ViPNet xFirewall

Настройка с помощью командного интерпретатора

infotecs

ФРКЕ.00217-01 90 15

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

О документе

В документе описаны основные сценарии настройки ViPNet xFirewall с помощью командного интерпретатора, а также работа с журналами ViPNet xFirewall.

Для кого предназначен документ

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

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.

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены только в режиме администратора, содержат приглашение с символом «#». Например:

  ```
  hostname# команда
  ```

- Команды, которые могут быть выполнены в режиме и пользователя, и администратора, содержат приглашение с символом «>». Например:

  ```
  hostname> команда
  ```

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки. Например:

  ```
  команда <параметр>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

  ```
  команда <обязательный параметр> [необязательный параметр]
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой. Например:

  ```
  команда {вариант-1 | вариант-2}
  ```

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 веб-интерфейса»	Описание основных сценариев настройки ViPNet xFirewall с помощью веб-интерфейса
«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. 271) 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

Работа с командным интерпретатором

Основные сведения по работе с командным интерпретатором

Все операции по администрированию ViPNet xFirewall вы можете выполнить с помощью командного интерпретатора ViPNet. Работа в командном интерпретаторе возможна при различных способах подключения к ViPNet xFirewall:

- Локальное подключение к ViPNet xFirewall с помощью консоли (на стр. 20).
- Удаленное подключение к ViPNet xFirewall с помощью протокола SSH (на стр. 22).

Командный интерпретатор независимо от способа подключения к ViPNet xFirewall запускается автоматически после успешной аутентификации пользователя (см. Аутентификация пользователя на ViPNet xFirewall на стр. 25). После запуска командный интерпретатор находится в режиме пользователя (обозначается символом «>» в приглашении интерпретатора). В режиме пользователя недоступны некоторые команды, требующие прав администратора.

Чтобы перейти в режим администратора, требуется пройти аутентификацию администратора (см. Аутентификация администратора на ViPNet xFirewall на стр. 26). В режиме администратора доступны все возможные настройки.

В случае одновременной работы нескольких командных интерпретаторов (независимо от типа подключения — локального или удаленного) только один из них может находиться в режиме администратора. При попытке перейти в некотором командном интерпретаторе в режим администратора проверяется режим работы остальных запущенных интерпретаторов. Если остальные интерпретаторы находятся в режиме пользователя, то данный интерпретатор переходит в режим администратора. Если один из интерпретаторов находится в режиме администратора, то выводится информация об узле, на котором он запущен, и предложение принудительно завершить работу этого интерпретатора. В случае согласия работа интерпретатора, находящегося в режиме администратора, завершается, после чего данный интерпретатор переходит в режим администратора.

Чтобы просмотреть информацию обо всех запущенных сессиях командного интерпретатора, выполните команду `who`.

Чтобы принудительно завершить любую сессию командного интерпретатора, выполните команду `admin kick`. Выполнить команду можно только в режиме администратора.

Чтобы вернуться в режим пользователя, выполните команду `exit`.

Чтобы выйти из командного интерпретатора, используйте сочетание клавиш **Ctrl+D** (в режиме пользователя или администратора) или выполните команду `exit` (в режиме пользователя). В случае выхода из командного интерпретатора в консоли снова появится приглашение для аутентификации пользователя.

Интерфейс командного интерпретатора

Командный интерпретатор ViPNet принимает от вас текстовые команды, состоящие из слов, разделенных пробелами. Для облегчения ввода команд в этом интерпретаторе предусмотрены следующие средства:

- сокращенный ввод команд (на стр. 17);
- автодополнение команд (на стр. 17);
- контекстная справка (на стр. 18);
- сочетания клавиш (на стр. 18).

Сокращенный ввод команд

Слова команды распознаются по минимальному числу символов, позволяющих отличить ее от других команд, ввод которых возможен в текущей ситуации.

Например:

- Если у двух команд первое слово начинается с символа «i» (`inet` и `iplir`), то для указания этих команд достаточно ввести первые две буквы соответствующего слова (`in` и `ip`).
- После слова `iplir` в качестве второго слова возможны только слова `stop` и `start`. Поэтому для указания соответствующих команд достаточно ввести `sto` и `sta`.

Таким образом, вместо полной команды `iplir start` достаточно ввести `ip sta`.

Если среди введенных символов есть ошибочные, то вся команда считается ошибочной, даже если она может быть однозначно определена по первым правильно введенным символам (то есть в приведенном выше примере команда `iplor sta` будет ошибочной).

Автодополнение команд

Если введенные символы однозначно определяют какую-либо команду или параметр команды, то вы можете выполнить автоматическое дополнение недостающих символов, нажав клавишу **Tab**:

```
hostname> en<Tab>
hostname> enable _
```

Автодополнение работает только для слова, на котором находится курсор. Автодополнение можно использовать при вводе любых команд и параметров, кроме параметров, значение которых задается пользователем произвольно (например, имена созданных пользователем объектов).

Контекстная справка

Контекстная справка позволяет вам просмотреть информацию о командах и параметрах, ввод которых возможен в текущей ситуации. Контекстная справка вызывается с помощью символа «?».

Чтобы просмотреть список всех доступных вам групп команд, в приглашении интерпретатора ViPNet введите символ «?»:

```
hostname> ?
inet                a group of commands intended for working with routing, interfaces and
network tools
failover            control command for Failover daemon
iplir               control command for IpLir daemon

webui               control WebUI service
mftp                commands for managing the MFTP daemon
enable       switch to the administrator mode
exit                exit the command line interface
version             view the versions of the appliance
who                 view currently running sessions of the command line interface
machine             a group of system commands
firewall            firewall's objects commands
hostname> _
```

Левая колонка списка содержит первое слово группы команд, правая — краткое описание ее назначения.

В случае ввода символа «?» в процессе набора команд интерпретатор ViPNet предложит вам варианты завершения текущего или следующего слова команды, в зависимости от положения курсора:

```
hostname> machi?
machine a group of system commands
hostname> machi_
hostname> machine ?
show                a group of commands for viewing system settings

reboot       reboot the software and hardware appliance
halt                turn off the software and hardware appliance
hostname> machine _
```

После информации о вариантах завершения команды отображается приглашение интерпретатора ViPNet с ранее введенной командой для редактирования. Редактировать команды можно как обычно: стирать символы клавишей **Backspace** или **Delete**, перемещаться по тексту с помощью клавиш со стрелками влево и вправо.

Сочетания клавиш

Командный интерпретатор поддерживает стандартные сочетания клавиш, перечисленные в таблице ниже.

Таблица 4. Поддерживаемые интерпретатором сочетания клавиш

Сочетание клавиш	Действие
Ctrl+U	стереть всю команду
Ctrl+K	стереть все от курсора до конца строки
Ctrl+A	перейти в начало строки
Ctrl+E	перейти в конец строки
Ctrl+B	перейти на один символ назад
Ctrl+F	перейти на один символ вперед
Ctrl+H	стереть символ перед курсором
Ctrl+W	стереть слово перед курсором

Локальное подключение к ViPNet xFirewall с помощью консоли

Чтобы локально подключиться к ViPNet xFirewall, выполните следующие действия:

1. Если это не было сделано ранее, выберите и настройте консоль для подключения к ViPNet xFirewall (см. Выбор консоли при локальном подключении к ViPNet xFirewall на стр. 20).
2. Выполните аутентификацию пользователя (см. Аутентификация пользователя на ViPNet xFirewall на стр. 25).
3. Если требуется выполнить настройку параметров ViPNet xFirewall, выполните аутентификацию администратора (см. Аутентификация администратора на ViPNet xFirewall на стр. 26).

Примечание. Если на ViPNet xFirewall истекают или уже истекли сроки действия персонального ключа пользователя или ключей защиты ключей обмена, то на экране появится соответствующее сообщение. Обратитесь к администратору ViPNet xFirewall для обновления ключей (см. Обновление ключей и лицензии при истечении срока их действия на стр. 41).

Выбор консоли при локальном подключении к ViPNet xFirewall

При локальном подключении к ViPNet xFirewall в качестве консоли вы можете использовать следующее оборудование:

- монитор и клавиатура (обычная консоль);
- любое устройство, подключенное к COM-порту ViPNet xFirewall (COM-консоль).

Примечание. На некоторых аппаратных платформах ViPNet xFirewall вместо COM-порта RS-232 присутствует служебный Ethernet-порт RJ45. Этот порт также может использоваться для подключения к ViPNet xFirewall через COM-консоль. Подробнее об аппаратных платформах см. документ «ViPNet xFirewall. Общее описание».

При подключении COM-консоли к ViPNet xFirewall (например, с помощью программы PuTTY) установите значения параметров COM-порта, приведенные в таблице ниже.

Таблица 5. Требования к параметрам COM-порта для подключения консоли

Параметр	Значение
Speed (скорость обмена данными)	38400

Параметр	Значение
Data (размер данных)	8
Parity (четность)	None
Stopbits (стоповые биты)	1
Тип терминала	VT100+

Примечание. В ViPNet xFirewall поддерживается только кодировка KOI8-R. Поэтому при подключении к компьютеру, на котором используется другая кодировка, возможны проблемы при вводе с клавиатуры и отображении на экране символов нелатинского алфавита.

К ViPNet xFirewall локально можно подключиться с помощью нескольких консолей. Одновременная работа во всех запущенных консолях возможна только в режиме пользователя. В режиме администратора при этом можно работать только в одной консоли. Поскольку возможна одновременная работа сразу в нескольких консолях при каждом включении ViPNet xFirewall, независимо от количества подключенных консолей, предлагается выбрать консоль для дальнейшей работы следующим образом:

1. На все консоли, подключенные к ViPNet xFirewall, выводится приглашение нажать любую клавишу. Если в течение 10 секунд вы не нажмете клавишу ни на одной из консолей, то считается, что клавиша нажата на обычной консоли.
2. На консоль, на которой нажата клавиша, выводится список возможных консолей и приглашение выбрать нужную. Если в течение 5 секунд вы не выберите консоль, то автоматически выбирается обычная консоль.

Все последующие сообщения о загрузке ОС и приглашение для входа в систему будут выводиться на выбранной консоли.

Удаленное подключение к ViPNet xFirewall с помощью протокола SSH

Удаленное подключение к командному интерпретатору следует осуществлять только с выделенных рабочих мест по каналу, защищенному средствами ViPNet. Вы можете подключаться к ViPNet xFirewall с других узлов сети ViPNet, связанных с ним (связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 272)).

Внимание! Предоставлять удаленный доступ к ViPNet xFirewall с узлов за пределами сети ViPNet запрещено.

Для удаленного подключения вы можете использовать любой SSH-клиент с парольным типом аутентификации.

Примечание. В ViPNet xFirewall поддерживается только кодировка KOI8-R. Поэтому при подключении к компьютеру, на котором используется другая кодировка, возможны проблемы при вводе с клавиатуры и отображении на экране символов нелатинского алфавита.

Чтобы удаленно подключиться к ViPNet xFirewall, выполните следующие действия:

1. С помощью SSH-клиента подключитесь к ViPNet xFirewall, указав необходимые параметры подключения и пароль.
2. Если в момент вашего подключения к ViPNet xFirewall установлены удаленные сессии других пользователей и количество удаленных сессий максимальное, появится сообщение с предложением подключиться к ViPNet xFirewall в режиме администратора. В случае согласия на такое подключение выполните аутентификацию администратора (см. Аутентификация администратора на ViPNet xFirewall на стр. 26).

   Если запущена другая удаленная сессия в режиме администратора, то прервите ее. В противном случае ваша попытка удаленного подключения будет завершена.

   Если в течение 30 секунд вы не подтвердите подключение к ViPNet xFirewall в режиме администратора, то ваша удаленная сессия будет завершена.

Примечание. Если во время удаленной сессии с ViPNet xFirewall вы не будете выполнять никакие действия в течение 30 минут, то сессия будет прервана. Подробнее см. Мониторинг неактивных удаленных сессий (на стр. 23).

Если на ViPNet xFirewall истекают или уже истекли сроки действия персонального ключа пользователя или ключей защиты ключей обмена, то на консоли появится

соответствующее сообщение. Обратитесь к администратору ViPNet xFirewall для обновления ключей (см. Обновление ключей и лицензии при истечении срока их действия на стр. 41).

Ограничение количества удаленных сессий

На ViPNet xFirewall установлено ограничение на количество одновременно запущенных удаленных сессий пользователей. В зависимости от исполнения ViPNet xFirewall разрешено:

- 5 удаленных сессий одновременно, если используется ViPNet xFirewall в исполнении xF100.
- 30 удаленных сессий одновременно, если используется ViPNet xFirewall остальных исполнений.

Установленное ограничение изменить нельзя, так как увеличение одновременных удаленных подключений может отрицательно сказаться на выполнении основных функций ViPNet xFirewall.

При удаленном подключении пользователя к ViPNet xFirewall проверяется количество открытых удаленных сессий пользователей. Если количество сессий максимальное, то пользователю выдается сообщение об этом с предложением подключиться в режиме администратора. Если в течение 30 секунд от пользователя не будет получен ответ, подключение будет завершено. В случае ввода пользователем корректного пароля администратора будет открыта сессия. Возможна только одна удаленная сессия в режиме администратора. Поэтому если на момент запуска вашей сессии в режиме администратора запущена другая сессия, то ее потребуется прервать. После завершения работы администратора при выполнении команды `exit` сессия завершается без возможности перейти в режим пользователя.

Мониторинг неактивных удаленных сессий

При одновременном удаленном подключении по протоколу SSH большого количества пользователей нагрузка на ViPNet xFirewall значительно увеличивается, что может привести к сбою в работе. Во избежание такой ситуации производится мониторинг активности пользователей в удаленных сессиях.

Проверка активности пользователя в каждой удаленной сессии осуществляется один раз в 5 минут. Если пользователь не выполняет никаких действий в течение 30 минут, его сессия принудительно завершается.

Для просмотра текущего допустимого времени неактивности сессии пользователя выполните команду:

```
hostname> machine show session-timeout
```

Для установки максимально допустимого времени неактивности сессии пользователя в удаленной сессии выполните команду:

```
hostname# machine set session-timeout <время>
```

При работе ViPNet xFirewall в режиме кластера горячего резервирования указанные настройки резервируются.

Аутентификация пользователя на ViPNet xFirewall

Для аутентификации в ViPNet xFirewall требуется ввести имя учетной записи и пароль пользователя. Каждый раз при вводе пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу.

Чтобы выполнить аутентификацию пользователя, выполните следующие действия:

1. Введите имя учетной записи пользователя `user`.
2. Введите пароль пользователя. Пароль будет совпадать с паролем дистрибутива лицензии, если он не изменялся в процессе работы с ViPNet xFirewall (см. Изменение пароля пользователя на стр. 38). При вводе пароля на экране ничего не отображается. Если введен неверный пароль, на консоли появляется соответствующее сообщение и приглашение для повторной аутентификации.

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.

В случае успешной аутентификации интерпретатор будет запущен в режиме пользователя. Вы можете приступать к работе с ViPNet xFirewall. О том, как перейти в режим администратора, см. раздел Аутентификация администратора на ViPNet xFirewall (на стр. 26).

Аутентификация администратора на ViPNet xFirewall

Чтобы перейти в режим администратора, выполните следующие действия:

1 Выполните команду `enable`.

2 Введите пароль администратора сетевого узла ViPNet. При вводе пароля на экране ничего не отображается. Если введен неверный пароль, на консоли появляется соответствующее сообщение и приглашение для повторной аутентификации.

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.

В случае ввода верного пароля интерпретатор перейдет в режим администратора — на консоли появится символ «#» в приглашении интерпретатора. В этом режиме вы можете выполнить те настройки, которые были недоступны в режиме пользователя.

2

Настройка системных параметров

Настройка даты и времени

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

Внимание! Если системные дата и время заданы неверно, соединения с узлами сети ViPNet могут блокироваться.

Рекомендуется настроить синхронизацию системного времени по протоколу NTP.

Если требуется настроить системные дату и время вручную, выполните следующие действия:

1 Для просмотра текущего времени выполните команду:

```
hostname> machine show date
```

2 Если требуется изменить часовой пояс, выполните команду:

```
hostname# machine set timezone {<Континент/Пояс> | <UTC>}
```

Примечание. Название континента и часового пояса должны начинаться с прописной буквы. Например, чтобы установить часовой пояс города Москвы, выполните команду:

```
hostname# machine set timezone Europe/Moscow
```

Чтобы посмотреть список всех существующих часовых поясов, введите данную команду без параметра.

3 Если требуется изменить системное время, выполните следующие действия:

3.1 Остановите демоны iplircfg, failoverd и mftpd с помощью команд:

```
hostname# iplir stop
hostname# failover stop
hostname# mftp stop
```

3.2 Настройте дату и время с помощью команды:

```
hostname# machine set date <YYYY-MM-DD> <hh:mm:ss>,
```

где `YYYY` — год, `MM` — месяц, `DD` — день, `hh` — часы, `mm` — минуты, `ss` — секунды.

3.3 Запустите демоны iplircfg, failoverd и mftpd с помощью команд:

```
hostname# iplir start
hostname# failover start
hostname# mftp start
```

Настройка параметров использования файла подкачки

Чтобы увеличить производительность ViPNet xFirewall за счет оптимизации скорости его процессов, рекомендуется настроить использование на нем файла подкачки.

Чтобы настроить параметры файла подкачки, выполните следующие действия:

1 Задайте размер файла подкачки с помощью команды:

```
hostname# machine swap set <size>,
```

указав с помощью параметра `<size>` нужный размер файла подкачки в мегабайтах.

Если будет задан размер файла подкачки, превышающий размер доступного пространства на диске, появится соответствующее сообщение.

Внимание! После создания файла подкачки на диске должно остаться не менее 256 Мбайт свободного пространства.

---

2 Включите использование файла подкачки с помощью команды:

```
hostname# machine swap mode on
```

3 Чтобы отключить использование файла подкачки, выполните команду:

```
hostname# machine swap mode off
```

После выполнения данной команды размер файла подкачки будет установлен в значение «0».

