

Новые возможности ViPNet Client и ViPNet Coordinator версии 4.x

Приложение к документации ViPNet

1991–2013 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00116-03 90 13

Этот документ входит в комплект поставки программного обеспечения, 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 зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТеКС».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: <http://www.infotecs.ru>

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе	6
Для кого предназначен документ	6
Соглашения документа.....	6
Обратная связь	7
Глава 1. Установка и обновление	8
Установка программного обеспечения ViPNet.....	9
Установка ПО с использованием Microsoft System Center.....	9
Установка ПО с использованием сценария входа в систему	9
Неинтерактивный режим установки	10
Установка и настройка программы ViPNet CSP	10
Совместимость с ОС Windows	12
Логика отключения Windows Firewall.....	12
Установка ключей ViPNet	13
Система обновления ViPNet.....	15
Глава 2. Защита трафика	17
Фильтрация трафика	18
Получение и применение политик безопасности из ViPNet Policy Manager.....	18
Новый формат сетевых фильтров, совместимый с ViPNet Policy Manager	20
Особенности формата фильтров в версии 4.x по сравнению с версией 3.2.x	22
Приоритет сетевых фильтров.....	27
Правила трансляции IP-адресов.....	28
Группы объектов	30
Системные группы объектов.....	31
Пользовательские группы объектов	32
Антиспуфинг.....	34
Настройка параметров сетевых интерфейсов	36
Блокировка компьютера и IP-трафика.....	37

Новые алгоритмы электронной подписи.....	39
Глава 3. Подключение к сети ViPNet	40
Настройка подключения координатора к внешней сети через межсетевой экран со статической или динамической трансляцией адресов.....	41
Настройка TCP-туннеля.....	43
Настройка подключения клиентов.....	46
Глава 4. Безопасность и полномочия пользователя.....	48
Способы аутентификации.....	49
Режимы безопасности	51
Ограниченный интерфейс пользователя	52
Смена конфигураций программы по расписанию.....	54
Глава 5. Прочие доработки	55
Добавление туннелируемых узлов.....	56
Определение и проверка IP-адресов.....	57
Журнал IP-пакетов.....	58
Интеграция с программой SafeDisk-V.....	60
Передача конвертов MFTR через почтовые серверы	61
Изменения в мастере обновления сертификата.....	62
Изменения в программе ViPNet Деловая почта.....	64
Встроенная база данных SQLite.....	64
Хранение вложений в базе данных и архивация.....	64
Просмотр статуса сообщения.....	65
Обмен защищенными сообщениями	66
Изменения в интерфейсе.....	68
Изменения в терминологии	71
Приложение А. Глоссарий.....	72
Приложение В. Указатель	75



Введение

О документе	6
Обратная связь	7

О документе

Для кого предназначен документ

Данный документ предназначен для технических специалистов, партнеров ОАО «ИнфоТеКС» и администраторов сетей ViPNet, планирующих обновление ПО ViPNet до версии 4.x.

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

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet <http://docs.infotecs.ru>.
- Сборник часто задаваемых вопросов (FAQ) <http://www.infotecs.ru/support/faq/>.
- Законодательная база в сфере защиты информации <http://www.infotecs.ru/laws/>.
- Информация о решениях ViPNet <http://www.infotecs.ru/solutions/vpn/>.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки <http://www.infotecs.ru/support/request/>.
- Форум ОАО «ИнфоТеКС» <http://www.infotecs.ru/forum>.
- 8 (495) 737-6196 — «горячая линия» службы технической поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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



Установка и обновление

Установка программного обеспечения ViPNet	9
Установка ключей ViPNet	13
Система обновления ViPNet	15

Установка программного обеспечения ViPNet

Для программ ViPNet Client и ViPNet Coordinator версии 4.x доработана программа установки, а именно:

- разработан установочный пакет MSI, который позволяет устанавливать программу с использованием Microsoft System Center (см. «[Установка ПО с использованием Microsoft System Center](#)» на стр. 9) или сценария входа в систему logon script (см. «[Установка ПО с использованием сценария входа в систему](#)» на стр. 9);
- изменен сценарий установки программы из командной строки (см. «[Неинтерактивный режим установки](#)» на стр. 10).

Установка ПО с использованием Microsoft System Center

Для программ ViPNet Client, ViPNet Coordinator, ViPNet CSP версии 4.x разработаны установочные пакеты MSI. Использование технологии Windows Installer обеспечивает возможность групповой установки программного обеспечения ViPNet на компьютерах в домене Windows. Администратор сети ViPNet с помощью средств Windows может формировать пакеты, содержащие в себе установочные файлы MSI, и публиковать их на сервере обновлений для рассылки на компьютеры домена. Пользователи получают уведомления Центра обновления Windows и могут выполнить установку программного обеспечения.

Установка ПО с использованием сценария входа в систему

Благодаря разработке установочного пакета MSI вы можете выполнить групповую установку программного обеспечения ViPNet с помощью сценария входа в систему (logon script). Таким образом, установить ПО можно одновременно на любое количество компьютеров в домене Windows. Для выполнения такой установки:

- 1 Поместите установочный файл MSI в папку, доступную всем пользователям, на чьи компьютеры требуется установить ПО.

- 2 Настройте групповую политику, создав установочный пакет и сценарий входа в систему, согласно которому на компьютерах пользователей будет выполнена установка ПО.

Неинтерактивный режим установки

Для версии 4.x изменен принцип установки программы ViPNet Монитор в неинтерактивном режиме. В версии 3.2.x установочный файл запускается из командной строки, а параметры установки считываются из специального файла `silent.ini`. В версии 4.x вы можете запустить установочный файл и задать параметры установки в командной строке. Например, можно указать, нужна ли принудительная перезагрузка компьютера после установки программы, и задать список устанавливаемых компонентов.

Использование неинтерактивного режима позволяет:

- выполнять удаленную установку;
- создавать программы, обращающиеся к командной строке Windows и запускающие автоматическую установку ПО ViPNet Client или ViPNet Coordinator с заданными параметрами.

Установка и настройка программы ViPNet CSP

Для работы программ ViPNet Client и ViPNet Coordinator на компьютере должен быть установлен криптопровайдер ViPNet CSP, который может использоваться для реализации криптографических функций в операционной системе Windows.



Примечание. Программы ViPNet Client и ViPNet Coordinator версии 4.x совместимы с программой ViPNet CSP только версии 4.x.

Программа ViPNet CSP теперь может быть установлена как из отдельного установочного файла, так и вместе с программами ViPNet Client и ViPNet Coordinator. При любом из способов ViPNet CSP устанавливается как отдельная программа, что обеспечивает удобство обновления ViPNet CSP независимо от программ ViPNet Client и ViPNet Coordinator.

При запуске установочного пакета для ViPNet Client или ViPNet Coordinator программа установки проверяет наличие на компьютере программы ViPNet CSP и автоматически устанавливает ее в случае отсутствия.

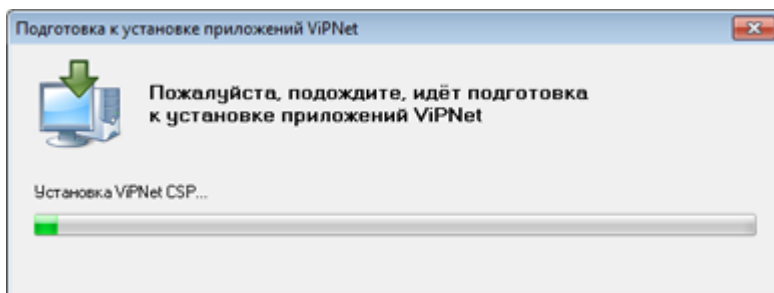


Рисунок 1: Автоматическая установка ViPNet CSP

В версии 3.2.x настройка криптопровайдера ViPNet CSP выполняется в программе ViPNet Монитор в окне **Настройка параметров безопасности** на вкладке **Криптопровайдер**. В версии 4.x настройка криптопровайдера выполняется в отдельной программе ViPNet CSP. На вкладке **Криптопровайдер** программы ViPNet Монитор доступен только переход к настройке криптопровайдера (кнопка **Настройка ViPNet CSP**).

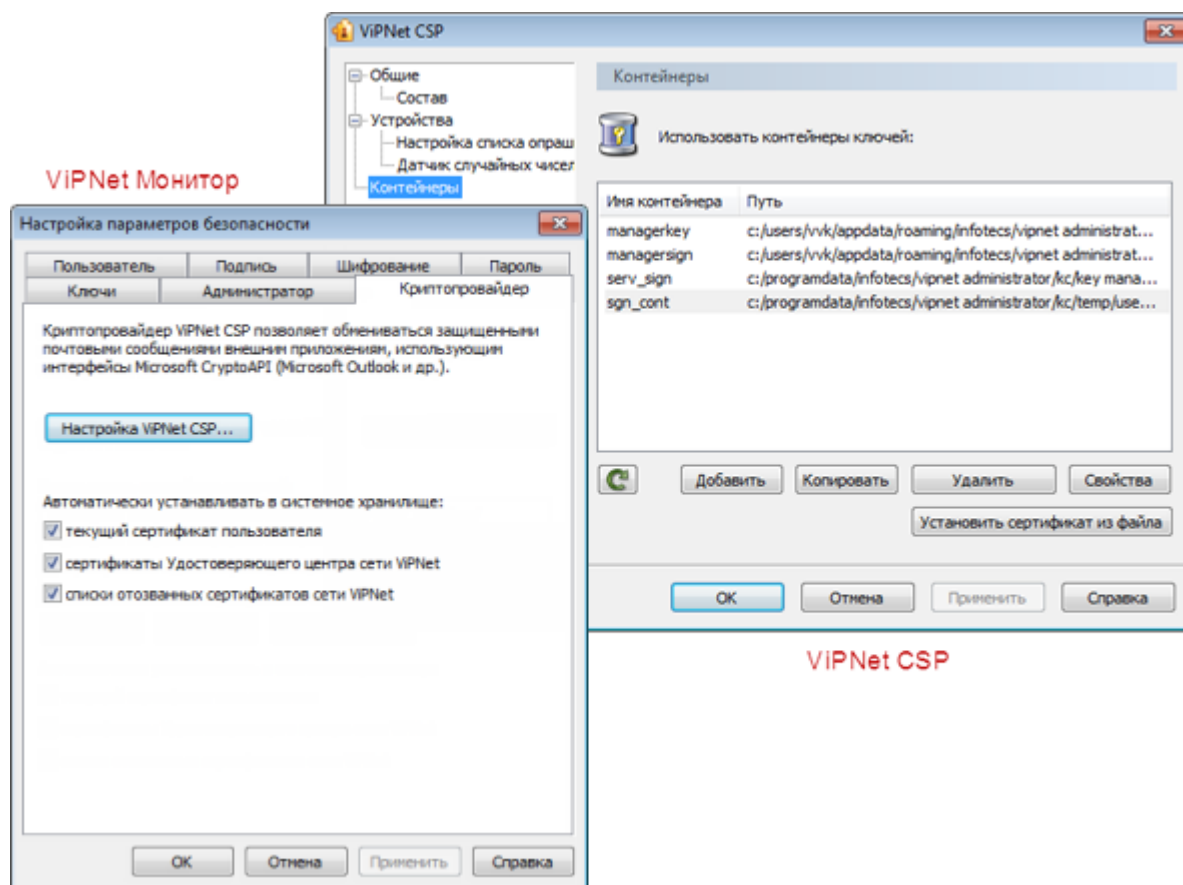


Рисунок 2: Настройка параметров криптопровайдера

Совместимость с ОС Windows

Программы ViPNet Client и ViPNet Coordinator версии 4.x могут быть установлены на компьютер под управлением ОС Windows 8 (32/64-разрядной) и Windows Server 2012 (64-разрядной).

Начиная с версии 4.x, программу ViPNet Policy Manager невозможно установить на компьютер под управлением операционной системы Windows более ранней версии, чем Windows 7.

Логика отключения Windows Firewall

При установке программ ViPNet Client и ViPNet Coordinator версии 4.x стандартный сетевой экран Windows остается включенным и выключается автоматически только при первом запуске программы. Такая логика позволяет обеспечить непрерывную защиту вашего компьютера при развертывании сети. Сообщение об отключении сетевого экрана не выводится. В версиях 3.2.x сетевой экран выключается при установке программного обеспечения.

Установка ключей ViPNet

В программе ViPNet Монитор версии 4.x мастер первичной инициализации больше не используется. Мастер установки ключей позволяет выполнять все сценарии, связанные с установкой или заменой ключей на сетевом узле ViPNet, а именно:

- Установка справочников и ключей ViPNet (см. «Справочники и ключи» на стр. 74) на сетевом узле.
- Добавление пользователя на сетевой узел.
- Смена сетевого узла, развернутого на компьютере.
- Повторная установка ключей.
- Удаление справочников и ключей из папки ключей сетевого узла.

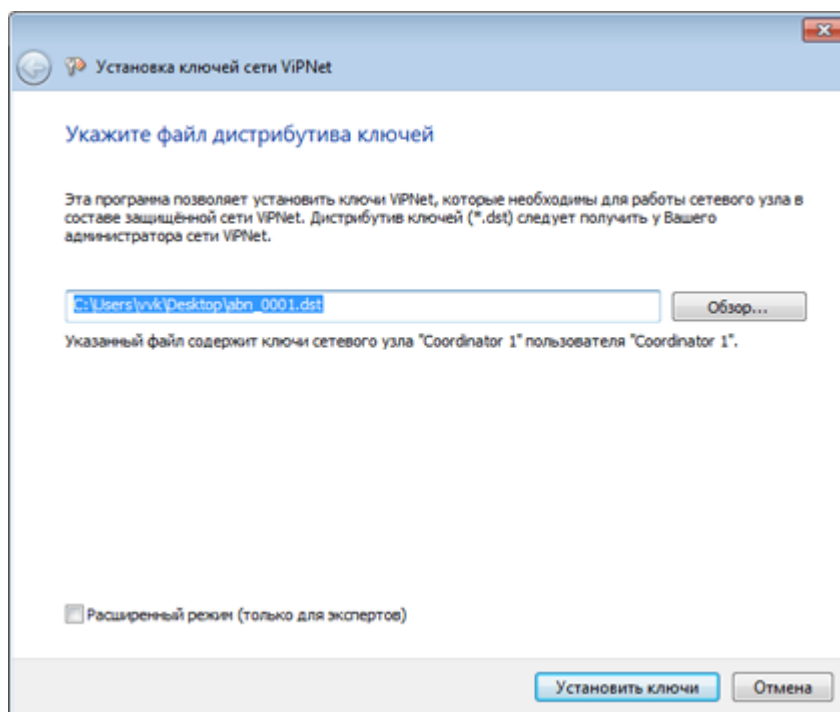


Рисунок 3: Мастер установки ключей в версии 4.x

В версии ViPNet CUSTOM 4.x мастер установки ключей ViPNet производит более полный анализ данных, содержащихся в дистрибутиве ключей (см. «[Дистрибутив ключей](#)» на стр. 73), а также файлов, находящихся в папке ключей сетевого узла.

Система обновления ViPNet

В ViPNet Монитор версии 3.2.x информация о поступлении файлов обновления программного обеспечения или справочников и ключей отображается в виде сообщений. В окне сообщения можно принять или отклонить полученное обновление.

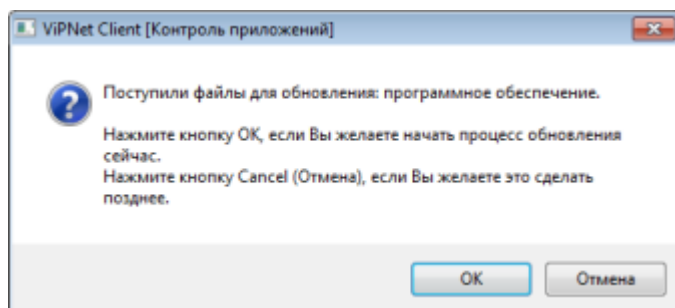


Рисунок 4: Сообщение о поступлении файлов для обновления ПО ViPNet

В ViPNet Монитор версии 4.x прием и установка обновлений осуществляется с помощью системы обновления ViPNet. При совместной работе с ViPNet Policy Manager сюда также поступают и обновления политик безопасности.

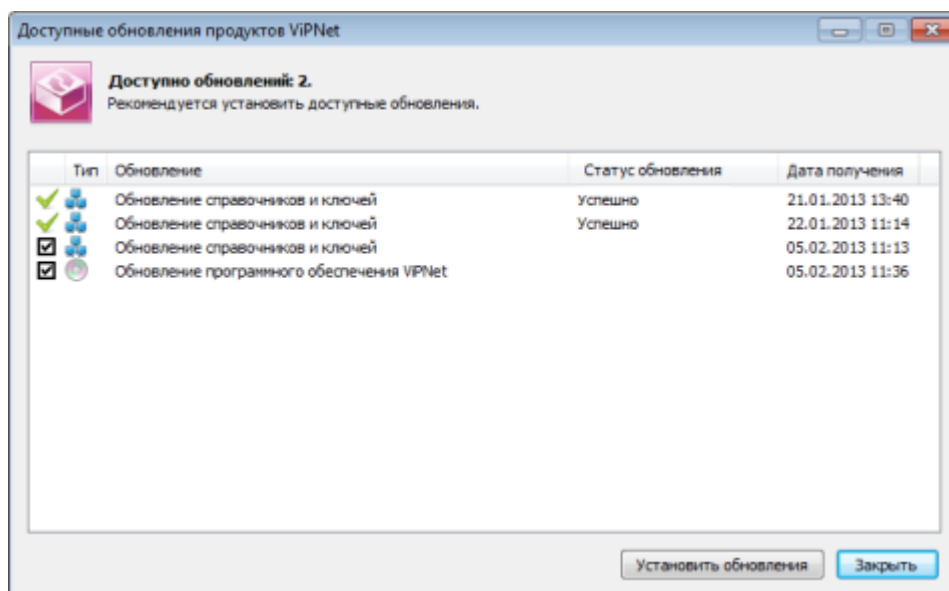


Рисунок 5: Система обновления ViPNet

Установка обновлений может осуществляться как в автоматическом режиме, так и вручную.

Если настроена автоматическая установка обновлений, то все операции система обновления ViPNet производит в «тихом» режиме без выдачи сообщений на экран. Если настроена установка обновлений вручную, то при поступлении файлов обновления в области уведомлений отображается соответствующая информация.

