ViPNet xFirewall

Настройка с помощью веб-интерфейса

infotecs

ФРКЕ.00217-01 90 16

Версия продукта 4.1.0

ОАО «ИнфоТеКС»

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

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

Веб-сайт: https://infotecs.ru/

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение ... **7**

О документе ... 8

Соглашения документа ... 9

Связанные документы ... 10

О программно-аппаратном комплексе ViPNet xFirewall ... 11

Обратная связь ... 12

Глава 1. Начало работы с веб-интерфейсом ViPNet xFirewall ... **13**

Назначение веб-интерфейса ... 14

Режимы пользователя и администратора ... 15

Режим ограниченной функциональности ... 17

Подключение к веб-интерфейсу ... 19

Настройка даты и времени ... 22

Перезагрузка ViPNet xFirewall ... 24

Глава 2. Настройка подключения к сети ... **25**

Настройка сетевых интерфейсов Ethernet ... 26

Назначение дополнительных IP-адресов ... 29

Организация обработки трафика из нескольких VLAN ... 30

Настройка интерфейсов для обработки трафика из нескольких VLAN ... 30

Пример организации обработки трафика из нескольких VLAN ... 33

Использование агрегированных сетевых интерфейсов ... 36

Создание агрегированного интерфейса ... 36

Режимы работы агрегированного интерфейса ... 39

Пример создания агрегированного канала между ViPNet xFirewall и коммутатором ... 42

Глава 3. Управляющие соединения ViPNet xFirewall ... **47**

Просмотр сведений о сетевых узлах ViPNet ... 48

Управление сертификатами ... 52

Настройка сертификатов ... 52

Настройка списков CRL ... 55

Глава 4. Настройка межсетевого экрана ... **57**

Настройка сетевых фильтров ... 58

Основные принципы фильтрации трафика ... 58

Общие сведения о сетевых фильтрах 60
Группы объектов 62
Системные группы объектов 63
Пользовательские группы объектов по умолчанию 64
Просмотр групп объектов 64
Создание и изменение группы объектов 65
Группа сетевых узлов ViPNet 66
Группа IP-адресов 68
Группа сетевых интерфейсов 69
Группа протоколов 71
Группа расписаний 72
Создание и изменение сетевого фильтра 74
Создание транзитных фильтров открытой сети 76
Примеры использования транзитных фильтров открытой сети 79
Создание локальных фильтров открытой сети 83
Создание фильтров защиты канала управления 84
Просмотр сетевых фильтров 85
Настройка правил трансляции адресов 87
Трансляция сетевых адресов 87
Трансляция адреса назначения 88
Трансляция адреса источника 89
Просмотр правил трансляции адресов 90
Создание и изменение правила трансляции адресов 90
Примеры использования правил трансляции адресов 92
Организация доступа пользователей к Интернету 92
Размещение общедоступного сервера в демилитаризованной зоне 97
Настройка параметров прокси-сервера 101
Настройка основных параметров прокси-сервера 102
Настройка правил фильтрации трафика 104
Пример настройки фильтрации трафика 106
Настройка антивирусной проверки 107
Настройка встроенного антивируса KAV4Proxy 107
Настройка внешнего антивируса 109
Настройка взаимодействия с Active Directory 111
Настройка учетной записи технологического пользователя на контроллере домена 111
Настройка взаимодействия с контроллером домена 112
Настройка взаимодействия с LDAP-сервером 114
Пример настройки взаимодействия с LDAP-сервером 115

Получение и импорт сертификатов ... 116
Настройка параметров Captive portal ... 119
Просмотр списка пользователей ... 121

Глава 5. Настройка сетевых служб ... 123
Настройка параметров DHCP-сервера ... 124
Настройка DHCP-relay ... 127
Настройка параметров DNS-сервера ... 128
Настройка параметров NTP-сервера ... 130
Пример настройки доступа к корпоративным DNS- и NTP-серверам ... 133

Глава 6. Настройка маршрутизации ... 135
Общие сведения о маршрутизации ... 136
Принципы формирования таблиц маршрутизации в ViPNet xFirewall ... 137
Просмотр общей таблицы маршрутизации ... 139
Общие сведения о протоколе OSPF ... 141
Настройка статической маршрутизации ... 143
Добавление статических маршрутов ... 143
Настройка балансировки IP-трафика ... 144
Настройка динамической маршрутизации ... 146
Настройка параметров динамических маршрутов от DHCP-протокола ... 146
Настройка административной дистанции для маршрутов DHCP-сервера ... 146
Настройка метрики для маршрутов DHCP-сервера ... 147
Изменение метрики по умолчанию для маршрутов от DHCP-протокола ... 149
Настройка параметров динамической маршрутизации по протоколу OSPF ... 150
Настройка протокола OSPF ... 151
Настройка перераспределения маршрутов ... 153

Глава 7. Мониторинг состояния ViPNet xFirewall и просмотр журнала IP-пакетов ... 156
Мониторинг состояния ViPNet xFirewall ... 157
Мониторинг по протоколу SNMP ... 159
Просмотр журнала регистрации IP-пакетов ... 161
Просмотр статистической информации об IP-пакетах ... 164
Просмотр журнала событий ... 165
Просмотр журнала транспортных конвертов (MFTP) ... 166

Приложение A. Сетевые фильтры по умолчанию ... 169

Приложение B. Пользовательские группы протоколов по умолчанию ... 173

Приложение C. Типы событий в журнале регистрации IP-пакетов..... 176

Приложение D. Записи в журнале событий, связанные с аутентификацией и настройкой оборудования.....181

Приложение E. Поддерживаемые приложения..... 187

Приложение F. Поддерживаемые прикладные протоколы..... 189

Приложение G. Поддерживаемые группы приложений..... 190

Приложение H. Известные ограничения фильтрации по приложениям и прикладным протоколам..... 196

Приложение I. Глоссарий.....200

Введение

О документе 8

Соглашения документа 9

Связанные документы 10

О программно-аппаратном комплексе ViPNet xFirewall 11

Обратная связь 12

О документе

В документе описана настройка ViPNet xFirewall с помощью веб-интерфейса. Документ предназначен для администраторов и пользователей, которые планируют работать с ViPNet xFirewall, используя веб-интерфейс.

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.

Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ViPNet xFirewall помимо данного документа.

Таблица 3. Связанные документы

Документ	Содержание
«ViPNet xFirewall. Общее описание»	Общая информации по ViPNet xFirewall, способы настройки и управления, описание существующих исполнений и характеристики аппаратных платформ
«ViPNet xFirewall. Подготовка к работе»	Описание подготовки ViPNet xFirewall к использованию, развертывание виртуального образа ViPNet xFirewall, работа со справочниками и ключами узла, обновление ПО, резервное копирование и восстановление настроек
«ViPNet xFirewall. Настройка с помощью командного интерпретатора»	Описание основных сценариев настройки ViPNet xFirewall с помощью командного интерпретатора, работы с журналами и мониторинга ViPNet xFirewall
«ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам»	Описание команд ViPNet xFirewall Описание конфигурационных файлов управляющего демона и системы защиты от сбоев
«ViPNet xFirewall. Лицензионные соглашения на компоненты сторонних производителей»	Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet xFirewall

О программно-аппаратном комплексе ViPNet xFirewall

ViPNet xFirewall представляет собой программно-аппаратный комплекс, который выступает в роли межсетевого экрана и предназначен для фильтрации трафика между внешней сетью и узлами локальной сети. ViPNet xFirewall выполняет фильтрацию трафика на сетевом и транспортном уровнях модели OSI (с контролем состояния сессий), а также реализует механизм расширенной инспекции IP-пакетов DPI (см. глоссарий, стр. 201) на уровнях 2 — 7 модели OSI и накопления статистики. Благодаря этому ViPNet xFirewall обеспечивает защиту локальной сети и контролирует работу пользователей с сетевыми приложениями.

ViPNet xFirewall производится в нескольких исполнениях, в том числе для развертывания на платформах виртуализации.

Обратная связь

Дополнительная информация

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

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

Контактная информация

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

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

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

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

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

1

Начало работы с веб-интерфейсом ViPNet xFirewall

Назначение веб-интерфейса 14

Режимы пользователя и администратора 15

Режим ограниченной функциональности 17

Подключение к веб-интерфейсу 19

Настройка даты и времени 22

Перезагрузка ViPNet xFirewall 24

Назначение веб-интерфейса

Веб-интерфейс является одним из способов администрирования ViPNet xFirewall. С другими способами настройки ViPNet xFirewall вы можете ознакомиться в документе «ViPNet xFirewall. Общее описание», глава «Возможности управления ViPNet xFirewall»).

Подключение к ViPNet xFirewall через веб-интерфейс следует осуществлять только с других защищенных узлов ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 202)).

Внимание! Предоставлять удаленный доступ к ViPNet xFirewall с незащищенных узлов запрещено. С помощью фильтров защищенной сети следует ограничить соединения между ViPNet xFirewall и рабочими местами администраторов, разрешив только удаленное управление и передачу данных по служебным протоколам ViPNet.

С помощью веб-интерфейса ViPNet xFirewall вы можете выполнять следующие действия:

- Настройка подключения ViPNet xFirewall к сети (настройка сетевых интерфейсов).
- Управление межсетевым экраном:
  - настройка сетевых фильтров, в том числе для приложений, прикладных протоколов, групп приложений и пользователей, авторизованных в домене Active Directory или на LDAP-сервере;
  - настройка правил трансляции адресов;
  - настройка прокси-сервера, включая проверку трафика встроенным антивирусом KAV4Proxy или внешним антивирусом, расположенным на ICAP-сервере).
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP-серверов.
- Настройка статической и динамической маршрутизации.
- Мониторинг состояния ViPNet xFirewall и просмотр журнала IP-пакетов и системного журнала.
- Просмотр статистики и журнала конвертов MFTP.

Режимы пользователя и администратора

Вы можете работать с веб-интерфейсом ViPNet xFirewall в режиме пользователя или в режиме администратора. Действия, которые вы можете выполнять, в этих режимах см. в таблице ниже.

Таблица 4. Работа в веб-интерфейсе в режимах пользователя и администратора

Действие	Режим пользователя	Режим администратора
Настройка подключения к сети (на стр. 25): • настройка сетевых интерфейсов Ethernet; • назначение дополнительных IP-адресов; • организация обработки трафика из нескольких VLAN; • использование агрегированных сетевых интерфейсов.	–	+
Просмотр сетевых фильтров (на стр. 85)	+	+
Создание и изменение сетевого фильтра (на стр. 74)	–	+
Просмотр правил трансляции адресов (на стр. 90)	+	+
Создание и изменение правила трансляции адресов	–	+
Просмотр групп объектов (на стр. 64)	+	+
Создание и изменение группы объектов (на стр. 65)	–	+
Изменение настроек сетевых служб (DHCP, DNS, NTP и прокси-сервера) (см. Настройка сетевых служб на стр. 123)	–	+
Просмотр общей таблицы маршрутизации (на стр. 139)	+	+
Настройка маршрутизации (на стр. 135)	–	+
Просмотр информации о сетевых узлах ViPNet (см. Просмотр сведений о сетевых узлах ViPNet на стр. 48)	+	+
Проверка соединения с сетевым узлом ViPNet	+	+
Мониторинг состояния ViPNet xFirewall (на стр. 157):	+	+
• Просмотр системного журнала (см. Просмотр журнала событий на стр. 165)	–	+
• Просмотр журнала регистрации IP-пакетов (на стр. 161)	–	+

Действие	Режим пользователя	Режим администратора
• Просмотр статистической информации об IP-пакетах (на стр. 164)	+	+

Режим ограниченной функциональности

При выключении одного или нескольких демонов (основных процессов) ViPNet xFirewall (iplircfg, failoverd, mftpd , uc) веб-интерфейс автоматически переходит в режим ограниченной функциональности. При этом появляется соответствующее сообщение с предложением выйти из веб-интерфейса либо продолжить работу с ограничением некоторых функций.

Примечание. Работа демонов может быть завершена как автоматически (в случае неполадок или на время выполнения некоторых операций), так и вручную администратором ViPNet xFirewall с помощью соответствующих команд.

В режиме ограниченной функциональности в зависимости от выключенного процесса ViPNet xFirewall могут быть недоступны следующие разделы веб-интерфейса:

- В случае обновления справочников и лицензий, поступивших из программы ViPNet Центр управления сетью или завершения работы демона iplircfg блокируются:
  - раздел **Межсетевой экран;**
  - подразделы **Сетевые фильтры и NAT** и **Управляющие соединения**.

  При этом вы не сможете настраивать сетевые фильтры и правила трансляции адресов, работать со списком управляющих соединений ViPNet.
- В случае завершения работы демона failoverd в разделе **Мониторинг** не отображается информация о работе системы.
- В случае завершения работы демона mftpd в разделе **Мониторинг** подраздел **MFTP** не отображается очередь конвертов и журнал MFTP.
- В случае завершения работы демона UC в разделе **Межсетевой экран** > подраздел **Пользователи** не отображается список активных пользователей Active Directory и Captive Portal.

Также веб-интерфейс переходит в режим ограниченной функциональности при работе ViPNet xFirewall в режиме кластера горячего резервирования и при обновлении справочников и лицензии, поступивших из программы ViPNet Центр управления сетью. В этом случае разделы **Системные настройки** и **Сетевые настройки** доступны только для просмотра.

В режиме ограниченной функциональности вы можете просмотреть информацию об остановленных процессах, недоступных настройках или ограниченных функциях, щелкнув значок  в верхнем правом углу страницы.

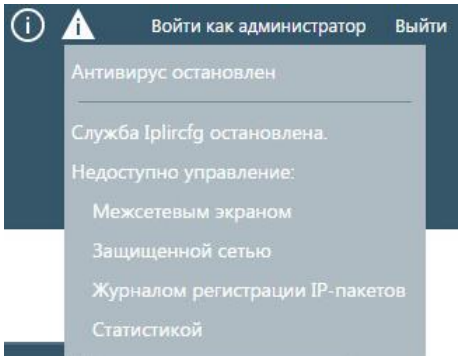

Рисунок 1. Просмотр информации об ограничениях функциональности

Подключение к веб-интерфейсу

Внимание! В ViPNet xFirewall по умолчанию включен сетевой фильтр Allow ViPNet WebGUI, разрешающий передачу трафика по протоколу TCP через порт 8080 со всех узлов сети. Не удаляйте и не отключайте этот фильтр, иначе в противном случае вы не сможете подключиться.

Чтобы подключиться к веб-интерфейсу, выполните следующие действия:

1 В адресной строке веб-браузера введите `http://<IP-адрес>:8080`, указав текущий IP-адрес для доступа к узлу ViPNet xFirewall.

Текущий IP-адрес доступа к узлу ViPNet xFirewall вы можете посмотреть в ПО ViPNet, установленном на вашем узле.

Примечание. Для подключения к веб-интерфейсу ViPNet xFirewall используйте следующие веб-браузеры:

- Internet Explorer 10, 11.
- Edge, Google Chrome и Mozilla Firefox последних версий.

2 В открывшемся окне аутентификации введите пароль пользователя сетевого узла ViPNet и нажмите кнопку **Войти**.

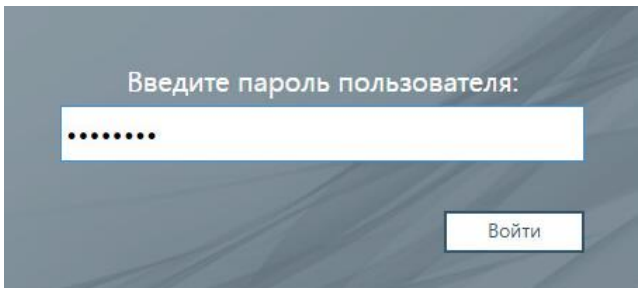

Рисунок 2. Аутентификация пользователя

Примечание. Если вы три раза подряд ввели неверный пароль, то чтобы сделать очередную попытку ввода пароля, подождите несколько секунд. Задержка реализована для предотвращения возможности подбора пароля методом перебора. С каждой новой неуспешной попыткой ввода пароля задержка увеличивается. При успешной попытке ввода пароля счетчик, который фиксирует неуспешные попытки, обнуляется. Также счетчик обнуляется после десятой неуспешной попытки ввода пароля. При этом после перезагрузки ViPNet xFirewall счетчик не обнуляется.

События обо всех неуспешных попытках ввода пароля фиксируются в журнале событий.

После успешной аутентификации откроется начальная страница веб-интерфейса ViPNet xFirewall в режиме пользователя. В данном режиме вы можете только просматривать настройки ViPNet

xFirewall. Чтобы изменять настройки, войдите в режим администратора (см. Режимы пользователя и администратора на стр. 15).

Рисунок 3. Начальная страница веб-интерфейса ViPNet xFirewall

Для входа в режим администратора выполните следующие действия:

1 В правом верхнем углу страницы щелкните ссылку **Войти как администратор**.

2 Введите пароль администратора данного сетевого узла или администратора группы сетевых узлов ViPNet.

Внимание! В режиме администратора возможен только один сеанс работы с ViPNet xFirewall.

---

3 Чтобы прервать сеанс другого администратора, который возможно сейчас работает с узлом ViPNet xFirewall с помощью веб-интерфейса или командной строки с другого сетевого узла ViPNet, установите соответствующий флажок. Если вы не установите данный флажок, то сеанс другого администратора не будет прерван, а ваша попытка входа в режим администратора будет отклонена.

4 Нажмите кнопку **Войти**.

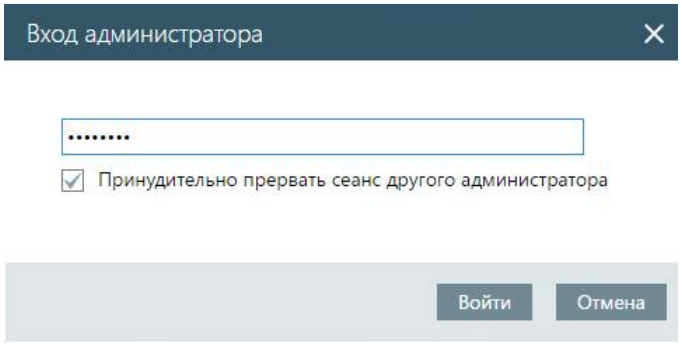

Рисунок 4. Вход в режим администратора

В результате вы будете работать в режиме администратора, сможете просматривать и изменять настройки ViPNet xFirewall с помощью веб-интерфейса.

Примечание. Если на ViPNet xFirewall истекают или уже истекли сроки действия персонального ключа пользователя (см. глоссарий, стр. 205) или ключей защиты ключей обмена (см. глоссарий, стр. 204), то в веб-интерфейсе появится соответствующее сообщение. В этом случае требуется обновить ключи. О том, как обновить ключи, см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора».

Настройка даты и времени

Чтобы компьютер с программным обеспечением ViPNet xFirewall корректно взаимодействовал с другими защищенными узлами ViPNet, необходимо правильно настроить системные дату и время.

Внимание! Если системные дата и время заданы неверно, защищенные соединения с другими узлами ViPNet могут быть заблокированы.

Чтобы настроить системные дату и время, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Системные настройки** > **Дата и время**.

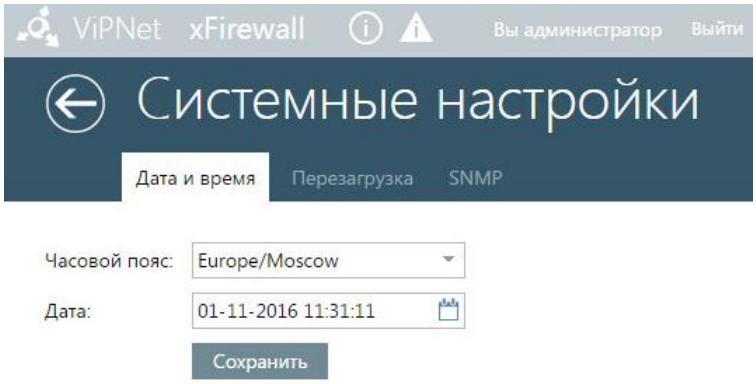

Рисунок 5. Настройка даты и времени

3 Если требуется изменить часовой пояс, в списке **Часовой пояс** выберите регион, где расположен сетевой узел с установленным программным обеспечением ViPNet xFirewall.

4 В поле **Дата** щелкните значок . Появится форма задания даты и времени.

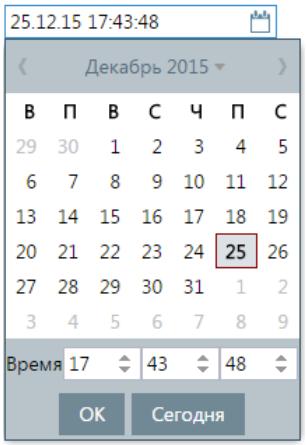

Рисунок 6. Задание даты и времени в соответствующей форме

5 В появившейся форме выполните следующие действия:

5.1 В календаре выберите необходимую дату.

5.2 Под календарем, в области **Время**, задайте необходимое время.

Примечание. Если вы хотите указать значения даты и времени, используемые в данный момент на компьютере, с помощью которого производится подключение к веб-интерфейсу, нажмите кнопку **Сегодня**.

5.3 Нажмите кнопку **OK**.

6 На странице **Дата и время** нажмите кнопку **Сохранить**.

Перезагрузка ViPNet xFirewall

В случае выявления каких-либо неполадок в работе ViPNet xFirewall, вы можете удаленно перезагрузить его с помощью веб-интерфейса. Для этого выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Системные настройки** > **Перезагрузка** и нажмите кнопку **Перезагрузить устройство**. При этом соединение с веб-интерфейсом будет разорвано, после перезагрузки повторно подключитесь к нему (см. Подключение к веб-интерфейсу на стр. 19).

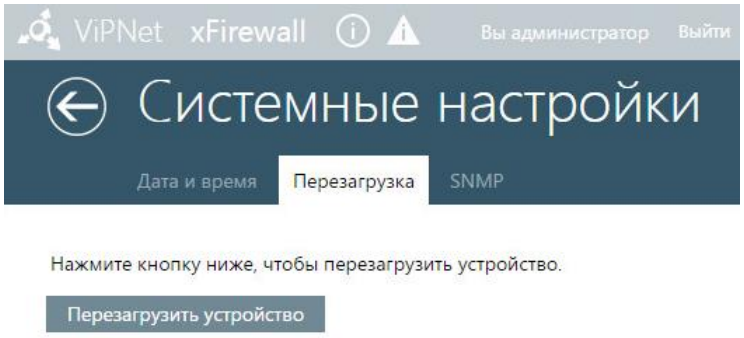

Рисунок 7. Перезагрузка ViPNet xFirewall

2

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet 26

Назначение дополнительных IP-адресов 29

Организация обработки трафика из нескольких VLAN 30

Использование агрегированных сетевых интерфейсов 36

Настройка сетевых интерфейсов Ethernet

Чтобы настроить сетевые интерфейсы Ethernet, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.

3 На левой панели выберите сетевой интерфейс Ethernet, который вы хотите настроить.

Внимание! Не изменяйте настройки сетевого интерфейса Ethernet, по которому вы подключились к ViPNet xFirewall. В противном случае вы можете потерять связь с ViPNet xFirewall.

Сетевым интерфейсам Ethernet, установленным в системе, присваиваются имена `eth0`, `eth1` и так далее (по количеству таких интерфейсов в системе).

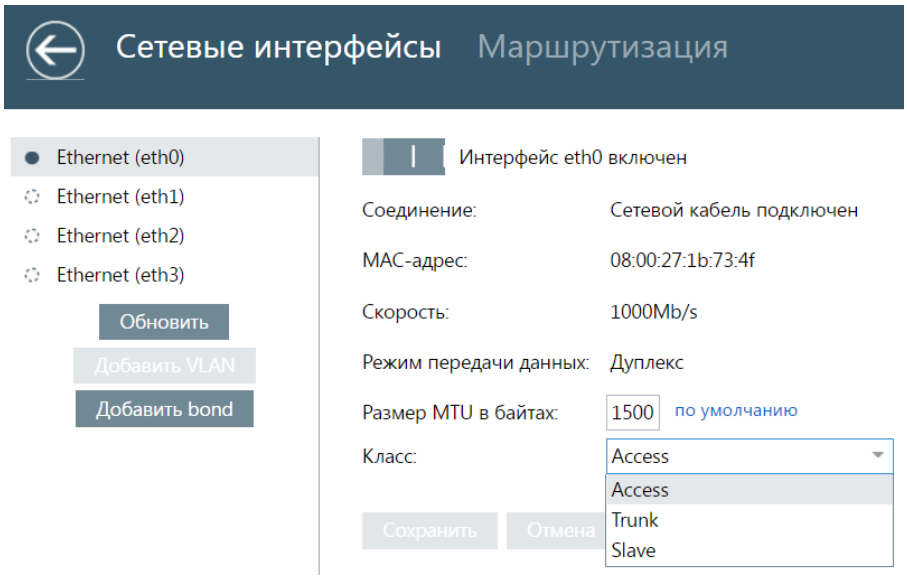

Рисунок 8. Настройка сетевого интерфейса Ethernet

4 По умолчанию для передачи данных через сетевой интерфейс используется размер MTU (см. глоссарий, стр. 201), равный 1500 байт. Чтобы оптимизировать передачу данных через интерфейс, вы можете изменить размер MTU. Для этого в поле **Размер MTU в байтах** задайте новое значение MTU из диапазона 1280–9000 байт. Чтобы вернуть значение по умолчанию, щелкните ссылку **по умолчанию**.

Внимание! В зависимости от платформы виртуализации, на которой развернуто исполнение ViPNet xFirewall xF-VA, накладываются следующие ограничения:

- VMware Workstation — изменение MTU не поддерживается.
- VMware vSphere — для изменения MTU необходимо предварительно настроить платформу виртуализации, разрешив использование Jumbo-кадров.
- Oracle VM VirtualBox — изменение MTU не поддерживается при использовании сетевых устройств AMD.

5 По умолчанию сетевому интерфейсу назначен класс `Access` (см. глоссарий, стр. 203). При необходимости смените класс интерфейса в соответствующем списке:

- Если требуется, чтобы данный интерфейс Ethernet обрабатывал трафик из нескольких VLAN (см. Настройка интерфейсов для обработки трафика из нескольких VLAN на стр. 30), назначьте ему класс `trunk`.
- Если вы хотите объединить данный интерфейс Ethernet с другими в составе агрегированного интерфейса (см. Использование агрегированных сетевых интерфейсов на стр. 36), назначьте ему класс `slave`.

6 В правой части страницы выполните одно из действий:

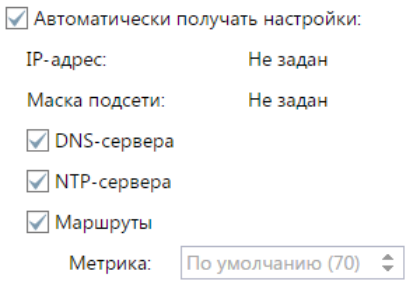

Рисунок 9. Настройка сетевого интерфейса

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Автоматически получать настройки.**

  Также для режима DHCP вы можете задать дополнительные параметры:

  - Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
  - Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
  - Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

    Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка параметров динамических маршрутов от DHCP-протокола на стр. 146). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах.

Подробнее см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию. Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера (на стр. 147).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите кнопку **Сохранить**.

7 Включите сетевой интерфейс. Для этого щелкните переключатель в верхней части страницы. Состояние сетевого интерфейса отображается рядом с переключателем.

Примечание. Сетевой интерфейс можно включить только после задания настроек интерфейса.

---

8 При необходимости выполните настройку маршрутизации (см. Настройка маршрутизации на стр. 135).

9 При необходимости задайте дополнительные IP-адреса для сетевого интерфейса (см. Назначение дополнительных IP-адресов на стр. 29).

Внимание! Максимальное количество интерфейсов в ViPNet xFirewall не может превышать 128 (как физических, так и виртуальных, включая loopback).

Назначение дополнительных IP-адресов

Назначение дополнительных IP-адресов (alias) для сетевых интерфейсов Ethernet ViPNet xFirewall удобно при развертывании сетей некоторых топологий. Например, с помощью дополнительных IP-адресов вы можете в рамках своей сети организовать логическую подсеть, узлам которой, в отличие от узлов остальной сети, будет разрешен доступ в Интернет.

Чтобы задать дополнительные IP-адреса на сетевом интерфейсе, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.
3. На левой панели выберите сетевой интерфейс, который вы хотите настроить.
4. Включите сетевой интерфейс. Для этого щелкните переключатель в верхней части страницы. Состояние сетевого интерфейса отображается рядом с переключателем.
5. На правой панели выполните следующие действия:
   - **5.1** Убедитесь, что сетевому интерфейсу назначен класс `access`.
   - **5.2** При задании дополнительного IP-адреса на сетевом интерфейсе должен быть установлен статический основной IP-адрес. Поэтому убедитесь, что снят флажок **Автоматически получать настройки**.
   - **5.3** В группе **Дополнительные IP-адреса** выполните одно из действий:
     - Чтобы добавить для сетевого интерфейса дополнительный IP-адрес, нажмите кнопку **Добавить** и появившейся строке задайте требуемый IP-адрес и маску подсети. Затем нажмите кнопку **Сохранить**.
     - Чтобы удалить дополнительный IP-адрес, в строке рядом с ним щелкните значок ✕. В окне сообщения нажмите кнопку **ОК**.

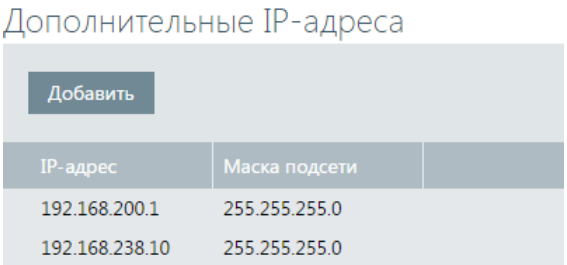

Рисунок 10. Изменение дополнительных IP-адресов

Организация обработки трафика из нескольких VLAN

Вы можете использовать ViPNet xFirewall для обработки трафика в физической локальной сети, разделенной на нескольких независимых виртуальных локальных сетей VLAN (см. глоссарий, стр. 202). Это возможно благодаря поддержке виртуальных интерфейсов и тегированию (маркировке) трафика в соответствии со стандартом IEEE 802.1 Q. Каждой VLAN присваивается идентификатор из диапазона от 1 до 4094 (значения 0 и 4095 зарезервированы).

Настройка интерфейсов для обработки трафика из нескольких VLAN

Для организации обработки трафика из нескольких VLAN подключите один из сетевых интерфейсов ViPNet xFirewall (или компьютера, на котором развернут виртуальный образ ViPNet xFirewall) к коммутатору, объединяющему виртуальные сети, и выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.
3. На левой панели выберите сетевой интерфейс Ethernet, к которому подключен коммутатор, и на правой панели в списке **Класс** выберите класс `trunk`. Нажмите кнопку **Сохранить**.
4. На левой панели нажмите кнопку **Добавить VLAN**. Появится окно **Создание VLAN**.

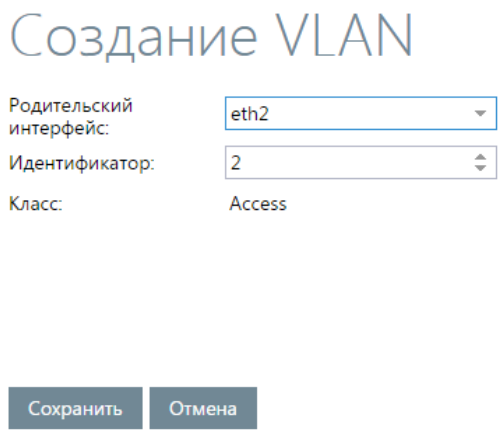

Рисунок 11. Создание виртуального интерфейса VLAN

5. В списке **Родительский интерфейс** отображаются интерфейсы Ethernet вашего ViPNet xFirewall, для которых указан класс `trunk`. Если таких интерфейсов несколько, выберите нужный вам.

6 В списке **Идентификатор** выберите номер создаваемого виртуального интерфейса. Создаваемому виртуальному интерфейсу будет присвоено имя в следующем формате:

`<физический интерфейс>.<номер виртуального интерфейса>`

7 В правой части страницы укажите настройки для одной из сетей, находящихся за коммутатором:

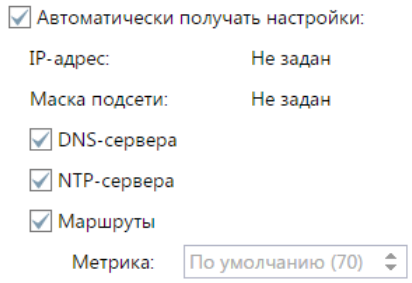

Рисунок 12. Настройка сетевого интерфейса

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Автоматически получать настройки.**

  Также для режима DHCP вы можете задать дополнительные параметры:

  - Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
  - Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
  - Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

    Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка параметров динамических маршрутов от DHCP-протокола на стр. 146). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

    Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию. Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера (на стр. 147).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите кнопку **Сохранить**.

8 В результате будет создан виртуальный интерфейс VLAN для одной из виртуальных сетей, находящихся за коммутатором. Он появится в списке сетевых интерфейсов на левой панели. Чтобы создать виртуальные интерфейсы для других сетей, повторите шаги 4–7.

9 Чтобы разрешить прохождение трафика через виртуальные интерфейсы и задать их тип, отредактируйте файл конфигурации `iplir.conf`. Для этого подключитесь к ViPNet xFirewall с

помощью командного интерпретатора в режиме администратора (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора»):

Внимание! При подключении к ViPNet xFirewall с помощью командного интерпретатора в режиме администратора текущий сеанс администратора в веб-интерфейсе будет завершен.

9.1 Для редактирования файла конфигурации `iplir.conf` выполните команду:

```
hostname# iplir config
```

Примечание. Перед редактированием файла `iplir.conf` остановите демон iplir с помощью команды:

```
hostname# iplir stop
```

После завершения редактирования файла `iplir.conf` запустите демон iplir с помощью команды:

```
hostname# iplir start
```

9.2 Добавьте секции `[adapter]`, описывающие созданные виртуальные интерфейсы (см. документ «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», раздел «Секция [adapter]»). В каждой секции укажите следующие параметры:

```
name= <физический интерфейс>.<номер виртуального интерфейса>
type= internal
allowtraffic=on
```

9.3 В секции `[adapter]` с описанием интерфейса, к которому подключен коммутатор, присвойте параметру `allowtraffic` значение `off`:

9.4 Нажмите сочетание клавиш **Ctrl+O**, чтобы сохранить файл конфигурации, затем нажмите клавишу **Enter**.

9.5 Нажмите сочетание клавиш **Ctrl+X**, чтобы закрыть файл.

10 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

11 На левой панели выберите интерфейс, к которому подключен коммутатор, и включите его с помощью переключателя в верхней части страницы. Созданные виртуальные интерфейсы VLAN включатся автоматически.

После произведенных настроек ViPNet xFirewall сможет обрабатывать трафик из виртуальных сетей на соответствующих виртуальных интерфейсах.

Пример организации обработки трафика из нескольких VLAN

Рассмотрим пример организации обработки трафика из нескольких VLAN.

На рисунке ниже приведена схема использования ViPNet xFirewall в сети с тремя VLAN, которым присвоены номера 10, 20 и 30.

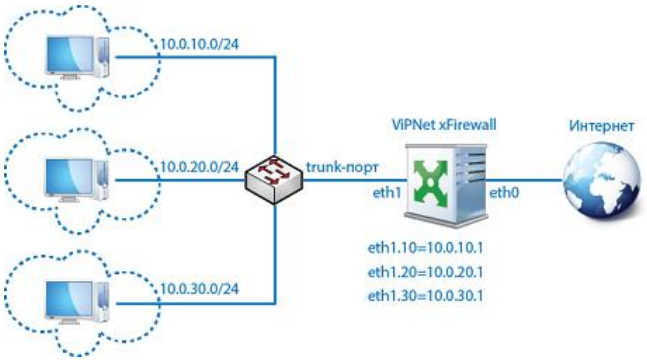

Рисунок 13. Схема использования ViPNet xFirewall в сети с VLAN

Чтобы обеспечить работоспособность этой схемы, выполните описанные ниже действия.

Предполагается, что сетевые настройки соответствуют приведенным на рисунке.

Внимание! Максимальное количество интерфейсов в ViPNet xFirewall не может превышать 128 (как физических, так и виртуальных, включая loopback)

---

1. Войдите в веб-интерфейс в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы** и выберите интерфейс eth1.
3. Для параметра **Класс** выберите из списка значение **Trunk** и нажмите кнопку **Сохранить**.

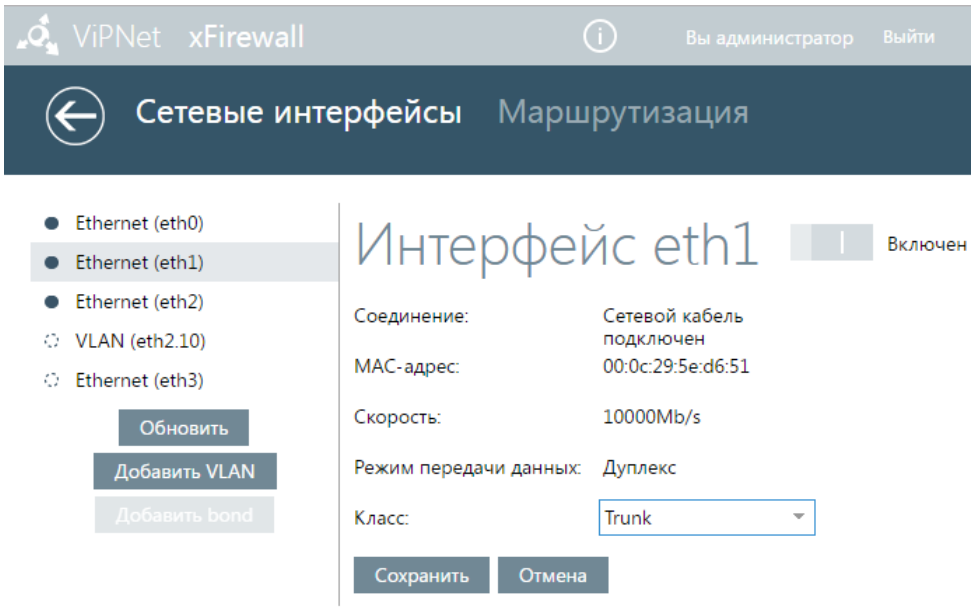

Рисунок 14. Изменение класса интерфейса eth1

4 Добавьте виртуальные интерфейсы eth1.10, eth1.20, eth1.30, которые будут соответствовать виртуальным сетям с номерами 10, 20 и 30:

4.1 Нажмите кнопку **Добавить VLAN**. Откроется страница добавления виртуального интерфейса.

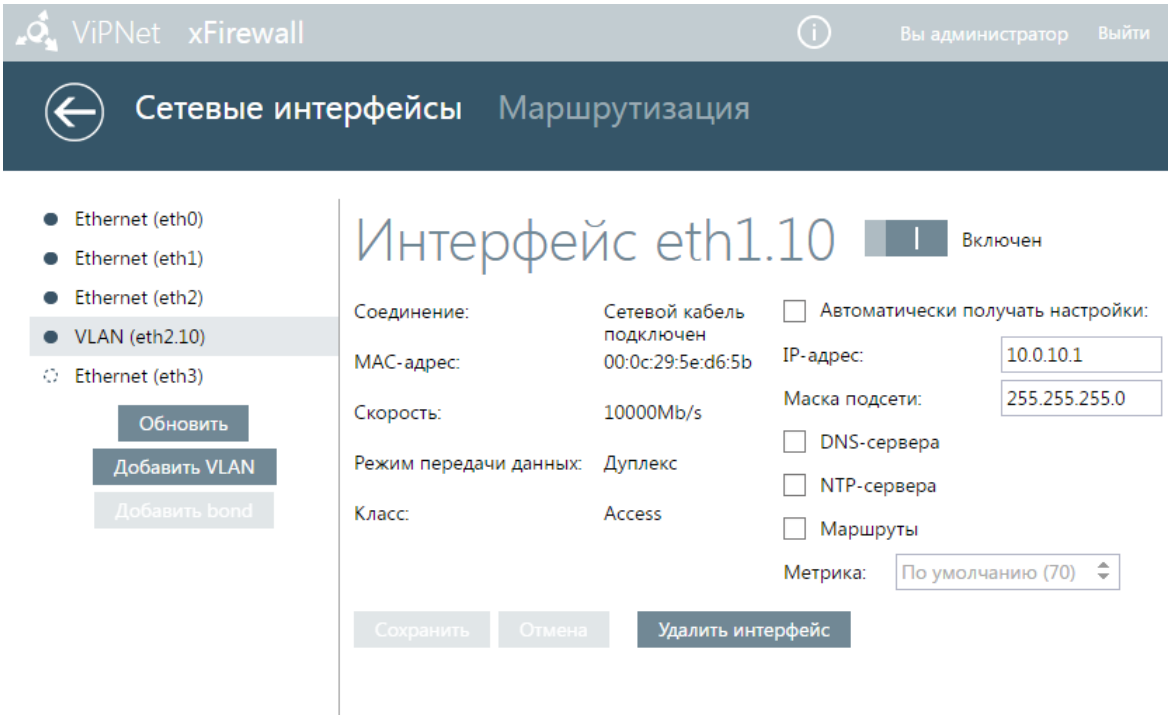

Рисунок 15. Добавление виртуального интерфейса

4.2 Укажите идентификатор интерфейса `10`, IP-адрес `10.0.10.1` и маску подсети `255.255.255.0`.

4.3 Нажмите кнопку **Сохранить**.

4.4 Аналогичным образом добавьте виртуальные интерфейсы с идентификаторами 20 и 30 и IP-адресами `10.0.20.1` и `10.0.30.1`.

5 Включите созданные виртуальные интерфейсы с помощью переключателей.

6 Войдите в командный интерпретатор и выполните команду `enable`, чтобы перейти в режим администратора. В ответ на приглашение введите пароль администратора.

7 Завершите работу управляющего демона с помощью команды:

```
hostname# iplir stop
```

8 Откройте файл конфигурации `iplir.conf` для редактирования с помощью команды:

```
hostname# iplir config
```

9 Добавьте секции `[adapter]`, описывающие виртуальные интерфейсы eth1.10, eth1.20, eth1.30. В каждой секции укажите следующие параметры (на примере интерфейса eth1.10):

```
name= eth1.10
type= internal
allowtraffic= on
```

10 В секции `[adapter]` с описанием интерфейса `eth1` (то есть в секции, содержащей строку «`name= eth1`») измените значение параметра `allowtraffic` на `off`:

```
[adapter]
name= eth1
allowtraffic= off
```

11 Нажмите сочетание клавиш **Ctrl+O**, чтобы сохранить файл конфигурации, затем нажмите клавишу **Enter**.

12 Нажмите сочетание клавиш **Ctrl+X**, чтобы закрыть файл.

13 Запустите управляющий демон с помощью команды:

```
hostname# iplir start
```

После выполненных настроек ViPNet xFirewall сможет обрабатывать трафик из трех виртуальных сетей на соответствующих виртуальных интерфейсах.

Использование агрегированных сетевых интерфейсов

Если пропускной способности отдельных сетевых интерфейсов ViPNet xFirewall недостаточно для ваших задач или если требуется повысить надежность ваших каналов передачи данных, вы можете объединить несколько физических сетевых интерфейсов ViPNet xFirewall в один логический — агрегированный интерфейс (см. глоссарий, стр. 203). При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

Например, если вам нужен канал связи с пропускной способностью выше 1 Гбит/с, а на вашем исполнении ViPNet xFirewall есть только гигабитные интерфейсы, вы можете объединить два или три из них в один агрегированный. При этом даже если один из объединенных интерфейсов выйдет из строя, агрегированный канал продолжит работать.

Кроме того, вы можете использовать агрегированный интерфейс только для резервирования канала связи, без увеличения его пропускной способности. В этом случае весь трафик будет передаваться через один из подчиненных физических интерфейсов, остальные же начинают работать только при его сбое.

Агрегированные каналы целесообразно использовать в отказоустойчивых сетях, по каналам которых передаются большие объемы данных, например, в сетях центров обработки данных.

Чтобы задать, как будет распределяться нагрузка по подчиненным физическим интерфейсам, необходимо выбрать один из режимов работы агрегированного интерфейса.

Создание агрегированного интерфейса

Чтобы добавить новый агрегированный сетевой интерфейс, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.
3. На левой панели последовательно выберите сетевые интерфейсы Ethernet, которые вы хотите объединить, и на правой панели установите для них класс `slave`.
4. На левой панели нажмите кнопку **Добавить bond**. Откроется страница **Создание bond**.

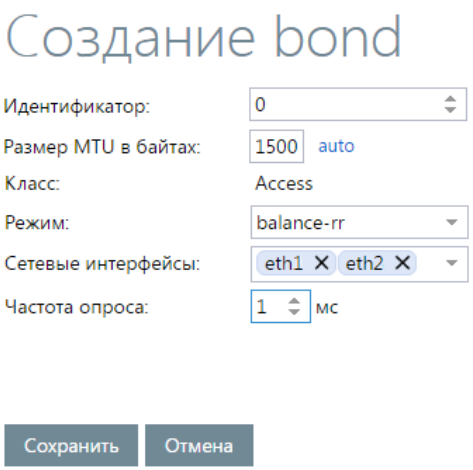

Рисунок 16. Создание агрегированного канала

5 На странице **Создание bond** задайте следующие параметры:

- В поле **Идентификатор** задайте номер создаваемого агрегированного интерфейса. Вы можете создать до трех агрегированных интерфейсов с номерами 0, 1 или 2. Созданный агрегированный интерфейс будет иметь имя `bond<номер>`.
- В списке **Режим** выберите режим работы агрегированного интерфейса.
- В списке **Сетевые интерфейсы** последовательно выберите физические интерфейсы класса `slave`, которые вы хотите объединить. Эти интерфейсы станут подчиненными для создаваемого агрегированного интерфейса. Вы можете выбрать до трех подчиненных интерфейсов. При создании агрегированного интерфейса необходимо выбрать не менее одного подчиненного интерфейса.
- В поле **Частота опроса** задайте частоту проверки соединения на подчиненных физических интерфейсах в миллисекундах. Вы можете задать от 1 до 1000 миллисекунд.

6 Для режимов, в которых это требуется, задайте дополнительные параметры.

7 По умолчанию созданному интерфейсу назначается класс `access`. Если вы хотите, чтобы интерфейс обрабатывал трафик из нескольких VLAN (см. Настройка интерфейсов для обработки трафика из нескольких VLAN на стр. 30), назначьте ему класс `trunk`.

8 В правой части страницы выберите одно из действий:

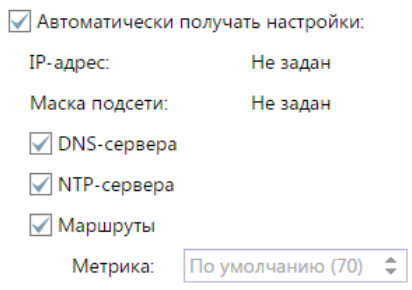

Рисунок 17. Настройка сетевого интерфейса

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, установите флажок **Автоматически получать настройки.**

Также для режима DHCP вы можете задать дополнительные параметры:

- Чтобы включить автоматическое получение адресов DNS-серверов от DHCP-сервера, установите флажок **DNS-сервера**.
- Чтобы включить автоматическое получение адресов NTP-серверов от DHCP-сервера, установите флажок **NTP-сервера**.
- Чтобы включить автоматическое получение маршрутов от DHCP-сервера, установите флажок **Маршруты**.

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка параметров динамических маршрутов от DHCP-протокола на стр. 146). При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах. Подробнее см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Просмотр настроек DHCP в режиме клиента».

  Первоначально для маршрутов, полученных от DHCP-сервера, задана метрика по умолчанию. Если вы хотите задать для этих маршрутов другую метрику, укажите ее в поле **Метрика**. Подробнее о том, как настраивается метрика, см. в разделе Настройка метрики для маршрутов DHCP-сервера (на стр. 147).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, задайте этот адрес и маску подсети в соответствующих полях.

После задания необходимых настроек нажмите кнопку **Сохранить**.

9 Дальнейшие настройки необходимо производить в командном интерпретаторе (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора»):

9.1 Для редактирования файла конфигурации `iplir.conf` выполните команду:

```
hostname# iplir config
```

Примечание. Перед редактированием файла `iplir.conf` остановите демон iplir с помощью команды:

```
hostname# iplir stop
```

После завершения редактирования файла `iplir.conf` запустите демон iplir с помощью команды:

```
hostname# iplir start
```

9.2 Добавьте секцию `[adapter]`, описывающую созданный агрегированный интерфейс (см. документ «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», раздел «Секция [adapter]»). В секции укажите следующие параметры:

```
name= bond<номер агрегированного интерфейса>
type= internal
allowtraffic= on
```

9.3 Нажмите сочетание клавиш **Ctrl+O**, чтобы сохранить файл конфигурации, затем нажмите клавишу **Enter**.

9.4 Нажмите сочетание клавиш **Ctrl+X**, чтобы закрыть файл.

10 Последовательно перейдите на страницы с настройками подчиненных физических интерфейсов и включите их с помощью соответствующих переключателей.

11 Вернитесь на страницу с агрегированным каналом и включите его с помощью переключателя в верхней части страницы.

В результате будет создан агрегированный канал с именем `bond<номер>`, работающий в заданном режиме и имеющий заданный класс. В дальнейшем вы можете работать с агрегированным интерфейсом так же, как и с обычным физическим.

Внимание! Максимальное количество интерфейсов в ViPNet xFirewall не может превышать 128 (как физических, так и виртуальных, включая loopback).

Режимы работы агрегированного интерфейса

При создании агрегированного интерфейса необходимо указать режим его работы, наиболее подходящий для решения ваших задач. В ViPNet xFirewall предусмотрено несколько режимов, позволяющих по-разному распределять нагрузку между подчиненными интерфейсами. Эти режимы и их параметры описаны в таблице ниже.

Таблица 5. Режимы работы агрегированного интерфейса

Режим	Описание
`balance-rr`	Режим, подходящий как для балансировки нагрузки на подчиненных интерфейсах, так и для защиты от сбоев. Может применяться в сетях с простой топологией. В этом режиме исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.
`balance-xor`	Режим, предназначенный для защиты от сбоев и распределения нагрузки таким образом, чтобы пакеты от одного и того же отправителя к одному и тому же получателю всегда отправлялись через один и тот же подчиненный интерфейс. В этом режиме для определения подчиненного физического интерфейса, через который отправляется пакет, используется специальная хэш-функция, алгоритм вычисления которой вы можете задать с помощью списка **Алгоритм хеширования** после создания агрегированного интерфейса. Вы можете задать один из следующих алгоритмов: • `layer2` — в алгоритме используются MAC-адреса отправителя и получателя пакета, таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами;

Режим	Описание
	• `layer2+3` — в алгоритме используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протокола IPv4), таким образом, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами и IP-адресами; • `layer3+4` — в алгоритме используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии), таким образом, одинаковыми считаются сетевые узлы с одинаковыми IP-адресами, а также портами TCP или UDP.
`balance-tlb`	Режим, предназначенный для балансировки нагрузки на подчиненных интерфейсах и рекомендуемый к использованию при передаче большого числа пакетов разного размера, когда более простые режимы не распределяют нагрузку равномерно. В этом режиме ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных физических интерфейсов, и на основе этого выполняется выбор интерфейса, через который будет передан пакет, попавший на агрегированный интерфейс. **Примечание.** Для работы агрегированного интерфейса в режиме `balance-tlb` необходимо, чтобы все подчиненные физические интерфейсы были подключены к сети через коммутатор.
`802.3ad`	Режим динамического агрегирования с использованием протокола LACP, предназначен для комплексной балансировки нагрузки. В этом режиме агрегированный интерфейс работает следующим образом: • Среди подчиненных физических интерфейсов формируются группы — «агрегаторы», скорость передачи данных на интерфейсах которых одинакова (например, группа гигабитных интерфейсов и группа 10-гигабитных интерфейсов). • Один из агрегаторов выбирается активным в соответствии с алгоритмом, задаваемым с помощью списка **Режим агрегатора** после создания агрегированного интерфейса. Вы можете выбрать один из приведенных ниже алгоритмов: `stable` — алгоритм, при котором первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора. `bandwidth` — режим, при котором первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора. `count` — режим, при котором первоначально выбирается агрегатор с наибольшим количеством подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора. • Внутри агрегатора подчиненный физический интерфейс, через который

Режим	Описание
	отправляются исходящие пакеты, выбирается аналогично режиму `balance-xor`. • С другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью списка **Частота обмена пакетами** после создания агрегированного интерфейса. В случае выбора параметра `slow` обмен пакетами по протоколу LACP выполняется каждые 30 секунд, в случае выбора параметра `fast` — каждую секунду. Обмен пакетами позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую.
`active-backup`	Режим, предназначенный для защиты от сбоев, но не для балансировки нагрузки на подчиненных физических интерфейсах. В этом режиме один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью списка **Основной интерфейс** после создания агрегированного интерфейса), и все исходящие пакеты отправляются через него. При этом, в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
`broadcast`	Режим предоставляет наибольшую защиту от сбоев. В этом режиме пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно. **Примечание**. Режим `broadcast` требует специальной настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов данных. Если агрегированный канал работает в режиме `broadcast`, организовать на этом канале защиту соединения по технологии L2OverIP невозможно.

