



Развертывание сети ViPNet с помощью ViPNet Administrator

Руководство администратора

Версия продукта: 4.6.11

© АО «ИнфоТеКС», 2023

ФРКЕ.00068-03 32 02

Версия продукта 4.6.11

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

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

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

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

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе.....	6
Для кого предназначен документ	6
Соглашения документа.....	6
Обратная связь.....	7
Глава 1. Общее представление о сети ViPNet.....	8
Конфигурации сети ViPNet	9
Описание узлов сети ViPNet.....	11
Защита IP-трафика в сети ViPNet	17
Глава 2. Подготовка к развертыванию сети ViPNet.....	19
Планирование сети	20
Перечень вопросов для определения оптимальной конфигурации сети ViPNet.....	23
Развертывание рабочих мест администраторов	25
Рекомендации по установке.....	25
Установка ViPNet Administrator	26
Глава 3. Создание топологии сети в ViPNet Administrator	29
Создание сетевых узлов и пользователей.....	30
Создание сети с помощью мастера	30
Дополнительная настройка сети	31
Рекомендации по созданию связей.....	32
Добавление ролей на сетевые узлы.....	36
Настройка свойств сетевых узлов.....	38
Создание дистрибутивов ключей	39
Глава 4. Развертывание координатора	40
Рекомендации по установке	41
Установка ПО ViPNet Coordinator for Windows	42
Настройка ПО ViPNet Coordinator for Windows	43
Глава 5. Развертывание клиента.....	44
Рекомендации по установке	45
Настройка ViPNet Client for Windows	46

Глава 6. Проверка функционирования сети ViPNet	47
--	----

Приложение А. Термины и сокращения	48
--	----



Введение

О документе	6
Обратная связь	7

О документе

Документ описывает развертывание сети ViPNet® под управлением ПО ViPNet Administrator®.

Документ дает общее представление о сетях ViPNet и позволяет определить, какая конфигурация сети ViPNet более всего удовлетворяет задачам защиты данных и коммуникации, стоящим перед вашей компанией. Также в документе содержится пошаговое руководство по развертыванию типовой сети ViPNet, включающей рабочее место администратора сети, один или несколько координаторов и клиентские рабочие места.

Для кого предназначен документ

Документ адресован системным администраторам, желающим ознакомиться со способами организации сетей ViPNet. Помимо этого, документ будет полезен IT-специалистам, выполняющим развертывание сети ViPNet, без необходимости погружения во все особенности и технические подробности технологии ViPNet.

Соглашения документа

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



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

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов компании ИнфоТеКС регулируется [политикой ответственного разглашения](#).

1

Общее представление о сети ViPNet

Конфигурации сети ViPNet	9
Описание узлов сети ViPNet	11
Защита IP-трафика в сети ViPNet	17

Конфигурации сети ViPNet

ПО ViPNet Administrator позволяет развертывать частные виртуальные сети любых конфигураций, обеспечивающие прозрачное взаимодействие узлов сети независимо от способа их подключения, расположения и типов IP-адресов. Сети ViPNet позволяют безопасно передавать информацию по общедоступным каналам связи различных типов. Это достигается путем создания логических сетей, защищенных криптографическими средствами высокой надежности.

Сети ViPNet обеспечивают следующие возможности:

- Легкая интеграция в структуру существующей сети.
- Защита трафика путем шифрования.
- Гибкая настройка фильтрации защищенного и открытого трафика.
- Фильтрация содержимого трафика на прикладном уровне модели OSI с помощью глубокой инспекции IP-пакетов (Deep Packet Inspection, DPI).
- Централизованное управление [политиками безопасности](#).
- Широкий выбор средств коммуникации между [защищенными узлами](#) (почта, чат, обмен файлами).
- Система слежения за состоянием сети.
- Организация иерархической системы сетей.
- Организация удостоверяющего центра, издание [сертификатов ключей проверки электронной подписи](#).
- Дополнительные возможности по регистрации пользователей, публикации сертификатов в общедоступных хранилищах.
- Организация защищенных соединений в промышленных системах и автоматизированных системах управления технологическим процессом (АСУ ТП).
- Обнаружение сетевых атак и вторжений.

Построение сетей ViPNet — процесс, имеющий свои особенности в каждом конкретном случае. В первую очередь он зависит от существующей топологии сети и от тех коммуникационных задач, которые стоят перед организацией. Именно поэтому универсальной схемы сети ViPNet не существует. В данном документе представлено описание лишь одного из типовых вариантов сети ViPNet под управлением ПО ViPNet Administrator.

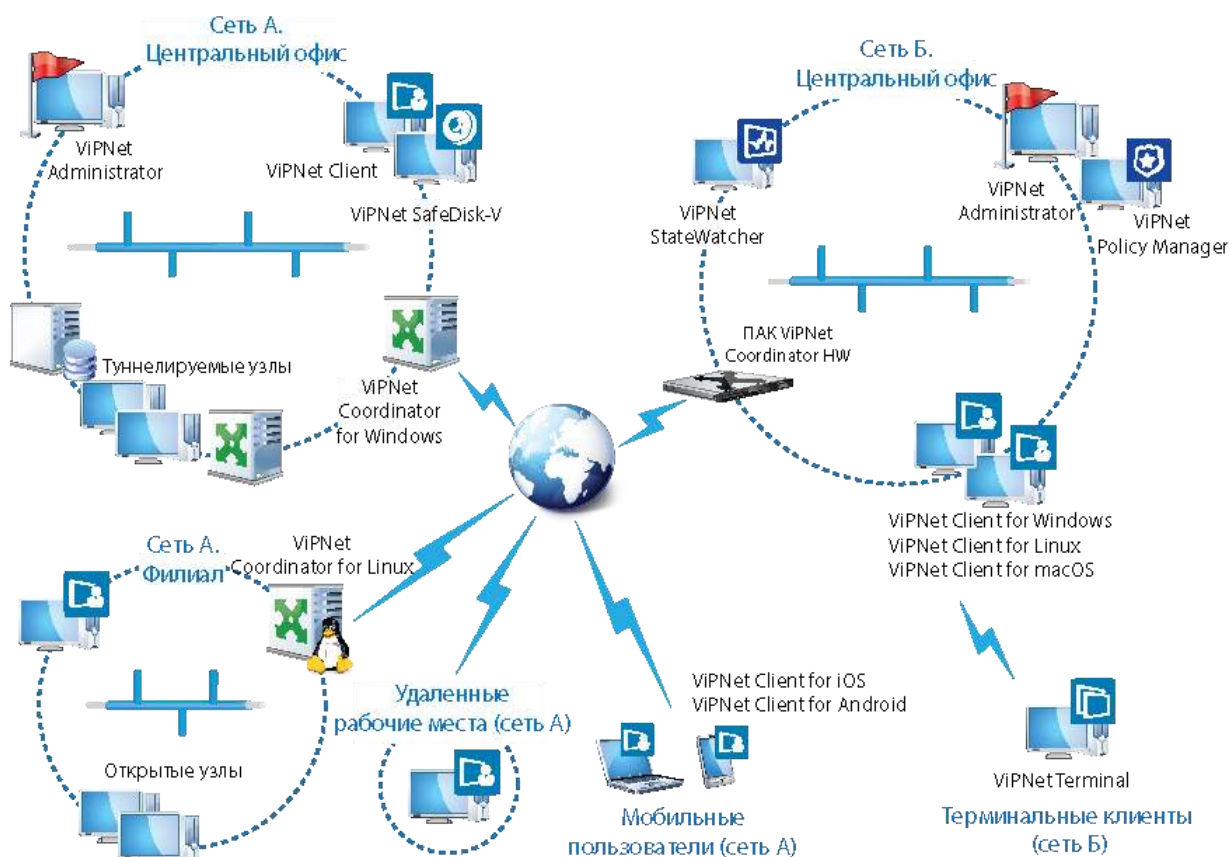


Рисунок 1. Схема сети ViPNet под управлением ПО ViPNet Administrator

В приведенном на схеме примере технология ViPNet позволяет объединить центральный офис компании «А», филиалы, удаленных пользователей (например, сотрудников, работающих на дому) и мобильных пользователей (сотрудников в командировке, на выезде) в защищенную сеть. Кроме того, можно организовать защищенное взаимодействие сети компании «А» с сетью компании «Б», если в сети последней также используется технология ViPNet.

Описание узлов сети ViPNet

Для обеспечения безопасности корпоративной сети необходима установка программного обеспечения ViPNet, которое позволяет защитить сетевой трафик, письма и файлы, передаваемые по сети, а также информацию, хранящуюся на компьютерах. При этом доступ к защищенному компьютеру открытых или других защищенных компьютеров может быть в той или иной степени ограничен.