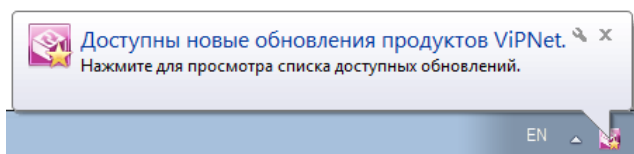


Рисунок 6: Отображение наличия обновлений в области уведомлений



2

Защита трафика

Фильтрация трафика	18
Группы объектов	30
Антиспуфинг	34
Настройка параметров сетевых интерфейсов	36
Блокировка компьютера и IP-трафика	37
Новые алгоритмы электронной подписи	39

Фильтрация трафика

В данном разделе описаны доработки программ ViPNet Client и ViPNet Coordinator, касающиеся фильтрации трафика, трансляции IP-адресов, а также совместимости с программой ViPNet Policy Manager для централизованного управления политиками безопасности.

Получение и применение политик безопасности из ViPNet Policy Manager

В программе ViPNet Монитор реализована возможность применять сетевые фильтры (см. «Сетевой фильтр» на стр. 73) и правила трансляции IP-адресов, созданные в программе ViPNet Policy Manager. Программа ViPNet Policy Manager предназначена для централизованного управления политиками безопасности (см. «Политика безопасности» на стр. 73) узлов защищенной сети ViPNet. Программа ViPNet Policy Manager позволяет задавать различные политики безопасности как для отдельных сетевых узлов, так и для групп узлов и централизованно рассылать их на сетевые узлы.



Рисунок 7: Рассылка политик безопасности

Когда политики безопасности из ViPNet Policy Manager поступают на сетевой узел, пользователь получает уведомление системы обновления ViPNet.

Если пользователь подтверждает обновление политики безопасности на сетевом узле, то программа ViPNet Монитор перезапускается, после чего политика безопасности

применяется на узле. Полученные в составе политики фильтры и правила недоступны для редактирования.

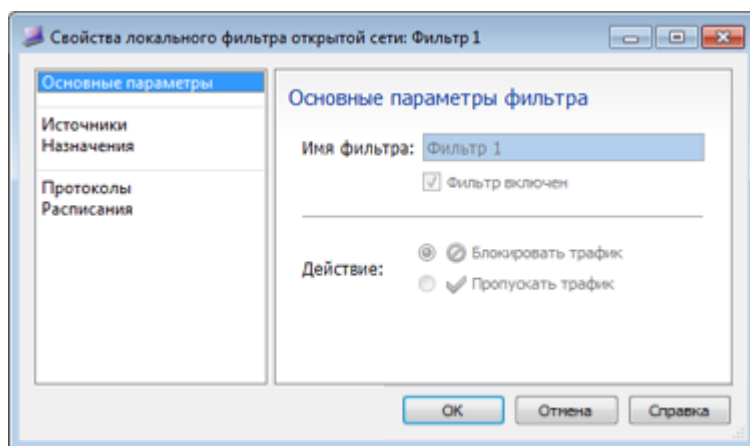


Рисунок 8: Свойства сетевого фильтра, созданного в программе ViPNet Policy Manager

Если возникла необходимость отменить действие всех примененных политик безопасности ViPNet Policy Manager, в программе ViPNet Монитор при работе от имени администратора сетевого узла в разделе **Администратор** снимите флажок **Применять политики безопасности**.

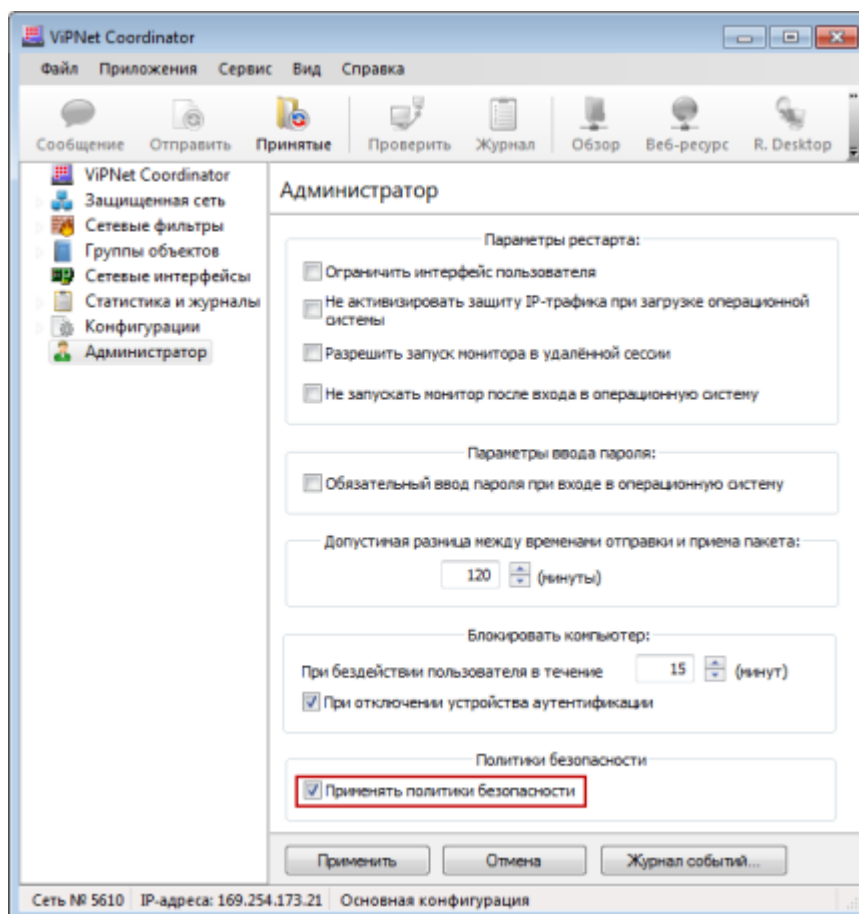


Рисунок 9: Настройка применения политик безопасности Policy Manager

В этом случае действие уже принятых политик безопасности будет прекращено (сетевые фильтры, которые были получены в составе политик, будут скрыты и перестанут использоваться), на узел ViPNet Policy Manager будет отправлена информация о том, что новые политики безопасности на данном узле приниматься не будут.

Если флажок **Применять политики безопасности** впоследствии будет повторно установлен, то действие уже принятых политик и получение новых политик из программы ViPNet Policy Manager будет возобновлено.

Новый формат сетевых фильтров, совместимый с ViPNet Policy Manager

Чтобы применение политик безопасности, созданных в программе ViPNet Policy Manager, стало возможным, разработан новый общий формат сетевых фильтров и правил трансляции IP-адресов для программ ViPNet Монитор и ViPNet Policy Manager. Подробнее об особенностях сетевых фильтров и правил трансляции IP-адресов версии 4.x

см. в разделе [Особенности формата фильтров в версии 4.x по сравнению с версией 3.2.x](#) (на стр. 22). Для удобства просмотра и работы с фильтрами и правилами трансляции представление фильтров в программах ViPNet Монитор и ViPNet Policy Manager приведено к единому виду.

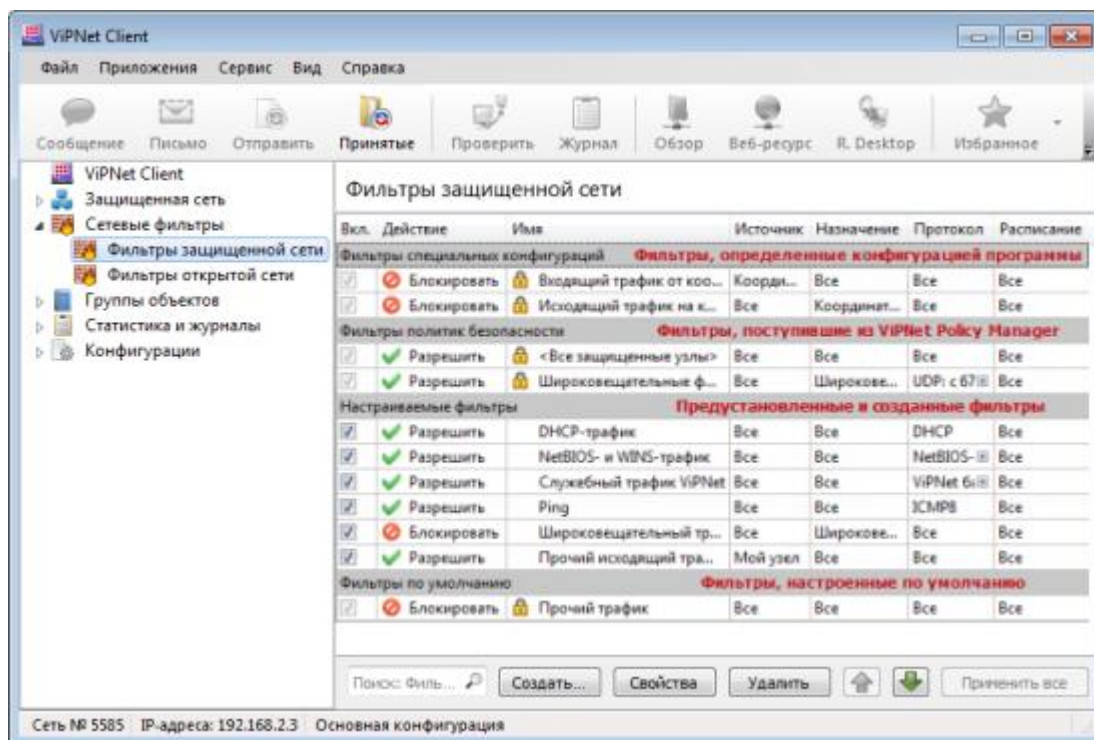


Рисунок 10: Отображение сетевых фильтров в программе ViPNet Монитор

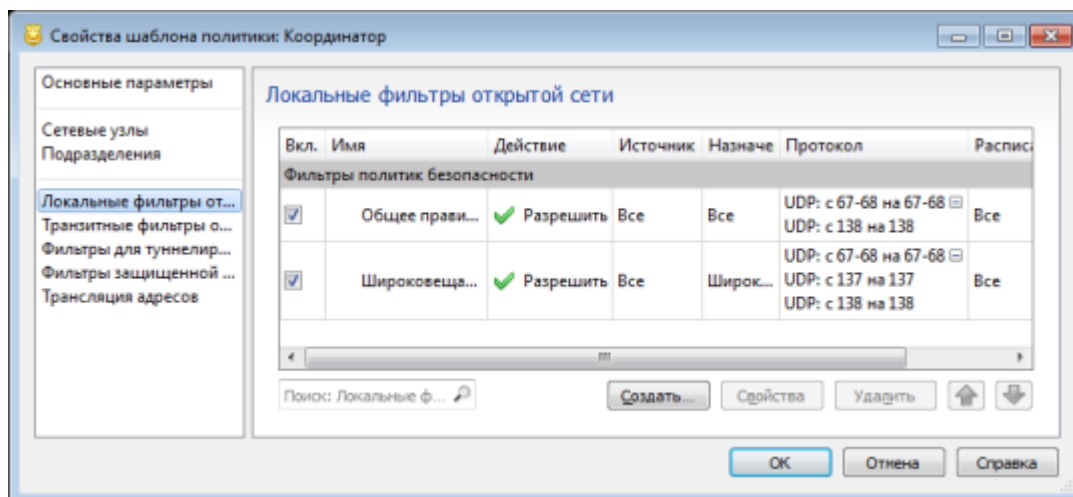


Рисунок 11: Отображение фильтров в программе ViPNet Policy Manager

В связи с использованием политик безопасности, созданных в программе ViPNet Policy Manager, изменился порядок применения сетевых фильтров и правил трансляции IP-адресов. Подробнее см. раздел [Приоритет сетевых фильтров](#) (на стр. 27).

При создании сетевых фильтров и правил трансляции в программах ViPNet Монитор и ViPNet Policy Manager параметры можно задавать, используя группы объектов (на стр. 30), например, источник или назначение можно задавать группой сетевых узлов или IP-адресов.

Особенности формата фильтров в версии 4.x по сравнению с версией 3.2.x

В связи с использованием нового формата фильтров при обновлении программ ViPNet Client и ViPNet Coordinator до версии 4.x выполняется конвертация правил фильтрации трафика версии 3.2.x в сетевые фильтры и правила трансляции IP-адресов версии 4.x. Конвертация правил фильтрации приводит к преобразованию их формата, но не затрагивает содержание, поэтому никаких дополнительных действий со стороны пользователя после перехода на новый формат не требуется.

Особенности нового формата сетевых фильтров и правил трансляции IP-адресов:

- **Новая концепция задания правил и фильтров**

В программе ViPNet Монитор версии 3.2.x для фильтрации трафика нужно задавать правила фильтрации трафика и в рамках правила задавать фильтры.

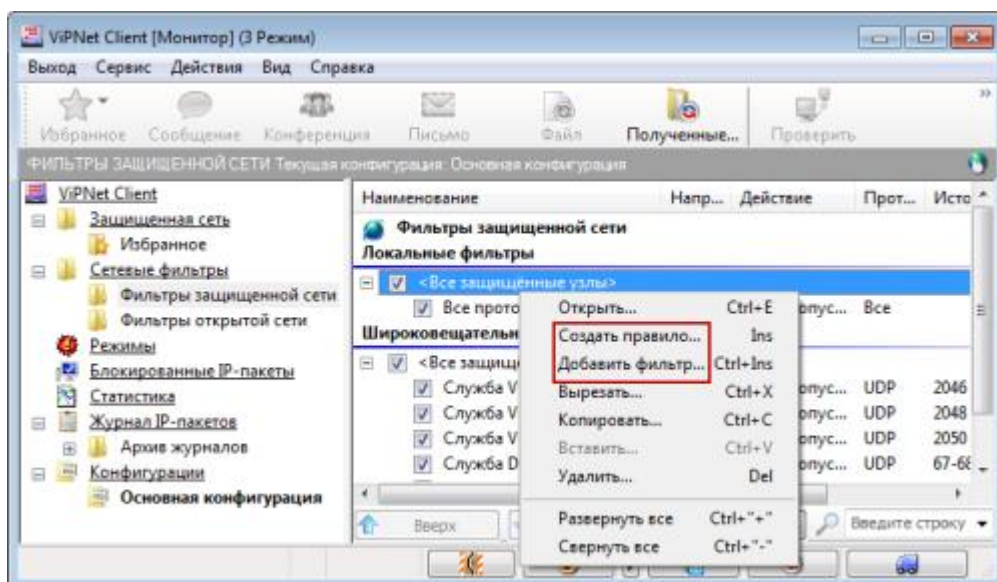


Рисунок 12: Создание правил и фильтров в версии 3.2.x

В версии 4.x правила и фильтры объединены и представлены как сетевые фильтры. Понятие правил фильтрации не используется. В обеих версиях можно задать правила трансляции IP-адресов.

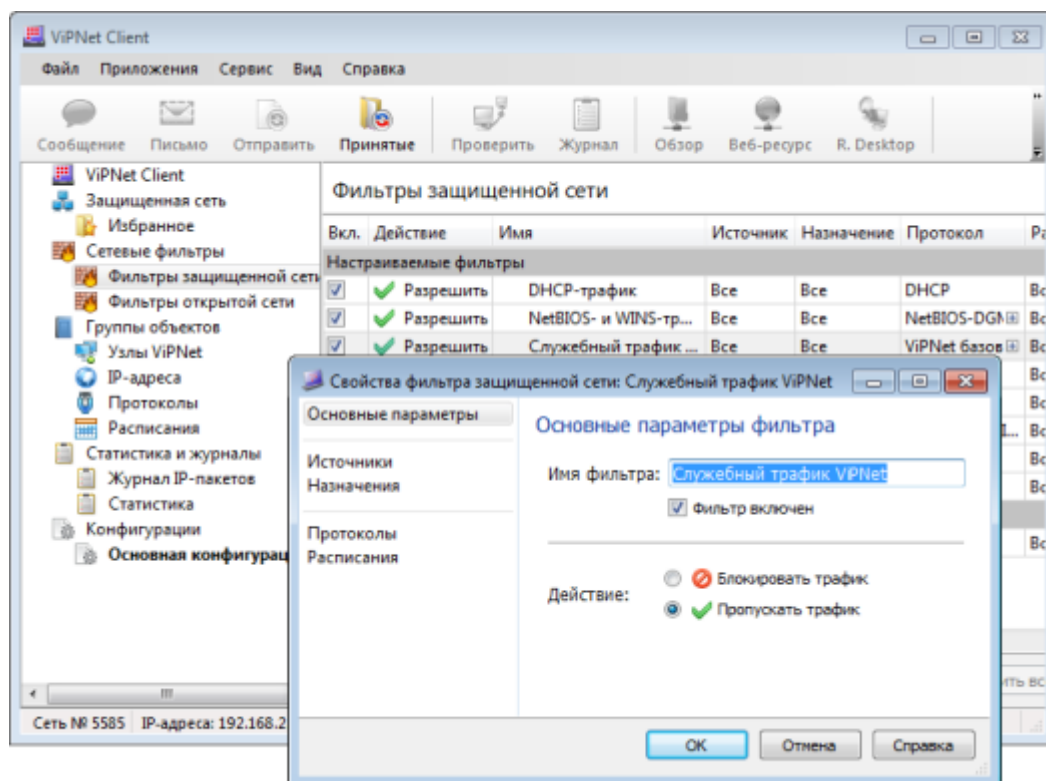


Рисунок 13: Создание правил и фильтров в версии 4.x

- **Направление соединения**

В программе ViPNet Монитор 3.2.x в правилах фильтрации трафика направление соединения может быть входящим, исходящим и двунаправленным.

В программе ViPNet Монитор 4.x при создании фильтров источник (узел или адрес отправителя) и назначение (узел или адрес получателя) можно задавать группами объектов или системными объектами, по которым определяется направление соединения. Например, если в качестве источника выбран объект **Мой узел**, значит, фильтр будет действовать на исходящие соединения. Если в качестве источника выбран объект **Другие узлы**, значит, фильтр будет действовать на входящие соединения.