4 Чтобы просмотреть сведения об использовании оперативной памяти и файле подкачки, выполните команду:

```
hostname# machine show memory
```

Управление копиями конфигурации

Виды копий конфигурации

В ViPNet xFirewall существует возможность создания копий конфигурации, которые позволяют при необходимости осуществлять возврат программного обеспечения к другому состоянию (например, к состоянию до выполнения настроек или до приема обновленных справочников).

Копия конфигурации — это совокупность настроек ViPNet xFirewall. Существуют два вида копий конфигурации:

- частичная — включает в себя следующие конфигурационные файлы ПО ViPNet xFirewall: `iplir.conf` и все файлы с именем, соответствующим маске `iplir.conf-<интерфейс или группа интерфейсов>`, `failover.ini`, `mftp.conf`;
- полная — включает в себя все файлы частичной копии конфигурации, включая справочники.

Копии конфигурации могут создаваться следующими способами:

- Автоматически (перед обновлением ПО или справочников). В этом случае по умолчанию создаются частичные копии конфигурации. Вы можете изменить вид копии конфигурации, создаваемой автоматически, или выключить автоматическое создание копий конфигурации, отредактировав значение параметра `confsave` в секции `[upgrade]` в файле `mftp.conf`.

  Кроме того, с помощью параметра `maxautosaves` этой же секции вы можете задать максимальное число автоматически созданных копий конфигурации, которое может храниться на ViPNet xFirewall. По умолчанию может храниться не более 10 автоматически созданных копий конфигурации.

  Описание параметров секции `[upgrade]` см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», в разделе «Секция [upgrade]».

- Вручную по команде. В этом случае всегда создаются только полные копии конфигурации.

Для выполнения операций с копиями конфигураций в ПО ViPNet xFirewall используется vpn-компонент ViPNet. Номер версии vpn-компонента `<версия vpn>` указывается в качестве параметра команд работы с копиями конфигураций и выводится в сообщениях о результатах выполнения команд.

Внимание! Номер версии vpn-компонента может не совпадать с номером версии ViPNet xFirewall. Чтобы посмотреть номер версии vpn-компонента, выполните команду `version full`.

Создание копии конфигурации

Внимание! По умолчанию перед обновлением ПО или справочников автоматически создается частичная копия конфигурации. Вы можете изменить эту настройку в секции `[upgrade]` файла `mftp.conf` (подробнее см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам»).

Чтобы вручную создать копию текущей конфигурации, выполните следующие действия:

1 Завершите работу демонов iplircfg, failoverd и mftpd с помощью команд:

```
hostname# iplir stop
hostname# failover stop
hostname# mftp stop
```

2 Выполните команду:

```
hostname# admin config save <имя>,
```

указав имя копии конфигурации, используя только буквы латинского алфавита, цифры, символы «–» и «_». Если имя копии конфигурации состоит из нескольких слов, заключите его в кавычки (например: `"settings copy_1"`).

3 Если копия конфигурации с выбранным именем уже существует, будет предложено ее перезаписать:

```
Config '<имя копии конфигурации>' (version <версия vpn>) exists. Overwrite?
```

Выполните одно из действий:

- Чтобы подтвердить перезапись, введите символ `y` и нажмите клавишу **Enter**.
- Чтобы создать конфигурацию с другим именем, введите символ `n` и нажмите клавишу **Enter**.

4 Запустите демоны iplircfg, failoverd и mftpd с помощью команд:

```
hostname# iplir start
hostname# failover start
hostname# mftp start
```

Созданную копию конфигурации вы можете использовать для восстановления настроек ViPNet xFirewall.

При необходимости вы также можете просмотреть список всех созданных копий конфигурации.

Просмотр списка копий конфигурации

Чтобы просмотреть список ранее созданных копий конфигурации, выполните команду:

```
hostname# admin config list
"settings copy_1",       version 4.3.0,  full, saved on 07.05.2018 at 17:13, never loaded
```

В результате отобразится список, каждая строка которого содержит следующую информацию:

- имя копии конфигурации;
- версия vpn-компонента ViPNet, в которой была создана копия конфигурации (после слова `version`);
- вид копии конфигурации — полная (`full`) или частичная (`part`);
- дата и время создания копии конфигурации (после слова `saved`).

Если копия конфигурации была создана автоматически, то ее имя начинается со слова `autosave` и содержит дату создания. Например: `autosave-2018-08-05`.

Если копия конфигурации уже использовалась для восстановления настроек ViPNet xFirewall, дата и время использования отображаются после даты и времени создания копии конфигурации (после слова `loaded`). Если копия конфигурации ни разу не использовалась, после даты и времени создания будет указано `never loaded`.

Восстановление настроек из копии конфигурации

Чтобы восстановить настройки ViPNet xFirewall из копии конфигурации, выполните следующие действия:

1 Завершите работу всех демонов и драйверов ViPNet xFirewall с помощью команды:

```
hostname# vpn stop
```

2 Выполните команду:

```
hostname# admin config load <имя> [<версия vpn>],
```

указав:

- имя копии конфигурации;
- версию VPN-компонента ViPNet, в которой была создана копия конфигурации.

Если имя копии конфигурации состоит из нескольких слов, заключите его в кавычки.

3 Если текущая версия VPN-компонента выше версии, в которой была создана выбранная для восстановления настроек копия конфигурации, подтвердите возврат к более ранней версии.

4 Будет предложено сохранить все текущие настройки ViPNet xFirewall:

```
Save current configuration [Y/n]?
```

Выполните одно из действий:

- Чтобы сохранить все текущие настройки, введите символ `Y` и нажмите клавишу **Enter**. Затем укажите имя соответствующей полной копии конфигурации.
- Чтобы не сохранять текущие настройки ViPNet xFirewall, введите символ `n` и нажмите клавишу **Enter**. Для подтверждения действия введите фразу `Yes, do as I say`.

5 Дождитесь завершения процесса восстановления настроек ViPNet xFirewall.

6 Запустите демоны и драйверы ViPNet xFirewall с помощью команды:

```
hostname# vpn start
```

Теперь вы можете продолжить работу с ViPNet xFirewall.

Удаление копии конфигурации

Чтобы удалить ненужные копии конфигурации, выполните команду:

```
hostname# admin config delete <имя> [<версия vpn>],
```

указав:

- имя копии конфигурации;
- версию VPN-компонента ViPNet, в которой была создана копия конфигурации.

Чтобы не писать имя копии конфигурации полностью или удалить сразу несколько копий конфигурации, имена которых содержат определенные символы, вместо имени укажите маску имени, используя символ «*».

Примечание. Если имя копии конфигурации состоит из нескольких слов либо если для указания имени используется маска, заключите его в кавычки.

Например, чтобы удалить все копии конфигурации, созданные автоматически в мае 2018 года, выполните команду:

```
hostname# admin config delete "rollback-2018-05-*"
```

Если несколько копий конфигурации имеют имя, соответствующие указанной маске, то будет отображено количество таких копий конфигурации:

```
<количество копий конфигурации> configs match that pattern. Delete? (y/n)
```

Выполните одно из действий:

- Чтобы подтвердить удаление всех копий конфигурации, введите символ `y` и нажмите клавишу **Enter**.
- Чтобы отменить удаление всех копий конфигурации, введите символ `n` и нажмите клавишу **Enter**.

Чтобы удалить копии конфигурации, созданные в определенной версии VPN-компонента ViPNet, укажите номер этой версии. Например:

```
hostname# admin config delete "rollback-2018-05-*" 4.3.0
```

Контроль целостности файлов ViPNet xFirewall

Во избежание возникновения сбоев ПО целостность критически важных файлов ViPNet xFirewall регулярно проверяется с помощью встроенных скриптов. Контролируются следующие компоненты:

- ядро Linux и образы модулей ViPNet xFirewall, используемые при загрузке ПО;
- системные демоны и библиотеки;
- конфигурационные файлы демонов ViPNet xFirewall;
- справочники ViPNet.

Указанные файлы защищены контрольными суммами, которые хранятся в файлах с расширением `*.crg`. Проверка целостности выполняется путем вычисления текущей контрольной суммы файла и ее сравнения с контрольной суммой из файла `*.crg`.

Каждый файл `*.crg` содержит также собственную контрольную сумму. Проверка контрольной суммы файла `*.crg` выполняется перед проверкой целостности остальных файлов, контрольная сумма которых в нем указана.

Проверка целостности файлов автоматически выполняется в следующих случаях:

- Установка ПО ViPNet xFirewall.
- Обновление ПО ViPNet xFirewall.
- Загрузка ПО ViPNet xFirewall.

Кроме того, вы можете проверить целостность конфигурационных файлов вручную с помощью команды:

```
hostname# machine self-test
```

Примечание. Команду проверки целостности конфигурационных файлов нельзя использовать при удаленном администрировании с помощью SSH (подробнее см. в документе «ViPNet xFirewall. Общее описание»).

Нарушением целостности файлов также считается отсутствие хотя бы одного файла конфигурации или файла с контрольными суммами.

При несовпадении контрольных сумм в ходе периодической проверки ViPNet xFirewall автоматически перезагружается.

При несовпадении контрольных сумм в ходе проверки во время установки, обновления или загрузки ПО, а также в ходе проверки, выполняемой вручную, выводится сообщение о нарушении целостности файла. Затем выполняется одно из следующих действий:

- Если для искаженного файла имеется резервная копия, файл будет автоматически восстановлен. При этом будет выведено соответствующее сообщение. При восстановлении ViPNet xFirewall может быть перезагружен.
- Если резервная копия искаженного конфигурационного файла не найдена, будет выведено соответствующее сообщение. После этого демоны, отвечающие за работу в сети ViPNet, не будут запущены либо будут остановлены и сетевые интерфейсы будут выключены.

Совет. Если у вас есть файл экспорта справочников и настроек с расширением `*.vbe`, попробуйте восстановить систему, импортировав этот файл (подробнее см. в документе «ViPNet xFirewall. Подготовка к работе», в главе «Резервное копирование и восстановление настроек»). Если восстановить работу ViPNet xFirewall не удалось, обратитесь в службу поддержки ОАО «ИнфоТеКС».

- Если при загрузке обнаружено нарушение целостности ядра Linux или одного из образов модулей ViPNet xFirewall, и соответствующая резервная копия не найдена, то будет выведено соответствующее сообщение и загрузка ViPNet xFirewall завершится. Для выключения ViPNet xFirewall нажмите любую клавишу.

Использование резервного раздела в ViPNet xFirewall

Чтобы обеспечить возможность оперативного восстановления критически важных компонентов ViPNet xFirewall, целостность которых регулярно проверяется, такие файлы периодически копируются на специальный резервный раздел накопителя ViPNet xFirewall.

Копии файлов сохраняются в резервный раздел `/mnt/reserv` того накопителя ViPNet xFirewall, с которого не происходит загрузка ПО. При проверке целостности критически важных файлов искаженные файлы автоматически восстанавливаются из своих резервных копий.

Копирование файлов в резервный раздел выполняется в следующих случаях:

- Успешная проверка целостности файлов при первоначальной установке и обновлении ПО либо при выполнении команды `machine self-test`.
- Успешная проверка целостности при загрузке ViPNet xFirewall.
- Обновление справочников.
- Изменение пароля пользователя.

Примечание. В первом случае копируются все конфигурационные файлы, а в остальных — только часть файлов.

Если два ViPNet xFirewall работают в режиме кластера горячего резервирования, то резервные копии файлов регулярно копируются с активного сервера на пассивный. При изменении справочников на кластере, копии справочников и ключей обновляются как на активном, так и на пассивном сервере.

3

Настройка параметров безопасности

Изменение пароля пользователя

Пароль пользователя ViPNet xFirewall назначается администратором сети ViPNet. После первичной установки справочников и ключей рекомендуется его изменить. Это дополнительно повысит безопасность, поскольку пароль не будет известен администратору сети ViPNet.

Примечание. Пароль пользователя ViPNet xFirewall можно изменить только локально, как описано ниже. Смена пароля пользователя удаленно (с помощью программы ViPNet Центр управления сетью (ЦУС)) невозможна.

Чтобы изменить пароль пользователя, выполните следующие действия:

1 Выполните команду:

```
hostname# admin passwd
```

2 Введите текущий пароль пользователя или пароль администратора сетевого узла.

Примечание. При вводе паролей на экране ничего не отображается, введенные символы отредактировать нельзя.

3 Введите новый пароль пользователя и подтвердите его. Появится сообщение об успешном изменении пароля пользователя.

В результате с помощью нового пароля будут перешифрованы ключи пользователя, в том числе резервный набор персональных ключей при наличии.

Совет. Мы рекомендуем запомнить пароль, назначенный администратором сети ViPNet. Он может потребоваться вам при установке нового дистрибутива лицензии (см. глоссарий, стр. 274) или РНПК, поскольку они будут защищены этим паролем и без него не смогут быть установлены на ViPNet xFirewall. Если вы забудете пароль, запросите его у администратора сети ViPNet вместе с дистрибутивом или РНПК.

Просмотр информации об установленной лицензии

При необходимости вы можете просмотреть информацию о следующих ключах, установленных на ViPNet xFirewall:

- персональный ключ пользователя;
- набор персональных ключей (РНПК);
- ключи узла.

Получение сведений об установленных ключах может требоваться вам перед добавлением РНПК на ViPNet xFirewall, чтобы убедиться, что РНПК отсутствует на узле. Остальная информация может быть востребована сотрудниками технического сопровождения при возникновении проблем с ключевой системой ViPNet xFirewall (например, после некорректного обновления справочников и ключей на узле или в других случаях).

Для просмотра информации о ключах выполните команду:

```
hostname# iplir show key-info
```

В результате выполнения команды отобразятся списки с информацией по типам ключей. Пример выводимой информации о ключах представлен на рисунке ниже.

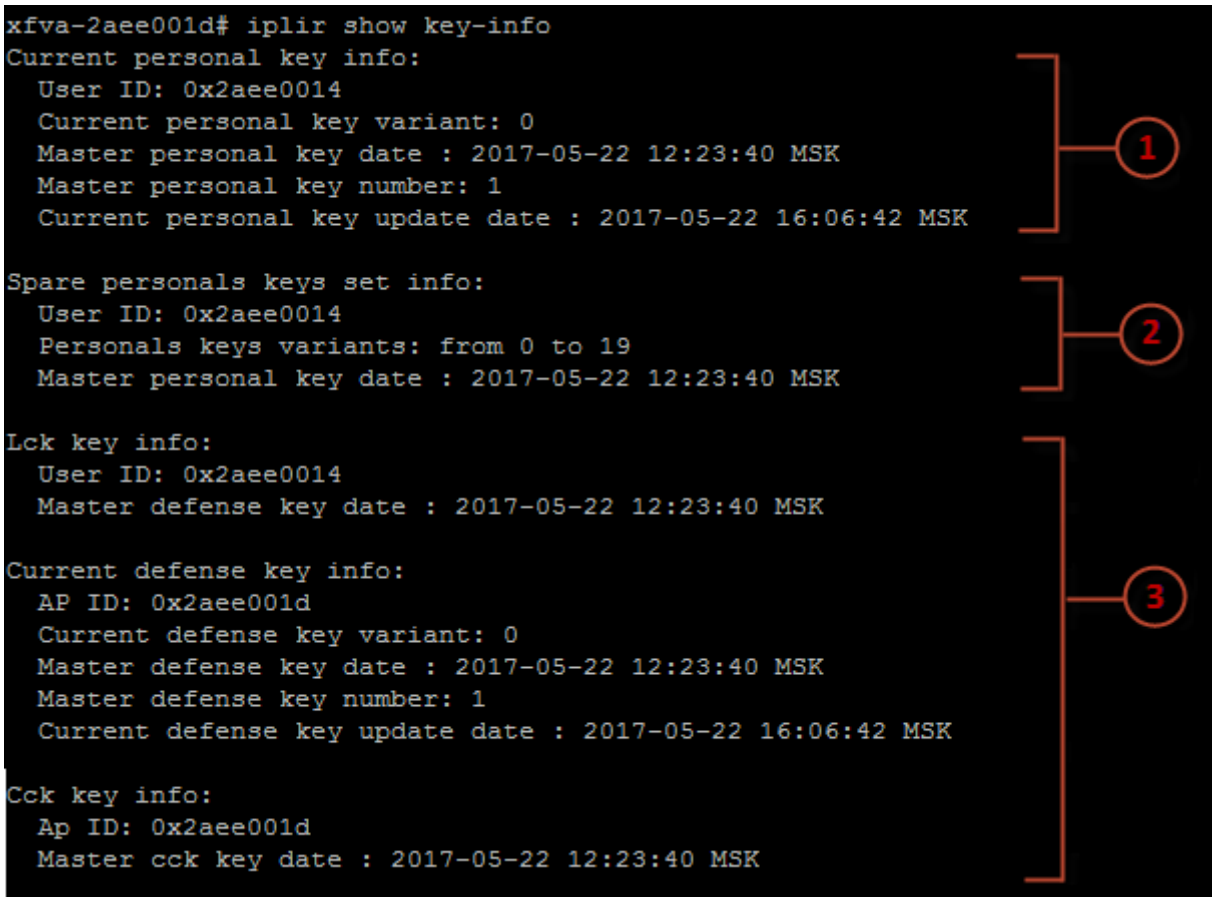


Рисунок 1. Просмотр информации о лицензии

Цифрами на рисунке обозначены:

1 Информация о текущем персональном ключе пользователя.

2 Информация о РНПК.

3 Информация о ключах узла.

Обновление ключей и лицензии при истечении срока их действия

Персональный ключ пользователя, который входит в состав ключей пользователя, а также ключи защиты ключей обмена, которые входят в состав ключей узла, имеют ограниченный срок действия — 12 месяцев. В ViPNet xFirewall реализован механизм, который проверяет срок действия этих ключей с момента их установки на узел при первоначальном развертывании дистрибутива лицензии или после обновления. За месяц, неделю и по истечении срока действия ключей производится специальное оповещение пользователя. В командном интерпретаторе и веб-интерфейсе появляются соответствующие сообщения. Кроме этого, информация об истечении срока действия ключей и лицензии добавляется в журнал событий.