Для организации такой защиты необходимы следующие базовые элементы сети:

- Рабочее место администратора сети ViPNet со следующим установленным ПО:
 - ViPNet Administrator, состоящее из следующих компонентов:
 - серверное приложение ViPNet Центр управления сетью (ЦУС);
 - одно или несколько клиентских приложений ЦУСа;
 - программа ViPNet Удостоверяющий и ключевой центр (УКЦ).
 - ViPNet Client® for Windows (далее — ViPNet Client) для организации обмена служебной информацией с другими [узлами сети ViPNet](#).
- Один или несколько серверов с установленным ViPNet Coordinator for Windows (далее — ViPNet Coordinator), ViPNet Coordinator Linux или программно-аппаратных комплексов ViPNet Coordinator HW. Обычно такие узлы (далее — координаторы) устанавливаются на границе сети или на границах участков сети. В зависимости от своих задач в сети такие узлы могут выполнять различные функции (см. таблицу).
- Компьютеры пользователей с установленным ViPNet Client, ViPNet Terminal или ViPNet CryptoService (далее — клиенты).

Помимо перечисленных базовых элементов, в сети ViPNet могут присутствовать и другие функциональные компоненты, например, компоненты, решающие задачи резервирования, мониторинга, управления политиками безопасности, общего доступа к сертификатам. Разновидности ПО ViPNet, используемого при организации частных виртуальных сетей, представлены на схеме ниже.

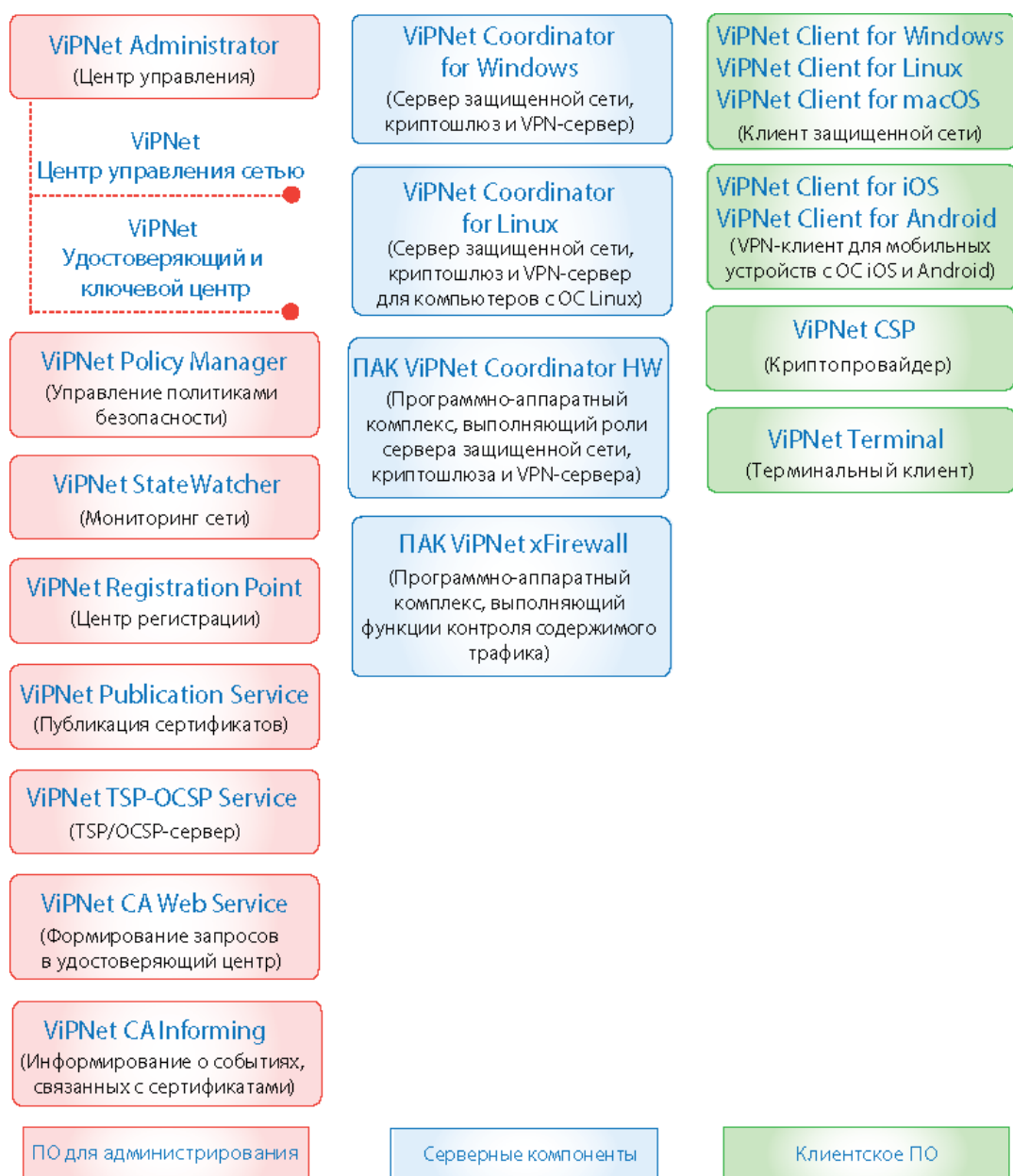


Рисунок 2. Программное обеспечение ViPNet, используемое при организации частных виртуальных сетей

Описание функций и ролей узлов, из которых может состоять защищенная сеть ViPNet, приведено в таблице.

Таблица 1. Назначение узлов сети ViPNet

Узел сети ViPNet	Описание
 ViPNet Центр управления сетью (ЦУС)	Обязательный компонент сети ViPNet. Выполняет следующие основные функции: • Создание и модификация топологии сети ViPNet. • Разграничение уровней полномочий пользователей сети. • Отправка ключей, полученных из УКЦ, информации о топологии сети, а также обновлений ключей и ПО на сетевые узлы. Роли: «Network Control Center», «VPN-клиент». Описание развертывания рабочего места администратора см. в разделе Развертывание рабочих мест администраторов, а также подробное описание процесса установки и первичной настройки компонентов ПО ViPNet Administrator в документе «ViPNet Administrator. Руководство по установке».
 ViPNet Удостоверяющий и ключевой центр (УКЦ)	Обязательный компонент сети ViPNet. Выполняет следующие функции: • Формирование ключевой структуры сети. • Издание и управление сертификатами пользователей, в том числе квалифицированными сертификатами в формате, соответствующем требованиям приказа ФСБ РФ от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» и требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». УКЦ в сети ViPNet обменивается данными с ЦУС через базу данных SQL, в которой хранится информация о структуре и объектах сети ViPNet. База данных размещается на SQL-сервере, который может быть установлен на одном компьютере с серверным приложением или на удаленном компьютере. УКЦ получает из базы данных информацию об узлах и пользователях сети, на основе которой формирует ключи, а затем отправляет их обратно в базу данных. Роли: если компьютер с УКЦ подключен к сети — «VPN-клиент», иначе на компьютер с УКЦ установка ПО ViPNet Client необязательна. Описание развертывания рабочего места администратора см. в разделе Развертывание рабочих мест администраторов, а также подробное описание процесса установки и первичной настройки компонентов ПО ViPNet Administrator в документе «ViPNet Administrator. Руководство по установке». Для автоматической выдачи сертификатов по запросам пользователей и управления их жизненным циклом, вы можете также установить на узел с УКЦ веб-службу ViPNet CA Web Service. Чтобы организовать информирование пользователей, для которых в УКЦ изданы сертификаты, а также администраторов УКЦ о событиях, связанных с сертификатами, вы можете также установить на узел с УКЦ программу ViPNet CA Informing.

Узел сети ViPNet	Описание
 ViPNet Policy Manager	Программа предназначена для централизованного управления политиками безопасности узлов, входящих в состав сети ViPNet. Централизованное управление особенно актуально для больших сетей, состоящих из сотен и тысяч узлов, однородных по выполняемой задаче и характеру сетевого окружения. Роли: «Policy Manager», «VPN-клиент».
 ViPNet StateWatcher	Система централизованного мониторинга сети ViPNet. Выполняет следующие основные функции: • Сбор информации о текущем состоянии узлов сети ViPNet и установленных на них компонентов ПО ViPNet. • Анализ информации для определения состояния узлов и выявления критических событий на них. • Оповещение администратора о сбоях в работе узлов и критических событиях на них. • Разграничение доступа к информации и управлению системой мониторинга. Роли: «StateWatcher», «VPN-клиент».
 ViPNet Registration Point	Программа предназначена для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов ключа проверки электронной подписи и дистрибутивов ключей, создаваемых в программе ViPNet Удостоверяющий и ключевой центр по соответствующим запросам. Роль: «Registration Point», «VPN-клиент».
 ViPNet Publication Service	Основное назначение программы — публикация сертификатов и списков аннулированных сертификатов в общедоступных хранилищах данных. Публикация сертификатов применяется в процессе защищенного обмена информацией между пользователями сети ViPNet и пользователями, не входящими в сеть ViPNet. Роли: «Publication Service», при необходимости — «VPN-клиент».
 ViPNet TSP-OCSP Service	Программа позволяет развернуть на узле сети ViPNet TSP/OCSP-сервер и осуществляет выдачу штампов времени пользователям по TSP-запросам.
 ViPNet Coordinator for Windows	Координатором в терминологии ViPNet называется сервер с ПО ViPNet Coordinator либо программно-аппаратный комплекс ViPNet Coordinator HW. Координатор является обязательным компонентом сети ViPNet. В зависимости от круга задач в корпоративной сети он может выполнять следующие функции:

Узел сети ViPNet	Описание
 ViPNet Coordinator for Linux	• VPN-сервер: сервер IP-адресов и транспортный сервер. • Маршрутизатор VPN-пакетов. • Сервер соединений. • VPN-шлюз. • Межсетевой экран. • Защищенный интернет-шлюз (ранее — сервер открытого Интернета). Для получения более подробной информации см. раздел Планирование сети.
 ViPNet Coordinator HW ViPNet Coordinator KB ViPNet Coordinator IG	Набор ролей, которые могут быть добавлены на координатор, может быть различным, в зависимости от его задач и функций в сети. Роль «Программный VPN-координатор» позволяет использовать на координаторе программное обеспечение ViPNet Coordinator для Windows или Linux для работы в качестве сервера защищенной сети ViPNet и несовместима с ролями, предназначенными для ПАКов.
 ViPNet xFirewall	Описание и шаги по разворачиванию координатора см. в разделе Развертывание координатора.
 ViPNet Client for Windows ViPNet Client 4U for Windows	Сетевой узел с ПО ViPNet Client выполняет следующие основные функции: • Шифрование сетевого трафика компьютера. • Фильтрация трафика (персональный сетевой экран — компонент ViPNet Монитор). • Предоставление дополнительных функций для оперативного защищенного обмена сообщениями, проведения конференций, обмена файлами, обмена электронными письмами (компонент ViPNet Деловая почта). • Защита от несанкционированной сетевой активности программ, установленных на компьютере (компонент ViPNet Контроль приложений). Набор ролей, которые могут быть добавлены на клиент, может быть различным, в зависимости от его задач и функций в сети. Для типового случая это роли «VPN-клиент» и «Business Mail». Описание и шаги по разворачиванию рабочего места пользователя см. в разделе Развертывание клиента.
 ViPNet Terminal	Сетевой узел с программным обеспечением ViPNet Terminal (ранее — ViPNet ThinClient) выполняет роль терминального клиента и позволяет организовать защищенный доступ к удаленному рабочему столу, опубликованным службам и приложениям на терминальном сервере. Роль: «Terminal».
 ViPNet CryptoService	Программное обеспечение ViPNet CryptoService предназначено для защиты информации сторонних прикладных систем. Благодаря наличию транспортного модуля, с помощью данного ПО можно автоматически обновлять сертификаты. Роль: «CryptoService».

Узел сети ViPNet	Описание
 ViPNet Client for iOS ViPNet Client for Android ViPNet Client для ОС Аврора	Приложения предназначены для защиты сетевого трафика при подключении мобильных устройств к сети ViPNet или к Интернету. Защита трафика выполняется благодаря функции шифрования, расшифрования и фильтрации IP-пакетов. Роль: «VPN Client для мобильных устройств».
 ViPNet CSP ViPNet CSP Linux	Программа ViPNet CSP необходима для корректной работы большинства программ ViPNet и входит в их комплекты поставки. Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений Microsoft и другого ПО, использующего интерфейс CryptoAPI 2.0. На узле с программой ViPNet CSP пользователь может создавать запросы на сертификат для отправки в удостоверяющий центр и работать с полученным сертификатом.
 ViPNet SafeDisk-V	Программа ViPNet SafeDisk-V предназначена для совместного использования с программой ViPNet Client и позволяет разграничить доступ пользователей к конфиденциальной информации, находящейся на сетевом узле. Роли: «SafeDisk», «VPN-клиент».
 Открытые или туннелируемые узлы	Открытые узлы сети ViPNet — это узлы, с которыми обмен информацией происходит в незашифрованном виде. Соединения с участием таких узлов могут быть защищены с помощью технологии туннелирования. Данная технология предполагает направление исходящего и входящего трафика узла через ViPNet Coordinator, где трафик фильтруется и защищается криптографическими методами (см. Защита IP-трафика в сети ViPNet).

Таким образом, перед развертыванием сети ViPNet необходимо определить круг задач, которые требуется решить в корпоративной сети, выбрать ПО ViPNet для решения этих задач и построить оптимальную логическую схему сети.

Защита IP-трафика в сети ViPNet

Обычно задачи по защите и разграничению доступа к информации не требуют защиты абсолютно всех узлов сети. Достаточно обеспечить защищенный обмен информацией на участках сети, не имеющих той степени доверия, которая регламентируется политикой безопасности компании. Таким образом, необходимо определить, какие участки сети являются небезопасными, и построить логическую сеть ViPNet так, чтобы на данных участках конфиденциальная информация была полностью защищена.

Рассмотрим, какой функциональностью по обмену и защите информации обладают узлы сети ViPNet.

Компьютер с установленным ПО ViPNet Client осуществляет шифрование исходящего трафика, а также функции по фильтрации и расшифрованию входящего трафика. Таким образом, информация, проходящая между двумя компьютерами с установленным ПО ViPNet Client, полностью защищена.



Рисунок 3. Обмен информацией между узлами ViPNet Client

При организации доступа к сети Интернет координатор ViPNet выступает в качестве межсетевого экрана и осуществляет фильтрацию открытого трафика для защиты локальных сетевых узлов. Кроме того, ViPNet Coordinator выполняет функции трансляции IP-адресов (NAT), и нет необходимости устанавливать дополнительные NAT-устройства на границе локальной и публичной сети. Если же такое устройство необходимо, можно настроить подключение координатора к Интернету через это устройство.



Рисунок 4. Обмен информацией между узлом ViPNet Client и Интернетом

Если требуется защитить информацию, которая проходит небезопасный участок сети (например, сеть Интернет), а внутри локальной сети защита не требуется, можно воспользоваться технологией туннелирования. Координатор, установленный между сетями, возьмет на себя все функции защиты сетевого трафика, а также функции маршрутизации.



Рисунок 5. Обмен информацией между открытыми узлами через Интернет

Таким образом, при составлении логической структуры сети ViPNet следует учитывать, на каких участках сети передача информации может быть небезопасной и каким способом ее требуется защитить.

Квалифицированную и детальную консультацию по структуре и составу сети [предоставляют специалисты ИнфоТеКС](#).

После определения и согласования всех описанных факторов можно переходить к планированию сети (см. [Планирование сети](#)).

2

Подготовка к развертыванию сети ViPNet

Планирование сети	20
Перечень вопросов для определения оптимальной конфигурации сети ViPNet	23
Развертывание рабочих мест администраторов	25

Планирование сети

При планировании сети ViPNet следует исходить из задач существующей физической структуры сети организации и применяемой политики информационной безопасности.

Если организация, в которой планируется развернуть сеть ViPNet под управлением ПО ViPNet Administrator, имеет несколько филиалов, в этих филиалах можно развернуть собственные сети ViPNet и установить между ними межсетевое взаимодействие. В этом случае целесообразно создать иерархическую структуру сетей ViPNet, чтобы централизованно управлять распределением лицензий в подчиненных сетях из главного Центра управления сетью (ЦУСа).

Логическая структура создаваемой сети ViPNet (в первую очередь, это связь клиентов с координаторами) в большинстве случаев определяется существующей физической структурой сети. С помощью ПО ViPNet Administrator можно создавать структуры, объединяющие в единую защищенную виртуальную сеть произвольное количество локальных подсетей, удаленных и мобильных пользователей.

Координаторы, выступающие в качестве серверов сети ViPNet, в зависимости от потребностей и применяемой политики безопасности могут выполнять следующие задачи:

- **VPN-сервер** — функция, объединяющая в себе следующие подфункции:
 - **Сервер IP-адресов** — функция VPN-сервера, которая в автоматическом режиме обеспечивает взаимодействие защищенных узлов (клиентов и координаторов) как внутри данной виртуальной сети, так и при взаимодействии с другими виртуальными сетями ViPNet. Это возможно благодаря использованию специального протокола динамической маршрутизации VPN-трафика, реализующего обмен информацией о параметрах доступа узлов друг к другу. Данный протокол обеспечивает маршрутизацию VPN-трафика между узлами в сети ViPNet тем методом, который наиболее оптимален для используемого способа подключения узла к сети.
 - **Транспортный сервер** — функция VPN-сервера, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами между узлами.

Маршрутизация прикладных и управляющих конвертов осуществляется с помощью транспортного модуля ViPNet MFTP, работающего на прикладном уровне. Транспортный модуль на координаторе принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения.