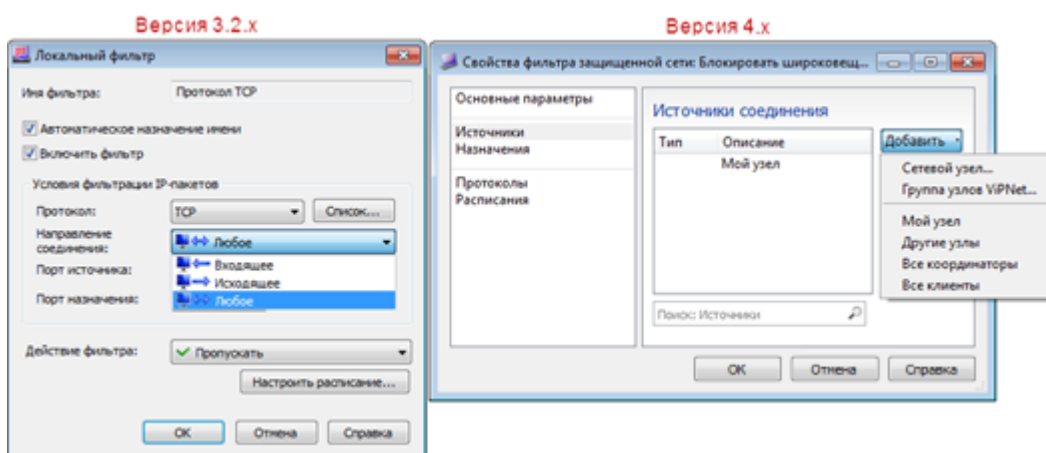


Рисунок 14: Определение направления фильтра

- **Правила трансляции IP-адресов**

В программе ViPNet Монитор 3.2.x при настройке правил трансляции в рамках одного правила можно задавать трансляцию либо только адреса источника (статическое правило), либо только адреса назначения IP-пакетов (динамическое правило).

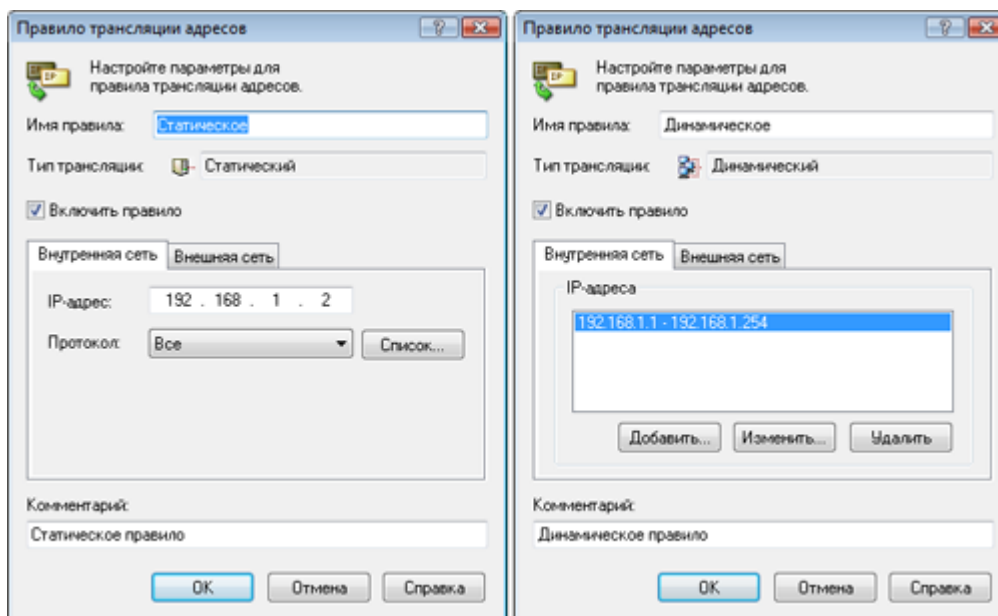


Рисунок 15: Создание правил трансляции IP-адресов в версии 3.2.x

В программе ViPNet Монитор 4.x при создании [правила трансляции IP-адресов](#) (на стр. 28) можно задать трансляцию одновременно и источника, и назначения IP-пакетов.

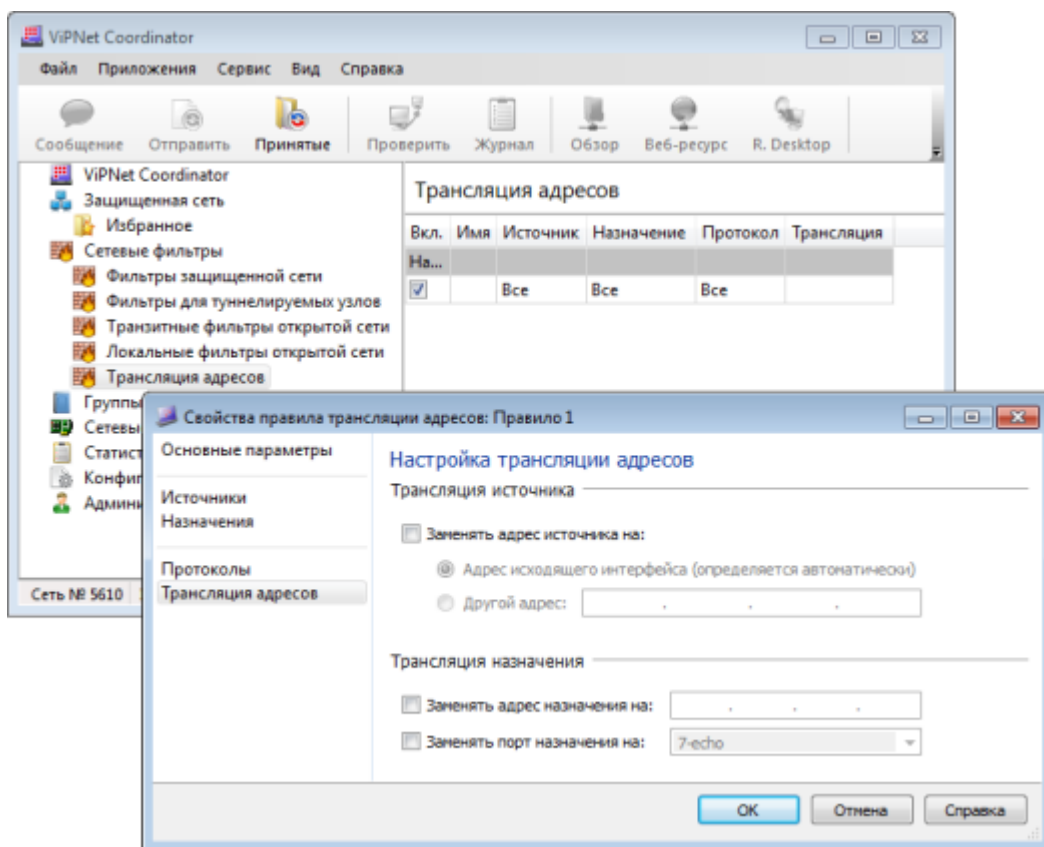


Рисунок 16: Создание правил трансляции IP-адресов в версии 4.x

- **Расписание**

В программе VIPNet Монитор 3.2.x при создании расписания действия фильтра можно указать время, когда фильтр будет действовать (**В указанное время**), а также задать исключение, другими словами расписание, согласно которому фильтр применяться не будет (**Все время кроме указанного**).

В программе VIPNet Монитор 4.x задавать исключения нужно не в свойствах сетевых фильтров, а в свойствах группы расписаний.

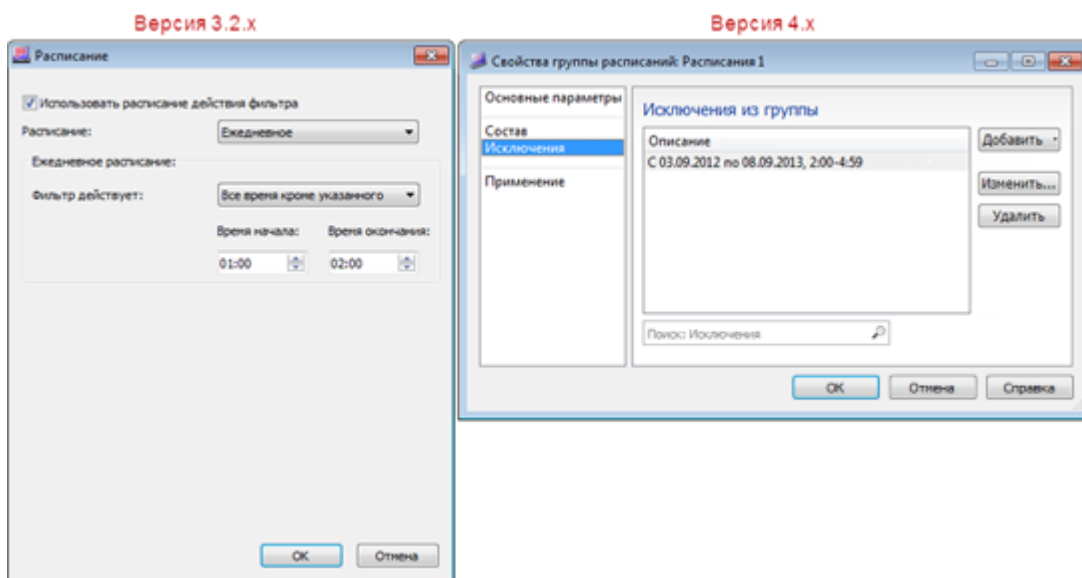


Рисунок 17: Задание исключения из расписания

- **Широковещательные фильтры**

В программе VIPNet Монитор 3.2.x широковещательные фильтры вынесены в отдельные списки в разделах фильтров защищенной и открытой сетей.

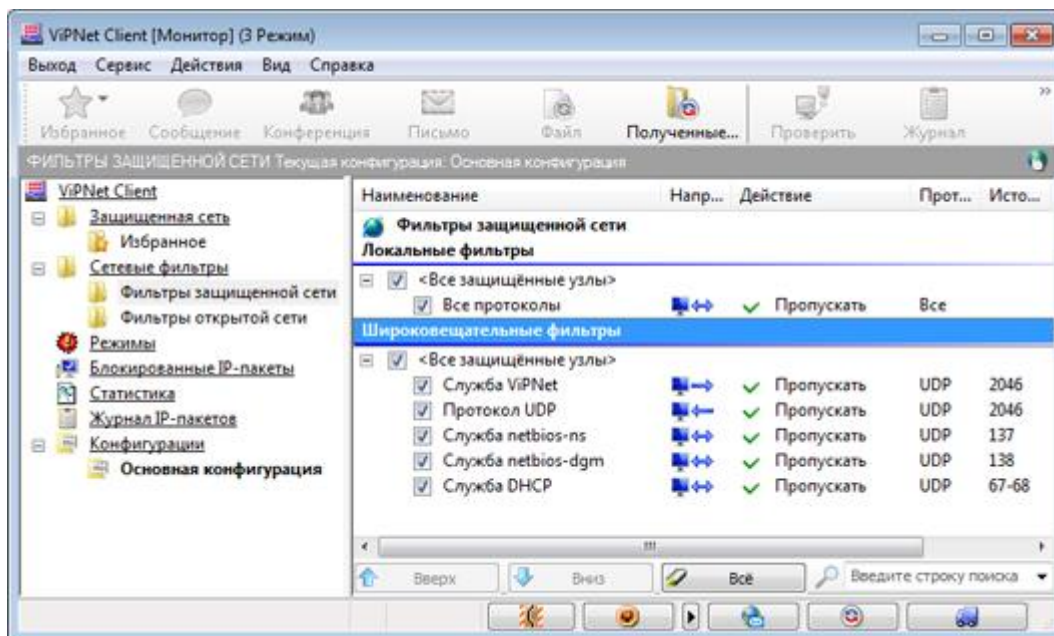


Рисунок 18: Отображение широковещательных фильтров в версии 3.2.x

В программе VIPNet Монитор 4.x широковещательные фильтры не выделяются в отдельную группу, а отображаются в общем списке фильтров защищенной или

открытой сети. При создании широковещательных фильтров в качестве назначения нужно указывать **Широковещательные адреса**.

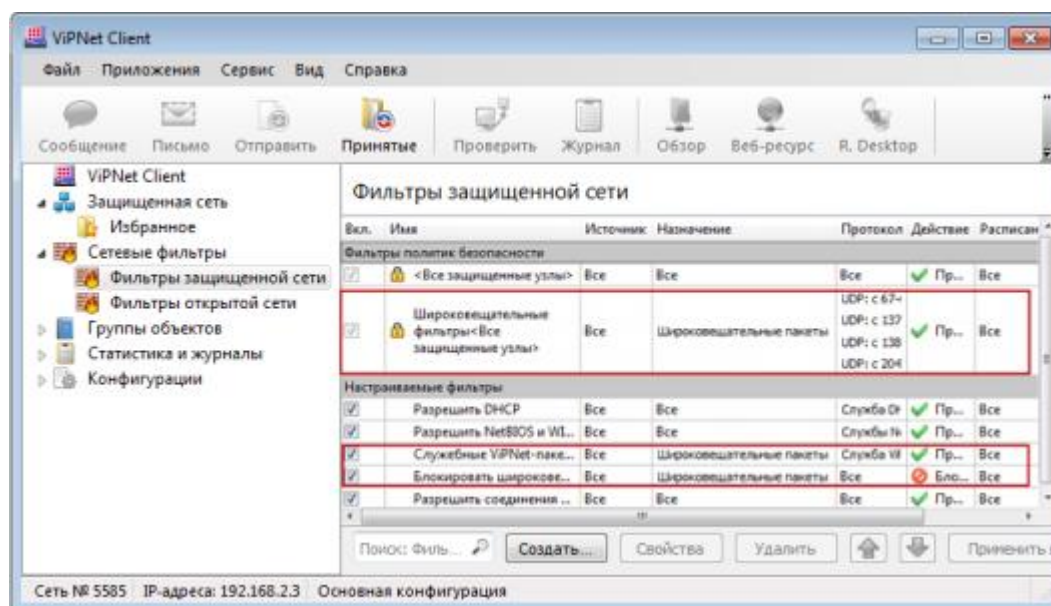


Рисунок 19: Отображение широковещательных фильтров в версии 4.x

Приоритет сетевых фильтров

В программе ViPNet Монитор версии 4.x сетевые фильтры и правила трансляции IP-адресов применяются сверху вниз согласно спискам сетевых фильтров, которые можно просмотреть в главном окне программы в разделе **Сетевые фильтры**.

Фильтры, зависящие от специальных конфигураций программы, имеют более высокий приоритет, чем все остальные фильтры и применяются в первую очередь. Они могут использоваться только в программе ViPNet Client Монитор. Их нельзя редактировать или удалять. Фильтры, поступившие из программы ViPNet Policy Manager, идут после фильтров конфигураций и недоступны для редактирования. Далее размещаются предустановленные фильтры и фильтры, заданные пользователем в программе ViPNet Монитор. При определенных полномочиях их можно изменить или удалить. Последними по приоритету являются фильтры по умолчанию. Данная категория представлена одним сетевым фильтром, блокирующим IP-трафик, который не соответствует ни одному из сетевых фильтров из категорий выше.

Последовательность применения сетевых фильтров согласно приоритету в программе ViPNet Client Монитор изображена на схеме ниже.

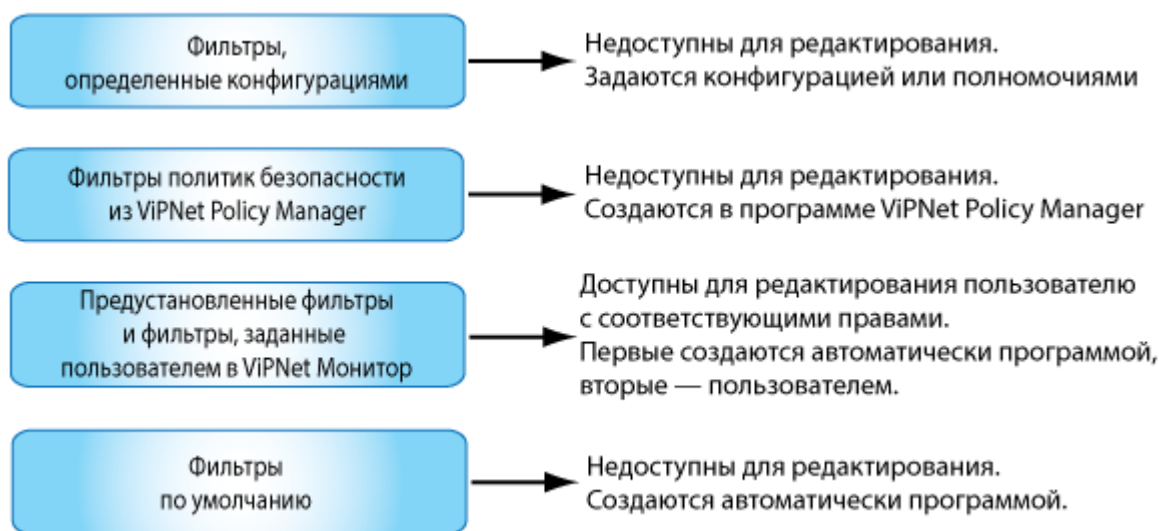


Рисунок 20: Приоритет применения сетевых фильтров



Примечание. В программе ViPNet Coordinator Монитор фильтры, определенные конфигурациями, не используются. Политики безопасности ViPNet Policy Manager и фильтры, заданные пользователем, применяются согласно приоритету, изображенному на схеме.

Правила трансляции IP-адресов

В программе ViPNet Монитор версии 4.x вы можете задавать трансляцию источника и трансляцию назначения в одном правиле. Такая возможность обеспечивает удобство при организации взаимодействия между сегментами сети через координатор, выполняющий трансляцию IP-адресов, при этом обеспечивая изолированность этих сегментов друг от друга. Таким образом, информация об IP-адресах, используемых в этих сегментах, имеется только на координаторе. Эта функциональность применима, например, в схеме DMZ (см. «DMZ (демилитаризованная зона)» на стр. 72).

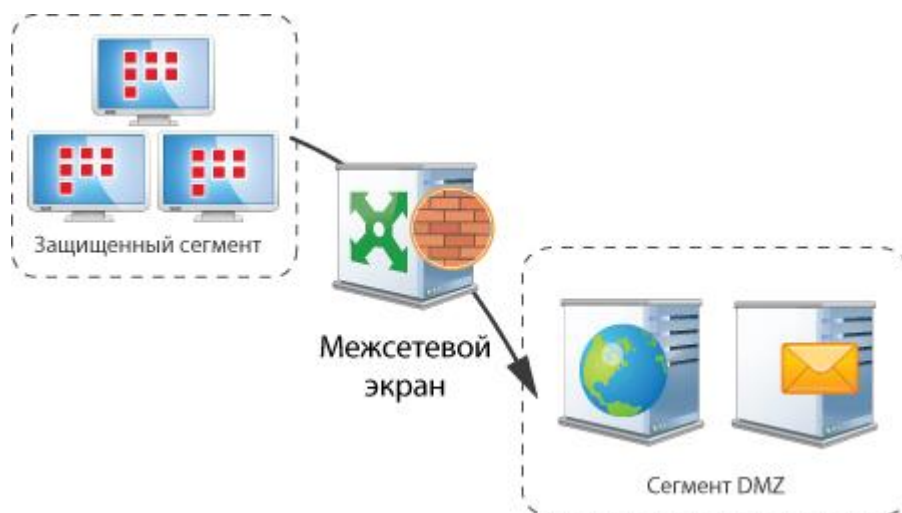


Рисунок 21: Взаимодействие сегментов сети в схеме DMZ

Допустим, сетевые узлы защищенного сегмента устанавливают соединение с узлами сегмента DMZ по IP-адресу координатора со стороны защищенного сегмента. Согласно правилу трансляции, IP-адреса сетевых узлов защищенного сегмента (IP-адреса источника) будут преобразованы в IP-адрес координатора со стороны сегмента DMZ. IP-адрес координатора со стороны защищенного сегмента, указанный в качестве назначения, будет преобразован в IP-адрес нужного узла в сегменте DMZ.