Примечание. Если в процессе функционирования агрегированного канала вы измените режим работы агрегированного интерфейса, возможно кратковременное пропадание соединения (до 1 секунды).

Пример создания агрегированного канала между ViPNet xFirewall и коммутатором

Рассмотрим пример организации агрегированного канала для взаимодействия ViPNet xFirewall, имеющего три физических интерфейса Ethernet, и коммутатора производства компании Cisco.

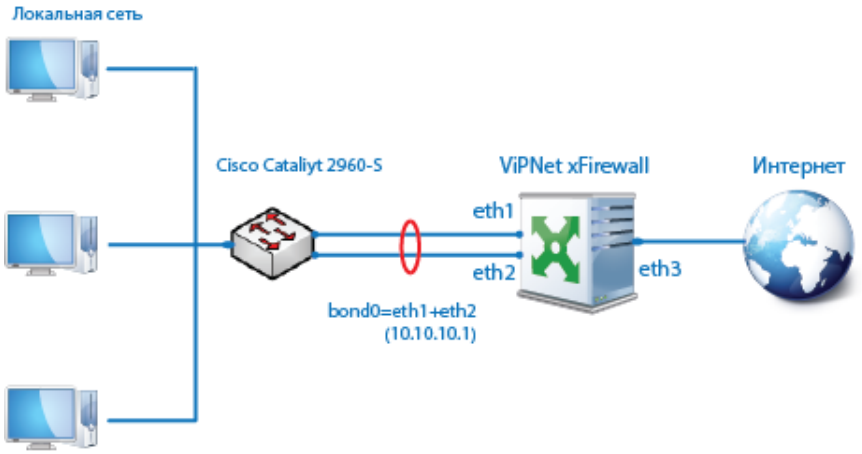

Рисунок 18. Создание агрегированного интерфейса между ViPNet xFirewall и коммутатором

Для обеспечения отказоустойчивости и повышения пропускной способности вы можете объединить на ViPNet xFirewall интерфейсы `eth1` и `eth2` в агрегированный интерфейс `bond0` и организовать агрегированный канал связи с коммутатором.

Так как при передаче пакетов от компьютеров локальной сети через коммутатор MAC-адрес, IP-адрес и порт сетевого узла отправителя не подменяется, помимо режимов работы агрегированных каналов `balance-rr`, `active-backup` и `broadcast` можно использовать режимы, связанные с распределением нагрузки по MAC-адресам, IP-адресам и портам: `balance-xor`, `balance-tlb` и `802.3ad`. Подробнее о режимах работы агрегированных интерфейсов см. раздел (см. Режимы работы агрегированного интерфейса на стр. 39).

Используем режим `802.3ad`. В этом режиме для определения подчиненного физического интерфейса, через который отправляется пакет, используется специальная хэш-функция, поэтому пакеты от одного и того же отправителя к одному и тому же получателю всегда будут отправляться через один и тот же подчиненный физический интерфейс. Хэш-функция вычисляется по алгоритму `layer3+4`, поэтому учитываются MAC-адреса, IP-адреса, а также порты TCP или UDP отправителей и получателей.

Чтобы настроить описанный агрегированный канал связи, на ViPNet xFirewall выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.

3 Установите для физических интерфейсов **eth1** и **eth2** класс **Slave**. Для этого на левой панели выберите сетевой интерфейс Ethernet и на правой панели в списке **Класс** выберите класс **Slave**. Нажмите кнопку **Сохранить**.

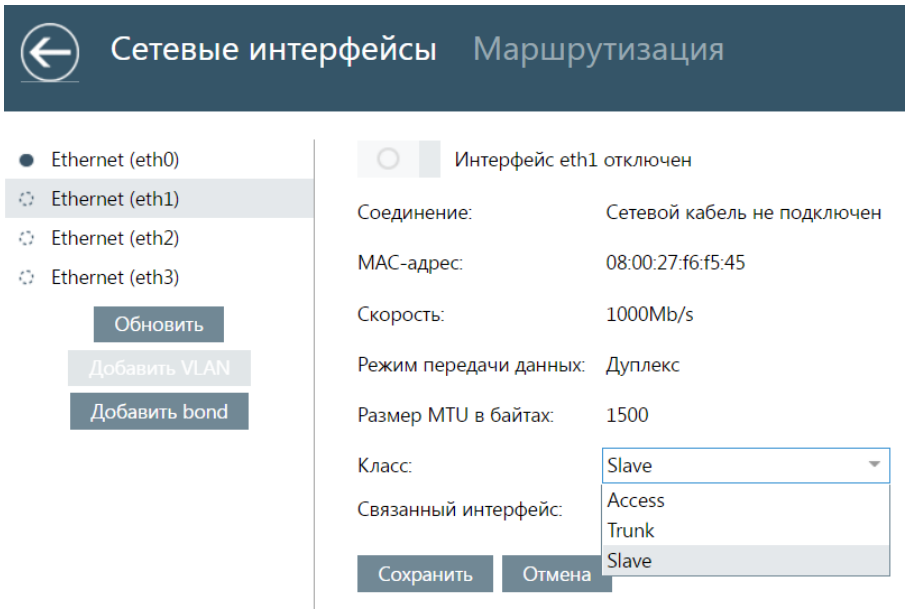

Рисунок 19. Настройка класса slave для интерфейса eth1

4 Создайте агрегированный интерфейс `bond0`. Для этого на левой панели нажмите кнопку **Добавить bond**. Далее выберите режим **802.3ad**, добавьте сетевые интерфейсы **eth1** и **eth2**. Задайте параметры создаваемого интерфейса `bond0`. Нажмите кнопку **Сохранить**.

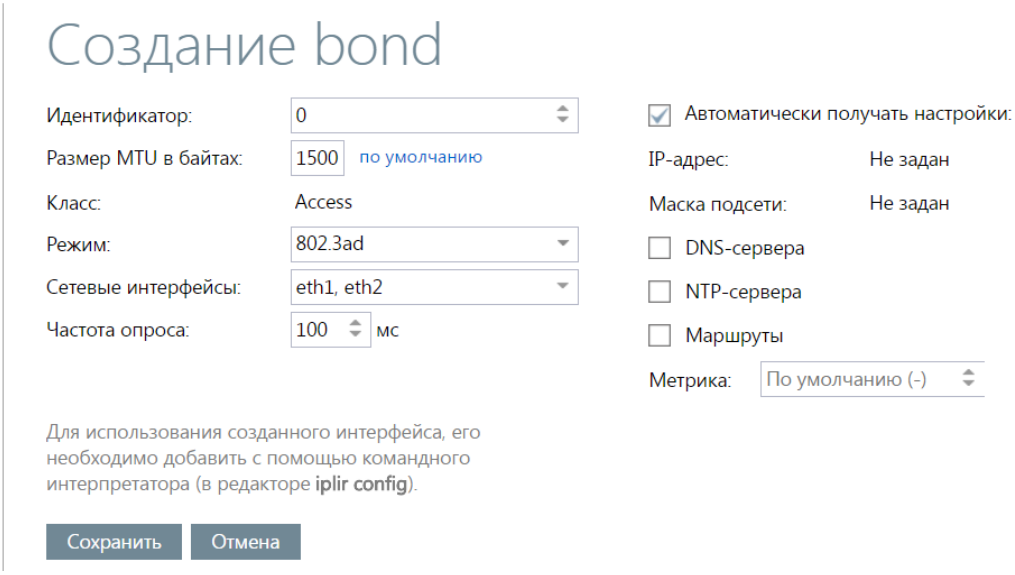

Рисунок 20. Создание агрегированного интерфейса bond

5 Выберите в левой части экрана интерфейс `bond0`. Задайте для него алгоритм вычисления хэш-функции `layer3+4`, значение IP-адреса `10.10.10.0` и маски подсети `255.255.255.0`. Нажмите кнопку **Сохранить**.

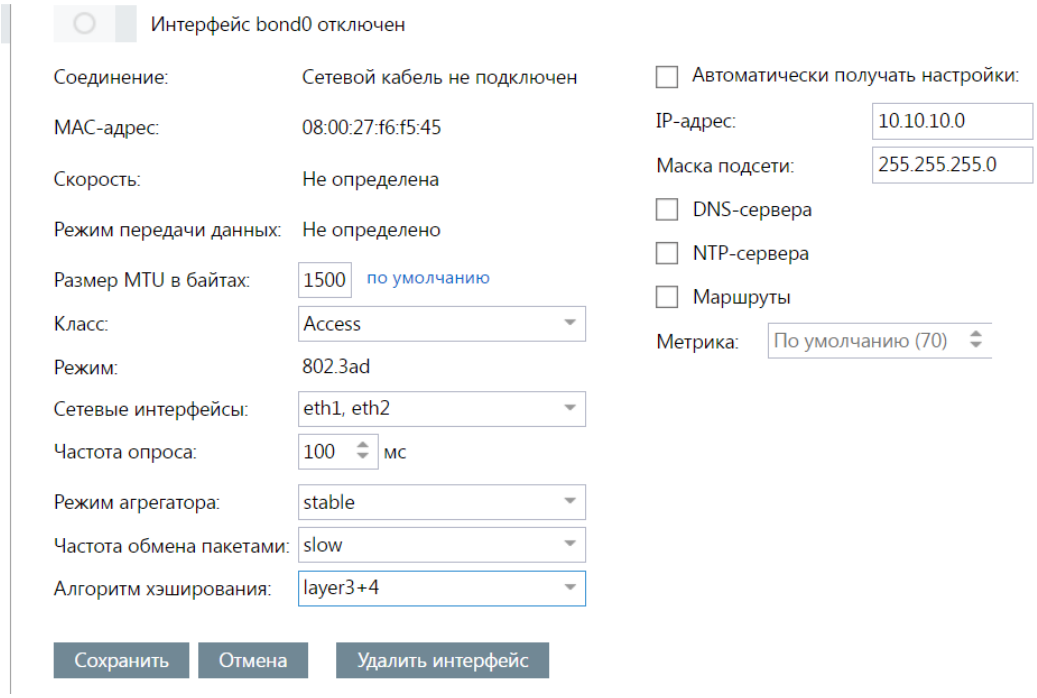

Рисунок 21. Настройка агрегированного интерфейса bond0

6 Чтобы разрешить прохождение трафика через агрегированный интерфейс и задать его тип, отредактируйте файл конфигурации `iplir.conf`. Для этого подключитесь к ViPNet xFirewall с помощью командного интерпретатора в режиме администратора (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора»).

Внимание! При подключении к ViPNet xFirewall с помощью командного интерпретатора в режиме администратора текущий сеанс администратора в веб-интерфейсе будет завершен.

Выполните следующие действия:

6.1 Остановите управляющий демон с помощью команды:

```
hostname> iplir stop
```

6.2 Откройте файл `iplir.conf` с помощью команды:

```
hostname# iplir config
```

6.3 Добавьте секцию `[adapter]` следующего содержания:

```
[adapter]
name= bond0
allowtraffic= on
type= internal
```

6.4 Сохраните файл конфигурации с помощью сочетания клавиш **Ctrl+O**. Затем нажмите клавишу **Enter**.

6.5 Закройте файл с помощью сочетания клавиш **Ctrl+X**.

6.6 Запустите управляющий демон с помощью команды:

```
hostname> iplir start
```

7 Соедините интерфейсы `eth1` и `eth2` с интерфейсами коммутатора.

8 Последовательно включите подчиненные физические интерфейсы `eth1` и `eth2`.

9 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

10 С помощью переключателя включите агрегированный сетевой интерфейс `bond0`.

Чтобы настроить подключение к агрегированному каналу на коммутаторе Cisco (например, Cisco Catalyst 2960-S), выполните следующие действия:

1 Предварительно объедините сетевые интерфейсы коммутатора, к которым подключены компьютеры локальной сети, а также интерфейсы, которые будут подключены к агрегированному каналу, в виртуальную сеть VLAN с определенным номером (в примере VLAN имеет номер 116).

2 Создайте логический интерфейс `port-channel` (в примере он имеет номер 2):

```
interface Port-channel2
    switchport access vlan 116
    swithcport mode access
end
```

3 Укажите два физических интерфейса (в примере имена этих интерфейсов — `GigabitEthernet0/1` и `GigabitEthernet0/2`), которые будут входить в состав логического интерфейса `port-channel2`. Эти физические интерфейсы будут использоваться для подключения к агрегированному каналу.

```
interface GigabitEthernet0/1
    switchport access vlan 116
    swithcport mode access
    channel-group 2 mode active
!
interface GigabitEthernet0/2
    switchport access vlan 116
    swithcport mode access
    channel-group 2 mode active
!
```

4 Настройте интерфейсы, к которым подключены компьютеры локальной сети, следующим образом:

```
interface GigabitEthernet<номер интерфейса>
    switchport access vlan <номер VLAN>
    swithcport mode access
!
```

В результате ViPNet xFirewall будет доступен по заданному IP-адресу, а трафик между коммутатором и ViPNet xFirewall будет идти по агрегированному каналу, состоящему из двух подчиненный физических каналов. В случае отказа одного из подчиненных каналов оставшийся продолжает работу и сессии с отказавшего канала перенаправляются на оставшийся. Этим обеспечивается отказоустойчивость полученного агрегированного канала.

3

Управляющие соединения ViPNet xFirewall

Просмотр сведений о сетевых узлах ViPNet 48

Управление сертификатами 52

Просмотр сведений о сетевых узлах ViPNet

Удаленную настройку и управление ViPNet xFirewall необходимо выполнять только по доверенному каналу, защищенными средствами шифрования ViPNet. Для этого ViPNet xFirewall должен быть закреплен за ViPNet-координатором и иметь связи с узлами сети ViPNet, с которых разрешены управление и настройка ViPNet xFirewall. Связи устанавливаются администратором сети ViPNet в программе ViPNet Центр управления сетью (см. глоссарий, стр. 202).

Для удаленной настройки и управления на узлах ViPNet вы можете использовать:

- веб-браузер;
- командный интерпретатор;
- программу ViPNet Центр управления сетью (см. глоссарий, стр. 202).

Подробнее о способах управления ViPNet xFirewall см. в документе «ViPNet xFirewall. Общее описание», раздел «Возможности управления ViPNet xFirewall».

Просмотр сведений о сетевых узлах ViPNet

Вы можете просмотреть сведения об узлах ViPNet, для которых с вашим узлом установлены связи: например, чтобы узнать IP-адреса узлов, с которых разрешена настройка и управление. Для этого выполните следующие действия:

1. На начальной странице веб-интерфейса щелкните плитку **Управляющие соединения**.
2. На странице **Узлы ViPNet** просмотрите список имен и IP-адресов сетевых узлов ViPNet, с которыми у вашего узла есть связь, а также сведения о времени последней активности пользователей этих узлов. В этом списке:
   - слева от имен узлов, являющихся клиентами ViPNet, отображается значок  ;
   - слева от имен узлов, являющихся координаторами ViPNet, отображается значок  ;
   - узлы, которые в текущий момент недоступны либо статус которых неизвестен, выделены серым цветом.

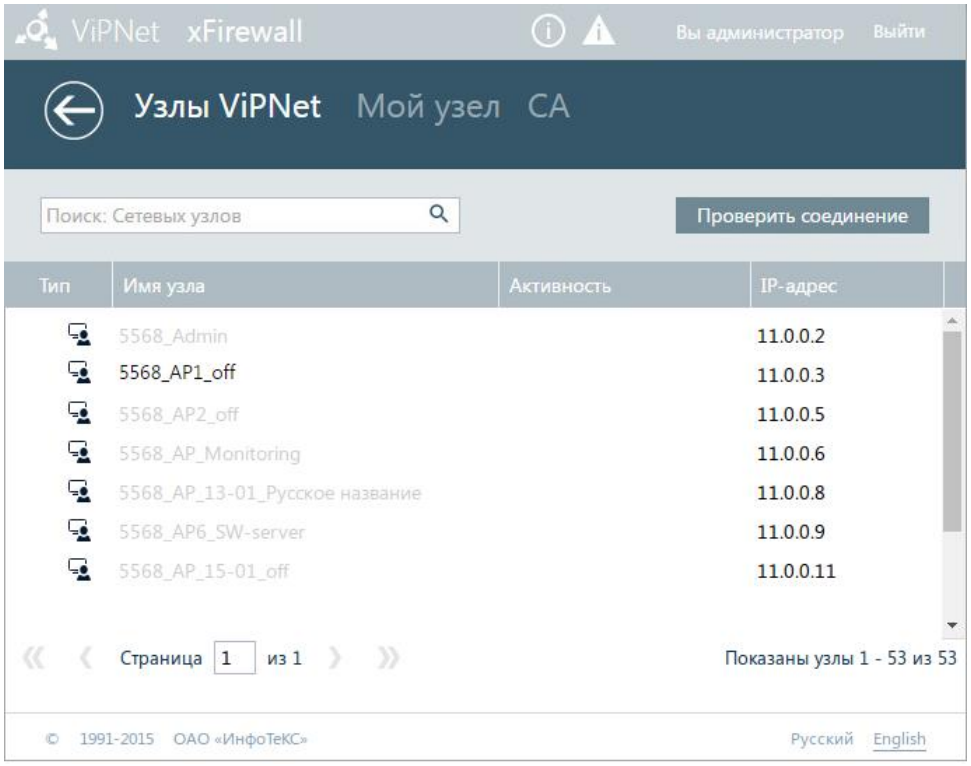

Рисунок 22. Просмотр списка узлов сети ViPNet

3 Чтобы просмотреть подробные сведения о каком-либо узле, дважды щелкните его в списке. На открывшейся странице на панели навигации выберите соответствующий раздел, чтобы просмотреть следующую информацию:

- общая информация: имя узла, версия ПО ViPNet и операционной системы, установленных на узле, текущие IP-адреса видимости узла, порт доступа для TCP-туннеля;

Примечание. Информация о версиях ПО ViPNet и операционной системы, установленных на узле, отображается только после проверки соединения с этим узлом.

- IP-адреса доступа к узлу: реальные и виртуальные;
- настройки межсетевого экрана при подключении к внешней сети (для координаторов сети ViPNet);
- настройки туннелирования (для координаторов сети ViPNet).

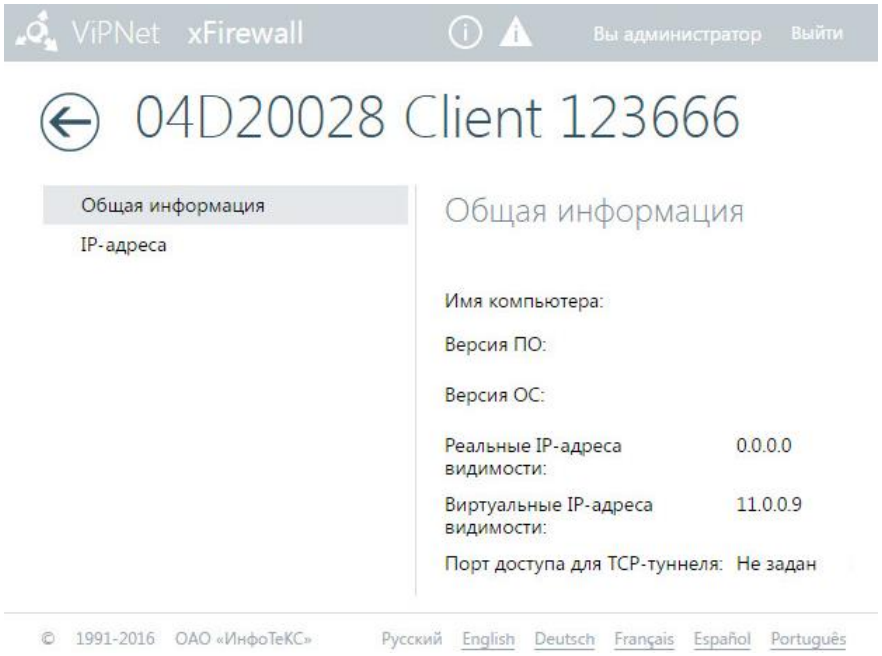

Рисунок 23. Просмотр информации о сетевом узле ViPNet

Проверка соединения с сетевым узлом ViPNet

Вы можете проверить соединение с сетевым узлом ViPNet: например, если сеанс управления с этого узла был прерван, и вы хотите выяснить причину неполадки. Для этого выполните следующие действия:

1. Перейдите на страницу **Управляющие соединения** > **Узлы ViPNet**.
2. В списке выберите узел, соединение с которым вы хотите проверить.

Совет. Чтобы быстро найти нужный узел в списке, воспользуйтесь полем поиска на панели инструментов.

---

3. На панели инструментов нажмите кнопку **Проверить соединение**. Если узел доступен, его имя будет выделено черным цветом и будет отображаться информация о времени последней активности пользователя этого узла.

Просмотр сведений о собственном сетевом узле ViPNet

Вы можете просмотреть сведения о собственном сетевом узле ViPNet. Для этого перейдите на страницу **Управляющие соединения** > **Мой узел**.

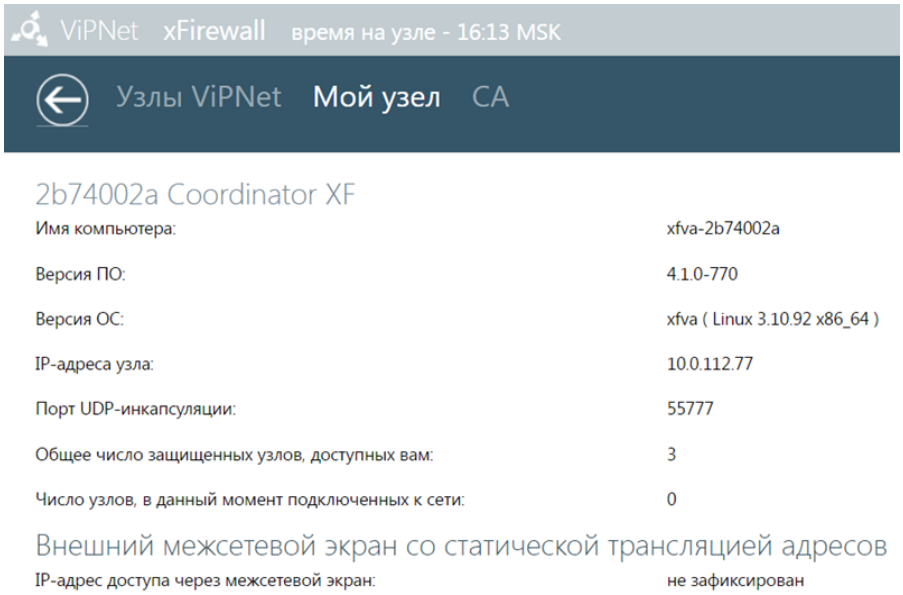

Рисунок 24. Просмотр сведений о собственном сетевом узле ViPNet

Управление сертификатами

ViPNet xFirewall позволяет использовать учетные данные пользователей, хранящиеся на LDAP-сервере (см. глоссарий, стр. 201) и выполнять аутентификацию этих пользователей через сервис Captive portal (см. глоссарий, стр. 200), встроенный в ViPNet xFirewall. Для проверки подлинности LDAP-сервера и веб-сервера Captive portal при создании защищенного канала между ViPNet xFirewall и LDAP-сервером, а также между браузером пользователя и ViPNet xFirewall, используются сертификаты (см. глоссарий, стр. 205). Для проверки факта аннулирования сертификата со стороны удостоверяющего центра (см. глоссарий, стр. 206) используются списки аннулированных сертификатов CRL (см. глоссарий, стр. 206). Пример использования сертификатов и CRL при аутентификации пользователей через сервис Captive portal приведен в разделе (см. Пример настройки взаимодействия с LDAP-сервером на стр. 115) настоящего документа.

В ViPNet xFirewall вы можете:

- импортировать сертификаты и CRL в кодировке Base64 (см. глоссарий, стр. 200), подписанные открытым ключом RSA;
- создавать запросы на сертификат в формате PKCS#12 (см. глоссарий, стр. 202);
- удалять сертификаты, закрытые ключи, CLR и запросы на сертификаты;
- просматривать списки сертификатов, закрытых ключей, CLR и запросов на сертификаты;
- просматривать содержимое сертификатов и CLR.

Настройка сертификатов

Настройка сертификатов в ViPNet xFirewall выполняется в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

Чтобы перейти к настройке, выполните следующие действия:

1. На начальной странице веб-интерфейса щелкните плитку **Управляющие соединения.**
2. Перейдите на страницу **CA**.
3. В открывшемся окне перейдите на вкладку **Установленные сертификаты**.

Импорт сертификата

Вы можете импортировать существующий сертификат. Для импорта сертификата выполните следующие действия:

1. Нажмите кнопку **Импорт сертификата**.
2. В открывшемся окне вставьте текст сертификата или нажмите кнопку **Загрузить файл** и выберите файл сертификата.

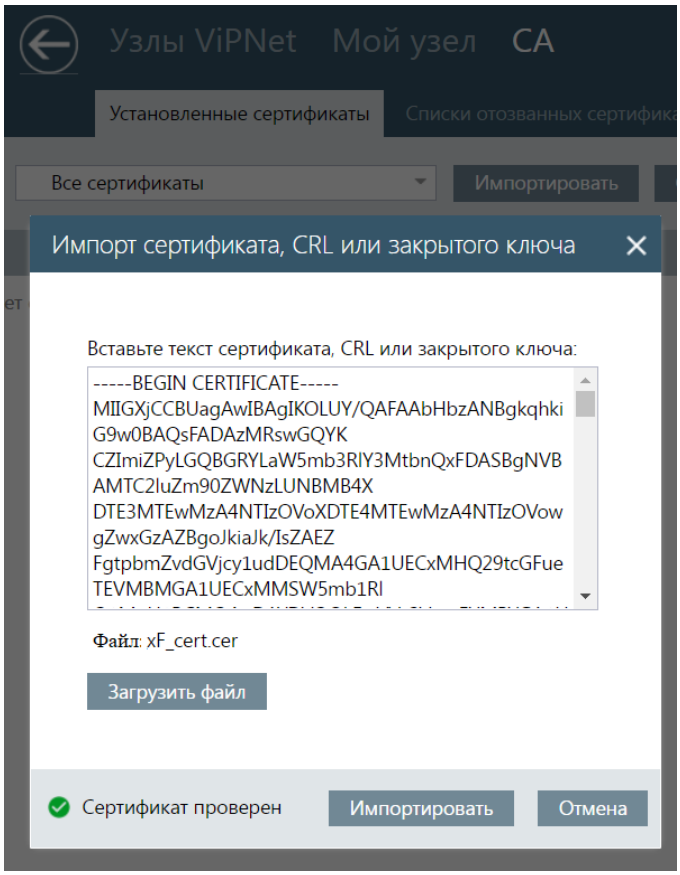

Рисунок 25. Импорт сертификата

Примечание. При настройке ViPNet xFirewall с помощью веб-интерфейса вы можете импортировать только сертификаты в кодировке Base64 (см. глоссарий, стр. 200), подписанные открытым ключом RSA.

Если после загрузки сертификата отображается сообщение **Сертификат проверен**, то вы можете навести указатель мыши на окно с текстом сертификата и получить подсказку с данными о сертификате. Если сертификат имеет неправильный формат, вы увидите сообщение **Неправильный формат сертификата, CRL или закрытого ключа**.

3 Нажмите кнопку **Импортировать**.

Импортированный сертификат появится в списке установленных сертификатов.

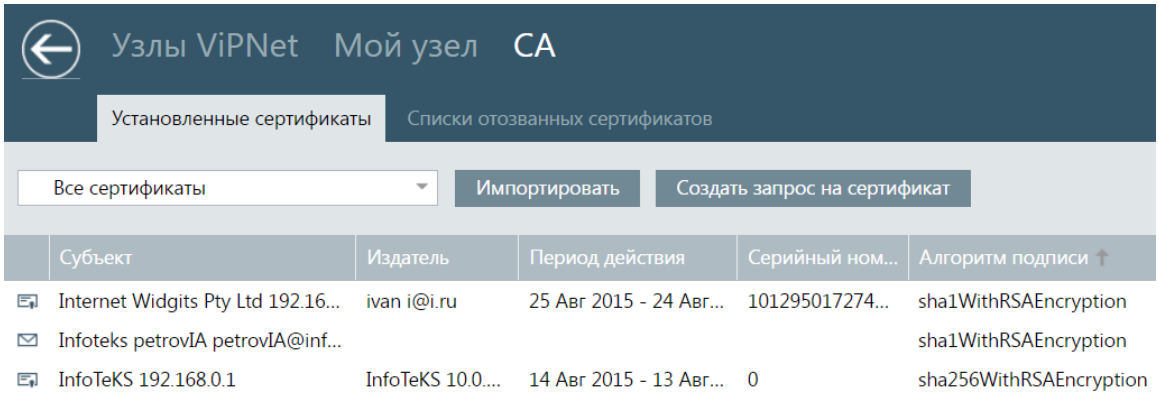

Рисунок 26. Список установленных сертификатов

Отображение списка сертификатов

Вы можете выбрать тип сертификата для отображения в списке установленных сертификатов. Для этого выберите из списка в левой части экрана один из возможных типов:

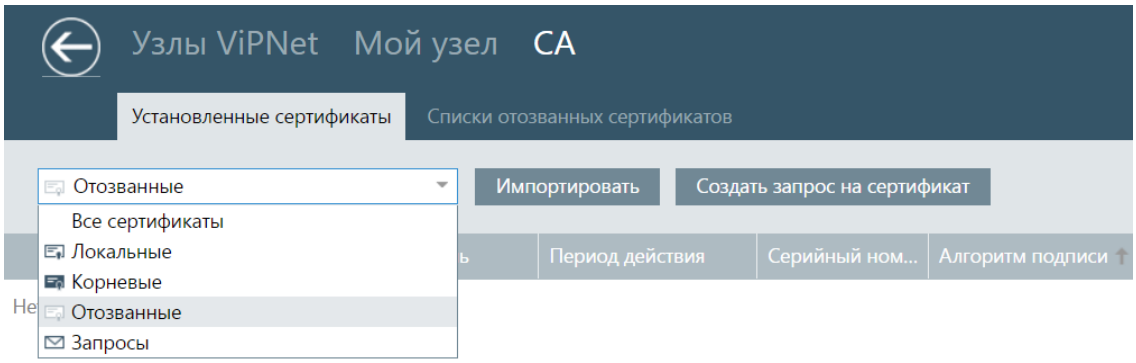

Рисунок 27. Выбор типа отображаемых сертификатов

В списке сертификатов будут показаны сертификаты выбранного типа.

Создание запроса на сертификат

Вы можете создать запрос на выпуск сертификата. Для этого выполните следующие действия:

1 Нажмите кнопку **Создать запрос на сертификат** и в открывшемся окне укажите параметры сертификата.

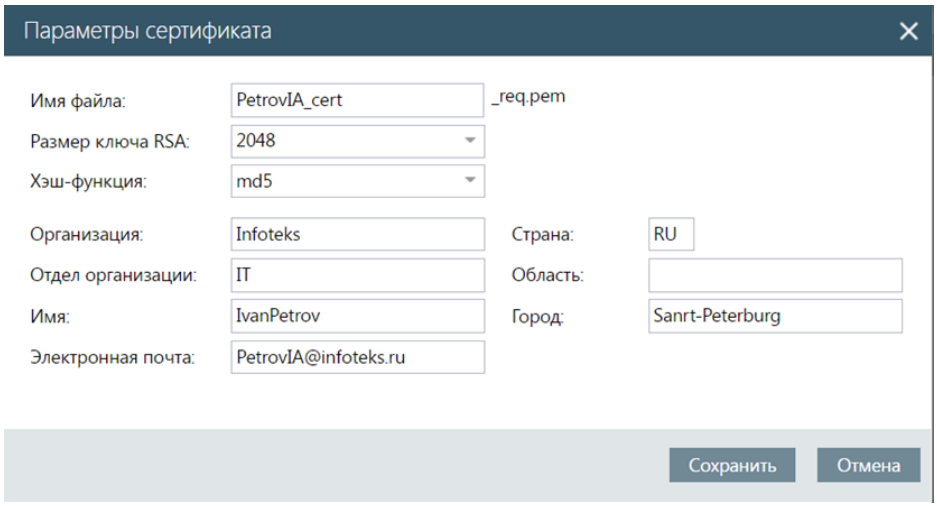

Рисунок 28. Создание запроса на сертификат

2 Нажмите кнопку **Сохранить**.

Созданный запрос на сертификат будет отображен в списке сертификатов.

3 Наведите указатель мыши на созданный запрос и нажмите кнопку . Файл запроса на сертификат будет сохранен в папке, которая используется браузером для загрузки файлов, например `c:\users\user_profile\download`. Передайте файл запроса на сертификат в удостоверяющий центр (см. глоссарий, стр. 206) для выпуска сертификата.

Удаление сертификата или запроса на сертификат

Вы можете удалить установленный сертификат или созданный запрос на сертификат. Для этого выполните следующие действия:

1 Наведите указатель на строку с требуемым сертификатом или запросом и нажмите кнопку ;

2 Если вы удаляете сертификат, то в открывшемся окне установите или снимите флажок **Удалить и связанный закрытый ключ**;

3 Нажмите кнопку **OK**.

Настройка списков CRL

Чтобы перейти к настройке списка отозванных сертификатов (CRL), выполните следующие действия:

1 На начальной странице веб-интерфейса щелкните плитку **Управляющие соединения.**

2 Перейдите на страницу **CA**.

3 В открывшемся окне перейдите на вкладку **Списки отозванных сертификатов**.

Импорт списка отозванных сертификатов

Вы можете импортировать в ViPNet xFirewall список отозванных сертификатов. Для импорта списка отозванных сертификатов выполните следующие действия:

1. Нажмите кнопку **Импортировать**.
2. В открывшемся окне вставьте через буфер обмена текст списка отозванных сертификатов или нажмите кнопку **Загрузить файл** и выберите файл списка.
3. Нажмите кнопку **Импортировать**.

Импортированный CRL будет отображен на странице **Списки отозванных сертификатов**.

Рисунок 29. Списки отозванных сертификатов

Примечание. Если у CLR истек срок действия, он будет отмечен значком .

Просмотр отозванных сертификатов локального хранилища ViPNet xFirewall

Для просмотра отозванных сертификатов локального хранилища ViPNet xFirewall выполните следующие действия:

1. Перейдите на вкладку **Установленные сертификаты**.
2. Выберите из списка в левой части экрана тип отображения сертификатов **Отозванные**.

На странице браузера будет отображен список отозванных сертификатов, находящихся в локальном хранилище ViPNet xFirewall.

Удаление списка отозванных сертификатов

Вы можете удалить список отозванных сертификатов. Для этого наведите указатель мыши на строку с требуемым CRL и нажмите на кнопку . Для подтверждения удаления нажмите кнопку **OK**.

4

Настройка межсетевого экрана

Настройка сетевых фильтров 58

Настройка правил трансляции адресов 87

Настройка параметров прокси-сервера 101

Настройка взаимодействия с Active Directory 111

Настройка взаимодействия с LDAP-сервером 114

Просмотр списка пользователей 121

Настройка сетевых фильтров

Основные принципы фильтрации трафика

ViPNet xFirewall выполняет фильтрацию следующих типов трафика:

- Локальный трафик. Под локальным трафиком понимается входящий или исходящий трафик ViPNet xFirewall (то есть когда ViPNet xFirewall логически является отправителем или получателем IP-пакетов).
- Широковещательный трафик. Под широковещательным трафиком имеется в виду передача ViPNet xFirewall IP-пакетов, у которых IP-адрес или MAC-адрес назначения является широковещательным адресом (то есть когда пакеты передаются всем узлам определенного сегмента сети).
- Транзитный трафик. Под транзитным трафиком имеется в виду трафик, для которого ViPNet xFirewall логически не является ни отправителем, ни получателем IP-пакетов, такие пакеты следуют через него на другие узлы. Этот тип трафика является основным для ViPNet xFirewall, поэтому ниже подробнее рассматриваются особенности фильтрации транзитного трафика.

Внимание! Для корректной обработки транзитного трафика через ViPNet xFirewall должны проходить как входящие, так и соответствующие исходящие IP-пакеты. Если входящий или исходящий трафик проходит по альтернативному маршруту в обход ViPNet xFirewall, корректная обработка не гарантируется.

Чтобы правильно настроить сетевые фильтры (см. глоссарий, стр. 206), ознакомьтесь со схемой фильтрации транзитного трафика в ViPNet xFirewall (см. Рисунок 30 на стр. 60). В ViPNet xFirewall фильтрация транзитного трафика происходит в следующем порядке:

1. Все IP-пакеты, поступающие на сетевые интерфейсы ViPNet xFirewall, проверяются на фрагментацию, если включена соответствующая настройка межсетевого экрана (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Тонкая настройка межсетевого экрана»). Если IP-пакет фрагментирован, то он блокируется, в противном случае пропускается.
2. Затем для IP-пакета выполняется трансляция адреса назначения (Destination NAT) (см. Трансляция адреса назначения на стр. 88), если создано соответствующее правило трансляции адресов.
3. После трансляции адреса назначения IP-пакет проходит проверку встроенным средством антиспуфинга, если оно включено (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Настройка антиспуфинга»).
4. В случае успешной проверки встроенным средством антиспуфинга для IP-пакета возможны следующие варианты дальнейшего пути фильтрации:
   - Если IP-пакет относится к протоколу HTTP (транспортный протокол TCP, порт 80) и прокси-сервер включен:

- IP-пакет проходит контент-фильтрацию содержимого трафика (см. Пример настройки фильтрации трафика на стр. 106).
- В случае успешной проверки IP-пакет проходит антивирусную проверку, если она включена.
- В случае успешной антивирусной проверки IP-пакет пропускается.

- Если IP-пакет не относится к протоколу HTTP или прокси-сервер выключен:
  - IP-пакет проходит классификацию DPI на предмет соответствия приложению, прикладному протоколу или группе приложений.
  - Если IP-пакет относится к установленному соединению, которое было разрешено, и при этом классификация DPI для IP-пакета не изменилась, то для IP-пакета выполняется трансляция адреса источника (Source NAT) (см. Трансляция адреса источника на стр. 89), если создано соответствующее правило трансляции адресов. Затем IP-пакет пропускается.
  - Если IP-пакет не относится к установленному соединению, которое было разрешено, или классификация DPI для IP-пакета изменилась, то IP-пакет проходит проверку сетевыми фильтрами (см. Общие сведения о сетевых фильтрах на стр. 60).
  - В случае успешной проверки сетевыми фильтрами для IP-пакета выполняется трансляция адреса источника (Source NAT) (см. Трансляция адреса источника на стр. 89), если создано соответствующее правило трансляции адресов. Затем IP-пакет пропускается.

При этом в работе сетевых фильтров необходимо учитывать следующие особенности:

- Все входящие и исходящие открытые и зашифрованные IP-пакеты проверяются на соответствие условиям сетевых фильтров в порядке убывания приоритета этих фильтров (см. Рисунок 31 на стр. 61).
- Если IP-пакет соответствует условию одного из фильтров, то он пропускается или блокируется этим фильтром. При этом фильтры с более низким приоритетом не применяются.
- Если IP-пакет был пропущен одним из фильтров, то ответные IP-пакеты в рамках текущего соединения будут пропускаться автоматически.
- Если IP-пакет не был обработан ни одним из фильтров, то он блокируется фильтром по умолчанию.

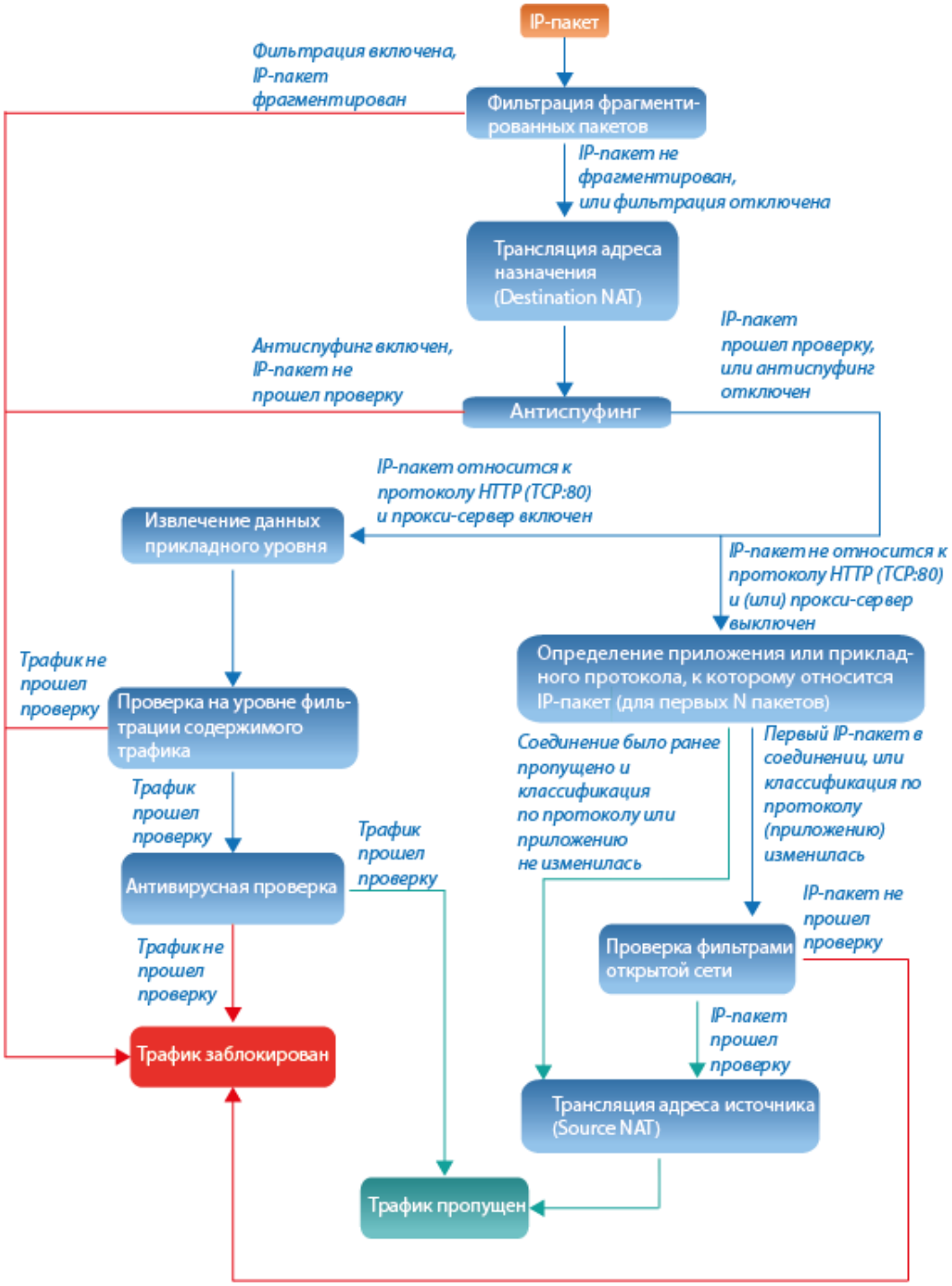

Рисунок 30. Схема фильтрации трафика ViPNet xFirewall

Общие сведения о сетевых фильтрах

Для ViPNet xFirewall весь проходящий через него трафик (за исключением трафика управляющих соединений), фильтруется как открытый. Поэтому сетевые фильтры ViPNet xFirewall работают как фильтры для открытого трафика. К ним относятся:

- Служебные фильтры, включающие:
  - Фильтры, блокирующие входящий и исходящий IP-трафик по TCP- и UDP-протоколам и служебным портам. Передача IP-трафика по указанным протоколам и портам разрешена только службам ViPNet.
  - Фильтры, разрешающие IP-трафик, который используется для проверки работоспособности сетевых интерфейсов в режиме кластера горячего резервирования.
- Фильтры, поступившие в составе политик безопасности. Политика безопасности представляет собой набор параметров, регулирующих безопасность сетевого узла. Она формируется администратором сети ViPNet в программе ViPNet Policy Manager (см. глоссарий, стр. 202), может включать сетевые фильтры и правила трансляции адресов и рассылается на узлы с помощью транспортного модуля MFTP. При получении политики безопасности из программы ViPNet Policy Manager она немедленно применяется на узле.
- Предустановленные фильтры и фильтры, заданные пользователем. Предустановленные фильтры разрешают только некоторые типы IP-пакетов. Для работы с какими-либо дополнительными сервисами пользователю необходимо создать соответствующие фильтры.
- Блокирующий фильтр по умолчанию.

Служебные фильтры создаются в ViPNet xFirewall автоматически, имеют самый высокий приоритет, то есть применяются в первую очередь, и недоступны для редактирования. После служебных фильтров применяются фильтры, поступившие в составе политик безопасности из программы ViPNet Policy Manager. Эти фильтры также недоступны для редактирования. Затем применяются предустановленные фильтры и фильтры, заданные пользователем. Их можно изменять и удалять. Наименьший приоритет имеет блокирующий фильтр по умолчанию, который нельзя ни изменить, ни удалить.

Последовательность применения сетевых фильтров в порядке убывания приоритета представлена ниже.

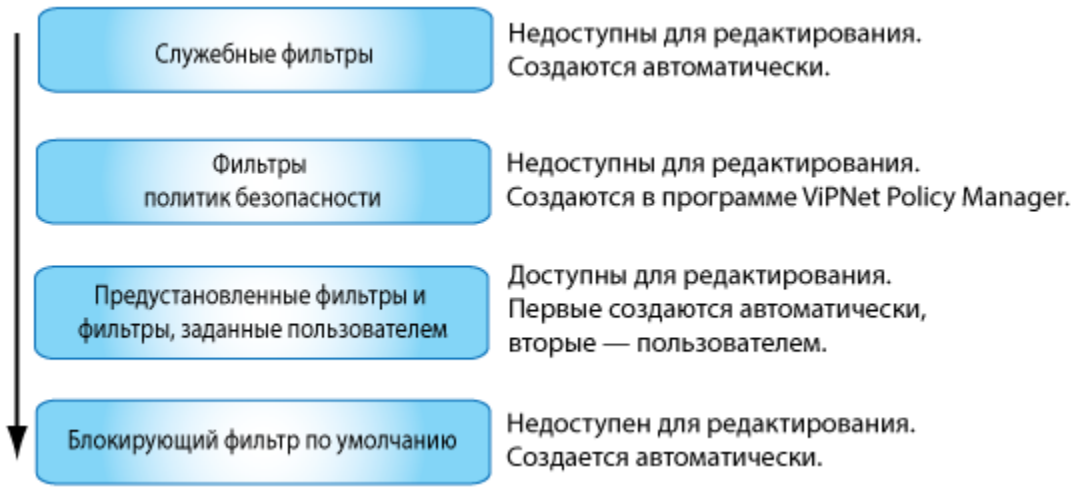

Рисунок 31. Последовательность применения сетевых фильтров

Сетевые фильтры могут включать в себя следующие параметры:

- условие — адрес отправителя и получателя IP-пакетов, на которые действует фильтр, и протоколы, используемые для передачи этих IP-пакетов (например, TCP, UDP, ICMP);
- расписание применения фильтра — ежедневно, еженедельно или по календарю;
- действие, применяемое к IP-пакетам — пропускать или блокировать IP-пакеты, соответствующие условию фильтра.

О том, как просмотреть фильтры, заданные на узле, создать или изменить фильтры на узле, см. в соответствующем разделе ниже.

Группы объектов

Группы объектов позволяют упростить процессы создания и изменения сетевых фильтров и правил трансляции сетевых адресов (см. глоссарий, стр. 206) в ViPNet xFirewall. Каждая группа объединяет несколько объектов одного типа (например, IP-адреса или сетевые интерфейсы). Группы можно указывать при задании параметров фильтра или правила трансляции вместо перечисления отдельных объектов.

В зависимости от типа объединяемых объектов различаются следующие группы:

- Группа узлов ViPNet — содержит любую комбинацию сетевых узлов ViPNet, используется в фильтрах защиты канал управления.
- Группа IP-адресов — содержит любую комбинацию IP-адресов, диапазонов IP-адресов и DNS-имен, используется в локальных и транзитных фильтрах открытой сети, и правилах трансляции адресов.
- Группа сетевых интерфейсов — содержит любую комбинацию сетевых интерфейсов, используется в локальных и транзитных фильтрах открытой сети.
- Группа протоколов — содержит любую комбинацию сетевых протоколов и портов, используется в локальных и транзитных фильтрах открытой сети и правилах трансляции адресов.
- Группа расписания — содержит любую комбинацию параметров, определяющих время действия фильтра, используется в локальных и транзитных фильтрах открытой сети.

Каждая группа объектов относится к одному из следующих видов:

- Системные группы объектов (на стр. 63) — настроенные по умолчанию группы с фиксированными именами, которые могут использоваться для задания адресов отправителей и получателей IP-пакетов в фильтрах и правилах трансляции адресов, а также при создании пользовательских групп объектов. Такие группы объектов не отображаются в списках групп (см. Просмотр групп объектов на стр. 64), их нельзя ни изменить, ни удалить.
- Группы объектов из программы ViPNet Policy Manager (см. глоссарий, стр. 202) — группы, получаемые в составе политик безопасности, и используемые в соответствующих фильтрах. Такие группы нельзя ни удалять, ни изменять, ни использовать для задания параметров пользовательских фильтров и групп объектов.

- Пользовательские группы объектов — группы, создаваемые пользователем на узле, а также несколько групп, настроенных по умолчанию (см. Пользовательские группы объектов по умолчанию на стр. 64). Такие группы можно использовать для задания параметров фильтров и правил трансляции, а также при создании других пользовательских групп объектов. При необходимости их можно удалить.

Системные группы объектов

В таблице ниже описаны доступные системные группы объектов.

Таблица 6. Системные группы объектов

Имя группы объектов в веб-интерфейсе (в командном интерпретаторе ViPNet)	**Описание**
Широковещательные адреса (`broadcast`)	Все широковещательные адреса. Можно использовать в локальных фильтрах открытой сети для идентификации широковещательных адресов получателей. Использование других адресов совместно с этой группой недопустимо.
Мой узел (`local`)	Собственный узел. Можно использовать в локальных фильтрах открытой сети для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла. Использование других адресов совместно с этой группой недопустимо.
Другие узлы (`remote`)	Другие узлы ViPNet (любые, кроме собственного). Можно использовать в локальных фильтрах открытой сети для задания источника входящих IP-пакетов или назначения исходящих IP-пакетов узла.
Групповые адреса (`multicast`)	Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255). Можно использовать в локальных фильтрах открытой сети для задания назначения исходящих IP-пакетов узла. Использование других адресов совместно с этой группой недопустимо.
Все объекты (`any`)	Все объекты группы конкретного типа. Можно использовать только при создании других групп объектов.

Пользовательские группы объектов по умолчанию

По умолчанию в ViPNet xFirewall настроены следующие пользовательские группы объектов:

- Группы IP-адресов:
  - `PrivateNetworkIP` (частные IP-адреса) — включает IP-адреса локальных сетей: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16.
  - `InternetIP` (публичные IP-адреса) — включает все IP-адреса, за исключением частных IP-адресов.
  - `HttpProxyUsers` — включает IP-адреса локальных сетей, которым разрешен доступ к прокси-серверу.

  

  Внимание! Группа объектов `HttpProxyUsers` автоматически создается при первом запуске прокси-сервера.

- Группы протоколов, которые наиболее часто используются при создании сетевых фильтров. Они перечислены в приложении (см. Пользовательские группы протоколов по умолчанию на стр. 173).
- Группы расписаний:
  - `Workdays` (рабочие дни) — включает рабочие дни недели (с понедельника по пятницу).
  - `Weekends` (выходные дни) — включает выходные дни недели (субботу и воскресенье).

Просмотр групп объектов

Чтобы просмотреть пользовательские группы объектов и группы объектов, полученные из программы ViPNet Policy Manager, выполните следующие действия:

1. На начальной странице веб-интерфейса щелкните плитку **Межсетевой экран** и перейдите в раздел **Группы объектов**.
2. На странице **Группы объектов** выберите вкладку групп объектов нужного типа. В результате отобразится список, содержащий имена групп объектов и информацию об объектах, входящих и не входящих в группу.

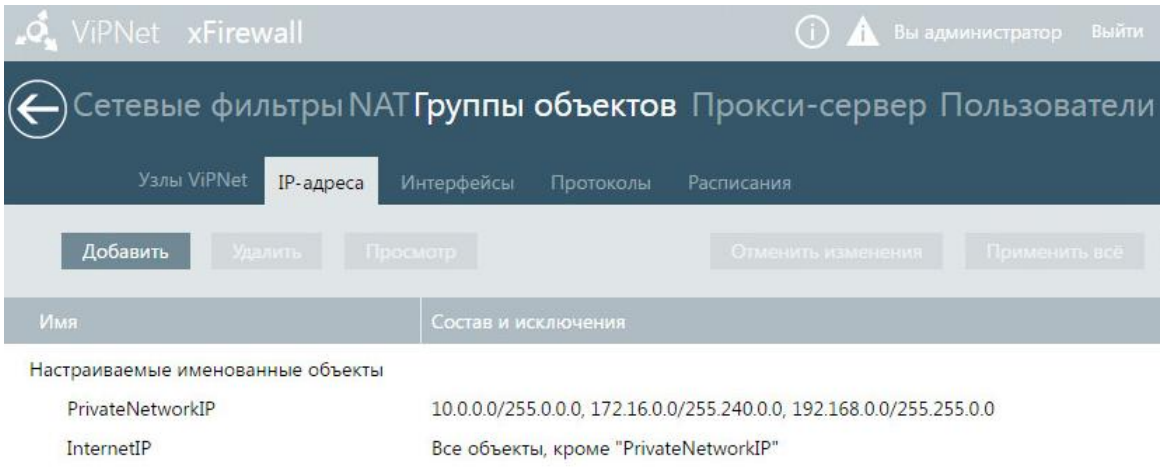

Рисунок 32. Просмотр групп IP-адресов

3 Для просмотра подробной информации об использовании группы объектов дважды щелкните ее в списке и на открывшейся странице нажмите кнопку **Просмотр**.