Маршрутизация данных между координаторами выполняется на основании межсерверных каналов, заданных для этих координаторов. Межсерверные каналы могут быть организованы по любой схеме. Если есть несколько маршрутов передачи конвертов между координаторами, передача информации осуществляется по кратчайшему из них. Передача информации из одной сети в другую выполняется через шлюзовые координаторы, с помощью которых происходит взаимодействие двух сетей.

По умолчанию координатор выступает сервером IP-адресов и транспортным сервером. Администратор ЦУСа может создать координатор без функций VPN-сервера, чтобы уменьшить нагрузку на вычислительные ресурсы координатора.

- **Маршрутизатор VPN-пакетов** — функция VPN-сервера, обеспечивающая маршрутизацию транзитного защищенного трафика, проходящего через координатор, на другие защищенные узлы. Маршрутизация осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется трансляция адресов (NAT). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора.
- **Сервер соединений** — функция, обеспечивающая соединение между клиентами и координаторами по кратчайшему пути, если они находятся в разных подсетях и не могут соединиться друг с другом напрямую.
- **VPN-шлюз** — стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты. VPN-шлюз интегрирован с межсетевым экраном для защищенных и открытых соединений, который осуществляет фильтрацию незашифрованного трафика, а также трафика внутри защищенного соединения.
- **Межсетевой экран** — функция, благодаря которой координатор выполняет фильтрацию открытых, транзитных и локальных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.

На координаторе может быть настроен TCP-туннель, позволяющий обеспечить получение IP-пакетов по протоколу TCP и их дальнейшую передачу по протоколу UDP.

В сегментированных сетях можно использовать каскадную схему установки координаторов.

В качестве координаторов могут выступать серверы с установленным ПО ViPNet Coordinator for Windows и ViPNet Coordinator for Linux, а также программно-аппаратные комплексы ViPNet Coordinator HW, ViPNet Coordinator KB и ViPNet Coordinator IG. Для создания отказоустойчивого решения на базе ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW предназначена система защиты от сбоев ViPNet Failover.

ПО ViPNet Coordinator или ViPNet Client, установленное на прикладном сервере, можно использовать для защиты трафика определенных прикладных серверов (например, контроллер домена, SMTP/FTP/веб-серверы, сервер базы данных).

В сети ViPNet существует возможность централизованного управления политиками безопасности на сетевых узлах. С помощью программы ViPNet Policy Manager, установленной на одном из клиентов, для отдельных узлов или групп формируются шаблоны политики безопасности, содержащие сетевые фильтры и правила трансляции.

С помощью ПО ViPNet Publication Service можно организовать публикацию сертификатов пользователей сети ViPNet в общедоступных хранилищах сертификатов. Это может быть необходимо при взаимодействии со сторонними удостоверяющими центрами. Также в сети ViPNet с помощью ПО ViPNet Registration Point можно создать один или несколько центров регистрации пользователей.

Если на каких-либо рабочих местах защита трафика не требуется, можно установить на них ПО ViPNet CryptoService, обеспечивающее возможность использования криптографических функций в прикладных программах, а также работу с ключом электронной подписи и ключом проверки электронной подписи пользователя.

Для наблюдения за состоянием сетевых узлов в сети ViPNet можно развернуть комплекс мониторинга защищенной сети ViPNet StateWatcher. Сервер мониторинга собирает информацию о состоянии сетевых узлов и установленных на них компонентах ПО ViPNet. При обнаружении сбоев система оповещает об этом администратора сети.

Кроме того, сеть ViPNet может включать терминальные клиенты для организации защищенных удаленных рабочих мест пользователя, мобильные клиенты на платформе iOS или Android и другие специализированные решения.

Перечень вопросов для определения оптимальной конфигурации сети ViPNet

Чтобы определить оптимальную конфигурацию сети ViPNet, необходимо ответить на следующие вопросы:

- Сколько сетей ViPNet нужно создать, и требуется ли иерархическая система сетей ViPNet?
- Требуется ли установить ПО ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр на разные компьютеры?
- Будут ли в сети использоваться центры регистрации пользователей и сервис публикаций?
- Будет ли в сети использоваться система централизованного мониторинга, централизованное управление политиками безопасности?
- Сколько рабочих мест пользователей, серверов и сегментов локальной сети нуждаются в защите трафика?
- Какие открытые узлы должны туннелироваться координаторами?
- Какая логическая структура VPN-соединений наиболее полно отвечает существующей физической структуре сети?
- Сколько должно быть координаторов?
- Будет ли в сети использоваться система резервирования координаторов?
- Какие IP-адреса (публичные или частные) будут иметь координаторы?
- Требуется ли устанавливать координаторы на отдельные компьютеры или их можно совместить с какими-либо существующими серверами или рабочими станциями?
- Как оптимально распределить клиенты между координаторами?
- Как осуществляется доступ к координаторам из внешней сети? Как организована маршрутизация входящего и исходящего трафика и трансляция адресов? Какие типы сетевых экранов используются, осуществляется ли трансляция адресов? Желательно изобразить подробную схему топологии сети.
- Какие прикладные серверы планируется защищать с помощью VPN (серверы с базами данных, CRM/CMS/ERP-системами, веб-серверы и так далее)?
- Каков характер трафика между сегментами, серверами, рабочими станциями (используемые службы, номера портов и протоколов)?
- Как должны быть настроены интегрированные в ПО ViPNet сетевые экраны для правильной работы сети и сетевых сервисов? Например, клиенты и координаторы по умолчанию будут блокировать входящий нешифрованный трафик. Если на каких-либо сетевых устройствах,

обеспечивающих работу общих сетевых сервисов, не установлено ПО ViPNet, то узлы ViPNet будут блокировать входящий трафик от этих устройств. Чтобы клиенты и координаторы могли обмениваться трафиком с такими сетевыми устройствами, в их интегрированных сетевых экранах должны быть заданы пропускающие фильтры для этих устройств. Трафик от других сетевых узлов ViPNet не блокируется.

Развертывание рабочих мест администраторов

Рекомендации по установке

Администрирование защищенной сети ViPNet осуществляется с помощью ПО ViPNet Administrator, которое включает два компонента:

- ViPNet Центр управления сетью (ЦУС) — предназначен для регистрации сетевых узлов и пользователей сети ViPNet, создания связей между ними, определения полномочий пользователей, централизованного обновления [справочников](#), ключей, программного обеспечения и так далее. ЦУС, в свою очередь, состоит из серверного и одного или нескольких клиентских приложений.
- ViPNet Удостоверяющий и ключевой центр (УКЦ) — предназначен для создания ключей и издания сертификатов ключа проверки электронной подписи.

Для установки ПО ViPNet Administrator требуется соответствующий установочный комплект.

Серверное приложение ЦУСа и программу УКЦ можно установить на одном компьютере или на двух разных компьютерах, если этого требует политика безопасности. Одно или несколько клиентских приложений ЦУСа можно установить как на компьютер с остальными приложениями, входящими в ПО ViPNet Administrator, так и на отдельные компьютеры.

На компьютер с серверным приложением ЦУСа обязательно установите ПО ViPNet Client. На отдельном компьютере с УКЦ установка ViPNet Client требуется только в случае необходимости защиты IP-трафика компьютера (этот компьютер можно не подключать к сети, соединив его только с компьютером с серверным приложением ЦУСа посредством кросс-кабеля).

На отдельных компьютерах с клиентскими приложениями ЦУСа выполните следующие действия:

- 1 Установите ПО ViPNet Client.
- 2 Создайте в программе ViPNet Монитор (компонент ПО ViPNet Client) на компьютере с серверным приложением сетевой фильтр, разрешающий входящие соединения с открытыми узлами, на которых установлены клиентские приложения ЦУСа.

Ограничения на количество сетевых узлов, одновременно туннелируемых соединений, на роли, которые могут быть добавлены на сетевые узлы, на количество сертификатов, которые могут быть изданы, и другие параметры сети ViPNet определяются приобретенной лицензией и хранятся в лицензионном файле *.itslic или infotecs.reg. Этот файл необходимо предоставить при первом запуске программы ViPNet Центр управления сетью, иначе продолжить работу будет невозможно (подробнее см. в документе «ViPNet Administrator. Руководство по установке»).

Несколько сетей ViPNet можно объединить в иерархическую систему. Такая необходимость может возникнуть, если несколько удаленных филиалов организации имеют свои собственные сети

ViPNet. В этом случае в главном ЦУСе осуществляется централизованное управление лицензиями подчиненных сетей.

Для организации иерархической системы сетей ViPNet требуется специальный лицензионный файл *.itcslic или infotecs.reg с поддержкой иерархии сетей, в котором указаны общие лицензионные ограничения на главную и подчиненные сети ViPNet, а также номера главной и подчиненных сетей. Сначала необходимо установить и запустить ПО ViPNet Administrator в главной сети, воспользовавшись специальным общим файлом лицензии. Затем в главном ЦУСе следует распределить лицензионные ограничения для подчиненных сетей и сформировать для них файлы лицензии *.itcslic или infotecs.reg. После этого можно выполнять развертывание подчиненных сетей (подробнее см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Иерархическая система сетей ViPNet»).