Группы объектов

В версии 4.x реализована возможность создания групп объектов. Группы объектов — это средство, позволяющее упростить создание сетевых фильтров и правил трансляции адресов в программе ViPNet Монитор. Они объединяют несколько значений одного типа и могут быть заданы при настройке параметров фильтра или правила вместо отдельных объектов. Группы объектов могут использоваться при создании других групп объектов, а также при создании сетевых фильтров и правил трансляции в программе ViPNet Policy Manager.

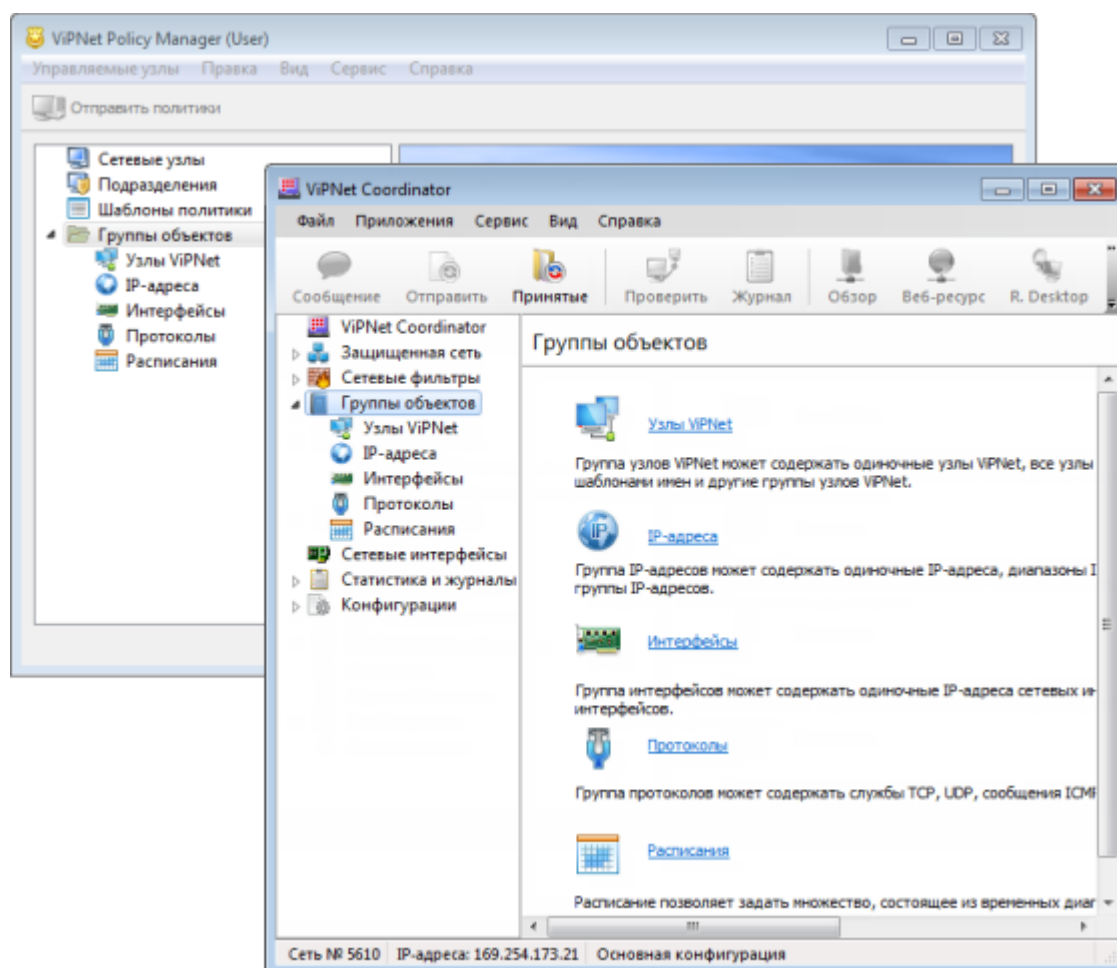


Рисунок 22: Группы объектов в программах ViPNet Монитор и ViPNet Policy Manager

Существуют следующие виды групп объектов:



Рисунок 23: Виды групп объектов

- Системные группы объектов. Встроены в ПО ViPNet Policy Manager, ViPNet Client Монитор и ViPNet Coordinator Монитор и не могут быть изменены.
- Группы объектов, создаваемые пользователями программы ViPNet Policy Manager. Рассылаются вместе с политиками безопасности и недоступны для редактирования на сетевом узле.
- Группы объектов, создаваемые пользователями программ ViPNet Client Монитор и ViPNet Coordinator Монитор, а также некоторые группы, заданные по умолчанию. Могут редактироваться пользователем на узле.

Системные группы объектов

Системные группы объектов — это встроенные в ПО ViPNet группы объектов с фиксированными именами, которые могут использоваться при создании сетевых фильтров и групп объектов.



Примечание. Системные группы объектов нельзя изменить или удалить.

Каждая системная группа объектов имеет свою область применения:

- 1 Группа **Все клиенты** содержит все клиенты из справочников узла.
- 2 Группа **Все координаторы** содержит все координаторы из справочников узла.

- 3 Группа **Все объекты** содержит все объекты в группы конкретного типа. Эта группа задается только в составе группы объектов и предназначена для создания групп, состоящих из всех объектов, кроме некоторых исключений.
- 4 Группа **Широковещательные адреса** содержит все широковещательные адреса и используется при создании фильтров широковещательных пакетов.
- 5 Группа **Мой узел** содержит свой узел, и эту группу можно указать в качестве источника IP-пакетов для исходящих соединений узла или в качестве назначения для входящих соединений.
- 6 Группа **Другие узлы** содержит любые сетевые узлы, кроме своего. Эту группу можно указать в качестве источника IP-пакетов для входящих соединений узла или в качестве назначения для исходящих соединений.
- 7 Группа **Туннелируемые IP-адреса** содержит все IP-адреса, туннелируемые координатором.
- 8 Группа **Групповые адреса** содержит диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255). Эту группу можно указать только в качестве назначения для локальных открытых соединений.
- 9 Группа **Координаторы Открытого Интернета** содержит множество координаторов открытого Интернета, присутствующих в сети ViPNet. Эта группа используется только в программе ViPNet Client и только в фильтрах, определенных конфигурацией «Открытый Интернет». В создаваемых фильтрах ее указать нельзя.

Пользовательские группы объектов

Пользовательские группы объектов — это группы, которые пользователи программ ViPNet Policy Manager, ViPNet Монитор могут создавать для определенных целей. Имена создаваемых групп объектов должны быть уникальными и отличаться от имен системных групп объектов.

Поддерживаются следующие типы групп объектов:

- **Узлы ViPNet** — группа узлов защищенной сети. Используется в фильтрах защищенной сети и туннелируемых узлов.
- **IP-адреса** — любая комбинация отдельных IP-адресов и диапазонов IP-адресов или DNS-имен. Используется в правилах трансляции IP-адресов и сетевых фильтрах (за исключением фильтров защищенной сети). По умолчанию заданы группы **Публичные IP-адреса** и **Частные IP-адреса**.

- **Интерфейсы** — любая комбинация сетевых интерфейсов или IP-адресов интерфейсов. Используется в сетевых фильтрах только на координаторе (за исключением фильтров защищенной сети).
- **Протоколы** — любая комбинация протоколов и портов. Используется во всех фильтрах и правилах трансляции IP-адресов. По умолчанию данная группа содержит большое количество наиболее распространенных протоколов.
- **Расписания** — любая комбинация условий применения сетевых фильтров по времени и дням недели. Используется во всех фильтрах. По умолчанию заданы группы **Рабочие дни** и **Выходные дни**.

Антиспуфинг

Для обеспечения высокого уровня безопасности сети рекомендуется, чтобы на координаторе была включена функция антиспуфинга (см. «[Антиспуфинг](#)» на стр. 72). В программе ViPNet Coordinator версии 3.2.x требуется выполнять настройку антиспуфинга вручную.

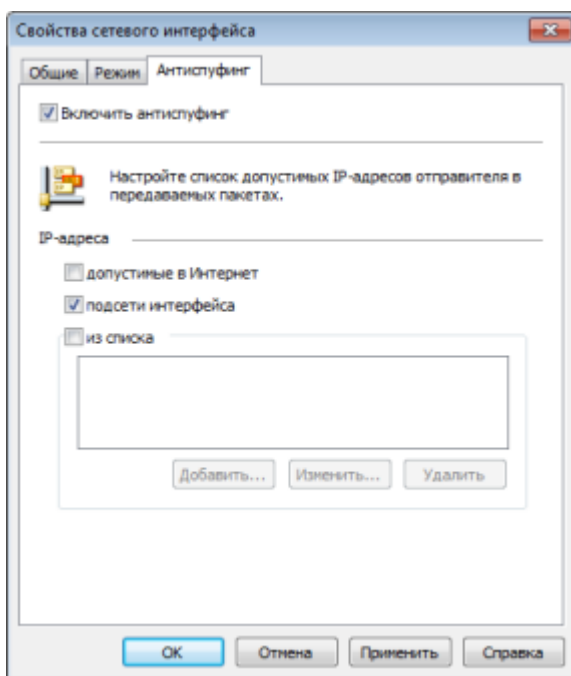


Рисунок 24: Включение функции антиспуфинга в версии 3.2.x

В версии 4.x настройка антиспуфинга не требуется. При включении антиспуфинга соответствующие фильтры формируются автоматически на основе таблицы маршрутизации данного сетевого узла.

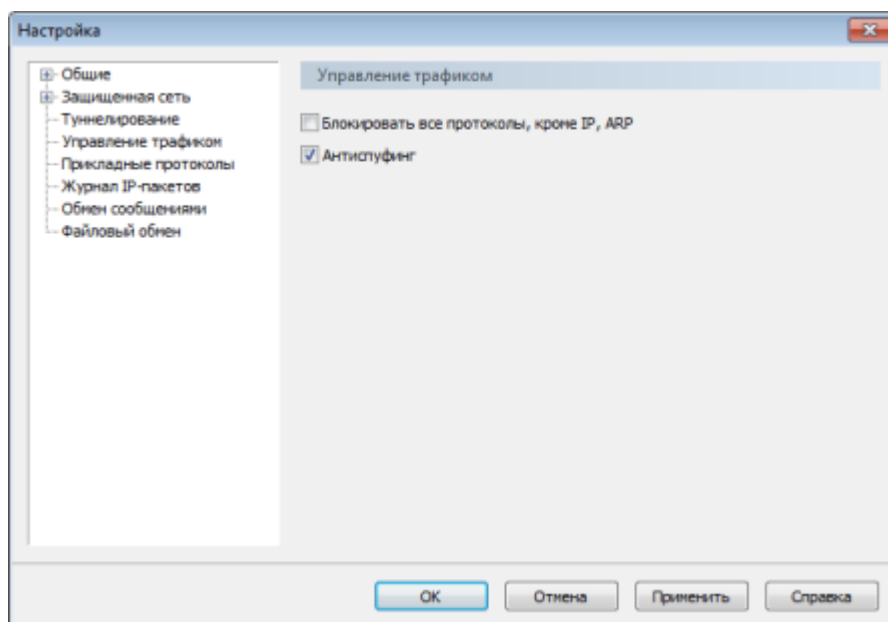


Рисунок 25: Включение функции антиспуфинга в версии 4.x

Настройка параметров сетевых интерфейсов

В программе ViPNet Coordinator Монитор версии 3.2.x в разделе **Сетевые интерфейсы** можно выполнить настройку параметров сетевых интерфейсов, а именно задать псевдоним интерфейса, режим безопасности и параметры пропускания или блокирования пакетов (антиспуфинг). В версии 4.x в разделе **Сетевые интерфейсы** вы можете только просмотреть список сетевых интерфейсов на данном компьютере. Для настройки необходимого уровня безопасности (см. «[Режимы безопасности](#)» на стр. 51) нужно создать соответствующие фильтры и указать в них нужные интерфейсы.

Блокировка компьютера и IP-трафика

В программе ViPNet Монитор версии 4.x из главного окна программы удалена кнопка блокировки компьютера. Блокировка компьютера осуществляется стандартными средствами операционной системы.

С помощью программы ViPNet Монитор версии 4.x вы можете заблокировать весь IP-трафик компьютера. В этом случае любые соединения с защищенными и открытыми узлами будут запрещены.

При необходимости вы можете отключить защиту трафика. В этом случае будет прекращена любая обработка трафика и ведение журнала регистрации IP-пакетов. Соединение с защищенными узлами ViPNet будет невозможно.

Для блокировки или отключения защиты IP-трафика выберите соответствующие пункты (**Блокировать IP-трафик** или **Отключить защиту**) в меню **Файл > Конфигурации**.

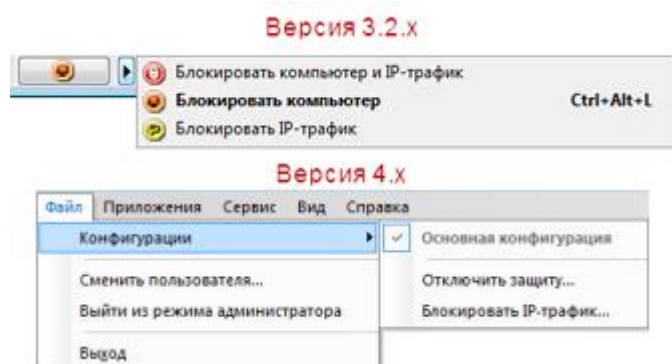


Рисунок 26: Настройка блокировки компьютера и IP-трафика

Обратите также внимание, что для упрощения процедуры блокировки IP-трафика из окна настройки от имени администратора удалена возможность блокировки IP-трафика при отключении устройства аутентификации. Блокируйте IP-трафик вручную, когда это необходимо.

При работе от имени администратора сетевого узла в версиях 3.2.x и 4.x можно настроить автоматическую блокировку компьютера при бездействии пользователя, а также при отключении устройства аутентификации. Для удобства в версии 4.x настройка блокировки компьютера представлена по-новому.

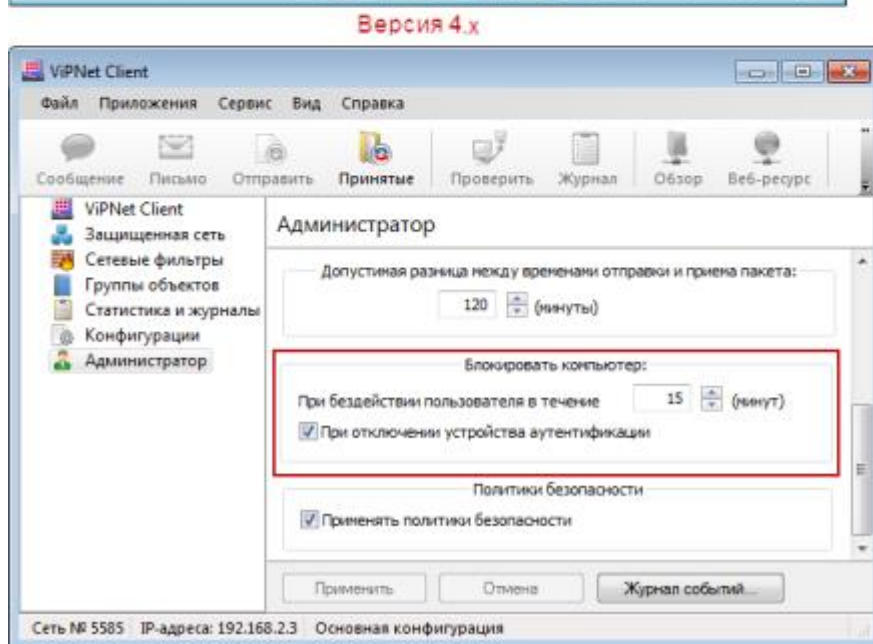
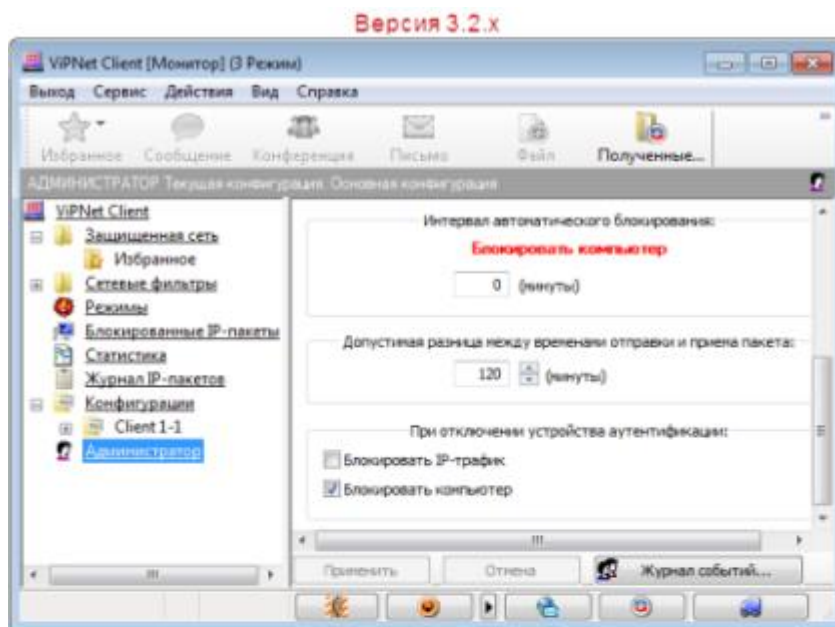


Рисунок 27: Блокировка компьютера при работе от имени администратора

Новые алгоритмы электронной подписи

В программе ViPNet Монитор версии 4.x реализована поддержка ключей электронной подписи, созданных по алгоритму ГОСТ 34.10.2012.