Создание и изменение группы объектов

Чтобы создать или изменить группу объектов, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 На странице **Межсетевой экран** > **Группы объектов** выберите вкладку групп объектов нужного типа.

3 Выполните одно из действий:

- Чтобы создать группу объектов, на панели инструментов нажмите кнопку **Добавить**.
- Чтобы изменить группу объектов, дважды щелкните ее в списке групп.

Примечание. Чтобы просмотреть, в каких сетевых фильтрах, правилах трансляции адресов и группах объектов используется группа, которую вы хотите изменить, нажмите кнопку **Показать**.

---

4 На странице создания или изменения группы задайте следующие параметры:

4.1 В соответствующем поле задайте имя группы.

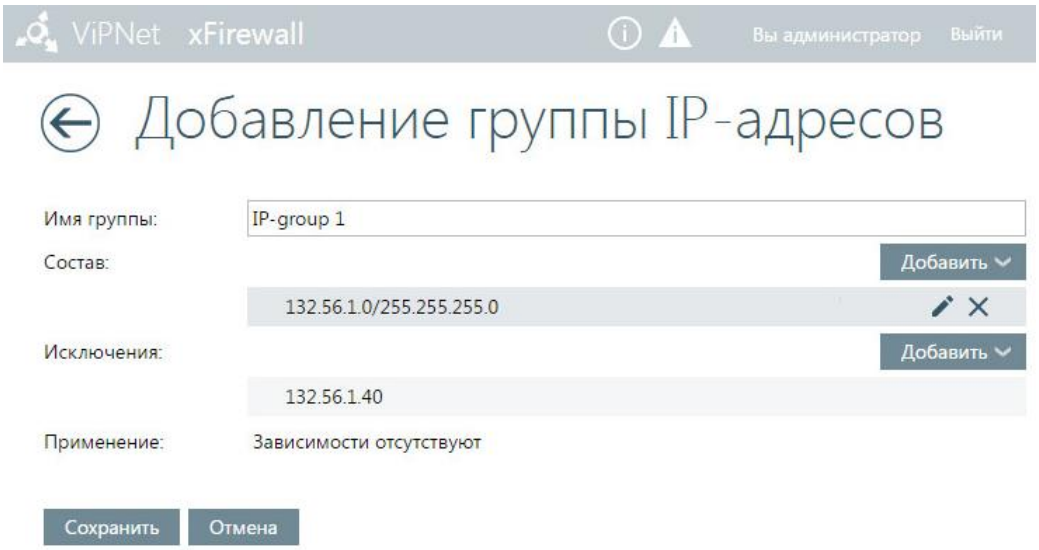

Рисунок 33. Добавление группы IP-адресов

4.2 В разделах **Состав** и **Исключения** укажите объекты, входящие и не входящие в группу соответственно. Для этого в зависимости от типа объектов воспользуйтесь рекомендациями соответствующего раздела:

- Группа сетевых узлов ViPNet (на стр. 66).
- Группа IP-адресов (на стр. 68).
- Группа сетевых интерфейсов (на стр. 69).
- Группа протоколов (на стр. 71).
- Группа расписаний (на стр. 72).

4.3 Нажмите кнопку **Сохранить**.

Примечание. Чтобы удалить объект, который вы ранее добавили в группу, в строке этого объекта нажмите кнопку ✕.

---

5 Чтобы изменения вступили в силу, на странице **Группы объектов** нажмите кнопку **Применить все**.

Группа сетевых узлов ViPNet

При создании или изменении группы сетевых узлов ViPNet вы можете добавить или исключить следующие объекты:

- сетевые узлы ViPNet, с которыми связан узел ViPNet xFirewall;
- сеть ViPNet, с которой связана ваша сеть ViPNet;
- ранее созданную группу сетевых узлов ViPNet;

- системные группы объектов: **Все координаторы**, **Все клиенты**, **Все объекты**.

Рисунок 34: Добавление сетевого узла ViPNet в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) один или несколько сетевых узлов, выберите пункт **Сетевой узел** и установите флажки рядом с нужными узлами. Первым в этом списке отображается собственный узел.
- Если вы хотите добавить (исключить) несколько сетевых узлов с незначительно отличающимися именами, выберите пункт **Шаблон имени сетевых узлов** и укажите маску имен узлов, используя символ «?» для замены одного символа, и символ «*» для замены нескольких символов.
- Если вы хотите добавить (исключить) все узлы определенной сети ViPNet, выберите пункт **Номер защищенной сети** и укажите номер этой сети.
- Если вы хотите добавить (исключить) ранее созданную группу сетевых узлов ViPNet, выберите пункт **Группа узлов ViPNet** и щелкните нужную группу. Чтобы добавить несколько групп сетевых узлов, удерживайте клавишу **Ctrl** и по очереди щелкните нужные группы.
- Если вы хотите добавить (исключить) системную группу объектов, выберите соответствующую группу.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров защиты канала управления (см. Создание и изменение сетевого фильтра на стр. 74).

Группа IP-адресов

При создании или изменении группы IP-адресов вы можете добавить или исключить следующие объекты:

- IP-адреса или диапазоны IP-адресов;
- DNS-имена;
- ранее созданные группы IP-адресов;
- системная группа: **Все объекты**.

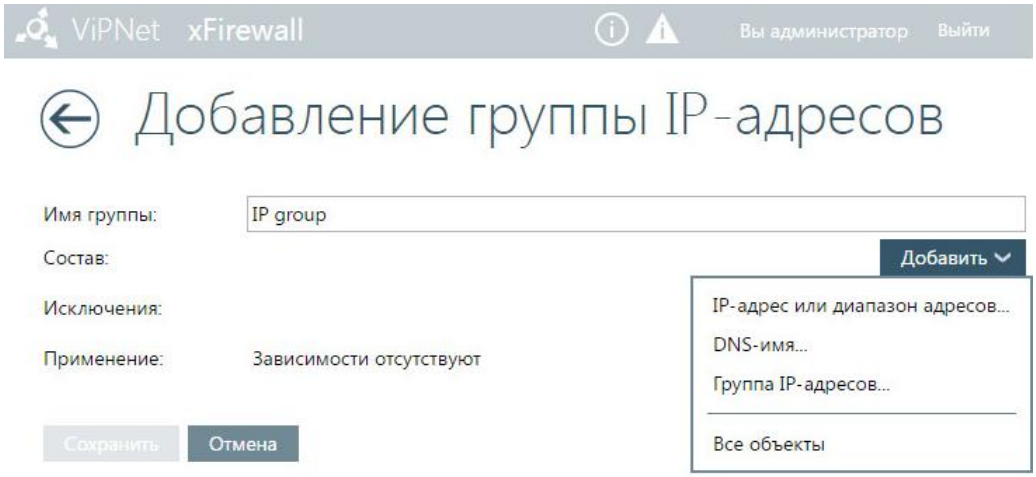

Рисунок 35: Добавление IP-адресов в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) один или несколько IP-адресов либо диапазонов IP-адресов, выберите пункт **IP-адрес или диапазон адресов** и выполните одно из действий:
  - для задания одного IP-адреса в списке выберите соответствующий тип адреса и укажите этот IP-адрес;
  - для задания IP-адресов подсети в списке выберите соответствующий тип адреса и укажите адрес и маску этой подсети (по умолчанию — `255.255.255.0/24`);
  - для задания диапазона IP-адресов в списке выберите соответствующий тип адреса и укажите начальный и конечный IP-адреса этого диапазона.

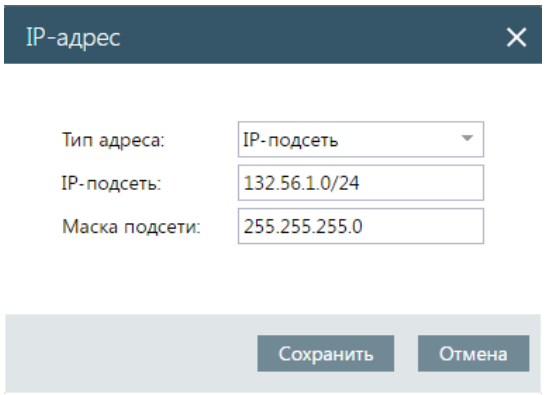

Рисунок 36. Добавление IP-адреса подсети

- Если вы хотите добавить (исключить) DNS-имя, выберите пункт **DNS-имя** и укажите DNS-имя.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп IP-адресов, выберите пункт **Группы IP-адресов** и установите флажки рядом с нужными группами. При необходимости вы можете изменить выбранную группу IP-адресов с помощью кнопки **Редактировать** (см. Создание и изменение группы объектов на стр. 65).
- Если вы хотите добавить (исключить) системную группу объектов, выберите соответствующую группу.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать узлы отправителей и получателей IP-пакетов при создании и изменении фильтров открытой сети (см. Создание и изменение сетевого фильтра на стр. 74) и правил трансляции адресов.

Группа сетевых интерфейсов

При создании или изменении группы сетевых интерфейсов вы можете добавить или исключить следующие объекты:

- сетевые интерфейсы собственного узла;
- IP-адрес или диапазон IP-адресов сетевых интерфейсов узлов;
- ранее созданную группу сетевых интерфейсов;
- системную группу объектов **Все объекты**.

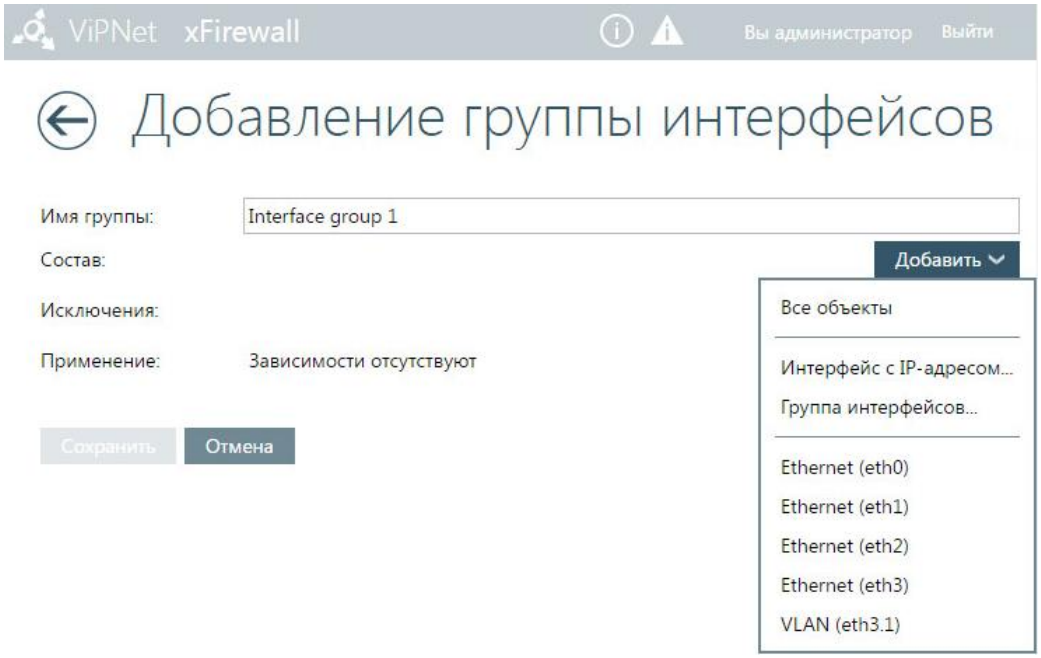

Рисунок 37. Добавление сетевых интерфейсов в группу

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) один или несколько интерфейсов собственного узла, выберите имя этого интерфейса (`Ethernet (eth0)`, `Ethernet (eth1)` и так далее).
- Если вы хотите добавить (исключить) IP-адрес или диапазон IP-адресов интерфейсов, выберите пункт **Интерфейс с IP-адресом** и выполните одно из действий:
  - для задания одного IP-адреса в списке выберите соответствующий тип адреса и укажите этот IP-адрес.
  - для задания IP-адресов подсети в списке выберите соответствующий тип адреса и укажите адрес и маску этой подсети (по умолчанию — `255.255.255.0/24`).
  - для задания диапазона IP-адресов в списке выберите соответствующий тип адреса и укажите начальный и конечный IP-адреса этого диапазона.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп сетевых интерфейсов, выберите пункт **Группа интерфейсов** и установите флажки рядом с нужными группами. При необходимости вы можете изменить выбранную группу сетевых интерфейсов с помощью кнопки **Редактировать** (см. Создание и изменение группы объектов на стр. 65).
- Если вы хотите добавить (исключить) системную группу объектов **Все объекты**, выберите ее.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать сетевые интерфейсы при создании и изменении фильтров открытой сети (см. Создание и изменение сетевого фильтра на стр. 74) и правил трансляции адресов.

Группа протоколов

При создании и изменении группы протоколов вы можете добавить или исключить следующие объекты:

- протокол TCP, UDP, ICMP или другой протокол;
- ранее созданную группу протоколов;
- системную группу **Все объекты**.

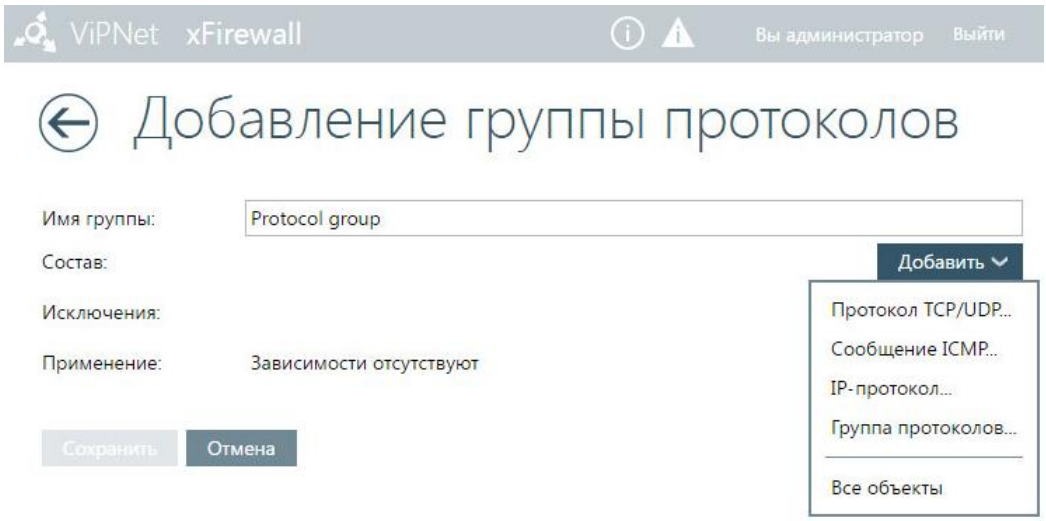

Рисунок 38. Добавление группы протоколов

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите добавить (исключить) протокол TCP или UDP, выберите пункт **Протокол TCP/UDP** и установите переключатель **Протоколы** в нужное положение. По умолчанию для протокола выбраны все порты источника и назначения (**Все порты**). Для задания одного или нескольких портов источника или назначения выполните одно из действий:
  - для задания номера одного порта в соответствующем списке выберите пункт **Номер порта**, затем выберите один из стандартных номеров портов в списке или укажите произвольный номер порта в диапазоне от 0 до 65535;
  - для задания диапазона портов в соответствующем списке выберите пункт **Диапазон портов** и укажите начальный и конечный номера портов в диапазоне от 0 до 65535.

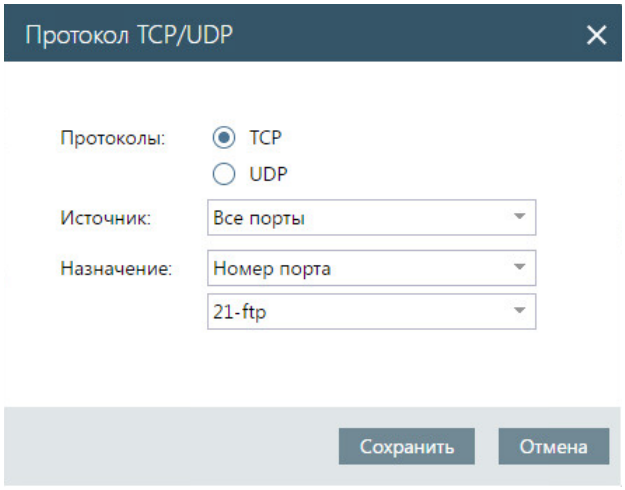

Рисунок 39. Добавление протокола в группу

- Если вы хотите добавить (исключить) протокол ICMP, выберите пункт **Сообщение ICMP**, затем выберите нужный тип ICMP-сообщений в списке и при необходимости их код.
- Если вы хотите добавить (исключить) другой протокол, выберите пункт **Протокол IP**, затем выберите один из протоколов в списке либо введите его номер. Для добавления (исключения) всех протоколов, выберите пункт **All**.
- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп проколов, выберите пункт **Группа протоколов** и установите флажки рядом с нужными группами. При необходимости вы можете изменить выбранную группу протоколов с помощью кнопки **Редактировать** (см. Создание и изменение группы объектов на стр. 65).
- Если вы хотите добавить (исключить) системную группу **Все объекты**, выберите ее.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать протоколы при создании и изменении сетевых фильтров (см. Создание и изменение сетевого фильтра на стр. 74) и правил трансляции адресов.

Группа расписаний

При создании или изменении группы расписаний вы можете добавить или исключить следующие объекты:

- временной диапазон;
- ранее созданную группу расписаний;
- системную группу объектов **Все объекты**.

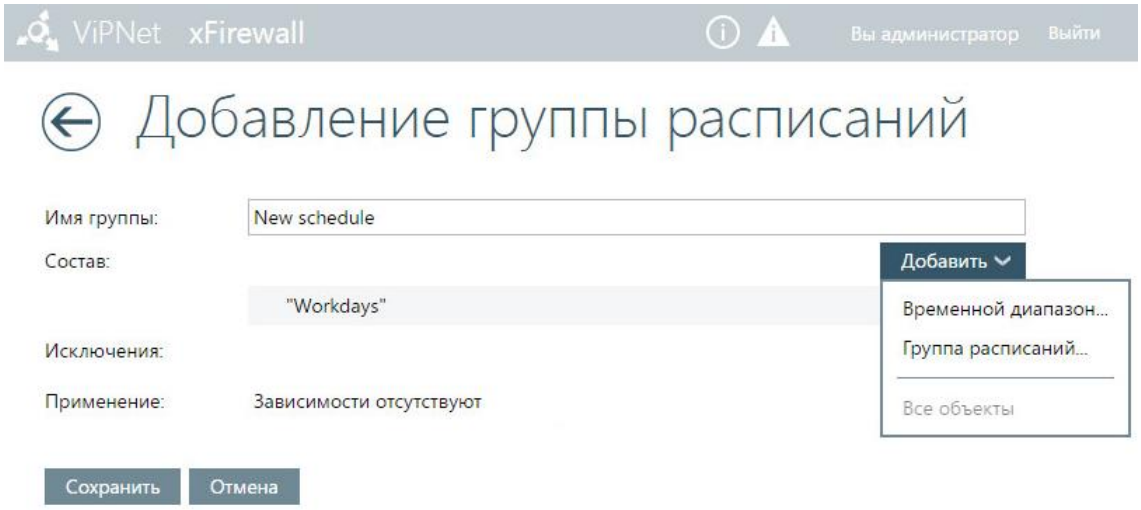

Рисунок 40. Добавление группы расписаний

Чтобы добавить (исключить) объект, на странице создания или изменения этой группы в разделе **Состав** (**Исключения**) нажмите кнопку **Добавить** и выполните следующие действия:

- Если вы хотите указать интервал времени и периодичность, когда фильтр или правило трансляции будет применяться (не будет применяться), выберите пункт **Временной диапазон** и выполните следующие действия:
  - в разделе **Время выполнения фильтра** укажите интервал времени;
  - в разделе **Период выполнения фильтра** выберите один из вариантов:
    - **Ежедневно —** чтобы фильтр или правило трансляции применялось (не применялось) каждый день. При необходимости установите флажок **в период** и укажите интервал дат, в который фильтр или правило трансляции будет применяться (не будет применяться) ежедневно;
    - **Еженедельно** — чтобы фильтр или правило трансляции применялось (не применялось) в определенные дни недели. Установите флажки рядом с нужными днями недели.

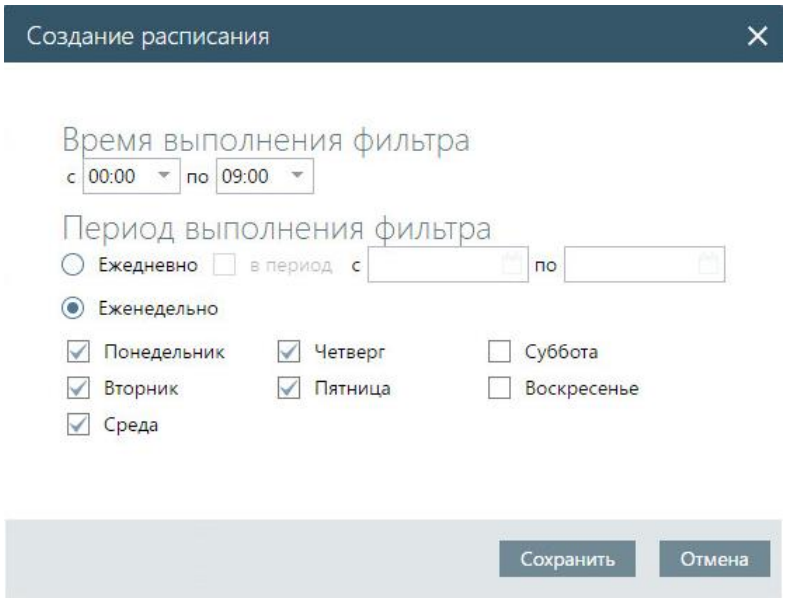

Рисунок 41. Добавление расписания в группу

- Если вы хотите добавить (исключить) одну или несколько ранее созданных групп расписаний, выберите пункт **Группа расписаний** и установите флажки рядом с нужными группами. При необходимости вы можете изменить выбранную группу расписаний с помощью кнопки **Редактировать** (см. Создание и изменение группы объектов на стр. 65).
- Если вы хотите добавить (исключить) системную группу **Все объекты**, выберите ее.

Затем нажмите кнопку **Сохранить**.

Примечание. Аналогичным образом вы можете добавлять или исключать расписания при создании и изменении сетевых фильтров (см. Создание и изменение сетевого фильтра на стр. 74) и правил трансляции адресов.

Создание и изменение сетевого фильтра

Чтобы создать или изменить сетевой фильтр на узле ViPNet xFirewall, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 На странице **Межсетевой экран** > **Сетевые фильтры** выберите вкладку сетевых фильтров нужного типа:

   - **Транзитные фильтры открытой сети**;
   - **Локальные фильтры открытой сети**;
   - **Защита канала управления**.

3 Выполните одно из действий:

- Чтобы создать фильтр, на панели инструментов нажмите кнопку **Добавить**;
- Чтобы изменить фильтр, дважды щелкните его в списке или нажмите кнопку **Редактировать**;

4 На открывшейся странице выполните следующие действия:

- В поле **Имя фильтра** укажите название фильтра;
- Установите переключатели **Состояние** и **Действие**;
- В разделе **Добавить** в соответствии с типом фильтра установите параметры:
  - для транзитных фильтров открытой сети: **Пользователей**, **Приложения**, **Протоколы**, **Источники**, **Назначения**, **Расписания**;
  - для локальных фильтров открытой сети: **Протоколы**, **Источники**, **Назначения**, **Расписания**;
  - для фильтров защиты канала управления: **Протоколы**, **Источники**, **Назначения**, **Расписания**;

  В разделе **Признаки трафика** будут сформированы значение признаков трафика по группам пользователей, приложений, протоколов, источников, назначений и расписаний в соответствии с типом фильтра. Вы можете изменить ранее введенные настройки выполнив следующие действия:
  - выберите группу и нажмите кнопку ;
  - используя кнопки и и измените значения признаков трафика;
  - нажмите кнопку и сверните группу;

Рисунок 42. Редактирование признаков трафика по группам

Примечание. Если признаки трафика не указаны , правило применяется ко всем пользователям, приложениям, протоколам, источникам и назначениям, всегда.

- Нажмите кнопку **Сохранить, Сохранить и применить** или **Отмена**.

Внимание! Кнопки сохранения заблокированы пока в сетевом фильтре имеются неподдерживаемые признаки.

В результате вновь созданный или отредактированный фильтр отобразится в списке на соответствующей вкладке страницы **Сетевые фильтры**.

По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем транспортным протоколам. Чтобы фильтр применялся к IP-пакетам, передаваемым по определенным протоколам, в соответствующем разделе укажите транспортные протоколы (см. Группа протоколов на стр. 71).

По умолчанию фильтр применяется постоянно. Чтобы фильтр применялся периодически в определенное время, в соответствующем разделе укажите расписания (см. Группа расписаний на стр. 72).

Чтобы изменить приоритет фильтра, перетащите его на нужную строку списка.

Если для того, чтобы зафиксировать внесенные изменения в сетевые фильтры любого типа вы использовали кнопку **Сохранить**, то эти изменения не вступают в силу. Вы можете задействовать их, нажав кнопку **Применить все** или отказаться от внесенных изменений (кнопка **Отменить изменения**).

Внимание! На сетевые фильтры, определяющие параметры фильтрации трафика, существуют количественные ограничения в зависимости от исполнения ViPNet xFirewall (см. "ViPNet xFirewall. Общее описание", раздел "Ограничения на количество сетевых фильтров").

Создание транзитных фильтров открытой сети

Транзитные фильтры открытой сети регулируют прохождение через ViPNet xFirewall открытых транзитных IP-пакетов (пакетов, адреса источника и назначения которых не совпадают ни с одним из адресов ViPNet xFirewall).

Примечание. Запрещающий транзитный фильтр открытой сети действует сразу после его применения. Если разрешенное ранее соединение попадает под действие запрещающего транзитного фильтра, то оно будет заблокировано сразу, не дожидаясь истечения времени жизни соединения.

Примечание. Если для компьютеров вашей сети вы настроили доступ в Интернет через прокси-сервер ViPNet xFirewall, то HTTP-трафик (трафик по протоколу TCP и порту 80) не будет обрабатываться транзитными фильтрами открытой сети. В этом случае для фильтрации HTTP-трафика используйте средства прокси-сервера (см. Пример настройки фильтрации трафика на стр. 106).

В ViPNet xFirewall для фильтрации транзитных IP-пакетов применяется технология DPI (см. глоссарий, стр. 201). Вы можете указать в качестве параметров транзитного фильтра открытой сети приложение и прикладной протокол. Кроме того, для удобства работы, приложения и поддерживаемые ими прикладные протоколы, разбиты на группы приложений, которые вы также можете указывать в качестве параметров транзитного фильтра открытой сети. Списки доступных приложений, прикладных протоколов и групп приложений обновляются вместе с модулем DPI. См. в разделах настоящего документ состав списков приложений (см. Поддерживаемые приложения на стр. 187), прикладных протоколов (см. Поддерживаемые прикладные протоколы на стр. 189) и групп приложений (см. Поддерживаемые группы приложений на стр. 190).

Чтобы создать транзитный фильтр открытой сети, выполните следующие действия:

1 Перейдите на страницу **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

2 На панели инструментов нажмите кнопку **Добавить**.

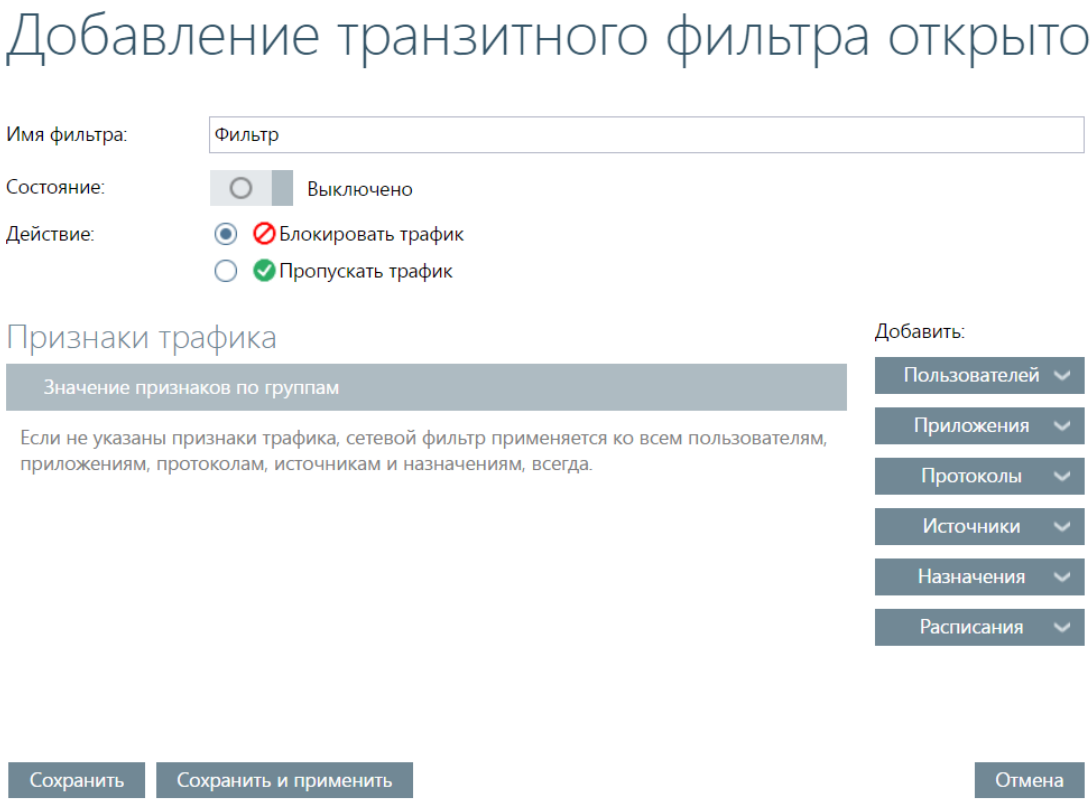

Рисунок 43. Создание транзитного фильтра открытой сети

3 На открывшейся странице в поле **Имя фильтра** укажите название фильтра.

4 Установите переключатели **Состояние** и **Действие**.

5 В разделе **Добавить** нажмите кнопку **Пользователей**, и выберите пользователя домена Active Directory или Captive portal из списка или введите имя пользователя вручную.

Примечание. Для сетевых фильтров, в которых заданы пользователи сети, существуют следующие особенности работы:

- Если IP-пакет попадает под действие сетевого фильтра, в котором задан пользователь,

то IP-адрес этого пользователя сопоставляется с IP-адресом источника или назначения IP-пакета. Сетевой фильтр сработает в том случае, если IP-адрес источника или назначения IP-пакета совпадет с IP-адресом пользователя Active Directory или Captive portal.

- В случае, когда на одном сетевом узле, подключенном к контроллеру домена Active Directory, выполнили вход несколько пользователей, то будут действовать сетевые фильтры для последнего пользователя, который вошел в домен.

6 В разделе **Добавить** нажмите кнопку **Приложения** и укажите приложение или группу приложений.

Примечание. При задании приложения в сетевом фильтре необходимо учитывать ограничения, действующие для некоторых приложений (см. Известные ограничения фильтрации по приложениям и прикладным протоколам на стр. 196). Если вы выбрали отдельное приложение или прикладной протокол, то вы не можете выбрать группу приложений и наоборот.

7 В разделе **Добавить** нажмите кнопку **Протоколы** и укажите протоколы для фильтрации. Вы можете добавить прикладной протокол, протокол TCP/UDP, сообщение ICMP, IP-протокол и группу протоколов.

Примечание. Если вы уже указали приложение, то выбор прикладных протоколов будет ограничен протоколами, которые поддерживает выбранное приложение.

8 В разделе **Добавить** нажмите кнопку **Источники** раздела **Добавить** и укажите отправителя IP-пакетов:

- Чтобы добавить один или несколько IP-адресов, выберите **IP-адрес или диапазон адресов**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Применить**.
- Чтобы добавить доменное имя, выберите пункт **DNS**. В открывшемся окне укажите доменное имя и нажмите кнопку **Применить**.
- Чтобы добавить группу IP-адресов, выберите пункт **Группа IP-адресов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Применить**.

Также вы можете установить ограничения на сетевой интерфейс, через который будут получены транзитные IP-пакеты. Для этого щелкните переключатель **Ограничения по интерфейсу** и нажмите кнопку **Добавить**. Вы можете выбрать из списка один из сетевых интерфейсов ViPNet xFirewall, указать IP-адрес интерфейса (пункт меню **Интерфейс с IP-адресом**) или добавить группу интерфейсов (пункт меню **Группа интерфейсов**).

9 В разделе **Добавить** нажмите кнопку **Назначения** и по аналогии с настройкой **Источники** добавьте получателя IP-пакетов.

10 В разделе **Добавить** нажмите кнопку **Расписания** и укажите расписание действия фильтра. Вы можете добавить временной диапазон действия расписания и выбрать группу расписаний.

11 Нажмите кнопку **Сохранить** для сохранения введенных данных настройки или **Сохранить и применить** для сохранения данных и применения фильтра.

В результате новый фильтр отобразится в списке транзитных фильтров открытой сети.

Примеры использования транзитных фильтров открытой сети

По умолчанию, после установки ViPNet xFirewall, весь открытый транзитный трафик блокируется. Вы можете создавать транзитные фильтры открытой сети и задействовать их для управления трафиком.

Настройка фильтрации трафика по пользователю

Предположим, что вам нужно настроить фильтрацию трафика для пользователя `ivanov` в локальной сети, защищенной ViPNet xFirewall таким образом, чтобы:

- разрешить отправку электронных писем только с помощью корпоративного почтового сервиса Microsoft Exchange и запретить использование сторонних почтовых сервисов;
- запретить доступ к социальным сетям;
- запретить доступ к облачным файловым сервисам.

Для настройки сетевых фильтров согласно описанным выше условиям, выполните следующие действия:

1 Войдите в веб-интерфейс в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Межсетевой экран** > **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

3 Нажмите кнопку **Добавить**. Откроется страница добавления транзитного фильтра открытой сети.

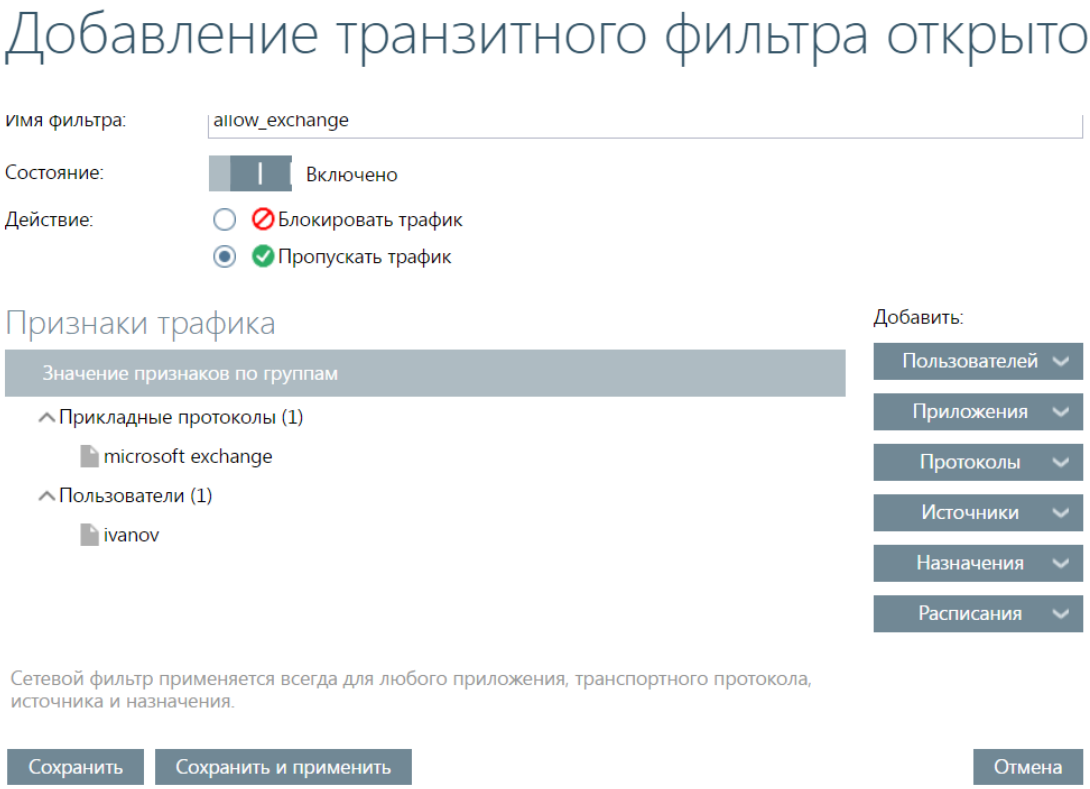

Рисунок 44. Добавление транзитного фильтра открытой сети

4 Создайте транзитный фильтр открытой сети, который будет разрешать отправку писем по протоколу Microsoft Exchange для пользователя `ivanov`:

4.1 В поле **Имя фильтра** укажите название фильтра `Allow_exchange`.

4.2 Установите переключатель **Состояние** в положение **Включено**.

4.3 Установите переключатель **Действие** в положение **Пропускать трафик**.

4.4 В разделе **Добавить** нажмите кнопку **Пользователей** и введите `ivanov`.

4.5 Нажмите кнопку **Протоколы**, далее **Прикладные протоколы** и выберите протокол **Microsoft Exchange**.

4.6 Нажмите кнопку **Сохранить и Применить**.

5 Создайте транзитный фильтр открытой сети, который будут блокировать отправку писем по протоколам SMTP и IMAP для пользователя `ivanov`:

5.1 В поле **Имя фильтра** укажите название фильтра.

5.2 Установите переключатель **Состояние** в положение **Включено**.

5.3 Установите переключатель **Действие** в положение **Блокировать трафик**.

5.4 В разделе **Добавить** нажмите кнопку **Пользователей** и введите `ivanov`.

5.5 Нажмите кнопку **Протоколы**, далее **Прикладные протоколы** и выберите протоколы **SMTP** и **IMAP**.

5.6 Нажмите кнопку **Сохранить и Применить**.

6 По аналогии создания блокирующего фильтра для протоколов SMTP и IMAP создайте транзитный фильтр открытой сети, который будет блокировать трафик приложений социальной сети Facebook и облачных файловых сервисов Dropbox и Google Drive. В качестве значения **Приложения** выберите **Facebook**, **Dropbox** и **Google Drive,** а для значения **Пользователей** укажите `ivanov`.

Настройка фильтрации трафика для работы Skype

Чтобы разрешить использование приложения Skype на компьютерах локальной сети, защищенной ViPNet xFirewall, выполните следующие действия:

1 Войдите в веб-интерфейса в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Межсетевой экран** > **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

3 Нажмите кнопку **Добавить**. Откроется страница добавления транзитного фильтра открытой сети.

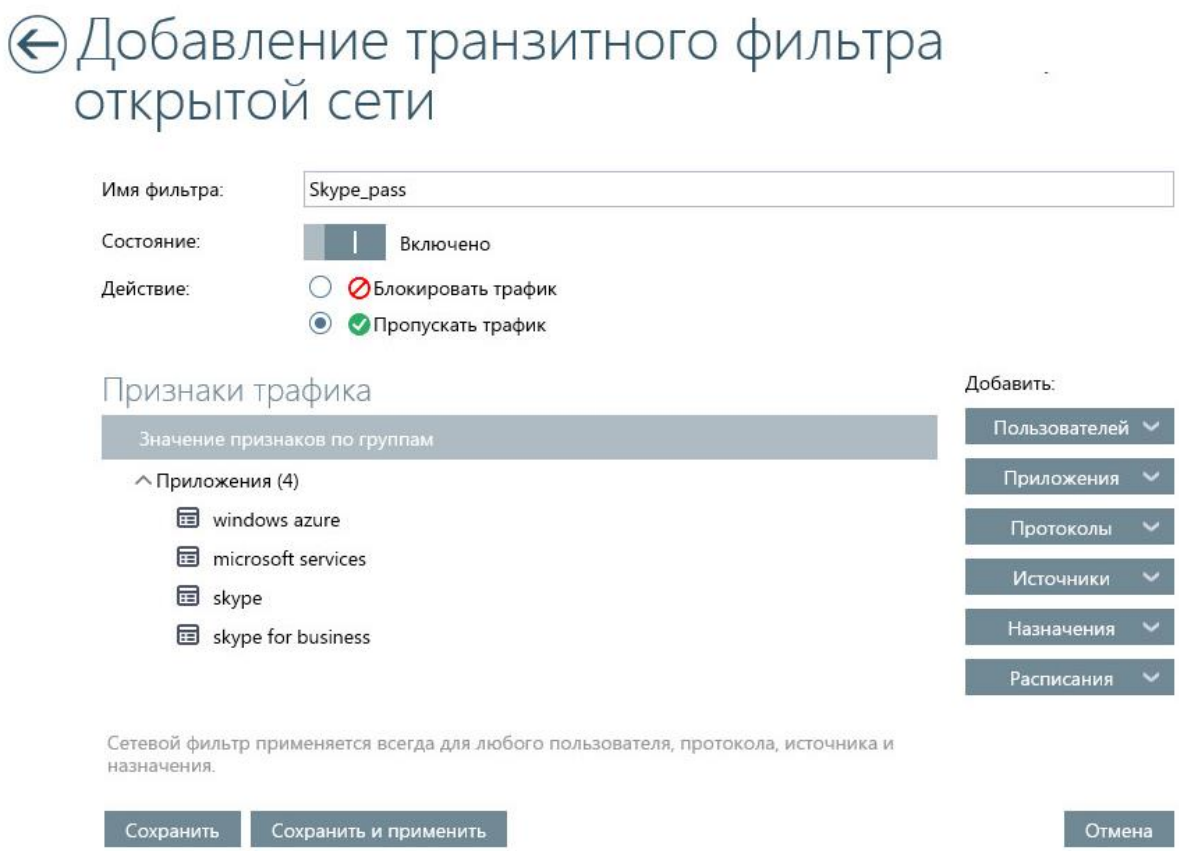

Рисунок 45: Добавление разрешающего сетевого фильтра для приложения Skype

4 Создайте транзитный фильтр открытой сети с именем Skype_pass:

4.1 В поле **Имя фильтра** укажите название фильтра.

4.2 Установите переключатель **Состояние** в положение **Включено**.

4.3 Установите переключатель **Действие** в положение **Пропускать трафик**.

4.4 Нажмите кнопку **Приложения** раздела **Добавить** и укажите **Skype**, **Skype for business**, **Windows Azure** и **Microsoft Services**.

4.5 Нажмите кнопку **Сохранить и Применить**.

Внимание! Убедитесь, что разрешение доменных имен для пользователей вашей сети работает корректно. При необходимости создайте разрешающий фильтр для прикладного протокола DNS.

Если вы хотите запретить использование приложений Skype на компьютерах локальной сети, защищенной ViPNet xFirewall, создайте транзитный фильтр открытой сети с именем Skype_drop:

1 В поле **Имя фильтра** укажите название фильтра.

2 Установите переключатель **Состояние** в положение **Включено**.

3 Установите переключатель **Действие** в положение **Блокировать трафик**.

4 Нажмите кнопку **Приложения** раздела **Добавить** и укажите **Skype** и **Skype for business**.

5 Нажмите кнопку **Сохранить и Применить**.

В результате пользователям вашей локальной сети будет или разрешено, или запрещено использовать приложение Skype.

Настройка фильтрации трафика Torrent-клиентов

Чтобы заблокировать работу Torrent-клиентов на компьютерах локальной сети, защищенной ViPNet xFirewall, создайте запрещающие сетевые фильтры для протоколов:

- BitTorrent — протокол обмена файлами между Torrent-клиентами;
- Teredo — протокол инкапсуляции пакетов IPv6 в IPv4, позволяющий Torrent-клиентам обмениваться файлами даже при блокировке протокола BitTorrent.

Для этого выполните следующие действия:

1 Войдите в веб-интерфейс в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Межсетевой экран** > **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

3 Нажмите кнопку **Добавить**. Откроется страница добавления транзитного фильтра открытой сети.

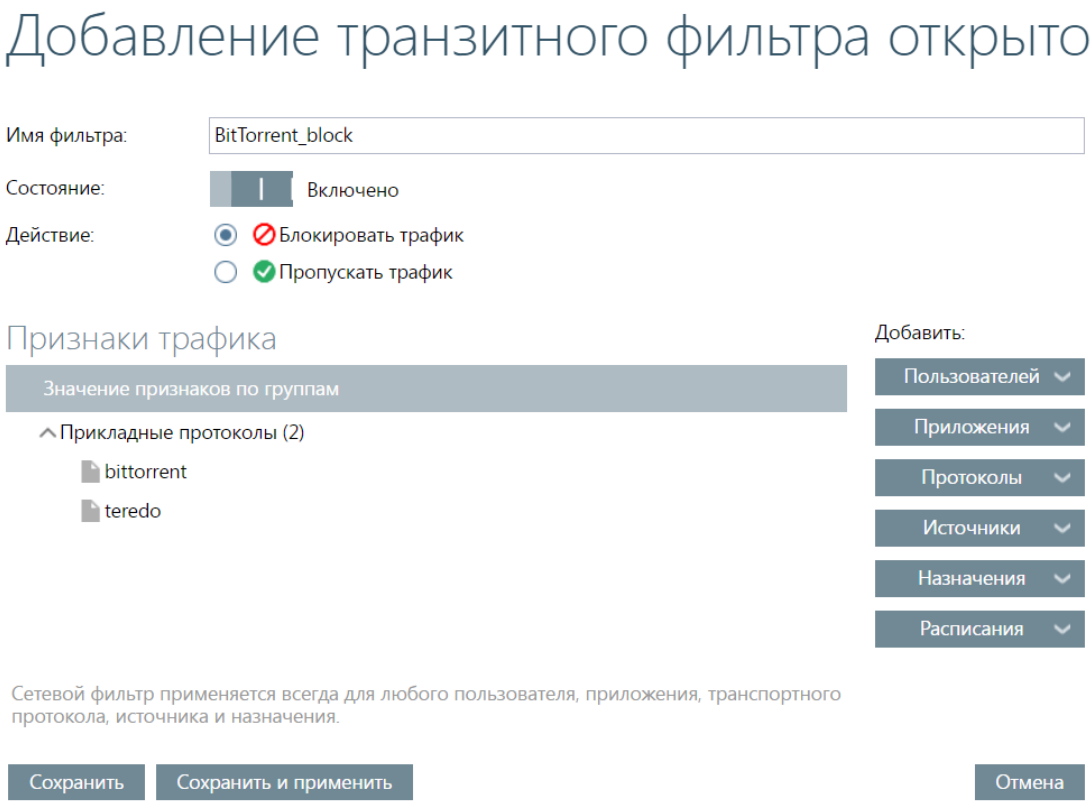

Рисунок 46. Добавление запрещающего сетевого фильтра для протокола BitTorrent

4 Создайте транзитный фильтр открытой сети с именем BitTorrent_block:

4.1 В поле **Имя фильтра** укажите название фильтра.

4.2 Установите переключатель **Состояние** в положение **Включено**.

4.3 Установите переключатель **Действие** в положение **Блокировать трафик**.

4.4 Нажмите кнопку **Протоколы** раздела **Добавить**, далее **Прикладные протоколы** и выберите bittorrent и teredo.

4.5 Нажмите кнопку **Сохранить и Применить**.

В результате выполненных действий вы заблокируете работу Torrent-клиентов в вашей сети.

Создание локальных фильтров открытой сети

Локальные фильтры открытой сети регулируют обмен IP-трафиком между ViPNet xFirewall и открытыми узлами.

Чтобы создать локальный фильтр открытой сети, выполните следующие действия:

1 Перейдите на страницу **Сетевые фильтры** > **Локальные фильтры открытой сети**.

2 На панели инструментов нажмите кнопку **Добавить**.

3 На открывшейся странице в поле **Имя фильтра** укажите название фильтра.

4 Установите переключатели **Состояние** и **Действие**.

5 Нажмите кнопку **Протоколы** раздела **Добавить** и укажите протоколы для фильтрации. Вы можете добавить протокол TCP/UDP, сообщение ICMP, IP-протокол и группу протоколов.

6 Нажмите кнопку **Источники** раздела **Добавить** и укажите отправителя IP-пакетов. Вы можете добавить IP-адрес или диапазон адресов, DNS-имя, группу IP-адресов, системные группы объектов и задать ограничения по интерфейсу:

- Чтобы добавить один или несколько IP-адресов, выберите **IP-адрес или диапазон адресов**. В открывшемся окне выберите способ указания адресов (**IP-адрес**, **IP-подсеть** или **Диапазон IP-адресов**), укажите IP-адрес, диапазон адресов или адрес и маску подсети, затем нажмите кнопку **Сохранить**.
- Чтобы добавить DNS-имя, выберите соответствующий пункт. В открывшемся окне укажите DNS-имя и нажмите кнопку **Сохранить**.
- Чтобы добавить группу IP-адресов, выберите пункт **Группа IP-адресов**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Сохранить**.
- Для добавления системной группы объектов выберите один из пунктов: **Мой узел**, **Другие узлы**.
- Чтобы задать ограничения по интерфейсу, задайте значения для **Интерфейс с IP-адресом** или для **Группы интерфейсов** и нажмите кнопку **Сохранить**.

7 Нажмите кнопку **Назначения** в разделе **Добавить** и укажите получателя IP-пакетов. **IP-адрес или диапазон адресо**в , **DNS-имя** и **Группа IP-адресов** задайте по аналогии с настройкой **Источники**. В случае использования системных групп объектов, вы можете указать группы **Мой узел**, **Другие узлы**, **Широковещательные адреса**, **Групповые адреса**.

8 Нажмите кнопку **Расписания** раздела **Добавить** и укажите расписание действия фильтра. Вы можете добавить временной диапазон действия расписания и выбрать группу расписаний.

9 Нажмите кнопку **Сохранить** для сохранения введенных данных настройки или **Сохранить и применить** для сохранения данных и применения фильтра.

В результате новый фильтр отобразится в списке локальных фильтров открытой сети.

Примечание. Применение запрещающего локального фильтра открытой сети к установленному соединению не блокирует его работу до истечения времени жизни соединения. После этого, при попытке повторного соединения на него уже будет действовать новое заданное запрещающее правило.

Создание фильтров защиты канала управления

Сетевые фильтры защиты канала управления позволяют ограничивать обмен IP-трафиком с узлами сети ViPNet, с которыми имеет связь ViPNet xFirewall (см. Общие сведения о сетевых фильтрах на стр. 60).

Чтобы создать фильтр защиты канала управления, выполните следующие действия:

1. Перейдите на страницу **Сетевые фильтры** > **Защита канала управления**.
2. На панели инструментов нажмите кнопку **Добавить**.
3. На открывшейся странице в поле **Имя фильтра** укажите название фильтра.
4. Нажмите кнопку **Протоколы** раздела **Добавить** и укажите протоколы для фильтрации. Вы можете добавить протокол TCP/UDP, сообщение ICMP, IP-протокол и группу протоколов.
5. Нажмите кнопку **Источники** раздела **Добавить** и укажите отправителя IP-пакетов. Вы можете добавить сетевой узел, группу узлов ViPNet и системные группы объектов:
   - Чтобы добавить один или несколько узлов сети ViPNet, выберите **Сетевой узел**. В открывшемся окне установите флажок рядом с нужными узлами и нажмите кнопку **Выбрать N узлов**.
   - Чтобы добавить группу узлов сети ViPNet, выберите пункт **Группа узлов ViPNet**. В открывшемся окне установите флажок рядом с нужной группой (или несколькими группами) и нажмите кнопку **Добавить**.
   - Для добавления системной группы объектов выберите один из пунктов: **Мой узел**, **Другие узлы**, **Все координаторы**, **Все клиенты**.
6. Нажмите кнопку **Назначения** раздела **Добавить** и по аналогии с настройкой **Источники** добавьте получателя зашифрованных IP-пакетов.
7. Нажмите кнопку **Расписания** раздела **Добавить** и укажите расписание действия фильтра. Вы можете добавить временной диапазон действия расписания и выбрать группу расписаний.
8. Нажмите кнопку **Сохранить** для сохранения введенных данных настройки или **Сохранить и применить** для сохранения данных и применения фильтра.

В результате новый фильтр отобразится в списке фильтров защиты канала управления.

Примечание. Применение запрещающего фильтра защиты канала управления к установленному соединению не блокирует его работу до истечения времени жизни соединения. После этого, при попытке повторного соединения на него уже будет действовать новое заданное запрещающее правило.

Просмотр сетевых фильтров

Чтобы просмотреть сетевые фильтры, заданные на узле ViPNet xFirewall, выполните следующие действия:

1. На начальной странице веб-интерфейса щелкните плитку **Межсетевой экран**.
2. На странице **Сетевые фильтры** выберите вкладку сетевых фильтров нужного типа. В результате отобразится список таких фильтров в порядке убывания их приоритета.

