для всех клиентов, выполните следующие действия:

3.1 Создайте шаблон сетевых узлов типа **Только клиенты**.

3.2 В настройках шаблона выберите атрибут **Роли узлов** и добавьте роль «ViPNet Terminal» или «ViPNet ThinClient».

3.3 В свойствах роли «ViPNet Terminal» или «ViPNet ThinClient» настройте следующие параметры:

- На вкладке **Сессия** настройте полномочия пользователя ViPNet Terminal и дополнительные параметры.
- На вкладке **Подключение к серверу** задайте список терминальных серверов.

4 Чтобы задать параметры роли «ViPNet Terminal» или «ViPNet ThinClient» индивидуально для клиента, выполните следующие действия:

4.1 Дважды щелкните клиент и в списке его ролей дважды щелкните роль «ViPNet Terminal» или «ViPNet ThinClient».

4.2 На вкладках **Сессия** и **Подключение к серверу** выполните настройки, как описано выше.

5 Задайте связь клиентов с терминальным сервером или координатором, который туннелирует терминальный сервер. Если требуется, свяжите клиенты с несколькими терминальными серверами.

6 Выполнив необходимые настройки сетевых узлов, в окне программы ViPNet Центр управления сетью на панели инструментов нажмите кнопку **Справочники и ключи** и в меню выберите пункт **Создать справочники**.

7 В окне **Создание справочников** нажмите кнопку **Создать для всего списка**. В результате будут сформированы и переданы в УКЦ справочники, предназначенные для создания дистрибутивов ключей сетевых узлов. При создании дистрибутивов ключи пользователя могут быть сохранены в составе дистрибутива либо перенесены на внешнее устройство.

8 Созданные дистрибутивы ключей перенесите на USB-носитель и установите справочники и ключи на сетевых узлах ViPNet Terminal.

Особенности работы с терминальным сервером

Если на терминальном сервере не установлено ПО ViPNet и он туннелируется координатором, на сервер необходимо установить криптопровайдер ViPNet CSP версии не ниже 3.2.5. Если терминальный сервер является защищенным узлом ViPNet, установка дополнительных программ не требуется, так как криптопровайдер входит в состав ПО ViPNet Client и ViPNet Coordinator.

Если во время работы в терминальной сессии пользователям ViPNet Terminal требуется использовать сертификаты электронной подписи, эти сертификаты следует записать на внешнее устройство аутентификации. Для работы с внешними устройствами аутентификации на терминальном сервере должны быть установлены драйверы устройств.

Если во время работы в терминальной сессии требуется использовать принтер, подключенный к компьютеру с ПО ViPNet Terminal, на терминальном сервере должен быть установлен драйвер принтера.

Если во время работы в терминальной сессии требуется использовать съемный носитель, подключенный к компьютеру с ПО ViPNet Terminal, на терминальном сервере должно быть разрешено перенаправление съемных носителей.

A

Возможные неполадки и способы их устранения

При загрузке компьютера возникает ошибка

Если при загрузке компьютера на экране появляется информация об ошибке `Superblock last mount time <время и дата> is in the future`, проверьте, верно ли заданы дата и время в настройках BIOS.

При каждой загрузке на сертифицированной платформе возникает предложение восстановить параметры BIOS

Если при загрузке на сертифицированной платформе возникает предложение восстановить параметры BIOS, и при согласии с восстановлением после перезагрузки появляется вновь, то для решения данной проблемы при загрузке войдите в BIOS и установите вручную пароль Администратора `vipnet`.

Потеря подключения устройства аутентификации

Если во время работы в терминальной сессии перестало определяться устройство аутентификации (криптотокен), подключенное к вашему компьютеру, выполните следующие действия:

1. Отключите устройство аутентификации от компьютера.
2. В течение 30 секунд снова подключите устройство.

Не удается выполнить аутентификацию с помощью eToken PRO Java 72K

Если вы подключаетесь к терминальному серверу по протоколу RDP и используете для аутентификации на сервере устройство eToken PRO Java 72K, после завершения терминальной сессии и повторного подключения устройство аутентификации может не определяться.

Для решения проблемы используйте один из следующих способов:

- Для завершения терминальной сессии в меню **Пуск** выберите пункт **Завершение работы** > **Выйти из системы** (**Shut down** > **Log off**). Тогда при следующем подключении к терминальному серверу будет возможна аутентификация с помощью eToken PRO Java 72K.
- Установите на терминальном сервере программное обеспечение SafeNet Authentication Client.

Не удается установить справочники и ключи из-за предложения восстановить BIOS

Внимание! ОАО «ИнфоТеКС» не гарантирует работу ViPNet Terminal при изменении настроек BIOS.

В случае если настройки BIOS по каким-либо причинам изменены, при попытке установки справочников и ключей появляется окно с сообщением о необходимости восстановления BIOS. В этом окне необходимо нажать кнопку **Восстановить BIOS и перезагрузить**. При попытке игнорировать это окно произойдет перезагрузка ViPNet Terminal и окно появится вновь.

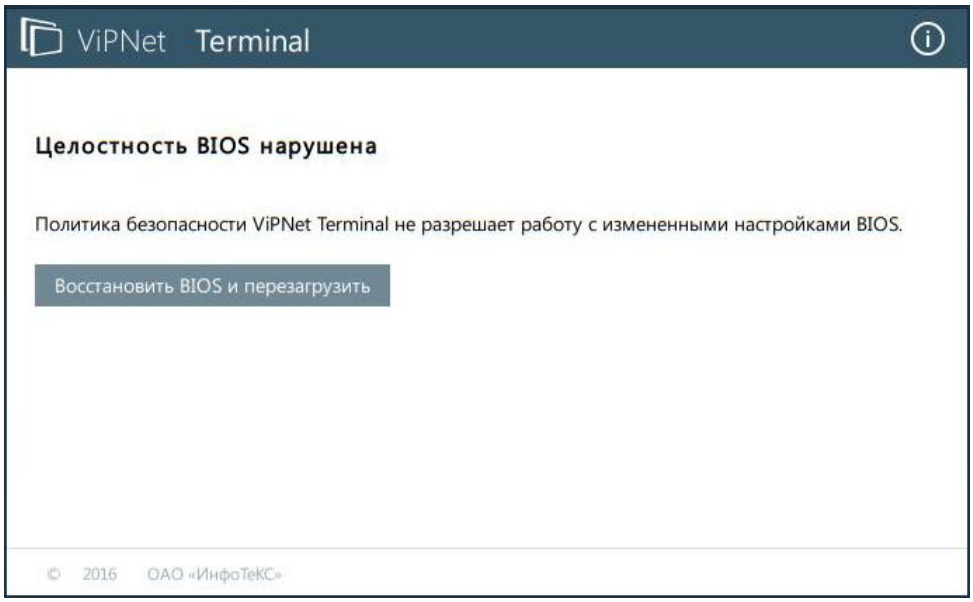

Рисунок 5. Предложение восстановить настройки BIOS

Не удается использовать съемные носители в терминальной сессии

Если в настройках ViPNet Terminal разрешено перенаправление съемных носителей на терминальный сервер, но вы не видите подключенный съемный носитель в терминальной сессии, для решения проблемы включите перенаправление звуковых устройств. Эта неполадка может возникать при подключении к терминальному серверу Windows Server 2008 и Windows Server 2012.