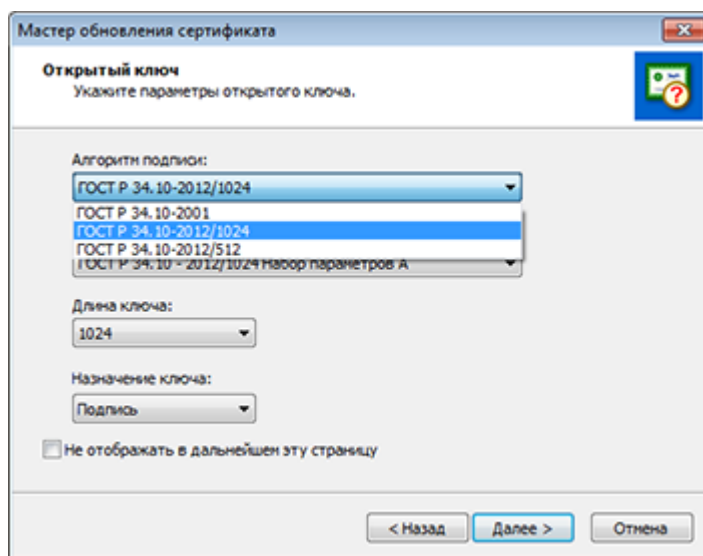


Рисунок 28: Новый алгоритм подписи



3

Подключение к сети ViPNet

Настройка подключения координатора к внешней сети через межсетевой экран со статической или динамической трансляцией адресов	41
Настройка TCP-туннеля	43
Настройка подключения клиентов	46

Настройка подключения координатора к внешней сети через межсетевой экран со статической или динамической трансляцией адресов

В программе ViPNet Coordinator Монитор версии 3.2.x при настройке подключения ViPNet-координатора к внешней сети через межсетевой экран со статической или динамической трансляцией адресов требуется указать сетевой интерфейс, через который будет осуществляться подключение (список **Адаптер, со стороны которого установлен межсетевой экран**).

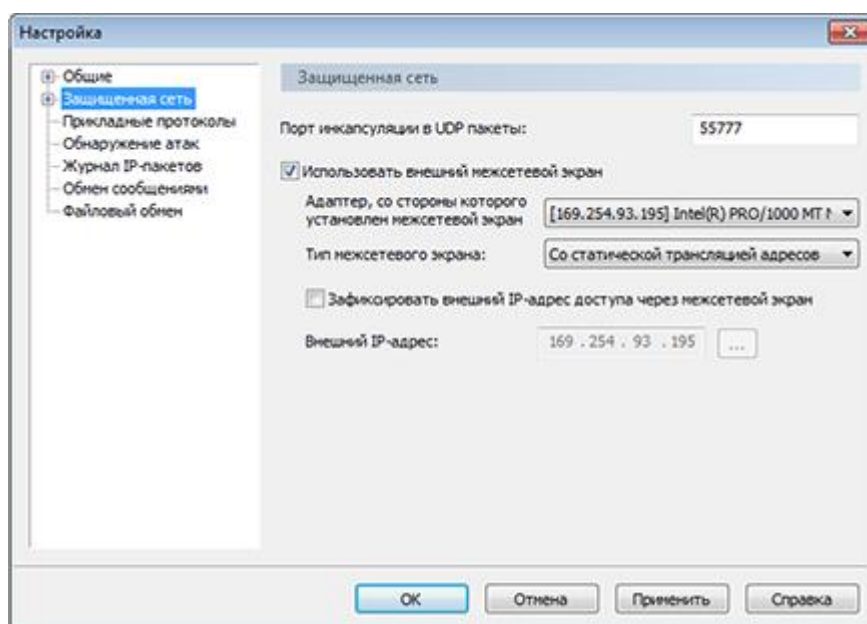


Рисунок 29: Настройка межсетевого экрана со статической трансляцией адресов в версии 3.2.x

В версии 4.x для удобства пользователя данная настройка убрана, а интерфейс определяется автоматически при отправке IP-пакета. Теперь вам нужно указывать интерфейс, только если вы хотите, чтобы все входящие пакеты были направлены через определенный адрес межсетевого экрана (флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран**).

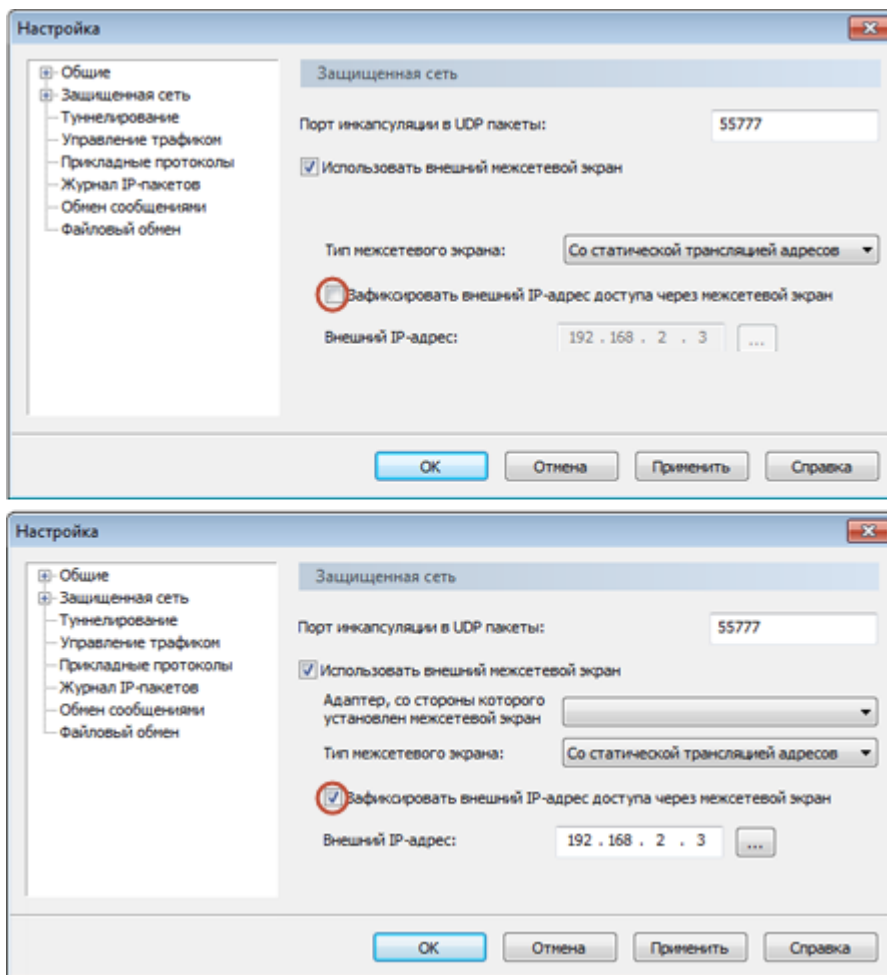


Рисунок 30: Указание интерфейса межсетевого экрана в версии 4.x

Настройка TCP-туннеля

В программном обеспечении ViPNet Coordinator версии 4.x можно настроить TCP-туннель, через который будут осуществляться соединения клиентов, находящихся во внешних сетях, с другими узлами сети ViPNet, в том случае, если при подключении клиентов к внешним сетям провайдером услуг блокируется UDP-протокол.



Рисунок 31: Функция TCP-туннеля

При удаленном подключении клиентов к сетям ViPNet иногда возникает проблема с передачей IP-пакетов по протоколу UDP из-за того, что данный протокол блокируется некоторыми провайдерами услуг. Например, при подключении к сети из гостиниц или других общественных мест. Для решения подобной проблемы можно организовать взаимодействие узлов ViPNet через TCP-туннель на координаторе, с помощью которого они осуществляют соединение. В этом случае, если удаленный клиент не может связаться с другими узлами по протоколу UDP, он автоматически начинает устанавливать с ними соединение через TCP-туннель своего координатора соединений. На координаторе полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.



Примечание. Соединение через TCP-туннель или TCP-соединение — это универсальное HTTP-соединение, которое используется при работе в Интернете и не блокируется провайдерами услуг.

Для настройки TCP-туннеля на координаторе требуется установить соответствующий флажок и задать порт, на который должны поступать TCP-пакеты. Стоит учесть, что TCP-туннель можно настроить только на координаторе, который не установлен за межсетевой экран или установлен за межсетевой экран со статической трансляцией адресов.

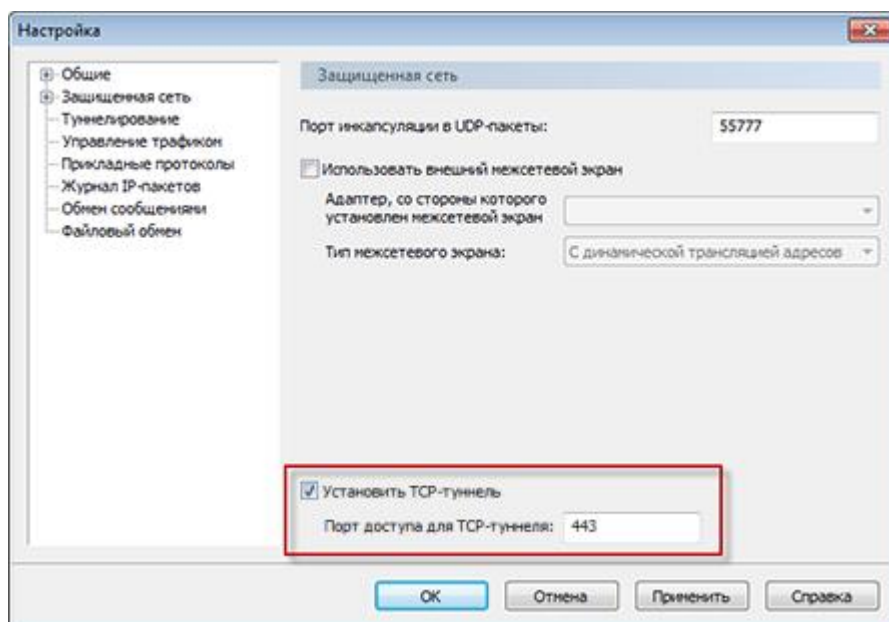


Рисунок 32: Возможность настройки TCP-туннеля в ViPNet Coordinator

Информация о настройке TCP-туннеля с номером порта для передачи TCP-пакетов рассылается на все сетевые узлы, для которых координатор является координатором соединений. На клиенте номер порта доступа к координатору через TCP-туннель отображается в свойствах данного координатора. Если в свойствах координатора порт не указан, но при этом известно, что на этом координаторе развернут TCP-туннель, порт может быть задан вручную.

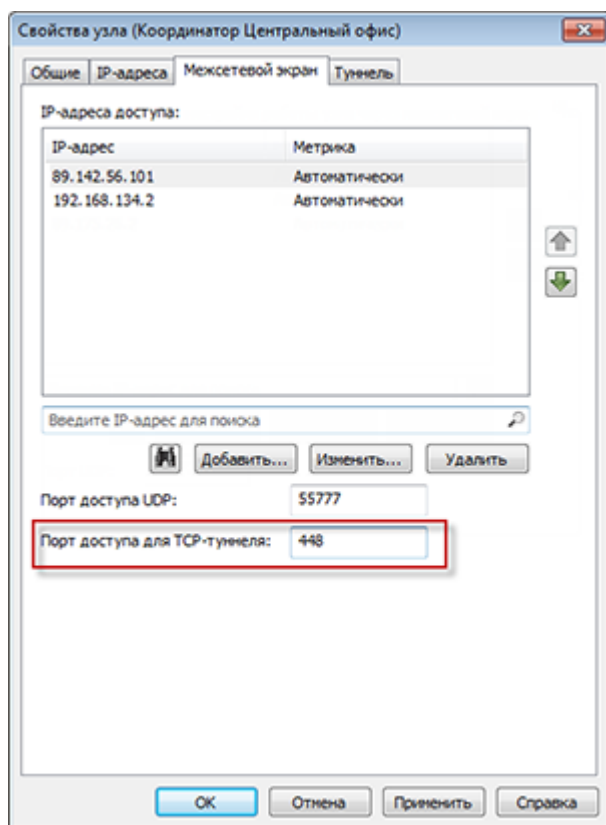


Рисунок 33: Возможность задания порта TCP-туннеля

Настройка подключения клиентов

Клиентские узлы ViPNet теперь автоматически выполняют соединения с другими узлами по прямым доступным маршрутам, а не через координаторы, как это было в предыдущих версиях. За счет этого повысилась скорость обмена шифрованным IP-трафиком.

Для установки соединений клиенты теперь используют координаторы соединений, которые назначаются им в процессе настройки параметров подключения к сети.

Клиенты в процессе соединения с удаленными узлами направляют IP-трафик на свой координатор соединений, с которым постоянно поддерживают связь. Но одновременно с этим они пытаются установить связь с удаленными узлами напрямую либо через их координаторы соединений. Если связь удастся установить, то весь IP-трафик начинает передаваться напрямую.

В связи с этим в новой версии программного обеспечения ViPNet Client была упрощена процедура настройки подключения клиентов к сети ViPNet. Раньше при настройке подключения требовалось указывать сервер IP-адресов и задавать параметры межсетевого экрана, если он использовался. Теперь подключение клиентов к сети в общем случае не требует никаких настроек. Дополнительные настройки при подключении могут потребоваться только в некоторых особых ситуациях. Например, вы подключаете свой ноутбук к локальной сети другой организации, в которой нет доступа к вашему координатору соединений, но есть координатор, имеющий связь с вашим узлом. Или, например, ваш координатор соединений по каким-то причинам оказался недоступным. В этих случаях вы можете изменить координатор соединений для клиента в настройках подключения. Сервер IP-адресов для клиента теперь изменять крайне не рекомендуется. По умолчанию им назначен координатор соединений.

В случае работы клиента через устройство NAT может быть выполнена расширенная настройка подключения, например, установлен параметр фиксирования порта при работе через устройство со статической трансляцией адресов или изменен интервал отправки IP-пакетов координатору при работе через устройство с динамической трансляцией адресов.

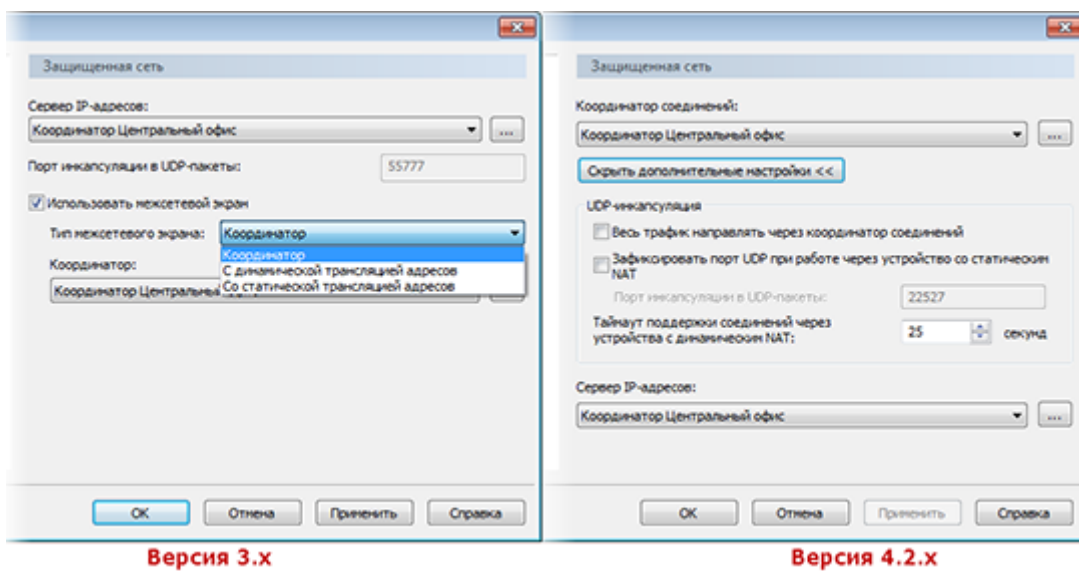


Рисунок 34: Изменение настроек подключения к сети ViPNet в ViPNet Client



4

Безопасность и полномочия пользователя

Способы аутентификации	49
Режимы безопасности	51
Ограниченный интерфейс пользователя	52
Смена конфигураций программы по расписанию	54

Способы аутентификации

В программе ViPNet Монитор версии 4.x при использовании устройства аутентификации (способ **Устройство**) для входа в программу реализована возможность выполнять аутентификацию пользователя не только с помощью персонального ключа (как в версии 3.2.x), но и с помощью сертификата.

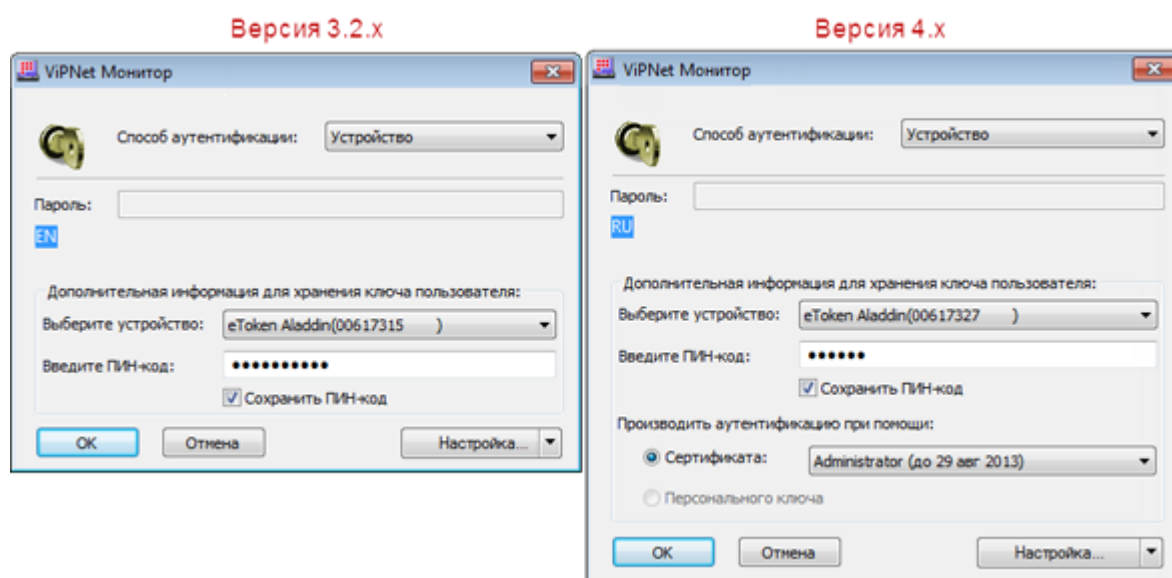


Рисунок 35: Использование устройства для аутентификации пользователя

Используемый для аутентификации сертификат должен быть издан сторонним удостоверяющим центром (см. «[Удостоверяющий центр](#)» на стр. 74). На устройстве также должен быть и закрытый ключ, соответствующий сертификату.