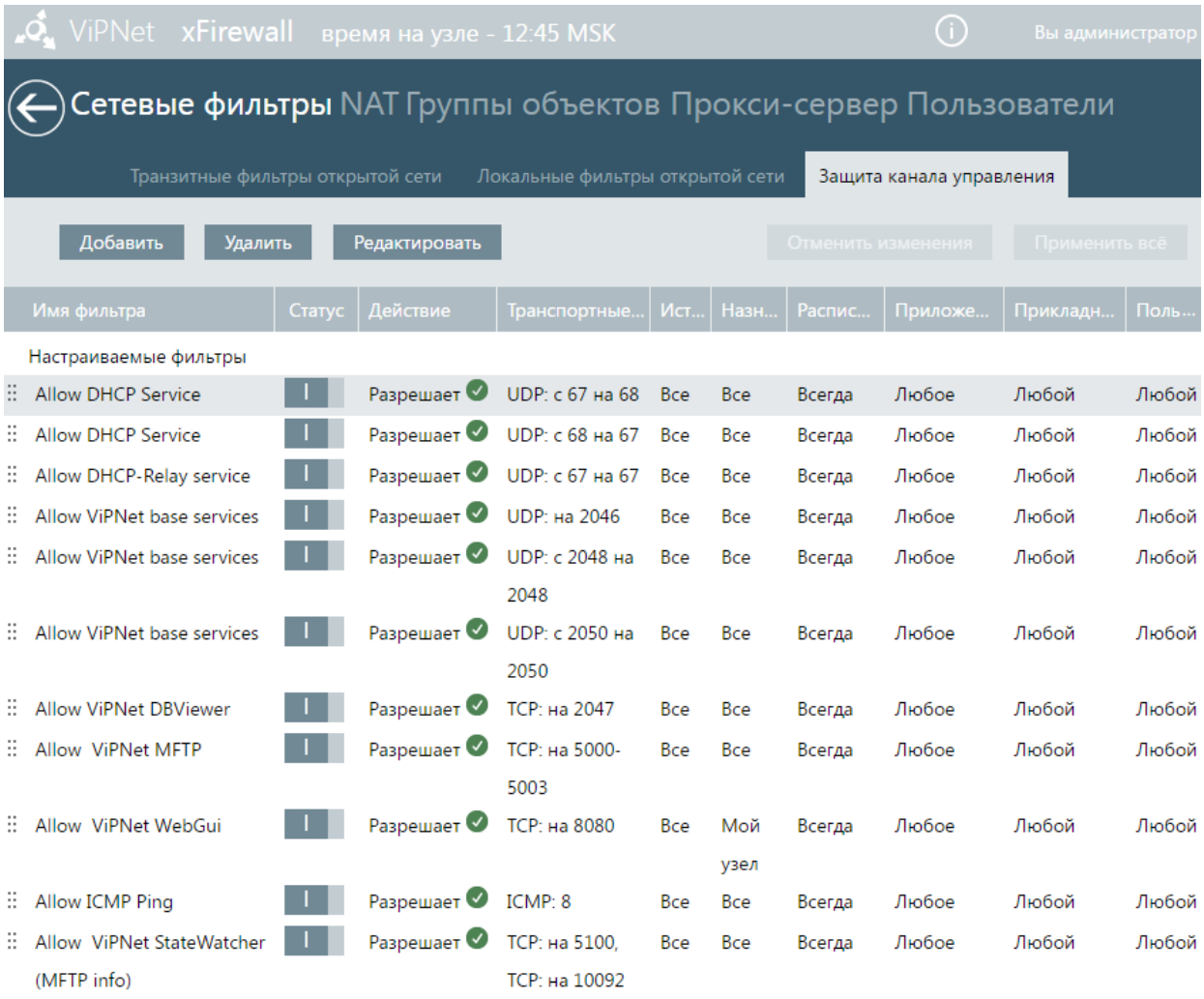

Рисунок 47. Просмотр сетевых фильтров

3 Для просмотра подробной информации о фильтре дважды щелкните его в списке.

Чтобы удалить сетевой фильтр ViPNet xFirewall, выполните следующие действия:

1 Установите указатель на фильтр и нажмите левую кнопку мыши.

2 Нажмите кнопку **Удалить**.

3 В окне **Внимание** нажмите кнопку **ОК** для подтверждения или кнопку **Отмена**.

Настройка правил трансляции адресов

Трансляция сетевых адресов

Трансляция сетевых адресов (NAT) — это механизм преобразования IP-адресов одной сети в IP-адреса другой сети. Технология трансляции адресов описана в RFC 2663 (http://tools.ietf.org/html/rfc2663).

ViPNet xFirewall может выполнять трансляцию адресов следующих типов:

- Трансляция адреса источника (на стр. 89), называемая также маскарадингом (masquerading) или динамической трансляцией.

  В этом случае при прохождении через ViPNet xFirewall пакетов от отправителей с частными адресами в них заменяется адрес отправителя на внешний (реальный) адрес маршрутизатора. При получении ответных пакетов в них подменяется адрес получателя обратно на частный адрес, и в таком виде пакет доставляется в частную сеть.

  Используется для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов (см. глоссарий, стр. 205). В результате локальные сети, использующие частные адреса (см. глоссарий, стр. 206), получают доступ к ресурсам Интернета.

- Трансляция адреса назначения (на стр. 88), называемая также форвардингом портов (port forwarding) или статической трансляцией.

  В этом случае пакеты, приходящие из Интернета на определенный порт внешнего адреса маршрутизатора, перенаправляются на указанный адрес внутренней сети путем подмены в них адреса получателя, а у ответных пакетов от компьютера внутренней сети подменяется адрес отправителя.

  Используется для организации доступа к ресурсам локальной сети из Интернета. В результате локальные сети, использующие частные адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

- Одновременная трансляция адресов источника и назначения. Может использоваться в сложных схемах маршрутизации трафика.

ViPNet xFirewall выполняет трансляцию сетевых адресов, только если настроены соответствующие правила. В ViPNet xFirewall должны быть задействованы минимум два сетевых интерфейса (см. глоссарий, стр. 205):

- внешний интерфейс — имеет публичный IP-адрес и обеспечивает доступ в Интернет;
- внутренний интерфейс — имеет частный IP-адрес.

Трансляция адреса назначения

Трансляция адреса узла назначения предназначена для организации доступа из Интернета (или другой внешней сети) к серверам локальной сети, не имеющим публичного IP-адреса. Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных узлов публичный IP-адрес ViPNet xFirewall. В соответствии с правилом, в заголовках IP-пакетов публичный IP-адрес (или IP-адрес и порт) назначения заменяется частным адресом локальной сети. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.

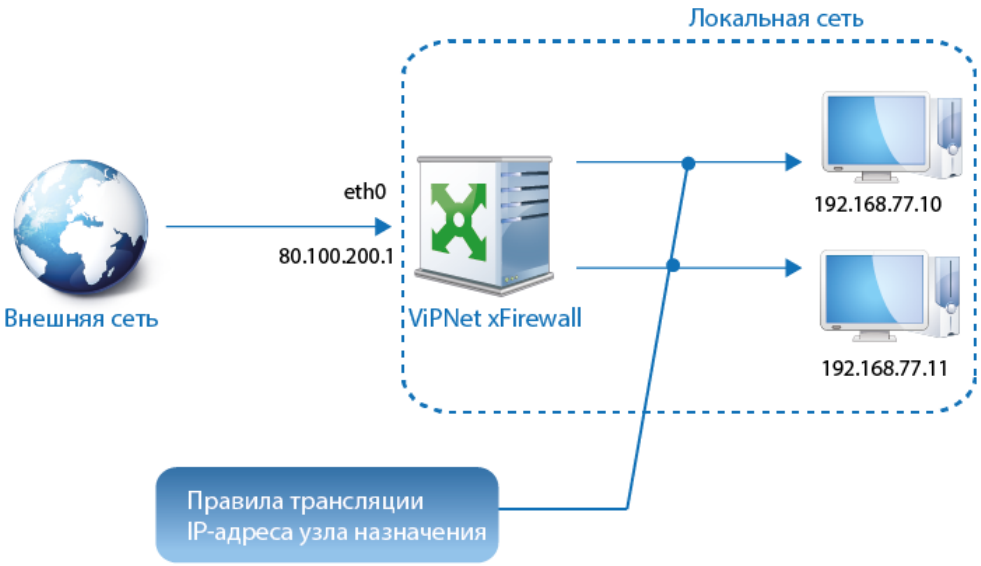

Рисунок 48. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

Если для внешнего IP-адреса ViPNet xFirewall задано правило трансляции адреса назначения, то при обращении к этому адресу из внешней сети будут выполняться следующие преобразования:

- Во входящих IP-пакетах от внешнего узла ViPNet xFirewall подменяет адрес получателя (публичный IP-адрес ViPNet xFirewall) локальным адресом в соответствии с описанным правилом. Затем пакет передается через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.
- При прохождении ответных пакетов (в рамках уже созданной сессии) ViPNet xFirewall производит обратную замену IP-адресов. Адрес отправителя (IP-адрес локального узла) подменяется публичным IP-адресом внешнего сетевого интерфейса ViPNet xFirewall. Затем ответный пакет отправляется по назначению (узлу во внешней сети).

  Таким образом, при передаче во внешней сети пакет выглядит так, будто отправитель и получатель этого пакета имеют публичные IP-адреса.

Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний узел. Чтобы локальный узел мог также иметь доступ в Интернет (двусторонний NAT), необходимо в дополнение к правилу трансляции адреса узла назначения задать также правило трансляции адреса источника (см. Трансляция адреса источника на стр. 89).

Трансляция адреса источника

Трансляция адреса источника предназначена для организации доступа локальных компьютеров в Интернет. Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных узлов публичный IP-адрес ViPNet xFirewall. В соответствии с правилом, в заголовках IP-пакетов частные IP-адреса источника заменяются на публичный IP-адрес. Таким образом, узлы локальной сети могут устанавливать соединения с узлами в Интернете от имени публичного IP-адреса ViPNet xFirewall.

Рисунок 49. Организация доступа в Интернет при помощи правила трансляции IP-адреса источника

Если на ViPNet xFirewall настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через ViPNet xFirewall из локальной сети в Интернет (или другие глобальные сети) будут преобразованы следующим образом:

- В момент передачи IP-пакета из локальной сети в Интернет ViPNet xFirewall преобразует адрес и (или) порт отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. В процессе преобразования частный адрес отправителя пакета заменяется на публичный адрес внешнего сетевого интерфейса ViPNet xFirewall, обеспечивающего доступ в глобальную сеть. При дальнейшей передаче в Интернете пакет имеет публичный IP-адрес отправителя. Номера портов отправителя (для протоколов TCP и UDP) и запоминаемые параметры (для протокола ICMP) пакетов имеют уникальные значения для всех исходящих IP-соединений внешнего сетевого интерфейса ViPNet xFirewall. После преобразования пакет отправляется адресату в Интернете.
- При прохождении ответных пакетов ViPNet xFirewall производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета ViPNet xFirewall заменяет в нем адрес получателя на частный адрес узла локальной сети, которому адресован ответный пакет. Преобразование происходит на основании уникальных номеров портов, присвоенных исходящим пакетам (для протоколов TCP и UDP), и запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также

преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.

Примечание. Для всех протоколов, кроме TCP, UDP и ICMP, преобразуются только IP-адреса. Для протоколов с частичным преобразованием трансляция IP-адреса источника не будет работать, если несколько узлов локальной сети одновременно инициируют соединение с одним и тем же IP-адресом публичной сети.

Просмотр правил трансляции адресов

Чтобы просмотреть правила трансляции адресов (см. глоссарий, стр. 206), заданные на узле ViPNet xFirewall, выполните следующие действия:

1 На начальной странице веб-интерфейса щелкните плитку **Межсетевой экран**.

2 Перейдите на страницу **NAT**. В результате отобразится список правил трансляции адресов в порядке убывания приоритета.

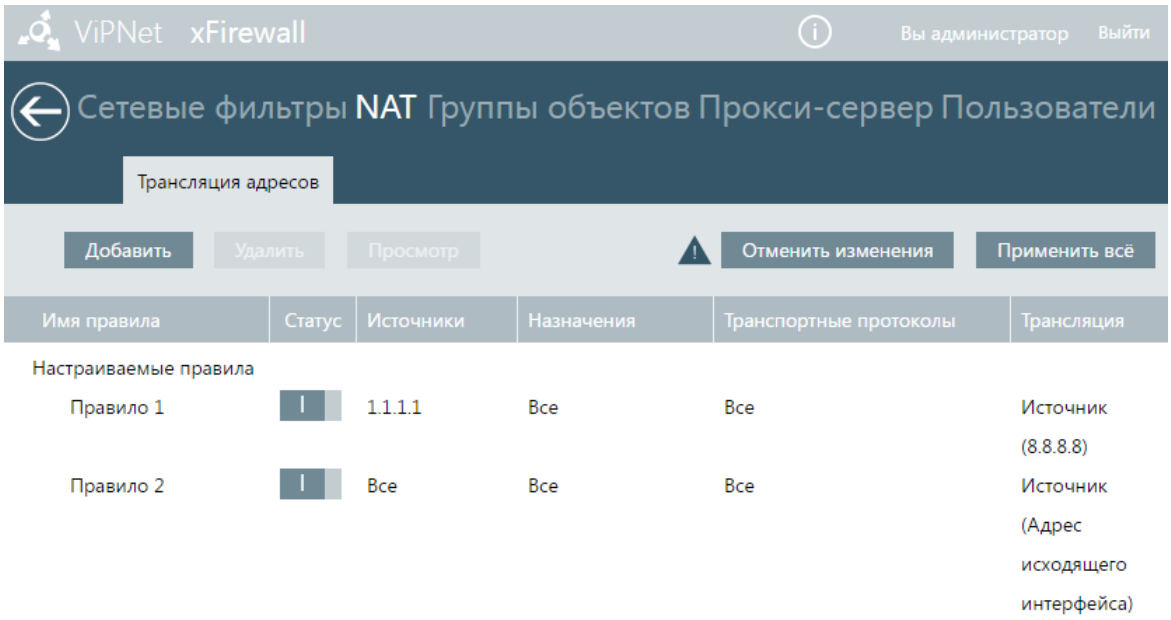

Рисунок 50. Просмотр правил трансляции адресов

3 Для просмотра подробной информации о правиле трансляции дважды щелкните его в списке.

Создание и изменение правила трансляции адресов

Чтобы создать или изменить правило трансляции адресов, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Межсетевой экран** > **NAT**.

3 Выполните одно из действий:

- Чтобы создать правило трансляции, на панели инструментов нажмите кнопку **Добавить**.
- Чтобы изменить правило трансляции, дважды щелкните его в списке или нажмите кнопку **Редактировать**.

4 На открывшейся странице выполните следующие действия:

- В соответствующем поле укажите имя правила трансляции.
- Чтобы правило трансляции начало действовать после создания, установите флажок **Правило включено**.
- Если требуется трансляция адреса источника для исходящих IP-пакетов, в разделе **Трансляция источника** установите флажок **Заменять адрес источника на** и выполните одно из действий:
  - чтобы IP-адрес отправителя заменялся на адрес внешнего сетевого интерфейса ViPNet xFirewall, установите переключатель в положение **адрес исходящего интерфейса (определяется автоматически)**;
  - чтобы указать другой IP-адрес для замены IP-адреса отправителя, установите переключатель в положение **другой IP-адрес** и укажите нужный IP-адрес.
- Если требуется трансляция адреса назначения для входящих IP-пакетов, в разделе **Трансляция назначения** установите флажок **Заменять адрес назначения на** и при необходимости флажок **Заменять порт назначения на** и укажите IP-адрес и порт, которые будут иметь IP-пакеты, переданные ViPNet xFirewall в локальную сеть. При создании правила трансляции с использованием порта назначения указание адреса назначения и транспортного протокола TCP или UDP обязательно.
- В разделе **Источники** по умолчанию указаны все отправители IP-пакетов (**Все**). Чтобы выбрать определенных получателей IP-пакетов, нажмите кнопку **Добавить** и укажите IP-адреса, диапазоны IP-адресов или группы IP-адресов (см. Группа IP-адресов на стр. 68).
- В разделе **Назначения** по умолчанию указаны все получатели IP-пакетов (**Все**). Чтобы выбрать определенных получателей IP-пакетов, нажмите кнопку **Добавить** и укажите IP-адреса, диапазоны IP-адресов или группы IP-адресов (см. Группа IP-адресов на стр. 68).
- По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам. Чтобы фильтр применялся к IP-пакетам, передаваемым по определенным протоколам, в соответствующем разделе укажите протоколы (см. Группа протоколов на стр. 71).
- Нажмите кнопку **Сохранить**. В результате созданное правило трансляции отобразится в списке на странице **Межсетевой экран** > **NAT**.

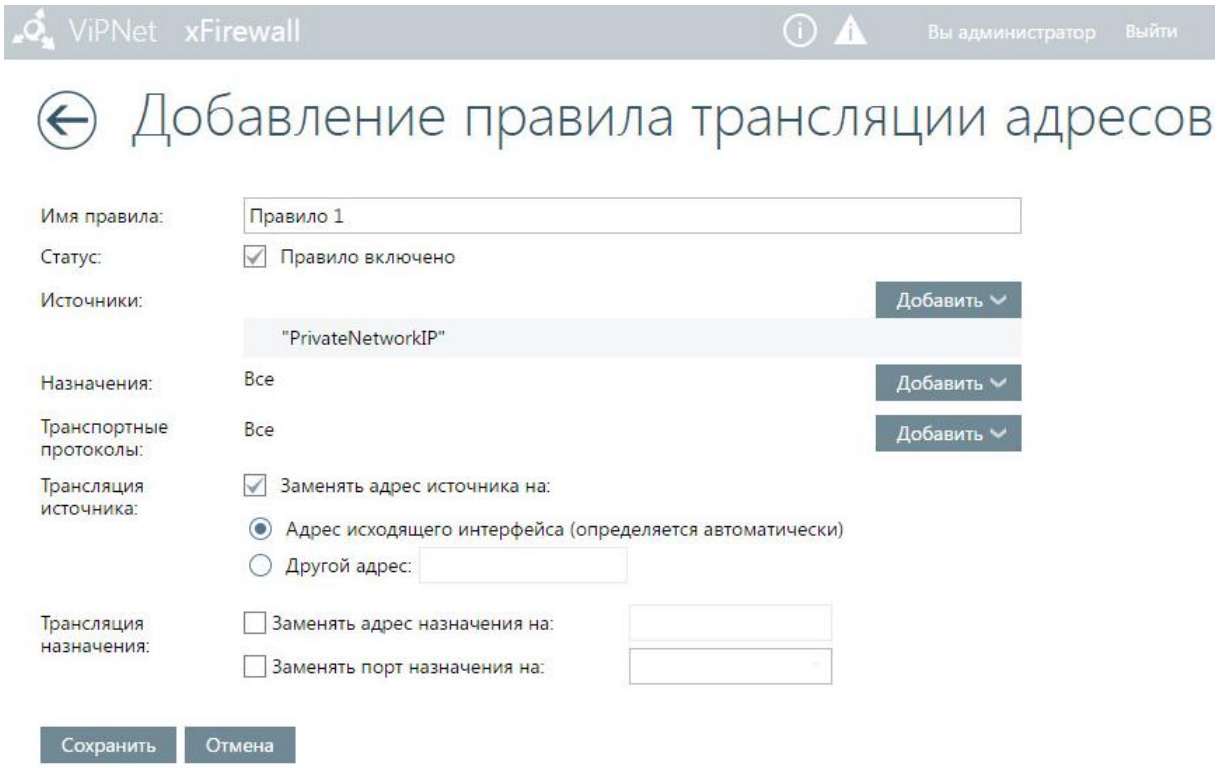

Рисунок 51. Создание правила трансляции адресов

5 Чтобы изменить приоритет правила трансляции, перетащите его на нужную строку списка.

6 Чтобы правило вступило в действие, нажмите кнопку **Применить все**.

Примечание. Примененное правило трансляции адресов будет работать для вновь устанавливаемых соединений. Для уже установленных соединений правило будет работать после истечения времени жизни соединения.

Примеры использования правил трансляции адресов

Организация доступа пользователей к Интернету

С помощью ViPNet xFirewall можно организовать доступ пользователей, имеющих частные адреса (см. глоссарий, стр. 206), к Интернету. Такая задача обычно возникает, когда число выделенных организации публичных адресов меньше числа компьютеров локальной сети, которым необходим доступ к Интернету. Для решения этой задачи используется трансляция адресов источников (см. глоссарий, стр. 206), которая заключается в преобразовании частных адресов локальной сети в один публичный адрес (см. глоссарий, стр. 205).

На рисунке ниже представлена схема организации доступа пользователей локальной сети к Интернету с помощью ViPNet xFirewall.

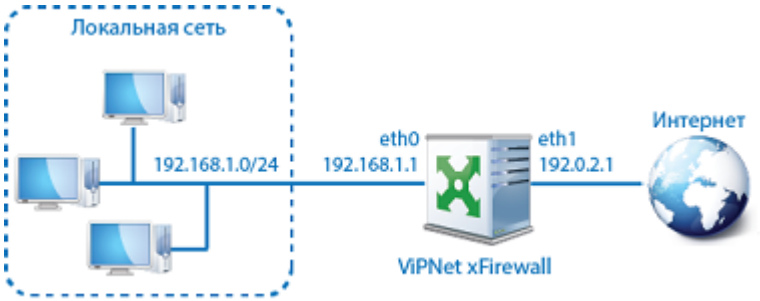

Рисунок 52. Организация доступа пользователей к Интернету с помощью ViPNet xFirewall

На приведенной схеме локальная сеть имеет адресное пространство 192.168.1.0/24. Один интерфейс ViPNet xFirewall (eth0) подключен к локальной сети и имеет частный адрес 192.168.1.1, другой интерфейс (eth1) подключен к Интернету и имеет публичный адрес 192.0.2.1.

Чтобы пользователи могли подключаться к Интернету, на ViPNet xFirewall необходимо задать правило трансляции IP-адресов и сетевой фильтр транзитных IP-пакетов. Для этого выполните следующие действия:

1. Войдите в веб-интерфейс в режиме администратора (см. Назначение веб-интерфейса на стр. 14).
2. Создайте правило трансляции частных адресов отправителей в адрес внешнего интерфейса ViPNet xFirewall. Для этого выполните следующие действия:
   - **2.1** Перейдите на страницу **Межсетевой экран** > **NAT**.
   - **2.2** Нажмите кнопку **Добавить**. Откроется страница добавления правила трансляции адресов.

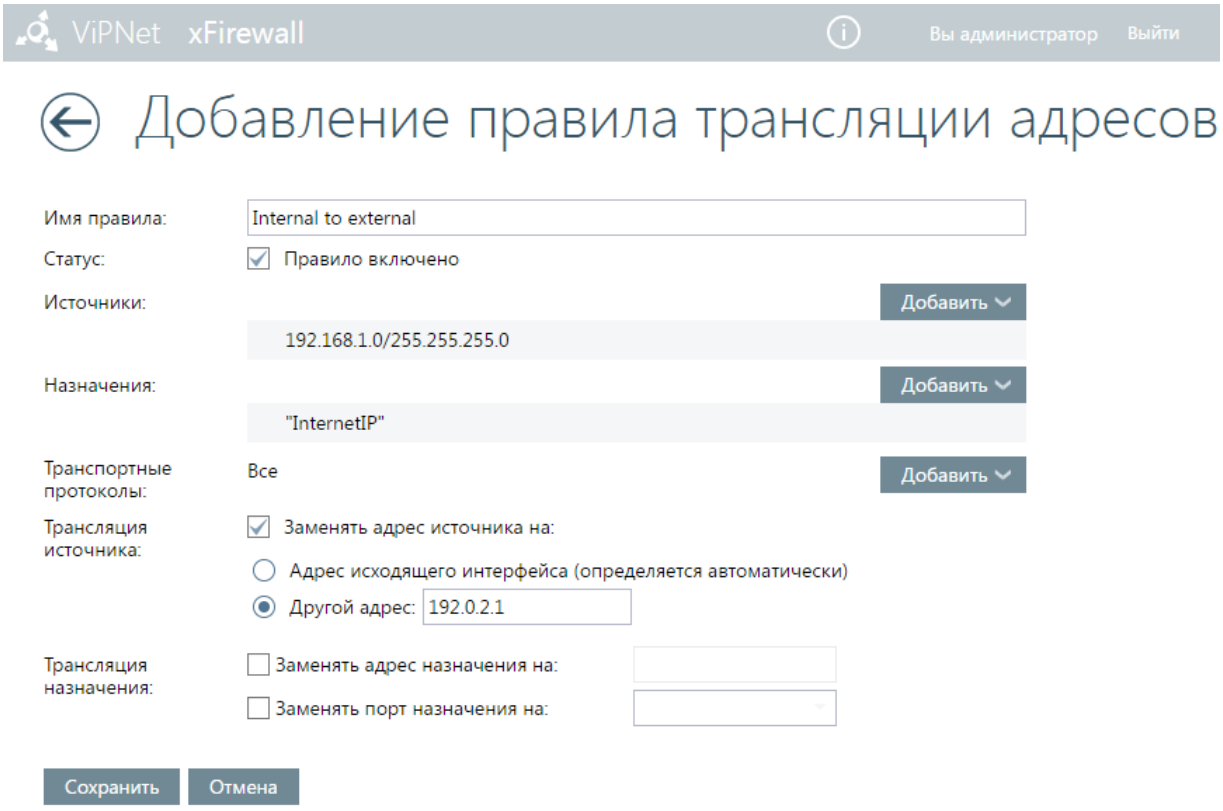

Рисунок 53. Добавление правила трансляции адресов

2.3 На странице **Правила трансляции адресов** выполните следующие действия:

- Напротив параметра **Статус** установите флажок **Правило включено**.
- Напротив параметра **Источники** нажмите кнопку **Добавить** и выберите в качестве источника **IP-адрес или диапазон IP-адресов**.

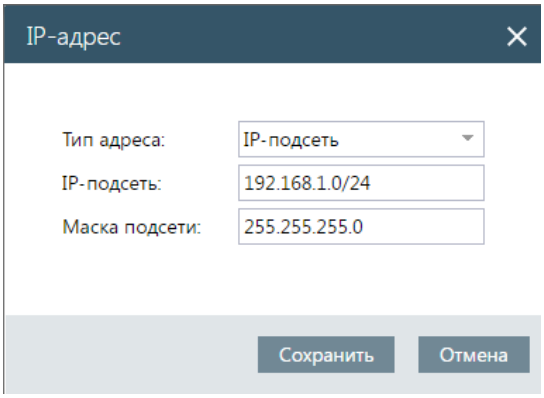

Рисунок 54. Добавление IP-подсети

- В появившемся диалоговом окне в списке **Тип адреса** выберите тип **IP-подсеть** и в соответствующем поле задайте подсеть `192.168.1.0/24`. Нажмите кнопку **Сохранить**.
- Напротив параметра **Назначения** нажмите кнопку **Добавить** и выберите пункт **Группа IP-адресов**.

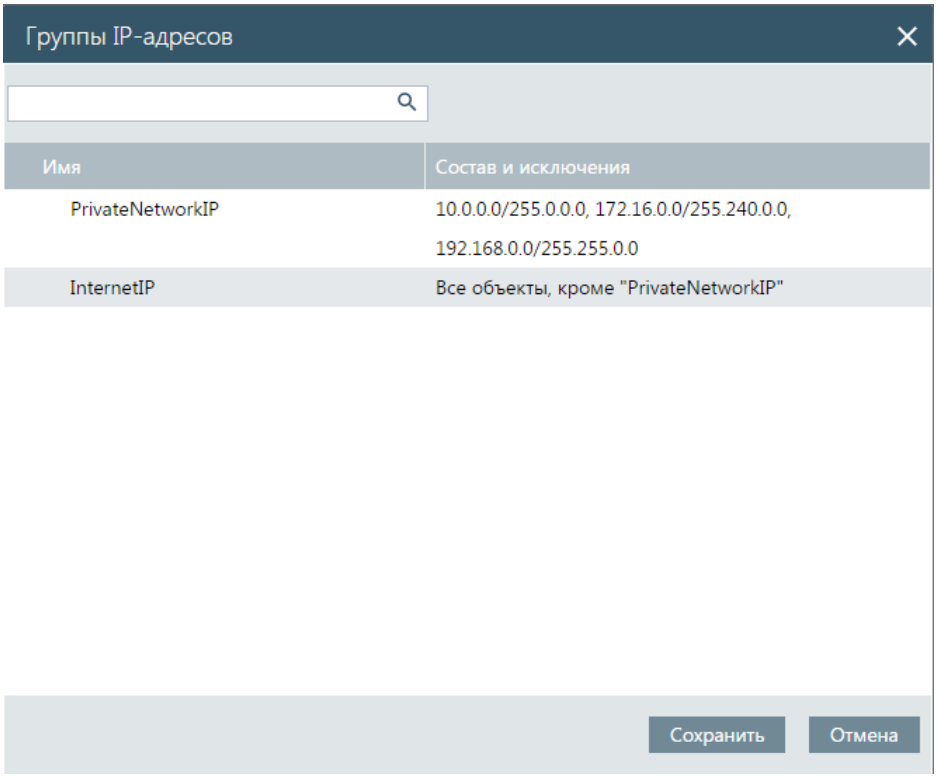

Рисунок 55. Выбор группы IP-адресов

- В появившемся диалоговом окне выберите группу **InternetIP** и нажмите кнопку **Сохранить**.
- Напротив параметра **Трансляция источника** установите флажок **Заменять адрес источника на** и выберите вариант **Другой адрес**.
- В появившемся поле задайте IP-адрес `192.0.2.1`. Нажмите кнопку **Сохранить**.

3 Создайте разрешающий транзитный фильтр открытой сети Allow_web:

3.1 Перейдите на страницу **Межсетевой экран** > **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

3.2 Нажмите кнопку **Добавить**. Откроется страница добавления транзитного фильтра открытой сети.

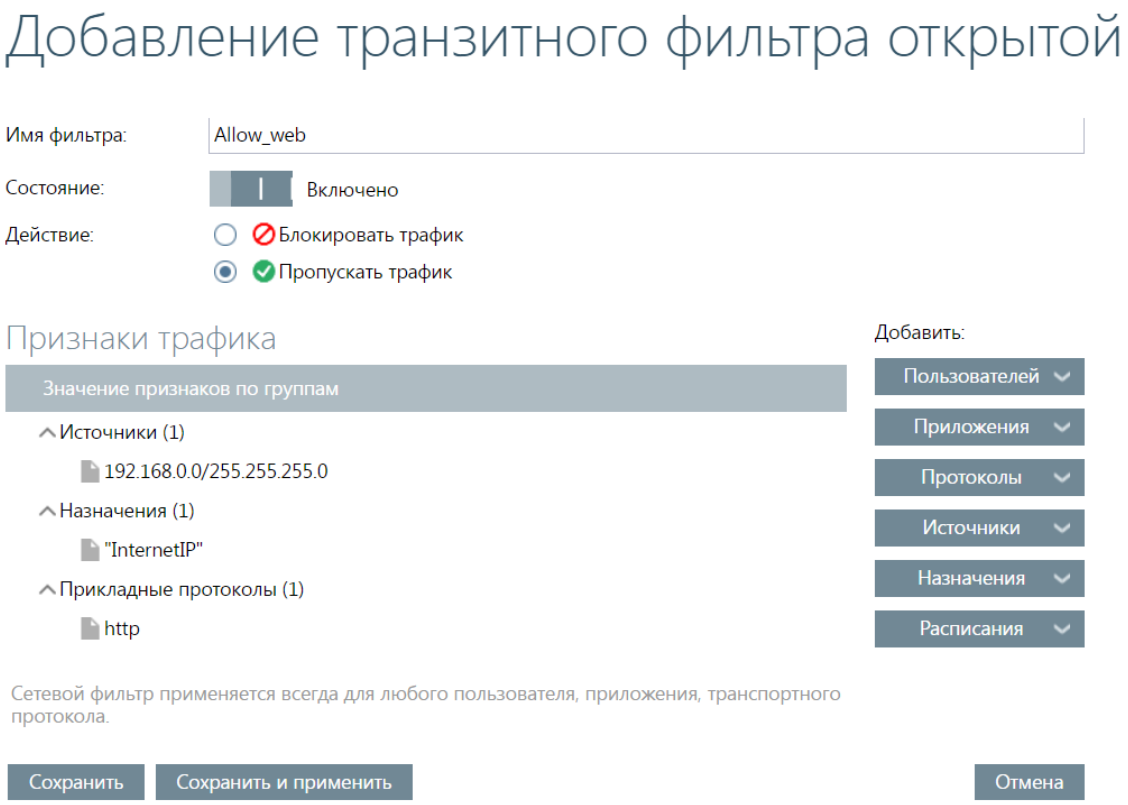

Рисунок 56. Добавление транзитного фильтра открытой сети Allow_web

3.3 На странице **Добавление транзитного фильтра открытой сети** выполните следующие действия:

- В поле **Имя фильтра** укажите название фильтра `Allow_web`.
- Установите переключатель **Состояние** в положение **Включено**.
- Установите переключатель **Действие** в положение **Пропускать трафик**.
- В разделе **Добавить** нажмите кнопку **Протоколы**, далее **Прикладные протоколы** и выберите протокол **HTTP**. Выполните это действие, если вы хотите ограничить доступ пользователей к сети Интернет только по протоколу HTTP, в противном случае не выполняйте это действие.
- В разделе **Добавить** нажмите кнопку **Источники**, далее выберите в качестве источника **IP-адрес или диапазон IP-адресов**. В появившемся диалоговом окне (см. Рисунок 54 на стр. 94) в списке **Тип адреса** выберите **IP-подсеть** и в соответствующем поле задайте подсеть `192.168.1.0/24`. Нажмите кнопку **Сохранить**.
- В разделе **Добавить** нажмите кнопку **Назначения**, далее выберите в качестве назначения **Группа IP-адресов**. В появившемся диалоговом окне (см. Рисунок 55 на стр. 95) выберите группу **InternetIP** и нажмите кнопку **Сохранить**.
- Нажмите кнопку **Сохранить и применить**.

В результате выполненных настроек пользователи локальной сети будут иметь доступ к Интернету.

Размещение общедоступного сервера в демилитаризованной зоне

В локальной сети наиболее уязвимыми для сетевых атак являются узлы (серверы), которые взаимодействуют с внешними системами или предоставляют различные сервисы внешним пользователям (почтовые, веб-серверы и так далее). В случае атаки на такие серверы под угрозой оказываются остальные компьютеры сети. Чтобы защитить локальную сеть, ее разбивают на сегменты, размещая серверы в демилитаризованной зоне. Эту зону отделяют от остальной сети межсетевым экраном (см. глоссарий, стр. 204), который контролирует трафик между сегментами. При этом сервисы, предоставляемые серверами, доступны как внешним пользователям, так и пользователям локальной сети. В то же время локальная сеть недоступна внешним пользователям.

В качестве межсетевого экрана, отделяющего демилитаризованную зону от внутреннего сегмента сети, можно использовать ViPNet xFirewall. На рисунке ниже приведена схема сети с веб-сервером, размещенным в демилитаризованной зоне, и ViPNet xFirewall с тремя интерфейсами, установленным на границе локальной сети.

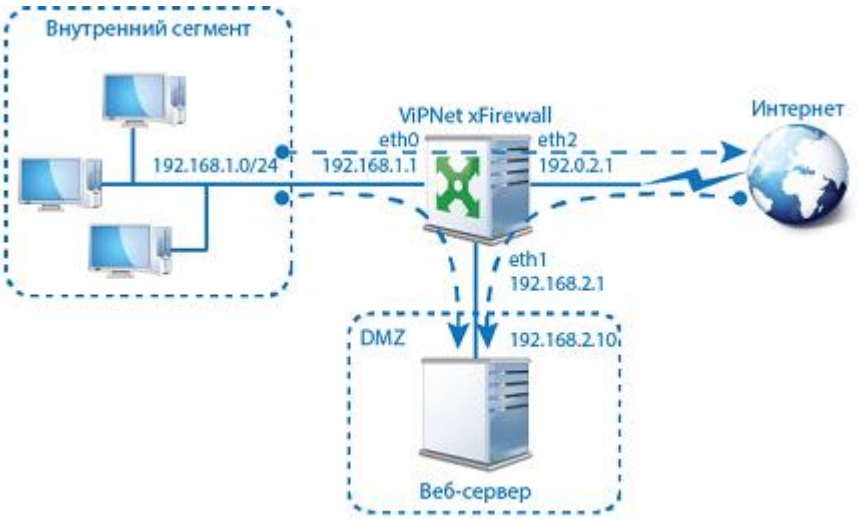

Рисунок 57. Использование ViPNet xFirewall для размещения общедоступного сервера в DMZ

Два интерфейса ViPNet xFirewall (eth0 и eth1) имеют частные IP-адреса (см. глоссарий, стр. 206) и подключены к сегментам локальной сети, интерфейс eth2 имеет публичный IP-адрес (см. глоссарий, стр. 205) и подключен к Интернету. Пусть заданы следующие сетевые настройки:

- компьютеры во внутреннем сегменте имеют адреса 192.168.1.0/24;
- веб-сервер имеет адрес 192.168.2.10;
- интерфейсы eth0, eth1, eth2 имеют адреса 192.168.1.1, 192.168.2.1, 192.0.2.1 соответственно.

Предполагается, что в приведенной схеме допустимы инициативные соединения по следующим направлениям:

- из внутреннего сегмента в Интернет;
- из внутреннего сегмента к веб-серверу, находящемуся в демилитаризованной зоне (DMZ);
- из Интернета к веб-серверу.

Чтобы установление таких соединений было возможно, на ViPNet xFirewall необходимо создать сетевые фильтры транзитных IP-пакетов и правила трансляции IP-адресов. Для этого выполните следующие действия:

1 Войдите в веб-интерфейс в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Межсетевой экран** > **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

3 Нажмите кнопку **Добавить**. Откроется страница добавления транзитного фильтра открытой сети.

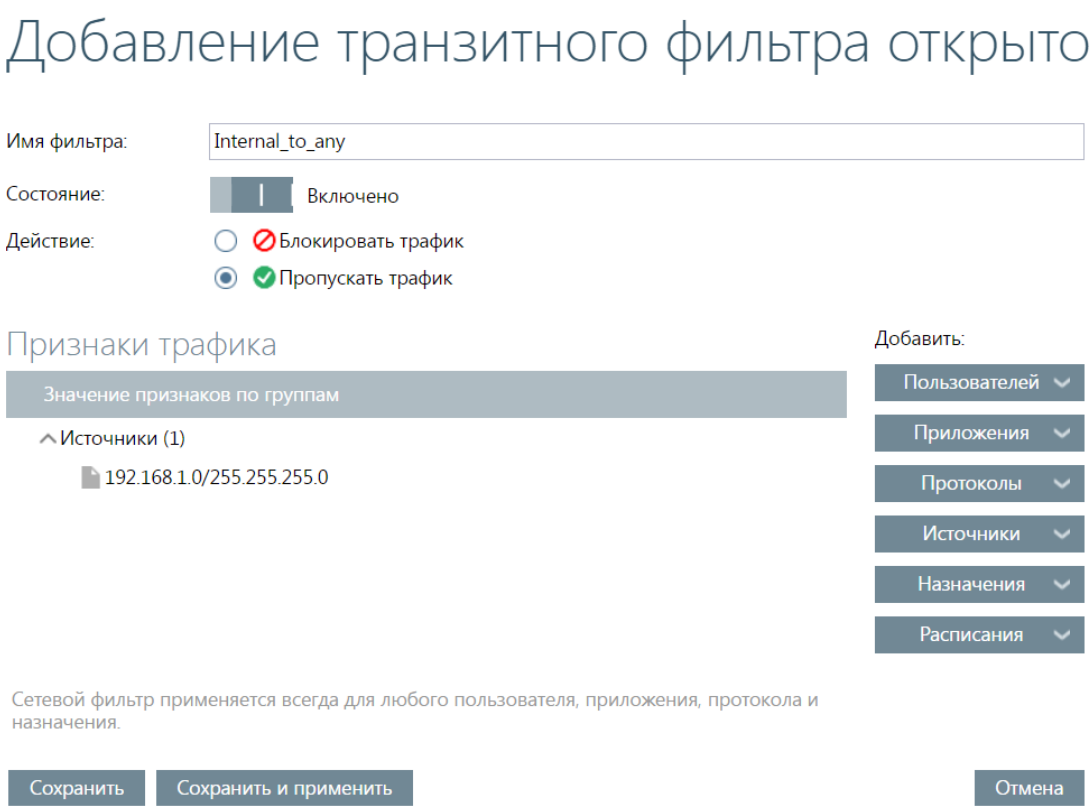

Рисунок 58. Добавление транзитного фильтра для демилитаризованной зоны

4 Создайте транзитный фильтр открытой сети с именем Internal_to_any:

4.1 В поле **Имя фильтра** введите `Internal_to_any`.

4.2 Установите переключатель **Состояние** в положение **Включено**.

4.3 Установите переключатель **Действие** в положение **Пропускать трафик**.

4.4 В разделе **Добавить** нажмите кнопку **Источники**, далее выберите в качестве источника **IP-адрес или диапазон IP-адресов**. В появившемся диалоговом окне (см. Рисунок 54 на стр. 94) в списке **Тип адреса** выберите **IP-подсеть** и в соответствующем поле задайте подсеть `192.168.1.0/24`. Нажмите кнопку **Сохранить**.

4.5 На странице добавления транзитного фильтра нажмите кнопку **Сохранить и применить**.

5 На странице **Межсетевой экран** > **Сетевые фильтры** > **Транзитные фильтры открытой сети** нажмите кнопку **Добавить.**

6 Создайте транзитный фильтр открытой сети с именем Internet_to_DMZ:

6.1 В поле **Имя фильтра** введите `Internet_to_DMZ`.

6.2 Установите переключатель **Состояние** в положение **Включено**.

6.3 Установите переключатель **Действие** в положение **Пропускать трафик**.

6.4 В разделе **Добавить** нажмите кнопку **Протоколы**, далее **Прикладные протоколы** и выберите протокол **HTTP**.

6.5 В разделе **Добавить** нажмите кнопку **Источники**, далее выберите в качестве источника **Группа IP-адресов**. В появившемся диалоговом окне (см. Рисунок 55 на стр. 95) выберите группу **InternetIP** и нажмите кнопку **Сохранить**.

6.6 В разделе **Добавить** нажмите кнопку **Назначения**, далее выберите в качестве назначения **IP-адрес или диапазон IP-адресов**. В появившемся диалоговом окне задайте IP-адрес `192.0.2.10` и нажмите кнопку **Сохранить**.

6.7 Напротив параметра **Прикладной протокол** выберите из списка протокол **HTTP**.

6.8 Нажмите кнопку **Сохранить и применить**.

7 Перейдите на страницу **Межсетевой экран** > **NAT**.

8 Нажмите кнопку **Добавить**. Откроется страница добавления правила трансляции адресов.

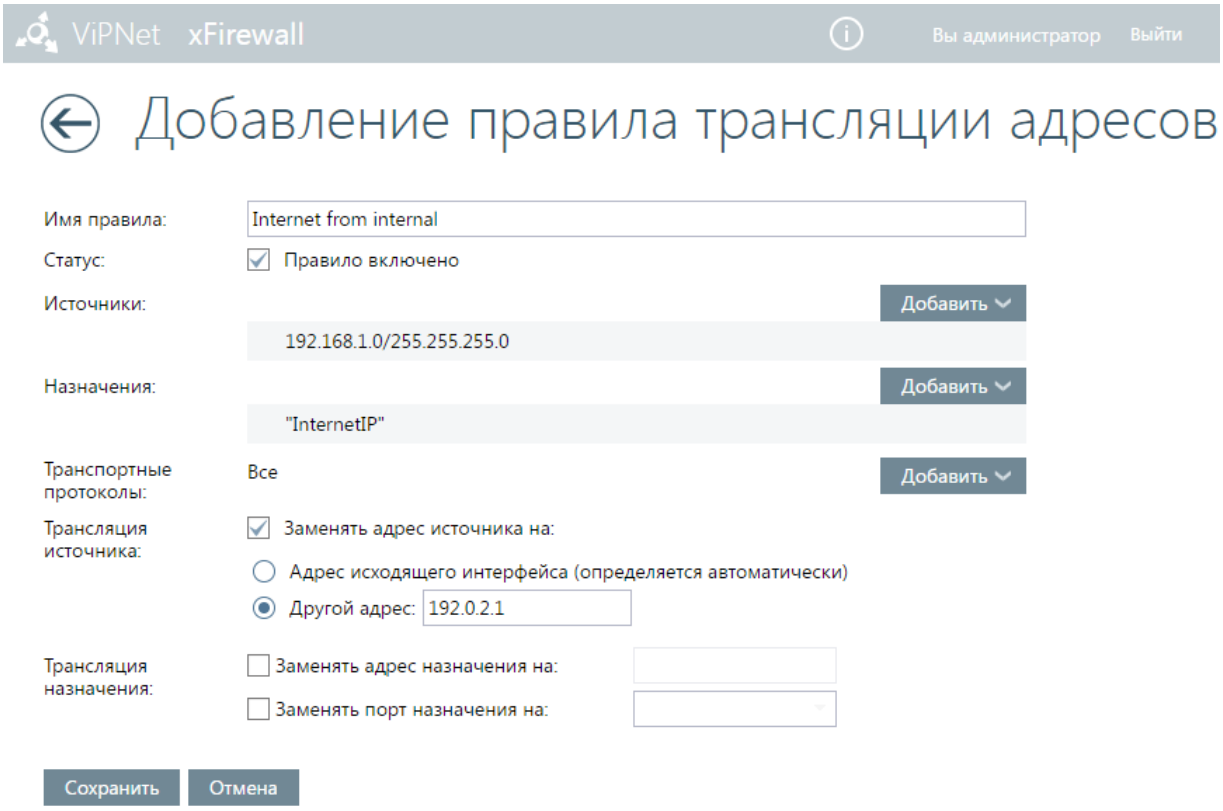

Рисунок 59. Добавление правила трансляции адресов для демилитаризованной зоны

9 На странице **Добавление правила трансляции адресов** выполните следующие действия:

9.1 Напротив параметра **Статус** установите флажок **Правило включено**.

9.2 Напротив параметра **Источники** нажмите кнопку **Добавить** и выберите в качестве источника **IP-адрес или диапазон IP-адресов**.

9.3 В появившемся диалоговом окне (см. Рисунок 54 на стр. 94) в списке **Тип адреса** выберите **IP-подсеть** и в соответствующем поле задайте подсеть `192.168.1.0/24`. Нажмите кнопку **Сохранить**.

9.4 Напротив параметра **Назначения** нажмите кнопку **Добавить** и выберите в качестве назначения **Группа IP-адресов**.

9.5 В появившемся диалоговом окне (см. Рисунок 55 на стр. 95) выберите группу **InternetIP** и нажмите кнопку **Сохранить**.

9.6 На странице добавления правила трансляции адресов установите флажок **Заменять адрес источника на** и выберите **Другой адрес**.

9.7 В появившемся поле задайте адрес `192.0.2.1`.

9.8 Нажмите кнопку **Сохранить**.

10 На странице **Межсетевой экран > NAT** нажмите кнопку **Добавить.** Откроется страница добавления правила трансляции адресов.

11 На странице **Добавление правила трансляции адресов** выполните следующие действия:

11.1 Напротив параметра **Статус** установите флажок **Правило включено**.

11.2 Напротив параметра **Источники** нажмите кнопку **Добавить** и выберите в качестве источника **Группа IP-адресов**.

11.3 В появившемся диалоговом окне выберите группу **InternetIP** и нажмите кнопку **Сохранить**.

11.4 Напротив параметра **Назначения** нажмите кнопку **Добавить** и выберите в качестве назначения **IP-адрес или диапазон IP-адресов**.

11.5 В появившемся диалоговом окне задайте IP-адрес `192.0.2.1` и нажмите кнопку **Сохранить**.

11.6 Напротив параметра **Транспортные протоколы** нажмите кнопку **Добавить** и выберите протокол **TCP/UDP**.

11.7 В появившемся диалоговом окне выберите протокол TCP и в списке **Назначение** номер порта **80-http**. Нажмите кнопку **Сохранить**.

11.8 Напротив пункта **Трансляция назначения** установите флажок **Заменять адрес назначения на** и выберите вариант **Другой адрес**.

11.9 В появившемся поле задайте адрес `192.168.2.10`. Нажмите кнопку **Сохранить**.

В результате пользователи локальной сети смогут обращаться к веб-серверу по его внутреннему адресу 192.168.2.10, а внешние пользователи — по внешнему адресу ViPNet xFirewall 192.0.2.1. Пользователи локальной сети также будут иметь доступ в Интернет, при этом их компьютеры будут защищены от атак из Интернета.

Настройка параметров прокси-сервера

С помощью встроенного прокси-сервера ViPNet xFirewall вы можете организовать фильтрацию HTTP-трафика между внешней сетью и узлами локальной сети. При фильтрации трафика выполняются следующие проверки:

- Проверка соответствия IP-пакетов MIME-типу или HTTP-методу.
- Антивирусная проверка встроенным антивирусом KAV4Proxy или внешним антивирусом по протоколу ICAP.

На рисунке ниже представлена схема фильтрации HTTP-трафика прокси-сервером ViPNet xFirewall.

Рисунок 60. схема фильтрации HTTP-трафика прокси-сервером ViPNet xFirewall

При обращении пользователя локальной сети к какому-либо интернет-ресурсу по протоколу HTTP (транспортный протокол TCP, порт 80) запрос обрабатывается встроенным прокси-сервером ViPNet xFirewall, при условии, что прокси-сервер включен. Обработка запроса прокси-сервером происходит следующим образом:

1 Запрос от пользователя локальной сети поступает на прокси-сервер ViPNet xFirewall:

- Если на прокси-сервере включена функция контент-фильтрации содержимого трафика, то запрос обрабатывается ее правилами:
  - если ни одно правило не сработало для данного типа содержимого HTTP-трафика, то применяется правило по умолчанию (блокирующее или разрешающее);
  - если для данного типа содержимого трафика сработало запрещающее правило, то передача данных этого типа содержимого блокируется.

- Если на прокси-сервере включена антивирусная проверка трафика, данные проверяются на наличие вирусов. Если пользователь попытается отправить файл, в котором обнаружен вирус, то попытка отправки файла будет заблокирована. Запись об этом событии будет создана в системном журнале (см. Записи в журнале событий, связанные с аутентификацией и настройкой оборудования на стр. 181).

2 Если запрос не был заблокирован при фильтрации содержимого трафика или при проверке антивирусом, он передается на интернет-ресурс.

3 Ответ от интернет-ресурса поступает на прокси-сервер ViPNet xFirewall:

- Если на прокси-сервере включена функция контент-фильтрации содержимого трафика, то ответ обрабатывается ее правилами аналогично п. 1.
- Если на прокси-сервере включена антивирусная проверка трафика, данные проверяются на наличие вирусов. Если пользователь попытается загрузить файл (в том числе открыть HTML-страницу), в котором был обнаружен вирус, он увидит соответствующее сообщение от антивируса и попытка загрузки файла будет заблокирована. Запись об этом событии будет создана в системном журнале (см. Записи в журнале событий, связанные с аутентификацией и настройкой оборудования на стр. 181).

4 В случае успешного прохождения всех проверок трафик от прокси-сервера передается пользователю.

Настройка основных параметров прокси-сервера

Если вы хотите использовать встроенный прокси-сервер для защиты вашей локальной сети, настройте основные параметры прокси-сервера. Вы также можете включить фильтрацию содержимого и антивирусную проверку трафика. Для получения более подробной информации см. разделы Настройка фильтрации содержимого трафика и Настройка антивирусной проверки (на стр. 107).

Настройка основных параметров предполагает выбор внешнего сетевого интерфейса сервера, задание IP-адресов, на которых прокси-сервер будет принимать запросы от пользователей (прослушивать их), и IP-адресов локальных сетей, которым разрешено использовать прокси-сервер.

Прокси-сервер ViPNet xFirewall работает в «прозрачном» режиме (см. глоссарий, стр. 205), поэтому дополнительная настройка приложений на стороне пользователей не требуется. Направление пользовательского трафика на ViPNet xFirewall, который выполняет роль прокси-сервера, должно обеспечиваться за счет маршрутизации в локальной сети.

Примечание. При настройке параметров прокси-сервера в файле конфигурации межсетевого экрана автоматически создаются необходимые сетевые фильтры и правила трансляции адресов.

Чтобы настроить основные параметры прокси-сервера, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 На начальной странице щелкните плитку **Межсетевой экран**.

3 Перейдите на страницу **Прокси-сервер** > **Общие настройки**.

4 В группе **Основные параметры** выполните следующие действия:

- В списке **Внешний сетевой интерфейс** выберите сетевой интерфейс, подключенный к Интернету.
- В поле **Размер кэша** укажите размер кэша прокси-сервера. Напротив этого поля указан объем свободного места на диске. Кэш используется для хранения копии данных, к которым часто обращаются пользователи.
- Нажмите кнопку **Сохранить**.