Дефекты изображения на экране компьютера

Если вы подключаетесь к терминальному серверу по протоколу RDP, на экране компьютера могут появляться различные артефакты, например мерцание символов. Чтобы изображение в окне не искажалось, мы рекомендуем задавать значения ширины и высоты окна, кратные четырем.

Не работают подключенные к компьютеру USB-устройства

Если после подключения к компьютеру USB-устройство (например, аудиогарнитура или съемный носитель) недоступно в терминальной сессии, завершите эту терминальную сессию и запустите ее снова.

Примечание. Чтобы завершить терминальную сессию, недостаточно закрыть соответствующее окно ViPNet Terminal. Используйте штатные средства операционной системы, установленной на удаленном рабочем столе. Например, если на удаленном рабочем столе установлена операционная система Windows 7, в меню **Пуск** выберите пункт **Выйти из системы**.

Также убедитесь, что разрешено перенаправление вашего устройства на терминальный сервер.

Не удается включить 3G/LTE-модем

Модемы, работающие в режиме RNDIS (например, в этом режиме могут работать модели Huawei 3572s-152, Yota WLTUBA-107), не включаются с помощью стандартных команд включения модема `inet usb-modem mode on` или `inet lte-modem mode on`. Вместо этого они определяются как сетевой интерфейс Ethernet с именем `eth1` или `eth2`. Чтобы предварительно настроить и включить такой модем, выполните следующие действия:

1. Подключите модем к компьютеру.
2. Просмотрите параметры сетевых интерфейсов с помощью команды:

   ```
   vpnshell> inet show interface
   ```

   На экране отобразится информация о сетевом интерфейсе `eth0`, а также о новом интерфейсе (`eth1` или `eth2`).
3. Остановите демон `iplircfg` с помощью команды:

   ```
   vpnshell> iplir stop
   ```
4. Перейдите в режим администратора с помощью команды `enable` и откройте для редактирования конфигурационный файл `iplir.conf` с помощью команды:

   ```
   vpnshell# iplir config
   ```
5. Добавьте секцию `[adapter]` следующего вида (приведен пример для случая, когда новый интерфейс — `eth1`):

   ```
   [adapter]
   name = eth1
   allowtraffic = on
   ```
6. Чтобы сохранить изменения в конфигурационном файле, нажмите сочетание клавиш **Ctrl+O**. Затем нажмите клавишу **Enter**.
7. Чтобы закрыть файл, нажмите сочетание клавиш **Ctrl+X**.
8. Запустите демон `iplircfg` с помощью команды:

   ```
   vpnshell> iplir start
   ```
9. Запустите модем с помощью команды (приведен пример для случая, когда новый интерфейс — `eth1`):

   ```
   vpnshell> inet ifconfig eth1 up
   ```

В результате 3G/LTE-модем будет запущен. Для его остановки используйте команду:

```
vpnshell> inet ifconfig eth1 down
```

Внимание! При использовании таких модемов в веб-интерфейсе может отображаться неверное состояние подключения.

Не определяется 3G-модем

Если в течение одной минуты после подключения 3G-модема к компьютеру в окне настройки ViPNet Terminal не появилась вкладка **3G-модем**, отключите модем от компьютера, затем подключите его снова.

Модем также может не определиться в случае, если после его подключения ViPNet Terminal перезагружался. Это связано с тем, что с USB-порта не снимается питание, и поэтому 3G-модем не может перейти в начальное состояние, которое требуется для его корректной работы. В этом случае также отключите модем от компьютера, затем подключите его снова.

Не удается подключиться к терминальному серверу Citrix по протоколу ICA

Если на терминальном сервере установлено программное обеспечение Citrix XenDesktop 7.x, то в настройках подключения к терминальному серверу необходимо установить Режим киоска, или использовать протокол HTTP или HTTPS. При подключении по HTTP/HTTPS выполните следующие настройки:

- В качестве адреса терминального сервера укажите IP-адрес или DNS-имя контроллера Delivery Controller.
- В качестве относительного URL-адреса укажите адрес `/Cirtix/StoreWeb`.

При подключении к терминальному серверу Citrix окно с терминальной сессией выходит за рамки экрана

Если при подключении к терминальному серверу Citrix окно с терминальной сессией выходит за рамки экрана, обратитесь к администратору терминального сервера.

В этом случае на терминальном сервере необходимо с помощью функции поиска операционной системы найти файл `default.ica` (например, этот файл может находиться в папке

`C:\inetpub\wwwroot\Citrix\Store\App_Data`) и в секции `[Application]` этого файла добавить следующие строки:

```
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
```

Не удается подключиться по протоколу RDP к терминальному серверу, использующему SSL-сертификаты

Если при попытке RDP-подключения к терминальному серверу, на котором настроено использование SSL-сертификатов, появляется сообщение о невозможности установить соединение, выполните одно из действий:

- В веб-интерфейсе на странице подключения к терминальному серверу установите флажок **Не проверять подлинность сертификата сервера**.
- В командном интерпретаторе выполните команду:
  `terminal server set rdp-ssl-verification-mode ignore-untrusted`.

После этого повторите попытку подключения.

Если проблему удалось решить указанным образом, обратитесь к администратору терминального сервера с просьбой проверить корректность своего сертификата, а также сертификата издателя или цепочки сертификации.

Составное устройство хранения данных перенаправляется некорректно

Если вы используете устройство, одна часть памяти которого предназначена для хранения ключей электронной подписи, а вторая — для хранения файлов (например, Aladdin eToken PRO Java NG-FLASH), для корректного перенаправления выполните одно из следующих действий:

- В настройках перенаправления (см. документ «ViPNet Terminal. Руководство администратора», раздел «Настройка перенаправления устройств ») одновременно задайте следующие типы устройств:
  - `token` (в веб-интерфейсе — **Устройства аутентификации**);
  - `usb` (в веб-интерфейсе — **Съемные носители**).
- Используйте команды для перенаправления USB-устройств (см. документ «ViPNet Terminal. Руководство администратора», раздел «Настройка перенаправления USB-устройств») и задайте класс устройства, а также идентификатор устройства.

Не удается перенаправить принтер HP Laserjet Professional p1102/p1102w

Если после установки принтера HP Laserjet Professional p1102/p1102w его не удается перенаправить на терминальный сервер, выполните следующие действия:

1 Обновите прошивку принтера до последней версии. Для этого подключите принтер к компьютеру под управлением операционной системы Windows, а затем скачайте и запустите утилиту для обновления FW_Update_Security http://ftp.hp.com/pub/softlib/software12/COL32489/bi-80484-9/LJP1100_P1560_P1600_FW_Update_Security.exe.