Для аутентификации пользователя с помощью сертификата должны быть выполнены следующие условия:


- Внешнее устройство хранения данных поддерживает стандарт PKCS#11, в том числе операции подписи и шифрования. В текущий момент внешние устройства с поддержкой алгоритма ГОСТ 34.10-2001 использоваться не могут, поскольку они поддерживают только операцию вычисления подписи.
- Сертификат действителен (срок действия сертификата не истек).
- Сертификат не отозван.

- Сертификат имеет назначение «Проверка подлинности клиента». Это назначение отображается в окне **Сертификат**, на вкладке **Состав**, в поле **Расширенное использование ключа**.
- Сертификат издателя установлен в системное хранилище **Доверенные корневые центры сертификации**.

Таким образом, для аутентификации в программе ViPNet Монитор и аутентификации в других приложениях и системах вы можете использовать одно и то же устройство, что обеспечивает удобство и универсальность его использования.

Если в программе ViPNet Монитор версии 3.2.x в качестве способа аутентификации выбран **Пароль на устройстве**, то после обновления на версию 4.x мы настоятельно рекомендуем вам перейти на другой способ аутентификации. В последующих версиях программы ViPNet Монитор способ аутентификации **Пароль на устройстве** поддерживаться не будет.

Внимание! При работе в программе ViPNet Монитор версии 4.x администратор сетевого узла не может задать способ аутентификации **Пароль на устройстве**. Использование данного способа возможно, только если он был выбран еще при работе в версии 3.2.x.

 Способ аутентификации **Пароль на устройстве** не отвечает требованиям безопасности, и возможность его использования оставлена исключительно для совместимости с программным обеспечением ViPNet более ранних версий.

При аутентификации пользователя с помощью пароля (способ **Пароль**) теперь нужно выбирать пользователя, от имени которого выполняется вход в программу. В списке отображаются имена всех пользователей, чьи ключи установлены на данном сетевом узле. По умолчанию предлагается имя пользователя, чьи ключи установлены последними.

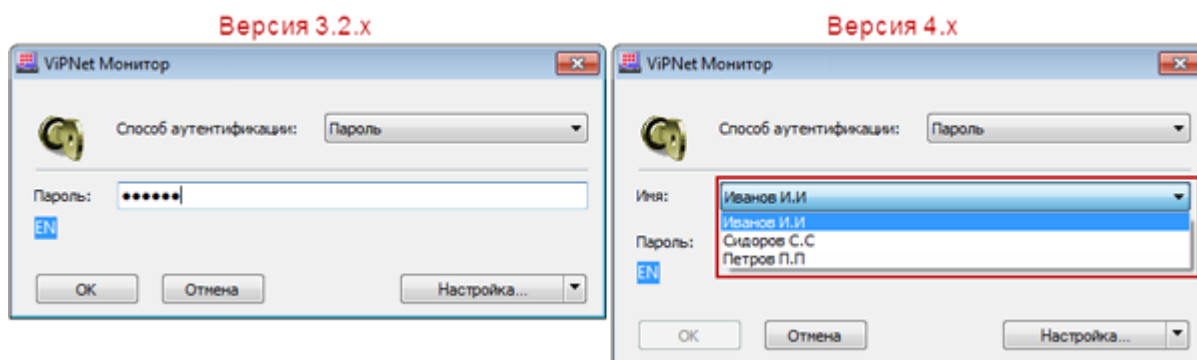


Рисунок 36: Аутентификация пользователя с помощью пароля

Режимы безопасности

В программах ViPNet Client и ViPNet Coordinator версии 3.2.x предусмотрено пять режимов безопасности (см. «[Режим безопасности ПО ViPNet](#)» на стр. 73), которые представляют собой наборы правил для обработки открытых IP-пакетов.

В версии 4.x режимы безопасности не используются. Для настройки необходимого уровня безопасности нужно создать соответствующие фильтры или назначить сетевому узлу определенные полномочия (см. «[Полномочия пользователя](#)» на стр. 73). Примеры настройки приведены в таблице ниже.

Таблица 3. Соответствие режимов безопасности в версии 3.2.x полномочиям и фильтрам в версии 4.x

Режим безопасности	Описание
1 Блокировать IP-пакеты всех соединений	В разделе Локальные фильтры открытой сети создайте блокирующий фильтр для всех IP-адресов
2 Блокировать все соединения кроме разрешенных	Уровень полномочий 0 — для клиента Уровень полномочий 0, 1, 2, 3 — для координатора Используются предустановленные фильтры
3 Пропускать все исходящие соединения кроме запрещенных	Уровень полномочий 1, 2, 3 — для клиента Используются предустановленные фильтры
4 Пропускать все соединения	В разделе Локальные фильтры открытой сети (на координаторе) или Фильтры открытой сети (на клиенте) создайте разрешающий фильтр для всех IP-адресов
5 Пропускать IP-пакеты без обработки	Команда Отключить защиту (меню Файл > Конфигурации)

Ограниченный интерфейс пользователя

При работе от имени администратора сетевого узла в программах ViPNet Client и ViPNet Coordinator версий 3.2.x и 4.x есть возможность ограничить интерфейс пользователя, тем самым запрещая пользователю создавать, изменять или удалять сетевые фильтры. В результате при работе от имени пользователя в главном окне программы отображается только список узлов сети ViPNet, с которыми установлена связь.

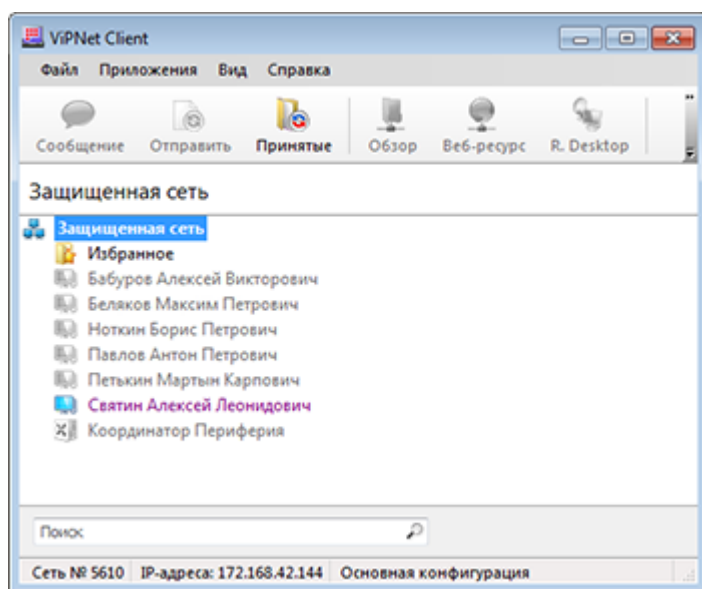


Рисунок 37: Главное окно программы в режиме ограниченного интерфейса в версии 4.x

В режиме ограниченного интерфейса пользователю также недоступна возможность настройки программы и параметров безопасности.

В версии 4.x возможность ограничивать интерфейс пользователя приравнена к назначению уровня полномочий 3. Таким образом, если пользователю сетевого узла назначен уровень полномочий 3, то флажок ограничения интерфейса пользователя в разделе **Администратор** станет недоступным.



Примечание. В сетях ViPNet VPN на клиентских узлах по умолчанию ограничен интерфейс программы ViPNet Client. Настройки программы можно выполнить только в режиме администратора сетевого узла.

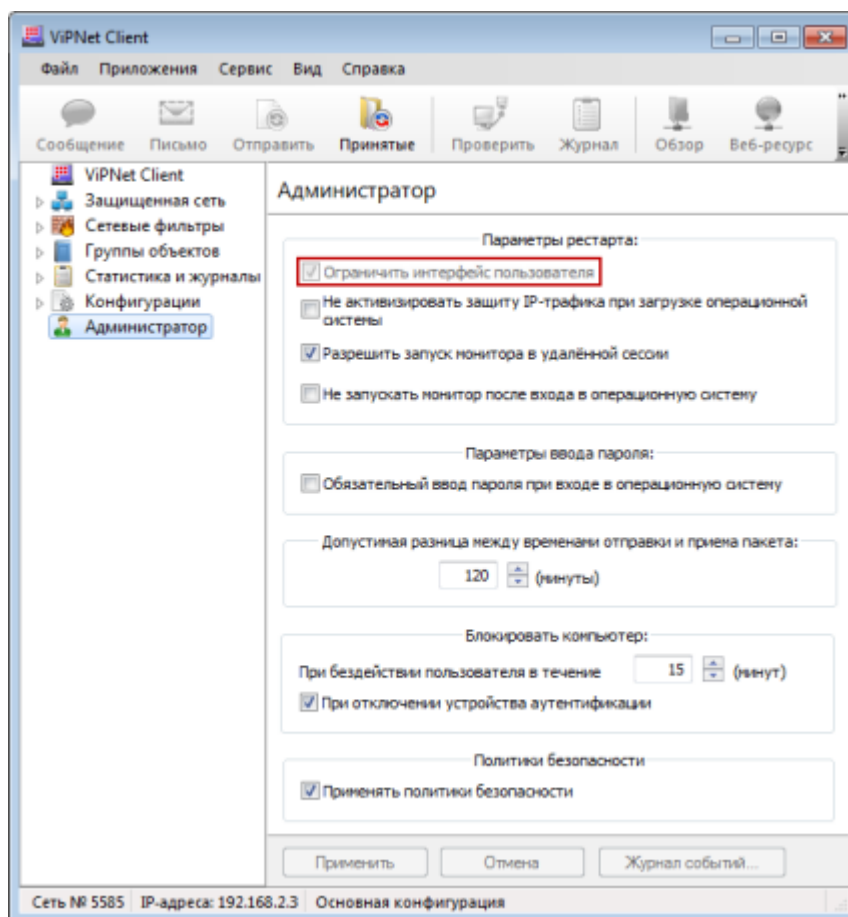


Рисунок 38: Ограничение интерфейса пользователя и уровень специальных полномочий 3

Смена конфигураций программы по расписанию

В программе ViPNet Монитор версии 4.x реализована возможность автоматической смены конфигураций. Если вы работаете с несколькими конфигурациями программы, каждую из которых нужно устанавливать в определенное время, вы можете настроить расписание смены этих конфигураций. Настройка расписания, а также оповещения о смене конфигурации выполняется в разделе **Конфигурации**.

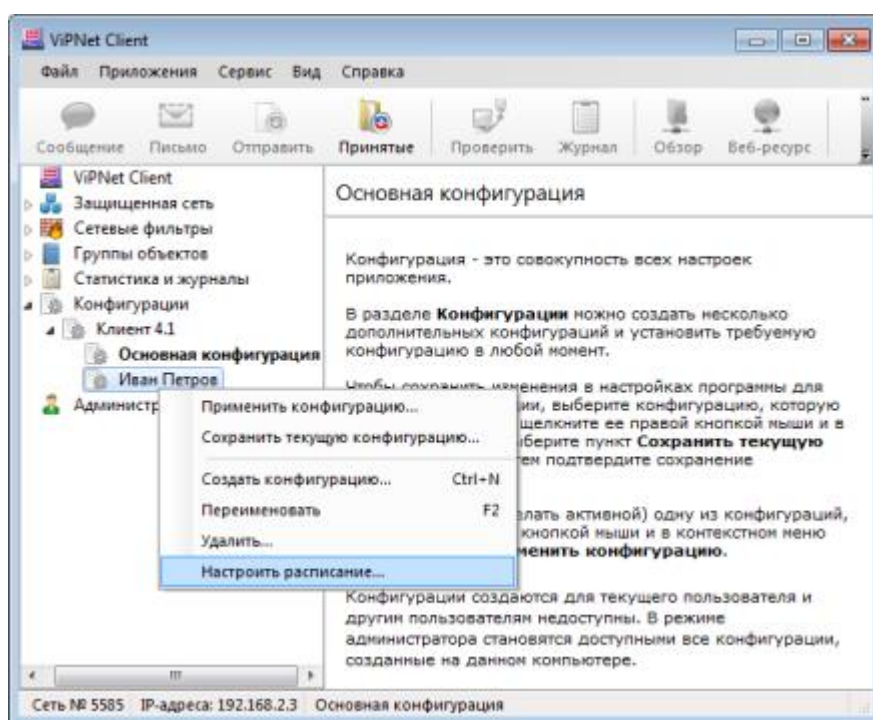


Рисунок 39: Создание расписания смены конфигураций



5

Прочие доработки

Добавление туннелируемых узлов	56
Определение и проверка IP-адресов	57
Журнал IP-пакетов	58
Интеграция с программой SafeDisk-V	60
Передача конвертов MFTR через почтовые серверы	61
Изменения в мастере обновления сертификата	62
Изменения в программе ViPNet Деловая почта	64
Обмен защищенными сообщениями	66
Изменения в интерфейсе	68
Изменения в терминологии	71

Добавление туннелируемых узлов

В программе ViPNet Монитор 3.2.x для задания IP-адресов туннелируемых узлов в соответствующем разделе нужно нажать кнопку **IP-адреса** и добавить адреса. В версии 4.x IP-адреса туннелируемых узлов можно добавлять в окне настройки туннелирующего координатора в разделе **Туннелирование**. В этом разделе также отображается разрешенное количество одновременно туннелируемых узлов.

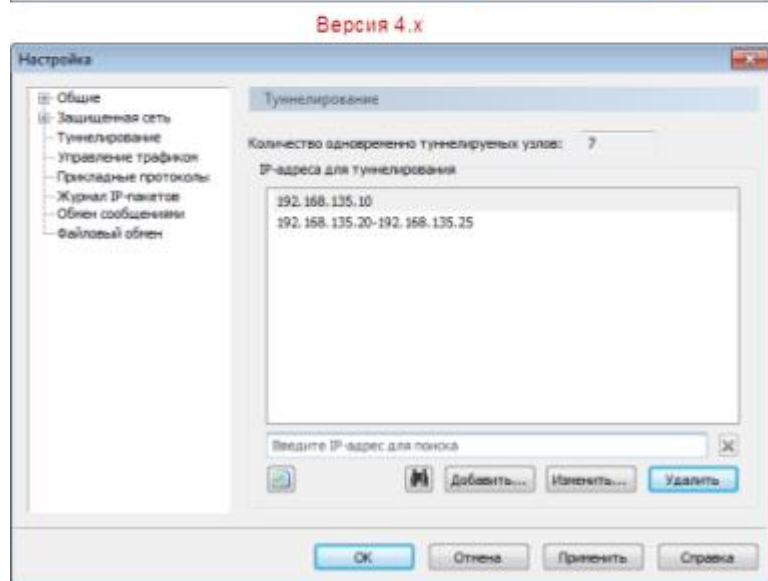
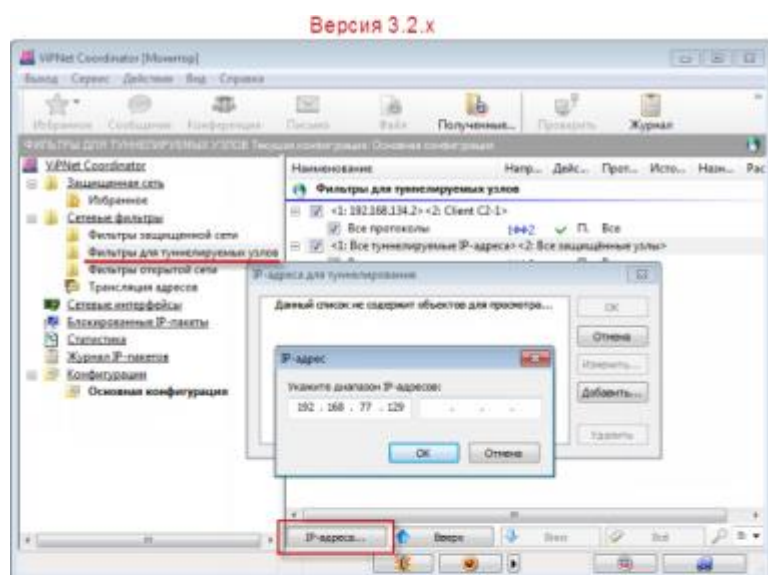




Рисунок 40: Задание адресов туннелируемых узлов

Определение и проверка IP-адресов

В версии 4.x при добавлении IP-адресов вы можете определить IP-адрес сетевого узла по имени компьютера, нажав кнопку .

При добавлении IP-адреса в версии 3.2.x выполняется проверка на пересечение всех IP-адресов из списка с адресами, заданными для других узлов сети ViPNet. Данная проверка позволяет исключить возможность задания одинаковых IP-адресов. В результате проверки пользователь получает сообщения обо всех конфликтах IP-адресов, обнаруженных в сети ViPNet.

При добавлении IP-адреса в версии 4.x выполняется проверка только этого адреса на пересечение с IP-адресами, уже заданными в списке, и IP-адресами других сетевых узлов. Если обнаружен конфликт, то пользователь получает сообщение, касающееся только добавляемого IP-адреса. При необходимости вы можете выполнить проверку всех IP-адресов в версии 4.x вручную, нажав кнопку .

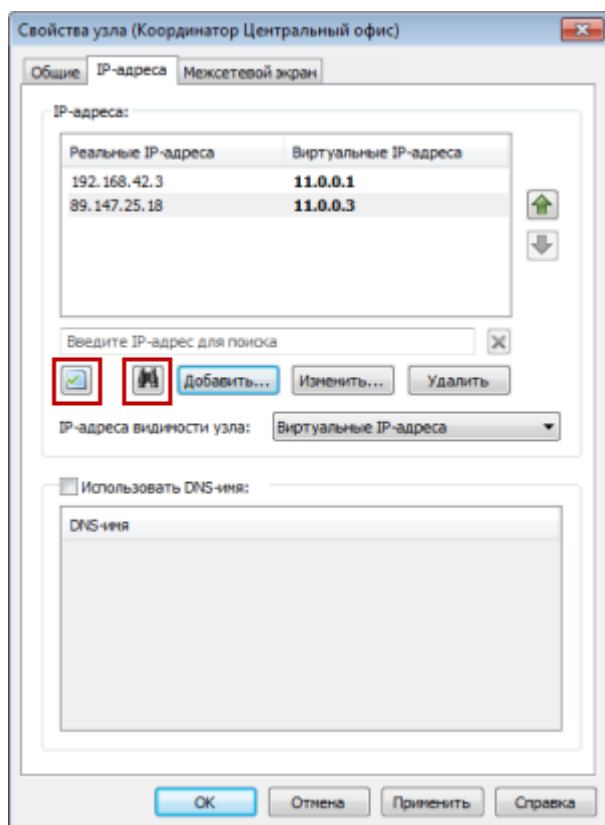


Рисунок 41: Добавление и проверка IP-адресов в версии 4.x

Журнал IP-пакетов

В программе ViPNet Монитор версии 3.2.x журнал заблокированных IP-пакетов вынесен в отдельный раздел, где на основе параметров заблокированных пакетов можно создавать разрешающие правила фильтрации. При этом в журнале IP-пакетов возможности создавать правила нет.