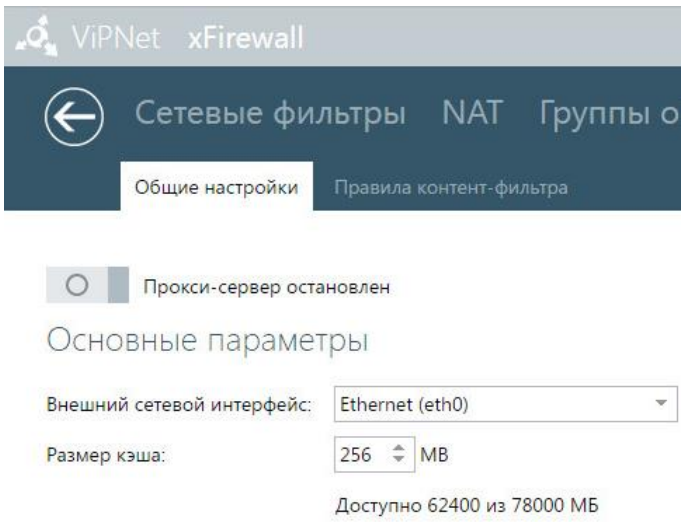

Рисунок 61. Настройка основных параметров прокси-сервера

5 В группе **Прослушиваемые адреса** задайте IP-адреса и порты, которые прокси-сервер должен использовать, чтобы принимать запросы пользователей. Для этого нажмите кнопку **Добавить** и в появившемся списке выберите IP-адрес, а также укажите номер порта для прослушивания. Затем нажмите кнопку **Сохранить**.

Рисунок 62. Задание прослушиваемых IP-адресов

Внимание! Мы рекомендуем задавать для прослушивания сетевые интерфейсы со статическими IP-адресами. После изменения IP-адресов сетевых интерфейсов необходимо завершить работу прокси-сервера, задать текущие IP-адреса интерфейсов,

использующихся для организации соединения, а затем снова запустить прокси-сервер.

6 Чтобы запустить прокси-сервер, щелкните переключатель в верхней части страницы. Состояние прокси-сервера отображается напротив переключателя.

Внимание! Перед запуском прокси-сервера необходимо задать IP-адрес и порт для прослушивания, а также внешний сетевой интерфейс ViPNet xFirewall.

При запуске прокси-сервера будут автоматически сформированы сетевые фильтры и правила трансляции адресов, необходимые для доступа в Интернет через прокси-сервер для узлов защищенной и открытой сети. При завершении работы прокси-сервера правила автоматически удаляются, при повторном запуске правила формируются заново.

После первого запуска использование прокси-сервера будет разрешено для IP-адресов локальных сетей, входящих в пользовательскую группу объектов `HttpProxyUsers` (см. Пользовательские группы объектов по умолчанию на стр. 64). По умолчанию в эту группу входят те же IP-адреса, что и в пользовательскую группу объектов `PrivateNetworkIP` (10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16).

Внимание! Пользовательская группа объектов `HttpProxyUsers` автоматически создается при первом запуске прокси-сервера.

Чтобы добавить или удалить IP-адреса из списка локальных сетей, которым разрешено использовать прокси-сервер, остановите сервер, затем измените группу объектов `HttpProxyUsers` (см. Создание и изменение группы объектов на стр. 65) и вновь запустите прокси-сервер.

Внимание! Если для подключения к Интернету ViPNet xFirewall использует маршрут с несколькими шлюзами (multi-hop route), для корректной работы прокси-сервера на ViPNet xFirewall создайте фильтр открытой сети со следующими параметрами:

- Действие: **Пропускать трафик**.
- Источники: **Мой узел**.
- Назначения: **Группа IP-адресов** > **InternetIP**, флажок **Все объекты, кроме "PivateNetworkIP"**.
- Протоколы: TCP: 21, TCP: 80, TCP: 443.

Подробнее о создании сетевых фильтров см. в разделе Создание и изменение сетевого фильтра (на стр. 74).

Настройка правил фильтрации трафика

Вы можете настраивать правила контент-фильтрации трафика, проходящего через прокси-сервер ViPNet xFirewall.

Настройка правил фильтрации выполняется при остановленном прокси-сервере в режиме администратора. Чтобы остановить прокси-сервер, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 На начальной странице щелкните плитку **Межсетевой экран**.

3 Перейдите на страницу **Прокси-сервер** > **Правила контент-фильтра**.

4 Остановите прокси-сервер с помощью переключателя в правой верхней части страницы. Состояние прокси-сервера отображается напротив переключателя.

Чтобы создать новое правило фильтрации, выполните следующие действия:

1 Нажмите кнопку **Добавить.** В открывшемся окне **Пользовательские правила** задайте параметры правила.

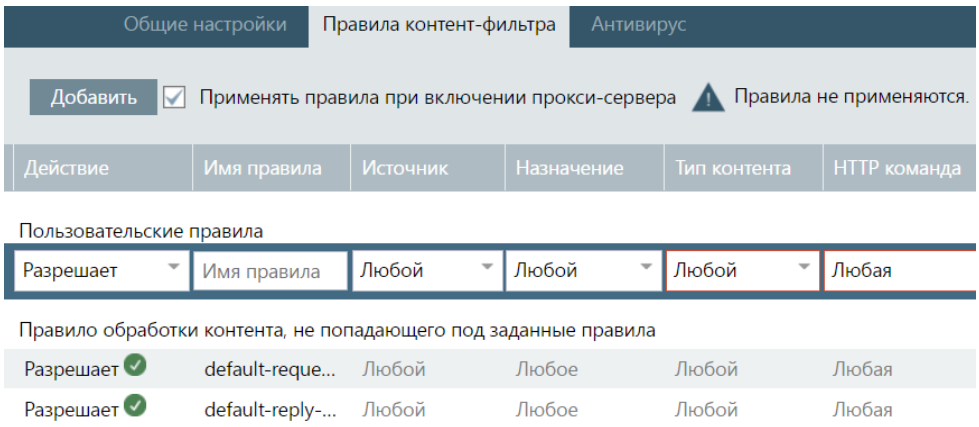

Рисунок 63. Добавление правила фильтрации

2 Нажмите кнопку  для сохранения правила или кнопку  для отмены.

Чтобы изменить существующее правило фильтрации, выполните следующие действия:

1 Наведите курсор на строку с правилом, которое вы хотите отредактировать и нажмите кнопку  справа. В открывшемся окне **Пользовательские правила** задайте параметры правила.

2 Нажмите кнопку  для сохранения правила или кнопку  для отмены.

Чтобы удалить существующее правило фильтрации, выполните следующие действия:

1 Наведите курсор на строку с правилом, которое вы хотите удалить и нажмите кнопку  справа.

2 В открывшемся окне подтверждения нажмите кнопку **OK** для удаления правила или кнопку **Отмена**.

Чтобы изменить порядок пользовательских правил в таблице, перетащите правило вверх или вниз.

По завершении операций по созданию или редактированию правил фильтрации запустите прокси-сервер с помощью переключателя в правой верхней части страницы. Состояние прокси-сервера отображается напротив переключателя.

Пример настройки фильтрации трафика

Чтобы с помощью прокси-сервера запретить загрузку на сетевые узлы исполняемых файлов с расширением `.exe`, выполните следующие действия:

1 Перейдите на страницу **Межсетевой экран** > **Прокси-сервер** > **Правила контент-фильтра** и остановите работу прокси-сервера с помощью переключателя в правой верхней части страницы.

2 Создайте правило фильтрации содержимого трафика прокси-сервера, которое будет блокировать загрузку исполняемых файлов с расширением `.exe`:

2.1 Нажмите кнопку **Добавить**. Появится форма добавления правила фильтрации содержимого трафика.

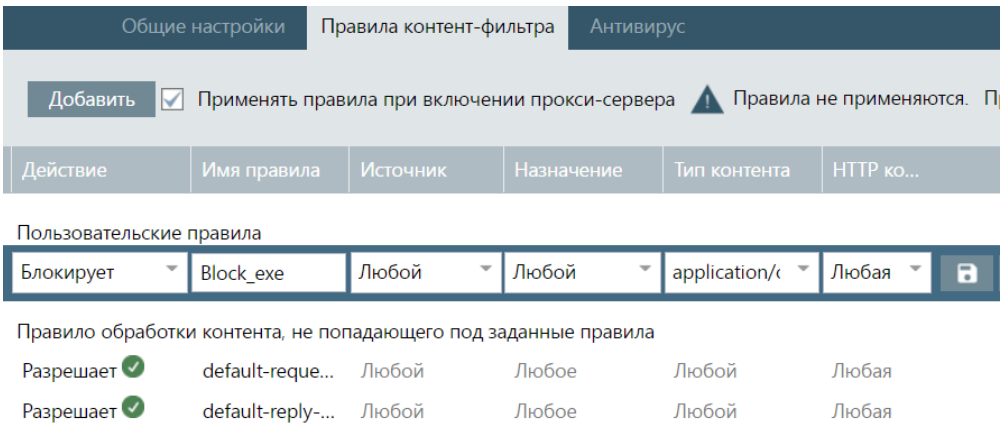

Рисунок 64. Создание правила фильтрации block.exe

2.2 В поле **Имя правила** задайте название правила `Block_exe`.

2.3 В списке **Действие** выберите **Блокирует**.

2.4 В списке **Тип контента** выберите тип **application** > **octet-stream**.

2.5 В списке **Источник**, **Назначение** и **HTTP-команда** оставьте значение по умолчанию.

Внимание! Контентный фильтр прокси-сервера работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса назначения доменного имени узла фильтрация будет осуществляться только по доменному имени, а при использовании IP-адреса узла, только по IP-адресу, без взаимного разрешения DNS-имя — IP-адрес.

2.6 Нажмите кнопку  .

2.7 Запустите прокси-сервер с помощью переключателя в правой верхней части экрана.

В результате применения правила `Block_exe` будет запрещена загрузка исполняемых файлов с расширением `.exe` на узлы сети.

Настройка антивирусной проверки

Если ViPNet xFirewall используется в качестве прокси-сервера, вы можете настроить антивирусную проверку данных, передаваемых через прокси-сервер по протоколу HTTP в обоих направлениях: из Интернета к пользователю и от пользователя в Интернет (например, при добавлении вложения в сообщение электронной почты, используя веб-интерфейс).

Антивирусная проверка осуществляется либо с помощью встроенного антивируса KAV4Proxy, либо с помощью внешнего антивируса по протоколу ICAP (см. глоссарий, стр. 201).

Внимание! Для фильтрации трафика встроенным антивирусом KAV4Proxy и обновления антивирусной базы необходимо установить лицензионный ключ антивируса (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора).

Настройка встроенного антивируса KAV4Proxy

Для настройки параметров встроенного антивируса KAV4Proxy выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора.
2. На начальной странице щелкните плитку **Межсетевой экран,** далее перейдите на страницу **Прокси-сервер** > **Общие настройки**. С помощью переключателя состояния остановите прокси-сервер.
3. Перейдите на страницу **Антивирус**.

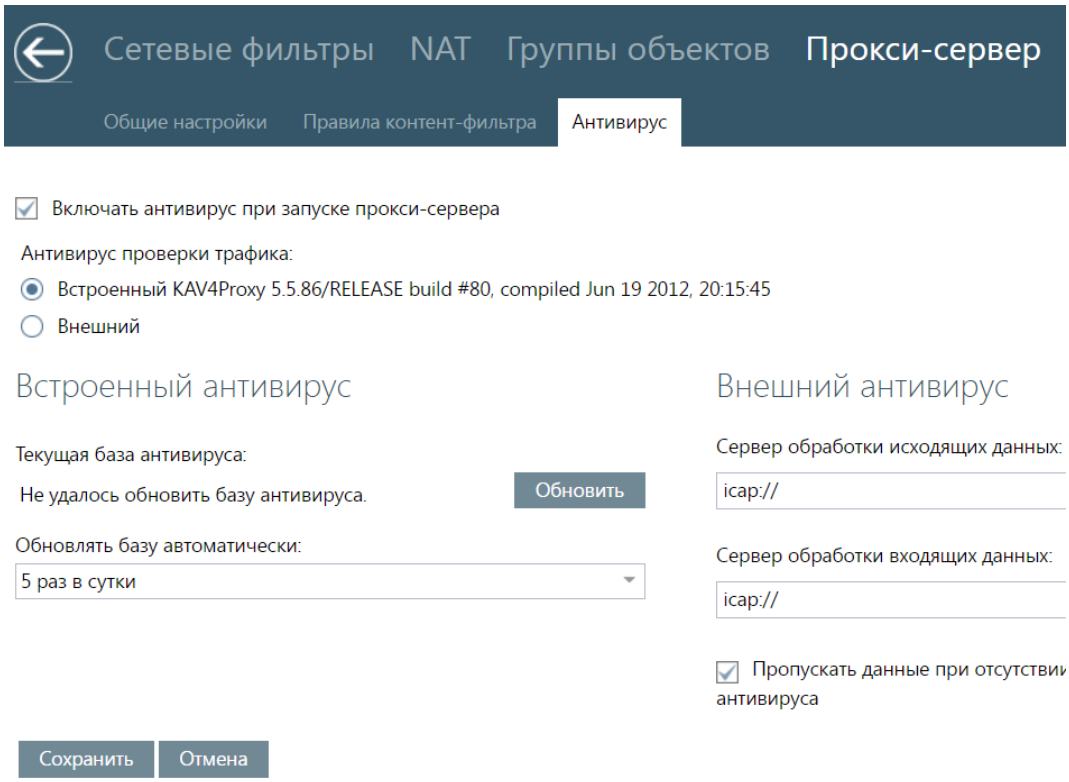

Рисунок 65. Настройка встроенного антивируса KAV4Proxy

4 Установите флажок **Включать антивирус при запуске прокси-сервера**.

5 Установите переключатель **Антивирус проверки трафика** в положение **Встроенный KAV4Proxy**.

6 В разделе **Встроенный антивирус** выберите из списка **Обновлять базу автоматически** периодичность обновления.

7 Нажмите кнопку **Сохранить**.

8 Перейдите на страницу **Общие настройки** и с помощью переключателя состояния запустите прокси-сервер. Дождитесь запуска прокси-сервера.

9 Вернитесь на страницу **Антивирус**. Для обновления базы антивируса до актуального состояния нажмите кнопку **Обновить**.

Внимание! Обновление антивирусных баз возможно только при наличии действующей лицензии антивируса. Если вы не установили лицензионный ключ или срок действия ключа истек, установите лицензионный ключ с помощью командного интерпретатора (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», раздел «Настройка встроенного антивируса KAV4Proxy»).

В результате выполнения действий встроенный антивирус KAV4Proxy будет выполнять проверку трафика, передаваемого через прокси-сервер.

Примечание. При попытке отправить зараженный файл, передача файла будет заблокирована антивирусом KAV4Proxy и будет создана запись о событии в системном журнале. При этом сообщение пользователю о блокировке передачи файла не выводится.

Настройка внешнего антивируса

Для настройки параметров внешнего антивируса выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 На начальной странице щелкните плитку **Межсетевой экран**, далее перейдите на страницу **Прокси-сервер** > **Общие настройки**. С помощью переключателя состояния остановите прокси-сервер.

3 Перейдите на страницу **Антивирус**.

4 Установите флажок **Включать антивирус при запуске прокси-сервера**.

5 Установите переключатель **Антивирус проверки трафика** в положение **Внешний**.

6 В разделе **Внешний антивирус** задайте путь к **Сервер обработки исходящих данных** и **Сервер обработки входящих данных** в формате icap://адрес[:порт]/.

Внимание! В конце адреса ICAP-сервера необходимо указать символ «/». Если не указано значение параметра `порт`, то будет использоваться значение по умолчанию 1344.

7 Чтобы пропускать трафик через прокси-сервер в случае недоступности ICAP-сервера антивируса, установите флажок **Пропускать данные при отсутствии связи с сервером антивируса**. Чтобы блокировать трафик в случае недоступности ICAP-сервера антивируса, снимите этот флажок.

8 Нажмите кнопку **Сохранить**.

9 Перейдите на страницу **Общие настройки** и с помощью переключателя состояния запустите прокси-сервер. Дождитесь запуска прокси-сервера.

На рисунке ниже приведен пример настройки внешнего антивируса.

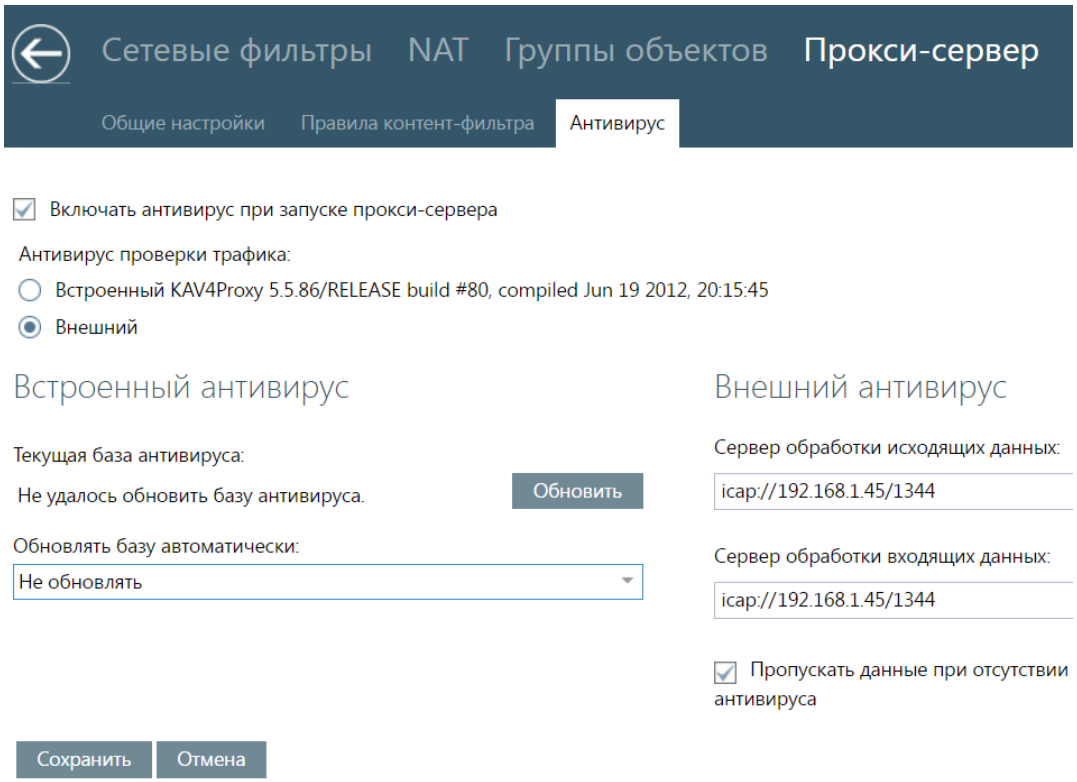

Рисунок 66. Пример настройки внешнего антивируса

Антивирус работает на ICAP- сервере с IP-адресом 192.168.1.45 и портом по умолчанию 1344. При недоступности ICAP- сервера трафик пропускается прокси-сервером без антивирусной фильтрации.

Настройка взаимодействия с Active Directory

Если вы хотите использовать имена пользователей при создании транзитных фильтров открытой сети и данные пользователей хранятся на контроллере домена Active Directory (см. глоссарий, стр. 200) вашей сети, то вам необходимо настроить взаимодействие ViPNet xFirewall с контроллером домена. ViPNet xFirewall поддерживает контроллеры домена, работающие на следующих операционных системах:

- Windows Server 2012 R2 (английская и русская версии);
- Windows Server 2008 R2 (английская и русская версии).

Чтобы настроить взаимодействие ViPNet xFirewall с контроллером домена Active Directory, выполните следующие действия:

1. Настройте учетную запись технологического пользователя (см. Настройка учетной записи технологического пользователя на контроллере домена на стр. 111) на контроллере домена.
2. На ViPNet xFirewall настройте взаимодействие с контроллером домена (см. Настройка взаимодействия с контроллером домена на стр. 112).

Настройка учетной записи технологического пользователя на контроллере домена

Для корректного взаимодействия контроллера домена с ViPNet xFirewall создайте на контроллере домена учетную запись технологического пользователя с произвольным именем.

Учетная запись технологического пользователя должна входить в следующие группы:

- **Читатели журнала событий** (**Event Log Readers**).
- **Пользователи DCOM** (**Distributed COM Users**).
- **Операторы сервера** (**Server Operators**).

Примечание. Учетная запись технического пользователя может не обладать правами Администратора домена.

Кроме того, для учетной записи технологического пользователя необходимо выполнить следующие настройки инфраструктуры управления Windows (WMI):

1. Добавьте учетную запись в следующие разделы инфраструктуры WMI:
   - `Root/CIMV2`;

- `Root/directory/LDAP`.

2 В свойствах учетной записи установите флажки напротив следующих полномочий:

- **Enable Account** (**Включить учетную запись**).
- **Remote Enable** (**Включить удаленно**).

Настройка взаимодействия с контроллером домена

Чтобы настроить взаимодействие ViPNet xFirewall с Active Directory, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Межсетевой экран** > **Пользователи** > **Active Directory**.

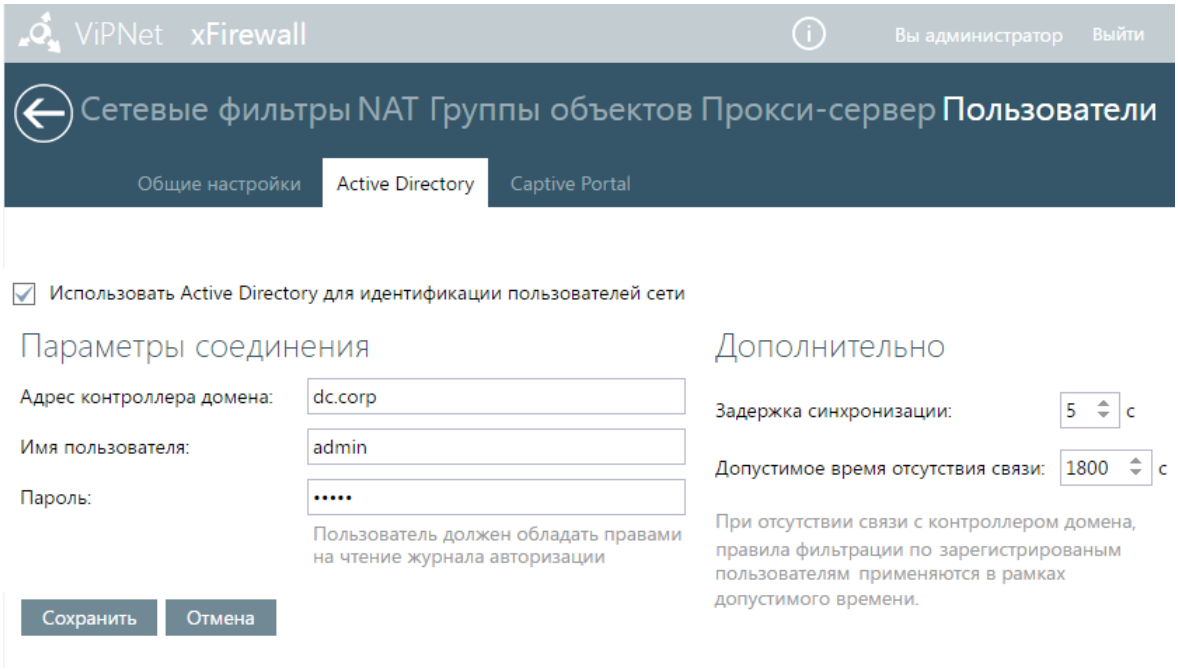

Рисунок 67. Настройка подключения к серверу Active Directory

3 Установите флажок **Использовать Active Directory для идентификации пользователей сети**.

4 В соответствующих полях задайте значения параметров:

- адрес контроллера домена Active Directory — IP-адрес или доменное имя сетевого узла, выполняющего роль контроллера домена.

Примечание. Доменное имя может содержать символы `A-z`, `0-9`, «-» и «`.`».

- имя учетной записи технологического пользователя (см. Настройка учетной записи технологического пользователя на контроллере домена на стр. 111).

Примечание. В имени пользователя вы можете использовать любые символы, кроме:
`" / \ [ ] : ; | = , + * ? < >`
В имени пользователя не учитывается регистр.

После задания имени пользователя введите его пароль.

5 При необходимости измените значения по умолчанию для параметров:

- **Задержка синхронизации —** период получения журнала контроллера домена (по умолчанию — 5 секунд). От значения этого параметра зависит, как часто ViPNet xFirewall будет запрашивать список активных пользователей домена.
- **Допустимое время отсутствия связи —** время жизни кэша пользовательских сессий (по умолчанию — 1800 секунд). От значения этого параметра зависит, сколько времени будут активны сессии пользователей Active Directory в ViPNet xFirewall при отсутствии связи с контроллером домена. Если по истечении заданного времени связь с контроллером домена не будет восстановлена, то:
  - кэш пользовательских сессий будет сброшен;
  - пользователи Active Directory не будут отображаться в списке активных пользователей (см. Просмотр списка пользователей на стр. 121);
  - транзитные фильтры открытой сети, в которых задан хотя бы один из пользователей Active Directory, будут показываться как активные, но не будут применяться.

6 Нажмите кнопку **Сохранить**.

7 Чтобы включить добавление в системный журнал записей о событиях, связанных с обменом данными между ViPNet xFirewall и контроллером домена, выполните следующие действия:

7.1 Перейдите на страницу **Межсетевой экран** > **Пользователи** > **Общие настройки**.

7.2 Установите флажок **Вести журнал событий** и в соответствующем поле задайте минимальный уровень событий, для которых необходимо добавлять записи в журнал.

Настройка взаимодействия с LDAP-сервером

В ряде случаев реализация политики безопасного доступа пользователей из внутренней сети компании к интернет-ресурсам с использованием аутентификации в службе каталогов Active Directory невозможна:

- в IT-инфраструктуре компании не используется служба каталогов Active Directory;
- сотрудники компании используют мобильные устройства с ОС iOS и Android, которые не могут быть аутентифицированы в Active Directory.

Тогда для аутентификации пользователей, в том числе подключающихся к корпоративной сети с мобильных устройств, используется сервис Captive portal, встроенный в ViPNet xFirewall. Сервис Captive portal работает совместно с LDAP-сервером.

Внимание! Для реализации аутентификации пользователей через сервис Captive portal в локальной сети компании должен быть установлен LDAP-сервер, поддерживающий LDAP-каталог.

Аутентификация пользователей с помощью Captive portal выглядит следующим образом:

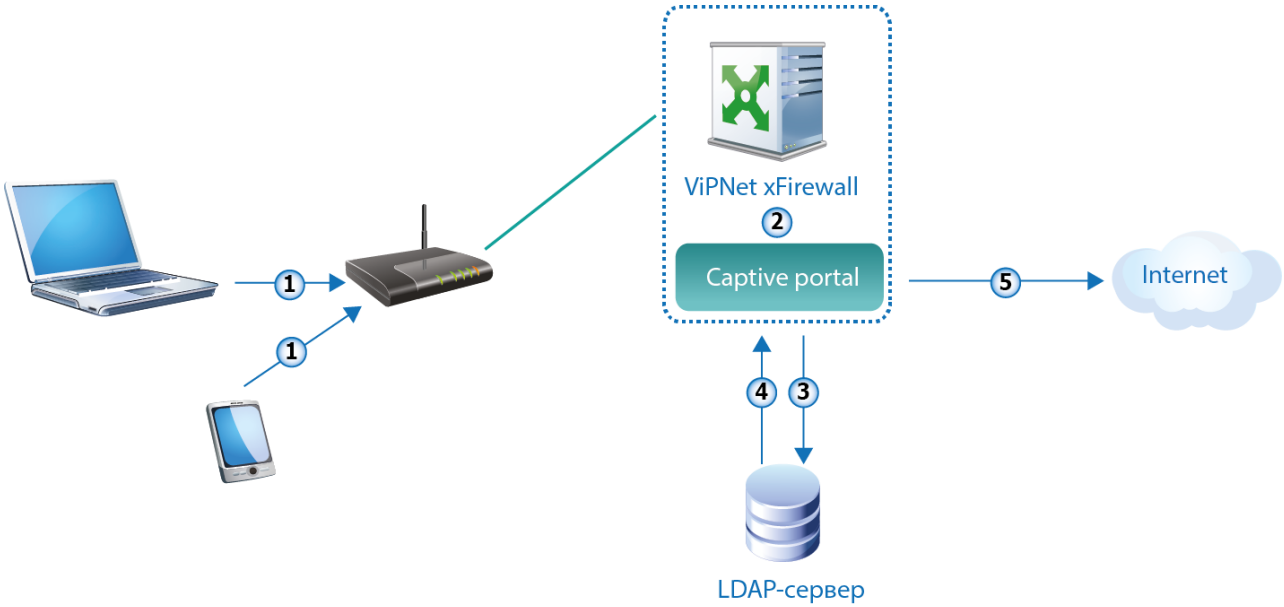

Рисунок 68. Схема аутентификации пользователей с помощью Captive portal

1 Пользователь подключается к внутренней сети (например, через точку доступа Wi-Fi, подключенную к ViPNet xFirewall) и отправляет запрос на внешний веб-ресурс.

2 ViPNet xFirewall переадресует запрос пользователя на страницу аутентификации Captive portal.

3 Пользователь вводит логин и пароль, Captive portal отправляет запрос на LDAP-сервер для проверки данных учетной записи пользователя.

4 LDAP-сервер отправляет на Captive portal результат проверки учетных данных пользователя.

5 Если проверка пользователя на LDAP-сервере прошла успешно, то пользователь видит на странице Captive portal ссылку для перехода на запрошенный веб-ресурс.

Примечание. Captive portal определяет пользователей по их уникальным IP-адресам и поэтому не сможет определить пользователей, которые находятся за NAT с трансляцией адреса источника.

Пример настройки взаимодействия с LDAP-сервером

В этом примере рассматривается задание следующих параметров взаимодействия с LDAP-сервером:

- Адрес LDAP-сервера: `192.168.203.155`;
- Выделенное имя (DN, Distinguished Name) учетной записи администратора LDAP-сервера: uid=`admin,ou=People,dc=example`;
- Выделенное имя (DN, Distinguished Name) базы поиска: `example`;
- Режим подключения к LDAP-серверу: Start TLS.

Для Captive portal рассматривается задание следующих параметров:

- Время жизни сессии пользователя (время, по истечении которого сессия пользователя будет завершена): 12 часов.
- Время неактивности пользователя (время отсутствия передачи данных со стороны пользователя, по истечении которого сессия пользователя будет завершена): 30 минут.
- Название сети, отображаемое на веб-странице Captive portal: `Guest Network`.

Чтобы настроить взаимодействие Captive portal с LDAP-сервером, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 7. Порядок действий для настройки взаимодействия Captive portal с LDAP-сервером

	Действие	Ссылка
☐	Создайте запросы на локальный сертификат веб-сервера Captive portal.	Получение и импорт сертификатов (на стр. 116)

	Действие	Ссылка
☐	Обратитесь в удостоверяющий центр для получения локального сертификата веб-сервера Captive portal, корневого сертификата LDAP-сервера и списка аннулированных сертификатов (CRL).	
☐	Импортируйте сертификаты и список аннулированных сертификатов в локальное хранилище сертификатов ViPNet xFirewall.	
☐	Настройте параметры подключения Captive portal к LDAP-серверу.	Настройка параметров Captive portal (на стр. 119)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Получение и импорт сертификатов

Перед тем как настроить Captive portal, вам необходимо импортировать в локальное хранилище сертификатов ViPNet xFirewall следующие объекты:

- Корневой сертификат удостоверяющего центра, выпустившего сертификат LDAP-сервера (см. глоссарий, стр. 201). Этот сертификат необходим для проверки подлинности сертификата LDAP-сервера. Вы можете загрузить корневой сертификат с сайта удостоверяющего центра (адрес сайта указан в сертификате LDAP-сервера).
- Сертификат веб-сервера Captive portal. Этот сертификат обеспечивает защиту данных (логина и пароля), которые пользователь передает при авторизации на Captive portal. Для получения этого сертификата создайте запрос на сертификат в формате PKCS#12 (см. глоссарий, стр. 202) и передайте его в удостоверяющий центр (см. глоссарий, стр. 206). В ответ на запрос вы получите в удостоверяющем центре сертификат веб-сервера Captive portal.

Примечание. Вы можете создать запрос на сертификат в формате PKCS#12 не только с помощью ViPNet xFirewall, но и с помощью других программных средств. Если вы уже создали запрос на сертификат, выполните действия, начиная с пункта 7.

Обратите внимание, что в этом случае вам необходимо импортировать в ViPNet xFirewall не только сертификат, но и закрытый ключ, которым подписан сертификат.

Для получения и импорта сертификатов в локальное хранилище ViPNet xFirewall выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Управляющие соединения** > **CA**.

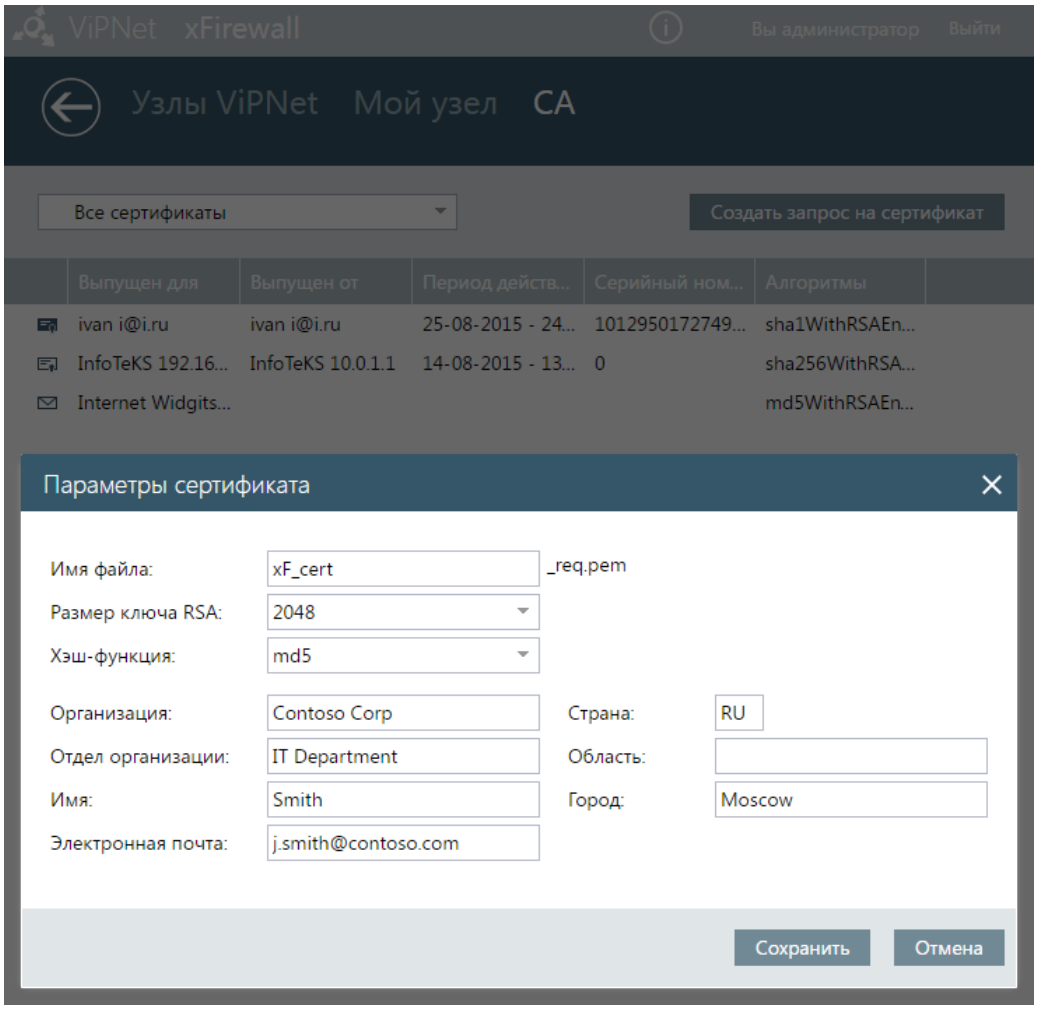

Рисунок 69. Создание запроса на сертификат

3 Для создания запроса на сертификат веб-сервера Captive portal нажмите кнопку **Создать запрос на сертификат**.

4 В окне **Параметры сертификата** заполните необходимые поля:

- имя файла запроса;
- размер ключа RSA: 2048;
- алгоритм хэширования: MD5.

5 Нажмите кнопку **Сохранить**.

6 Созданный запрос на сертификат появится в списке. Чтобы загрузить файл запроса, нажмите кнопку .

7 Обратитесь в удостоверяющий центр (см. глоссарий, стр. 206) и получите сертификат веб-сервера Captive portal.

8 Скопируйте сертификат веб-сервера Captive portal и корневой сертификат удостоверяющего центра, выдавшего сертификат LDAP-сервера на USB-носитель и импортируйте их в локальное хранилище сертификатов ViPNet xFirewall. Для этого выполните следующие действия:

8.1 Перейдите на страницу **Управляющие соединения** > **CA**.

8.2 Нажмите кнопку **Импортировать**.

8.3 В открывшемся окне нажмите кнопку **Загрузить файл**, выберите файл на USB-носителе и нажмите кнопку **Открыть**.

8.4 В открывшемся окне нажмите кнопку **Импортировать**.

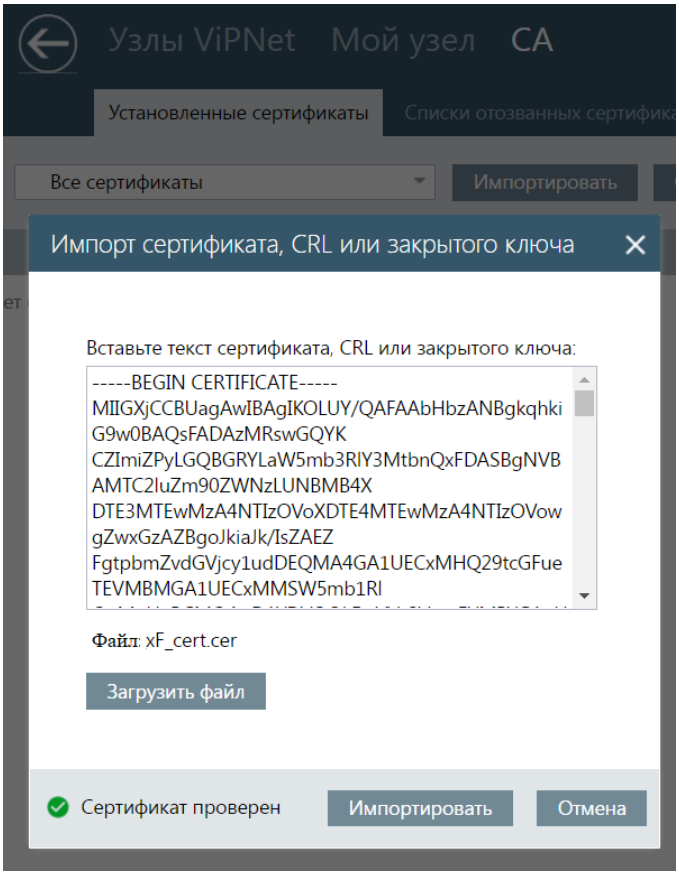

Рисунок 70. Импорт сертификата

Примечание. При настройке ViPNet xFirewall с помощью веб-интерфейса вы можете импортировать только сертификаты в кодировке Base64 (см. глоссарий, стр. 200), подписанные открытым ключом RSA.

Если вы создавали запрос на сертификат Captive portal не с помощью ViPNet xFirewall, то в этом случае также импортируйте закрытый ключ сертификата Captive portal.

Внимание! Корневой сертификат удостоверяющего центра, выдавшего сертификат веб-сервера Captive portal и список аннулированных сертификатов этого удостоверяющего центра необходимо импортировать на ПК пользователей, проходящих аутентификацию через Captive portal.

После выполнения описанных действий вы сможете настроить параметры Captive portal (см. Настройка параметров Captive portal на стр. 119).

Настройка параметров Captive portal

После того, как вы импортировали необходимые сертификата в локальное хранилище ViPNet xFirewall (см. Получение и импорт сертификатов на стр. 116), вы можете настроить параметры взаимодействия Captive portal с LDAP-сервером. Для этого выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Межсетевой экран** > **Пользователи** > **Captive portal**.

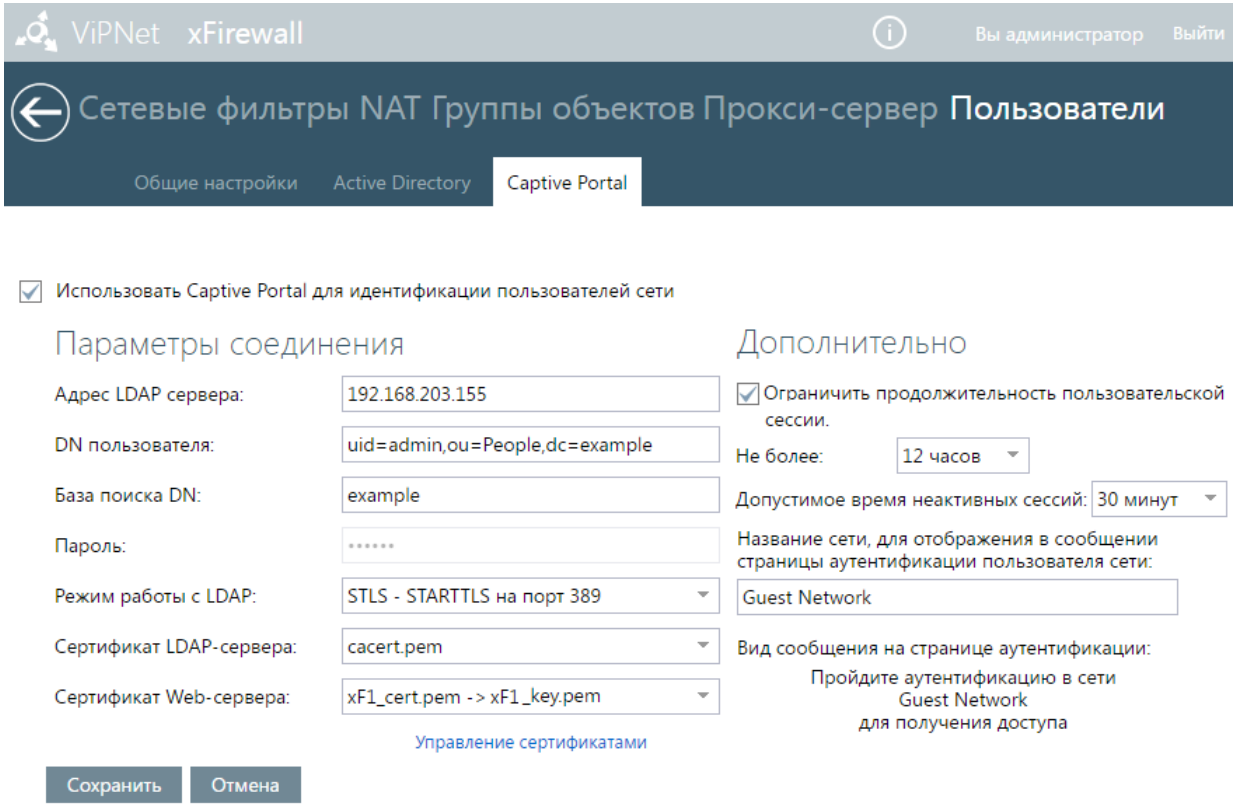

Рисунок 71. Настройка параметров Captive portal

3 В соответствующих полях задайте основные параметры подключения к Captive portal:

- Адрес LDAP-сервера.
- Выделенное имя (DN, Distinguished Name) (https://tools.ietf.org/html/rfc4514) учетной записи администратора LDAP-сервера, которая обладает правами на чтение записей LDAP-сервера.
- Выделенное имя (DN, Distinguished Name) базы поиска, от которой начинаются операции поиска в LDAP-каталоге.

Внимание! Для удобства настройки параметров **DN пользователя** и **База поиска DN** вы можете воспользоваться контекстной справкой, появляющейся при наведении указателя мыши в поле параметра.

- Режим соединения с LDAP-сервером.

4 Выберите из соответствующих списков корневой сертификат удостоверяющего центра, выдавшего сертификат LDAP-сервера и сертификат веб-сервера Captive portal.

Внимание! Если вы выбрали сертификат веб-сервера Captive portal и хотите отказаться от его использования, то вам необходимо сбросить настройки Captive portal, выполнив следующие действия:

1 Снимите флажок **Использовать Captive portal для идентификации пользователей сети** и нажмите кнопку **Сохранить**.

2 Снова установите флажок и нажмите кнопку **Сохранить**.

Если вы удалили сертификат веб-сервера Captive portal и не хотите использовать вместо него другой сертификат, то в этом случае также необходимо сбросить настройки Captive portal.

---

5 Задайте имя гостевой сети, которое пользователи будут видеть на странице авторизации Captive portal.

6 Нажмите кнопку **Сохранить**.

После выполнения описанных действий на вашем ViPNet xFirewall будет работать авторизация пользователей с помощью Captive portal, и вы сможете предоставлять безопасный доступ в Интернет, в т.ч. и для мобильных устройств.

Просмотр списка пользователей

Чтобы просмотреть список активных пользователей Active Directory (см. глоссарий, стр. 200) и Captive portal (см. глоссарий, стр. 200), перейдите на страницу **Межсетевой экран** > **Пользователи** > **Общие настройки**.

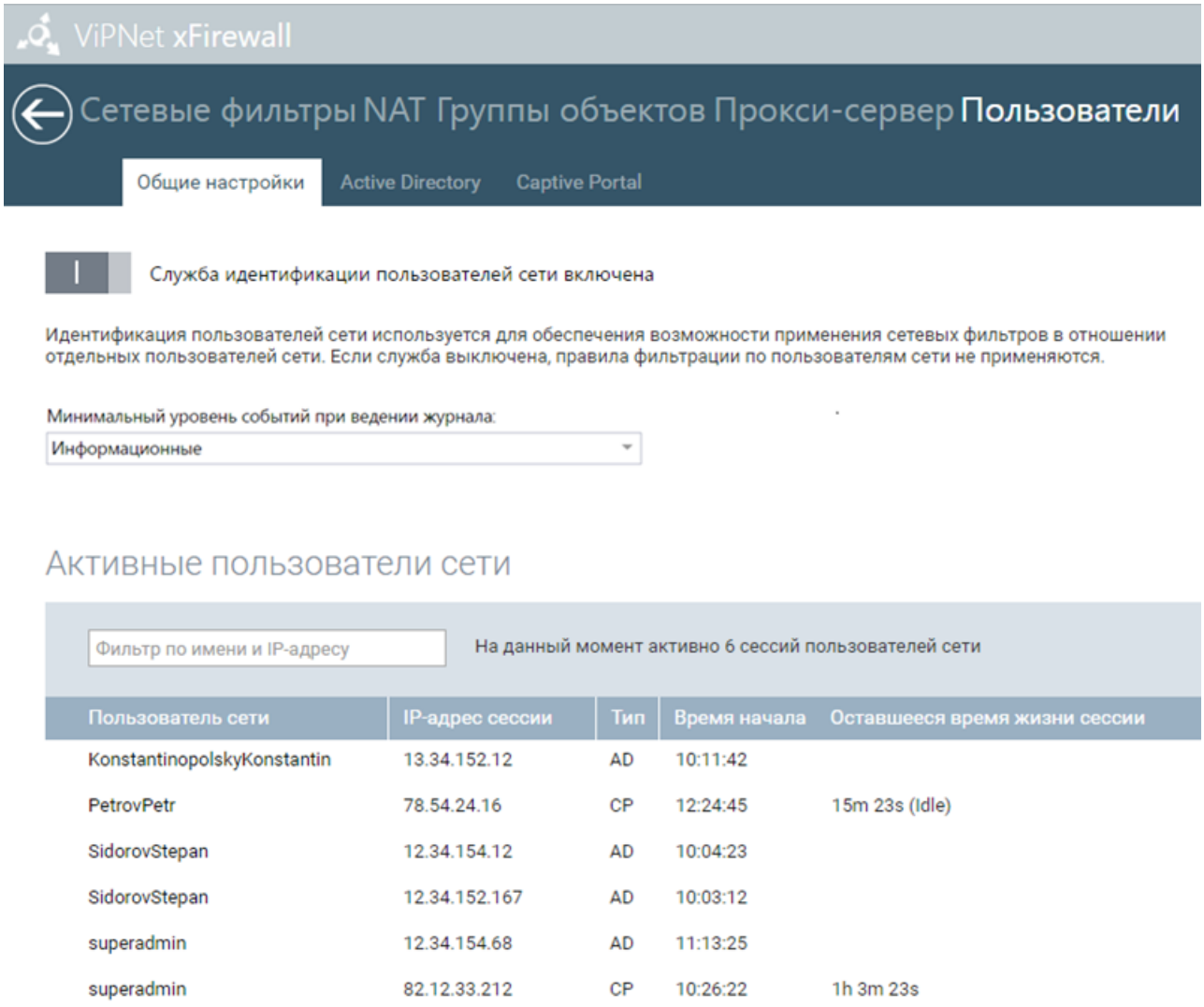

Рисунок 72. Список активных пользователей сети

Вы увидите список активных пользователей сети в следующем формате:

- Имя пользователя сети и его IP-адрес.
- Тип пользователя:
  - AD — пользователь домена Active Directory;
  - CP — пользователь, аутентифицированный с помощью Captive Portal.
- Время начала и оставшееся время жизни сессии пользователя. Отображается в случае, когда для пользователей Captive portal заданы ограничения продолжительности сессии.

Внимание! ViPNet xFirewall не отслеживает выход пользователей из сети (logout). Например, если пользователь Active Directory вышел из сети, то он будет отображаться в списке пользователей до тех пор, пока не истечет время жизни кэша пользовательских сессий или пока с этого IP-адреса в сеть не войдет другой пользователь.

Если список не отображается, выполните следующие действия:

- Если служба идентификации пользователей сети выключена, включите ее с помощью переключателя (для этого войдите в веб-интерфейс в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
- Включите хотя бы один из сервисов идентификации пользователей (Active Directory или Captive portal), установив соответствующие флажки на страницах **Межсетевой экран** > **Пользователи** > **Active Directory** и **Межсетевой экран** > **Пользователи** > **Captive portal**.

По умолчанию в ViPNet xFirewall установлен уровень событий **Информационные** при ведении системного журнала.

Внимание! Не рекомендуется изменять уровень событий при ведении системного журнала, установленный по умолчанию. Повышение уровня событий ведет к увеличению размера системного журнала и к снижению производительности ViPNet xFirewall.

Чтобы изменить уровень событий, выполните следующие действия:

1. Остановите службу идентификации пользователей сети с помощью переключателя.
2. Выберите уровень регистрации событий из списка **Минимальный уровень событий при ведении журнала**. Вы можете установить следующие уровни событий:
   - 0 — критические события;
   - 1 — ошибки;
   - 2 — извещения;
   - 3 — информационные события (по умолчанию);
   - 4 — отладочные события;
   - 5 — детализированные отладочные события.
3. Включите службу идентификации пользователей сети с помощью переключателя.

5

Настройка сетевых служб

Настройка параметров DHCP-сервера 124

Настройка DHCP-relay 127

Настройка параметров DNS-сервера 128

Настройка параметров NTP-сервера 130

Пример настройки доступа к корпоративным DNS- и NTP-серверам 133

Настройка параметров DHCP-сервера

В состав ПО ViPNet xFirewall входит DHCP-сервер, который может использоваться для динамического назначения IP-адресов сетевым узлам (DHCP-клиентам). Одновременно с выделением IP-адресов DHCP-сервер может назначать дополнительные параметры настройки клиентов, например, IP-адреса шлюза по умолчанию и WINS-серверов.

В качестве адресов DNS-сервера и NTP-сервера DHCP-сервер всегда предоставляет клиентам адрес интерфейса, с которым он работает. Клиенты, получившие от ViPNet xFirewall вместе с IP-адресом адреса DNS- и NTP-серверов, будут осуществлять запросы на разрешение имен и синхронизацию времени через соответствующие серверы, запущенные на ViPNet xFirewall. Если на ViPNet xFirewall эти серверы не запущены, то клиенты не смогут работать с доменными именами и синхронизировать свое время.

Внимание! Использование ViPNet xFirewall в качестве DHCP-сервера возможно только при работе в одиночном режиме. Работа DHCP-сервера в режиме кластера горячего резервирования не поддерживается.

Чтобы запустить DHCP-сервер на одном из сетевых интерфейсов Ethernet, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Прикладные сервисы** > **DHCP-сервер**.