2 Установите принтер (см. документ «ViPNet Terminal. Руководство пользователя», раздел «Установка принтера»), при этом на странице **Доступные принтеры** выполните следующие действия:

2.1 Выберите принтер, в названии которого присутствует слово USB.

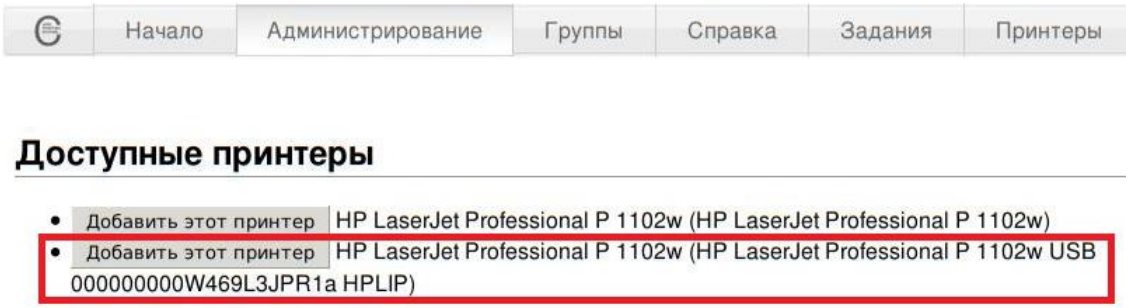

Рисунок 6. Выбор принтера HP Laserjet Professional p1102w

2.2 В списке **Модель** выберите модель, указанную на рисунке (для модели p1102 — аналогичную без буквы w).

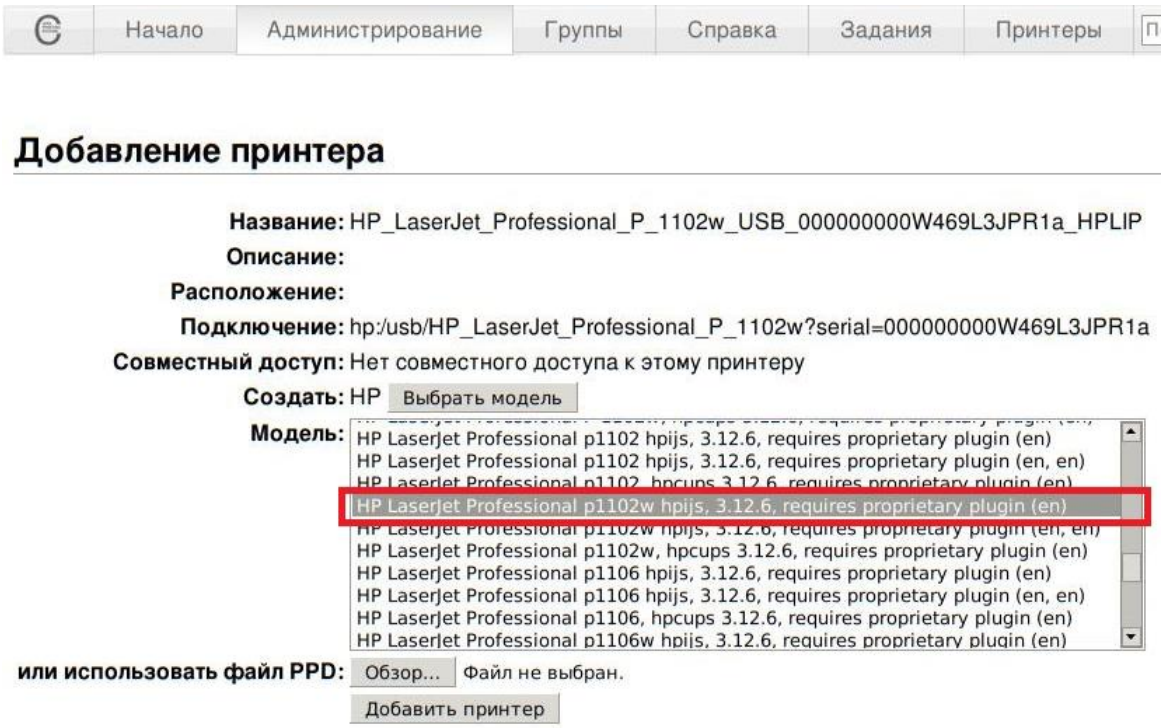

Рисунок 7. Выбор модели при настройке принтера HP Laserjet Professional p1102w

В результате такой установки принтер будет корректно перенаправляться на терминальный сервер.

Не удается возобновить печать на принтере HP LaserJet Professional p1102/p1102w

По умолчанию принтер HP LaserJet Professional p1102/p1102w переходит в режим сна через 4 часа простоя. При этом система помечает принтер как отсутствующий и помещает все задания печати в очередь. Чтобы продолжить печать, выполните следующие действия:

1. В многооконном режиме работы веб-интерфейса ViPNet Terminal нажмите кнопку .
2. В открывшемся меню выберите пункт **Принтеры**. В окне веб-браузера Firefox будет открыта страница системы печати CUPS.
3. На вкладке **Администрирование** нажмите кнопку **Управление принтерами**.
4. В открывшемся окне напротив принтера HP LaserJet Professional p1102/p1102w в списке **Обслуживание** выберите пункт **Возобновить печать**.

В результате печать будет возобновлена.

B

Список поддерживаемого оборудования

В данном приложении приведен список оборудования, поддержка которого была успешно протестирована.

Поддерживаемые 3G/4G-модемы

AnyDATA ADU-510A («Скай Линк»)

Huawei E150, E1552, E171 (МТС)

Huawei E1550, E171, E173, E1750, E1820, E303, E3276, E352, E352b, E367 («Мегафон»)

Huawei E3276 («Мегафон» 4G/LTE M150-1)

Huawei 3572s-152 («Мегафон» M-150)

Huawei E171 («Билайн»)

Huawei E369

Huawei E398 (Deutsche Telekom Speedstick LTE III)

Huawei EM770W

Huawei K4505 (Vodafone)

Yota WLTUBA-107

Поддерживаемые сетевые карты Wi-Fi

Atheros AR5001

Atheros AR9285

Broadcom BCM4313

Intel Centrino Advanced-N 6250 AGN

Intel PRO/Wireless 2200

Intel PRO/Wireless 3945ABG

Realtek 8188CE

Поддерживаемые графические адаптеры

ATI Radeon Mobility HD 5000

ATI Radeon Mobility X600

Intel N10

NVidia GeForce 410M

NVidia GeForce GS8400M

NVidia Ion

Поддерживаемые принтеры

Brother HL-2132R

Canon i-SENSYS MF4410

Canon i-SENSYS MF4430

HP DeskJet 2000

HP LaserJet 4250

HP LaserJet MFP 400 M425dn

HP LaserJet P1606DN

HP LaserJet Professional p1102/p1102w

Kyocera ECOSYS FS-1370DN

Olivetti PR2 PLUS

Samsung ML 1710

Xerox Phaser 3010

Xerox Phaser 3121

Xerox Phaser 3124

Xerox Phaser 3130

Xerox Phaser 3140

Поддерживаемые USB-гарнитуры

Plantronics D40

Plantronics P240M

Logitech USB Headset

Поддерживаемые криптотокены и смарт-карты

Aladdin eToken PRO (в том числе NG-FLASH) (0529:0600)

Aladdin eToken PRO Java (в том числе NG-FLASH) (0529:0620)

eToken ГОСТ (0529:0620, 24dc:0101)

JaCarta ГОСТ (24dc:0101)

JaCarta ГОСТ с FLASH (24dc:100f)

USB ЭЦП (в том числе FLASH) (0a89:0030 кроме версии 55.02.19.00)

Поддерживаемые считыватели смарт-карт

OMNIKEY CardMan 5121

Поддерживаемые сканеры штрих-кодов

Honeywell MS9500

Symbol Technologies Bar Code Scanner (05e0:1200)

C

История версий

Версия 4.1.7

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Terminal версии 4.1.7 по сравнению с версией 4.1.6.