Для подготовки одного или нескольких рабочих мест администраторов сети ViPNet выполните следующие действия:

- 1 Установите на одном или нескольких компьютерах ПО ViPNet Administrator, для этого:
 - Установите серверное приложение ViPNet Центр управления сетью и программу ViPNet Удостоверяющий и ключевой центр на один и тот же или на разные компьютеры.
 - Установите на компьютер с серверным приложением или на любой другой компьютер сети клиентское приложение ViPNet Центр управления сетью.
 - В случае необходимости установите клиентские приложения на другие компьютеры сети.
- 2 В ЦУСе создайте структуру защищенной сети ViPNet (см. [Создание топологии сети в ViPNet Administrator](#)). В случае организации нескольких рабочих мест администраторов ЦУСа создайте учетную запись для каждого администратора.
- 3 В УКЦ сформируйте [дистрибутивы ключей](#) для узлов с серверным приложением ЦУСа, программой УКЦ и для узлов с клиентским приложением ЦУСа, на которых установлено ПО ViPNet Client.
- 4 На компьютерах, на которых установлено серверное приложение ЦУСа, установите ПО ViPNet Client.
- 5 На компьютерах, на которых установлено клиентское приложение ЦУСа, установите ПО ViPNet Client либо на компьютере с серверным приложением создайте сетевой фильтр, разрешающий входящие соединения с открытыми узлами, на которых установлены клиентские приложения.

Установка ViPNet Administrator

Перед установкой компонентов ПО ViPNet Administrator убедитесь, что на компьютерах, на которых будет производиться установка, выполнены стандартные сетевые настройки, правильно заданы часовой пояс, дата и время. Отключите контроль учетных записей в соответствующей категории панели управления. Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Чтобы развернуть программное обеспечение ViPNet Центр управления сетью, требуется установить два компонента: серверное приложение и клиентское приложение. Для этого выполните следующие действия:

- 1 Убедитесь, что вы располагаете установочным комплектом программы ViPNet Центр управления сетью и файлом лицензии на сеть ViPNet. Выберите схему размещения компонентов программы ViPNet Центр управления сетью.
- 2 На рабочее место администратора или на специально выделенный сервер установите серверное приложение ViPNet Центр управления сетью. При установке серверного приложения:
 - На компьютер будут автоматически установлены сторонние программы, необходимые для работы серверного приложения.
 - Будут созданы экземпляр SQL-сервера (если в параметрах подключения не был указан существующий экземпляр) и база данных для хранения структуры и параметров сети ViPNet.

Также при установке серверного приложения потребуется перезагрузка компьютера.

- 3 На компьютер, на котором установлено серверное приложение, или на отдельный компьютер установите клиентское приложение ViPNet Центр управления сетью.

Вместе с клиентским приложением на компьютер будут автоматически установлены сторонние программы, необходимые для его работы.

- 4 Если требуется, установите клиентское приложение ViPNet Центр управления сетью на дополнительных рабочих местах администраторов.
- 5 Установите на компьютер с серверным приложением ViPNet Центр управления сетью программное обеспечение ViPNet Client, которое требуется для отправки обновлений из Центра управления сетью на сетевые узлы ViPNet.

После создания сети ViPNet и дистрибутивов ключей для сетевых узлов установите на компьютер с серверным приложением дистрибутив ключей для сетевого узла — Центра управления сетью.

При необходимости установите на компьютеры с клиентскими приложениями ViPNet Центр управления сетью программное обеспечение ViPNet Client, настройте подключение клиентских приложений к серверному приложению ЦУСа и создайте дополнительные учетные записи администраторов.

Чтобы развернуть программное обеспечение ViPNet Удостоверяющий и ключевой центр, выполните следующие действия:

- 1 Установите программу ViPNet Удостоверяющий и ключевой центр на компьютер с серверным приложением ЦУСа или на отдельный компьютер.
- 2 Выполните первый запуск программы. Файл лицензии при этом не запрашивается, так как лицензионные ограничения вступают в силу после подключения к базе данных, находящейся на компьютере с серверным приложением ЦУСа. Во время первого запуска запустите мастер первичной инициализации или произведите конвертацию имеющейся у вас базы данных 3.x. Подробная информация о конвертации базы данных содержится в документе «ViPNet Administrator. Руководство по обновлению с версии 3.x до версии 4.x».



Внимание! Выполнять первичную инициализацию целесообразно только после создания сети ViPNet в ЦУСе.

3 В процессе первичной инициализации:

- Производится подключение к SQL-серверу, заполняется база данных.
- Создается учетная запись администратора программы.
- Издаётся сертификат администратора.
- Создаются мастер-ключи.

Подробная информация об установке и первоначальной настройке ПО ViPNet Administrator содержится в документе «ViPNet Administrator. Руководство по установке».

3

Создание топологии сети в ViPNet Administrator

Создание сетевых узлов и пользователей	30
Добавление ролей на сетевые узлы	36
Настройка свойств сетевых узлов	38
Создание дистрибутивов ключей	39

Создание сетевых узлов и пользователей

Создание сети с помощью мастера

Структуру сети ViPNet вы можете создать автоматически с помощью специального мастера **Создание сети ViPNet**, хотя также существует возможность создания структуры вручную. Для создания сетевых узлов и пользователей сети ViPNet с помощью мастера выполните следующие действия:

- 1 При первом запуске программы ViPNet Центр управления сетью в окне **Начало работы с ViPNet Центр управления сетью** щелкните ссылку **Сформировать структуру защищенной сети автоматически**, будет запущен мастер **Создание сети ViPNet**.



Примечание. Впоследствии, в случае необходимости, мастер можно будет запустить из главного окна клиентского приложения ViPNet Центр управления сетью. Для этого в меню **Моя сеть** выберите пункт **Создать сеть ViPNet**.

- 2 На странице **Координаторы защищенной сети ViPNet** укажите желаемое количество координаторов в сети ViPNet и задайте роли (см. [Добавление ролей на сетевые узлы](#)), которые будут добавлены на координаторы при их создании, установив соответствующие флажки.



Примечание. При задании количества сетевых узлов и добавлении ролей следует учитывать текущие лицензионные ограничения. Если ограничение на количество узлов с какой-либо ролью будет превышено, появится соответствующее предупреждение.

- 3 На странице **Клиенты защищенной сети ViPNet** укажите количество клиентов, которые должны быть зарегистрированы на каждом координаторе. Задайте роли, которые будут добавлены на клиенты при их создании, установив для этого соответствующие флажки.
- 4 На странице **Связи между объектами защищенной сети ViPNet** с помощью переключателя установите нужный тип организации связей между защищенными узлами. По умолчанию выбран вариант **Связать все сетевые узлы**.

Рекомендуется задать связи между пользователями связанных сетевых узлов, для этого установите соответствующий флажок. Данная связь необходима, чтобы пользователи могли вести конфиденциальную переписку друг с другом в программе ViPNet Деловая почта.

На каждый созданный сетевой узел будет добавлен один пользователь, имя которого совпадает с именем сетевого узла.

- 5 На странице **Подготовка к созданию сети ViPNet** завершена установите флажок **Создать справочники для сетевых узлов**.

После того как процесс формирования первичной структуры сети будет завершен, будет создана следующая структура сети ViPNet:

- На каждом сетевом узле будет создано по одному пользователю.
- Первый созданный клиент будет зарегистрирован как Центр управления сетью.
- Между сетевыми узлами будут образованы связи, тип которых был указан при установке.
- Для всех сетевых узлов будут созданы [справочники](#).
- Между всеми координаторами будут образованы межсерверные каналы.



Примечание. Межсерверные каналы используются для обмена [прикладными и управляющими конвертами](#) между координаторами, выступающими в роли серверов-маршрутизаторов. После окончания работы мастера вы можете вручную настроить межсерверные каналы, например, соединить все координаторы с одним центральным (схема «звезда») или соединить все координаторы по схеме «кольцо». Необходимо, однако, чтобы от каждого координатора к каждому существовал маршрут, иначе создание справочников будет невозможно.

После создания первичной структуры сети необходимо сделать [дополнительные настройки](#).

Дополнительная настройка сети

После того как в мастере сформирована первичная структура сети, в программе Центр управления сетью можно приступить к настройке параметров сетевых узлов и пользователей:

- В меню **Сервис > Параметры** укажите:
 - действия, которые будут выполняться по умолчанию при создании или удалении узлов и пользователей сети;
 - роли, которые будут автоматически добавляться на создаваемые узлы;
 - параметры безопасности узлов.

Информацию о настройках параметров программы по умолчанию см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Управление сетью ViPNet».