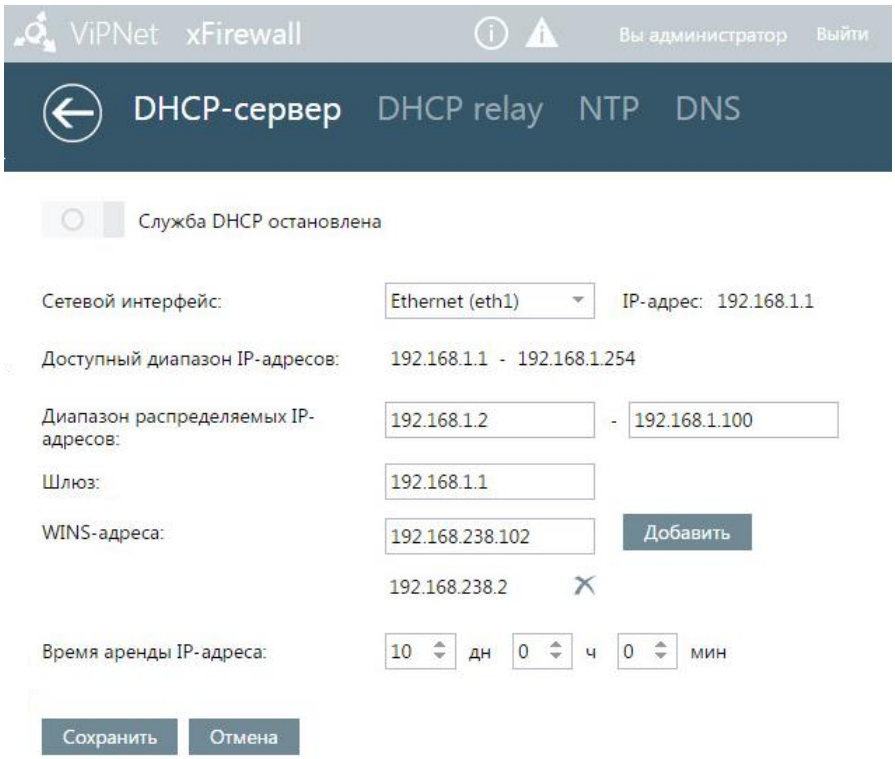

Рисунок 73. Настройка параметров DHCP-сервера

3 В списке **Сетевой интерфейс** выберите сетевой интерфейс, на котором должен быть запущен DHCP-сервер.

Примечание. Сетевой интерфейс для DHCP-сервера не должен быть дополнительным, а также должен быть включен и иметь статический IP-адрес.

---

4 В полях **Диапазон распределяемых IP-адресов** задайте интервал IP-адресов, которые должны присваиваться клиентам DHCP. Диапазон IP-адресов должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам.

Примечание. DHCP-сервер может выделять клиентам любые диапазоны IP-адресов. Однако в локальной сети, маршрутизируемой в сеть Интернет, рекомендуется выделять IP-адреса только из диапазонов, установленных стандартом для частных сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

---

5 В поле **Шлюз** введите IP-адрес шлюза по умолчанию, который должны получать клиенты от DHCP-сервера. IP-адрес шлюза должен принадлежать сети интерфейса и не должен совпадать с адресом самого интерфейса.

6 При необходимости добавьте адрес WINS-сервера (или нескольких серверов), для этого укажите адрес в поле **WINS-адреса** и нажмите кнопку **Добавить**.

7 Задайте время аренды IP-адреса в соответствующих полях.

8 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

9 Чтобы запустить DHCP-сервер или завершить его работу, щелкните переключатель в верхней части страницы. Состояние DHCP-сервера отображается напротив переключателя.

Настройка DHCP-relay

В состав ПО ViPNet xFirewall входит служба DHCP-relay, которая позволяет использовать ViPNet xFirewall в качестве агента DHCP-relay. Такая необходимость может возникнуть в случае, если сетевые узлы должны получать IP-адреса от удаленного DHCP-сервера, к которому они не могут обращаться напрямую. Агент DHCP-relay обеспечивает взаимодействие таких сетевых узлов с DHCP-сервером: он принимает от узлов DHCP-запросы и передает их DHCP-серверу. Ответы, полученные от DHCP-сервера, агент перенаправляет сетевым узлам.

С помощью агента DHCP-relay также можно организовать выделение IP-адресов узлам разветвленной сети, включающей несколько подсетей. В этом случае не нужно устанавливать в каждой подсети свой DHCP-сервер, а достаточно использовать только один DHCP-сервер.

ViPNet xFirewall может обслуживать в качестве агента DHCP-relay несколько локальных сетей. Это могут быть как сети, подключенные к разным физическим интерфейсам ViPNet xFirewall, так и виртуальные локальные сети, подключенные к одному физическому интерфейсу.

Чтобы включить службу DHCP-relay, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Прикладные сервисы** > **DHCP relay.**

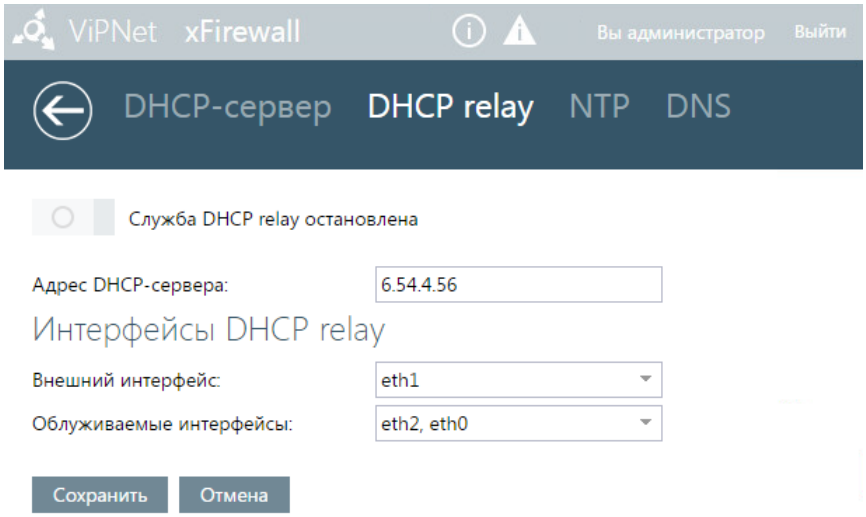

Рисунок 74. Настройка параметров DHCP-ретранслятора

3 В поле **Адрес DHCP-сервера** задайте адрес DHCP-сервера вашей сети.

4 В списке **Внешний интерфейс** выберите сетевой интерфейс, который должен получать данные от DHCP-сервера.

5 В списке **Обслуживаемые интерфейсы** выберите сетевые интерфейсы, с помощью которых должны распределяться IP-адреса DHCP-клиентам.

6 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

Настройка параметров DNS-сервера

В состав ПО ViPNet xFirewall входит DNS-сервер (далее — локальный DNS-сервер), который может использоваться для разрешения (преобразования) символьных имен в IP-адреса в ответ на собственные запросы и на запросы других сетевых узлов (DNS-клиентов).

Локальный DNS-сервер перенаправляет поступающие к нему DNS-запросы на вышестоящие DNS-серверы и передает полученные ответы DNS-клиентам. По умолчанию локальный DNS-сервер настроен таким образом, что он может выполнять разрешение имен с использованием корневых DNS-серверов. Для этого требуется наличие подключения к Интернету. При отсутствии доступа к Интернету для разрешения имен следует использовать другие доступные (не корневые) DNS-серверы. В этом случае необходимо добавить адреса доступных серверов в настройки локального DNS-сервера.

Все DNS-серверы, отличные от корневых, добавляются в качестве DNS-серверов пересылки (forwarder). Если адрес доступного DNS-сервера известен заранее, то его можно задать в процессе первоначальной установки справочников и ключей (подробнее см. в документе «ViPNet xFirewall. Подготовка к работе»).

Внимание! В ситуации, когда DNS-серверы пересылки, заданные в настройках локального DNS-сервера, недоступны, но при этом доступны корневые DNS-серверы, DNS-клиенты будут получать ответы на свои запросы с задержкой.

Список DNS-серверов пересылки можно сформировать вручную. Также можно получить адреса DNS-серверов от внешнего DHCP-сервера, если на одном из интерфейсов ViPNet xFirewall установлен режим DHCP. В полученный от DHCP-сервера список можно добавлять адреса вручную. После перезагрузки ViPNet xFirewall или установки на интерфейсе статического IP-адреса список, полученный от внешнего DHCP-сервера, удаляется из настроек локального DNS-сервера. В этом случае для разрешения имен будут использоваться корневые DNS-серверы.

Примечание. Если режим DHCP установлен на нескольких интерфейсах ViPNet xFirewall, то результат обработки собственных DNS-запросов и запросов DNS-клиентов не определен, так как неизвестно, какой интерфейс будет включен первым и какой список DNS-серверов пересылки получит ViPNet xFirewall.

Чтобы настроить параметры DNS-сервера, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Прикладные сервисы** > **DNS**.

На странице **DNS** содержится список DNS-серверов, который может включать в себя как IP-адреса, заданные пользователем, так и IP-адреса, полученные автоматически от DHCP-сервера. Тип каждого DNS-сервера показан в столбце **Тип**.

Напротив переключателя вверху страницы отображается состояние DNS-серверов.

Изменить или удалить IP-адреса серверов, полученные автоматически, невозможно.

Рисунок 75. Настройка параметров DNS-сервера

3 Чтобы добавить IP-адрес нового DNS-сервера в список, нажмите кнопку **Добавить** и задайте IP-адрес DNS-сервера.

Для изменения IP-адреса DNS-сервера дважды щелкните строку с ним и внесите необходимые изменения. Для удаления IP-адреса DNS-сервера из списка в строке рядом с ним щелкните значок ✕, и в появившемся сообщении нажмите кнопку **OK**.

4 Чтобы запустить все заданные в списке DNS-серверы или завершить их работу, щелкните переключатель в верхней части страницы.

5 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

Настройка параметров NTP-сервера

В состав ПО ViPNet xFirewall входит NTP-сервер (далее — локальный NTP-сервер), который может использоваться для синхронизации времени на самом ViPNet xFirewall и на других сетевых узлах (NTP-клиентах).

По умолчанию локальный NTP-сервер настроен таким образом, что при наличии подключения к Интернету он может осуществлять синхронизацию времени с использованием публичных NTP-серверов из кластера `pool.ntp.org`. Этот кластер серверов можно дополнить другими NTP-серверами (публичными или корпоративными).

Внимание! Для синхронизации времени рекомендуется использовать только доверенные NTP-серверы из сети ViPNet.

Такая необходимость может возникнуть в случае отсутствия доступа к Интернету или при наличии более близкого и менее нагруженного NTP-сервера (например, корпоративного). Если адрес дополнительного NTP-сервера известен заранее, то его можно задать в процессе первоначальной установки справочников и лицензии (подробнее см. в документе «ViPNet xFirewall. Подготовка к работе»).

Примечание. Если в качестве дополнительного NTP-сервера используется узел сети ViPNet, видимый по реальному адресу, то для успешной синхронизации времени с таким сервером при загрузке системы рекомендуется с помощью командного интерпретатора в файле `iplir.conf` в секции `[id]` для этого узла установить параметр `visibility` в значение `real`.

Описание команды, с помощью которого вы можете редактировать файл `iplir.conf`, а также описание секции и параметра см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».

Список дополнительных NTP-серверов можно сформировать вручную или получить их адреса от внешнего DHCP-сервера. При этом в полученный от DHCP-сервера список можно добавлять адреса вручную. После перезагрузки ViPNet xFirewall или установки на интерфейсе статического IP-адреса список, полученный от внешнего DHCP-сервера, удаляется из настроек локального NTP-сервера.

Примечание. Если режим DHCP установлен на нескольких интерфейсах ViPNet xFirewall, то результат синхронизации времени на самом ViPNet xFirewall и на NTP-клиентах не определен, так как неизвестно, какой интерфейс будет включен первым и какой список дополнительных NTP-серверов получит ViPNet xFirewall.

Чтобы настроить параметры NTP-сервера, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Прикладные сервисы** > **NTP**.

На странице **NTP** содержится список NTP-серверов, который может включать в себя как серверы, заданные пользователем, так и серверы, полученные автоматически от DHCP-сервера. Тип каждого NTP-сервера показан в столбце **Тип**. Изменить или удалить серверы, полученные автоматически, невозможно.

Примечание. Сервер `pool.ntp.org`, использующийся по умолчанию, не отображается в списке.

Напротив переключателя вверху страницы отображается состояние NTP-серверов.

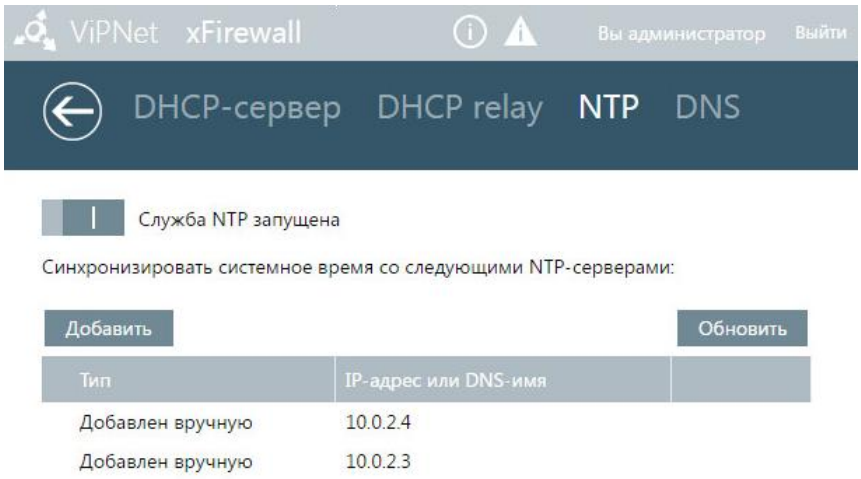

Рисунок 76. Настройка параметров NTP-сервера

3 Чтобы добавить IP-адрес нового NTP-сервера в список, нажмите кнопку **Добавить** и задайте IP-адрес или DNS-имя NTP-сервера.

Для изменения IP-адреса или DNS-имени NTP-сервера дважды щелкните строку с ним и внесите необходимые изменения. Для удаления IP-адреса или DNS-имени NTP-сервера из списка в строке рядом с ним щелкните значок ✕, и в появившемся сообщении нажмите кнопку **OK**.

Примечание. IP-адрес NTP-сервера должен соответствовать следующим требованиям:

- первый октет должен быть больше 0 и меньше 224;
- остальные октеты должны быть не больше 255.

4 Чтобы запустить все заданные в списке NTP-серверы или завершить их работу, щелкните переключатель в верхней части страницы.

Внимание! NTP-серверы, указанные по доменному имени, будут доступны, только если запущен DNS-сервер (см. Настройка параметров DNS-сервера на стр. 128).

Информация о попытках подключения к NTP-серверам записывается в журнал событий. Если ViPNet xFirewall не удалось подключиться ни к одному из NTP-серверов, локальный NTP-сервер запускается с тем временем, которое было задано при первоначальной настройке (см. документ «ViPNet xFirewall. Подготовка к работе», раздел «Настройка NTP-сервера»). Для таких случаев вы можете добавить в список NTP-серверов выбранный NTP-сервер локальной сети, с которым ViPNet xFirewall сможет синхронизировать время в случае невозможности подключения к внешним NTP-серверам.

5 Чтобы сохранить настройки, нажмите кнопку **Сохранить**.

Пример настройки доступа к корпоративным DNS- и NTP-серверам

Пусть у организации есть несколько офисов, при этом в центральном офисе установлены корпоративные DNS- (см. глоссарий, стр. 201) и NTP-серверы (см. глоссарий, стр. 202). Требуется, чтобы к этим серверам могли обращаться клиенты, находящиеся в филиале. Чтобы решить эту задачу, можно использовать ViPNet xFirewall. Для этого выполните следующие действия:

1 Установите в филиале ViPNet xFirewall.

2 В сетевых настройках клиентов задайте IP-адрес ViPNet xFirewall в качестве DNS- и NTP-серверов. Таким образом, клиенты филиала будут направлять запросы на разрешение DNS-имен и на синхронизацию времени непосредственно на ViPNet xFirewall.

3 Войдите в веб-интерфейс в режиме администратора.

4 Перейдите на страницу **Прикладные сервисы** > **NTP**.

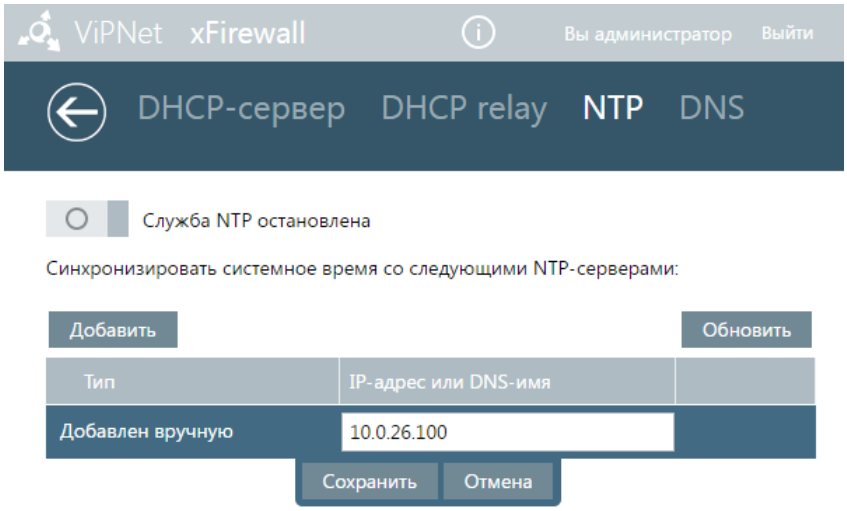

Рисунок 77. Настройка NTP-сервера

5 Нажмите кнопку **Добавить** и укажите адрес корпоративного NTP-сервера, который необходимо использовать для синхронизации времени.

6 Запустите NTP-сервер с помощью переключателя.

7 Перейдите на страницу **Межсетевой экран** > **Сетевые фильтры** > **Локальные фильтры открытой сети**.

8 Нажмите кнопку **Добавить**. Откроется страница добавления локального фильтра открытой сети.

9 На странице создания фильтра выполните следующие действия:

9.1 В поле **Имя фильтра** укажите название фильтра.

9.2 Установите переключатель **Состояние** в положение включено.

9.3 Установите переключатель **Действие** в состояние **Пропускать трафик**.

9.4 Нажмите кнопку **Протоколы** раздела **Добавить** и укажите протоколы для фильтрации. В появившемся диалоговом окне выберите группу протоколов **DNS** и нажмите кнопку **Сохранить**.

9.5 Нажмите кнопку **Источники** раздела **Добавить** и укажите отправителя IP-пакетов. Выберите в качестве источника **Группа IP-адресов**.

9.6 В появившемся диалоговом окне выберите группу IP-адресов **PrivateNetworkIP** и нажмите кнопку **Сохранить**.

9.7 Нажмите кнопку **Назначения** в разделе **Добавить** и укажите получателя IP-пакетов. Выберите в качестве назначения **Мой узел**.

9.8 Нажмите кнопку **Сохранить и применить** на странице создания фильтра.

10 Аналогично предыдущему пункту создайте фильтр для протокола NTP.

В результате произведенных настроек клиенты филиала смогут обращаться к корпоративным DNS- и NTP-серверам с соответствующими запросами.

6

Настройка маршрутизации

Общие сведения о маршрутизации 136

Принципы формирования таблиц маршрутизации в ViPNet xFirewall 137

Просмотр общей таблицы маршрутизации 139

Общие сведения о протоколе OSPF 141

Настройка статической маршрутизации 143

Настройка динамической маршрутизации 146

Общие сведения о маршрутизации

ViPNet xFirewall поддерживает функции маршрутизации IP-трафика в сетях со сложной структурой.

Под маршрутизацией понимается процесс выбора маршрута следования IP-пакета (см. глоссарий, стр. 204), передаваемого в сети от одного узла другому. Маршрут следования выбирается из подмножества маршрутов, заданных на маршрутизаторе и хранящихся в таблице маршрутизации.

В таблицу маршрутизации маршруты могут попадать в явном виде (статические маршруты) либо с помощью алгоритмов маршрутизации на основе информации о топологии и состоянии сети, предоставляемой протоколами маршрутизации (динамические маршруты). В первом случае не требуется никаких дополнительных условий. Но стоит заметить, что в сетях со сложной структурой процесс настройки статических маршрутов может стать весьма трудоемким из-за большого числа маршрутов, которые требуется создать. Во втором случае на всех маршрутизаторах в сети должно быть настроено использование определенного протокола динамической маршрутизации, по которому маршрутизаторы будут обмениваться друг с другом информацией о доступных им сетях, автоматически строить доступные маршруты в каждую сеть и выбирать из них наилучшие.

Статическую маршрутизацию удобно использовать в небольших сетях либо в крупных сетях в частных случаях. В сетях с разветвленной и неоднородной топологией рекомендуется использовать динамическую маршрутизацию. Кроме автоматического формирования таблиц маршрутизации, динамическая маршрутизация позволяет:

- Автоматически выбирать по определенным критериям наилучший маршрут из нескольких доступных.
- Организовать защиту от сбоев. В случае сбоя какого-либо маршрутизатора автоматически выбирается другой наилучший маршрут и загружается в таблицу маршрутизации.
- Организовать динамическую балансировку нагрузки передаваемого IP-трафика.

ViPNet xFirewall может выполнять маршрутизацию IP-трафика с использованием следующих видов маршрутов:

- статических маршрутов, в том числе на основе маршрутов с несколькими шлюзами;
- динамических маршрутов, формируемых по протоколу DHCP;
- динамических маршрутов, формируемых протоколом OSPF (см. глоссарий, стр. 202).

Принципы формирования таблиц маршрутизации в ViPNet xFirewall

В ViPNet xFirewall для хранения маршрутов используются две таблицы маршрутизации:

- Routing Information Base (далее — RIB) — полная таблица маршрутизации, которая содержит все статические маршруты, созданные администратором, и все динамические маршруты, полученные по протоколам DHCP и OSPF.
- Forwarding Information Base (далее — FIB) — таблица маршрутизации, которая содержит только наилучшие статические и динамические маршруты в каждую сеть, выбранные из RIB; загружается в ядро системы и используется при маршрутизации IP-трафика.

Все новые маршруты, независимо от способа их создания, попадают в RIB. Каждый маршрут имеет следующие характеристики:

- Источник получения маршрута — определяет, каким образом был сформирован маршрут: с использованием статического правила или по протоколу динамической маршрутизации.
- Административная дистанция — определяет приоритет маршрута от каждого источника. Используется тогда, когда в таблице маршрутизации задано несколько маршрутов в одну и ту же сеть. Чем меньше административная дистанция, тем более приоритетным считается маршрут.

  Административная дистанция задается для каждого статического маршрута. В случае динамических маршрутов административная дистанция задается не для конкретного маршрута, а для всего протокола сразу. Поэтому все динамические маршруты, добавленные в RIB этим протоколом, имеют одинаковую дистанцию.

  Административная дистанция для протоколов DHCP и OSPF не может быть одинаковой, чтобы маршруты этих протоколов не перемешивались. Также административная дистанция статических правил маршрутизации не может совпадать с дистанцией, заданной для какого-либо протокола динамической маршрутизации.

Примечание. В ViPNet xFirewall для каждого типа маршрутов задается по умолчанию следующая административная дистанция:

- для статических маршрутов — 10;
- для маршрутов DHCP-сервера — 70;
- для маршрутов протокола OSPF — 110.

Для первых двух типов маршрутов вы можете менять значение административной дистанции, для маршрутов последнего типа менять это значение нельзя.

Для маршрутов DHCP-сервера задается общая административная дистанция.

- Метрика — определяет приоритет внутри списка динамических маршрутов, сформированных и добавленных в RIB определенным протоколом динамической маршрутизации. Чем меньше метрика, тем выше приоритет маршрута.

Для DHCP-протокола метрики указываются вручную, причем на каждом сетевом интерфейсе, на котором включен режим DHCP и настроен параметр получения маршрутов от DHCP-сервера. Таким образом, если на разные сетевые интерфейсы будут получены одинаковые DHCP-маршруты в одну и ту же сеть, то будет выбран маршрут с наименьшей метрикой.

Для динамических маршрутов, формируемых протоколом OSPF, метрики формируются самим протоколом, поэтому их задавать не требуется.

- Вес — определяет долю IP-трафика, который будет проходить по маршруту через указанный шлюз. Используется только в статических маршрутах и задается для шлюза. Позволяет настроить балансировку передаваемого IP-трафика между несколькими шлюзами, когда часть IP-пакетов направляется на один шлюз, а часть — на другой. Поэтому вес задается тогда, когда создается несколько статических маршрутов с одинаковым IP-адресом назначения и разными шлюзами.

Таблица FIB формируется на основе содержания таблицы RIB и включает в себя только наилучшие маршруты в каждую сеть. Если в результате заполнения таблицы RIB в ней оказывается несколько маршрутов в одну сеть, то наилучший маршрут определяется по следующим правилам:

- Если в RIB присутствуют статические маршруты с разной дистанцией, то в FIB загружается маршрут с наименьшей дистанцией. Например, имеется два маршрута в сеть 10.0.5.0 с маской 255.255.255.0. Для первого маршрута задана административная дистанция — 10, для второго — 30. В результате в FIB попадет первый маршрут.
- Если в RIB присутствуют статические маршруты с одинаковой дистанцией, то в FIB загружаются все маршруты.
- Если в RIB присутствуют динамические маршруты, то в FIB загружается маршрут с наибольшим приоритетом (то есть наименьшей метрикой, заданной протоколом динамической маршрутизации). Если приоритеты равны, то в FIB попадают все маршруты.

Маршруты от одного источника (Static, DHCP, OSPF) в одну и ту же сеть с одинаковыми метриками (или административными дистанциями в случае статических маршрутов) при маршрутизации суммируются — объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре такие маршруты отображаются в виде одного маршрута с несколькими шлюзами:

```
10.100.2.0/24 [30/23] (weight 1) via 10.1.30.202, eth1
                      (weight 1) via 10.1.31.201, eth2
```

Внимание! Если хотя бы один из шлюзов объединенного маршрута multi-hop route выйдет из строя, работоспособность маршрута не может быть гарантирована.

Если маршрут был удален из RIB, то он также удаляется из FIB. При этом по вышеописанным правилам выбирается новый наилучший маршрут в ту же сеть из имеющихся в RIB и немедленно загружается в FIB.

Просмотр общей таблицы маршрутизации

Чтобы просмотреть список всех существующих маршрутов (содержимое таблицы RIB) перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **Сводная таблица**.

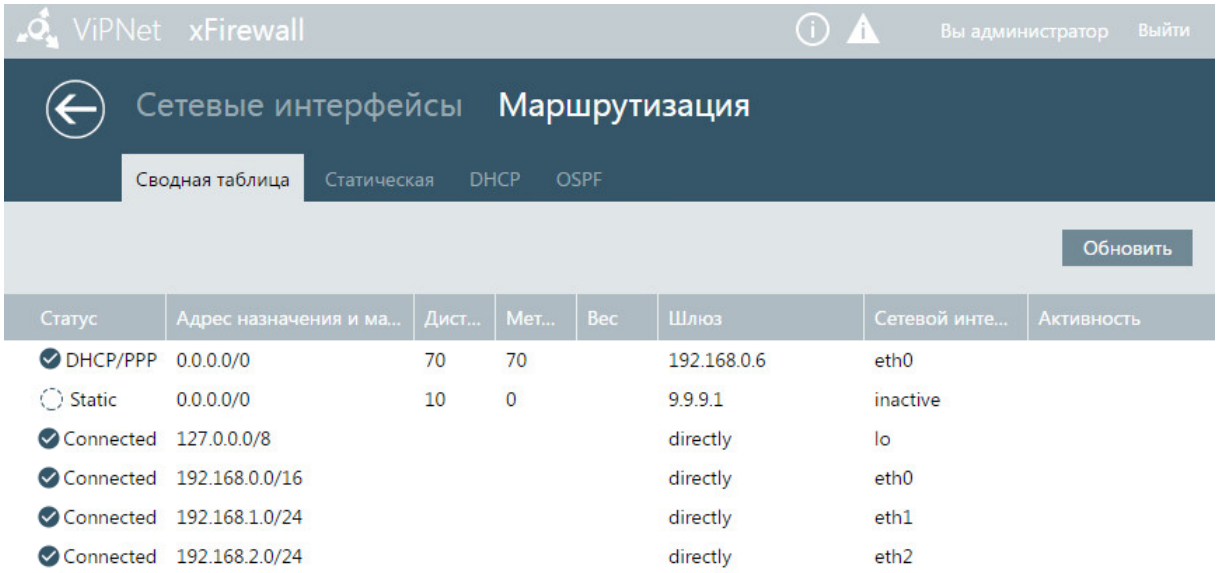

Рисунок 78. Просмотр общей таблицы маршрутизации

Совет. Чтобы обновить содержимое списка маршрутов, нажмите кнопку **Обновить**.

В списке для каждого маршрута отображается статус. Список всех возможных статусов приведен в таблице ниже.

Таблица 8. Статусы маршрутов

Статус	Пояснение
✓	Наилучший маршрут, который загружен в FIB и используется в процессе маршрутизации.
C	Маршрут в подсеть, к которой подключен один из интерфейсов ViPNet xFirewall.
D	Маршрут, предоставленный DHCP-сервером.
O	Маршрут протокола динамической маршрутизации OSPF.
S	Статический маршрут.

Списки маршрутов от конкретного источника вы можете посмотреть в разделе **Маршруты** на отдельных вкладках **Статическая**, **DHCP**, **OSPF**.

Общие сведения о протоколе OSPF

Протокол OSPF является внутренним шлюзовым протоколом (Interior Gateway Protocol, IGP) и используется для распространения данных маршрутизации внутри одной автономной системы (см. глоссарий, стр. 203).

Работа по данному протоколу устроена следующим образом. OSPF-маршрутизаторы сначала посредством широковещательной рассылки (multicast) устанавливают связь друг с другом. Затем посредством однонаправленной рассылки (unicast) начинают обмениваться друг с другом сообщениями типа Link State Advertise (LSA), в которых передают информацию о состоянии каналов связи. На маршрутизаторе при получении LSA-сообщения информация из него заносится в базу данных (link state database). Если LSA-сообщение содержит новую информацию о канале связи по сравнению с той, которая содержится в базе данных, то оно передается соседним маршрутизаторам (см. глоссарий, стр. 204). После заполнения базы данных на каждом маршрутизаторе по алгоритму Дейкстры вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость (см. глоссарий, стр. 206). Таким образом, каждый OSPF-маршрутизатор имеет собственное представление о состоянии каналов связи и топологии сети, но при этом все маршрутизаторы используют одну базу данных состояний каналов связи для вычисления кратчайших маршрутов.

Межсетевая среда, в которой находятся OSPF-маршрутизаторы, представляется как совокупность областей (см. глоссарий, стр. 204), соединенных друг с другом через некоторую базовую область. В зависимости от этого выделяют несколько типов областей и несколько типов маршрутизаторов.

Выделяют следующие типы областей маршрутизации:

- Область 0 или базовая область (backbone area) — область, с которой должны быть соединены все остальные области автономной системы.
- Стандартная область — область, способная граничить как с другими областями, так и с другими автономными системами.
- Стандартная тупиковая область (stub area) — область, граничащая только с другими областями.
- Полностью тупиковая область (totally stubby area) — область, граничащая только с одной областью.
- Не полностью тупиковая область (not-so-stubby area) — стандартная тупиковая область, имеющая возможность взаимодействовать с другими автономными системами с помощью пограничных маршрутизаторов (ABR).

Каждый OSPF-маршрутизатор входит в определенную область маршрутизации и обменивается информацией только с маршрутизаторами, входящими в эту же область. При этом обмен производится не напрямую, а через посредника — маршрутизатор, выбранный главным в этой области. Информация между разными областями передается через маршрутизатор, который располагается на границе этих областей. Если автономная система взаимодействует с другой

автономной системой, то информация передается через маршрутизатор, который располагается на границе систем. Такой подход позволяет уменьшить объем рассылаемых LSA-сообщений, тем самым уменьшить нагрузку на маршрутизаторы и повысить скорость построения таблиц маршрутизации.

Таким образом, выделяют следующие типы маршрутизаторов:

- Внутренний маршрутизатор (internal router, IR) — маршрутизатор, все сетевые интерфейсы которого находятся в одной области.
- Назначенный маршрутизатор (designated router, DR) — маршрутизатор, выбранный главным среди всех внутренних маршрутизаторов в одной области.
- Резервный назначенный маршрутизатор (backup designated router, BDR) — маршрутизатор, берущий на себя функции главного в случае, если он вышел из строя.
- Межобластной граничный маршрутизатор (area border router, ABR) — маршрутизатор, соединяющий несколько областей OSPF одной автономной системы.
- Граничный маршрутизатор автономной системы (autonomous system boundary router, ASBR) — маршрутизатор, граничащий с другой автономной системой, работающей по другому протоколу динамической маршрутизации (IGRP, EIGRP, IS-IS, RIP, BGP, Static).

Настройка статической маршрутизации

Если ViPNet xFirewall функционирует в сети, конфигурация которой никогда не меняется или в которой используется минимальное количество путей для доставки IP-пакетов, то вы можете настроить маршрутизацию на ViPNet xFirewall вручную с помощью статических маршрутов. Кроме этого, настройка маршрутизации вручную также может потребоваться, когда нет возможности использовать в сети маршрутизаторы, работающие по протоколам динамической маршрутизации, или в следующих случаях:

- Чтобы направлять часть IP-трафика всегда по конкретным маршрутам (например, есть требование направлять IP-трафик по самому надежному каналу), или направлять IP-трафик пользователей в Интернет через конкретный шлюз.
- Если нужен статический маршрут по умолчанию на случай, когда работа по протоколам динамической маршрутизации будет невозможна.
- Чтобы распределять передачу IP-трафика по нескольким маршрутам.

Добавление статических маршрутов

Чтобы добавить новый статический маршрут, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **Статическая**.
3. Нажмите кнопку **Добавить**.
4. Задайте следующие параметры маршрута:
   - IP-адрес назначения маршрута и маску подсети. Маска подсети должна быть указана в битовом формате через слэш после IP-адреса (0.0.0.0/0).
   - IP-адрес шлюза для доступа к IP-адресу назначения.
   - Административная дистанция (см. глоссарий, стр. 203). Если вы не укажете значение административной дистанции, то оно будет задано автоматически и равно 10. Если вы укажете административную дистанцию, и ее значение будет совпадать со значением административной дистанции, заданной протоколам динамической маршрутизации, маршрут не сможет быть добавлен. В этом случае создайте маршрут с другим значением административной дистанции.
   - Вес (см. глоссарий, стр. 203). Укажите его в том случае, если вы создаете несколько маршрутов в одну сеть с разными шлюзами, между которыми требуется производить

балансировку нагрузки. Подробнее см. раздел Настройка балансировки IP-трафика (на стр. 144).

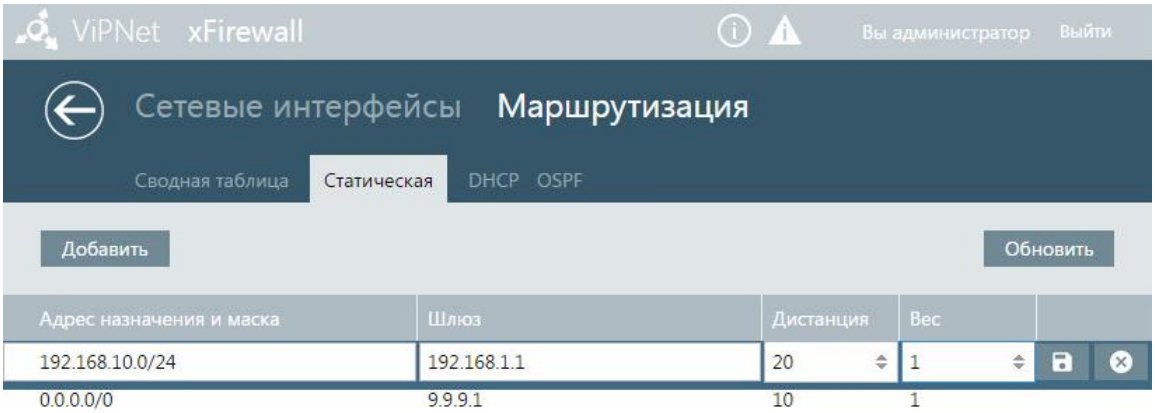

Рисунок 79. Добавление статического маршрута

5 Нажмите кнопку **Сохранить**.

В результате маршрут появится в списке статических маршрутов. Кроме этого, он будет добавлен в таблицу RIB и появится на вкладке **Сводная таблица**. Если маршрут будет выбран наилучшим, то он будет загружен в таблицу FIB и начнет использоваться при маршрутизации IP-трафика. В этом случае в списке маршрутов на вкладке **Сводная таблица** он будет иметь значок .

Совет. Если вам требуется получить один статический маршрут с несколькими шлюзами, создайте несколько статических маршрутов в одну и ту же сеть с одинаковой административной дистанцией, указав в каждом по одному шлюзу. В результате эти маршруты будут просуммированы и объединены в один с несколькими шлюзами. Как правило, такие маршруты требуются для балансировки нагрузки, поэтому в маршрутах также должен быть задан вес шлюзам (см. Настройка балансировки IP-трафика на стр. 144).

Если в списках не появился новый маршрут, обновите ее содержимое. Для этого нажмите кнопку **Обновить**.

При необходимости вы можете отредактировать значение административной дистанции и веса в маршруте. Для этого дважды щелкните строку маршрута, внесите необходимые изменения и нажмите кнопку **Сохранить**. Если вам нужно изменить IP-адрес назначения или шлюза, удалите маршрут и создайте новый с нужными параметрами. Чтобы удалить маршрут, в строке рядом с ним щелкните значок , после чего в появившемся окне сообщения нажмите кнопку **ОК**.

Настройка балансировки IP-трафика

Если вы хотите ускорить процесс отправки IP-пакетов в сеть назначения, то вы можете создать несколько статических маршрутов в данную сеть через разные шлюзы и настроить балансировку IP-трафика между этими маршрутами. Это позволит в процессе разных TCP-соединений отправлять часть IP-пакетов по одному маршруту, часть — по другому, что повысит скорость передачи IP-пакетов в сеть назначения. Балансировка IP-трафика настраивается с помощью одного из

параметров маршрутов — веса (см. глоссарий, стр. 203) (`weight`). При этом все маршруты, которые будут участвовать в балансировке IP-трафика, должны иметь одинаковую административную дистанцию, то есть иметь одинаковый приоритет.

Примечание. При маршрутизации маршруты в одну сеть назначения и с одинаковой дистанцией объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре общей таблицы маршрутизации они отображаются как один маршрут с несколькими шлюзами.

Для настройки балансировки IP-трафика выполните следующие действия:

1. Создайте нужное количество маршрутов (см. Добавление статических маршрутов на стр. 143) с одинаковым адресом назначения и с разными шлюзами.
2. Задайте каждому маршруту одинаковую административную дистанцию.
3. Задайте в каждом маршруте вес шлюзу. IP-трафик будет распределяться между шлюзами в соответствии с соотношением их весов. Например:
   - если вы создаете 2 маршрута и в каждом маршруте вес шлюза равен 1, то IP-трафик будет разделен между этими маршрутами поровну, то есть 50% IP-трафика будет передаваться по одному маршруту, 50% — по второму;
   - если вы создаете 3 маршрута, и в первом маршруте вес шлюза равен 1, во втором — вес шлюза равен 2, в третьем — вес шлюза равен 3, то по второму маршруту будет передаваться в два раза больше IP-трафика, чем по первому, по третьему — в три раза больше, чем по первому.

Пример создания статических маршрутов с весом шлюзов равным 1:

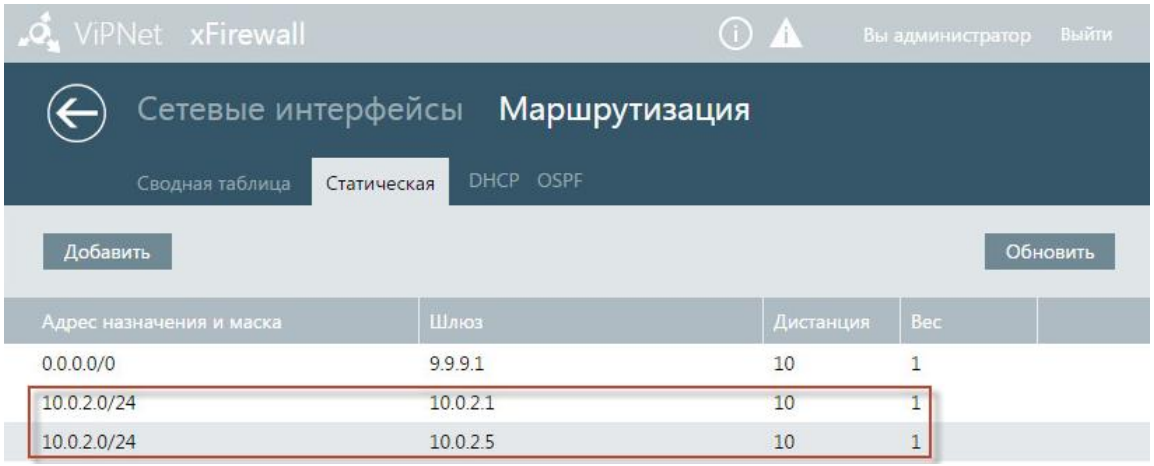

Рисунок 80. Распределение нагрузки между статическими маршрутами в одну сеть

Примечание. Если в процессе создания маршрута вы не укажете вес шлюза, то автоматически шлюзу будет назначен вес равный 1. Вы не можете задать вес равный 0.

Балансировка IP-трафика будет осуществляться, только если созданные маршруты признаны наилучшими и присутствуют в таблице FIB.

Настройка динамической маршрутизации

Если в вашей сети поддерживается работа по протоколу DHCP или OSPF (см. глоссарий, стр. 202), то вы можете настроить на ViPNet xFirewall динамическую маршрутизацию. Данные настройки позволят автоматически создавать таблицы маршрутизации на основе маршрутов, формируемых по данным протоколам, и распространять их между другими маршрутизаторами в рамках одной сети.

Внимание! Настройку динамической маршрутизации должен выполнять опытный администратор, понимающий принципы работы протоколов динамической маршрутизации, в том числе протокола OSPF. Приведенная в руководстве информация носит справочный характер.

Настройка параметров динамических маршрутов от DHCP-протокола

Если на каком-либо сетевом интерфейсе ViPNet xFirewall включен режим DHCP и настроено автоматическое получение маршрутов от DHCP-сервера, то в процессе маршрутизации будут использоваться эти маршруты. В этом случае выполните следующие дополнительные настройки:

1. Настройте административную дистанцию для протокола DHCP. Это позволит определить приоритет маршрутов DHCP-сервера среди всех маршрутов, имеющихся в таблице RIB (статических маршрутов, маршрутов протокола OSPF, если такие есть).
2. Если режим DHCP включен на нескольких сетевых интерфейсах, настройте метрики DHCP-протокола на каждом сетевом интерфейсе, на котором включен этот режим (см. Настройка метрики для маршрутов DHCP-сервера на стр. 147). Это позволит определить приоритет среди маршрутов DHCP-сервера в одну и ту же сеть, полученных с разных сетевых интерфейсов.

Настройка административной дистанции для маршрутов DHCP-сервера

Если на ViPNet xFirewall настроено взаимодействие с DHCP-сервером, от которого поступают динамические маршруты для маршрутизации IP-трафика, а также настроена статическая маршрутизация (см. Настройка статической маршрутизации на стр. 143) или динамическая маршрутизация по протоколу OSPF, то требуется задать административную дистанцию для

маршрутов DHCP-протокола. Административная дистанция определит приоритет данных маршрутов среди всех остальных, и в случае, если будет обнаружено несколько маршрутов в одну и ту же сеть из разных источников, будет выбран тот маршрут, у которого выше приоритет. Чем меньше значение административной дистанции (см. глоссарий, стр. 203), тем выше приоритет маршрута.

Примечание. Административная дистанция определяет приоритет всех маршрутов DHCP-сервера, независимо от того, на какой сетевой интерфейс они поступили.

Чтобы задать административную дистанцию для маршрутов, поступающих от DHCP-сервера, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **DHCP**.
3. Введите значение административной дистанции в поле **Дистанция по умолчанию** и нажмите кнопку **Сохранить**. По умолчанию указана административная дистанция 70.

Рисунок 81. Настройка дистанции DHCP

Настройка метрики для маршрутов DHCP-сервера

Если на ViPNet xFirewall режим DHCP включен на нескольких сетевых интерфейсах, то может сложиться ситуация, когда с этих интерфейсов поступят одинаковые маршруты от DHCP-сервера в одну и ту же сеть. В этом случае требуется определить, какой маршрут является наилучшим, чтобы добавить его в FIB и использовать при маршрутизации. Параметром, позволяющим выбрать наилучший маршрут, выступает метрика (см. глоссарий, стр. 204). Ее можно задать на каждом сетевом интерфейсе, на котором включен режим DHCP, чтобы определить приоритет маршрутов DHCP-сервера на разных интерфейсах. Чем меньше значение метрики, тем выше приоритет маршрута. Если на интерфейсах заданы одинаковые метрики, то поступившие маршруты в одну и ту же сеть будут объединены в один маршрут с несколькими шлюзами.

В ViPNet xFirewall вы можете задать или удалить метрику для маршрутов DHCP-сервера на конкретном сетевом интерфейсе (далее — специфичная метрика). Если специфичная метрика не задана, то вместо нее используется метрика по умолчанию.

Примечание. Задать специфичную метрику для протокола DHCP вы можете на сетевых интерфейсах следующих типов:

- Ethernet.
- VLAN (см. Настройка интерфейсов для обработки трафика из нескольких VLAN на стр. 30).
- Агрегированный интерфейс (см. Использование агрегированных сетевых интерфейсов на стр. 36).

При этом должны выполняться следующие условия:

- на нескольких сетевых интерфейсах включен режим DHCP;
- на этих интерфейсах настроен параметр автоматического получения маршрутов от DHCP-сервера.

Если режим DHCP включен только на одном сетевом интерфейсе, то настройка специфичной метрики не требуется, поскольку для группы маршрутов в рамках одного сетевого интерфейса она всегда будет одинаковой.

Чтобы настроить метрику для маршрутов, поступающих от DHCP-сервера, на сетевом интерфейсе одного из указанных типов, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Сетевые интерфейсы**.
3. На левой панели выберите интерфейс, на котором требуется задать метрику.
4. Убедитесь, что на данном интерфейсе включен режим DHCP (установлен флажок **Автоматически получать настройки**) и настроено автоматическое получение маршрутов от него (установлен флажок **Маршруты**).
5. Введите значение метрики в поле **Метрика** и нажмите кнопку **Сохранить**.

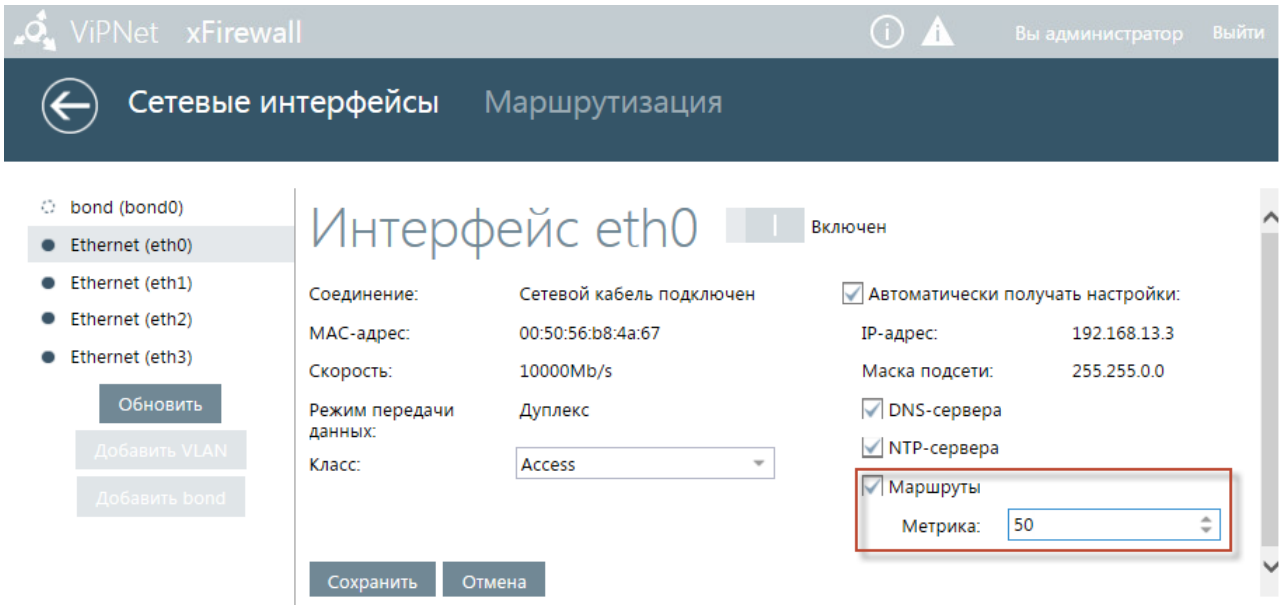

Рисунок 82. Задание метрики для протокола DHCP на конкретном сетевом интерфейсе

6 Если требуется удалить метрику на сетевом интерфейсе, удалите ее значение в указанном поле. После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

Изменение метрики по умолчанию для маршрутов от DHCP-протокола

Если для маршрутов DHCP-протокола не задавались специфичные метрики, то для определения приоритета маршрутов этих протоколов будет использоваться метрика по умолчанию. Первоначально метрика по умолчанию равна 70. При необходимости вы можете изменить это значение. Для этого выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **DHCP**.

3 Введите новое значение метрики в поле **Метрика** и нажмите кнопку **Сохранить**. Первоначально метрика по умолчанию равна 70.

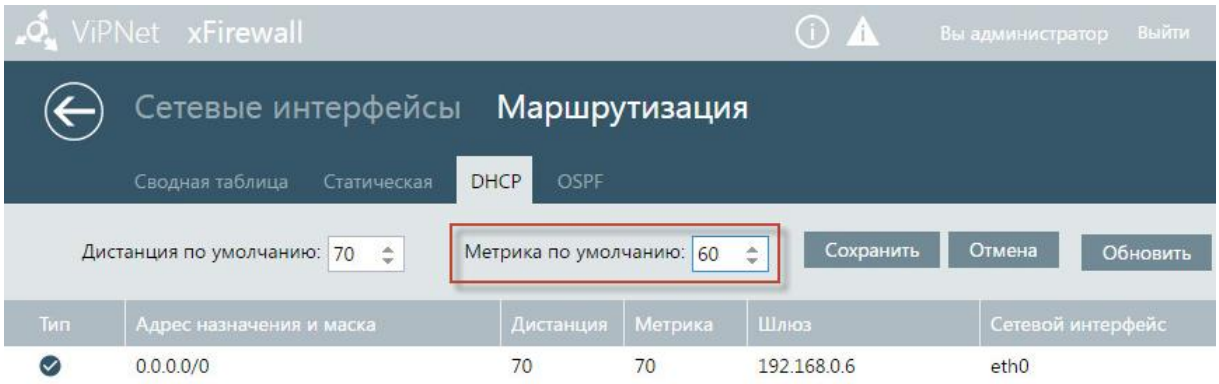

Рисунок 83. Задание метрики по умолчанию

Настройка параметров динамической маршрутизации по протоколу OSPF

Совет. Настройка динамической маршрутизации по протоколу OSPF имеет смысл в том случае, если в сети, в которой установлен ViPNet xFirewall, одновременно выполняются следующие условия:

- используются другие OSPF-маршрутизаторы и они напрямую связаны с ViPNet xFirewall;
- поддерживается многоадресное вещание (multicast);
- по требованиям безопасности вашей организации разрешена передача IP-трафика по протоколу OSPF между сетевыми узлами.

В процессе настройки маршрутизации по протоколу OSPF вам потребуется:

- включить использование протокола OSPF;
- указать сети, к которым подключен ViPNet xFirewall и которые будут участвовать в маршрутизации по протоколу OSPF, и области маршрутизации (см. глоссарий, стр. 204);
- создать ряд сетевых фильтров.

При настройке динамической маршрутизации по протоколу OSPF следует учитывать следующие рекомендации и ограничения:

- В случае сбоя на одном из маршрутов для переключения на альтернативный маршрут может потребоваться до 15 минут. Чтобы уменьшить время переключения, рекомендуется в файле `iplir.conf` в секциях `[id]`, соответствующих связанным маршрутизаторам или координаторам ViPNet, задать более короткий период опроса, изменив значение параметра `checkconnection_interval` (подробнее см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам»). Например, можно задать для параметра значение 30 секунд. При этом необходимо учитывать, что сокращение периода опроса приведет к увеличению количества служебного трафика между

маршрутизаторами (координаторами), в результате чего может снизиться производительность маршрутизаторов (координаторов).

- Если ваш ViPNet xFirewall непосредственно связан с координаторами или другими маршрутизаторами ViPNet, рекомендуется в файле `iplir.conf` в секциях `[id]`, соответствующих этим маршрутизаторам или координаторам, указать в параметре `accessiplist` метрику `1`. В этом случае при наличии нескольких альтернативных маршрутов защищенный трафик всегда будет передаваться по кратчайшему маршруту — через соседний координатор (маршрутизатор) ViPNet.

При необходимости вы также можете настроить перераспределение маршрутов (см. глоссарий, стр. 205) по протоколу OSPF.

Настройка протокола OSPF

Для настройки протокола OSPF выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **OSPF**.
3. В разделе **Настройки** включите использование протокола, установив переключатель в верхней части страницы в положение **Включена**.
4. Укажите подсеть, в которой должна осуществляться маршрутизация по протоколу OSPF. Для этого нажмите кнопку **Добавить** и укажите следующие параметры:
   - IP-адрес подсети и маску подсети в нотации CIDR (например, 0.0.0.0/0).
   - Область маршрутизации (см. глоссарий, стр. 204), в которую входит указанная подсеть.