- **Новая аппаратная платформа**

  Начиная с версии 4.1.7, ViPNet Terminal поддерживает работу на аппаратной платформе TONK TN1902 (см. «Аппаратная платформа TONK TN1902» на стр. 23).

Версия 4.1.6

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Terminal версии 4.1.6 по сравнению с версией 4.1.5.

- **Новая версия ядра Linux**

  В ПО ViPNet Terminal 4.1.6 используется ядро Linux версии 4.4.

- **Поддержка работы с двумя мониторами**

  ViPNet Terminal 4.1.6 позволяет одновременное подключение двух мониторов с одинаковым разрешением. При подключении второго монитора рабочий стол ViPNet Terminal расширяется автоматически. Окно любой программы. используемой в ViPNet Terminal (например, клиента RDP, окна настройки и так далее), также может быть расширено на два монитора.

Версия 4.1.5

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Terminal версии 4.1.5 по сравнению с версией 4.1.4.

- **Защита RDP-подключений к терминальному серверу по протоколу TLS/SSL**

  В новой версии ViPNet Terminal при подключении к терминальному серверу по протоколу RDP выполняется проверка SSL-сертификата. По умолчанию в случае, если проверить подлинность SSL-сертификата не удается, подключение к серверу не происходит. Если вы хотите разрешить подключение к серверу в любом случае, даже если не удалось проверить подлинность SSL-сертификата, выполните команду `terminal server set rdp-ssl-verification-mode ignore-untrusted` либо установите соответствующий флажок в веб-интерфейсе ViPNet Teriminal.

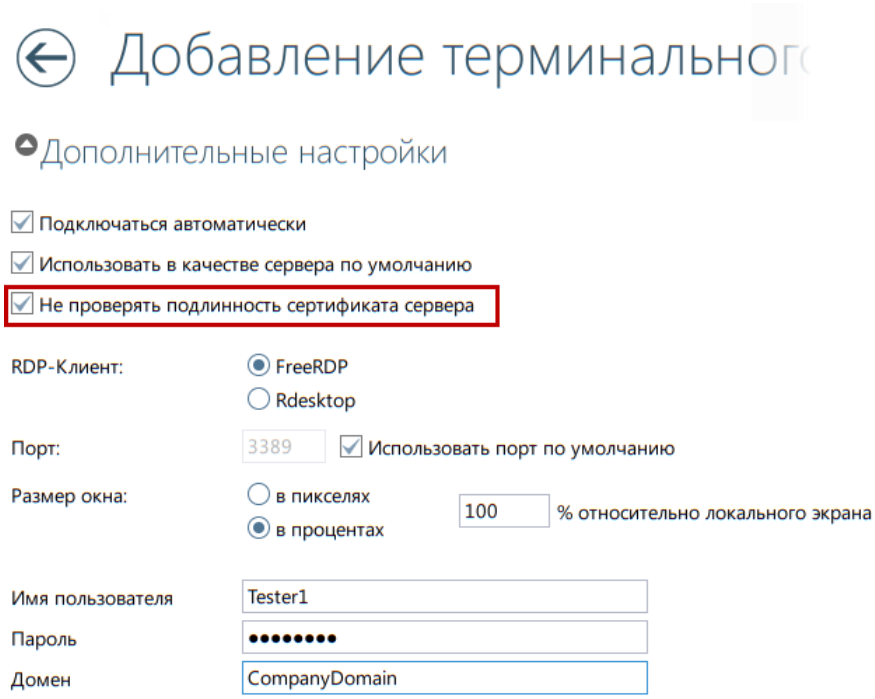

  Рисунок 8. Отключение проверки SSL- сертификата при RDP-подключении

- **Переименование команды, которая используется для задания режима проверки подлинности SSL-сертификата при подключении к терминальному серверу по протоколу VMware VDI**

  Ранее защита по протоколу TLS/SSL обеспечивалась только при подключении к терминальным серверам VMware. Так как в новой версии ViPNet Terminal такая защита соединения может обеспечиваться и при подключении по протоколу RDP, во избежание неверного понимания команда `terminal server set ssl-verification-mode`, которая использовалась для задания режима проверки подлинности SSL-сертификата при подключении к терминальному серверу VMware, была переименована в `terminal server set vdi-ssl-verification-mode`.

Версия 4.1.4

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Terminal версии 4.1.4 по сравнению с версией 4.1.3.

- **Доступ к виртуальным рабочим столам с помощью протокола IBS VDI**

  В новой версии ViPNet Terminal вы можете устанавливать соединение с терминальными серверами, на которых используются решения, работающие по технологии IBS Parallels VDI. Такая возможность ранее предоставлялась в версии 4.1.2, однако в новой версии вы можете также задать следующие дополнительные настройки терминальных сессий IBS VDI:

  - Включение и отключение использования брокера соединений IBS VDI в качестве шлюза. При включении этой возможности во время терминальной сессии трафик между ViPNet Terminal и терминальным сервером будет передаваться не напрямую, а через брокер соединений.
  - Включение и отключение использования резервного брокера соединений для организации отказоустойчивого соединения.
  - Выбор типа подключения к сети для достижения максимального быстродействия при взаимодействии с терминальным сервером.
  - Включение и отключение использования механизма перенаправления принтера Microsoft Easy Print.
  - Перенаправление устройств, подключенных к COM-порту, на терминальный сервер.

- **Работа в качестве клиента видеоконференций Vinteo**

  В веб-интерфейс новой версии ViPNet Terminal встроен клиент Vinteo, разработанный одноименной компанией, с помощью которого вы можете подключаться к серверу Vinteo и участвовать в видеоконференциях.

  Поддержка новых

- **Поддержка терминальных серверов VMware Horizon View 7**

  В новой версии ViPNet Terminal вы можете подключаться к виртуальным рабочим столам, работающим по технологии VMware Horizon View версии 7.

- **Поддержка новых устройств**

  В новой версии ViPNet Terminal добавлена поддержка следующих устройств:

  - USB-гарнитура Plantronix P240M.
  - 3G/4G-модем Huawei 3572s-152 («Мегафон» M-150).