- Чтобы добавить пользователя на сетевой узел или удалить пользователя с сетевого узла, используйте окно свойств узла.
- Чтобы узлы могли взаимодействовать, создайте связи между пользователями узлов. Информацию по созданию связей см. в разделе [Рекомендации по созданию связей](#).
- Чтобы определить, какие программы могут работать на узлах, добавьте на узлы роли. Информацию по добавлению ролей см. в разделе [Добавление ролей на сетевые узлы](#).
- Настройте другие параметры сетевых узлов, используя окно свойств узлов. Информацию по настройке свойств узлов см. в разделе [Настройка свойств сетевых узлов](#).

Если вы изменили роли, параметры узлов или добавили сетевые узлы после окончания работы мастера, повторно создайте справочники для узлов. Для этого на панели инструментов нажмите кнопку **Справочники и ключи** , в меню выберите пункт **Создать справочники** и в окне **Создание справочников** выберите сетевые узлы, для которых требуется создать справочники.

После создания справочников информация о структуре сети становится доступной в программе ViPNet Удостоверяющий и ключевой центр. В УКЦ создайте дистрибутивы ключей (см. [Создание дистрибутивов ключей](#)) для сетевых узлов и передайте их доверенным способом пользователям для установки на сетевых узлах ViPNet. При необходимости в настройках УКЦ выберите действия, которые будут выполняться в программе в автоматическом режиме работы, то есть без участия администратора (подробнее см. в документах «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», «ViPNet Coordinator Монитор. Руководство администратора», «ViPNet Client Монитор. Руководство пользователя», «ViPNet CryptoService. Руководство администратора»).

Для получения более подробной информации о создании структуры сети см. документ «ViPNet Центр управления сетью. Руководство администратора».

Рекомендации по созданию связей

После создания первичной структуры сети можно просмотреть и изменить списки сетевых узлов, с которыми связан клиент или координатор. Для этого выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
- 2 На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.
- 3 На панели просмотра дважды щелкните сетевой узел, связи которого требуется изменить.
- 4 В окне свойств сетевого узла на левой панели выберите раздел **Связи с узлами**.

На правой панели в разделе **Сетевые узлы, с которыми установлена связь** будет отображен список узлов своей и доверенных сетей, с которыми связан данный сетевой узел.

Связи с узлами, имена которых отображаются серым цветом, являются обязательными. Список можно изменять, удаляя и добавляя связи.

Следующие рекомендации по созданию связей относятся к сетевым узлам, на которые добавлены роли «VPN-клиент» или «Программный VPN-координатор».



Примечание. В данном разделе под выражением «клиенты данного координатора» подразумевается «клиенты, для которых данный координатор является сервером IP-адресов».

Для установления соединения между двумя клиентами сети необходимо, чтобы эти клиенты обладали информацией о параметрах доступа друг к другу. Такую информацию каждый клиент получает от своего сервера IP-адресов. Клиент также сообщает серверу IP-адресов информацию о собственных параметрах доступа. По умолчанию в качестве сервера IP-адресов используется

координатор, на котором клиент зарегистрирован в ЦУСе, то есть его сервер-маршрутизатор. На клиенте в качестве сервера IP-адресов можно выбрать и другой координатор.

Координаторы обмениваются информацией о клиентах, для которых они являются серверами IP-адресов, с учетом связей, установленных между клиентами. Для обеспечения этого обмена в ЦУСе также должны быть установлены связи между координаторами, выполняющими функции сервера IP-адресов. Вы можете связать каждый координатор со всеми координаторами своей и чужих сетей, но в больших сетях это приведет к загрузке каналов служебной информацией, а координаторы будут загружены ее обработкой.

При задании связей между координаторами следует учитывать следующие особенности обмена служебной информацией между серверами IP-адресов по умолчанию:

- Координатор «А», являющийся сервером IP-адресов клиента «В», отправляет информацию об этом клиенте на координатор «С», если клиент «В» связан с координатором «С» или с клиентами координатора «С».
- Координатор «С», получивший информацию о клиенте «В» от координатора «А» своей сети ViPNet:
 - Никогда не передает ее третьему координатору своей сети, то есть цепочка передачи информации о клиентах в одной сети всегда состоит только из двух координаторов.
 - Если координатор «А» не связан с координаторами другой сети ViPNet, а клиент «В» связан с узлами другой сети, то координатор «С» передает полученную информацию на один из доступных координаторов этой сети (координатор «D»).
- Координатор «D», получивший информацию о клиенте «В» от координатора «С» другой сети, передает ее на координатор «Е» своей сети, если клиент «В» связан с координатором «Е» или с клиентами координатора «Е».

В общем случае, если трафик между узлами по правилам маршрутизации проходит через два и более координаторов, то эти узлы должны быть связаны с этими координаторами или клиентами, связанными с этими координаторами и находящимися в сети данных координаторов.

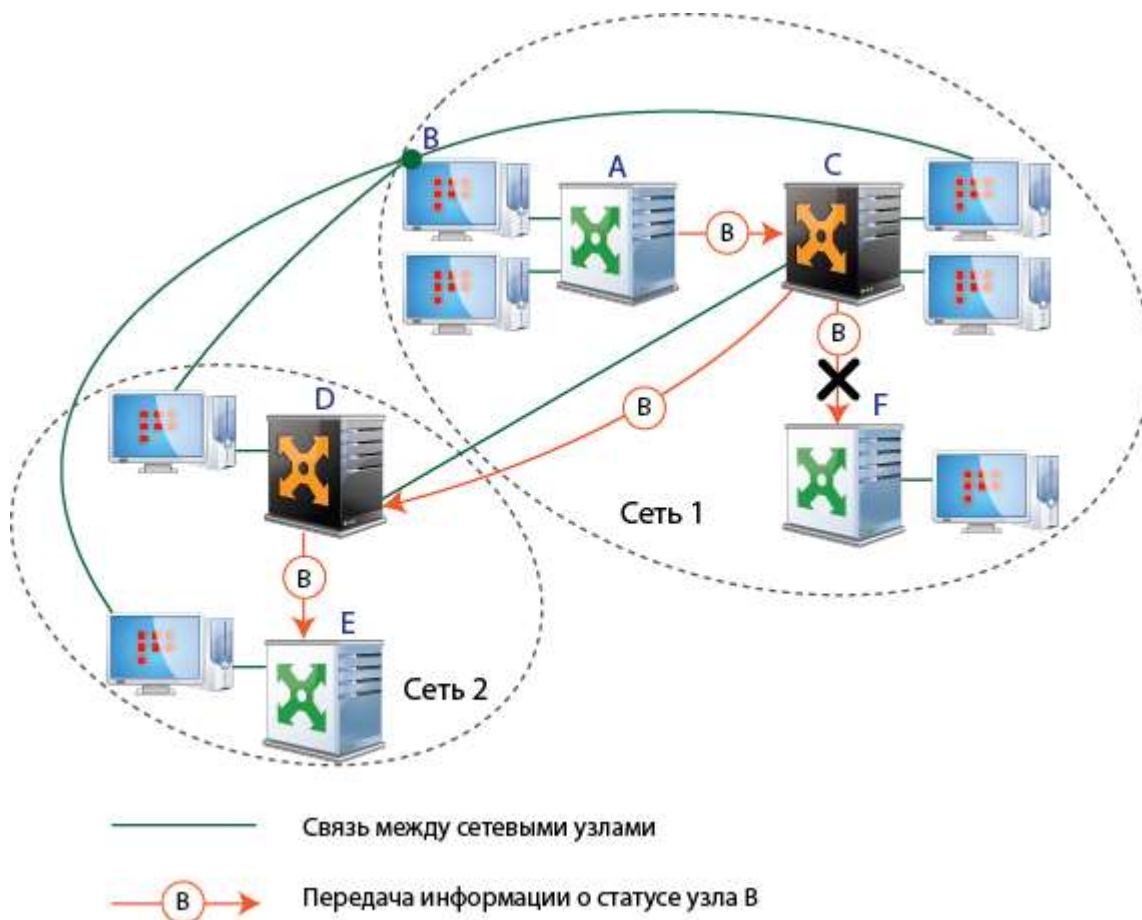


Рисунок 6. Особенности обмена служебной информацией в сетях ViPNet

Исходя из указанных свойств, при задании связей следует руководствоваться следующими требованиями и рекомендациями:

- 1 Если координаторы «А» и «F» из одной сети ViPNet являются серверами IP-адресов по умолчанию для клиентов, которые связаны между собой, то координаторы «А» и «F» необходимо также связать между собой. То есть если клиенты одной сети, зарегистрированные на разных координаторах, связаны, то их координаторы также должны быть связаны.
- 2 Если клиент зарегистрирован в ЦУСе на координаторе «А», то нет необходимости явным образом устанавливать между ними связь. Такая связь создается автоматически.
- 3 Если координатор «С» из сети 1 и координатор «D» из сети 2 являются шлюзовыми между сетями 1 и 2, то нет необходимости явным образом устанавливать связь между этими координаторами. Такая связь создается автоматически.
- 4 Если клиенту координатора «А» не требуется устанавливать соединение с координатором «F» или его туннелируемыми узлами, то не рекомендуется устанавливать связь этого клиента с координатором «F».
- 5 Если клиент сети 1 связан с клиентом сети 2, то его сервер IP-адресов по умолчанию (его координатор) в сети 1 должен быть либо шлюзовым в сеть 2, либо связан со шлюзовым координатором сети 1 в сеть 2, либо связан со шлюзовым координатором сети 2 в сеть 1.
- 6 Если координатор «А» сети 1, который не является шлюзовым координатором в сеть 2, связан с координатором «Е» сети 2 (например, для взаимодействия между туннелируемыми узлами

координаторов), то координатор «А» необходимо связать также со всеми другими координаторами сети 1, клиенты которых связаны с узлами сети 2.