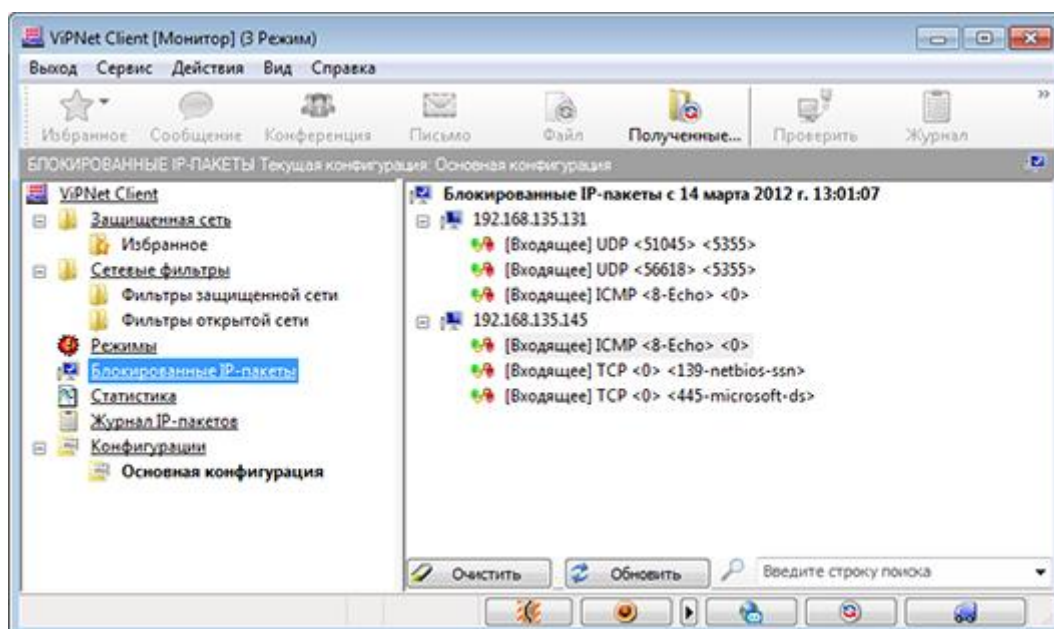


Рисунок 42: Список заблокированных IP-пакетов

В программе ViPNet Монитор версии 4.x реализована возможность создавать в журнале IP-пакетов как разрешающие, так и блокирующие фильтры. В связи с этим нет необходимости выносить заблокированные IP-пакеты в отдельный раздел, и все действия над IP-пакетами выполняются в разделе **Журнал IP-пакетов**.

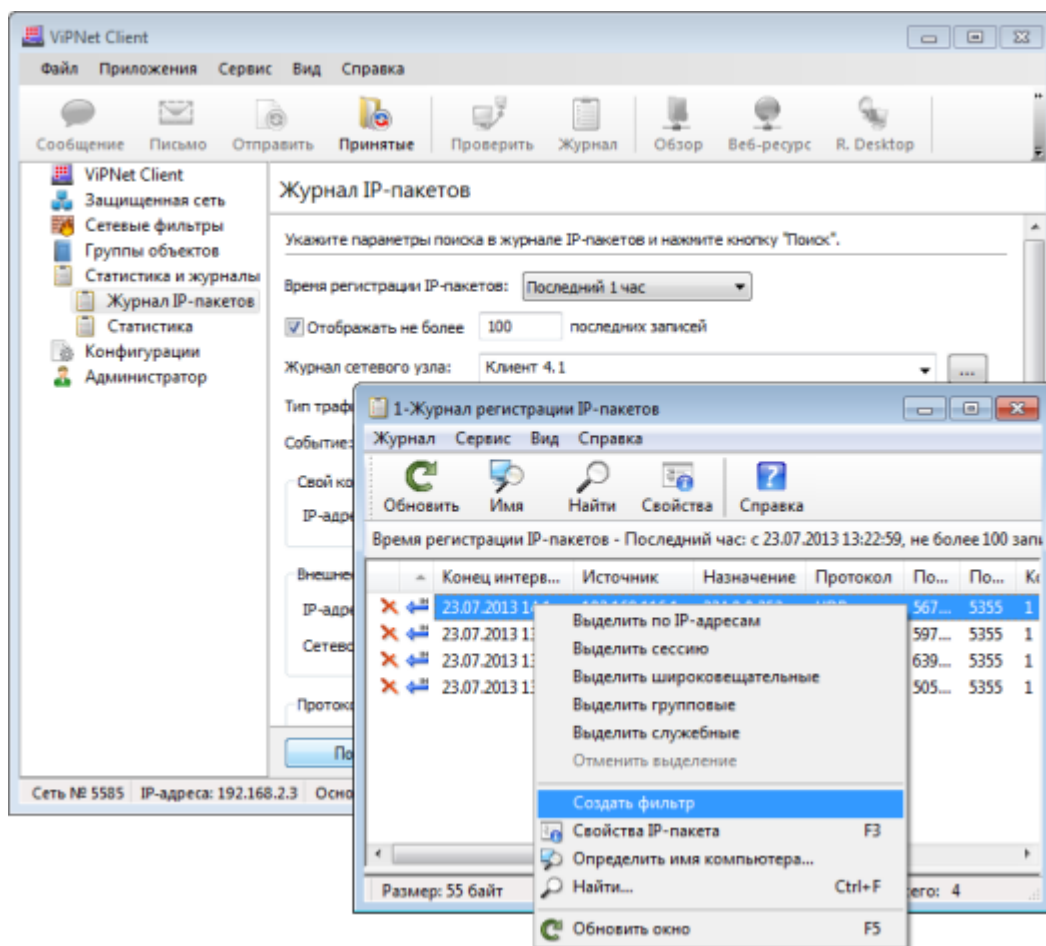


Рисунок 43: Работа с журналом IP-пакетов в версии 4.x

Интеграция с программой SafeDisk-V

В программе ViPNet Монитор версии 3.2.x обеспечена поддержка совместной работы с программой ViPNet SafeDisk-V 4.1. Теперь обеспечена интеграция программ ViPNet Coordinator и ViPNet Client версии 4.x с программой ViPNet SafeDisk-V версии 4.2.

Принцип взаимодействия новых версий программ ViPNet SafeDisk-V и ViPNet Монитор изменился. Программу ViPNet SafeDisk-V теперь можно использовать только при включенной защите IP-трафика. При запуске ViPNet SafeDisk-V программа ViPNet Coordinator Монитор или ViPNet Client Монитор перезапускается, и большинство настроек становятся недоступными для редактирования, в том числе в целях безопасности невозможно сменить пользователя, отключить защиту IP-трафика или выйти из программы ViPNet Монитор.

Вместо защищенных и незащищенных конфигураций программы ViPNet Монитор теперь автоматически создаются дополнительные сетевые фильтры, которые запрещают открытые соединения. Параметры защиты трафика задаются в специальном окне, которое открывается при запуске ViPNet SafeDisk-V.

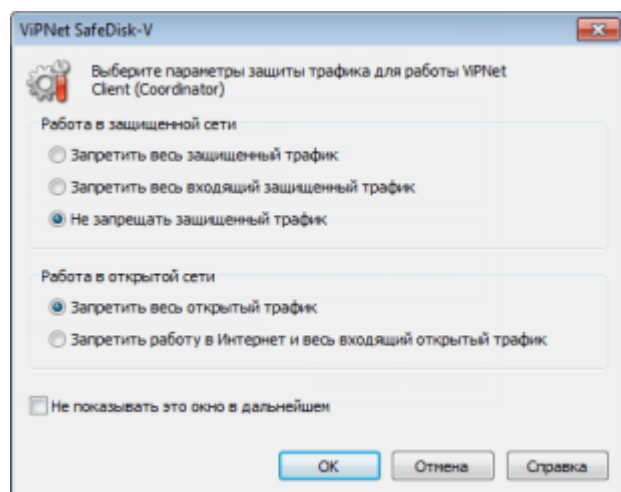


Рисунок 44: Параметры защиты трафика при работе с программой ViPNet SafeDisk-V

Передача конвертов MFTP через почтовые серверы

В ViPNet Монитор версии 4.x при передаче конвертов по каналу SMTP/POP3 появилась возможность разбивать конверты на фрагменты. Эта возможность позволит вам отправлять большие конверты, даже если на почтовом сервере существует ограничение на размер передаваемых конвертов.

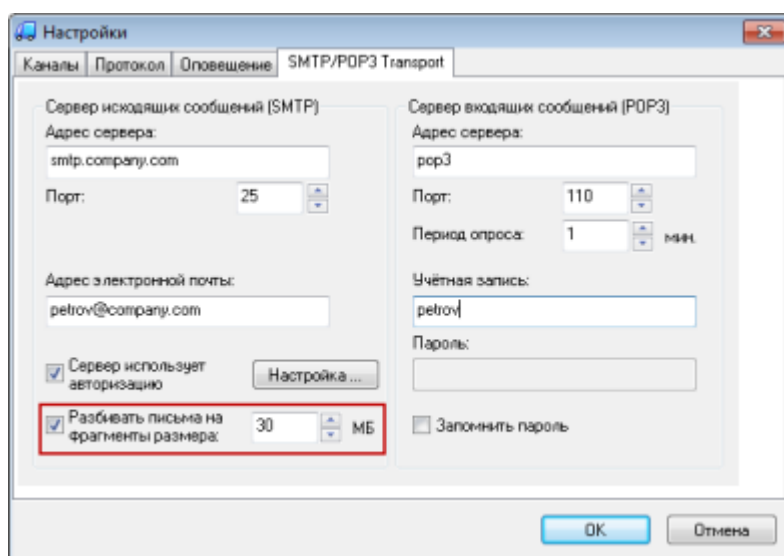


Рисунок 45: Настройка фрагментации конвертов

Изменения в мастере обновления сертификата

В предыдущих версиях программы была возможность передачи запроса на обновление сертификата в программу ViPNet Удостоверяющий и ключевой центр (УКЦ) как с помощью транспортного модуля MFTR, так и отдельно в виде файла с расширением *.sok.

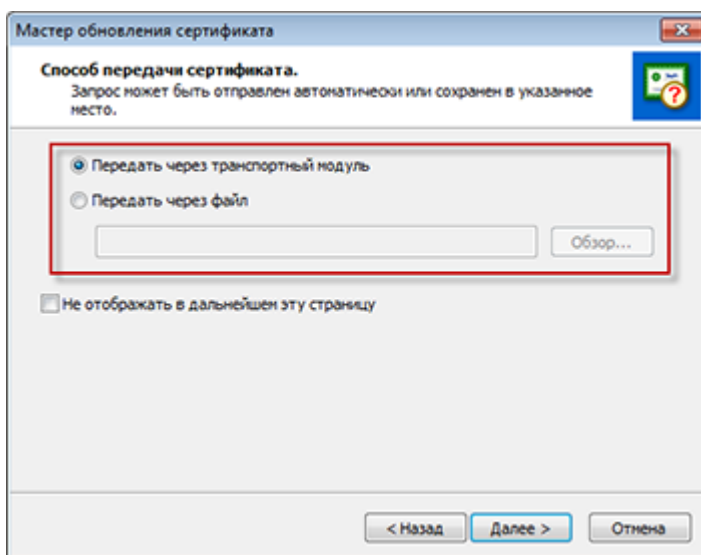


Рисунок 46: Выбор способа передачи запроса на обновление сертификата

В связи с тем, что в УКЦ версии 4.x обработка файлов с расширением *.sok, полученных напрямую от пользователя, невозможна, способ передачи запроса через файл стал не востребовавшимся. В связи с этим в мастере обновления сертификата была убрана настройка способа передачи запроса. Теперь созданные запросы на обновление сертификатов могут быть переданы в УКЦ только через транспортный модуль ViPNet MFTR.

Кроме этого, в мастере была исключена возможность выбора режима ожидания сертификата из УКЦ в реальном времени и параметра ввода сертификата в действие сразу после получения — на последней странице мастера убраны флажки **Ожидать ответа на запрос** и **Ввести изданный сертификат в действие**.

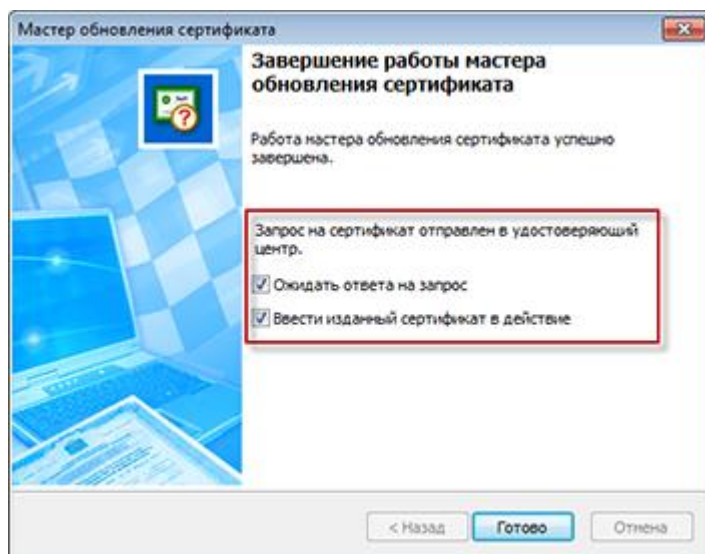


Рисунок 47: Возможность выбора режима ожидания ответа на запрос и ввода сертификата в действие

Использование указанных настроек в некоторых случаях приводило к сбою процесса ввода в действие полученного из УКЦ сертификата (как правило, если контейнер с закрытым ключом, в который должен быть помещен сертификат, размещался на внешнем устройстве). В результате сбоя процесс ввода в действие сертификата не мог быть завершен.

Теперь возможность сбоя при вводе в действие полученного сертификата исключена. Сертификат автоматически вводится в действие при получении, если в окне настроек параметров безопасности на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по инициативе пользователя**. Однако в случае размещения контейнера с закрытым ключом на устройстве для автоматического ввода в действие сертификата необходимо не только наличие указанного флажка, но и сохраненного ПИН-кода для устройства. В противном случае ввод сертификата в действие должен производиться пользователем вручную.

Изменения в программе ViPNet Деловая почта

В программе ViPNet Деловая почта версии 4.x реализованы следующие изменения:

- использование встроенной базы данных SQLite (см. [«Встроенная база данных SQLite»](#) на стр. 64);
- хранение вложений в базе данных (см. [«Хранение вложений в базе данных и архивация»](#) на стр. 64);
- графическое представление статуса сообщения (см. [«Просмотр статуса сообщения»](#) на стр. 65).

В интерфейсе программы ViPNet Деловая почта также используются новые значки.

Встроенная база данных SQLite

В программе ViPNet Деловая почта версии 4.x используется встроенная база данных SQLite. Конвертация данных в новый формат осуществляется автоматически при первом после обновления запуске программы ViPNet Деловая почта. Использование базы данных SQLite позволяет снять ограничение на количество писем в архиве (в версии 3.2.9 в архиве можно хранить не более 120000 писем), а также обеспечивает возможность одновременной обработки входящих и исходящих писем при автопроцессинге.

Хранение вложений в базе данных и архивация

В более ранних версиях программы ViPNet Деловая почта письма хранятся отдельно от вложений. В этом случае при архивации создается архив, содержащий в себе файл с базой данных писем и набор папок, в которых размещены отдельные файлы вложений. В версии 4.x реализована дополнительная возможность переноса вложений в базу данных для размещения в архиве вместе с письмами. В этом случае архив представляет собой один файл. Размещение архива писем и вложений в одном файле позволяет упростить копирование или перенос архива на внешний носитель, например, с целью резервирования.

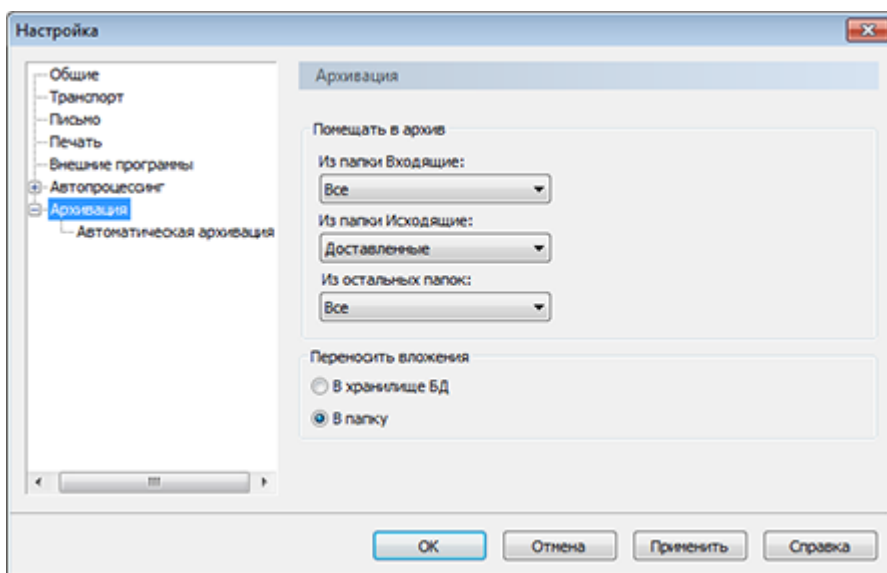


Рисунок 48: Настройка архивации писем и вложений

Просмотр статуса сообщения

В программе ViPNet Деловая почта версии 4.x вы можете выбрать наиболее удобный для вас способ просмотра атрибутов сообщения, а именно, в буквенном представлении в колонке **Атрибуты** (данная возможность была доступна и в более ранних версиях программы) и в графическом в новой колонке **Статус**.