Совет. Если требуется узнать, какого числа истекает срок действия персонального ключа или ключей защиты, вы можете просмотреть сведения об установленных ключах с помощью команды `iplir show key-info`.

Как правило, персональный ключ и ключи защиты устанавливаются и обновляются на узле одновременно, поэтому даты начала и окончания срока их действия чаще всего будут совпадать.

При истечении срока действия ключей никакие ограничения на работу ViPNet xFirewall не накладываются, но настоятельно рекомендуется обновить ключи, для чего следует обратиться к администратору сети ViPNet.

Обновление ключей производится по следующему алгоритму:

1. После вашего обращения администратор сети должен выполнить следующие действия:
   - Поднять вариант ключей пользователя при обновлении персонального ключа, ключей узла — при обновлении ключей защиты ключей обмена.
   - После изменения варианта ключей сформировать и выслать обновления ключей на узел ViPNet xFirewall.
   - В случае обновления персонального ключа — перезаписать персональный ключ на внешнем устройстве, если пользователь ViPNet xFirewall производит аутентификацию с помощью устройства.
2. На ViPNet xFirewall вы должны принять поступившие обновления ключей и убедиться в их успешной установке.

4

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet

Сетевым интерфейсам Ethernet, установленным в системе, присваиваются имена `eth0`, `eth1` и так далее (по количеству таких интерфейсов в системе). Чтобы настроить подключение к сети, задайте параметры сетевых интерфейсов Ethernet. Для этого выполните следующие действия:

1 По умолчанию сетевому интерфейсу назначен класс `access` (см. глоссарий, стр. 275). При необходимости смените класс с помощью команды:

```
hostname# inet ifconfig <имя интерфейса> class {access | trunk | slave}
```

Если требуется, чтобы данный интерфейс Ethernet обрабатывал трафик из нескольких VLAN (см. Организация обработки трафика из нескольких VLAN на стр. 46), назначьте ему класс `trunk`.

Если вы хотите объединить данный интерфейс Ethernet с другими в составе агрегированного интерфейса (см. Использование агрегированных сетевых интерфейсов на стр. 50), назначьте ему класс `slave`.

2 Выполните одно из действий:

- Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, выполните команду:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp
  ```

  Также для режима DHCP вы можете задать дополнительные параметры:

  - включить или выключить автоматическое получение адресов DNS-серверов командой:

    ```
    hostname# inet ifconfig <имя интерфейса> dhcp dns {on | off}
    ```

  - включить или выключить автоматическое получение NTP-серверов командой:

    ```
    hostname# inet ifconfig <имя интерфейса> dhcp ntp {on | off}
    ```

  - включить или выключить автоматическое получение маршрутов от DHCP-сервера командой:

    ```
    hostname# inet ifconfig <имя интерфейса> dhcp route {on | off}
    ```

  - задать специфичное значение метрики для маршрутов, полученных от DHCP-сервера, с помощью команды:

    ```
    hostname# inet ifconfig <имя интерфейса> dhcp route-metric {<1-255> | none}
    ```

  По умолчанию для всех дополнительных параметров режима DHCP установлено значение `on (none` для метрики маршрутов, полученных от DHCP-сервера`)`.

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах (см. Просмотр настроек DHCP в режиме клиента на стр. 166).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, выполните команду:

  ```
  hostname# inet ifconfig <имя интерфейса> address <IP-адрес> netmask <маска сети>
  ```

  Если до выполнения этой команды интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

3 По умолчанию для передачи данных через сетевой интерфейс используется размер MTU (см. глоссарий, стр. 272), равный 1500 байт. Чтобы оптимизировать передачу данных через интерфейс, вы можете изменить размер MTU. Для этого задайте новое значение MTU из диапазона 1280–9000 байт с помощью команды:

```
hostname# inet ifconfig <имя интерфейса> MTU {<значение MTU> | auto}
```

Чтобы вернуть значение по умолчанию, используйте параметр `auto`.

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.

4 Включите сетевой интерфейс с помощью команды:

```
hostname# inet ifconfig <имя интерфейса> up
```

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 добавить дополнительный статический IP-адрес на сетевой интерфейс Ethernet, убедитесь, что на этом интерфейсе задан статический основной IP-адрес, и выполните команду:

```
hostname# inet ifconfig <имя интерфейса> address add <IP-адрес> netmask <маска сети>
```

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. 273). 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).

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. Завершите работу управляющего демона с помощью команды:

   ```
   hostname> iplir stop
   ```

2. Измените класс интерфейса (см. глоссарий, стр. 275), к которому подключен коммутатор, с помощью команды:

   ```
   hostname# inet ifconfig <физический интерфейс> class trunk
   ```

3. Задайте номера виртуальных интерфейсов, которые будут соответствовать виртуальным сетям за коммутатором, с помощью следующих команд:

   ```
   hostname# inet ifconfig <физический интерфейс> vlan add <номер виртуального интерфейса>
   ```

4. Задайте параметры созданных виртуальных интерфейсов. Для этого выполните одно из действий:

   - Чтобы включить на сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, выполните команду:

     ```
     hostname# inet ifconfig <имя интерфейса> dhcp
     ```

     Также для режима DHCP вы можете задать дополнительные параметры:

     - включить или выключить автоматическое получение адресов DNS-серверов командой:

       ```
       hostname# inet ifconfig <имя интерфейса> dhcp dns {on | off}
       ```

     - включить или выключить автоматическое получение NTP-серверов командой:

       ```
       hostname# inet ifconfig <имя интерфейса> dhcp ntp {on | off}
       ```

     - включить или выключить автоматическое получение маршрутов от DHCP-сервера командой:

       ```
       hostname# inet ifconfig <имя интерфейса> dhcp route {on | off}
       ```

     - задать специфичное значение метрики для маршрутов, полученных от DHCP-сервера, с помощью команды:

       ```
       hostname# inet ifconfig <имя интерфейса> dhcp route-metric {<1-255> | none}
       ```

По умолчанию для всех дополнительных параметров режима DHCP установлено значение `on (none` для метрики маршрутов, полученных от DHCP-сервера`)`.

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах (см. Просмотр настроек DHCP в режиме клиента на стр. 166).

- Чтобы присвоить сетевому интерфейсу статический IP-адрес, выполните команду:

  ```
  hostname# inet ifconfig <имя интерфейса> address <IP-адрес> netmask <маска сети>
  ```

  Если до выполнения этой команды интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

5 Для редактирования конфигурационного файла `iplir.conf` выполните команду:

```
hostname# iplir config
```

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

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

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

8 Чтобы сохранить изменения в конфигурационном файле, нажмите сочетание клавиш **Ctrl+O**. Затем нажмите клавишу **Enter**.

9 Чтобы закрыть файл, нажмите сочетание клавиш **Ctrl+X**.

10 Включите физический интерфейс, к которому подключен коммутатор, с помощью команды:

```
hostname# inet ifconfig <физический интерфейс> up
```

При этом автоматически будут включены созданные виртуальные интерфейсы.

11 Запустите управляющий демон с помощью команды:

```
hostname> iplir start
```

Теперь ViPNet xFirewall сможет обрабатывать трафик из виртуальных сетей на соответствующих виртуальных интерфейсах.

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

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.

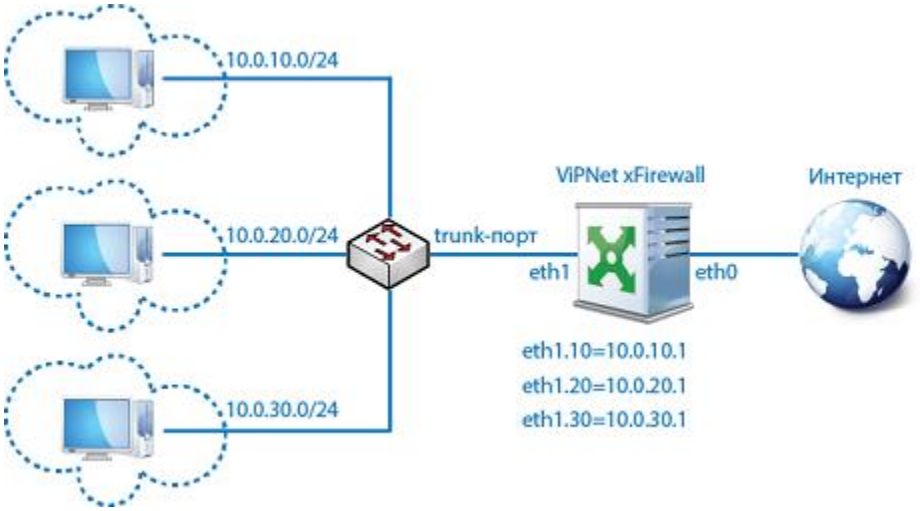


Рисунок 2. Схема использования ViPNet xFirewall в сети с VLAN

Предполагается, что сетевые настройки соответствуют приведенным на рисунке.

Чтобы настроить обработку трафика из нескольких VLAN с помощью командного интерпретатора, выполните следующие действия:

1. Перейдите в режим администратора (см. Аутентификация администратора на ViPNet xFirewall на стр. 26).
2. Завершите работу управляющего демона с помощью команды:

   ```
   hostname# iplir stop
   ```
3. Измените класс интерфейса eth1 с помощью команды:

   ```
   hostname# inet ifconfig eth1 class trunk
   ```
4. Добавьте виртуальные интерфейсы eth1.10, eth1.20, eth1.30, которые будут соответствовать виртуальным сетям с номерами 10, 20 и 30, с помощью следующих команд:

   ```
   hostname# inet ifconfig eth1 vlan add 10
   hostname# inet ifconfig eth1 vlan add 20
   hostname# inet ifconfig eth1 vlan add 30
   ```
5. Задайте параметры созданных виртуальных интерфейсов с помощью следующих команд:

   ```
   hostname# inet ifconfig eth1.10 address 10.0.10.1 netmask 255.255.255.0
   hostname# inet ifconfig eth1.20 address 10.0.20.1 netmask 255.255.255.0
   hostname# inet ifconfig eth1.30 address 10.0.30.1 netmask 255.255.255.0
   ```

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

```
hostname# iplir config
```

7 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
```

8 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
```

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

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

11 Включите интерфейс eth1 с помощью команды:

```
hostname# inet ifconfig eth1 up
```

При этом автоматически будут включены виртуальные интерфейсы eth1.10, eth1.20, eth1.30.

12 Запустите управляющий демон с помощью команды:

```
hostname# iplir start
```

После произведенных 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. 273). 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 (см. Режимы работы агрегированного интерфейса на стр. 52).

Создание агрегированного интерфейса

Чтобы добавить новый агрегированный сетевой интерфейс, выполните следующие действия:

1. Выберите физические интерфейсы ViPNet xFirewall, которые вы хотите объединить, и установите для них класс `slave` (см. глоссарий, стр. 275) с помощью команды:

   ```
   hostname# inet ifconfig <имя интерфейса> class slave
   ```

2. Выберите режим работы создаваемого агрегированного интерфейса (см. Режимы работы агрегированного интерфейса на стр. 52), затем создайте агрегированный канал с помощью команды:

   ```
   hostname# inet bonding add <номер> mode <режим> slaves <интерфейс 1> [<интерфейс 2>] [<интерфейс 3>]
   ```

   , где:

   - `<номер>` — номер агрегированного интерфейса. Вы можете создать до трех агрегированных интерфейсов с номерами 0, 1 или 2. В результате выполнения команды создается агрегированный интерфейс с именем `bond<номер>`.

- `<режим>` — режим работы агрегированного интерфейса.
- `<интерфейс 1>`, `<интерфейс 2>`, `<интерфейс 3>` — физические интерфейсы, подчиненные создаваемому агрегированному интерфейсу. Вы можете задать до трех подчиненных интерфейсов. При создании агрегированного интерфейса необходимо задать не менее одного подчиненного интерфейса. В дальнейшем вы можете добавлять подчиненные интерфейсы с помощью команды `inet ifconfig bonding add` и удалять подчиненные интерфейсы с помощью команды `inet ifconfig bonding delete`.

3 По умолчанию соединение на подчиненных физических интерфейсах проверяется каждые 0,1 секунды. Вы можете изменить это значение и задать частоту от 1 до 1000 миллисекунд с помощью следующей команды:

```
hostname# inet ifconfig <имя агрегированного интерфейса> bonding miimon <частота в миллисекундах>
```

4 Для режимов, в которых это требуется, задайте также дополнительные параметры с помощью команд, указанных в разделе Режимы работы агрегированного интерфейса (на стр. 52).

5 Выполните одно из действий:

- Чтобы включить на агрегированном сетевом интерфейсе режим автоматического получения параметров от DHCP-сервера, выполните команду:

  ```
  hostname# inet ifconfig <имя агрегированного интерфейса> dhcp
  ```

  Также для режима DHCP вы можете задать дополнительные параметры:

  - включить или выключить автоматическое получение адресов DNS-серверов командой:

    ```
    hostname# inet ifconfig <имя агрегированного интерфейса> dhcp dns {on | off}
    ```

  - включить или выключить автоматическое получение адресов NTP-серверов командой:

    ```
    hostname# inet ifconfig <имя агрегированного интерфейса> dhcp ntp {on | off}
    ```

  - включить или выключить автоматическое получение маршрутов от DHCP-сервера командой:

    ```
    hostname# inet ifconfig <имя агрегированного интерфейса> dhcp route {on | off}
    ```

  По умолчанию всем дополнительным параметрам режима DHCP установлено значение `on`.

  Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера. При необходимости вы можете просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах (см. Просмотр настроек DHCP в режиме клиента на стр. 166).

- Чтобы присвоить агрегированному сетевому интерфейсу статический IP-адрес, выполните команду:

  ```
  hostname# inet ifconfig <имя агрегированного интерфейса> address <IP-адрес> netmask <маска сети>
  ```

  Если до выполнения этой команды агрегированный интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

6 Отредактируйте файл конфигурации `iplir.conf`. Для этого выполните следующие действия:

6.1 Остановите управляющий демон с помощью команды:

```
hostname> iplir stop
```

6.2 Чтобы открыть файл конфигурации `iplir.conf` для редактирования, выполните команду:

```
hostname# iplir config
```

6.3 Добавьте секцию `[adapter]`, описывающую созданный агрегированный интерфейс (см. документ «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», главу «Файл iplir.conf»):

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

6.4 Запустите управляющий демон с помощью команды:

```
hostname> iplir start
```

7 По умолчанию созданному интерфейсу назначается класс `access`. Если вы хотите, чтобы интерфейс обрабатывал трафик из нескольких VLAN, назначьте ему класс `trunk` (см. Организация обработки трафика из нескольких VLAN на стр. 46).

8 Последовательно включите все подчиненные физические интерфейсы с помощью команды:

```
hostname# inet ifconfig <подчиненный интерфейс> up
```

9 Включите агрегированный сетевой интерфейс с помощью команды:

```
hostname# inet ifconfig <агрегированный интерфейс> up
```

В результате будет создан агрегированный интерфейс с именем `bond<номер>`. В дальнейшем вы можете работать с агрегированным интерфейсом так же, как с обычным физическим.

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 6. 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.

Режим	Описание
`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 можно задать с помощью команды: `inet ifconfig <имя агрегированного интерфейса> bonding xmit-hash-policy <алгоритм>` 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; • `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 команды: `inet ifconfig <интерфейс> bonding ad-select <алгоритм>` 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

Режим	Описание
	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 отправляются исходящие пакеты, выбирается аналогично режиму `balance-xor`. • С другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью команды: `inet ifconfig <интерфейс> bonding lacp-rate <slow | fast>` 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 команды `inet ifconfig bonding primary`), 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.

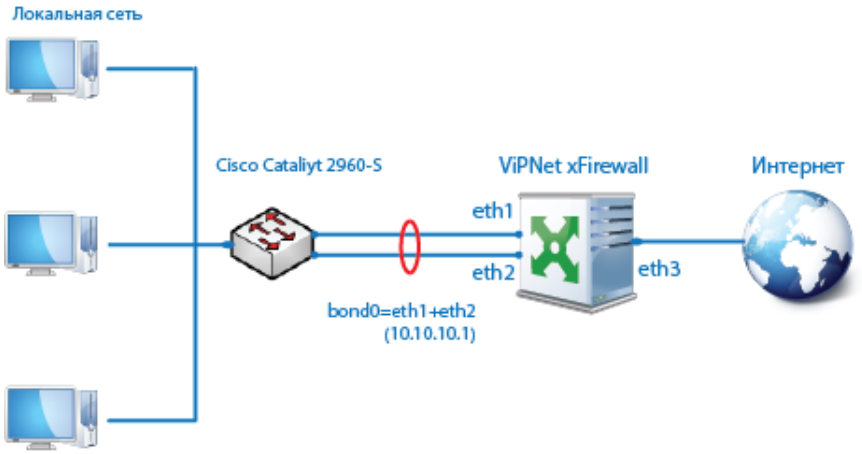


Рисунок 3. Агрегированный канал между ViPNet xFirewall и коммутатором

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. 52).

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 Установите для физических интерфейсов `eth1` и `eth2` класс `slave` с помощью команд:

```
hostname# inet ifconfig eth1 class slave
hostname# inet ifconfig eth2 class slave
```

2 Задайте режим работы создаваемого агрегированного интерфейса `802.3ad` с помощью команды:

```
hostname# inet bonding add 0 mode 802.3ad slaves eth1 eth2
```

3 Задайте алгоритм вычисления хэш-функции с помощью команды:

```
hostname# inet ifconfig bond0 bonding xmit-hash-policy layer3+4
```

4 Отредактируйте файл конфигурации `iplir.conf`. Для этого выполните следующие действия:

4.1 Остановите управляющий демон с помощью команды:

```
hostname# iplir stop
```

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