- 7 Если требуется создать резервный сервер IP-адресов для группы клиентов, необходимо связать эти клиенты с некоторым координатором. Клиенты при необходимости смогут выбрать этот координатор в качестве резервного сервера IP-адресов. Для такого координатора должны быть заданы такие же связи, как и для резервируемого координатора.

Добавление ролей на сетевые узлы

Роли определяют, какие программы ViPNet могут работать на тех или иных сетевых узлах, а также функциональность программ ViPNet. В ходе создания защищенной сети ViPNet в ЦУСе необходимо добавить роли на клиенты и координаторы.

На все сетевые узлы при создании могут быть автоматически добавлены роли, если установить соответствующие флажки в мастере **Создание сети ViPNet**. Чтобы просмотреть или изменить список ролей сетевого узла, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
- 2 На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа сетевого узла, который требуется настроить.
- 3 На панели просмотра дважды щелкните сетевой узел, список ролей которого нужно просмотреть или изменить.
- 4 В окне свойств сетевого узла на левой панели выберите раздел **Роли узла**. На правой панели в разделе **Роли клиента (координатора)** будет отображен список ролей, добавленных на текущий сетевой узел. Этот список можно редактировать, добавляя и удаляя роли, а также изменяя свойства ролей.



Примечание. Возможность изменения свойств доступна не для всех ролей.

Роль «Network Control Center» автоматически добавляется на первый клиент сети ViPNet и не может быть добавлена на другие клиенты. Роль «Network Control Center» позволяет на этом клиенте установить серверное приложение ViPNet Центр управления сетью.



Примечание. В случае если одно или несколько клиентских приложений ЦУСа установлены на отдельных компьютерах, для их корректной работы добавления на эти узлы специальных ролей не требуется.

При необходимости измените следующие свойства ролей:

- 1 На клиентах, на которые добавлены роли «VPN-клиент», «Business Mail» и «CryptoService», измените уровень полномочий. Уровень полномочий определяет допустимость изменения пользователем различных настроек ПО ViPNet на сетевом узле. Ограничения функциональных возможностей продуктов ViPNet, которые зависят от уровня полномочий пользователя, описаны в документации соответствующих продуктов.

- 2 На узле, который является Центром управления сетью и на который автоматически при его создании добавляется роль «Policy Manager» укажите списки узлов, политиками безопасности которых требуется управлять.
- 3 На клиентах, на которые добавлена роль «Registration Point», установите ограничения числа запросов на дистрибутивы и сертификаты.
- 4 На клиентах, на которые добавлена роль «StateWatcher», задайте ограничения на число узлов мониторинга и дочерних серверов.
- 5 Чтобы обеспечить отдельный доступ узлов в Интернет при отсутствии соединения с узлами ViPNet или к ресурсам сети ViPNet при отсутствии подключения к Интернет, на одном или нескольких координаторах, на которые добавлена роль «Программный VPN-координатор» или соответствующие роли для координаторов на базе модификаций ПАК ViPNet Coordinator HW, ПАК ViPNet Coordinator IG, укажите, что они являются [защищенным интернет-шлюзом](#).

Подробную информацию о добавлении ролей на сетевые узлы см. в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Настройка параметров сетевых узлов», в разделе «Добавление ролей на сетевые узлы».

Кроме свойств ролей существует ряд параметров, которые можно изменить в окне свойств сетевых узлов. Задание этих параметров рассмотрено в разделе [Настройка свойств сетевых узлов](#).

Настройка свойств сетевых узлов

Ряд параметров сетевых узлов можно задать в окне свойств клиентов и координаторов.

В окне свойств координаторов можно задать следующие параметры:

- IP-адреса и DNS-имена (раздел **Адреса во внешних сетях**).
- Параметры подключения координатора к внешней сети (раздел **Межсетевой экран**).
- Настройки межсетевого экрана для клиентов, зарегистрированных на этом координаторе (раздел **Межсетевой экран клиентов**).
- Адреса туннелируемых соединений и максимальное число одновременно туннелируемых адресов (раздел **Туннелирование**).

В окне свойств клиентов можно задать следующие параметры:

- IP-адреса клиентов, указываются при необходимости (раздел **Адреса во внешних сетях**).
- Специальные параметры для клиентов, у которых настройки межсетевого экрана должны отличаться от заданных на сервере IP-адресов (раздел **Межсетевой экран**).

Настройки подключения через межсетевой экран, заданные в ЦУСе, будут применяться только на клиентах с версией ПО ViPNet Client for Windows ниже 4.2. На клиентах с версией 4.2 и выше такие настройки отсутствуют, так как эти клиенты автоматически определяют параметры подключения к внешней сети и устанавливают взаимодействие с внешними узлами с помощью [сервера соединений](#).

Подробную информацию о настройках сетевых узлов см. в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Настройка параметров сетевых узлов».

Создание дистрибутивов ключей

Чтобы развернуть сетевые узлы, необходимо создать [дистрибутивы ключей](#). Для этого выполните следующие действия:

- 1 В ЦУСе создайте справочники.
 - 2 В главном окне программы ViPNet Удостоверяющий и ключевой центр:
 - 2.1 В окне **Сервис > Настройка** в разделе **Дистрибутивы ключей** настройте параметры создания дистрибутивов ключей.
 - 2.2 Выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Сетевые узлы**.
 - 2.3 В списке сетевых узлов на панели просмотра выберите узлы, для которых требуется создать дистрибутивы ключей.
 - 2.4 Щелкните узлы правой кнопкой мыши и в контекстном меню выберите пункт **Выдать новый дистрибутив ключей**.
- Будет запущен процесс создания дистрибутивов.
- 3 Задайте пароль администратора для группы «Вся сеть» (в эту группу по умолчанию входят все сетевые узлы), который используется для входа в режим администратора на сетевых узлах.
 - 4 Следуйте указаниям мастера выдачи дистрибутивов. Созданные дистрибутивы ключей будут сохранены в заданную папку. Если была настроена печать паролей, пароли пользователей будут переданы на печать.
 - 5 Защищенным способом передайте дистрибутивы ключей и пароли на компьютеры, на которых планируется развертывание сетевых узлов, и выполните установку ПО ViPNet.

Установка и настройка ПО ViPNet на сетевых узлах описана в разделах [Развертывание координатора](#) и [Развертывание клиента](#).

4

Развертывание координатора

Рекомендации по установке	41
Установка ПО ViPNet Coordinator for Windows	42
Настройка ПО ViPNet Coordinator for Windows	43

Рекомендации по установке

В данной главе описывается установка и настройка программного обеспечения ViPNet Coordinator для ОС Windows. Чтобы получить информацию об установке и настройке ViPNet Coordinator Linux или программно-аппаратного комплекса ViPNet Coordinator HW, обратитесь к соответствующей документации.

Требования к аппаратному и программному обеспечению компьютеров, на которых устанавливается ПО ViPNet Coordinator, содержатся в документе «ViPNet Coordinator Монитор. Руководство администратора», в разделе «Системные требования».



Внимание! На компьютере, на котором устанавливается ПО ViPNet Coordinator, не должны быть установлены никакие сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT). Использование ViPNet Coordinator одновременно с такими программами может привести к конфликтам и вызвать проблемы с доступом в сеть.

Компьютер, на котором устанавливается ПО ViPNet Coordinator, может быть подключен к любым локальным или глобальным сетям с IP-адресацией. Подключение к Интернету может осуществляться с помощью xDSL, ISDN, GPRS, UMTS, Wi-Fi, WiMAX или любым другим способом. Возможно подключение к сети через различные межсетевые экраны и устройства, осуществляющие трансляцию адресов (NAT).

Компьютер может иметь несколько сетевых интерфейсов. Если координатор планируется использовать для подключения к сети ViPNet удаленных пользователей или в качестве шлюза при взаимодействии с другими сетями ViPNet, по крайней мере один сетевой интерфейс координатора должен иметь публичный IP-адрес или находиться за межсетевым экраном со статической трансляцией адресов.

Для правильной работы координатора в ОС Windows должна быть включена функция маршрутизации IP-пакетов. Если маршрутизация IP-пакетов отключена, она будет автоматически включена во время установки ПО ViPNet Coordinator.