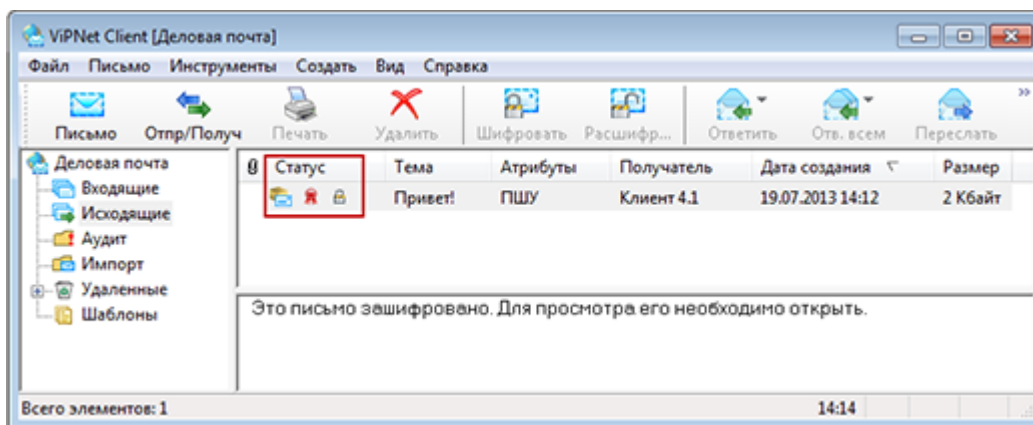




Рисунок 49: Новая колонка для отображения статуса письма

Обмен защищенными сообщениями

В версии 3.2.x при закрытии программы обмена защищенными сообщениями закрываются все сеансы с возможностью сохранения каждого из сеансов в отдельном текстовом файле. В версии 4.x вы можете закрыть программу обмена защищенными сообщениями, не завершая при этом все сеансы обмена. Когда вы в следующий раз запустите программу, будут открыты все начатые ранее сеансы обмена сообщениями. При желании, так же как и в предыдущих версиях программы, вы можете закрыть отдельные сеансы обмена сообщениями и сохранить их в текстовых файлах.

Кроме этого, в программе обмена защищенными сообщениями версии 4.x появились дополнительные возможности:

- Отправка письма или файла во время сеанса обмена сообщениями. Отправка писем возможна, только если вашему узлу назначена роль «Деловая почта» и на нем установлена программа ViPNet Деловая почта.
- Поиск слов в сообщениях открытых сеансов на панели **Протокол сеанса** с помощью строки поиска. В версии 3.x строка поиска предназначалась только для фильтрации списка получателей на панели **Сеансы**.
- Переход к предыдущему или к следующему просмотренному сеансу с помощью кнопок  и  на панели **Сеансы**. В истории переходов между сеансами запоминается 10 последних сеансов, просмотр которых продолжался более 5 секунд.
- Просмотр даты и времени последнего обмена сообщениями с участником сеанса.

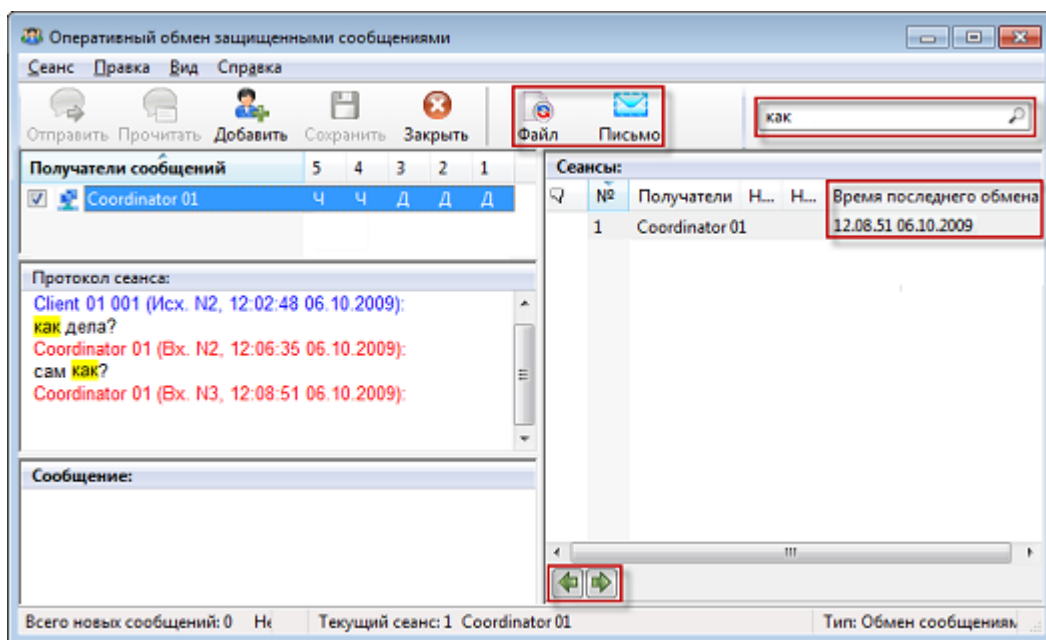


Рисунок 50: Новые возможности при обмене защищенными сообщениями

Изменения в интерфейсе

В связи с изменениями в работе с некоторыми функциями программы ViPNet Монитор был переработан интерфейс. Все доработки направлены на упрощение работы с программой, а также удобство работы с сетевыми фильтрами и правилами трансляции IP-адресов, полученными от программы ViPNet Policy Manager. Основные изменения в интерфейсе программы ViPNet Монитор описаны ниже.

Кнопки вызова программных компонентов «Деловая почта», «Контроль приложений», «Файловый обмен» и транспортный модуль MFTR удалены из строки состояния главного окна программы ViPNet Монитор. Переход к любому из этих компонентов, а также к программе обмена защищенными сообщениями теперь можно осуществить с помощью меню **Приложения**. В строке состояния теперь отображается номер сети ViPNet, IP-адрес сетевого узла, на котором запущена программа ViPNet Монитор и текущая конфигурация программы.

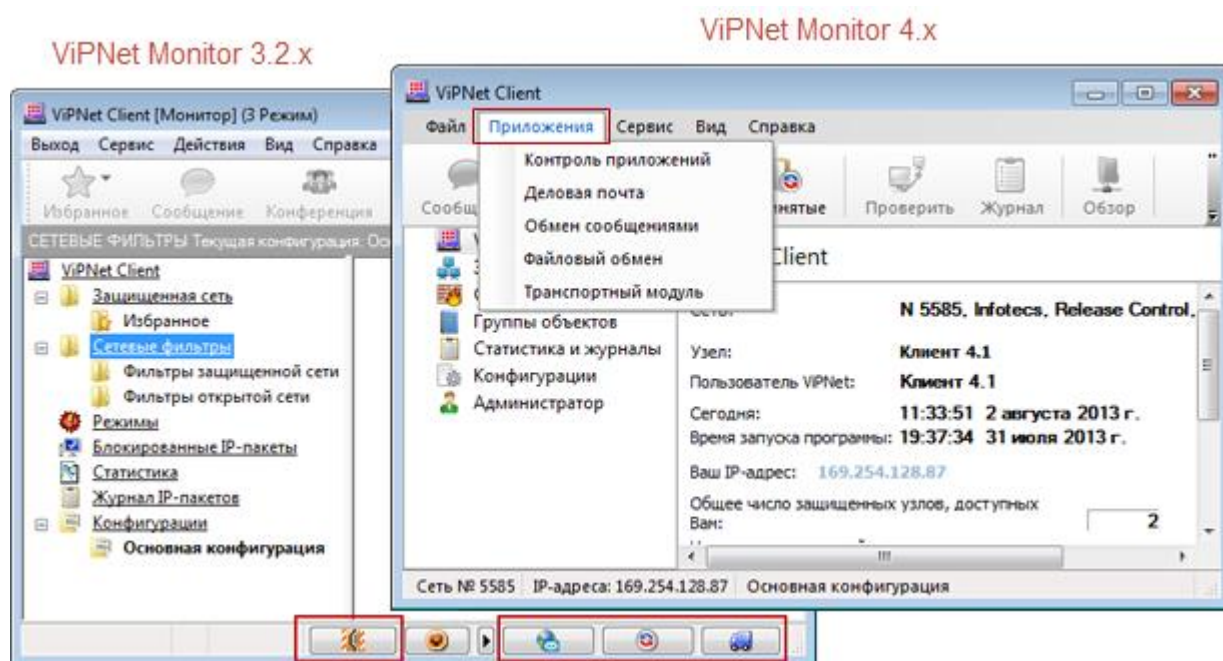


Рисунок 51: Переход к компонентам ПО ViPNet

В версии 4.x все действия над сетевыми узлами, с которыми есть связь, ранее доступные из меню **Действия**, теперь доступны только из контекстного меню. Пункт **Действия** удален из главного меню.

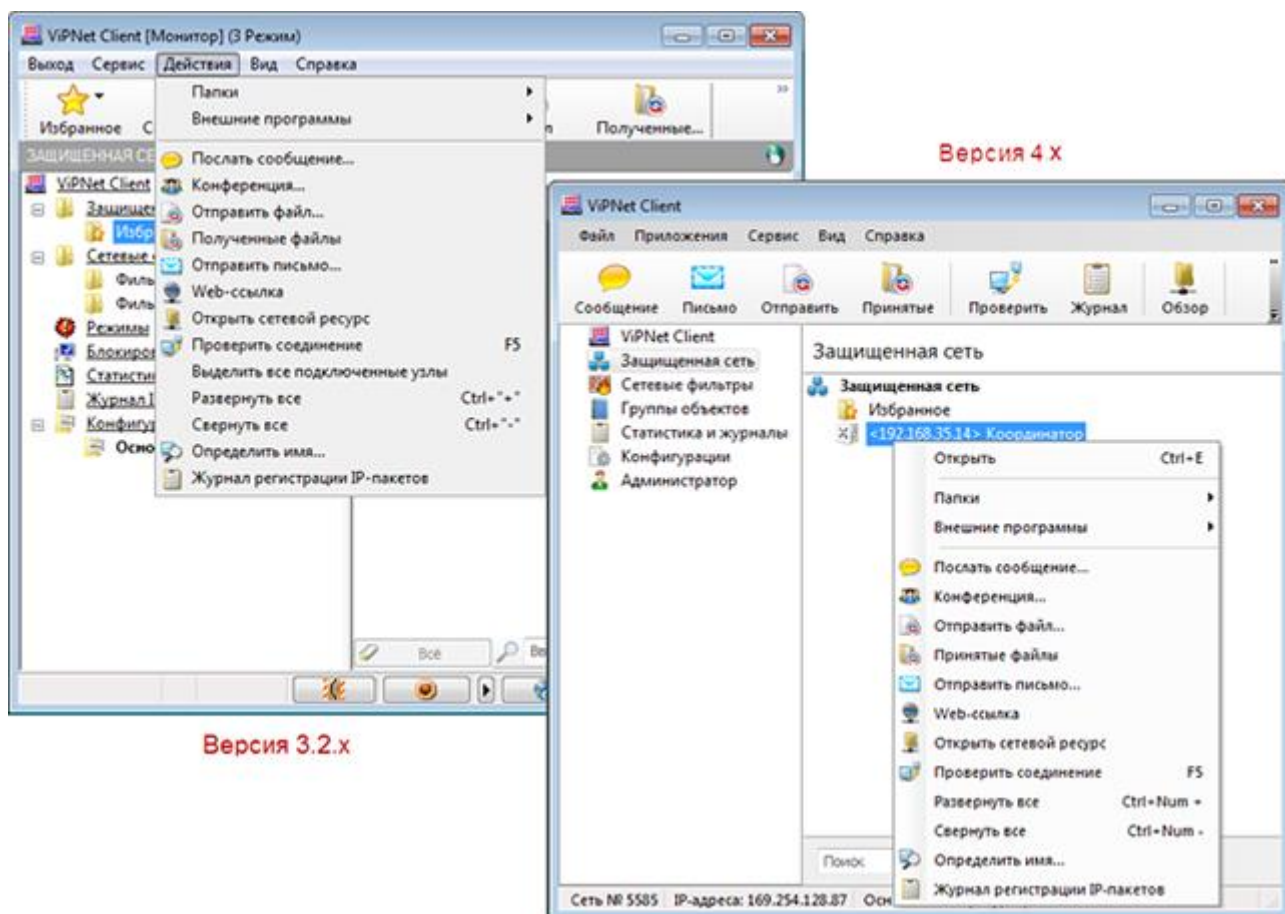


Рисунок 52: Возможные действия

В разделе **Защищенная сеть** главного окна программы теперь не отображается свой узел ViPNet.

Удалена кнопка блокировки компьютера (см. «[Блокировка компьютера и IP-трафика](#)» на стр. 37). В версии 4.x блокировка компьютера осуществляется только стандартными средствами операционной системы.

Изменилось представление сетевых фильтров. Чтобы обеспечить удобство просмотра и работы с фильтрами и правилами трансляции, представление фильтров в программах ViPNet Монитор и ViPNet Policy Manager приведено к единому виду (см. «[Фильтрация трафика](#)» на стр. 18).

В версии 4.x включение антиспуфинга (см. «[Антиспуфинг](#)» на стр. 34) и блокировка протоколов, кроме IP и ARP, выполняются в окне **Настройка** в разделе **Управление трафиком**.

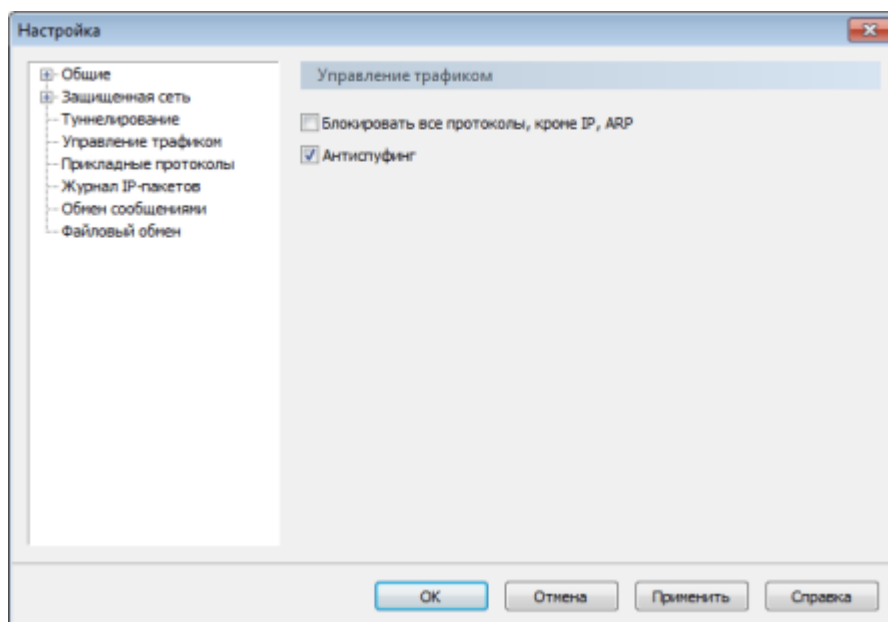



Рисунок 53: Включение функции антиспуфинга в версии 4.x

В версии 4.x во время загрузки Windows для аутентификации в программе ViPNet Монитор вы можете использовать экранную клавиатуру. Для этого нажмите кнопку  и в меню выберите пункт **Экранная клавиатура**.

Изменения в терминологии

Изменения в терминологии, произошедшие в программах ViPNet Client Монитор и ViPNet Coordinator Монитор версии 4.x, перечислены в таблице ниже.

Таблица 4. Изменения в терминологии и интерфейсе

Термин в версии 3.2.x	Термин в версии 4.x
Абонентский пункт	Клиент
Прикладная задача	Роль
Правила фильтрации трафика	Сетевые фильтры
Экспорт настроек	Сохранение настроек
Импорт настроек	Восстановление настроек
Политика безопасности (в программе ViPNet Контроль приложений)	Правила контроля приложений



Глоссарий

Д

DMZ (демилитаризованная зона)

Физическая или логическая подсеть, предоставляющая доступ к внешним корпоративным службам из большей сети, с которой нет отношений доверия, как правило, из Интернета. При этом серверы, отвечающие на запросы из внешней сети или направляющие туда запросы, находятся в этой подсети и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана. Прямых соединений между внутренней сетью и внешней нет: любые соединения возможны только с серверами в DMZ, которые обрабатывают запросы и формируют свои, возвращая ответ получателю уже от своего имени.

А

Антиспуфинг

Защита от спуфинг-атак, при которых злоумышленник подделывает адрес источника для обхода межсетевых экранов и организации DoS-атак (от англ. Denial of Service, отказ в обслуживании).

Д

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager 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.

П

Политика безопасности

Набор параметров, регулирующих безопасность сетевого узла. В технологии ViPNet безопасность сетевых узлов обеспечивается с помощью сетевых фильтров и правил трансляции IP-адресов.

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

Р

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.

С

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

Справочники и ключи

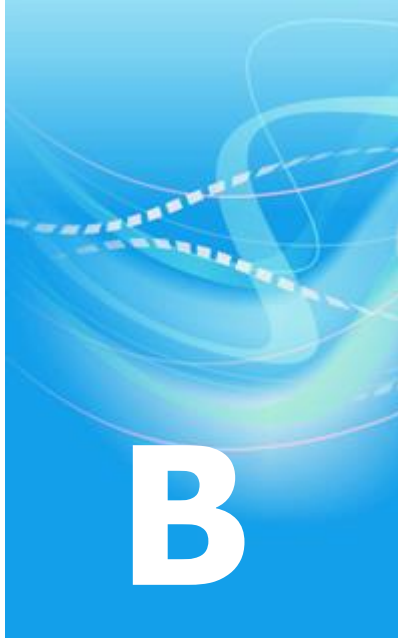
Справочники, ключи узла и ключи пользователя.

У

Удостоверяющий центр

В широком смысле, удостоверяющий центр — организация, осуществляющая выпуск сертификатов открытых ключей подписи пользователя, а также сертификатов другого назначения. В сетях ViPNet сертификаты выпускаются в программе ViPNet Удостоверяющий и ключевой центр (УКЦ).

В контексте сети ViPNet, термином «Удостоверяющий центр» также обозначается сетевой узел с установленной программой ViPNet Удостоверяющий и ключевой центр.



Указатель

Д

DMZ (демилитаризованная зона) - 28

А

Антиспуфинг - 34, 69

Б

Блокировка компьютера и IP-трафика - 69

В

Встроенная база данных SQLite - 64

Г

Группы объектов - 22

Д

Дистрибутив ключей - 14

Н

Неинтерактивный режим установки - 9

О

Особенности формата фильтров в версии 4.x по сравнению с версией 3.2.x - 21

П

Политика безопасности - 18

Полномочия пользователя - 51

Правила трансляции IP-адресов - 24

Приоритет сетевых фильтров - 22

Просмотр статуса сообщения - 64

Р

Режим безопасности ПО ViPNet - 51

Режимы безопасности - 36

С

Сетевой фильтр - 18

Справочники и ключи - 13

У

Удостоверяющий центр - 49

Установка ПО с использованием Microsoft System Center - 9

Установка ПО с использованием сценария входа в систему - 9

Ф

Фильтрация трафика - 69

Х

Хранение вложений в базе данных и архивация - 64