```
hostname# iplir config
```

4.3 Добавьте секцию `[adapter]` следующего содержания:

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

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

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

4.6 Запустите управляющий демон с помощью команды:

```
hostname> iplir start
```

5 Задайте для созданного агрегированного интерфейса IP-адрес с помощью следующей команды:

```
hostname# inet ifconfig bond0 address 10.10.10.1 netmask 255.255.255.0
```

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

7 Последовательно включите все подчиненные физические интерфейсы с помощью команд:

```
hostname# inet ifconfig eth1 up
hostname# inet ifconfig eth2 up
```

8 Включите агрегированный сетевой интерфейс с помощью команды:

```
hostname# inet ifconfig bond0 up
```

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 ViPNet-клиенты, 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
```

```
    switchport 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
    switchport mode access
    channel-group 2 mode active
!
interface GigabitEthernet0/2
    switchport access vlan 116
    switchport 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>
    switchport 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.

5

ViPNet xFirewall в сети ViPNet

Подключения к сети ViPNet

Настройка и управление программно-аппаратным комплексом ViPNet xFirewall возможны только по защищенному каналу управления. Для этих целей ViPNet xFirewall должен быть закреплен за ViPNet-координатором и иметь связь с ViPNet-клиентом (см. глоссарий, стр. 275), с которого будет выполняться управление и настройка ViPNet xFirewall.

Вне зависимости от расположения ViPNet xFirewall, его координатора и ViPNet-клиента необходимо настроить подключение ViPNet xFirewall к сети ViPNet в режиме с динамической трансляцией адресов.

Внимание! Для работы ViPNet xFirewall в сети ViPNet также необходимо задать в программе ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 272) координатор, который будет выполнять роль VPN-сервера для сетового узла ViPNet xFirewall. Подробнее см. документ «ViPNet Центр управления сетью. Руководство администратора» раздел «Добавление координатора без функций VPN-сервера». В свойства координатора без функций VPN-сервера установите межсетевой экран с динамической трансляцией адресов.

Для настройки подключения ViPNet xFirewall к сети ViPNet в режиме с динамической трансляцией адресов выполните следующие действия:

1 Завершите работу управляющего демона с помощью команды:

```
hostname> iplir stop
```

2 Откройте файл iplir.conf для редактирования с помощью команды:

```
hostname# iplir config
```

3 В собственной секции `[id]`:

- параметр `usefirewall` установите в значение `on`.
- в параметре `port` укажите значение из диапазона 1–65535 (по умолчанию — 55777).

4 В секции `[dynamic]`:

- параметр `dynamic_proxy` установите в значение `on`;
- в параметре `forward_id` укажите идентификатор внешнего координатора, с помощью которого ViPNet xFirewall будет устанавливать соединение с ViPNet-клиентом.

Внимание! Выбранный координатор должен быть доступен напрямую или через межсетевой экран со статической трансляцией адресов.

При подключении через межсетевой экран с динамическим NAT параметры `firewallip` и `port` секции `[dynamic]` определяются автоматически по информации, полученной от внешних узлов, редактировать их вручную не следует.

5 При необходимости в секции `[dynamic]`:

- измените значение параметра `timeout` (период отправки IP-пакетов координатору);
- параметр `always_use_server` установите в значение `on`, если требуется направлять весь IP-трафик через координатор. При этом учтите, что передача всего IP-трафика через координатор может привести к снижению скорости обмена данными между узлами.

6 Чтобы сохранить изменения в конфигурационном файле, нажмите сочетание клавиш **Ctrl+O**. Затем нажмите клавишу **Enter**.

7 Чтобы закрыть файл, нажмите сочетание клавиш **Ctrl+X**.

8 Запустите управляющий демон с помощью команды:

```
hostname> iplir start
```

Настройка виртуальных адресов сети ViPNet

Принципы назначения виртуальных адресов

Виртуальные адреса назначаются узлам сети ViPNet, которые подключаются к внешней сети через межсетевой экран. Необходимость использования виртуальных адресов обусловлена тем, что узлы, стоящие за разными межсетевыми экранами, могут иметь одинаковые адреса в своих частных сетях, и в случае обращения к ним по реальным адресам могла бы возникнуть неоднозначность. Для узлов, не находящихся за внешним межсетевым экраном, виртуальные адреса также назначаются, но не используются.

Параметры, необходимые для назначения виртуальных адресов, задаются в секции `[virtualip]` файла `iplir.conf`.

При появлении каждого сетевого узла в списке связей ему назначается виртуальный адрес, который привязан к уникальному идентификатору этого узла и соответствует его первому реальному адресу. Такой виртуальный адрес называется базовым, и он является точкой отсчета при назначении виртуальных адресов для каждого из реальных адресов узла.

Остальные виртуальные адреса сетевого узла, характеризующие каждый из реальных адресов узла, называются вторичными виртуальными адресами или для простоты — виртуальными адресами, и указываются в параметре `ip` соответствующей секции `[id]` через запятую после реального адреса.

При обновлениях адресных справочников, а также изменениях в списке реальных адресов для какого-либо узла сетевые узлы сохраняют свои виртуальные адреса, а вновь добавленные узлы и реальные IP-адреса получают новые свободные виртуальные адреса (с учетом ограничения на максимально возможный адрес, регулируемого параметрами `startvirtualip` и `maxvirtualip` секции `[virtualip]`).

Настройка IP-адресов доступа к узлу и их приоритета

Каждый узел сети ViPNet взаимодействует с другим узлом, с которым у него есть связь, по определенному адресу доступа. Однако нередко некоторые узлы подключены к нескольким независимым каналам связи и имеют несколько адресов доступа, каждый из которых может использоваться для связи с другими узлами.

При наличии разных каналов для связи между узлами может возникнуть ситуация, когда для взаимодействия будет выбран менее предпочтительный канал (более дорогостоящий или менее быстродействующий). Например, если ViPNet xFirewall, находящийся в центральном офисе

организации, для выхода в Интернет использует одновременно два канала, предоставляемых разными провайдерами, то в результате автоматического определения адреса доступа может быть выбран менее предпочтительный канал, а более предпочтительный канал будет простаивать. Во избежание такой ситуации вы можете задать приоритеты каналов связи, исходя из стоимости их обслуживания, быстродействия или других параметров.

Приоритеты каналов связи задаются путем настройки метрик на стороне того сетевого узла, которому необходимо получить доступ к сегменту сети ViPNet. Например, в случае взаимодействия узлов филиала и центрального офиса, если в центральном офисе используется одновременно два канала, то настройки производятся на стороне сетевого узла филиала.

Исходя из значений метрик каналов, ПО ViPNet xFirewall будет выбирать более приоритетный канал связи. Для этого при включении ViPNet xFirewall отправляет служебные сообщения на все известные адреса доступа узлов с определенной задержкой, равной метрике, заданной для этих адресов в миллисекундах. Выбор канала для связи производится с учетом следующего:

- Адрес с наименьшей метрикой считается наиболее приоритетным. Соединение с узлом устанавливается по адресу с наименьшей метрикой всегда, когда этот адрес доступен.
- Если адрес с наименьшей метрикой недоступен или если все метрики равны, то соединение с узлом устанавливается по тому адресу, доступность которого определяется быстрее в результате опроса.
- Если помимо адресов с заданными метриками, есть адреса, для которых метрика установлена в значение `auto` (определяется автоматически), значение `auto` всегда будет на 100 миллисекунд больше максимального значения заданной метрики. То есть канал с автоматически определяемой метрикой всегда будет иметь самый низкий приоритет по сравнению с каналами, для которых метрика задана вручную.
- После установления соединения с узлом определение доступности других его адресов выполняется только при разрыве текущего соединения.

Настройка адресов доступа для узлов, связанных с ViPNet xFirewall, осуществляется в соответствующих секциях `[id]` файла `iplir.conf`. Каждый адрес доступа узла указывается в параметре `accessiplist` этой секции, количество данных параметров в секции не ограничено.

Примечание. IP-адреса доступа узла могут быть настроены централизованно в ПО ViPNet Центр управления сетью. В этом случае они будут указаны в соответствующих секциях `[id]` файла `iplir.conf`. Для таких адресов вы также можете настроить приоритет, изменив соответствующие значения метрик (по умолчанию они определяются автоматически).

Чтобы указать IP-адреса доступа к какому-либо узлу, связанному с ViPNet xFirewall, и определить приоритеты этих адресов, выполните следующие действия:

1 Завершите работу управляющего демона с помощью команды:

```
hostname> iplir stop
```

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

```
hostname# iplir config
```

3 В параметрах `accessiplist` секции `[id]` соответствующего узла выполните одно из действий:

- Укажите IP-адреса доступа к узлу и задайте метрики для каждого из этих адресов в следующем виде:

  ```
  accessiplist = <IP-адрес узла>, <метрика>
  ```

  При задании значения метрики необходимо учитывать следующее:

  - рекомендуется указывать значения метрик больше максимального времени задержки при прохождении служебного сообщения и ответа на него по соответствующему каналу, но не превышающее 9999 миллисекунд;
  - рекомендуемая минимальная разница между метриками — 100 миллисекунд.

- Если вы уже указали IP-адреса доступа ранее или они были получены из программы ViPNet Центр управления сетью автоматически, в параметре `accessiplist` задайте метрики для этих адресов в соответствии с рекомендациями, описанными выше.

4 Сохраните изменения в файле `iplir.conf` и запустите управляющий демон с помощью команды:

```
hostname> iplir start
```

В результате в параметры `accessiplist` файла `iplir.conf` автоматически будут добавлены реальный IP-адрес сетевого интерфейса узла, через который будут передаваться IP-пакеты для выбранного IP-адреса доступа, условный номер этого интерфейса и тип регистрации данного IP-адреса доступа узла в виде:

```
accessiplist = <IP-адрес узла>, <метрика>, <IP-адрес интерфейса>, <номер интерфейса>, <тип регистрации>
```

Настройка параметров видимости узлов

Для связи ViPNet xFirewall с узлами сети ViPNet могут использоваться реальные или виртуальные IP-адреса. По умолчанию для связи с узлами, от которых ViPNet xFirewall получает широковещательные пакеты, используются их реальные адреса. Вы можете изменить настройки адресов видимости с помощью параметра `visibility` в секциях `[id]` и параметров в секции `[visibility]` файла `iplir.conf`.

Видимость каждого узла сети ViPNet определяется следующим образом:

1 Если в секции `[id]` узла, присутствует параметр `visibility`, то видимость узла определяется значением этого параметра.

2 Если в секции `[id]` узла нет параметра `visibility`, но при этом сеть, которой принадлежит узел, указана в параметре `subnet_real` или `subnet_virtual` секции `[visibility]`, то видимость узла определяется значением этого параметра.

3 В иных случаях видимость узла определяется значением параметра `default` секции `[visibility]`.

То есть индивидуальные настройки видимости узлов приоритетнее настроек видимости сетей, а настройки видимости сетей приоритетнее настроек видимости по умолчанию.

Чтобы настроить параметры видимости узлов, выполните следующие действия:

1 Завершите работу управляющего демона с помощью команды:

```
hostname> iplir stop
```

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

```
hostname# iplir config
```

3 Чтобы настроить параметры видимости узлов по умолчанию и параметры видимости сетей, в секции `[visibility]`:

- параметр `default` установите в одно из значений:
  - `auto` (по умолчанию) — видимость узлов определяется автоматически;
  - `real` — для доступа к узлам используются их реальные IP-адреса;
  - `virtual` — для доступа к узлам используются их виртуальные IP-адреса.
- при необходимости укажите идентификаторы вашей сети ViPNet и доверенных сетей в одном из параметров:
  - `subnet_auto` — идентификаторы сетей ViPNet, для которых необходимо настроить автоматическую видимость узлов;
  - `subnet_real` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по реальным IP-адресам;
  - `subnet_virtual` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по виртуальным IP-адресам.

  В каждом из этих параметров можно указать один либо несколько идентификаторов через запятую.

4 Чтобы настроить параметры видимости отдельных узлов, в соответствующих секциях `[id]` параметр `visibility` установите в одно из значений:

- `auto` — определять видимости узла автоматически, в зависимости от его текущего адреса видимости.
- `real` — всегда обращаться к узлу по его реальному адресу.
- `virtual` — всегда обращаться к узлу по его виртуальному адресу.

Внимание! Настраивать параметры видимости отдельных узлов нужно с осторожностью, так как если для двух узлов с одинаковыми реальными адресами, но разными виртуальными, установить параметр `visibility` в значение `real`, возникнет конфликт IP-адресов.

5 Сохраните изменения в файле `iplir.conf` и запустите управляющий демон с помощью команды:

```
hostname> iplir start
```

Настройка параметров виртуальных адресов

Каждый узел сети ViPNet автоматически формирует один или несколько виртуальных IP-адресов для каждого узла сети ViPNet, с которым он связан. Каждому реальному адресу узла ставится в соответствие виртуальный IP-адрес. То есть число формируемых виртуальных адресов зависит от числа реальных адресов узла.

Чтобы настроить параметры виртуальных адресов ViPNet xFirewall, выполните следующие действия:

1. Завершите работу управляющего демона с помощью команды:

   ```
   hostname> iplir stop
   ```

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

   ```
   hostname# iplir config
   ```

3. В секции `[virtualip]` при необходимости измените значения следующих параметров:

   - `startvirtualip` — стартовый адрес для формирования базовых виртуальных адресов защищенных узлов (по умолчанию — `11.0.0.1`). При изменении данного параметра учитывайте, что назначение всех базовых виртуальных адресов производится заново, как при начальном формировании файлов конфигурации.
   - `maxvirtualip` — максимальный адрес для формирования базовых виртуальных адресов (по умолчанию — `11.0.254.254`). Данный параметр используется для ограничения диапазона назначаемых базовых виртуальных адресов. Вы можете его уменьшить, при этом необходимо следить за тем, чтобы оно было больше значения параметра `endvirtualip`.

4. Сохраните изменения в файле `iplir.conf` и запустите управляющий демон с помощью команды:

   ```
   hostname> iplir start
   ```

6

Управление сертификатами

Применение сертификатов в ViPNet xFirewall

ViPNet xFirewall позволяет использовать учетные данные пользователей, хранящиеся на LDAP-сервере (см. глоссарий, стр. 272) и выполнять аутентификацию этих пользователей через сервис Captive portal (см. глоссарий, стр. 270), 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. 275). Для проверки факта аннулирования сертификата со стороны удостоверяющего центра (см. глоссарий, стр. 276) используются списки аннулированных сертификатов CRL (см. глоссарий, стр. 276). Пример использования сертификатов и CRL при аутентификации пользователей через сервис Captive portal приведен в разделе (см. Получение и импорт сертификатов на стр. 129) настоящего документа.

В ViPNet xFirewall вы можете:

- импортировать сертификаты и CRL в кодировке Base64 (см. глоссарий, стр. 270) и DER (см. глоссарий, стр. 276), подписанные открытым ключом RSA;
- создавать запросы на сертификат в формате PKCS#12 (см. глоссарий, стр. 272);
- 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 выполняется в режиме администратора (см. Аутентификация администратора на ViPNet xFirewall на стр. 26), за исключением команд просмотра, которые доступны в режиме пользователя.

Подробное описание команд по работе с сертификатами и CRL см. в документе «ViPNet x Firewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».

Создание запроса на сертификат

Для получения сертификата выполните следующие действия:

1. Создайте запрос на сертификат с помощью команды:

   ```
   hostname# service cert request create name <имя сертификата> bits <длина ключа> digest {md5 | sha1}
   ```

   Длина RSA-ключа: `1024, 1536, 2048, 3072, 4096` бит.

   После выполнения команды будет создан файл закрытого ключа `<имя сертификата>_key.pem` и файл запроса на сертификат `<имя сертификата>_req.pem`.

2. Подключите USB-накопитель к ViPNet xFirewall и выполните экспорт файла запроса на сертификат:

   ```
   hostname# service cert request export <имя сертификата>_req.pem
   ```

3. Передайте файл запроса на сертификат в удостоверяющий центр (см. глоссарий, стр. 276).

Сертификат, выпущенный по запросу, должен быть импортирован в локальное хранилище ViPNet xFirewall.

Импорт сертификата и CRL

Вы можете импортировать в локальное хранилище ViPNet xFirewall:

- сертификаты (файлы `.cer` или `.pem` в кодировках BASE64 или DER);
- списки отозванных сертификатов (файлы `.crl`).

Для импорта сертификата или CRL подключите USB-накопитель с файлами к ViPNet xFirewall и выполните команду:

```
hostname# service cert import
```

При выполнении команды будет выведен список файлов сертификатов, находящихся на USB-накопителе.