Версия 4.1.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Terminal версии 4.1.3 по сравнению с версией 4.1.2.

- **Изменено название продукта ViPNet ThinClient**

  Продукту ViPNet ThinClient присвоено название ViPNet Terminal.

- **Возможность подключения к терминальным серверам Citrix XenDesktop 7.x в режиме киоска (Kiosk Mode)**

  В предыдущих версиях для подключения к терминальным серверам Citrix XenDesktop 7.x рекомендовалось использовать протокол HTTP или HTTPS, указав в качестве относительного пути к хранилищу путь `/Citrix/Store/StoreWeb/`. В новой версии ViPNet Terminal для подключения к терминальным серверам Citrix XenDesktop 7.x также добавлена возможность организации соединения по протоколу ICA в режиме киоска (Kiosk Mode), указав для доступа к настройкам протокол HTTP или HTTPS.

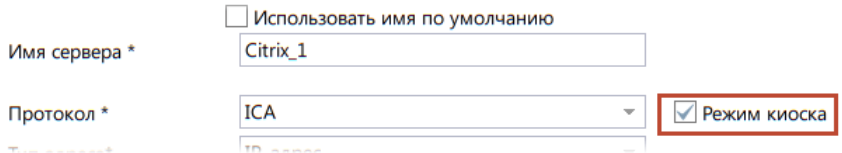

  Рисунок 9. Настройка подключения к терминальному серверу Citrix в «режиме киоска»

- **Прогрессивная задержка при вводе неверного пароля или ПИН-кода**

  Для предотвращения возможности подбора пароля методом перебора в новой версии ViPNet ThinClient после ввода неверного пароля или ПИН-кода требуется подождать несколько секунд. Каждый раз при последующем неверном вводе необходимая задержка увеличивается. Если неверно ввести пароль или ПИН-код 10 раз подряд, ViPNet Terminal выключается.

Версия 4.1.2

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 4.1.2 по сравнению с версией 4.1.1.

- **Работа в качестве клиента видеоконференций TrueConf**

  В веб-интерфейс новой версии ViPNet ThinClient встроен клиент TrueConf, разработанный одноименной компанией, с помощью которого вы можете подключаться к серверу TrueConf и участвовать в видеоконференциях.

- **Использование USB-накопителей с файловыми системами ext3 и ext4**

  Раньше для таких операций, как установка справочников и ключей, обновление программного обеспечения, а также резервное копирование и восстановление настроек, могли использоваться USB-накопители с файловой системой FAT32, NTFS или ext2. Новая версия ViPNet ThinClient может также работать с USB-накопителями, отформатированными в файловой системе ext3 или ext4.

Версия 4.1.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 4.1.1 по сравнению с версией 4.1.0.

- **Настройка перенаправления устройств с помощью веб-интерфейса**

  Раньше настроить перенаправление подключенных устройств на терминальный сервер администратор ViPNet ThinClient мог только с помощью командного интерпретатора. В новой версии ViPNet ThinClient перенаправление устройств вы можете настроить, войдя в веб-интерфейс в режиме администратора.

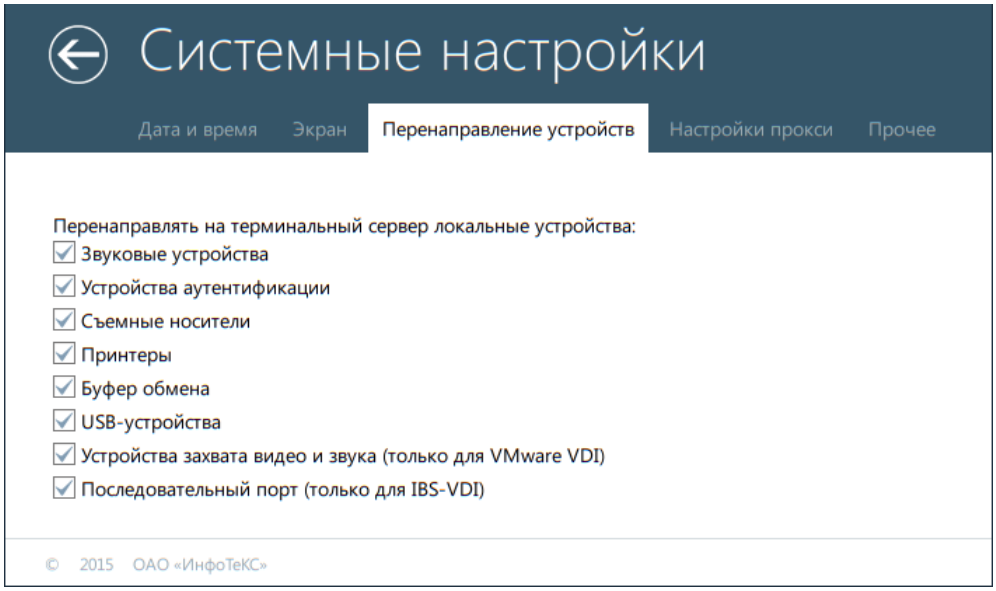

  Рисунок 10. Настройка перенаправления устройств на терминальный сервер

- **Перенаправление веб-камер на терминальный сервер с помощью протокола VMware VDI**

  В новой версии ViPNet ThinClient вы можете настроить перенаправление видео- и аудиопотоков с веб-камер на терминальный сервер в терминальных сессиях, организованных по протоколу VMware VDI, то есть с использованием технологии VMware View/Horizon.

- **Использование USB-накопителей с файловой системой NTFS**

  Раньше для таких операций, как установка справочников и ключей, обновление программного обеспечения, а также резервное копирование и восстановление настроек, могли использоваться USB-накопители с файловой системой FAT32 или ext2. Новая версия ViPNet ThinClient может также работать с USB-накопителями, отформатированными в файловой системе NTFS.

- **Сглаживание шрифтов по методу ClearType в RDP-сессиях**

  Раньше для терминальных сессий сглаживание шрифтов не применялось. В новой версии ViPNet ThinClient при установлении соединения с терминальным сервером по протоколу RDP для отображения шрифтов по умолчанию используется метод сглаживания ClearType. При необходимости вы можете отключить сглаживание.

- **Автоматическое скрытие панели задач**

Для увеличения рабочего пространства на экране в ViPNet ThinClient 4.1.1 появилась возможность скрывать панель задач. Панель появляется только при наведении указателя мыши на нижнюю границу экрана.

- **Возможность отслеживания, не извлечено ли из разъема компьютера внешнее устройство с ключами пользователя**

  Во избежание несанкционированного доступа, теперь, в случае аутентификации пользователя по внешнему устройству, ViPNet ThinClient может отслеживать, не отключено ли это устройство. Если обнаружено, что внешнее устройство отключено, компьютер автоматически выключится.