   Примечание. Вы можете указать не более 128 сетей, в которых осуществляется обмен информацией по протоколу OSPF.
5. Нажмите кнопку **Сохранить**.

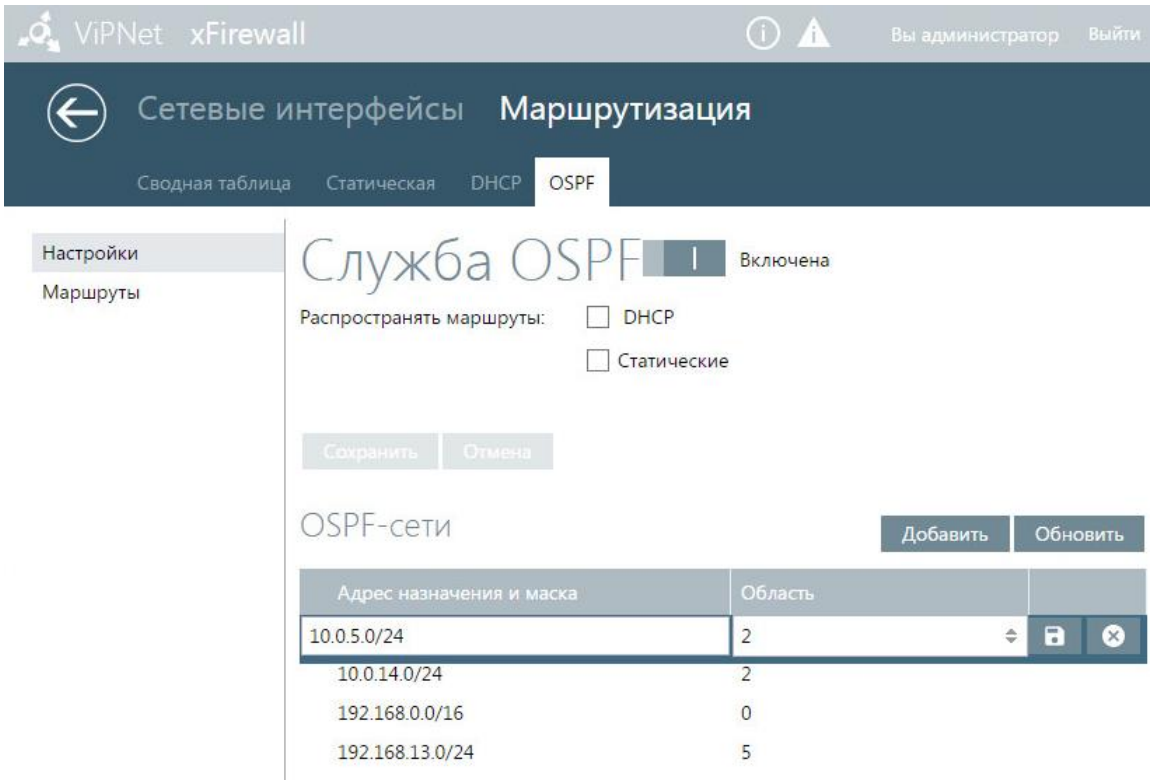

Рисунок 84. Настройка OSPF-протокола

6 Создайте следующие сетевые фильтры открытой сети:

- Фильтры, разрешающие входящий однонаправленный IP-трафик (unicast) и широковещательный (multicast) IP-трафик по протоколу OSPF от всех соседних OSPF-маршрутизаторов, с которыми взаимодействует ViPNet xFirewall:

Таблица 9. Фильтры для входящего OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Rule 1	<IP-адрес OSPF-маршрутизатора>	@local	IP:89	pass
Rule 2	<IP-адрес OSPF-маршрутизатора>	@multicast	IP:89	pass

Фильтры должны быть созданы для каждого соседнего OSPF-маршрутизатора в области, в которой находится ViPNet xFirewall.

- Фильтр, разрешающий исходящий IP-трафик ViPNet xFirewall по протоколу OSPF от любого IP-адреса источника:

Таблица 10. Фильтры для исходящего OSPF-трафика

Название	Источник	Назначение	Протокол	Действие
Rule 3	@local	@any	IP:89	pass

7 В следующих случаях на ViPNet xFirewall необходимо добавить фильтры защиты канала управления, разрешающие трафик протокола OSPF (протокол IP, порт 89):

- Между ViPNet xFirewall и координаторами сети ViPNet установлены связи на уровне пользователей — фильтры добавляются на ViPNet xFirewall и координаторах.
- Между двумя и более ViPNet xFirewall установлены связи на уровне пользователей — фильтры добавляются на этих (двух и более) ViPNet xFirewall.

Таблица 11. Фильтры защиты канала управления, разрешающие трафик протокола OSPF (протокол IP, порт 89)

Название	Источник	Назначение	Протокол	Действие
Rule 1	@any	@any	IP:89	pass

Подробнее о создании сетевых фильтров см. в разделе Создание и изменение сетевого фильтра (на стр. 74).

Внимание! Если вы не настроите указанные фильтры, то ViPNet xFirewall не сможет работать по протоколу OSPF (см. Общие сведения о протоколе OSPF на стр. 141).

Если впоследствии потребуется отказаться от использования протокола OSPF для маршрутизации, установите переключатель в положение **Отключена**.

Если в подсети прекращено использование протокола OSPF, удалите ее. Чтобы удалить подсеть, в строке рядом с ней щелкните значок ✕, после чего в появившемся окне сообщения нажмите кнопку **OK**.

Настройка перераспределения маршрутов

Протокол OSPF позволяет осуществлять перераспределение (redistribute) маршрутов (см. глоссарий, стр. 205). В каких случаях это может требоваться?

В одной разветвленной сети может быть образовано нескольких автономных систем (см. глоссарий, стр. 202) по причине использования в разных подсетях разных протоколов маршрутизации. Например, в одной подсети может использоваться статическая маршрутизация, в другой — динамическая маршрутизация по протоколу OSPF. В результате это образуется две автономные системы. Чтобы системы могли взаимодействовать друг с другом, на маршрутизаторе, который установлен на границе этих систем, требуется настроить перераспределение маршрутов. В результате произойдет обмен маршрутной информацией, получаемой из этих систем, и они будут иметь связь друг с другом.

На рисунке ниже показана схема взаимодействия нескольких автономных систем.

Рисунок 85. Схема взаимодействия автономных систем

В приведенном примере рассматривается 4 взаимодействующих подсети, 2 из которых входят в одну автономную систему, поскольку они работают по одному протоколу OSPF, остальные — в две другие автономные системы, в которых используются другие способы маршрутизаци. При этом маршрутизатор 1 является граничным маршрутизатором (см. Общие сведения о протоколе OSPF на стр. 141), поскольку он расположен на границе трех автономных систем.

Чтобы узлы сети филиала и сетей партнеров могли обмениваться IP-трафиком друг с другом, выполните следующие настройки:

- На маршрутизаторах 1, 2 и 3 настройте взаимодействие по протоколу OSPF.
- В сети партнера 1 используется статическая маршрутизации, поэтому добавьте вручную статические маршруты:
  - на маршрутизаторе 1 — для сетей за маршрутизатором 4;
  - на маршрутизаторе 4 — для сетей за маршрутизатором 1.

  На маршрутизаторе 1 включите перераспределение статических маршрутов, для того чтобы передать по протоколу OSPF маршрутизаторам 2 и 3 маршруты в сеть партнера 1.
- DHCP-сервер передает информацию маршрутизатору 1 о маршрутах в сеть партнера 2 за маршрутизатором 5. На маршрутизаторе 5 добавьте вручную статические маршруты для сетей за маршрутизатором 1.

  На маршрутизаторе 1 включите перераспределение маршрутов, полученных по DHCP, для того чтобы передать по протоколу OSPF маршрутизаторам 2 и 3 маршруты в сеть партнера 2.

В результате выполненных настроек узлы сети филиала и сетей партнеров смогут обмениваться IP-трафиком друг с другом.

Чтобы настроить параметры перераспределения маршрутов, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 Перейдите на страницу **Сетевые настройки** > **Маршрутизация**, а затем на вкладку **OSPF**.

3 В разделе **Настройки** установите флажок в группе **Распространять маршруты**:

- **DHCP**, чтобы включить перераспределение маршрутов DHCP-сервера.
- **Статические**, чтобы включить перераспределение статических маршрутов.

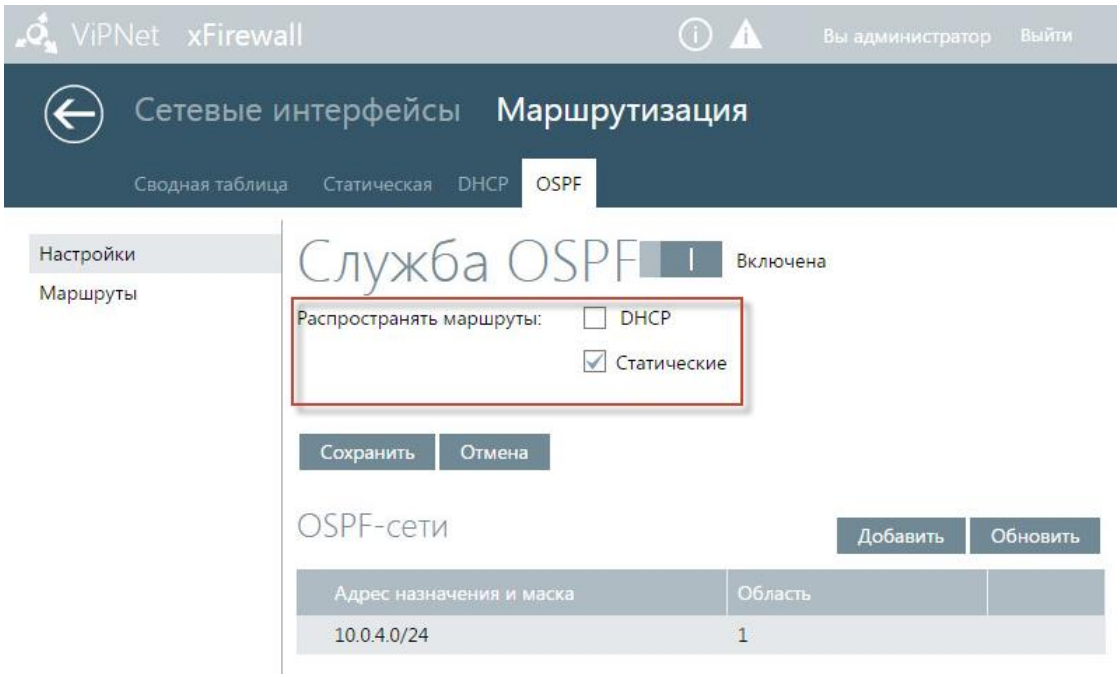

Рисунок 86. Включение перераспределения маршрутов DHCP-сервера

4 Чтобы выключить перераспределение маршрутов, снимите соответствующие флажки.

5 Нажмите кнопку **Сохранить**.

7

Мониторинг состояния ViPNet xFirewall и просмотр журнала IP-пакетов

Мониторинг состояния ViPNet xFirewall 157

Мониторинг по протоколу SNMP 159

Просмотр журнала регистрации IP-пакетов 161

Просмотр статистической информации об IP-пакетах 164

Просмотр журнала событий 165

Просмотр журнала транспортных конвертов (MFTP) 166

Мониторинг состояния ViPNet xFirewall

Вы можете следить за состоянием узла ViPNet xFirewall в режиме реального времени, просматривая графики загрузки процессора и оперативной памяти, время непрерывной работы, а также текущее состояние демонов и драйверов ViPNet xFirewall.

Примечание. Для демона системы защиты от сбоев Failover на странице **Состояние системы** также отображается режим работы (одиночный режим или режим кластера горячего резервирования).

При работе в режиме кластера горячего резервирования графики загрузки процессора и оперативной памяти отображаются только для активного сервера кластера.

Чтобы просмотреть информацию о текущем состоянии ViPNet xFirewall, выполните следующие действия:

1. На начальной странице веб-интерфейса щелкните плитку **Мониторинг**.
2. На странице **Состояние системы** будет отображена информация о ViPNet xFirewall. На данной странице вы можете следить за изменением отображенных параметров.

Внимание! При остановленной службе Failover информация о состоянии системы не отображается.

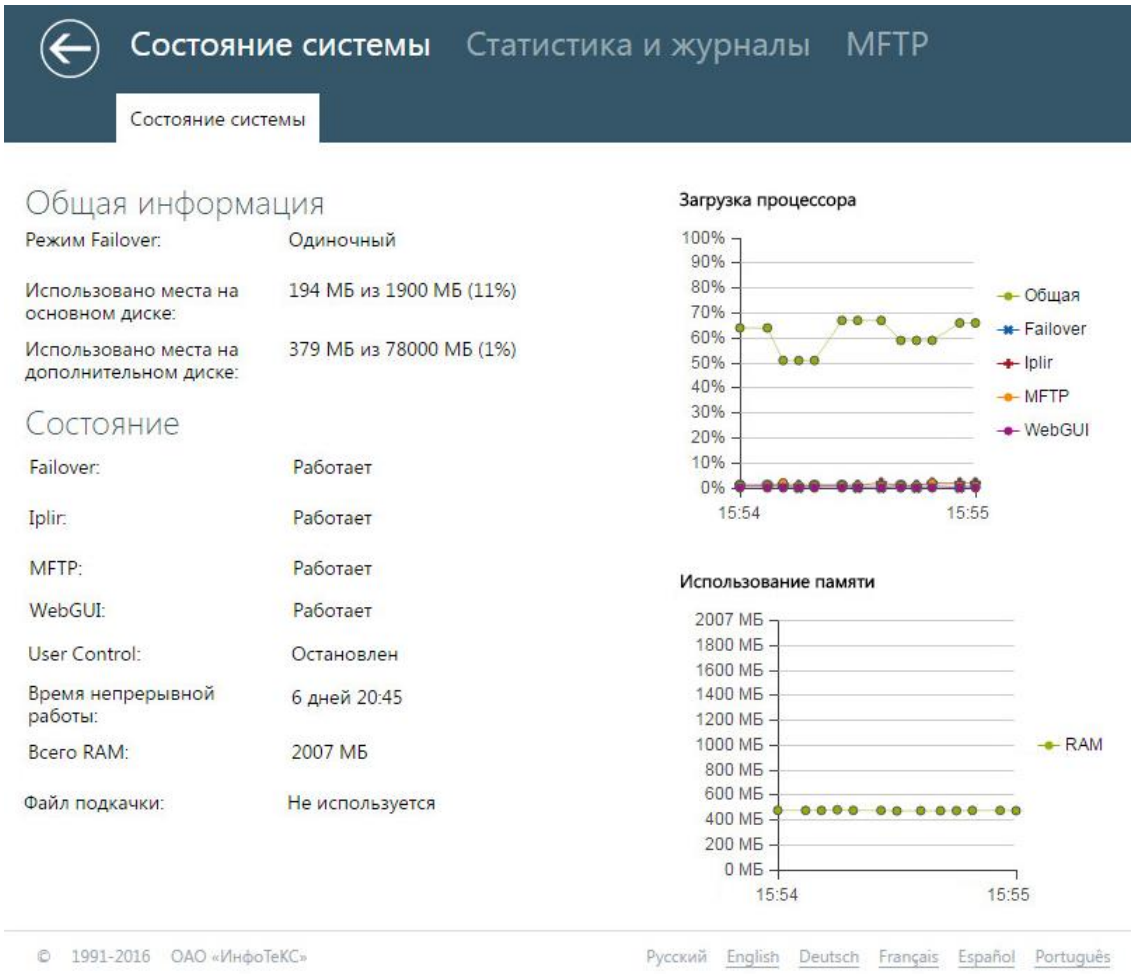

Рисунок 87. Мониторинг состояния ViPNet xFirewall

3 События, связанные с демонами, входящими в состав ViPNet xFirewall, записываются в системный журнал ПО ViPNet. Этот журнал позволяет диагностировать правильность функционирования ПО. Он содержит большое количество деталей о процессах, происходящих внутри служб ViPNet xFirewall, и предназначен для разработчиков.

Мониторинг по протоколу SNMP

С помощью SNMP-агента, входящего в состав ViPNet xFirewall, вы можете удаленно получать информацию о времени работы ViPNet xFirewall, активности сетевых интерфейсов и количестве пропущенных и блокированных пакетов на них, а также уведомлять удаленную станцию управления сетью (NMS) о наиболее важных событиях в работе ViPNet xFirewall (например, выходе из строя активного сервера при работе ViPNet xFirewall в режиме кластера горячего резервирования).

Примечание. ViPNet xFirewall поддерживает протокол SNMP версий 1 и 2.

При работе ViPNet xFirewall в режиме кластера горячего резервирования на удаленную станцию передается информация только о работе активного сервера кластера. Слежение за работой пассивного сервера кластера не производится.

Для получения информации о сетевых узлах ViPNet по протоколу SNMP необходимо выделить компьютер и установить на него специальное программное обеспечение управления сетью (NMS), например WhatsUp Gold. Чтобы получение информации было возможно, импортируйте файл `VIPNET-MIB.txt`, в котором описаны используемые ПО ViPNet объекты SNMP, в NMS (подробнее см. в документации по используемой NMS).

В результате на компьютер будет приходить информация о состоянии ViPNet xFirewall. Для получения этой информации должна использоваться ветка:

```
.iso.org.dod.internet.private.enterprises.infotecs.vipnet (.1.3.6.1.4.1.10812.1)
```

Опрос ViPNet xFirewall по протоколу SNMP рекомендуется выполнять с узлов сети ViPNet. Соответствующие сетевые фильтры по умолчанию включены в список фильтров защиты канала управления. Если опрос будет осуществляться с открытого узла, то в список локальных фильтров открытой сети необходимо добавить аналогичные разрешающие фильтры, указав в них IP-адрес этого узла.

Чтобы настроить мониторинг ViPNet xFirewall по протоколу SNMP, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Системные настройки** > **SNMP**.

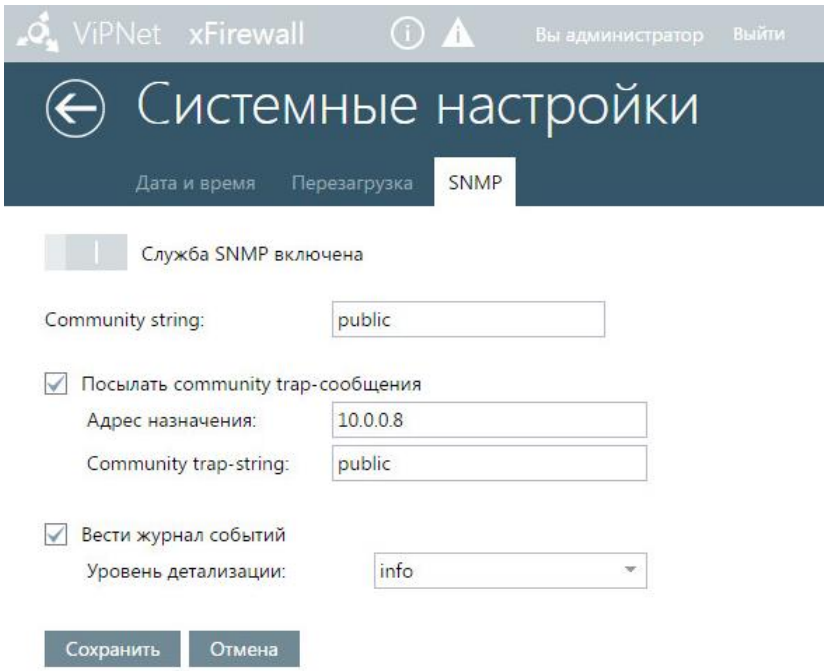

Рисунок 88. Настройка мониторинга по протоколу SNMP

3 Чтобы задать пароль доступа к SNMP-параметрам вашего ViPNet xFirewall, введите его в поле **Community string**. По умолчанию задан пароль `public`.

4 Чтобы использовать оповещения SNMP Traps, установите флажок **Посылать community trap-сообщения** и задайте значения для следующих полей

5 Чтобы задать IP-адрес удаленного узла, на который будут отправляться оповещения SNMP Traps, задайте его в поле **Адрес назначения.**

6 Чтобы на удаленной станции управления сетью при приеме оповещений SNMP Traps проводилась авторизация, задайте пароль в поле **Community trap-string.** По умолчанию задан пароль `public`.

7 Чтобы записывать в системный журнал информацию о работе SNMP-агента, установите флажок **Вести журнал событий** и выберите уровень детализации событий из соответствующего списка:

- `info` (по умолчанию) — записывается только информация, касающаяся инициализации SNMP-агента.
- `debug` — записывается служебная информация, используемая при отладке.
- `error` — записываются ошибки, после которых SNMP-агент может продолжать работу.
- `critical` — записываются критические ошибки, после которых SNMP-агент не может продолжить работу.

8 Чтобы применить изменения, нажмите кнопку **Сохранить**.

Просмотр журнала регистрации IP-пакетов

Управляющий демон ViPNet xFirewall ведет журнал регистрации IP-пакетов, в который заносится информация обо всех IP-пакетах, проходящих через сетевые интерфейсы узла.

Чтобы просмотреть этот журнал, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. На начальной странице веб-интерфейса щелкните плитку **Мониторинг** и перейдите на страницу **Статистика и журналы**. На вкладке **Журнал регистрации IP-пакетов** по умолчанию заданы параметры для просмотра записей обо всех IP-пакетов, прошедших через сетевые интерфейсы собственного узла за последний час (по умолчанию не более 100 записей). Чтобы просмотреть такие записи, нажмите кнопку **Найти**.
3. Чтобы выбрать записи из журнала регистрации IP-пакетов для просмотра, укажите следующие критерии поиска IP-пакетов:
   - В разделе **Признаки IP-пакетов** в соответствующих списках выберите:
     - пользователя Active Directory или Captive portal;
     - приложение, для которого передаются IP-пакеты;
     - прикладной протокол, с использованием которого передаются IP-пакеты;

Примечание.

- Тип прикладного протокола или приложения не всегда определяется по первому IP-пакету (в зависимости от сочетания транспортного и прикладного протоколов). Например, вы создали разрешающее правило для прикладного протокола HTTP. В этом случае для разрешенного HTTP-соединения в журнале регистрации IP-пакетов будут отображаться несколько записей о пакетах с транспортным протоколом TCP и неизвестным прикладным протоколом, так как прикладной протокол еще не определен. После того, как прикладной протокол будет определен, в журнале будут отображаться записи о пакетах с транспортным протоколом TCP и прикладным протоколом HTTP.
- При обновлении модуля DPI некоторые прикладные протоколы, приложения и группы приложений могут быть удалены из списка поддерживаемых. Записи в журнале IP-пакетов с такими протоколами или приложениями будут отображать в качестве имени протокола или приложения «Неизвестно/Неизвестен (ID=номер протокола или приложения)».

     - транспортный протокол, с использованием которого передаются IP-пакеты (TCP, UDP, ICMP или другой);
     - сетевой интерфейс, через который проходят IP-пакеты (eth0, eth1 и так далее);

- тип трафика, к которому относятся IP-пакеты (весь трафик, транзитный управляющий, транзитный открытый, локальный управляющий или локальный открытый);
- тип адреса IP-пакетов (одноадресный, широковещательный или групповой);
- признак трансляции IP-пакетов (транслированные, не транслированные);
- событие, к которому относятся IP-пакеты (блокированный, пропущенный или служебный);

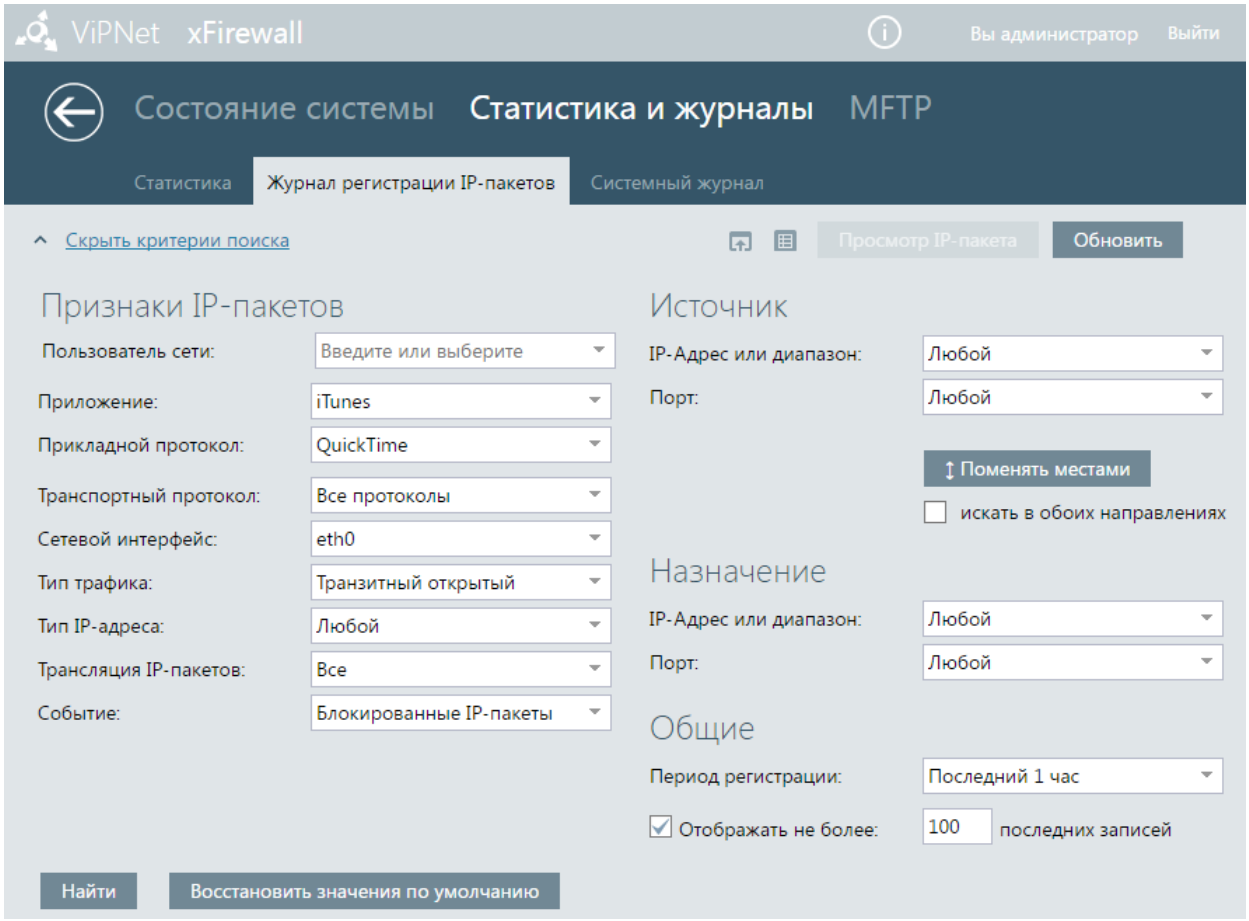

Рисунок 89. Просмотр журнала регистрации IP-пакетов

- В разделе **Источник** (**Назначение**) в соответствующих полях укажите:
  - IP-адрес отправителя (получателя) или диапазон IP-адресов отправителей (получателей);
  - номер порта отправителя (получателя).
- В разделе **Общие**:
  - в поле **Период регистрации** укажите диапазон времени, за который вы хотите просмотреть информацию об IP-пакетах;
  - чтобы ограничить число записей об IP-пакетах, отображаемое в результате поиска, установите соответствующий флажок и укажите это число.

Затем нажмите кнопку **Найти**. В результате на вкладке **Журнал регистрации IP-пакетов** отобразится список записей об IP-пакетах, отвечающих заданным критериям поиска.

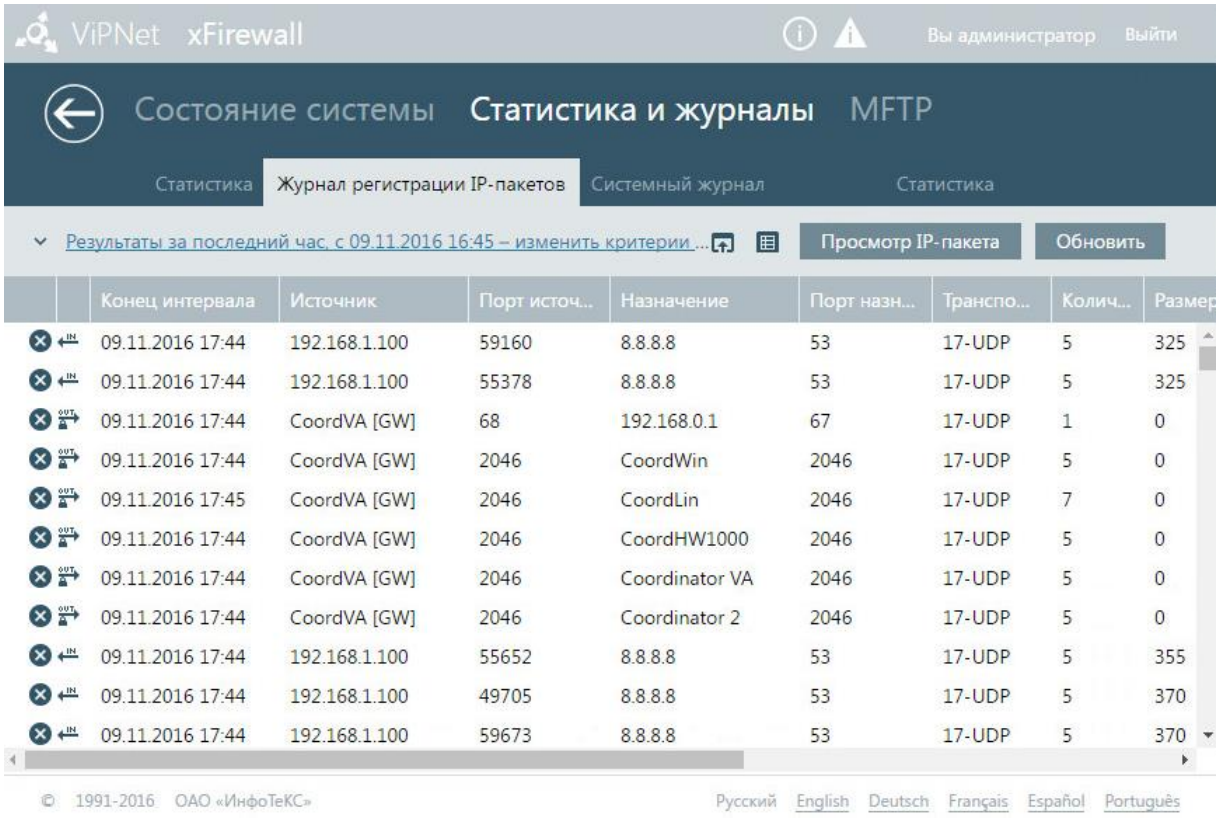

Рисунок 90. Просмотр результатов поиска в журнале IP-пакетов

4 Выполните одно из действий:

- Для просмотра подробной информации об IP-пакете дважды щелкните соответствующую запись в списке.
- Для экспорта списка найденных записей об IP-пакетах в файл формата XLS (например, для последующего анализа) на панели инструментов нажмите кнопку .
- Для завершения просмотра списка найденных записей об IP-пакетах или изменения параметров поиска IP-пакетов в журнале на панели инструментов нажмите ссылку Результаты.

Просмотр статистической информации об IP-пакетах

Чтобы просмотреть статистическую информацию о количестве IP-пакетов, блокированных или пропущенных на узле, выполните следующие действия:

1. Перейдите на страницу **Мониторинг** > **Статистика и журналы** и выберите вкладку **Статистика**. В результате отобразится информация о количестве открытых, зашифрованных, широковещательных открытых и широковещательных зашифрованных IP-пакетах, прошедших через все сетевые интерфейсы узла.
2. Чтобы просмотреть информацию о количестве IP-пакетов, прошедших через определенный сетевой интерфейс ViPNet xFirewall, выберите этот интерфейс в списке на панели инструментов.

Просмотр журнала событий

Чтобы просмотреть системный журнал ViPNet xFirewall, выполните следующие действия:

1 Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).

2 На начальной странице веб-интерфейса щелкните плитку **Мониторинг** и перейдите на страницу **Статистика и журналы**. На вкладке **Системный журнал** по умолчанию заданы параметры для просмотра записей обо всех службах за все время работы ViPNet xFirewall.

3 Чтобы выбрать записи из системного журнала для просмотра, укажите следующие критерии поиска записей:

- В разделе **Фильтр событий** выберите службу в соответствующем списке и введите текстовую строку для поиска. Нажмите кнопку **Применить фильтр**.
- В разделе **Переход к времени** задайте дату и время, чтобы просмотреть записи журнала с указанного момента времени. Нажмите кнопку **Перейти**.

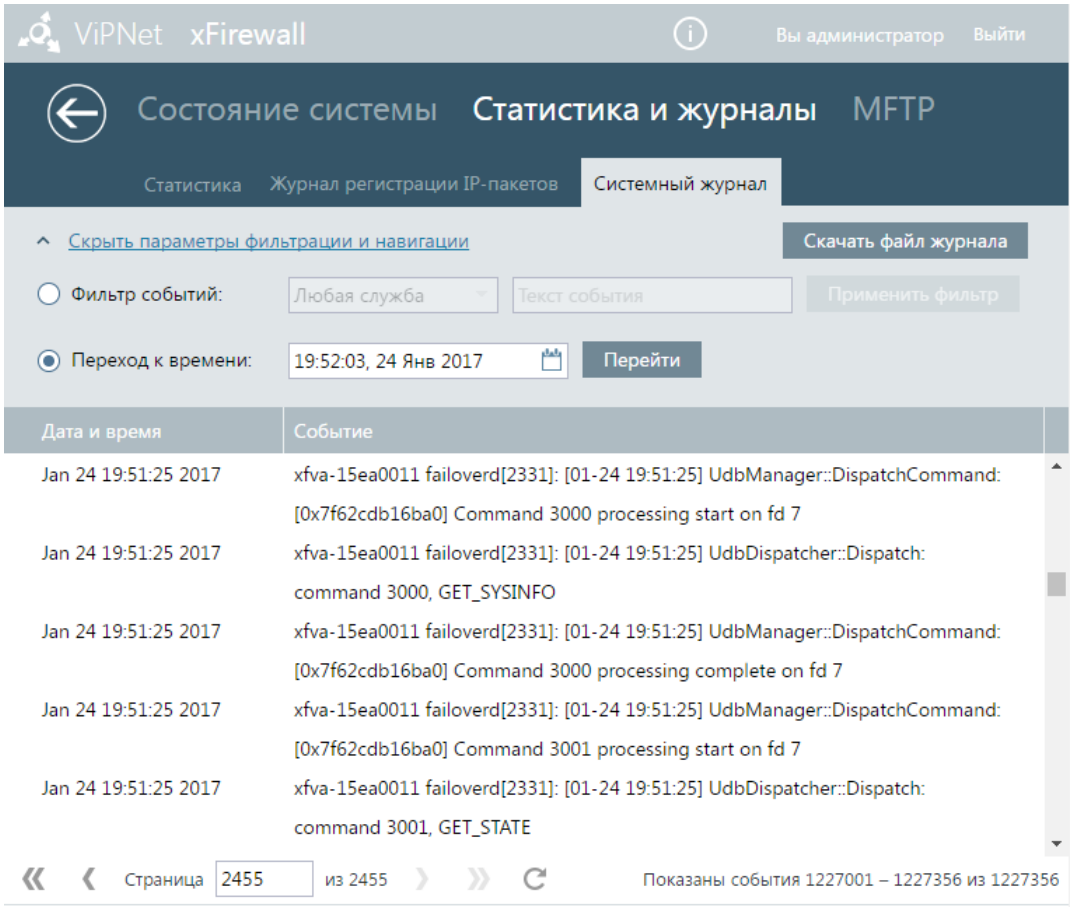

Рисунок 91. Просмотр записей в системном журнале

4 Чтобы загрузить архив с расширением `*.zip`, содержащий текстовый файл журнала событий ПО ViPNet xFirewall, нажмите кнопку **Скачать файл журнала**.

Просмотр журнала транспортных конвертов (MFTP)

Чтобы просмотреть очередь или журнал транспортных конвертов между узлом ViPNet xFirewall и другими узлами сети ViPNet, выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet xFirewall в режиме администратора (см. Подключение к веб-интерфейсу на стр. 19).
2. Перейдите на страницу **Мониторинг** > **Статистика и журналы** и выберите вкладку **MFTP**. В результате вы увидите параметры для просмотра записей обо всех транспортных конвертах между узлом ViPNet xFirewall и другими узлами сети ViPNet за последние три часа. Чтобы просмотреть такие записи, нажмите кнопку **Применить фильтр**.
3. Чтобы выбрать записи из журнала транспортных конвертов для просмотра, укажите следующие критерии поиска транспортных конвертов:
   - В разделе **Основные критерии** выберите:
     - область поиска конвертов — очередь конвертов или журнал конвертов;
     - маску имени файла в соответствующем поле. По умолчанию задана маска «*» для поиска всех файлов.
   - В разделе **Передающие узлы** укажите сетевые узлы сети ViPNet в качестве отправителя и получателя транспортных конвертов.

Примечание. Обратите внимание, что вы должны указать сетевой узел ViPNet xFirewall или в качестве отправителя, или в качестве получателя транспортных конвертов.

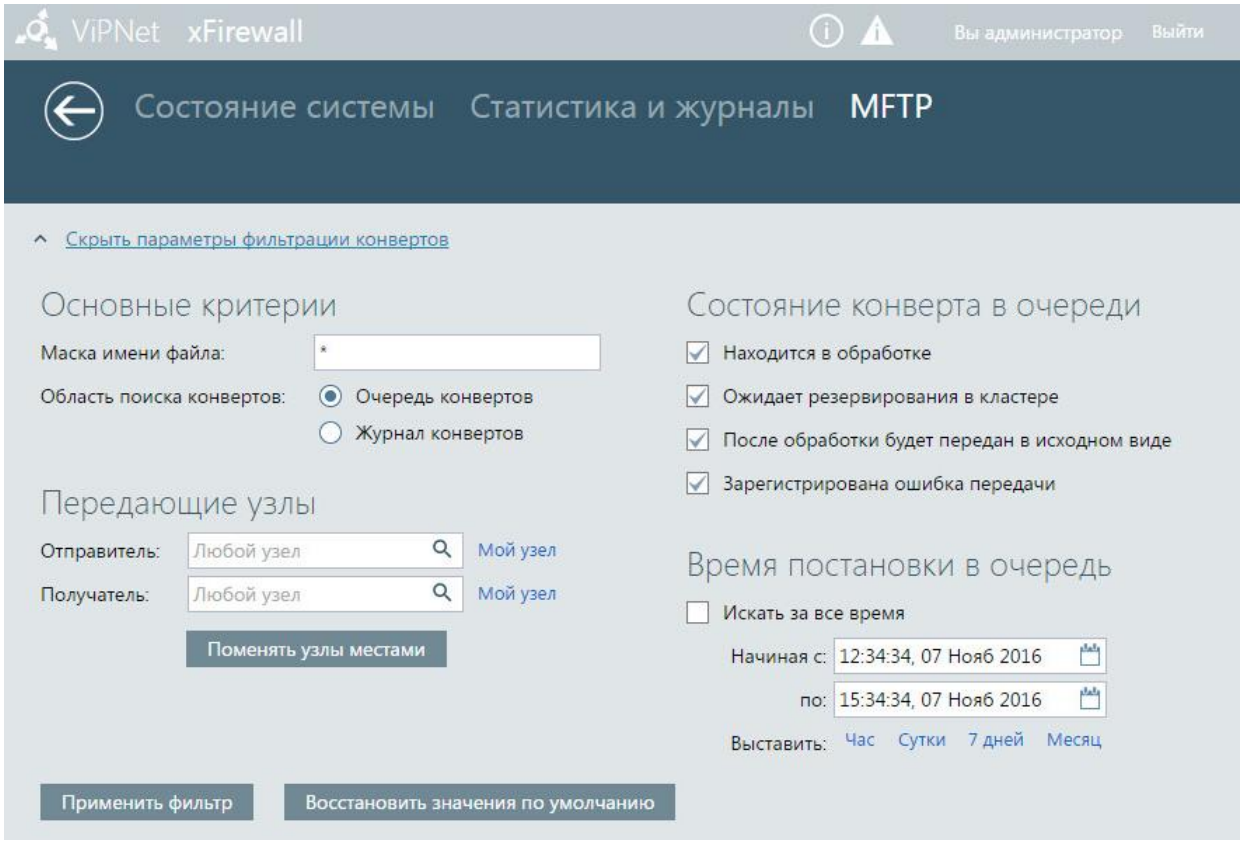

Рисунок 92. Настройка параметров журнала транспортных конвертов

Совет. В разделе **Передающие узлы**:

- Чтобы указать идентификатор сетевого узла, нажмите кнопку , в открывшемся окне выберите нужный узел в списке и нажмите кнопку **Далее**. Чтобы указать собственный сетевой узел, нажмите ссылку **Мой узел**.
- Чтобы поменять сетевые узлы отправителей и получателей, нажмите соответствующую кнопку.

- В разделе **Состояние конверта в очереди** (если вы указали область поиска конвертов как **Очередь конвертов**) установите флажки напротив состояний транспортных конвертов, информацию о которых вы хотите просмотреть:
  - «Находится в обработке»;
  - «Ожидает резервирования в кластере»;
  - «После обработки будет передан в исходном виде»;
  - «Зарегистрирована ошибка передачи».
- В разделе **Состояние конверта в** журнале (если вы указали область поиска конвертов как **Журнал конвертов**) установите флажки напротив состояний транспортных конвертов, информацию о которых вы хотите просмотреть:
  - «Принят»;

- «Отправлен»;
- «Удален»;
- «Поврежден».

○ В разделе **Время постановки в очередь** укажите интервал времени, за который вы хотите просмотреть информацию о транспортных конвертах:

- в списках **Начиная с (по)** укажите диапазон времени, за который вы хотите просмотреть информацию о транспортных конвертах. По умолчанию указан период за последние три часа;
- чтобы найти информацию о транспортных конвертах за все время, установите соответствующий флажок;
- чтобы установить периоды времени в один час, сутки, 7 дней или месяц, нажмите соответствующую ссылку.

Затем нажмите кнопку **Применить фильтр**. В результате отобразится список записей о транспортных конвертах, отвечающих заданным критериям поиска.

4 Для просмотра подробной информации об IP-пакете дважды щелкните соответствующую запись в списке.

A

Сетевые фильтры по умолчанию

Сетевые фильтры, в том числе фильтры системы защиты от сбоев, создаваемые в ViPNet xFirewall по умолчанию, перечислены в таблицах ниже.

Таблица 12. Фильтры защиты канала управления

Название	Источник	Назначение	Протокол	Действие
В активном режиме кластера (нередактируемый)				
ViPNet Service	@any	@local	udp: from 2060 to 2060	pass
В пассивном режиме кластера (нередактируемый)				
Block all vpn traffic	@any	@any	@any	drop
Общие фильтры				
Allow DHCP service	@any	@any	udp: from 67 to 68, from 68 to 67	pass
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Allow ViPNet base services	@any	@any	udp: to 2046, from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet DBViewer	@any	@any	tcp: to 2047	pass
Allow ICAP	@local	@any	tcp: to 1344	pass
Allow ViPNet StateWatcher	@any	@local	tcp: to 5100, 10092	pass

Название	Источник	Назначение	Протокол	Действие
Allow ViPNet MFTP	@any	@any	tcp: to 5000-5003	pass
Allow ViPNet WebGUI	@any	@local	tcp: to 8080	pass
Allow ICMP Ping	@any	@any	icmp8	pass
Allow SSH	@any	@any	tcp: to 22	pass
Allow DNS	@any	@any	udp: to 53	pass
Allow NTP	@any	@any	udp: to 123	pass
Allow UPS service **Примечание.** В исполнении ViPNet xFirewall xF-VA данный фильтр отсутствует.	@any	@any	tcp: to 3493	pass
Allow syslog outgoing	@local	@any	udp: to 514	pass
Allow SNMP	@any	@local	udp: to 161	pass
Allow SNMP traps	@local	@any	udp: to 162	pass
Allow AD WMI	@local	@addc	tcp: to 135	pass
Allow LDAP	@local	@ldap	tcp: to 389, 636	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 13. Локальные фильтры открытой сети (`local`)

Название	Источник	Назначение	Протокол	Действие
В одиночном режиме системы защиты от сбоев, в активном и пассивном режимах кластера (нередактируемые)				
ViPNet Service CommonIn	@any	@local	tcp/udp: to 2046, 2047, 10096, 5100, 10092	drop
ViPNet Service CommonOut	@local	@any	tcp/udp: from 2046	drop
В активном режиме кластера (нередактируемые)				
Failover test IP	@local	<список значений параметров `testip` из `failover.ini`>	icmp	pass

Название	Источник	Назначение	Протокол	Действие
Failover Channel	@local	iface <значение параметра `device` из `failover.ini`>	@any	pass
Failover Channel	<значение параметра `activeip` второго сервера из `failover.ini`>	iface <значение параметра `device` из `failover.ini`>	@any	pass
В пассивном режиме кластера (нередактируемые)				
Failover Channel	@local	iface <значение параметра `device` из `failover.ini`>	@any	pass
Failover Channel	<значение параметра `activeip` второго сервера из `failover.ini`>	iface <значение параметра `device` из `failover.ini`>	@any	pass
ARP requests to active	@local	<список значений параметров `activeip` из `failover.ini`>	udp: to <значение `connect_port` из `failover.ini`>	pass
Block all local traffic	@any	@any	@any	drop
Общие фильтры				
Allow DHCP service	@any	@any	udp: from 67 to 68, from 68 to 67	pass
Allow DHCP-Relay service	@any	@any	udp: from 67 to 67	pass
Allow ICMP Ping	@local	@any	icmp8	pass
Allow DNS	@local	@any	udp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Allow all	@any	@any	@any	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 14. Транзитные фильтры открытой сети (`forward`)

Название	Источник	Назначение	Протокол	Действие
В пассивном режиме кластера				
Block all forward traffic	@any	@any	@any	drop
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

B

Пользовательские группы протоколов по умолчанию

По умолчанию в ViPNet xFirewall настроены пользовательские группы протоколов (см. Группы объектов на стр. 62), перечисленные в таблице ниже.

Таблица 15. Пользовательские группы протоколов, настроенные по умолчанию

Имя группы протоколов	Состав группы протоколов
DHCP	UDP:from 67-68 to 67-68
CITRIX	TCP:to 1494
DNS	UDP:to 53
FTP	TCP:to 21
GRE	IP:47
H323	TCP:to 1720
HTTP	TCP:to 80, TCP:to 8080
HTTP-Proxy	TCP:to 3128
HTTPS	TCP:to 443
IGMP	IP:2
IKE	UDP:to 500
IMAP	TCP:to 143
IPSecESP	IP:50
Kerberos	TCP:to 88, TCP:to 749, UDP:to 88, UDP:to 749

Имя группы протоколов	Состав группы протоколов
L2TP	UDP:to 1701
LDAP	TCP:to 389, UDP:to 389
LotusNotes	TCP:to 1352
MS-SQL	TCP:to 1433-1434, UDP:to 1433-1434
MySQL	TCP:to 3306
NetBIOS-DGM	UDP:from 138 to 138
NetBIOS-NC	UDP:from 137 to 137
NetMeeting	TCP:to 1503
NTP	UDP:to 123
PING	ICMP:8
POP3	TCP:to 110
Postgres	TCP:to 5432
PPTP	TCP:to 1723
RADIUS	UDP:to 1812-1813
RDP	TCP:to 3389
RTSP	TCP:to 554
SCCP	TCP:to 2000
SIP	TCP:to 5060, UDP:to 5060
SMTP	TCP:to 25
SNMP	UDP:to 161
SNMP-Traps	UDP:to 162
SSH	TCP:to 22
Syslog	UDP:to 514
Telnet	TCP:to 23
TFTP	UDP:to 69
UPnP	TCP:to 1900, TCP:to 2869, UDP:to 1900, UDP:to 2869
MFTP	TCP:to 5000-5003
StateWatcher	TCP:to 2047, TCP:to 5100, TCP:to 10092
ViPNetBase	UDP:to 2046, UDP:from 2048 to 2048, UDP:from 2050 to 2050
Cluster	UDP:from 2060 to 2060
ClusterMonitoring	UDP:from 2060 to 2065, UDP:from 2065 to 2060

Имя группы протоколов	Состав группы протоколов
WindowsMobileDevices	TCP:to 990, TCP:to 999, TCP:to 5678, TCP:to 5721, TCP:to 26675
WindowsMobileDevices2	UDP:to 5679
VNC	TCP:to 5900
OSPF	IP:89

C

Типы событий в журнале регистрации IP-пакетов

Типы событий, регистрируемых в журнале IP-пакетов ViPNet xFirewall, можно поделить на следующие группы и подгруппы:

Рисунок 93. Классификация событий в журнале IP-пакетов

Описание типов событий каждой подгруппы приведено в таблицах.

*Таблица 16. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные сетевыми фильтрами защиты канала управления***

Номер события	Описание события
1	Не найден ключ для передачи пакета сетевому узлу с идентификатором, указанным в пакете
2	Неверное значение имитозащитной вставки пакета. Данные защиты канала управления или открытая информация в пакете были изменены при передаче
3	Входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет заблокирован фильтром защиты канала управления
4	Слишком большой тайм-аут пакета, то есть время его отправки отличается от времени его получения на величину, большую указанной в соответствующей настройке
5	Входящий пакет отправлен сетевым узлом с версией драйвера ViPNet, не совместимой с версией драйвера ViPNet на сетевом узле получателя
7	Метод шифрования, код которого указан во входящем пакете, не поддерживается
8	Недопустимые параметры в расшифрованном пакете
9	Неизвестен идентификатор сетевого узла отправителя пакета
10	Неизвестен идентификатор сетевого узла отправителя пакета
13	Превышено максимальное время пребывания пакета в сети
14	Неверный адрес получателя пакета
15	Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов
17	Неверный IP-адрес получателя
18	Неизвестный IP-адрес получателя
19	Подмена узла отправителя
70	Транзитный IP-пакет заблокирован фильтром защиты канала управления

*Таблица 17. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные сетевыми фильтрами открытой сети***

Номер события	Описание события
20	Заблокирован открытый пакет
21	Идентификатор отправителя пакета неизвестен
22	От узла сети ViPNet получен открытый пакет
23	От узла сети ViPNet получен открытый широковещательный пакет
24	На порт, используемый одним из демонов ViPNet, получен открытый пакет

Номер события	Описание события
30	Локальный пакет заблокирован фильтром открытой сети
31	Транзитный пакет заблокирован фильтром открытой сети
32	Широковещательный пакет заблокирован фильтром открытой сети
33	Пакет заблокирован фильтром антиспуфинга
39	Пакет заблокирован фильтром по умолчанию при загрузке компьютера

*Таблица 18. События подгруппы **Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные по другим причинам***

Номер события	Описание события
80	Размер заголовка IP-пакета меньше допустимого
81	Недопустимая версия протокола IP (поддерживается только IPv4)
82	Длина заголовка IP-пакет меньше допустимой
83	Длина IP-пакета меньше указанной в IP-заголовке
84	Значение контрольной суммы в заголовке IP-пакета отличается от ее значения в IP-пакете
85	Размер TCP-заголовка меньше допустимого
86	Размер UDP-заголовка меньше допустимого
87	Обработаны не все фрагменты IP-пакета
88	Широковещательный адрес отправителя в IP-пакете
89	Перекрытие фрагментов IP-пакета. Наиболее устаревший из перекрываемых фрагментов IP-пакета отброшен
90	Для обработки IP-пакета недостаточно ресурсов компьютера. В случае многократного повторения этого события рекомендуется обновить версию ViPNet xFirewall или улучшить вычислительные характеристики компьютера
91	IP-пакет получен во время инициализации драйвера ViPNet
92	Размер IP-пакета превышает 48 Кбайт
93	По истечении допустимого времени получены не все фрагменты IP-пакета
95	Получены два IP-пакета от узлов с разными IP-адресами и одинаковыми идентификаторами
99	Заблокирован фрагментированный IP-пакет
101	Транзитный IP-пакет не может быть маршрутизирован

Номер события	Описание события
102	Прикладной пакет не обработан, так как не загружен модуль обработки на прикладном уровне
103	Количество установленных соединений превышает допустимое значение, заданное в соответствующих настройках
104	Соединение заблокировано, так как параметры исходящих пакетов (socketpair) для этого соединения совпадают с такими параметрами для ранее установленного соединения
105	Не удалось выделить динамический порт для правила трансляции адресов (в пуле нет свободных портов)
111	Не найден ключ обмена
112	Неверное значение имитозащитной вставки в незашифрованном пакете версии 4.2
113	Неизвестный идентификатор сетевого узла отправителя
115	Не удалось найти маршрут для IP-пакета в таблице маршрутизации
116	Не найден сетевой адаптер
117	Не удалось определить MAC-адрес получателя пакета по его IP-адресу
118	Ошибка при шифровании исходящего IP-пакета для узла сети ViPNet
119	Получен зашифрованный IP-пакет неизвестного формата, который не может быть расшифрован
120	Ошибка при отправке IP-пакета защищенному узлу из-за проблем с доступом к этому узлу
121	Ошибка в работе кластера горячего резервирования
122	Получен IP-пакет неизвестного протокола канального уровня
130	Отсутствуют свободные динамические порты, необходимые для создания соединения
131	Ошибка обработки прикладных протоколов: не удалось построить маршрут
132	Ошибка обработки прикладных протоколов: отсутствуют свободные динамические порты UDP
133	Ошибка обработки прикладных протоколов: порты источника и назначения IP-пакета принадлежат разным прикладным сервисам
134	Ошибка обработки прикладных протоколов: ошибка в таблице соответствия между прикладными сервисами и сетевыми протоколами, портами
137	Шифрование исходящего IP-пакета с использованием данного алгоритма запрещено (тесты алгоритма не прошли)
138	Заблокирован IP-пакет на публичный DNS-сервер

*Таблица 19. События группы **Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные зашифрованные IP-пакеты***

Номер события	Описание события
40	Пропущен зашифрованный IP-пакет
41	Пропущен зашифрованный широковещательный IP-пакет
44	Маршрутизация зашифрованного транзитного IP-пакета с подменой адреса получателя

*Таблица 20. События группы **Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные незашифрованные IP-пакеты***

Номер события	Описание события
60	Пропущен незашифрованный IP-пакет
61	Пропущен незашифрованный широковещательный IP-пакет
62	Пропущен незашифрованный транзитный IP-пакет
64	IP-пакет пропущен при запуске операционной системы
65	Пропущен зашифрованный IP-пакет для незарегистрированного узла ViPNet

*Таблица 21. События группы **Все IP-пакеты/Служебные события***

Номер события	Описание события
42	Изменился IP-адрес сетевого узла
46	Изменились параметры доступа к сетевому узлу
47	Истек интервал отправки IP-пакетов, передаваемых сетевым узлом своему серверу соединений. Событие может возникать только для тех узлов, которые работают через межсетевой экран с динамической трансляцией адресов
48	Узел доступен по широковещательному адресу
49	Изменился IP-адрес собственного сетевого узла
110	Новый IP-адрес сетевого узла зарегистрирован на DNS-сервере
114	DNS-имя узла не зарегистрировано на DNS-сервере

D

Записи в журнале событий, связанные с аутентификацией и настройкой оборудования

Ниже приведены протоколируемые события ViPNet xFirewall, связанные с аутентификацией и настройкой оборудования, и соответствующие им записи в журнале событий.