ViPNet Coordinator можно установить на специально выделенном для этого компьютере или на каком-либо существующем сервере. В последнем случае весь IP-трафик сервера будет защищен. Кроме того, будет проще организовать обмен трафиком между этим сервером и другими сетевыми узлами ViPNet, так как по умолчанию между защищенными узлами разрешены любые соединения и настройка сетевых фильтров не требуется.

Установка ПО ViPNet Coordinator описана в следующем разделе. После установки в программе ViPNet Coordinator нужно выполнить ряд настроек (см. [Настройка ПО ViPNet Coordinator for Windows](#)).

Установка ПО ViPNet Coordinator for Windows



Примечание. Процесс установки ПО ViPNet Client ничем не отличается от установки ПО ViPNet Coordinator. Поэтому указания, содержащиеся в данном разделе, относятся к обоим перечисленным программам.

Перед установкой ViPNet Coordinator или ViPNet Client:

- Убедитесь, что на компьютере выполнены стандартные сетевые настройки и правильно заданы часовой пояс, дата и время.
- Отключите использование Юникода и не включайте после установки программы.
- Если локализация Windows не русская, то для правильного отображения кириллицы в интерфейсе ViPNet Coordinator или ViPNet Client измените региональные настройки Windows.

Для установки ViPNet Coordinator или ViPNet Client требуются:

- Установочный EXE-файл программы.
- **Дистрибутив ключей** для сетевого узла — файл с расширением *.dst или *.enc. Если на узле планируется работа нескольких пользователей, для каждого из них нужен отдельный дистрибутив ключей.
- Пароль пользователя сетевого узла или внешнее устройство аутентификации.



Примечание. Дистрибутивы и пароли пользователей создаются в программе ViPNet Удостоверяющий и ключевой центр (см. [Создание дистрибутивов ключей](#)).

Для установки ViPNet Coordinator или ViPNet Client выполните следующие действия:

- 1 Запустите установочный файл . Дождитесь завершения подготовки к установке.
- 2 Следуйте указаниям программы установки.
- 3 По завершении установки перезагрузите компьютер.
- 4 После перезагрузки установите [справочники и ключи пользователя сетевого узла](#).

Подробно установка ПО ViPNet Coordinator описана в документе «ViPNet Coordinator for Windows. Руководство администратора», в разделах «Установка, обновление и удаление ПО ViPNet Coordinator» и «Установка и обновление справочников и ключей».

Настройка ПО ViPNet Coordinator for Windows

Чтобы уменьшить количество настроек, выполняемых вручную непосредственно на координаторе, рекомендуется задать IP-адреса координаторов, туннелируемых узлов и настройки подключения координатора к сети в клиентском приложении ViPNet Центр управления сетью. Выполните следующие действия:

1 Настройте параметры межсетевого экрана:

- Задайте необходимые сетевые фильтры (см. документ «ViPNet Coordinator. Руководство администратора», главу «Интегрированный сетевой экран», раздел «Создание сетевых фильтров»).
- Включите или отключите антиспуфинг (см. документ «ViPNet Coordinator. Руководство администратора», главу «Интегрированный сетевой экран», раздел «Антиспуфинг»).
- Задайте правила трансляции адресов (см. документ «ViPNet Coordinator. Руководство администратора», главу «Трансляция сетевых адресов (NAT)»).
- Настройте параметры обработки прикладных протоколов (см. документ «ViPNet Coordinator. Руководство администратора», главу «Обработка прикладных протоколов»).

2 Задайте IP-адреса других координаторов сети ViPNet (см. документ «ViPNet Coordinator. Руководство администратора», главу «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к защищенным узлам»).

3 При необходимости задайте IP-адреса открытых узлов, туннелируемых координатором (см. документ «ViPNet Coordinator. Руководство администратора», главу «Защита трафика открытых узлов (туннелирование)»).

4 Если координатор должен подключаться к открытым узлам, которые туннелируются другими координаторами, задайте IP-адреса этих узлов (см. документ «ViPNet Coordinator. Руководство администратора», главу «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к узлам, туннелируемым другим координатором»).

5

Развертывание клиента

Рекомендации по установке	45
Настройка ViPNet Client for Windows	46

Рекомендации по установке

На клиенте сети следует установить одну из следующих программ ViPNet:

- ViPNet Client for Windows — выполняет функции VPN-клиента сети ViPNet и персонального сетевого экрана.
- ViPNet CryptoService — обеспечивает возможность использования криптографических функций в прикладных программах, но не обеспечивает защиту трафика.

Требования к аппаратному и программному обеспечению компьютеров, на которых устанавливается клиентское ПО ViPNet, содержатся в документах «ViPNet Client Монитор. Руководство администратора» и «ViPNet CryptoService. Руководство пользователя».



Внимание! На компьютере, на котором устанавливается ПО ViPNet Client, не должны быть установлены никакие сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT). Использование ViPNet Client одновременно с такими программами может привести к конфликтам и вызвать проблемы с доступом в сеть.

Компьютер, на котором устанавливается ПО ViPNet Client, может быть подключен к любым локальным сетям TCP/IP или к интернету. Компьютер подключается к интернету с помощью xDSL, ISDN, GPRS, UMTS, Wi-Fi, WiMAX или любым другим способом. Возможно подключение к сети через различные межсетевые экраны и NAT-устройства.

ПО ViPNet Client можно установить на какой-либо сервер для обеспечения защиты трафика этого сервера. Кроме того, это позволяет легко организовать обмен трафиком между этим сервером и другими сетевыми узлами ViPNet, так как по умолчанию между защищенными узлами разрешены любые соединения и настройка правил фильтрации трафика не требуется.

Установка ПО описана в документации указанных продуктов.

После установки в программе ViPNet Client нужно выполнить ряд настроек (см. [Настройка ViPNet Client for Windows](#)). Специальная настройка ПО ViPNet CryptoService не требуется.

Настройка ViPNet Client for Windows

Чтобы уменьшить количество настроек, выполняемых вручную непосредственно на клиентском компьютере, рекомендуется задать IP-адреса координаторов, туннелируемых узлов и настройки подключения клиента к сети в клиентском приложении ViPNet Центр управления сетью. Если необходимые настройки не были сделаны в ЦУСе, выполните следующие действия:

- 1 Настройте параметры межсетевого экрана:
 - Задайте необходимые сетевые фильтры (см. документ «ViPNet Client. Руководство пользователя», главу «Интегрированный сетевой экран», раздел «Создание сетевых фильтров»).
 - Настройте параметры обработки прикладных протоколов (см. документ «ViPNet Client. Руководство пользователя», главу «Обработка прикладных протоколов»).
- 2 Задайте IP-адрес сервера IP-адресов, выбранного для данного клиента (см. документ «ViPNet Client. Руководство пользователя», главу «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к защищенным узлам»).
- 3 Если клиент должен подключаться к туннелируемым узлам, задайте IP-адреса этих узлов (см. документ «ViPNet Client. Руководство пользователя», главу «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к туннелируемым узлам»).

6

Проверка функционирования сети ViPNet

Чтобы убедиться в том, что сеть ViPNet развернута и настроена правильно, достаточно проверить возможность установления соединений между защищенными сетевыми узлами ViPNet, а также возможность подключения к туннелируемым узлам:

- Для проверки соединения с выбранными сетевыми узлами в программе ViPNet Монитор нажмите на панели инструментов кнопку **Проверить** .
- Для проверки соединения с туннелируемыми узлами можно воспользоваться командой `ping`.

Для полноценного функционирования сети необходима возможность соединения между всеми координаторами, а также между клиентами и их серверами IP-адресов. Также следует проверить возможность подключения к сети ViPNet удаленных пользователей.

Если соединение между какими-либо узлами невозможно, убедитесь, что на этих узлах правильно заданы IP-адреса координаторов и параметры подключения к сети, а на используемых межсетевых экранах настроены необходимые правила трансляции адресов.



Термины и сокращения

ViPNet Administrator

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

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 для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Защищенный интернет-шлюз (открытый интернет)

Технология, реализованная в программном обеспечении ViPNet. При подключении к интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Контент-фильтрация

Фильтрация IP-трафика на прикладном уровне модели OSI с помощью технологии расширенной инспекции содержимого сетевого трафика (Deep Packet Inspection, DPI). На основании анализа полученных данных идентифицируются приложения и прикладные протоколы.

Политики безопасности

Набор параметров — сетевых фильтров и правил трансляции сетевых адресов, регулирующих безопасность сетевого узла.

Прикладной конверт

Файл, формируемый приложениями ViPNet (например, «Деловая почта», «Файловый обмен») для передачи другим сетевым узлам.

Роль

Функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

Сервер соединений

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

Сертификат ключа проверки электронной подписи

Документ, изданный удостоверяющим центром 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 управляющем ПО.

Сеть ViPNet

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

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Туннелирование

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

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.