- **Запрос пароля пользователя при переходе из графического интерфейса в командный интерпретатор**

  Чтобы ограничить доступ пользователя ViPNet Terminal к настройкам, выполняемым с помощью командного интерпретатора, теперь вы можете настроить запрос пароля пользователя при попытке перехода в командный интерпретатор из графического интерфейса. Администратор ViPNet ThinClient может включить или отключить эту функцию в веб-интерфейсе или в командном интерпретаторе.

- **Поддержка принтера Olivetti PR2 PLUS**

  В список поддерживаемого оборудование добавлен принтер Olivetti PR2 PLUS.

Версия 4.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 4.1.0 по сравнению с версией 3.4.0.

- **Изменено название продукта ViPNet Terminal**

  Продукту ViPNet Terminal присвоено новое название — ViPNet ThinClient.

- **Отказ от поддержки устройства МАРШ!**

  Использование устройства МАРШ! в качестве загрузочного диска более не поддерживается. Таким образом, теперь ViPNet ThinClient поставляется в трех вариантах исполнения.

- **Веб-интерфейс для работы с сетевым экраном и списком узлов защищенной сети**

  Раньше настройка сетевого экрана осуществлялась только с помощью командной консоли, теперь появилась возможность настраивать сетевые фильтры и работать со списком узлов защищенной сети ViPNet с помощью удобного веб-интерфейса.

Рисунок 11. Новые возможности веб-интерфейса ViPNet Terminal 4.1

- **Режим пользователя и администратора для работы с веб-интерфейсом**

  Раньше пользователю были доступны все настройки, выполняемые с помощью веб-интерфейса. В новой версии ViPNet ThinClient, чтобы создавать и редактировать сетевые фильтры и группы объектов, необходимо перейти в веб-интерфейсе в режим администратора, указав пароль администратора сетевого узла.

- **Конфигурации сетевого экрана**

  В новой версии ViPNet ThinClient пользователь может переключаться между предустановленными конфигурациями сетевого экрана, включающими наборы параметров работы узла ViPNet Terminal в сети. Например, выбирая соответствующие конфигурации, пользователь может оперативно блокировать весь сетевой трафик, проходящий через сетевой узел, запрещать Интернет-трафик и так далее.

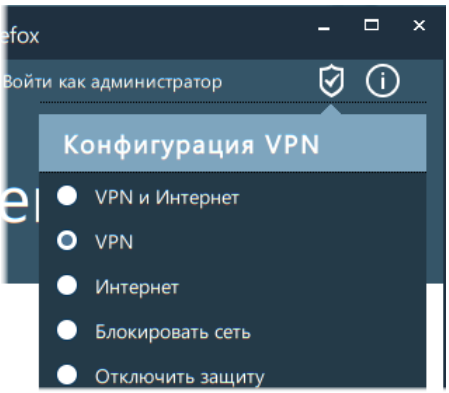

Рисунок 12. Смена конфигураций сетевого экрана ViPNet Terminal

- **Управление настройками модуля MFTP с помощью команд**

  Раньше настройка транспортного модуля осуществлялась путем редактирования конфигурационного файла `mftp.conf`, который мог иметь большой размер, и работа с ним в этом случае была затруднительна. Теперь управление настройками MFTP осуществляется с помощью специальных команд группы `mftp`. Данная возможность позволяет настраивать параметры транспортного модуля по отдельности без необходимости поиска нужной информации, также для удобства при вводе команд можно использовать подсказку.

- **Создание и настройка сетевых фильтров с помощью команд**

  В ViPNet ThinClient 4.1 был изменен механизм управления сетевыми фильтрами. Ранее все параметры фильтрации трафика задавались в конфигурационных файлах `firewall.conf` и `iplir.conf` соответственно. Теперь работа с сетевыми фильтрами выполняется с помощью командного интерпретатора.

- **Работа с группами объектов**

  Теперь вы можете объединять однотипные объекты в именованные группы. Группы объектов облегчают ввод условий при создании сетевых фильтров, если в них требуется указать целый ряд объектов одного типа. Например, если требуется создать несколько сетевых фильтров, в которых нужно указать IP-адреса сегмента сети, вы можете предварительно создать группу этих IP-адресов и далее добавлять ее в условия фильтров.

- **Поддержка расписаний**

  Появилась возможность привязывать действие сетевых фильтров к определенным временным интервалам — применять фильтры по расписанию. Например, вы можете создать сетевой фильтр, который будет блокировать доступ к некоторым веб-ресурсам в рабочее время в будние дни.

- **Обновление списка поддерживаемого оборудования**

  В список поддерживаемого оборудования были добавлены новые устройства.

- **Отказ от режимов безопасности**

  В ViPNet ThinClient 4.1 режимы безопасности не используются (см. глоссарий, стр. 63). Необходимый уровень безопасности можно настроить, создав соответствующие сетевые фильтры.

- **Изменения в мастере установки ключей**

  В мастере установки ключей при аутентификации с помощью внешнего устройства теперь требуется помимо ПИН-кода вводить пароль пользователя сетевого узла.

- **Изменение комплекта документации**

  Для ViPNet ThinClient 4.1 изменен комплект документации. Теперь документов больше, при этом объем некоторых документов стал меньше. Например, значительно сократился объем руководства администратора, так как из него удалено описание команд и описание конфигурационных файлов. Теперь эти описания содержатся в отдельных документах.

  Кроме того, в руководствах администратора и пользователя использован новый подход к описанию сценариев, который учитывает целевую аудиторию. Теперь в руководстве администратора приведено выполнение сценариев с помощью команд и в отдельных случаях — через веб-интерфейс (для тех сценариев, которые доступны в веб-интерфейсе только администратору). В руководстве пользователя приведено выполнение сценариев только через веб-интерфейс.

  Состав нового комплекта документации и содержание отдельных документов приведены в разделе Навигатор по документации (на стр. 12).

Версия 3.4.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 3.4.0 по сравнению с версией 3.3.0.

- **Возможность немедленной очистки очереди печати**

  Реализована возможность немедленной очистки очереди печати при перезапуске графической сессии с помощью сочетания клавиш **Ctrl+Alt+Backspace**.

- **Поддержка принтеров Canon**

  Список поддерживаемых принтеров пополнился двумя моделями: Canon i-SENSYS MF4410 и Canon i-SENSYS MF4430.

Версия 3.3.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 3.3.0 по сравнению с версией 3.2.0.

- **Возможность подключения к инфраструктуре виртуальных рабочих столов по технологии VMware Horizon View**

  Реализована возможность подключения к инфраструктуре виртуальных рабочих столов (VDI — Virtual Desktop Infrastructure), развернутой на терминальном сервере. В настройках ViPNet Terminal вы можете указать пул рабочих столов для автоматического подключения, а также протокол подключения — RDP или PCoIP.

- **Возможность настройки параметров прокси-сервера веб-браузера**

  Реализована возможность задания прокси-сервера веб-браузера Firefox. Теперь вы можете включить или отключить использование прокси-сервера, а также указать разные адреса прокси-серверов для отдельных протоколов подключения.