Таблица 22. Протоколируемые события операционной системы Linux

Событие	Пример записей в журнале
Запуск операционной системы	`vmunix: Linux version 3.10.92`

Завершение работы операционной системы	`vmunix: [] drviplir: ViPNet IpLir driver unloaded`
	`vmunix: [] itcscrpt: ViPNet Crypto Driver unloaded`
	`vmunix: [] itcswd: ViPNet WatchDog driver unloaded`
	`vmunix: [] itcskrniface: Kernel interface driver is unloaded`
	`acpid: exiting`
	`syslogd: exiting on signal 15`

Таблица 23. События, протоколируемые при работе пользователя или администратора ViPNet xFirewall

Событие	Пример записей в журнале
Завершение работы операционной системы по команде	`rvpn_shell[1380]: <HALT> Command 'machine halt'.`
Перезагрузка операционной системы по команде	`rvpn_shell[1356]: <REBOOT> Command: machine reboot`
Выход из командного интерпретатора, работающего в режиме пользователя	`login[20446]: pam_unix(login:session): session closed for user user` `rvpn_shell[2190]: <EXIT> Command 'exit'`
Успешный удаленный запуск командного интерпретатора по протоколу SSH	`login[20446]: pam_unix(sshd:session): session opened for user user` `sshd[20448]: Accepted password for user from 13.0.1.94 port 55650 ssh2`
Не удалось запустить командный интерпретатор при удаленном подключении по протоколу SSH	`sshd[20448]: Failed password for user from 13.0.1.94 port 55650 ssh2`
Завершение удаленного подключения по протоколу SSH	`sshd[20448]: pam_unix(sshd:session): session closed for user user`
Успешный переход в режим администратора	`rvpn_shell[1334]: <ENABLE> Command 'enable' – Administrator has logged on.`
Не удалось перейти в режим администратора	`rvpn_shell[2190]: <ENABLE> Command 'enable' - Failed to log on as administrator.`
Переход из режима администратора в режим пользователя	`rvpn_shell[2190]: <EXIT> Command 'exit'`
Вход в системную командную оболочку	`rvpn_shell[2190]: <I_SHELL> You have exited to theLinux system shell.`
Выход из системной командной оболочки	Запись о событии не заносится в журнал.
Принудительное завершение сессии командного интерпретатора	`rvpn_shell[1324]: <A_KICK> Command: 'admin kick'.`

Событие	Пример записей в журнале

Успешное изменение файла `iplir.conf`	`rvpn_shell: <I_CFG> Command: iplir config – starting`
	`rvpn_shell: <I_CFG> Command: iplir config. Config file edited successfully.`
	Отображение изменения:
	`rvpn_shell: 15655c15655`
	`rvpn_shell: < visibility= auto`
	`rvpn_shell: ---`
	`rvpn_shell: > visibility= real`
	`rvpn_shell: <I_CFG> Command: iplir config - iplir.conf has been edited successfully.`

Не удалось изменить содержимое файла `iplir.conf`	`rvpn_shell: <I_CFG> Command: iplir config – starting`
	`rvpn_shell: <I_CFG> Command: iplir config. Incorrect config file.`
	или
	`rvpn_shell: <I_CFG> Command: iplir config - starting`
	`rvpn_shell: <I_CFG> Command: iplir config Cannot edit config while iplir is running`

Успешная смена пароля пользователя	`rvpn_shell[1949]: <PSW> Command: 'admin password'. The new password has been set successfully.`
Не удалось сменить пароль пользователя	`rvpn_shell[1949]: <PSW> Command: 'admin password' could not be executed. The old password is incorrect.`
Удаление справочников и лицензии	`rvpn_shell[1664]: <RMKEYS> Command 'admin remove keys'`
Удаление файлов журнала устранения неполадок и журнала транспортных конвертов MFTP	`syslogd (GNU inetutils 1.9): restart` `rvpn_shell[1664]: <ADM_LOG> 'admin remove logs' (remove the logs).`
Успешная установка справочников и лицензии	`root: Keys will be installed from usb/tftp` `root: 'abn_000a.dst' has been successfully unpacked.`
Локальное обновление ПО	`rvpn_shell[1664]: Command: admin upgrade, starting upgrade script`

Удаленное обновление ПО	`mftpd[5776]: StartVUpgrade: Calling './vupgrade /opt/vipnet/ccc'`
	`mftpd[5776]: run command: ./vupgrade. Arguments:`
	…….
	`vupgrade: Check /mnt/main/opt/vipnet/user/mftpd-config.crg success.`
	`vupgrade: Check /mnt/main/etc/failoverd-config.crg success.`

Событие	Пример записей в журнале
Задание IP-адреса для сетевого интерфейса	`rvpn_shell[1949]: <IFCONF> Command: inet ifconfig eth2 10.0.0.1 netmask 255.255.255.0 Old ifconfig value: BROADCAST MULTICAST MTU:1500 Metric:1`
Сброс настроек сетевого интерфейса	`rvpn_shell[1949]: Interface eth2 is reset.`
Включение сетевого интерфейса	`rvpn_shell[1949]: <IFCONF> The command 'inet ifconfig eth2 up' executed.`
Выключение сетевого интерфейса	`rvpn_shell[1949]: <IFCONF> The command 'inet ifconfig eth2 down' executed.`
Установка параметров скорости сетевого интерфейса	`rvpn_shell[1949]: <IFCONF_SPD> Command: inet ifconfig eth2 speed 10 duplex full`
Добавление статического маршрута	`rvpn_shell[1949]: <RT_ADD> Command: inet route add 123.45.67.89 netmask 255.255.255.0 gateway 192.168.32.50. Static route has been added successfully.`
Удаление статического маршрута	`rvpn_shell[1949]: <RT_DEL> Command: inet route delete 123.45.67.89. Static route has been deleted successfully.`
Создания виртуального интерфейса VLAN	`rvpn_shell[1949]: <I_VLAN_ADD> Command: 'inet ifconfig eth2 vlan add 2'. The new vlan interface eth2.2 has been created.`
Удаление виртуального интерфейса VLAN	`rvpn_shell[1949]: <I_VLAN_DELETE> Command: 'inet ifconfig eth2 vlan delete 2'. The vlan interface eth2.2 has been deleted.`
Сохранение копии конфигурации	`rvpn_shell[1949]: <CFG_SV> Command: admin config save test_conf.`
Загрузка копии конфигурации	`rvpn_shell[1949]: <CFG_LD> Command: admin config load test_conf.`
Экспорт журнала регистрации IP-пакетов на USB-носитель	`rvpn_shell[1949]: <ADM_EXP> Command: 'admin export packetdb usb'.`
Экспорт файлов журнала устранения неполадок	`rvpn_shell[1949]: <ADM_EXP> Command: admin export logs usb`
Экспорт справочников, лицензии и настроек	`rvpn_shell[1949]: <ADM_EXP> Command: 'admin export binary-encrypted'.`

Изменение сетевых фильтров и правил трансляции адресов	Отображение изменения:
	`iplircfg[21590]: User rules dataname has been changed.`
	`iplircfg[21590]: <Rules>`
	`iplircfg[21590]: + <Rule IsActive="true" xsi:type="vn:LocalRule">`
	`iplircfg[21590]: + <RuleId>100001</RuleId>`
	`iplircfg[21590]: </Rule>`

Событие	Пример записей в журнале
Включение вывода сообщений о событиях	`rvpn_shell[1949]: <DBG_ON> Command 'debug on -device tty1, facility daemon, level debug'.`
Выключение вывода сообщений о событиях	`rvpn_shell[1949]: <DBG_OFF> Command 'debug off -device tty1'.`

Таблица 24. События, связанные с запуском или остановкой демонов ViPNet xFirewall

Событие	Пример записей в журнале
Загрузка драйверов и запуск демонов ViPNet xFirewall	`rvpn_shell[1399]: <ADM_VSTART> Command 'vpn start'.`
Выгрузка драйверов и завершение работы демонов ViPNet xFirewall	`rvpn_shell[1399]: <ADM_VSTOP> Command 'vpn stop'.`
Запуск демона failoverd, отвечающего за функционирование системы защиты от сбоев	`failoverd[1479]: Starting failover in single/cluster mode` `rvpn_shell[1399]: <F_STR> Command: failover start`
Завершение работы демона failoverd, отвечающего за функционирование системы защиты от сбоев	`failoverd[1217]: Caught quit signal, exiting` `rvpn_shell[1399]: <F_STP> Command: failover stop`
Запуск управляющего демона iplircfg	`iplircfg[1448]: IPLIR daemon is running` `rvpn_shell[1399]: <I_STR> Command: iplir start`
Завершение работы управляющего демона iplircfg	`iplircfg[1363]: Exiting daemon` `rvpn_shell[1399]: <I_STP> Command: iplir stop`
Запуск транспортного модуля MFTP	`rvpn_shell[1399]: <M_STR> Command: mftp start` `mftpd[1463]: Init MFTP manager ... OK`
Завершение работы транспортного модуля MFTP	`mftpd[1229]: Exiting MFTP manager` `rvpn_shell[1399]: <M_STP> Command: mftp stop`
Перезапуск веб-сервера ViPNet xFirewall	`rvpn_shell[1399]: <WUI_RST> Command: webui restart`

Таблица 25. События, связанные с работой системы защиты от сбоев

Событие	Пример записей в журнале
Смена режима работы сервера кластера из пассивного в активный	`failoverd[1284]: switching to active mode`

Событие	Пример записей в журнале

Перезагрузка сервера кластера из-за сбоя на сетевом интерфейсе	`failoverd[1258]: failure detected on interface eth1`
	`failoverd[1258]: one or more subsystems failed, rebooting`
	`failoverd[1258]: Rebooted due to network error on eth1 at <дата и время>`

Перезагрузка сервера кластера из-за конфликта режимов	`failoverd[1411]: Rebooted due conflict mode at <дата и время>`
Перезагрузка сервера кластера из-за обнаружения демоном failoverd ошибки другого контролируемого демона	`failoverd[1411]: [02-01 21:12:54] CheckApp: [mentor.cpp]: Reached maximum count of application restarts [iplircfg] pid 0` `failoverd[1411]: Rebooted due to watcher detected error at <дата и время>`

Таблица 26. События, связанные с работой антивируса и контроля содержимого трафика прокси-сервера

Событие	Пример записей в журнале
Сработало запрещающее правило контроля содержимого трафика по HTTP-методу	`0 192.168.56.121 TCP_DENIED/403 4293 GET http://www.address.com/ - NONE - text/html`
Сработало запрещающее правило контроля содержимого трафика по MIME-типу	`657 192.168.56.121 TCP_DENIED_REPLY/403 3974 GET http://www.address.com/file.zip - FIRST_UP_PARENT/10.0.25.3 text/html`
Антивирус заблокировал скачивание зараженного файла	`icapserver[6069]: RESPMOD 127.0.0.1 - 192.168.15.233 http://www.rexswain.com/eicar.zip INFECTED EICAR-Test-File`

E

Поддерживаемые приложения

Ниже приведен список приложений, которые можно указать в параметре `dpiapp <название приложение>` при создании транзитного фильтра открытой сети.

unknown, 1-upload-com, 10upload-com, 123upload, 139pan-com, 163pan-com, 1clickshare-net, 1fichier-com, 1kxun, 2channel, 2gis, 2shared-com, 360 total security, 4fastfile-com, 4share-ws, 4shared-com, 4us-to, 9ku, activesync, adobe creative cloud, adobeconnect, adrive, after school, age of warring empire, aim, aimini, airbnb, akamai cloud, alibaba, aliexpress, alipay, alldrives-ge, allshares-ge, amazon chime, amazon cloud, amazon drive, amazon prime music, amazon prime video, amazon services, amazon shopping, anghami, angry birds, annonhost-net, antsp2p, anydesk, apns, apple geolocation, apple maps, apple music, apple services, applejuice, ares, armagetron, asixfiles-com, audiko, audiogalaxy, auth0, avg antivirus, avira antivirus, azar, backblaze, badongo-com, badoo, baidu, banashare-com, battlefield, battlenet, bestsharing-com, betternet, biggerupload-com, bitshare-com, bittorrent, bluejeans, bolt, booking-com, boom beach, boosterking-com, box, bubble witch, burner, candy crush, candy crush soda, cedexis, channel 4od, channel one, chatcube, ciaomobile hdtv, citrix, citrix xenapp, citrixgoto, clash of clans, clash royale, cloudflare, cloudme, clubpenguin, cnn, cntv, cobrashare-sk, comodounite, constant contact, coolshare-cz, cramit-in, crashlytics, crashplan, crime city, crocko-com, crossfire, ctitv, cum-com, cyberghost, czshare-com, dailymotion, data-hu, data-loading-com, dataport-cz, datei-to, dazn, deezer, demand 5, dena, depositfiles-com, destiny, didi, digicel music, digicel playgo, digicel topup, directconnect, disney storytime, docusign, dofus, doook, dota 2, dota legend, downupload-com, drivelock, dropbox, dubsmash, duo duo, duokan, ea games, ea origin, easy taxi, easy-share-com, easybytez-com, easypaste-org, ebay, ebuddy, edisk, edonkey, endomondo, enlegion, enterupload-com, epic browser proxy, epic games, espn, euroshare-eu, evernote, extabit-com, eyvx-com, facebook, facebook cloud, facetime, farm hero, fastfileshare-com-ar, fastly, feidian, fetnet, ficall, fiesta, fik1-com, file-upload-net, file2upload-net, fileape-com, filearchiv-ru, filearn-com, filedude-com, filefactory-com, filehook-com, filehost-tv, filejungle-com, filemaze-ws, fileover-net, filepost-com, filepost-ru, filer-net, files-mail-ru, files-to, filesend-net, fileserve-com, filesflash-com, fileshare-in-ua, filesmonster-com, filesonic-com, filesonic-in, filestube-com, filetopia, fileupyours-com, filevo-com, flickr, florensia, forfone, foursquare, fox sports, freakshare-net, freenet, freespace-by, friendster, fring, fshare-vn, fsx-hu, fubon e-broker, funplus, funshion, fuze meeting, gadu-gadu,

gaiafile-com, game of war, gamefront-com, gamekit, gigapeta-com, gigasize-com, giphy, github, gnutella, good, google ads, google allo, google analytics, google apis, google app engine, google calendar, google cloud, google docs, google drive, google duo, google earth, google fcm, google hangouts, google mail, google maps, google play, google play music, google plus, google shared services, gotomeeting, gotomypc, gotoupload-com, grindr, grooveshark, guild wars 2, guildwars, half-life 2, halfbrick studios, hamachivpn, hamivideo, hay day, hellshare-com, here, hi5, hidrive, hightail, hike messenger, hinet, hitfile-net, hotmail, houseparty, httptunnel, huddle, hulkshare-com, hulu, hyperfileshare-com, hyread, i-filez-com, icecast, icflix, icloud, icq, icrypt, idrive, ifile-it, iflix, iheartradio, ileader, imesh, imessage, imgur, imo, implus, instagram, intralinks, io, ios app store, ip multimedia subsystem, iperf, iplayer, ipp, iptv, ipvanish, iskoot, itunes, itunes radio, itunesu, itv, ivi-ru, iwow systex, jakfile-com, jap, jingdong, jumbofiles-com, kakaotalk, kankan, kaspersky antivirus, kazaa/fasttrack, kewlshare-com, kickload-com, kik messenger, king gaming, king of avalon, king of pirates, kinopoisk, kollect book, kono, last-fm, league of legends, learninghub-online, leteckaposta-cz, letitbit-net, letv, life church, limelight cloud, line, line rangers, lineage 2, linkedin, livejasmin, liveperson, load-to, loadfiles-in, logmein, loop caribbean local news, loop pacific local news, loop trade classifieds, lotus notes, lyft, magicjack, magine tv, magv, magv kids, mail-ru, manolito, mapbox, maplestory, mapmyrun, maxdome, mediafire-com, meebo, meetic group, mega, megafree-kz, megaporn-com, megarapid-eu, megashare-com, megashare-vnn-vn, megashares-com, megaupload-com, mei lu, microsoft dynamics nav, microsoft exchange, microsoft services, miduplоad-com, mig33, minecraft, missupload-com, mitake, mobile strike, modern war, mojo, moves, movreel-com, mplus, msn, multishare-cz, musical_ly, mute, my digicel, mybook, mycard, myfitnesspal, mymusic, myspace, myvideo tw, national baseball, naver, net2phone, netflix, netload-in, netuploaded-com, new relic, next tv, niantic labs, nickelodeon play, niconico, nike plus, nimbuzz, nintendo network, norton security, ntt docomo, octoshape, odnoklassniki, odsiebie-najlepsze-net, off, office 365, onedrive, oovoo, openft, opera mini, oracle database, orkut, oron-com, os update, oscar, outlookmobile, paltalk, pando, pandora, path, path of exile, payeasy, paypal, pcanywhere, pdproxy, periscope, pinkfong, pinterest, plants vs zombies 2, platinshare-com, playstation network, playtales, pochta rossii, poison ivy, pokemon go, popcap, popo, pornhub, ppfilm, pplive, ppstream, prisma, private internet access, psiphon, pubu bookbuffet, putshare-com, qip-ru, qq, qqgame, qqlive, qshare-com, quake, qualys, quickshare-cz, qvod, rackspace cloud, rally, rapidshare-com, rapidshark-pl, rdio, realma, reddit, redmine, redtube, renren, rfactor, rhapsody, rovio gaming, runkeeper, runtastic, rusfolder, rutube, salesforce, sanupload-com, sap, sarahah, savefile-com, scribd-com, scydo, second life, sendspace-com, share-online, share-rapid-cz, sharebigfile-com, shareflare-net, shazam, shoutcast, shragle-com, signal, simcity buildit, simfy, simpleupload-net, sina weibo, sinatv, skinny, skout, sky go, skyking, skype, skype for business, slack, slacker, sling tv, slingbox, smule, snapchat, softbank onlineshop, softethernet, sohu, sopcast, soribada, soulseek, soundcloud, speakaboos, speedshare-org, speedtest, spideroak, splashfighter, spotify, spreecast, spreed, sptg tv, stackpath cloud, starwars galaxy of heroes, steam, storage-to, streetvoice, suda phone, sugarsync, supercell, surfeasy, surveymonkey, symantec, syncplicity, synology, taaze, tango, taobao, teamspeak, teamviewer, telegram, telnet, tenor, terafiles-net, textplus, three bamboo, threema, thunder/webthunder, tibia, tiger vpn, tigertext, timely tv, tinder, tmall, tomtom, tor, trend micro worry-free, tripadvisor, trulia, truphone, ttpod, tumblr, tunabox-net, tunein radio, tunnelbear, turbobit-net, turbobit-ru, turboupload-com, turner, tvbs, tvuplayer, twitch, twitter, u-115-com, uber, ubuntu one, ugotfile-com, uloz-to, ultrabac, ultrashare, ultrasurf, unibytes-com, unity, unlimit-co-il, up-4share-vn, up-file-com, upload-com-ua, uploadbox-com, uploadc-com, uploaded, uploader-pl, uploadfloor-com, uploading-com, uploadingit-com, uploadking-com, uploadstation-com, upnito-sk, upptalk, uptobox-com, usenet, usershare-net, ustream, uusee, vbulletin, vcast, ventrilo, veohtv, vevo, vibe, viber, videobb-com, vimeo, vine, vippie, vk, vnc, voipswitch, voipswitch voip tunnel, vonage, voxer, vpn-x, vudu, vyprvpn, warcraft 3, watchever, waze, wealth god, webdav, webex, webqq, wechat, whatsapp, wickr, wikipedia, windows azure, windows store, wire messenger, wish, workout trainer, world of kung fu, world of warcraft, wowza, wuala, wupload-com, x7-to, xbox gaming console, xing, xnxx, xvideos, yahoo, yandex, yelp, yik yak, youku tudou, youporn, yourfilehost-com, yourfreedom tunnel, youtube, yuanta web, yunfile, zalo, zattoo, zendesk, zenmate vpn, zero vpn, ziddu-com, zoho work online, zshare-net, zynga

F

Поддерживаемые прикладные протоколы

Ниже приведен список прикладных протоколов, которые можно указать в параметре `dpiprotocol <название протокола>` при создании транзитного фильтра открытой сети.

unknown, undetected, adobeconnect, afp, age of warring empire, aimini, amqp, applejuice, ares, armagetron, audiogalaxy, avi, bacnet, battlefield, battlenet, bgp, bitcoin, bittorrent, bolt, cassandra internode communication, cassandra query language, chatcube, citrixgoto, clubpenguin, coap, comodounite, crashplan, crossfire, cyberghost, dce rpc, destiny, dhcp, dhcpv6, diameter, directconnect, dnp3, dns, dofus, doook, dota 2, ea origin, ebuddy, edonkey, egp, fasp, fasttrack, feidian, fiesta, filetopia, fix, flash, florensia, flute, freenet, fring, ftp, funshion, fuze meeting, gadu-gadu, gamekit, gnutella, good, gre, gtp, guild wars 2, guildwars, h323, half-life 2, hamachivpn, hike messenger, http, iax, ica, icecast, icmp, icmpv6, idrive, iec61850, igmp, imap, imesh, imo, implus, ip in ip, iperf, ipfix, iplayer, ipmi, ipp, ipsec, ipv4, ipv6, irc, isakmp, jap, jbk3000, kakao, kerberos, kik messenger, kontiki, l2tp, ldap, ldp, league of legends, letv, line, lineage 2, local peer discovery, lotus notes, manolito, mapi, maplestory, meebo, megaco, mgcp, microsoft dynamics nav, microsoft exchange, mig33, minecraft, mms, modbus, mojo, move, mpeg, mplus, mqtt, msn, msrp, multicastdns, multimediamessaging, mute, mysql, netbios, netflow, netmotion, nfs, nintendo network, nntp, ntlm, ntp, ocsp, octoshape, off, ogg, oovoo, opc ua, openflow, openvpn, opera mini, oracle database, oscar, ospf, paltalk, pando, path of exile, pcanywhere, pcoip, pdproxy, playstation network, poison ivy, pop, popo, postgresql, ppfilm, pplive, ppp, ppstream, pptp, psiphon, qq, qqlive, quake, quic, quicktime, qvod, radius, rdp, realdatatransport, realmedia, rfactor, rhapsody, rim proprietary, rsvp, rsync, rtcp, rtmp, rtp, rtsp, s7comm, sap, scada, sctp, scydo, second life, shoutcast, silverlight, sip, skinny, skype, skype for business, smb/cifs, smtp, snmp, soap, socks, softethernet, sopcast, soulseek, speedtest, splashfighter, spotify, srtcp, srtp, ssdp, ssh, ssl, sstp, stealthnet, steam, stratum mining, stun, supercell, synology, syslog, t3, tacacs, tango, tcp, tds, teamspeak, teamviewer, telegram, telnet, teredo, tftp, threema, thrift, thunder/webthunder, tibia, tor, tvants, tvuplayer, twitch, udp, ultrasurf, uusee, ventrilo, veohtv, viber, vnc, voipswitch voip tunnel, vpn-x, vtun, vyprvpn, wap-wsp, wap-wtls, wap-wtp-wsp, warcraft 3, webex, webqq, websocket, wechat, whatsapp, whois, windowsmedia, winmx, winny, world of kung fu, world of warcraft, wowza, wuala, xbox, xdcc, xdmcp, xmpp, yahoo, yourfreedom tunnel, zalo, zattoo, zero, zero vpn, zeromq

G

Поддерживаемые группы приложений

Ниже приведен список групп приложений и их состав (приложения и прикладные протоколы). Названия групп приложений можно указать в параметре `dpigroup <группа приложений>` при создании транзитного фильтра открытой сети.

Группа business

Приложения в группе:

2gis, 360 total security, activesync, adobeconnect, airbnb, akamai cloud, alibaba, aliexpress, alipay, amazon chime, amazon drive, amazon shopping, apple geolocation, apple maps, apple services, auth0, avg antivirus, avira antivirus, backblaze, cedexis, citrix, citrix xenapp, cloudflare, constant contact, crashlytics, crashplan, digicel topup, docusign, drivelock, duokan, ebay, facebook cloud, fastly, fuze meeting, good, google ads, google analytics, google apis, google calendar, google docs, google earth, google maps, google play, hightail, huddle, ileader, intralinks, ios app store, iwow systex, jingdong, kaspersky antivirus, learninghub-online, limelight cloud, liveperson, lyft, magv, magv kids, mapbox, microsoft dynamics nav, microsoft exchange, microsoft services, mitake, new relic, norton security, ntt docomo, office 365, outlookmobile, payeasy, paypal, pochta rossii, qualys, rackspace cloud, rally, redmine, salesforce, sap, skype for business, slack, softbank onlineshop, stackpath cloud, surveymonkey, symantec, taobao, three bamboo, tmall, tomtom, trend micro worry-free, tripadvisor, trulia, uber, ultrabac, wealth god, windows store, wish, yuanta web, zendesk, zoho work online

Прикладные протоколы в группе:

adobeconnect, bitcoin, crashplan, fix, fuze meeting, good, ica, microsoft dynamics nav, microsoft exchange, nntp, quic, sap, skype for business, stratum mining, synology, zero

Группа conference

Приложения в группе:

citrixgoto, gotomeeting, lotus notes, oovoo, spreed, webex

Прикладные протоколы в группе:

citrixgoto, lotus notes, oovoo, webex

Группа database

Приложения в группе:

oracle database

Прикладные протоколы в группе:

cassandra internode communication, cassandra query language, mysql, oracle database, postgresql, tds

Группа e-commerce

Приложения в группе:

loop trade classifieds

Прикладные протоколы в группе:

нет

Группа filetransfer

Приложения в группе:

adrive, box, cloudme, dropbox, google drive, hidrive, icloud, idrive, mega, onedrive, spideroak, sugarsync, syncplicity, synology, ubuntu one, webdav, windows azure

Прикладные протоколы в группе:

afp, fasp, flute, ftp, idrive, nfs, rsync, smb/cifs, tftp

Группа gaming

Приложения в группе:

angry birds, armagetron, battlefield, battlenet, boom beach, bubble witch, candy crush, candy crush soda, clash of clans, clash royale, clubpenguin, crime city, crossfire, dena, destiny, dofus, dota 2, dota legend, ea games, ea origin, epic games, farm hero, fiesta, florensia, game of war, gamekit, guild wars 2, guildwars, half-life 2, halfbrick studios, hay day, king gaming, king of avalon, king of pirates, league of legends, line rangers, lineage 2, maplestory, mei lu, mig33, minecraft, mobile strike, modern war, national baseball, niantic labs, nintendo network, path of exile, plants vs zombies 2, playstation network, playtales, pokemon go, popcap, qqgame, quake, rfactor, rovio gaming, second life, simcity buildit, splashfighter, starwars galaxy of heroes, steam, supercell, tibia, unity, warcraft 3, world of kung fu, world of warcraft, xbox gaming console, zynga

Прикладные протоколы в группе:

age of warring empire, armagetron, battlefield, battlenet, clubpenguin, crossfire, destiny, dofus, dota 2, ea origin, fiesta, florensia, gamekit, guild wars 2, guildwars,

half-life 2, league of legends, lineage 2, maplestory, mig33, minecraft, nintendo network, path of exile, playstation network, quake, rfactor, second life, splashfighter, steam, supercell, tibia, warcraft 3, world of kung fu, world of warcraft, xbox

Группа generic

Приложения в группе:

unknown

Прикладные протоколы в группе:

ipv4, ipv6, tcp, thrift, udp, undetected, unknown, zeromq

Группа industrial

Приложения в группе:

нет

Прикладные протоколы в группе:

amqp, bacnet, coap, dnp3, iec61850, jbk3000, modbus, mqtt, opc ua, s7comm, scada

Группа mail

Приложения в группе:

google mail, hotmail, mail-ru

Прикладные протоколы в группе:

imap, mapi, pop, smtp

Группа messaging

Приложения в группе:

aim, apns, bluejeans, doook, ebuddy, enlegion, gadu-gadu, google allo, google fcm, google hangouts, hike messenger, icq, icrypt, imessage, imo, implus, io, kakaotalk, kik messenger, meebo, mplus, msn, nimbuzz, oscar, paltalk, popo, qq, signal, snapchat, telegram, tenor, threema, tigertext, upptalk, usenet, vibe, voxer, wechat, whatsapp, wickr, wire messenger, yahoo, zalo

Прикладные протоколы в группе:

doook, ebuddy, gadu-gadu, hike messenger, imo, implus, irc, kakao, kik messenger, meebo, mplus, msn, msrp, oscar, paltalk, popo, qq, telegram, threema, wechat, whatsapp, xdcc, xmpp, yahoo, zalo

Группа mobile

Приложения в группе:

bolt, funplus, ip multimedia subsystem, nike plus, opera mini

Прикладные протоколы в группе:

bolt, multimediamessaging, opera mini, rim proprietary, wap-wsp, wap-wtls, wap-wtp-wsp

Группа network management

Приложения в группе:

iperf, ipp, os update, speedtest

Прикладные протоколы в группе:

bgp, dhcp, dhcpv6, diameter, dns, egp, icmp, icmpv6, igmp, iperf, ipfix, ipmi, ipp, kerberos, ldap, ldp, megaco, multicastdns, netbios, netflow, ntlm, ntp, openflow, ospf, radius, rsvp, sctp, snmp, speedtest, ssdp, syslog, t3, tacacs, whois

Группа peer to peer

Приложения в группе:

aimini, antsp2p, applejuice, ares, bittorrent, directconnect, edonkey, filetopia, freenet, gnutella, imesh, manolito, mojo, mute, off, openft, pando, soulseek, thunder/webthunder

Прикладные протоколы в группе:

aimini, applejuice, ares, bittorrent, directconnect, edonkey, fasttrack, filetopia, freenet, gnutella, imesh, local peer discovery, manolito, mojo, mute, off, pando, soulseek, stealthnet, thunder/webthunder, winmx, winny

Группа remote control

Приложения в группе:

anydesk, gotomypc, logmein, pcanywhere, poison ivy, teamviewer, telnet, vnc

Прикладные протоколы в группе:

dce rpc, pcanywhere, pcoip, poison ivy, rdp, soap, ssh, teamviewer, telnet, vnc, xdmcp

Группа sharehosting

Приложения в группе:

1-upload-com, 10upload-com, 123upload, 139pan-com, 163pan-com, 1clickshare-net, 1fichier-com, 2shared-com, 4fastfile-com, 4share-ws, 4shared-com, 4us-to, alldrives-ge, allshares-ge, annonhost-net, asixfiles-com, badongo-com, banashare-com, bestsharing-com, biggerupload-com, bitshare-com, boosterking-com, cobrashare-sk, coolshare-cz, cramit-in, crocko-com, cum-com, czshare-com, data-hu, data-loading-com, dataport-cz, datei-to, depositfiles-com, downupload-com, easy-share-com, easybytez-com, easypaste-org, edisk, enterupload-com, euroshare-eu, extabit-com, eyvx-com, fastfileshare-com-ar, fik1-com, file-upload-net, file2upload-net, fileape-com, filearchiv-ru, filearn-com, filedude-com, filefactory-com, filehook-com, filehost-tv, filejungle-com, filemaze-ws, fileover-net, filepost-com, filepost-ru, filer-net, files-mail-ru, files-to, filesend-net, fileserve-com, filesflash-com, fileshare-in-ua, filesmonster-com, filesonic-com, filesonic-in, filestube-com, fileupyours-com, filevo-com, freakshare-net, freespace-by, fshare-vn, fsx-hu, gaiafile-com, gamefront-com, gigapeta-com, gigasize-com, gotoupload-com, hellshare-com, hitfile-net, hulkshare-com, hyperfileshare-com,

i-filez-com, ifile-it, jakfile-com, jumbofiles-com, kewlshare-com, kickload-com, leteckaposta-cz, letitbit-net, load-to, loadfiles-in, mediafire-com, megafree-kz, megaporn-com, megarapid-eu, megashare-com, megashare-vnn-vn, megashares-com, megaupload-com, midupload-com, missupload-com, movreel-com, multishare-cz, netload-in, netuploaded-com, odsiebie-najlepsze-net, oron-com, platinshare-com, putshare-com, qshare-com, quickshare-cz, rapidshare-com, rapidshark-pl, rusfolder, sanupload-com, savefile-com, scribd-com, sendspace-com, share-online, share-rapid-cz, sharebigfile-com, shareflare-net, shragle-com, simpleupload-net, speedshare-org, storage-to, terafiles-net, tunabox-net, turbobit-net, turbobit-ru, turbouplоad-com, u-115-com, ugotfile-com, uloz-to, ultrashare, unibytes-com, unlimit-co-il, up-4share-vn, up-file-com, upload-com-ua, uploadbox-com, uploadc-com, uploaded, uploader-pl, uploadfloor-com, uploading-com, uploadingit-com, uploadking-com, uploadstation-com, upnito-sk, uptobox-com, usershare-net, videobb-com, wupload-com, x7-to, yourfilehost-com, yunfile, ziddu-com, zshare-net

Прикладные протоколы в группе:

нет

Группа social

Приложения в группе:

after school, azar, badoo, dubsmash, easy taxi, endomondo, facebook, flickr, foursquare, friendster, giphy, google plus, grindr, hi5, houseparty, imgur, instagram, itunesu, kono, life church, linkedin, mapmyrun, meetic group, moves, musical_ly, myfitnesspal, myspace, odnoklassniki, orkut, path, pinterest, prisma, reddit, renren, runkeeper, runtastic, sarahah, shazam, sina weibo, skout, smule, tinder, tumblr, twitter, vbulletin, vine, vk, waze, workout trainer, xing, yelp, yik yak

Прикладные протоколы в группе:

нет

Группа streaming

Приложения в группе:

1kxun, 9ku, age of warring empire, amazon prime music, amazon prime video, anghami, apple music, audiko, audiogalaxy, channel 4od, channel one, ciaomobile hdtv, cntv, ctitv, dailymotion, dazn, deezer, demand 5, digicel music, digicel playgo, disney storytime, espn, feidian, fetnet, fox sports, funshion, google play music, grooveshark, hamivideo, hinet, hulu, icecast, icflix, iflix, iheartradio, iplayer, iptv, itunes, itunes radio, itv, ivi-ru, kankan, kazaa/fasttrack, last-fm, letv, livejasmin, magine tv, maxdome, mycard, mymusic, myvideo tw, netflix, next tv, nickelodeon play, niconico, octoshape, pandora, periscope, pinkfong, pornhub, ppfilm, pplive, ppstream, qqlive, qvod, rdio, realma, redtube, rhapsody, rutube, shoutcast, simfy, sinatv, sky go, skyking, slacker, sling tv, slingbox, sopcast, soribada, soundcloud, speakaboos, spotify, spreecast, sptg tv, streetvoice, timely tv, ttpod, tunein radio, turner, tvbs, tvuplayer, twitch, ustream, uusee, vcast, veohtv, vevo, vimeo, watchever, wowza, xnxx, xvideos, youku tudou, youporn, youtube, zattoo

Прикладные протоколы в группе:

audiogalaxy, avi, feidian, flash, funshion, icecast, iplayer, kontiki, letv, mms, move, mpeg, octoshape, ogg, ppfilm, pplive, ppstream, qqlive, quicktime, qvod, realdatatransport, realmedia, rhapsody, rtcp, rtmp, rtp, rtsp, shoutcast, silverlight, sopcast, spotify, srtcp, srtp, tvants, tvuplayer, twitch, uusee, veohtv, windowsmedia, wowza, zattoo

Группа tunnel

Приложения в группе:

betternet, comodounite, cyberghost, epic browser proxy, hamachivpn, httptunnel, ipvanish, jap, pdproxy, private internet access, psiphon, softethernet, surfeasy, tiger vpn, tor, tunnelbear, ultrasurf, vpn-x, vyprvpn, yourfreedom tunnel, zenmate vpn, zero vpn

Прикладные протоколы в группе:

comodounite, cyberghost, gre, gtp, hamachivpn, ip in ip, ipsec, isakmp, jap, l2tp, netmotion, openvpn, pdproxy, ppp, pptp, psiphon, socks, softethernet, ssl, sstp, teredo, tor, ultrasurf, vpn-x, vtun, vyprvpn, yourfreedom tunnel, zero vpn

Группа voice over ip

Приложения в группе:

burner, chatcube, didi, facetime, ficall, forfone, fring, google duo, iskoot, line, magicjack, net2phone, scydo, skinny, skype, suda phone, tango, teamspeak, textplus, truphone, ventrilo, viber, vippie, voipswitch, voipswitch voip tunnel, vonage

Прикладные протоколы в группе:

chatcube, fring, h323, iax, line, mgcp, scydo, sip, skinny, skype, stun, tango, teamspeak, ventrilo, viber, voipswitch voip tunnel

Группа web

Приложения в группе:

2channel, adobe creative cloud, amazon cloud, amazon services, baidu, booking-com, cnn, duo duo, evernote, fubon e-broker, github, google app engine, google cloud, google shared services, here, hyread, kinopoisk, kollect book, loop caribbean local news, loop pacific local news, my digicel, mybook, naver, pubu bookbuffet, qip-ru, sohu, taaze, vudu, webqq, wikipedia, wuala, yandex

Прикладные протоколы в группе:

http, ocsp, webqq, websocket, wuala

Известные ограничения фильтрации по приложениям и прикладным протоколам

Для ряда приложений и прикладных протоколов, которые вы можете задать при создании транзитных фильтров открытой сети, существуют следующие особенности:

- **Фильтр с заданным приложением Apple Music обрабатывает только трафик онлайн-радио в приложении Apple Music (iTunes)**.

  Например, запрещающий сетевой фильтр с заданным приложением Apple Music будет блокировать только прослушивание онлайн-радио в приложении Apple Music (iTunes), но не будет блокировать прослушивание онлайн-музыки в этом же приложении.

- **Для разрешения полноценного взаимодействия со службой Apple Music необходимо задать в разрешающем сетевом фильтре приложения Apple Music, iTunes и iOS App**.

  Чтобы разрешить прохождение трафика, необходимого для взаимодействия со службой Apple Music, требуется в разрешающем сетевом фильтре помимо приложения Apple Music также задать приложение iTunes и, для возможности использования платных музыкальных сервисов, — приложение iOS App.

- **Фильтр с заданным приложением Megaupload-com не обрабатывает трафик веб-сайта mega.co.nz и приложения MEGA**.

  Для блокирования трафика веб-сайта mega.co.nz используйте сетевой фильтр с заданным приложением MEGA.

- **Запрещающий фильтр с заданным протоколом TOR может не блокировать доступ клиентов к сети Tor**.

  При блокировке своего основного протокола клиент Tor работает по протоколам POP и SSL. Поэтому для полноценной блокировки клиентов к сети Tor создайте запрещающие сетевые фильтры с заданным приложением TOR.

- **Разрешающий фильтр с заданным приложением Skype может некорректно обрабатывать трафик клиентов Skype**.

  Приложение Skype использует в своей работе другие приложения компании Microsoft: Microsoft services и Windows Azure. Чтобы ViPNet xFirewall корректно классифицировал трафик клиентов Skype, создайте разрешающий сетевой фильтр с заданными приложениями Skype, Microsoft Services и Windows Azure (см. Настройка фильтрации трафика для работы Skype на стр. 81). Если вы также хотите разрешить работу клиентов Skype for business, добавьте в фильтр приложение Skype for business. Для запрещающего фильтра достаточно указать только приложения Skype и Skype for business.

- **Для работы клиента Skype на ОС iOS необходимо задать в разрешающем сетевом фильтре приложения Skype, Microsoft Services и iMessage.**

  Чтобы разрешить прием трафика приложения Skype на узлах защищаемой сети, работающих под управлением iOS, необходимо в разрешающем фильтре помимо приложений Skype и Microsoft Services также задать приложение iMessage.

- **Для блокировки трафика приложения Facebook необходимо в запрещающем фильтре задавать приложение Facebook, а не одноименный протокол.**

  Так как при запрете трафика, передаваемого по протоколу Facebook, приложение Facebook продолжит передавать данные, используя протокол SSL, для блокировки трафика Facebook необходимо задать в разрешающем фильтре приложение Facebook, а не одноименный протокол.

- **Запрещающий фильтр с заданным протоколом BitTorrent может не блокировать трафик Torrent-клиентов**.

  Чтобы заблокировать трафик Torrent-клиентов, создайте запрещающие сетевые фильтры с заданными протоколами BitTorrent и Teredo (см. Настройка фильтрации трафика Torrent-клиентов на стр. 82).

- **Запрещающий фильтр по приложению Mediafire-com не блокирует доступ к https://www.mediafire.com.**

  В текущей версии DPI для приложения mediafire-com реализована фильтрация только по протоколу HTTP. Фильтрация по протоколу HTTPS не поддерживается.

- **Фильтрацию трафика по приложениям Google Plus и Google Play Music рекомендуется использовать только совместно с фильтрацией по приложениям Google Shared Services и Google APIs.**

  Приложения Google Plus и Google Play Music в работе использует сервисы Google общего назначения. Поэтому, если требуется блокировать или пропустить трафик Google Plus или Google Play Music, рекомендуется в соответствующем сетевом фильтре задать помимо целевого приложения Google ещё приложения Google Shared Services и Google APIs.

- **Фильтрацию трафика по приложению Google Maps рекомендуется использовать только совместно с фильтрацией по приложениям Google Shared Services, Google APIs и Google Cloud.**

  Приложение Google Maps в работе использует сервисы Google общего назначения. Поэтому, если требуется блокировать или пропустить трафик Google Maps, рекомендуется в соответствующем сетевом фильтре задать не только приложение Google Maps, но и приложения Google Shared Services, Google APIs и Google Cloud.

- **Чтобы разрешить узлам защищаемой сети соединения по протоколу IPsec, необходимо задать в разрешающем сетевом фильтре протоколы IPsec и ISAKMP.**

  Так как при организации соединений IPsec используется протокол ISAKMP, для разрешения приема и передачи трафика по протоколу IPsec на узле защищаемой сети необходимо в разрешающем сетевом фильтре задать не только протокол IPsec, но и протокол ISAKMP.

- **Запрещающий фильтр для одного из приложений Google не может быть применен к сетевому соединению в том случае, если данное сетевое соединение ранее было открыто для приложения Google, для которого отсутствует запрещающий фильтр**.

  Например, запрещающий фильтр для приложения Google Cloud не будет работать, если пользователь сначала авторизовался на сайте mail.google.com.

  Это происходит из-за особенностей работы протокола HTTP (HTTPS), когда браузер может посылать различные запросы к серверу по уже установленному соединению (или соединениям), не открывая для этого новое соединение. Так как доступ к различным приложениям Google может предоставляться через один сервер, то браузер может использовать одно и то же соединение для доступа к разным приложениям Google. При этом ViPNet xFirewall определяет тип приложения для каждого соединения, и в дальнейшем невозможно изменить тип приложения для уже установленного соединения.

- **Фильтрацию трафика по приложению Flickr необходимо использовать только совместно с фильтрацией по приложению Yahoo.**

  В связи с тем, что веб-сайт `flickr.com` использует сертификаты Yahoo, для фильтрации его трафика необходимо создать сетевые фильтры с заданными приложениями Flickr и Yahoo.

- **Ограничения фильтрации трафика для приложений и прикладных протоколов, для которых передаче данных предшествует отправка служебных пакетов через протоколы нижестоящих уровней.**

  Определение приложения или прикладного протокола происходит на прикладном уровне передачи данных, однако для некоторых приложений или прикладных протоколов передаче прикладных данных предшествует обязательная отправка служебных пакетов протоколов нижестоящих уровней. В связи с этим, в процессе классификации таких приложений или протоколов может быть пропущено несколько первых IP-пакетов, пока трафик не будет однозначно классифицирован как относящийся к этому приложению или протоколу.

  Например, вы создали разрешающий сетевой фильтр для протокола Skype и запрещающий сетевой фильтр для протокола Telegram. Чтобы верно классифицировать трафик как относящийся к приложению Skype, требуется до 11 пропущенных IP-пакетов. При этом первые несколько IP-пакетов, относящихся к приложению Telegram, также могут быть пропущены разрешающим фильтром для приложения Skype, так как их будет недостаточно для верной

классификации трафика. В этом случае короткие сообщения приложения Telegram будут пропущены сетевым фильтром Skype, так как для ViPNet xFirewall будет недостаточно данных для их классификации.

Глоссарий

Active Directory (AD)

Служба каталогов, разработанная Microsoft для доменных сетей Windows. Эта служба интегрирована в большинство операционных систем Windows Server.

Active Directory является центром администрирования и обеспечения безопасности сети. Она служит для аутентификации и авторизации всех пользователей и компьютеров внутри сети доменного типа Windows. При помощи Active Directory задаются и применяются политики безопасности для всех компьютеров в сети, а также устанавливается или обновляется программное обеспечение на компьютерах сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

Base64

Кодировка текстовых файлов, применяемая в криптографии. Сертификаты и списки CRL, хранящиеся в файлах с данной кодировкой, поддерживаются криптопровайдером ViPNet CSP Linux.

Captive portal

Портал авторизации, предоставляющий пользователям внутренней сети доступ в Интернет. Чаще всего Captive portal используется в местах общего доступа в Интернет, например, оборудованных точками доступа Wi-Fi.

DHCP relay

Функция ретрансляции запросов и ответов от (к) внешнего DHCP-сервера (см. глоссарий, стр. 201) в локальную сеть.

DHCP-сервер

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

DNS-сервер

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

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

DPI (Deep Packet Inspection)

Технология расширенной инспекции содержимого трафика сетевых приложений на уровнях 2 — 7 модели OSI и накопления статистики.

На основании анализа полученных данных выполняется фильтрация трафика.

ICAP

ICAP (Internet Content Adaptation Protocol) — протокол для расширения функциональности прокси-серверов. Чаще всего ICAP используется для внедрения функций антивирусной проверки и контентной фильтрации трафика, проходящего через прокси-сервер.

ICAP-сервер

Сервер, выполняющий обработку трафика по протоколу ICAP (см. глоссарий, стр. 201).

LDAP (Lightweight Directory Access Protocol)

Упрощённая версия протокола доступа к каталогу стандарта X.500. LDAP является основным протоколом, используемым для доступа к Active Directory и ADAM.

LDAP-сервер

Сервер службы каталогов, обеспечивающий доступ к каталогам пользователей сети по протоколу LDAP (см. глоссарий, стр. 201).

MIME-тип

Тип данных, которые могут быть переданы с помощью Интернета с применением стандарта MIME.

MTU (Maximum Transmission Unit)

Максимальный размер полезного блока данных пакета, который может быть передан через сетевой интерфейс без фрагментации.

NTP-сервер

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

OSPF (Open Shortest Path First)

Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала для нахождения кратчайшего маршрута. Распространяет информацию о доступных маршрутах внутри автономной системы.

PKCS#12

Формат файлов, предназначенных для передачи зашифрованных на пароле закрытых ключей и сертификатов (файлы с расширениями `.pfx`, `.p12`). Файлы формата PKCS#12 формируются в соответствии с рекомендациями Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации».

ViPNet Policy Manager

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

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу узлов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет узлам группироваться вместе, даже если они не находятся в одной физической сети.

Автономная система

Один или несколько сегментов сети, в которых осуществляется маршрутизация по одному протоколу (OSPF, IGRP, EIGRP, IS-IS, RIP, BGP, Static). Также может трактоваться как домен маршрутизации — группа маршрутизаторов сети, работающих по одинаковым протоколам маршрутизации.

Агрегированный сетевой интерфейс

Логический сетевой интерфейс (см. глоссарий, стр. 205), образованный из нескольких физических интерфейсов Ethernet, объединенных на канальном уровне сетевой модели OSI.

Административная дистанция

Характеристика маршрута (см. глоссарий, стр. 204). Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

Вес

Параметр, который задается для шлюза в статическом маршруте (см. глоссарий, стр. 204) в виде целого числа в диапазоне от 1 до 255. Позволяет настроить балансировку IP-трафика между шлюзами в одинаковый адрес назначения. Определяет долю IP-трафика, который должен передаваться по маршруту на указанный шлюз.

Домен коллизий

Часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети.

Сеть Ethernet, построенная на повторителях, всегда образует один домен коллизий. Мосты, коммутаторы и маршрутизаторы делят сеть Ethernet на несколько доменов коллизий.

Защищенный узел

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

Класс сетевого интерфейса

Признак, определяющий назначение сетевого интерфейса. В ViPNet xFirewall интерфейсам можно назначить следующие классы: `access`, `trunk`, `slave`.

По умолчанию сетевому интерфейсу назначен класс `access`. Если требуется, чтобы интерфейс Ethernet или агрегированный интерфейс обрабатывал трафик из нескольких VLAN, ему необходимо назначить класс `trunk`. Чтобы объединить несколько интерфейсов Ethernet в агрегированный интерфейс, каждому из таких интерфейсов необходимо предварительно назначить класс `slave`.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных серверов ViPNet xFirewall, один из которых (активный) выполняет функции маршрутизатора, а другой сервер (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ViPNet xFirewall на активном сервере, пассивный сервер переключается в активный режим для выполнения функций сбойного сервера. При этом сбойный сервер перезагружается и становится пассивным.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от ViPNet xFirewall клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Маршрут

Путь следования IP-трафика при передаче в сети от одного узла другому.

Маршрут по умолчанию

Путь следования IP-пакетов, для которых не был найден подходящий маршрут в таблице маршрутизации.

Маршрутизатор-сосед

OSPF-маршрутизатор, находящиеся в одной области маршрутизации с другими маршрутизаторами этого типа.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Метрика маршрута

Предназначена для задания приоритета маршрута передачи IP-трафика.

Область маршрутизации

Одна или несколько IP-сетей, в которых осуществляется обмен информацией по определенному протоколу, в частности, по протоколу OSPF (см. глоссарий, стр. 202).

Протокол OSPF рассматривает межсетевую среду как множество областей, соединенных друг с другом через некоторую базовую область (backbone area). Для идентификации областей каждой из них выделяется специальный идентификатор (area ID), представляющий собой целое число в десятичном формате.

Открытый трафик

Поток незашифрованных IP-пакетов.

Перераспределение маршрутов

Обмен маршрутной информацией между двумя различными маршрутизирующими протоколами.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

Прозрачный режим работы прокси-сервера

Режим работы, при котором не требуется выполнять настройку программного обеспечения на рабочих местах пользователей, подключающихся к Интернету через прокси-сервер.

Прокси-сервер

Программа, транслирующая соединения по некоторым протоколам из внутренней сети во внешнюю и выступающая при этом как посредник между клиентами и сервером.

Публичный адрес

IP-адрес, который может применяться в Интернете.

Сертификат ключа проверки электронной подписи

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

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN (см. глоссарий, стр. 202).

Сетевой фильтр

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

Сеть ViPNet

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

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

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Стоимость маршрута

Количество издержек, которые возникнут при отправке IP-пакета в сеть назначения через тот или иной шлюз. Стоимость маршрута обратно пропорциональна его пропускной способности канала связи.

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных в сети.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Частный адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к Интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в Интернете. Чтобы выйти в Интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

Шлюз

Устройство, предназначенное для соединения двух сетей с разными канальными протоколами. Перед передачей данных из одной сети в другую шлюз их преобразует, обеспечивая совместимость протоколов.