- **Поддержка перенаправления буфера обмена и USB-устройств**

  Добавлена поддержка перенаправления буфера обмена и USB-устройств (веб-камер, сканеров и подобных устройств с USB-подключением). Перенаправление буфера обмена позволяет производить обмен данными между разными терминальными сессиями при подключении к серверу по протоколу RDP. Для перенаправления USB-устройств вы можете указать как отдельные устройства, так и целый класс устройств.

- **Изменение имени пользователя при подключении к ViPNet Terminal по протоколу SSH**

  Ранее для аутентификации пользователя при подключении к ViPNet Terminal по протоколу SSH использовалось имя `vipnet`. Теперь вместо этого имени используется имя `user`.

- **Изменение пароля для защиты файла экспорта**

  Ранее при аутентификации пользователя с помощью внешнего устройства для защиты файла экспорта использовался пароль `vipnet`. Теперь для защиты файла экспорта используется пароль `vbepass`.

- **Локализация интерфейса на различные языки и возможность изменения языка**

  Выполнена локализация интерфейса ViPNet Terminal на различные языки. Существующие локализации отображаются в интерфейсе, и теперь вы можете изменить язык. Поддерживаются следующие языки: русский, английский, немецкий, французский, испанский, португальский.

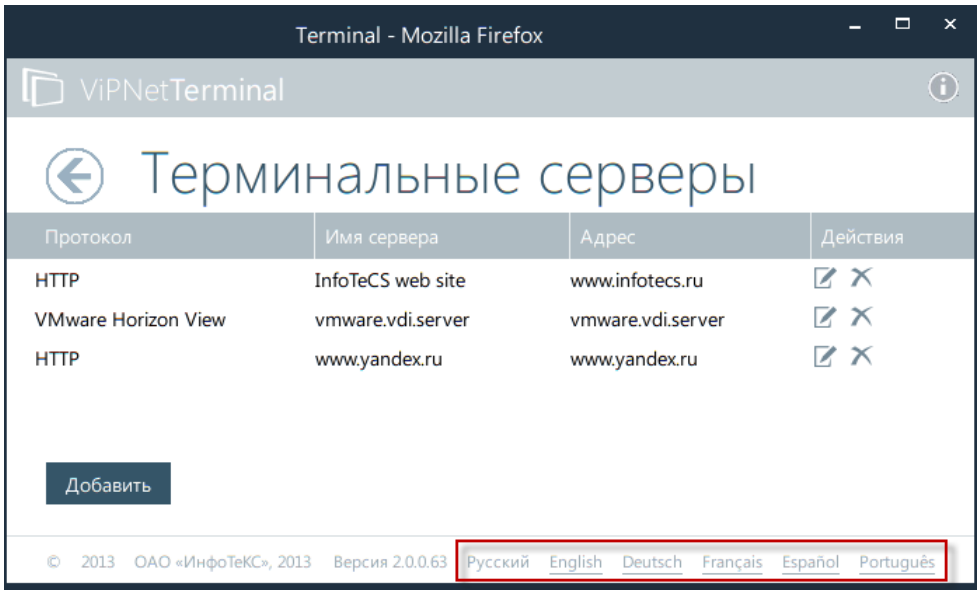

Рисунок 13. Поддерживаемые языки интерфейса

Версия 3.2.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 3.2.0 по сравнению с версией 3.1.0.

- **Обновление веб-интерфейса**

  Изменен внешний вид и повышено удобство использования веб-интерфейса, с помощью которого вы можете настроить ViPNet Terminal.

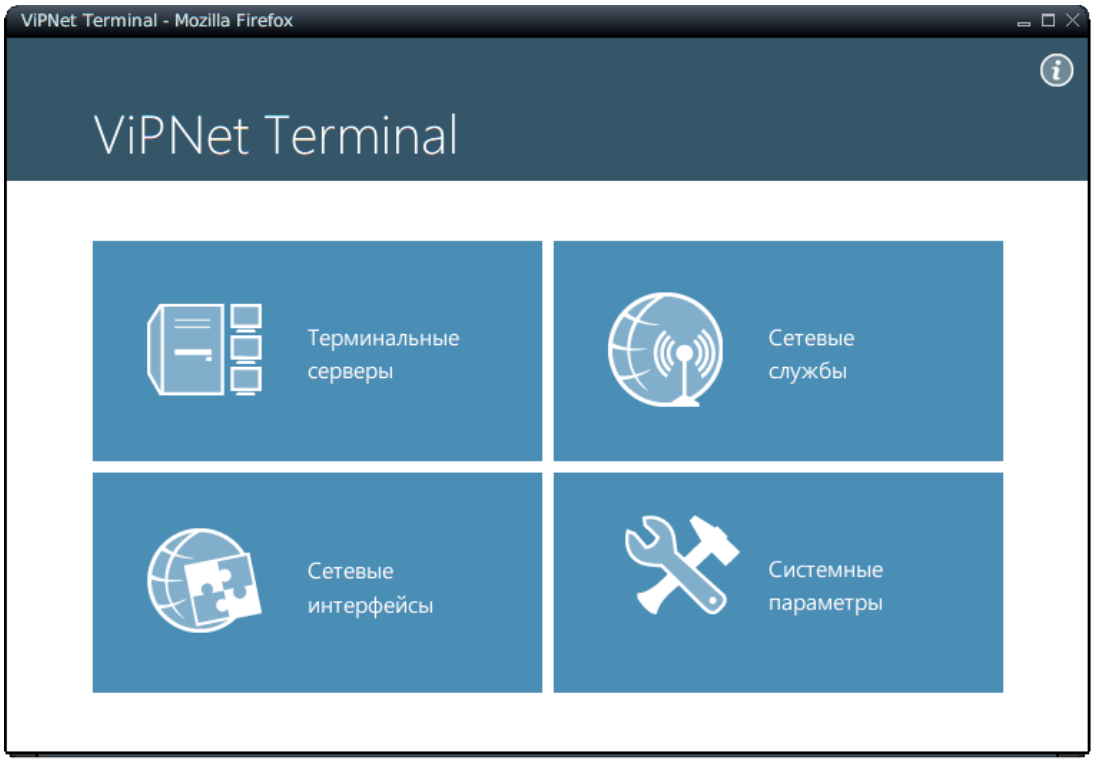

Рисунок 14. Начальная страница настройки ViPNet Terminal 3.2

- **Расширен список поддерживаемого оборудования**

  Добавлена поддержка считывателя смарт-карт OMNIKEY CardMan 5121 и сканера штрих-кодов Honeywell MS9500.

- **Запоминание сетей Wi-Fi**

  Программное обеспечение ViPNet Terminal автоматически запоминает параметры сетей Wi-Fi, к которым вы подключаетесь. При повторном подключении к сети не требуется вводить пароль.

- **Новый RDP-клиент по умолчанию**

  Теперь для подключения к терминальным серверам по протоколу RDP по умолчанию используется RDP-клиент FreeRDP, который обладает более богатыми возможностями, чем использовавшийся ранее Rdesktop. Однако в случае необходимости вы можете использовать клиент Rdesktop.

- **Постепенный переход на использование ключей нового формата**

Начиная с версии 3.2, ограничивается поддержка ключей, созданных с помощью ПО ViPNet Administrator устаревших версий 2.8.x. Последующие версии ViPNet Terminal не будут поддерживать работу с такими ключами, и для возможности обновления ПО ViPNet Terminal необходимо будет использовать ПО ViPNet Administrator версии не ниже 3.1.x.

Версия 3.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 3.1.0 по сравнению с версией 3.0.0.

- Реализован веб-интерфейс для настройки ViPNet Terminal. Теперь основные настройки можно задать не только с помощью команд, но и через веб-браузер в удобном для пользователей виде.
- Реализована возможность одновременного подключения к нескольким терминальным серверам. Управлять списком доступных серверов и параметрами подключения можно локально на терминале или удаленно с помощью программы ViPNet Центр управления сетью. Список серверов, сформированный в программе ViPNet Центр управления сетью и принятый на узле, полностью заменяет текущий список серверов.
- Переработан набор команд для управления списком терминальных серверов и параметрами подключения к ним. Появилась возможность задать параметры подключения для нескольких терминальных серверов, подключиться к ферме Citrix, указать сервер по умолчанию и другие возможности.
- Добавлена возможность включать и отключать использование USB-модема с помощью команды `inet usb-modem mode`. При отключении модем не будет использоваться для установления соединения.
- Реализована возможность работы в многооконном режиме. Этот режим позволяет использовать экран всем соединениям с терминальными серверами, если их несколько. Таким образом, при одновременном подключении к нескольким серверам на экране будет находиться несколько окон, соответствующих подключениям, с возможностью переключения с одного окна на другое. Для установки многооконного режима используется команда `terminal set multiwindow mode`.
- Реализована возможность электронной подписи документов в режиме онлайн при помощи устройства аутентификации. Вы можете использовать данную возможность в веб-приложениях, в которых применяется API электронной подписи ViPNet, при условии, что ваши ключи электронной подписи хранятся на устройстве eToken ГОСТ или USB ЭЦП. Подробнее см. документ «ViPNet Terminal. API электронной подписи в браузере Firefox. Руководство разработчика».
- Изменена процедура удаленного обновления ПО для терминалов с оперативной памятью и накопителем менее 2 Гбайт. На таких терминалах переход на версию 3.1 производится в два этапа.
- Расширен список поддерживаемого оборудования (см. Список поддерживаемого оборудования на стр. 44).

Версия 3.0.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 3.0.0 по сравнению с версией 2.2.0.

- Реализована поддержка устройств МАРШ! и USB ЭЦП Flash, которые могут использоваться в качестве загрузочного диска. Таким образом, ViPNet Terminal поставляется в различных вариантах исполнения — варианты с использованием в качестве загрузочного диска USB-носителей (eToken NG-FLASH (JAVA), МАРШ! и USB ЭЦП Flash) и вариант на базе компактного компьютера Kraftway Credo VV18.
- Добавлены команды для управления параметрами BIOS компактного компьютера Kraftway Credo VV18.

Версия 2.2.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 2.2.0 по сравнению с версией 2.1.0.

- В качестве аппаратной платформы для ViPNet Terminal используется компактный компьютер Kraftway Credo VV18.
- Реализовано перенаправление звука, USB-носителей и устройств аутентификации на терминальный сервер.
- Реализован клиент службы DNS, позволяющий определять IP-адрес узла по его DNS-имени, и клиент службы NTP, позволяющий синхронизировать системное время с сервером времени.

Версия 2.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet ThinClient версии 2.1.0 по сравнению с версией 2.0.0.

- Реализована возможность подключения к Интернету с помощью USB-модемов Yota и 3G-модемов операторов МТС, Билайн, Мегафон и Vodafone.
- Реализована возможность подключения к терминальным серверам Citrix XenApp по протоколам ICA, HTTP, HTTPS.
- Реализована возможность вызова командного интерпретатора из терминальной сессии и перезапуска терминальной сессии.
- Реализовано перенаправление локальных принтеров на терминальный сервер.

Версия 2.0.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Terminal версии 2.0.0.

- В качестве аппаратной платформы для ViPNet Terminal используется компактный компьютер eBox-4300.
- Для настройки параметров терминальной сессии вместо команд группы `admin set xwindow` используются команды группы `terminal`.
- Реализована поддержка устройств аутентификации eToken Pro.
- Реализована поддержка беспроводных сетей Wi-Fi.

D

Глоссарий

3G

Технология мобильной связи третьего поколения, которая используется для скоростного мобильного доступа в Интернет.

DHCP-сервер

Сервер, автоматически администрирующий IP-адреса DHCP-клиентов и выполняющий соответствующую настройку для сети.

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам компьютеров в интернет-домене. Например, ns.domain.net. Как правило, информация о домене хранится на двух DNS-серверах, называемых «Primary DNS» и «Secondary DNS» (дублирование делается для повышения отказоустойчивости системы).

Также DNS-сервер называют сервером доменных имен, сервером имен DNS.

Ethernet

Стандарт передачи данных в локальной компьютерной сети с помощью кабеля.

LTE

Технология мобильной связи четвертого поколения, которая представляет собой усовершенствование технологии 3G и используется для скоростного мобильного доступа в Интернет.

NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

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 Policy Manager

Программа, которая входит в состав программного комплекса ViPNet. Предназначена для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это 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 УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Клиент (ViPNet-клиент)

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

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Командный интерпретатор

Командная оболочка, предназначенная для администрирования программного обеспечения ViPNet Terminal с помощью ряда специальных команд.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Конфигурация сетевого экрана ViPNet Terminal

Фиксированный набор параметров работы узла ViPNet Terminal в сети, таких как режим фильтрации трафика и доступа к защищенной и открытой сетям. Набор доступных конфигураций определяет администратор сети ViPNet.

Координатор (ViPNet-координатор)

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

Режим безопасности ПО ViPNet

Набор предустановленных правил, определяющих правило фильтрации по умолчанию. По этим правилам производится обработка открытого IP-трафика.

Программное обеспечение ViPNet может работать в следующих режимах безопасности:

1. Блокировать IP-пакеты всех соединений.
2. Блокировать все соединения, кроме разрешенных.
3. Пропускать все исходящие соединения, кроме запрещенных.
4. Пропускать все соединения.
5. Пропускать все IP-пакеты без обработки.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

Сертификат ключа проверки — это электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Терминальная сессия

Сеанс удаленной работы с приложениями, выполняющимися на терминальном сервере.

Терминальный сервер

Выделенный компьютер, предоставляющий вычислительные ресурсы клиентам, которые подключаются к терминальному серверу по сети. Преимущества работы в терминальном режиме включают снижение расходов на программное и аппаратное обеспечение, уменьшение затрат времени на администрирование, повышение уровня защиты от внутренних злоумышленников.

Тонкий клиент

Компьютер, предназначенный для доступа к приложениям и данным, которые размещаются на терминальном сервере.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через Интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.