```
Insert USB flash drive into empty USB slot and press <Enter>

Try to mount /dev/sdc1 as vfat

/dev/sdc1 mounted

1 - /usb/Cert1.cer
```

```
2 - /usb/CRL1.crl
Enter file number [1-2] or [q] to cancel: 1
Certificate /usb/Cert1.cer will be converted to PEM
Certificate:
...
/usb/Cert1.cer was imported as Cert1.pem
hostname#
```

Выберите из списка нужный файл сертификата или CRL. Файл будет импортирован в локальное хранилище.

Просмотр локального хранилища сертификатов

Вы можете просмотреть состояние локального хранилища сертификатов ViPNet xFirewall, выполнив команду:

```
hostname> service cert list
Certificates:
...
Certificate revocation list:


Private keys:
...
hostname>
```

Просмотр содержимого сертификата

Вы можете просмотреть содержимое сертификата (в примере Cert1.pem), выполнив команду:

```
hostname> service cert show cert Cert1.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            8c:93:38:27:1b:36:9c:be
    Signature Algorithm: sha1WithRSAEncryption
...
hostname>
```

Просмотр содержимого списка отозванных сертификатов

Вы можете просмотреть содержимое списка отозванных сертификатов (в примере CRL1.pem), выполнив команду:

```
hostname> service cert show cert CRL1.pem

Certificate Revocation List (CRL):

        Version 2 (0x1)

    Signature Algorithm: sha1WithRSAEncryption

...

hostname>
```

7

Настройка межсетевого экрана

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, вы можете ознакомиться со схемой фильтрации транзитного трафика в ViPNet xFirewall (см. Рисунок 4 на стр. 74). В ViPNet xFirewall фильтрация транзитного трафика происходит в следующем порядке:

1. Все входящие IP-пакеты проверяются на фрагментацию, если включена соответствующая настройка межсетевого экрана (см. Настройка дополнительных параметров межсетевого экрана на стр. 137). 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. 100), если создано соответствующее правило трансляции адресов.
3. После трансляции адреса назначения IP-пакет проходит проверку встроенным средством антиспуфинга, если оно включено (см. Настройка антиспуфинга на стр. 135).
4. В случае успешной проверки встроенным средством антиспуфинга для IP-пакета возможны следующие варианты дальнейшего пути обработки:
   - Если IP-пакет относится к протоколу HTTP (транспортный протокол TCP, порт 80) и прокси-сервер включен:
     - IP-пакет проходит фильтрацию содержимого трафика (см. Настройка фильтрации содержимого трафика на стр. 116).

- 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 (см. Приложение на стр. 86), прикладному протоколу (см. Прикладной протокол на стр. 87) и 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. 99), 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. 74).
  - В случае успешной проверки сетевыми фильтрами для IP-пакета выполняется трансляция адреса источника (Source NAT) (см. Трансляция адреса источника на стр. 99), 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 5 на стр. 75).
- 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.

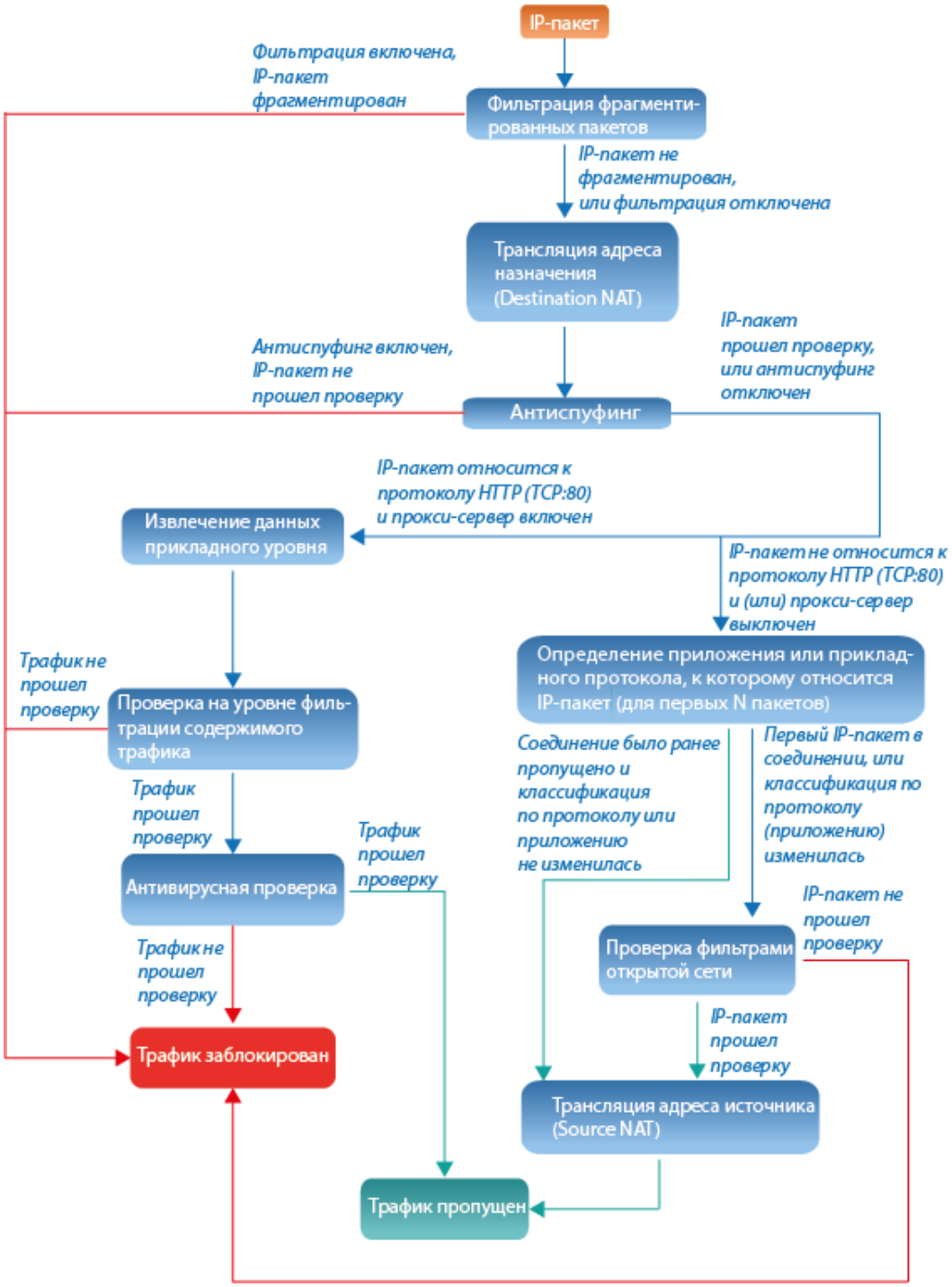


Рисунок 4. Схема фильтрации трафика ViPNet xFirewall

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. 272), может включать сетевые фильтры и правила трансляции адресов и рассылается на узлы с помощью транспортного модуля MFTP (см. глоссарий, стр. 276). 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 5. 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 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. 77) — настроенные по умолчанию группы с фиксированными именами, которые могут использоваться для задания адресов отправителей и получателей IP-пакетов в фильтрах (см. Создание сетевого фильтра на стр. 81) и правилах трансляции адресов (см. Создание правила трансляции адресов на стр. 101), а также при создании пользовательских групп объектов (см. Создание группы объектов на стр. 78). Такие группы объектов не отображаются в списках групп (см. Просмотр групп объектов на стр. 79), их нельзя ни изменить, ни удалить.
- Группы объектов из программы ViPNet Policy Manager (см. глоссарий, стр. 272) — 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. 78). Такие группы можно использовать для задания параметров фильтров (см. Создание сетевого фильтра на стр. 81) и правил трансляции (см. Создание правила трансляции адресов на стр. 101), а также при создании других пользовательских групп объектов (см. Создание группы объектов на стр. 78). При необходимости их можно удалить.

Системные группы объектов

В таблице ниже описаны доступные системные группы объектов.

Таблица 7. 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 добавлении сетевых фильтров и правил трансляции, необходимых для работы прокси-сервера, с помощью команды
`hostname# service http-proxy fw-rules apply`

- Группы протоколов, которые наиболее часто используются при создании сетевых фильтров. Они перечислены в приложении (см. Пользовательские группы протоколов по умолчанию на стр. 232).
- Группы расписаний:
  - `Workdays` (рабочие дни) — включает рабочие дни недели (с понедельника по пятницу).
  - `Weekends` (выходные дни) — включает выходные дни недели (субботу и воскресенье).

Примечание. О том, как просмотреть пользовательские группы объектов, созданные на узле, см. в разделе Просмотр групп объектов (на стр. 79).

Создание группы объектов

Чтобы создать группу объектов, выполните команду:

`hostname# firewall <тип объектов> add name @<имя> <состав> [exclude <исключения>]`, где:

- параметр `<тип объектов>` может принимать одно из следующих значений:
  - `ip-object` — IP-адреса или доменные имена;
  - `vpn-object` — ViPNet-узлы;
  - `interface-object` — сетевые интерфейсы;
  - `service-object` — протоколы;
  - `schedule-object` — расписания;
- имя группы должно начинаться с символа «`@`», не содержать пробелов и быть уникальным в рамках групп объектов одного типа;

- в параметрах `<состав>` и `<исключения>` указываются объекты, входящие и не входящие в группу соответственно, причем:
  - IP-адреса и идентификаторы ViPNet-узлов указываются через запятую или в виде диапазона (подробнее см. в разделах Адрес отправителя (на стр. 83) и Адрес получателя (на стр. 85));
  - сетевые интерфейсы разделяются пробелом, и перед именем каждого сетевого интерфейса необходимо указать слово `interface`;
  - протоколы или расписания указываются в соответствии с синтаксисом, описанным в разделах Протокол (см. Транспортный протокол на стр. 86) и Расписание (на стр. 89).

Примечание. Если при вводе команды была допущена синтаксическая ошибка, то в результате выполнения такой команды появится сообщение с указанием слова, содержащего ошибку. Исправьте ошибку и выполните команду еще раз.

В результате будет создана группа объектов, и вы сможете использовать ее для задания параметров сетевых фильтров (см. Создание сетевого фильтра на стр. 81) и правил трансляции адресов.

Примеры создания групп объектов

Чтобы создать группу IP-адресов, включающую сегмент сети за исключением нескольких IP-адресов, выполните команду:

```
hostname# firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude
110.35.14.3,110.35.14.13
```

Чтобы создать группу расписания, включающую выходные дни с 9 до 23 часов, выполните команду:

```
hostname# firewall schedule-object add name @weekend weekly sa su at 09:00-23:00
```

Чтобы создать группу интерфейсов, включающую сетевые интерфейсы `eth0` и `eth1`, выполните команду:

```
hostname# firewall interface-object add name @intgroup interface eth0 interface eth1
```

Просмотр групп объектов

Чтобы просмотреть пользовательские группы объектов и группы объектов, полученные из программы ViPNet Policy Manager, выполните одну из команд:

- для просмотра всех групп объектов:

  ```
  hostname> firewall object show
  ```

- для просмотра групп объектов определенного типа (см. Создание группы объектов на стр. 78):

  ```
  hostname> firewall <тип объектов> show
  ```

  Например, для просмотра всех групп IP-адресов:

  ```
  hostname> firewall ip-object show
  ```

В результате выполнения команды будет отображена таблица, содержащая те или иные группы объектов. Пример таблицы групп IP-адресов представлен на рисунке ниже.

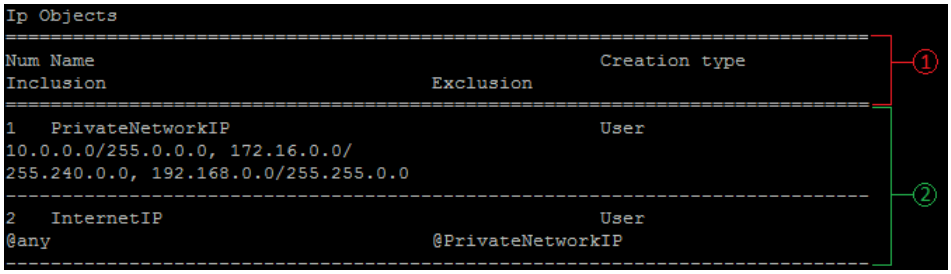


Рисунок 6. Просмотр групп IP-адресов

Цифрами обозначены:

1 Заголовок таблицы, где:

- `Num` — порядковый номер группы объектов.
- `Name` — имя группы объектов.
- `Creation type` — вид группы объектов: для групп из программы ViPNet Policy Manager — `Policy`, для пользовательских групп — `User`.
- `Inclusion` — состав группы объектов.
- `Exclusion` — исключения группы объектов.

2 Параметры групп объектов.

Удаление групп объектов

Вы можете удалить пользовательскую группу объектов, если она не используется в других группах объектов, сетевых фильтрах или правилах трансляции адресов.

Для удаления группы объектов выполните команду:

```
hostname# firewall object delete @<имя>
```

Примечание. При попытке удаления группы объектов, используемой в другой группе объектов, сетевом фильтре или правиле трансляции адресов, появится сообщение об ошибке со списком всех групп, фильтров и правил, которые используют данную группу. Удалите эти группы, фильтры и правила, затем выполните команду для удаления группы еще раз.

Чтобы удалить группу сетевых узлов ViPNet с именем `range_<диапазон узлов>`, которая создается при конвертации правил защищенной сети во время обновления ViPNet xFirewall, необходимо сначала удалить все сетевые фильтры, в которых содержится эта группа.

В результате группа объектов будет удалена, и вы больше не сможете использовать ее для задания параметров сетевых фильтров, правил трансляции адресов и при создании других групп объектов.

Создание сетевого фильтра

Для каждого вида трафика создаются отдельные сетевые фильтры, которые хранятся в соответствующей таблице.

Чтобы создать сетевой фильтр, выполните команду:

```
hostname# firewall <тип> add [<номер>] [rule <имя>] src <адрес отправителя>
dst <адрес получателя> [<транспортный протокол>] [dpiapp <приложение>] [dpiprotocol
<прикладной протокол>] [dpigroup <группа приложений>] [dnuser <пользователь>]
[<расписание>] <действие>,
```

указав следующие параметры:

- Тип фильтра:
  - `vpn` — фильтр защиты канала управления;
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети.

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.

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.

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.

- Порядковый номер фильтра в таблице, определяющий его приоритет. Чем меньше порядковый номер фильтра, тем выше его приоритет (наиболее приоритетный фильтр имеет номер 1). При создании фильтра с порядковым номером, меньшим максимального номера в таблице фильтров, номера фильтров, следующих за этим фильтром, автоматически увеличиваются на единицу (то есть их приоритет понижается).
- Имя фильтра. Если имя состоит из нескольких слов, разделенных пробелом, заключите его в кавычки (например, `rule "number one"`).

Примечание. Порядковый номер не является обязательным параметром фильтра. При создании фильтра без указания его номера ему будет присвоен номер, следующий за номером последнего фильтра в соответствующей таблице, и он

будет иметь самый низкий приоритет.

Имя фильтра можно указывать без слова `rule`. Кроме этого, имя фильтра также не является обязательным параметром фильтра.

- Параметры, определяющие процесс обработки IP-пакетов этим фильтром. Подробное описание этих параметров см. в соответствующих разделах:
  - Адрес отправителя (на стр. 83);
  - Адрес получателя (на стр. 85);
  - Транспортный протокол (на стр. 86);
  - Приложение (на стр. 86) — для транзитных фильтров открытой сети;
  - Прикладной протокол (на стр. 87) — для транзитных фильтров открытой сети;
  - Группа приложений (на стр. 88) — для транзитных фильтров открытой сети;
  - Пользователь (на стр. 88) — для транзитных фильтров открытой сети;
  - Расписание (на стр. 89);
  - Действие (на стр. 89).

Примечание. Если при вводе команды была допущена синтаксическая ошибка, то в результате выполнения такой команды появится сообщение с указанием слова, содержащего ошибку. Исправьте ошибку и выполните команду еще раз.

При создании транзитных фильтров открытой сети возможно использование нескольких значений параметров `<приложение>`, `<прикладной протокол>`, `<группа приложений>` и `<пользователь>`. Значения в списке разделяются запятой. Значение, содержащее пробелы, заключается в двойные кавычки.

Чтобы создать транзитный фильтр открытой сети с несколькими значениями параметров, используйте в команде `firewall forward add` следующие лексемы:

- `dpiapp <приложение 1>,<приложение N>`
- `dpiprotocol <прикладной протокол 1>,<прикладной протокол N>`
- `dpigroup <группа приложений 1>,<группа приложений N>`
- `dnuser <пользователь 1>,<пользователь N>`

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

Примеры создания сетевых фильтров

Чтобы разрешить отправку FTP-запросов со своего узла открытому узлу с адресом 192.168.2.4, выполните команду:

```
hostname# firewall local add src @local dst 192.168.2.4 service @FTP pass
```

Чтобы создать локальный фильтр, блокирующий IP-пакеты, отправляемые узлом с адресом 192.168.30.1 через порт 2525 на порт 443 открытого узла с адресом 172.16.35.1 по протоколу TCP/IP, выполните команду:

```
hostname# firewall local add src 192.168.30.1 dst 172.16.35.1 tcp sport 2525 dport 443 drop
```

Чтобы создать фильтр, разрешающий отправку открытых транзитных IP-пакетов от узла с адресом 192.168.0.1 на узел с адресом 192.168.30.3 через ViPNet xFirewall, выполните команду:

```
hostname# firewall forward add src 192.168.0.1 dst 192.168.30.3 pass
```

Чтобы создать транзитный фильтр открытой сети, блокирующий IP-пакеты приложения Skype по протоколу SSL для пользователя `ivanov`, выполните команду:

```
hostname# firewall forward add src @any dst @any dpiapp skype dpiprotocol SSL dnuser ivanov
drop
```

Чтобы создать транзитный фильтр открытой сети с номером 333, который запрещает MPEG и SSL трафик с ресурсов Youtube и Vimeo для пользователей PetrovPP, SidorovKP и Ivan Ivanov, выполните команду:

```
hostname# firewall forward add 333 src @any dst @any dpiapp Youtube,Vimeo dpiprotocol
MPEG,SSL dnuser PetrovPP,SidorovKP,"Ivan Ivanov" drop
```

Чтобы создать транзитный фильтр открытой сети с номером 444, запрещающий трафик мессенджеров и онлайн трансляций (группа `Messaging` и `Streaming`) для пользователей `PetrovPP` и `SidorovKP`, выполните команду:

```
hostname# firewall forward add 444 src @any dst @any dpigroup Messaging,Streaming dnuser
PetrovPP,SidorovKP drop
```

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. Настройка фильтрации содержимого трафика на стр. 116).

Адрес отправителя

Адрес отправителя IP-пакетов является обязательным параметром сетевого фильтра и описывается лексемой:

```
src <адрес отправителя>
```

Возможные значения адреса отправителя:

- для локальных фильтров открытой сети:
  - IP-адрес или доменное имя узла;

Примечание. При задании адреса отправителя в виде доменного имени на DNS-сервер отправляется соответствующий запрос для разрешения данного имени. DNS-запись, полученная в ответ на такой запрос, сохраняется в кэше и используется до истечения времени ее жизни. Актуальность данных в кэше обеспечивается регулярной отправкой запросов на DNS-сервер.

Если разрешения указанного в фильтре доменного имени по каким-либо причинам не произошло, то такой фильтр не загружается в драйвер ViPNet до тех пор, пока в результате отправки повторных запросов от DNS-сервера не будет получен корректный ответ.

  - диапазон IP-адресов узлов — два ограничивающие диапазон IP-адреса, разделенные дефисом. При этом второй адрес (конец диапазона) должен быть больше первого (начала диапазона), например:

```
src 192.168.1.1-192.168.1.10
```

  - маска адресов подсети — адрес подсети в формате классовой или бесклассовой адресации CIDR (Classless Internet Domain Routing), например:

`src 192.168.1.0/24` или `src 192.168.1.0/255.255.255.0`

  - доменное имя узла, например:

```
src mydomain.ru
```

Примечание. При необходимости вы можете задать несколько IP-адресов и доменных имен отправителей IP-пакетов в одной лексеме, перечислив их через запятую, например: `src 192.168.30.2,192.169.1.1,mydomain.ru`

  - системная группа объектов `any`, `local` или `remote` либо одна или несколько пользовательских групп IP-адресов. Имя группы необходимо дополнить символом «`@`», несколько групп указываются через запятую. Например:

```
src @IP_group_1,@IP_group_2
```

Внимание! Использование других адресов отправителей IP-пакетов совместно с системными группами объектов `any`, `local` и `remote` недопустимо.

  - сетевой интерфейс собственного узла, через который будут проходить IP-пакеты, в следующем виде:

```
src interface {<системное имя> | @<имя группы интерфейсов> | byip {<IP-адрес> |
<диапазон IP-адресов> | <маска адресов>}}
```

- для транзитных фильтров открытой сети: то же, что для локальных фильтров открытой сети, но в таких фильтрах нельзя использовать системные группы объектов.
- для фильтров защиты канала управления:

- идентификатор узла ViPNet, например:

  ```
  src 0x1a12000a
  ```

- системные группы объектов `any`, `allcoordinators`, `allclients`, `local` или `remote` либо пользовательские группы узлов ViPNet. Имя группы необходимо дополнить символом «`@`», несколько групп указываются через запятую. Например:

  ```
  src @allclients,@allcoordinators
  ```

- идентификатор сети ViPNet, например:

  ```
  src 0x1a12
  ```

Примечание. При задании адреса отправителя для фильтров защиты канала управления:

- В одной лексеме можно указать несколько идентификаторов узлов или сетей ViPNet, пользовательских групп узлов ViPNet и системную группу `allcoordinators` или `allclients`, перечислив их через запятую. Например: `src @allcoordinators,0x1a12000a`
- Недопустимо указывать IP-адреса, доменные имена, маски адресов и сетевой интерфейс узла.
- Недопустимо использовать другие адреса отправителей совместно с группами объектов `any`, `local` и `remote`.

Адрес получателя

Адрес получателя IP-пакетов является обязательным параметром сетевого фильтра. Синтаксис адреса получателя повторяет синтаксис адреса отправителя (см. Адрес отправителя на стр. 83), за исключением следующих особенностей:

- Адрес получателя описывается после адреса отправителя лексемой:

  ```
  dst <адрес получателя>
  ```

- Для задания адреса получателя нельзя использовать сетевой интерфейс узла.
- Для задания адреса получателя, помимо пользовательских групп объектов, можно использовать следующие системные группы объектов (на стр. 77):
  - для локальных фильтров открытой сети: `any`, `local`, `remote`, `broadcast`, `multicast`.
  - для фильтров защиты канала управления: `any, allcoordinators, allclients, local, remote, broadcast`.

Внимание! Использование других адресов получателей IP-пакетов совместно с системными группами объектов `any`, `local`, `remote`, `broadcast` и `multicast` недопустимо.

- Для задания адреса получателя нельзя использовать кириллицу.

Транспортный протокол

Транспортный протокол не является обязательным параметром сетевого фильтра.

Транспортные протоколы можно указывать, используя:

- имена протоколов, написанные строчными буквами и разделенные пробелами, например:

  `tcp udp icmp`

  В этом случае также можно задать дополнительные параметры для протоколов, например:

  - для протоколов TCP и UDP: `sport` (порт или диапазон портов источника пакета) и (или) `dport` (порт или диапазон портов назначения пакета). При использовании обоих этих параметров сначала необходимо указать параметр `sport`, затем — параметр `dport`. Например: `tcp sport 1024-65535 dport 1024`;
  - для протокола ICMP: `type` (тип пакета) и/или `code` (код пакета). При использовании обоих этих параметров сначала необходимо указать параметр `type`, затем — параметр `code`. Если параметр `type` не задан, то под условие будут попадать все ICMP-пакеты указанного типа, например: `icmp code 12`;
- номера протоколов. В этом случае для каждого протокола необходимо указать ключевое слово `proto` и его номер. Например, для протоколов TCP, UDP и ICMP: `proto 6 proto 17`

  Внимание! При использовании номеров протоколов задать дополнительные параметры протоколов невозможно.

- пользовательские группы протоколов, в том числе заданные по умолчанию (см. Пользовательские группы объектов по умолчанию на стр. 78), в виде:

  `service @<имя группы>`

  Например: `service @DNS`

Приложение

Приложение — параметр `dpiapp` транзитного фильтра открытой сети. При использовании в параметрах транзитного фильтра открытой сети приложения, анализируются все виды трафика, характерные для определенного сервиса. При этом приложение с заданным именем охватывает все источники, генерирующие этот тип трафика: программа, веб-сайт, мобильное приложение и так далее. Например:

- Запрещающий сетевой фильтр для приложения BitTorrent будет блокировать трафик как программы BitTorrent, так и других Torrent-клиентов.
- Запрещающий сетевой фильтр для приложения Skype будет блокировать трафик приложения Skype, а также браузерную версию Skype.

Список приложений приведен в разделе (см. Поддерживаемые приложения на стр. 251) настоящего документа.

Приложение не является обязательным параметром транзитного фильтра открытой сети.

Приложение описывается лексемой:

```
dpiapp <приложение>
```

Приложения необходимо указывать по их названиям (см. Поддерживаемые приложения на стр. 251). Вы можете указать несколько приложений в списке через запятую. При задании приложения, содержащего пробелы, его название необходимо заключить в двойные кавычки:

```
dpiapp "Google Mail",Skype,Facebook
```

Внимание! Для некоторых приложений существуют ограничения (см. Известные ограничения фильтрации по приложениям и прикладным протоколам на стр. 261).

Прикладной протокол

Прикладной протокол — параметр `dpiprotocol` транзитного фильтра открытой сети. При использовании в параметрах транзитного фильтра открытой сети прикладного протокола, в отличие от приложения (см. Приложение на стр. 86), анализируется только тип трафика, характерный для этого протокола. Например, запрещающий сетевой фильтр для протокола Skype будет блокировать трафик приложения Skype, так как оно использует этот протокол. В то же время этот сетевой фильтр не будет блокировать браузерную версию Skype, так как в этом случае используется прикладной протокол SSL.

Список прикладных протоколов приведен в разделе (см. Поддерживаемые прикладные протоколы на стр. 253) настоящего документа.

Прикладной протокол не является обязательным параметром транзитного фильтра открытой сети.

Прикладной протокол описывается лексемой:

```
dpiprotocol <прикладной протокол>
```

Прикладные протоколы необходимо указывать по их названиям (см. Поддерживаемые прикладные протоколы на стр. 253). Вы можете указать несколько прикладных протоколов в списке через запятую. Название протокола, содержащее пробелы, необходимо заключить в двойные кавычки:

```
dpiprotocol "Skype for Business",HTTP,SSL
```

Внимание! Если вы задали приложение (на стр. 86) в фильтре, то вы можете задать только те прикладные протоколы, которые относятся к этому приложению.

Группа приложений

Группа приложений — параметр `dpigroup` транзитного фильтра открытой сети. Приложения (см. Приложение на стр. 86) и прикладные протоколы (см. Прикладной протокол на стр. 87), используемые при анализе трафика методом DPI, логически объединены в 21 группу. В группу входят приложения и используемые ими прикладные протоколы схожего назначения.

Список поддерживаемых групп приложений приведен в разделе (см. Поддерживаемые группы приложений на стр. 255) настоящего документа.

Группа приложений не являются обязательным параметром транзитного фильтра открытой сети.

Группа приложений описывается лексемой:

```
dpigroup <группа приложений>
```

Внимание! В одном правиле указывать к группам приложений и прикладных протоколов `dpigroup` дополнительные приложения `dpiapp` и прикладные протоколы `dpiprotocol` запрещено.

Группы приложений необходимо указывать по их названиям (см. Поддерживаемые группы приложений на стр. 255). Вы можете указать несколько групп в списке через запятую. Название группы, содержащее пробелы, необходимо заключить в двойные кавычки:

```
dpigroup "Voice over IP","Remote Control",Streaming
```

Пользователь

Пользователь не является обязательным параметром транзитного фильтра открытой сети. Чтобы иметь возможность указывать пользователя при создании фильтра, настройте подключение к Active Directory (см. Настройка ViPNet xFirewall для взаимодействия с контроллером домена на стр. 125) или Captive portal (см. Настройка взаимодействия с LDAP-сервером на стр. 128).

Пользователь описывается лексемой:

```
dnuser <пользователь>
```

Пользователей необходимо указывать, используя их доменные имена (без указания имени самого домена) или имена, зарегистрированные на Captive portal. Вы можете указать несколько пользователей в списке через запятую. При задании имени пользователя, содержащего пробелы, его необходимо заключить в двойные кавычки:

```
dnuser ivanov_v,petrov_a, "petr ivanov"
```

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.

Расписание

Расписание задает время действия фильтра и не является обязательным параметром сетевого фильтра.

Примечание. Интервалы времени в расписании указываются для часового пояса (временной зоны) UTC, которое может отличаться от настроенного на ViPNet xFirewall. Если расписание не задано, то фильтр действует постоянно.

Расписание описывается одной из следующих лексем:

- `daily <чч:мм>-<чч:мм>` — фильтр действует ежедневно в течение заданного интервала времени. Время указывается в 24-часовом формате: `чч` — часы, `мм` — минуты.
- `weekly [mo] [tu] [we] [th] [fr] [sa] [su] [at <чч:мм>-<чч:мм>]` — фильтр действует еженедельно в заданные дни недели (`mo` — понедельник, `tu` — вторник, `we` — среда, `th` — четверг, `fr` — пятница, `sa` — суббота, `su` — воскресенье) и интервал времени.
- `calendar <дд.мм.гггг>-<дд.мм.гггг> [at <чч:мм>-<чч:мм>]` — фильтр действует в заданные даты и интервал времени. Дата указывается в следующем формате: `дд` — день, `мм` — месяц, `гггг` — год.
- `schedule <имя группы объектов>` — фильтр действует по расписанию, описанному группой объектов соответствующего типа.

Для задания расписания можно использовать соответствующие пользовательские группы, в том числе заданные по умолчанию (см. Пользовательские группы объектов по умолчанию на стр. 78).

Примечание. Расписание действует для новых сессий, поэтому в том случае, если сессия была установлена до временны*х* рамок расписания, то она будет работать до момента истечения. Например, в сетевом фильтре, разрешающем работу по протоколу RDP, задано расписание с 9:00 до 20:00. В этом случае пользователь, установивший RDP-сессию до 20:00, сможет работать в ней и после 20:00 до тех пор, пока она не будет прервана. После этого пользователь уже не сможет установить новую RDP-сессию.

Действие

Действие является обязательным параметром сетевого фильтра и определяет, что делает фильтр с IP-пакетом, соответствующим его условию.

Действие описывается одной из следующих лексем:

- `pass` — пропускать IP-пакет;
- `drop` — блокировать IP-пакет.

Просмотр сетевых фильтров

Вы можете просмотреть сетевые фильтры, заданные на узле. Для этого выполните одну из команд:

- для просмотра всех фильтров:

  ```
  hostname> firewall rules show
  ```

  Примечание. В результате выполнения команды `firewall rules show` отображаются не только сетевые фильтры, заданные на узле, но и правила трансляции адресов (см. Просмотр, изменение, удаление правил трансляции адресов на стр. 103).

- для просмотра сетевых фильтров определенного типа (см. Создание сетевого фильтра на стр. 81):

  ```
  hostname> firewall <тип> show
  ```

  Например, для просмотра локальных фильтров открытой сети:

  ```
  hostname> firewall local show
  ```

- для просмотра сетевых фильтров с конкретными параметрами:

  ```
  hostname> firewall <тип> show <параметр>,
  ```

  указав в качестве параметра порядковый номер, имя, адрес отправителя (на стр. 83), адрес получателя (на стр. 85), протокол (см. Транспортный протокол на стр. 86) или действие (на стр. 89) фильтра. При необходимости вы можете указать несколько параметров.

  Например, для просмотра локального фильтра открытой сети с несколькими адресами отправителей или одним адресом получателя выполните команду:

  ```
  hostname> firewall local show src 192.168.30.2,192.169.1.1,mydomain.ru dst 192.168.0.
  ```

- для просмотра сетевых фильтров и правил трансляции адресов с выборкой по имени:

  ```
  hostname> firewall rules show rule <имя>
  ```

  указав имя сетевого фильтра или правила трансляции адресов.

- для просмотра транзитных фильтров открытой сети по параметрам приложения (см. Приложение на стр. 86), прикладного протокола (см. Прикладной протокол на стр. 87), группы приложений (см. Группа приложений на стр. 88) и пользователя (см. Пользователь на стр. 88):

  ```
  hostname> firewall forward show [<номер>] [rule <имя>] src <адрес отправителя> dst
  <адрес получателя> [dpiapp <приложение>] [dpiprotocol <прикладной протокол>]
  [dpigroup <группа приложений> [dnuser <пользователь>]
  ```

Внимание! Поиск сетевых фильтров для отображения осуществляется по строгому совпадению с указанными параметрами. Например:

если указан параметр `src 192.168.1.10`, отобразится фильтр, содержащий адрес `src 1.1.1.1,192.168.1.10,2.2.2.2`, но не отобразится фильтр, содержащий адрес `src 192.168.1.10-192.168.1.11`.

если указан параметр `rule Name`, отобразится фильтр с именем `Name`, но не отобразится фильтр с именем `Name1`.

В результате выполнения команды будет отображена таблица, содержащая те или иные сетевые фильтры. Пример таблицы локальных фильтров открытой сети представлен на рисунке ниже.

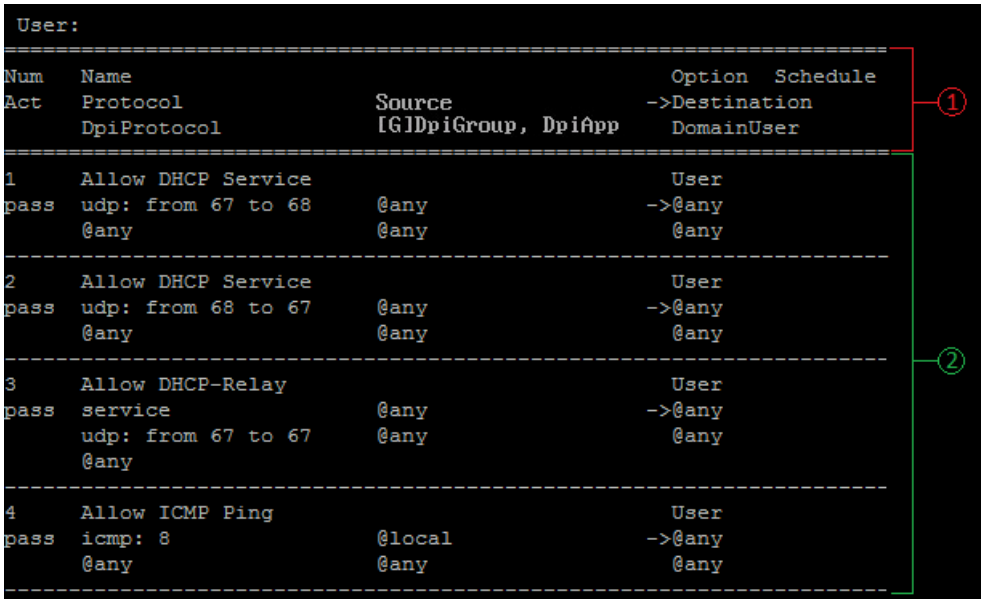


Рисунок 7. Просмотр локальных фильтров открытой сети

Цифрами на рисунке обозначены:

1 Заголовок таблицы, где:

- `Num` — порядковый номер фильтра, определяющий его приоритет.
- `Name` — имя фильтра.
- `Option` — категория сетевого фильтра: для фильтров из программы ViPNet Policy Manager — `Policy`, для предустановленных фильтров и фильтров пользователя — `User`, для фильтров системы защиты от сбоев — `Failover`.
- `Schedule` — расписание применения фильтра.
- `Act` — действие фильтра.
- `Protocol` — транспортный протокол.
- `Source` — адрес отправителя.
- `Destination` — адрес получателя.
- `DpiApp` — приложение.

- `DpiProrocol` — прикладной протокол.
- `[G] DpiGroup` — группа приложений.
- `DomainUser` — пользователь сети.

2 Параметры фильтров, включающие:

- строку с порядковым номером, именем и категорией фильтра;
- одну или несколько строк, содержащих адрес отправителя, адрес получателя, транспортный и прикладной протоколы, приложение, пользователя сети, расписание и действие фильтра.

Изменение сетевого фильтра

Вы можете изменить ранее созданный сетевой фильтр, добавив в него адрес отправителя, адрес получателя, транспортный протокол или расписание либо изменив его приоритет (порядковый номер в таблице фильтров соответствующего типа). Для транзитных фильтров открытой сети поддерживается задание нескольких значений параметров приложения, прикладного протокола, группы приложений и пользователя (параметры `dpiapp`, `dpiprotocol`, `dpigroup`, `dnuser`).

Чтобы внести изменения в ранее созданный фильтр выполните команду:

```
hostname# firewall <тип> change append [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> [<транспортный протокол>] [dpiprotocol <прикладной протокол>] [dpiapp <приложение>] [dpigroup <группа приложений>] [dnuser <пользователь>] [<расписание>],
```

указав в качестве параметров:

- адрес отправителя (на стр. 83);
- адрес получателя (на стр. 85);
- транспортный протокол (на стр. 86);
- прикладной протокол (на стр. 87);
- приложение (на стр. 86);
- группу приложений (см. Группа приложений на стр. 88);
- пользователя (см. Пользователь на стр. 88);
- расписание (на стр. 89).

При необходимости вы можете указать несколько параметров.

При изменении транзитных фильтров открытой сети вы можете использовать несколько значений параметров `<прикладной протокол>`, `<приложение>`, `<пользователь>` и `<группа приложений>`. Значения в списке разделяются запятой. Значение, содержащее пробелы, заключается в двойные кавычки.

Чтобы изменить транзитный фильтр открытой сети с несколькими значениями параметров, используйте в команде `firewall forward change append` следующие лексемы:

- `dpiprotocol <прикладной протокол 1>,<прикладной протокол N>`

- `dpiapp <приложение 1>,<приложение N>`
- `dnuser <пользователь 1>,<пользователь N>`
- `dpigroup <группа приложений 1>,<группа приложений N>`

Примечание. Если при вводе команды была допущена синтаксическая ошибка, то в результате выполнения такой команды появится сообщение с указанием слова, содержащего ошибку. Исправьте ошибку и выполните команду еще раз.

Чтобы изменить приоритет фильтра, в командном интерпретаторе выполните команду:

```
hostname# firewall <тип> move rule <текущий номер> to <новый номер>
```

В результате приоритет фильтра и, соответственно, его порядковый номер в таблице будут изменены. При этом номера фильтров, следующих за этим фильтром, автоматически увеличатся на единицу, то есть их приоритет понизится.

Примеры добавления условия в сетевой фильтр

Для добавления в фильтр

```
1 RuleName1 src 192.168.1.1,2.2.2.2/24 dst @local drop
```

нового адреса отправителя выполните команду:

```
hostname# firewall local change append 1 src 192.168.3.3
```

В результате фильтр будет изменен следующим образом:

```
1 RuleName1 src 192.168.1.1,2.2.2.2/24,192.168.3.3 dst @local drop
```

Чтобы добавить к транзитному фильтру открытой сети с номером 333 запрет Flash трафика, ресурса Вконтакте и пользователя MakarovTP и DeryuginAA, выполните команду:

```
hostname# firewall forward change append 333 dpiapp VK dpiprotocol Flash dnuser
MakarovTP,DeryuginAA
```

Удаление сетевого фильтра

Чтобы удалить ненужный сетевой фильтр, выполните следующие действия:

- Если вы знаете порядковый номер фильтра, который нужно удалить, выполните команду:

  ```
  hostname# firewall <тип> delete <номер>
  ```

  Например, для локального фильтра открытой сети с порядковым номером 1:

  ```
  hostname# firewall local delete 1
  ```

- Если вы не знаете номер фильтра, который нужно удалить, то найдите фильтр по известным вам параметрам, а затем удалите его. Для этого:
  - Выполните команду:

```
hostname# firewall <тип> delete <параметр>,
```

указав в качестве параметра имя, адрес отправителя (на стр. 83), адрес получателя (на стр. 85), протокол (см. Транспортный протокол на стр. 86) или действие (на стр. 89) фильтра. При необходимости вы можете указать несколько параметров.

Например, для локальных фильтров открытой сети с адресом отправителя 192.168.20.2:

```
hostname# firewall local delete src 192.168.20.2
```

В результате будет отображен список сетевых фильтров, которые содержат указанные параметры.

Внимание! Поиск сетевых фильтров для отображения осуществляется по строгому совпадению с указанными параметрами.

- Если найдено несколько фильтров:
  - введите номер фильтра (столбец `Num`), который надо удалить, и нажатием клавишу **Enter**;
  - для удаления всех найденных фильтров введите символ `a` и нажатием клавишу **Enter**.
- Если найден один фильтр:
  - подтвердите его удаление вводом символа `y` и нажатием клавиши **Enter**;
  - отмените его удаление вводом символа `n` и нажатием клавиши **Enter**.

В результате сетевой фильтр будет удален. При этом номера фильтров, имеющих более низкий приоритет по сравнению с удаленным фильтром, автоматически уменьшатся на единицу.

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 с именем `ivanov` в локальной сети, защищенной ViPNet xFirewall таким образом, чтобы:

- разрешить отправку электронных писем только с помощью корпоративного почтового сервера 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. Создайте транзитный фильтр открытой сети, который будет блокировать отправку писем по протоколам SMTP и IMAP, с помощью команды:

   ```
   hostname# firewall forward add src @any dst @any dpiprotocol smtp,imap dnuser ivanov drop
   ```

2. Создайте транзитный фильтр открытой сети, который будет разрешать отправку писем по протоколу Microsoft Exchange, с помощью команды:

   ```
   hostname# firewall forward add src @any dst @any dpiprotocol "Microsoft Exchange" dnuser ivanov pass
   ```

3. Создайте транзитный фильтр открытой сети, который будет блокировать трафик приложений социальных сетей, с помощью команды:

   ```
   hostname# firewall forward add src @any dst @any dpiapp Facebook dnuser ivanov drop
   ```

4. Создайте транзитный фильтр открытой сети, который будет блокировать трафик приложений облачных файловых сервисов, с помощью команды:

   ```
   hostname# firewall forward add src @any dst @any dpiapp Dropbox,"Google Drive" dnuser ivanov drop
   ```

После выполнения действий для пользователя локальной сети с именем `ivanov` будет выполняться фильтрация трафика согласно условиям.

Настройка фильтрации трафика для работы Skype

Чтобы разрешить или запретить использование приложения Skype на компьютерах локальной сети, защищенной ViPNet xFirewall, выполните одно из следующих действий:

- создайте разрешающие фильтры для приложений Skype, Skype for business, Windows Azure и Microsoft Services с помощью команд:

```
hostname# firewall forward add src @any dst @any dpiapp skype pass
hostname# firewall forward add src @any dst @any dpiapp "skype for business" pass
hostname# firewall forward add src @any dst @any dpiapp "Windows Azure" pass
hostname# firewall forward add src @any dst @any dpiapp "Microsoft Services" pass
```

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

- создайте запрещающие фильтры для приложений Skype и Skype for business с помощью команд:

```
hostname# firewall forward add src @any dst @any dpiapp skype drop
hostname# firewall forward add src @any dst @any dpiapp "skype for business" drop
```

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 создания запрещающих сетевых фильтров выполните команду:

```
hostname# firewall forward add src @any dst @any dpiprotocol bittorrent,teredo drop
```

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

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. 99), 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. В результате локальные сети, использующие частные адреса, получают доступ к ресурсам Интернета.

- Трансляция адреса назначения (на стр. 100), 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 (см. Создание правила трансляции адресов на стр. 101). В ViPNet xFirewall должны быть задействованы минимум два сетевых интерфейса:

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

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 8. 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.

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.

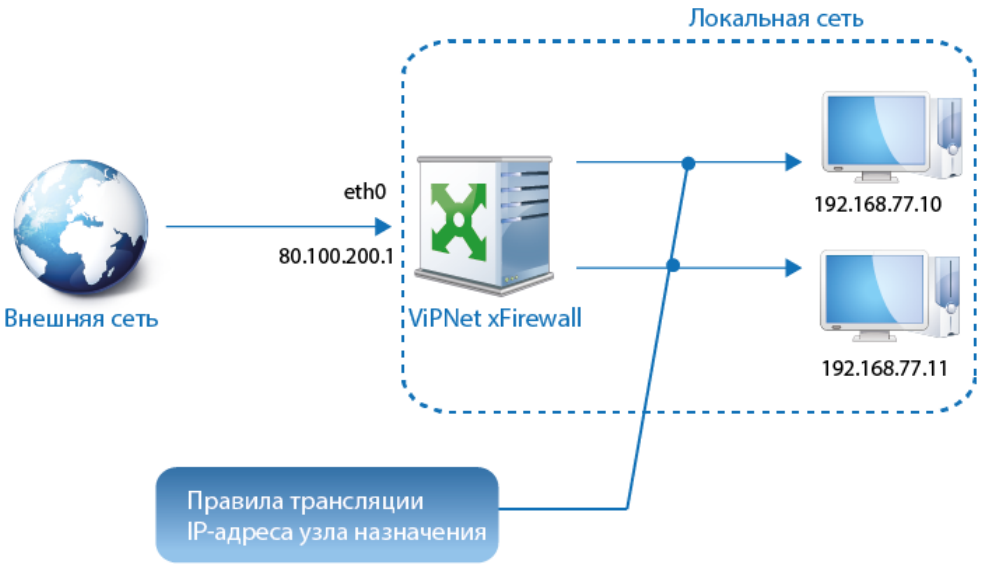


Рисунок 9. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

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. 99).

Создание правила трансляции адресов

Правила трансляции адресов хранятся в специальной таблице (см. Просмотр, изменение, удаление правил трансляции адресов на стр. 103).

Примечание. Правила трансляции IP-адресов работают только при наличии транзитных фильтров открытой сети (см. Создание сетевого фильтра на стр. 81), пропускающих трафик от узлов, к которым будет применяться трансляция адресов.

Чтобы создать правило трансляции адресов, выполните команду:

`hostname# firewall nat add [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> [<транспортный протокол>] [<расписание>] change {src <адрес отправителя> | dst <адрес получателя>}`, указав следующие параметры:

- Порядковый номер правила в таблице, определяющий его приоритет. Чем меньше порядковый номер правила, тем выше его приоритет (наиболее приоритетное правило имеет номер 1). При создании правила с порядковым номером, меньшим максимального номера в таблице правил, номера правил, следующих за этим правилом, автоматически увеличиваются на единицу (то есть их приоритет понижается).
- Имя правила. Если имя состоит из нескольких слов, разделенных пробелом, заключите его в кавычки (например, `rule "number one"`).

Примечание. При создании правила трансляции адресов можно не указывать его номер. В этом случае правилу будет присвоен номер, следующий за номером последнего правила в таблице, и оно будет иметь самый низкий приоритет.

Имя правила можно указывать без слова `rule`. Кроме этого, имя правила можно не указывать. В этом случае будет создано правило без имени.

- Параметры, определяющие процесс обработки трафика правилом:
  - адрес отправителя (на стр. 83) и адрес получателя (на стр. 85) являются обязательными параметрами правила и задаются в виде IP-адреса или доменного имени узла, диапазона

IP-адресов узлов, списка IP-адресов или доменных имен узлов, маски адресов подсети, доменного имени сети, одной или нескольких пользовательских групп IP-узлов;

- Транспортный протокол (на стр. 86) и расписание (на стр. 89) являются необязательными параметрами правила и задаются так же, как для сетевых фильтров;
- действие правила в виде одной из лексем:
  - для трансляции адреса источника: `change src {<адрес отправителя> | auto}`,

    указав внешний адрес маршрутизатора, на который будет заменяться адрес отправителя пакетов либо параметр `auto`, чтобы адрес отправителя автоматически заменялся на публичный адрес внешнего сетевого интерфейса маршрутизатора.
  - для трансляции адреса назначения: `change dst <адрес получателя>:[<порт>]`,

указав адрес и порт узла локальной сети, которому будут перенаправляться пакеты. Если вы используете параметр <порт>, указание транспортного протокола TCP или UDP обязательно.

Примечание. Если при вводе команды была допущена синтаксическая ошибка, то в результате выполнения такой команды появится сообщение с указанием слова, содержащего ошибку. Исправьте ошибку и выполните команду еще раз.

В результате будет создано правило трансляции адресов. Вы можете просмотреть, изменить или удалить его (см. Просмотр, изменение, удаление правил трансляции адресов на стр. 103).

Примечание. Созданное правило трансляции адресов будет работать для новых соединений. Для уже установленных соединений правило будет работать после истечения времени жизни соединения. Чтобы принудительно применить правило трансляции адресов для всех соединений, поочередно выполните команды:

```
hostname# vpn stop
hostname# vpn start
```

Примеры создания правил трансляции адресов

Чтобы при отправке пакета узлом с адресом 10.0.0.1 внешнему узлу с адресом 192.168.20.1 частный адрес отправителя пакета заменялся на публичный адрес внешнего сетевого интерфейса маршрутизатора, создайте правило трансляции адреса источника с помощью команды:

```
hostname# firewall nat add src 10.0.0.1 dst 192.168.20.1 change src auto
```

Чтобы при отправке пакета внешним узлом с адресом mydomain.ru узлу с адресом 192.168.20.1 маршрутизатор подменял адрес получателя (публичный IP-адрес маршрутизатора) на локальный адрес, создайте правило трансляции адреса назначения с помощью команды:

```
hostname# firewall nat add src mydomain.ru dst 192.168.20.1 change dst 10.0.0.7
```

Чтобы при отправке пакета внешним узлом с адресом mydomain.ru узлу с адресом 192.168.20.1 по протоколу TCP/IP через порт 8080 маршрутизатор подменял адрес получателя (публичный IP-адрес маршрутизатора) на локальный адрес, создайте правило трансляции адреса назначения с помощью команды:

```
hostname# firewall nat add src mydomain.ru dst 192.168.20.1 tcp dport 8080 change dst
10.0.0.7:8080
```

Чтобы одновременно транслировать адреса источника и назначения, например, от адреса 10.0.2.15 до адреса 192.168.1.2, выполните команду:

```
firewall nat add src 10.0.2.15 dst 192.168.1.2 change src auto dst 10.0.2.15
```

Просмотр, изменение, удаление правил трансляции адресов

Вы можете просмотреть, изменить или удалить правила трансляции адресов, заданные на узле.

Чтобы просмотреть правила, выполните одну из команд:

- для просмотра всех правил:

  ```
  hostname> firewall nat show
  ```

- для просмотра правил с конкретными параметрами:

  ```
  hostname> firewall nat show <параметр>,
  ```

  указав в качестве параметра порядковый номер, имя, адрес отправителя, адрес получателя, протокол или действие правила (см. Создание правила трансляции адресов на стр. 101). При необходимости вы можете указать несколько параметров.

Внимание! Поиск правил трансляции адресов для отображения осуществляется по строгому совпадению с указанными параметрами.

В результате выполнения команды будет отображена таблица, содержащая те или иные правила трансляции адресов. Пример такой таблицы показан на рисунке ниже.

```
 User:
=============================================================================
Num    Name                                          Option  Schedule
Act    Protocol                Source               ->Destination
       DpiProtocol             [G]DpiGroup, DpiApp   DomainUser
=============================================================================
1      HTTP-Proxy auto                               User
NAT    tcp: to 80, tcp: to 21 @HttpProxyUsers       ->@InternetIP
       Change DstPort: 1024    @any                  Change: 192.168.203.168
       @any                                          @any
-----------------------------------------------------------------------------
```

Рисунок 10. Просмотр правил трансляции адресов

Таблица содержит следующие столбцы:

- `Num` — порядковый номер правила, определяющий его приоритет.
- `Name` — имя правила.

- `Option` — категория правила: для правил из программы ViPNet Policy Manager — `Policy`, для правил пользователя — `User`.
- `Schedule` — расписание применения правила.
- `Act` — действие правила (`NAT`).
- `Protocol` — протокол.
- `Source` — адрес источника до или после трансляции.
- `Destination` — адрес назначения до или после трансляции.
- `DpiProrocol` — прикладной протокол.
- `DpiApp` — приложение.
- `DomainUser` — пользователь сети.

Изменение и удаление правил трансляции адресов выполняется аналогично изменению и удалению сетевых фильтров с помощью команд:

```
hostname# firewall nat change append <номер> <параметр>
```

```
hostname# firewall nat delete <параметр>
```

Подробнее см. в разделах Изменение сетевого фильтра (на стр. 92) и Удаление сетевого фильтра.

Примеры использования правил трансляции адресов

Организация доступа пользователей к сети Интернет

С помощью ViPNet xFirewall можно организовать доступ пользователей, имеющих частные адреса, 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, которая заключается в преобразовании частных адресов локальной сети в один публичный адрес.

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

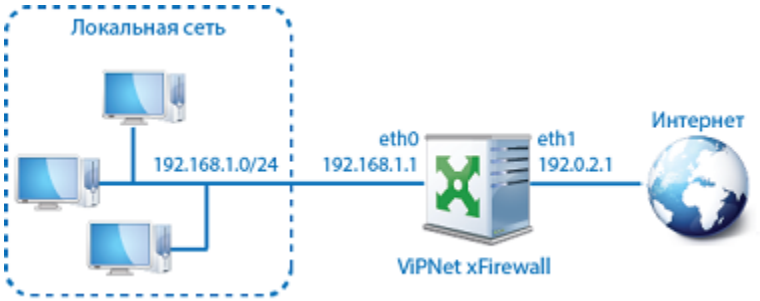


Рисунок 11. Организация доступа пользователей к Интернету с помощью ViPNet xFirewall

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. Перейдите в режим администратора с помощью команды `enable`.
2. Создайте транзитный фильтр открытой сети, разрешающий соединения из внутреннего сегмента с любыми IP-адресами:

   ```
   hostname# firewall forward add src 192.168.1.0/24 dst @any pass
   ```

3. Создайте правило трансляции адресов для организации доступа в Интернет из внутреннего сегмента:

   ```
   hostname# firewall nat add src 192.168.1.0/24 dst @InternetIP change src 192.0.2.1
   ```

В результате пользователи локальной сети будут иметь доступ в Интернет, и при этом их компьютеры будут защищены от атак из Интернета.

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, 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.

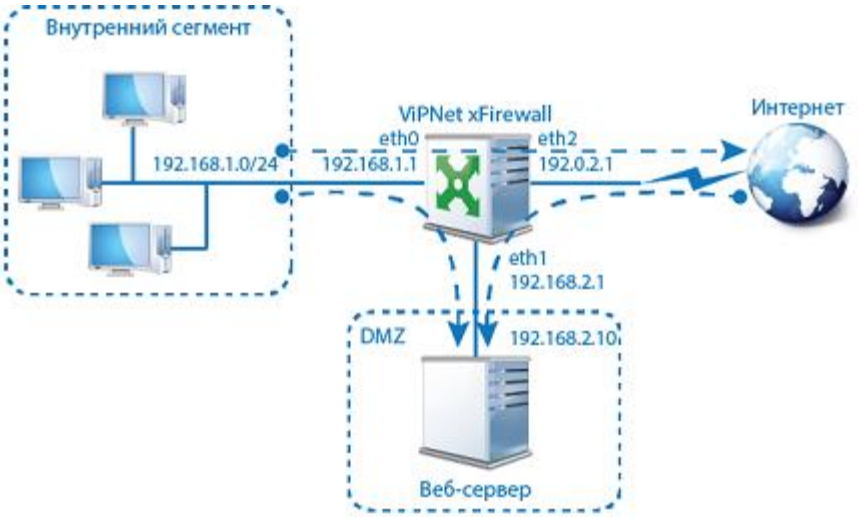


Рисунок 12. Использование ViPNet xFirewall для размещения общедоступного сервера в DMZ

Два интерфейса ViPNet xFirewall (eth0 и eth1) имеют частные IP-адреса и подключены к сегментам локальной сети, интерфейс eth2 имеет публичный IP-адрес 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. Перейдите в режим администратора с помощью команды `enable`.
2. Создайте транзитный фильтр открытой сети, разрешающий соединения из внутреннего сегмента с любыми IP-адресами:

   ```
   hostname# firewall forward add src 192.168.1.0/24 dst @any pass
   ```

3. Создайте транзитный фильтр открытой сети, разрешающий соединения внешних пользователей с веб-сервером:

   ```
   hostname# firewall forward add src @InternetIP dst 192.168.2.10 dpiprotocol http pass
   ```

4. Создайте следующие правила трансляции адресов:
   - правило для организации доступа в Интернет из внутреннего сегмента:

     ```
     hostname# firewall nat add src 192.168.1.0/24 dst @InternetIP change src 192.0.2.1
     ```

- правило для организации доступа к веб-серверу из Интернета:

```
hostname# firewall nat add src @InternetIP dst 192.0.2.1 tcp dport 80 change dst
192.168.2.10
```

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 трансляции адресов для прикладных протоколов

О прикладных протоколах

Прикладные протоколы обеспечивают работу пользовательских сетевых сервисов, например, IP-телефонии, FTP-службы. При использовании данных служб IP-адреса часто передаются в теле IP-пакета. Эта особенность может повлиять на доступность сервисов в защищенной сети с трансляцией адресов. Кроме того, некоторые протоколы, помимо управляющего соединения, открывают для передачи данных дополнительные соединения на случайно выбранный порт. Поскольку номер порта заранее неизвестен, то для IP-пакетов невозможно создать разрешающий фильтр, следовательно, соединение будет заблокировано.

Решить перечисленные проблемы позволяет функция обработки прикладных протоколов, которая обеспечивает:

- Подмену IP-адреса сетевого узла локальной сети на транслируемый адрес при статической или динамической трансляции IP-адресов (только для протокола FTP).
- Включение сетевого фильтра, пропускающего IP-пакеты, для дополнительного соединения на случайно выбранный порт, который используется прикладным протоколом. При этом для установления управляющего соединения с открытыми узлами на узле необходимо задать соответствующие фильтры открытой сети.

Вы можете использовать эту функцию для всех видов трафика.

Список поддерживаемых прикладных протоколов см. в разделе Поддерживаемые прикладные протоколы (на стр. 110).

Следует учитывать, что обработка прикладных протоколов не предполагает автоматического разрешения на установление управляющего соединения с открытыми узлами. Установление управляющего соединения с открытыми узлами выполняется в соответствии с фильтрами трафика.

Обработка протокола FTP

При передаче файлов между клиентом и сервером по протоколу FTP устанавливается как минимум два TCP-соединения:

- для отправки команд на сервер и получения ответов от него (управляющее TCP-соединение);
- для передачи данных (дополнительное TCP-соединение).

Установление TCP-соединений по протоколу FTP происходит в следующем порядке:

1 Клиент создает управляющее TCP-соединение с сервером со своего порта из диапазона 1024-65535 на 21-й порт сервера.

2. В зависимости от выбранного режима передачи данных, клиент отправляет по управляющему соединению следующую информацию:
   - номер порта, открытого клиентом для получения данных с сервера (активный режим передачи данных);
   - запрос на номер порта сервера, к которому будет подключаться клиент (пассивный режим передачи данных).
3. Далее, в зависимости от используемого режима передачи данных, соединение для передачи данных устанавливается одним из двух способов:
   - в активном режиме передачи данных — сервер создает дополнительное соединение для передачи данных на указанный клиентом порт;
   - в пассивном режиме передачи данных — сервер по управляющему соединению передает клиенту номер порта, к которому клиент создает дополнительное соединение для передачи данных.

Таким образом, в активном режиме соединение для передачи данных создает сервер, а в пассивном — клиент.

Для установления управляющего и дополнительного соединений в активном или пассивном режиме работы протокола FTP выполните следующие настройки:

- Создайте фильтр открытой сети (см. Создание сетевого фильтра на стр. 81), разрешающий исходящее TCP-соединение на 21-й порт FTP-сервера.
- Для разрешения дополнительного соединения в активном режиме работы включите обработку протокола FTP (см. Настройка параметров трансляции адресов для прикладных протоколов на стр. 110), которая добавляет необходимый фильтр трафика.
- Для разрешения дополнительного соединения в пассивном режиме работы настройки не требуются.

Обработка протокола SIP

Протокол SIP предназначен для организации сеансов связи (мультимедийных конференций, телефонных соединений) и распределения мультимедийной информации.

SIP-клиент отправляет запрос (например, приглашение для начала сеанса связи, подтверждение приема ответа на запрос, завершение сеанса связи) другому SIP-клиенту с указанием его SIP-адреса. В зависимости от способа установления соединения запрос направляется второму клиенту либо напрямую, либо с участием прокси-сервера SIP, либо с участием сервера переадресации. Вызываемый клиент передает вызывающему клиенту ответ на запрос (например, информацию об успешной обработке запроса, отклонении вызова, ошибке при обработке запроса).

Для организации сеанса связи протокол SIP регламентирует установление соединений TCP и UDP через порт 5060.

Чтобы установить сеанс связи между SIP-клиентами, убедитесь, что включена обработка протокола SIP (см. Настройка параметров трансляции адресов для прикладных протоколов на стр. 110), и

создайте фильтр открытой сети, разрешающий входящее и исходящее соединение по протоколам TCP и UDP на порт 5060.

Примечание. Некоторые SIP-клиенты, например SIP-клиент компании ZoiPer, могут устанавливать соединения TCP и UDP не через порт 5060, а через динамический порт, выбранный произвольно из определенного диапазона. Поэтому возможность использования динамических портов необходимо отключить в настройках SIP-клиента.

Между SIP-клиентами нельзя использовать статическую или динамическую трансляцию адресов.

Поддерживаемые прикладные протоколы

ViPNet xFirewall поддерживает следующие прикладные протоколы:

- FTP — для передачи файлов между FTP-клиентом и FTP-сервером.

  Команды FTP-протокола EPRT и EPSV, используемые некоторыми FTP-клиентами, не поддерживаются ViPNet xFirewall.

- H.323 — для передачи мультимедийных данных в IP-сетях (IP-телефония, видео- и аудиоконференции). Обработка протокола не поддерживается при использовании трансляции адресов (NAT).

  SCCP — для передачи сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты Cisco Unity и Cisco CallManager. Обработка протокола не поддерживается при использовании трансляции адресов (NAT).

- SIP — для установления соединений, включающих обмен мультимедийными данными между клиентами. Обработка протокола при использовании трансляции адресов (NAT) поддерживается в том случае, если в качестве транспортного протокола используется UDP и размер UDP-пакетов не превышает значение MTU.

Список поддерживаемых прикладных протоколов изменить нельзя.

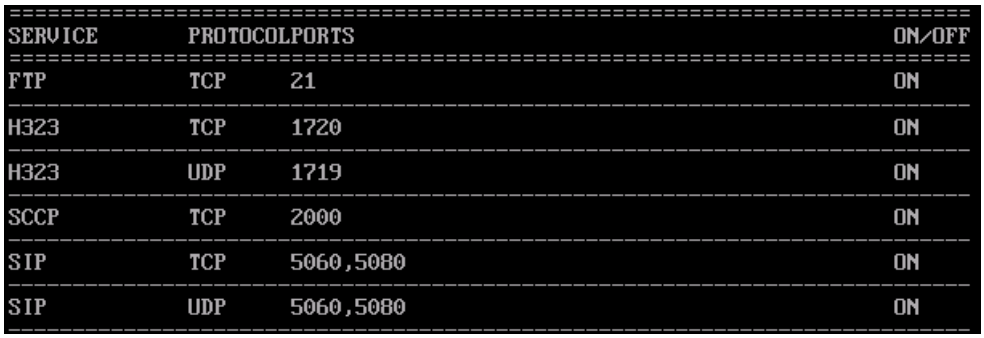
Настройка параметров трансляции адресов для прикладных протоколов

По умолчанию в ViPNet xFirewall включена трансляция адресов для всех поддерживаемых ViPNet xFirewall прикладных протоколов (см. Поддерживаемые прикладные протоколы на стр. 110).

Чтобы просмотреть текущие настройки обработки прикладных протоколов, выполните команду:

```
hostname> alg show
```

В результате отобразится таблица, показанная ниже.



SERVICE	PROTOCOL	PORTS	ON/OFF
FTP	TCP	21	ON
H323	TCP	1720	ON
H323	UDP	1719	ON
SCCP	TCP	2000	ON
SIP	TCP	5060,5080	ON
SIP	UDP	5060,5080	ON

Рисунок 13. Просмотр параметров прикладных протоколов

Таблица содержит следующие столбцы:

- `Service` — обрабатываемый прикладной протокол.
- `Protocol` — сетевой протокол для обработки.
- `Ports` — порты для обработки.
- `On/Off` — состояние обработки: `on` — включена, `off` — выключена.

Чтобы настроить и включить обработку прикладного протокола, выполните команду:

`hostname# alg module <прикладной протокол> process <сетевой протокол> <порты> on`, указав:

- один из поддерживаемых прикладных протоколов: `ftp`, `h323`, `sccp` или `sip`;
- один из транспортных протоколов для обработки выбранного прикладного протокола: `tcp` или `udp`;

Примечание. Не поддерживается обработка прикладных протоколов, работающих через нестандартный для них транспортный протокол.

- порт, диапазон портов либо список портов или диапазонов портов, разделенных запятой.

Внимание! Нулевое значение порта означает выключение обработки прикладного протокола для указанного сетевого протокола.

В результате на узле будет включена обработка прикладного протокола, и вы сможете работать с соответствующими приложениями.

Примечание. Выбранные параметры обработки прикладных протоколов должны соответствовать параметрам, указанным в настройках соответствующих приложений (FTP-клиент, SIP-клиент и так далее).

Чтобы изменить ранее выбранные сетевой протокол или порты для обработки какого-либо прикладного протокола, необходимо настроить и включить обработку этого прикладного протокола заново. Например, если кроме стандартных портов для обработки данных,

передаваемых по протоколу SIP, используются еще несколько портов для протокола UDP, то их можно добавить с помощью команды:

```
hostname# alg module sip process udp 10000,21-65 on
```

Чтобы выключить обработку прикладного протокола:

- для одного сетевого протокола — задайте для этого сетевого протокола порт, равный нулю, и включите обработку. Например:

  ```
  hostname# alg module sip process tcp 0 on
  ```

- для всех сетевых протоколов — выполните команду:

  ```
  hostname# alg module <прикладной протокол> process off
  ```

Внимание! При выключении обработки прикладного протокола работа соответствующих сетевых сервисов на сетевом узле будет невозможна.

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 14. 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. 243).

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. 243).

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 (на стр. 116) и Настройка антивирусной проверки (на стр. 122).

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. 275), 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.

Для настройки основных параметров прокси-сервера выполните следующие действия:

1 Завершите работу прокси-сервера, если он запущен, с помощью команды:

```
hostname# service http-proxy stop
```

Внимание! На запущенном прокси-сервере нельзя выполнить настройку параметров.

2 Укажите IP-адреса и порты, на которых прокси-сервер будет принимать запросы от пользователей:

- Чтобы добавить IP-адрес и порт, выполните команду:

  ```
  hostname# service http-proxy listen-address add <интерфейс> <порт>
  ```

- Чтобы просмотреть список заданных IP-адресов и портов, выполните команду:

  ```
  hostname> service http-proxy listen-address list
  ```

- Чтобы удалить IP-адрес и порт, выполните команду:

  ```
  hostname# service http-proxy listen-address delete <интерфейс> <порт>
  ```

Внимание! Для приема запросов рекомендуется использовать сетевые интерфейсы со статическими IP-адресами. При изменении IP-адресов сетевых интерфейсов необходимо завершить работу службы прокси-сервера, в качестве адресов для подключения указать текущие IP-адреса, затем снова запустить прокси-сервер.

3 Укажите внешний IP-адрес ViPNet xFirewall, который используется для подключения к Интернету. Для этого выполните команду:

```
hostname# service http-proxy external-address set <интерфейс>
```

Чтобы просмотреть заданный внешний IP-адрес, выполните команду:

```
hostname> service http-proxy external-address show
```

4 Если требуется, задайте размер кэша прокси-сервера с помощью команды:

```
hostname# service http-proxy cache <размер>
```

Размер кэша указывается в мегабайтах, значение по умолчанию 256 Мбайт. Кэш используется для хранения копии данных, к которым часто обращаются пользователи.

5 Добавьте сетевые фильтры и правила трансляции, необходимые для работы прокси-сервера, с помощью команды:

```
hostname# service http-proxy fw-rules apply
```

При выполнении команды все необходимые сетевые фильтры и правила трансляции будут созданы автоматически.

При выполнении команды также автоматически создается пользовательская группа объектов `HttpProxyUsers` (см. Пользовательские группы объектов по умолчанию на стр. 78), содержащая IP-адреса локальных сетей, для которых разрешено использование

прокси-сервера. 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).

Чтобы добавить или удалить IP-адреса из списка локальных сетей, которым разрешено использовать прокси-сервер, измените группу объектов `HttpProxyUsers`. Изменение пользовательских групп объектов возможно только с помощью веб-интерфейса. Подробнее см. документ «ViPNet xFirewall. Настройка с помощью веб-интерфейса», раздел «Создание и изменение группы объектов».

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 сетевой фильтр с помощью следующей команды:

```
hostname# firewall local add src @local dst @InternetIP tcp dport 80 tcp dport 21 tcp dport 443 pass
```

6 Чтобы включить или выключить автоматический запуск прокси-сервера при загрузке ViPNet xFirewall, выполните команду:

```
hostname# service http-proxy mode {on | off}
```

7 Чтобы запустить службу прокси-сервера, выполните команду:

```
hostname# service http-proxy start
```

Внимание! Для корректной работы прокси-сервера перед его запуском необходимо настроить и включить DNS-сервер.

Чтобы завершить работу службы прокси-сервера, выполните команду:

```
hostname# service http-proxy stop
```

Настройка фильтрации содержимого трафика

Прокси-сервер ViPNet xFirewall имеет функцию проверки HTTP-трафика по его содержимому. С помощью правил фильтрации содержимого трафика вы можете настроить блокировку трафика по MIME-типу (см. глоссарий, стр. 272) файла или приложения, а также по типу HTTP-метода запроса к удаленному ресурсу.

Примечание. При блокировке трафика ViPNet xFirewall в браузере отображается веб-страница с соответствующим сообщением. При этом время блокировки отображается на веб-странице в формате UTC+0.

Фильтрация содержимого трафика включается автоматически при запуске прокси-сервера. Для настройки параметров этой функции выполните следующие действия:

1 Если прокси-сервер запущен, завершите его работу с помощью команды:

```
hostname# service http-proxy stop
```

Внимание! Если прокси-сервер запущен, настроить его параметры невозможно.

2 Чтобы включить или выключить фильтрацию содержимого трафика, выполните команду:

```
hostname# service http-proxy content-filter mode {on | off}
```

3 Чтобы задать действие правила по умолчанию для запросов к HTTP-ресурсам, выполните команду:

```
hostname# service http-proxy content-filter default-request-action {pass | drop},
```

указав следующие параметры:

- `pass` — правило по умолчанию пропускает запросы к HTTP-серверам, не подпадающие под действие других правил;
- `drop` — правило по умолчанию блокирует запросы к HTTP-серверам, не подпадающие под действие других правил.

4 Чтобы задать действие правила по умолчанию для ответов от HTTP-ресурсов, выполните команду:

```
hostname# service http-proxy content-filter default-reply-action {pass | drop},
```

указав следующие параметры:

- `pass` — правило по умолчанию пропускает ответы от HTTP-серверов, не подпадающие под действие других правил;
- `drop` — правило по умолчанию блокирует ответы от HTTP-серверов, не подпадающие под действие других правил.

5 Чтобы добавить правило фильтрации содержимого трафика, выполните команду:

```
hostname# service http-proxy content-filter add [num <номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> {[command <HTTP-метод>] | [mime-type <тип содержимого>]} <действие>,
```

указав следующие параметры:

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет. Чем меньше порядковый номер правила, тем выше его приоритет (наиболее приоритетное правило имеет номер 1). Если указанный номер правила меньше последнего номера в таблице, нумерация правил, следующих после нового правила, будет автоматически изменена (их номера будут увеличены на 1). Например: последний номер правила в таблице — 5, вы добавили правило с номером 3. Правило добавится с указанным номером, при этом правило с номером 3, которое было создано ранее добавленного вами, получит номер 4. Правила с номерами 4 и 5, соответственно, получат номер 5 и 6;
- `<имя>` — имя правила. Если имя состоит из нескольких слов, разделенных пробелом, заключите его в кавычки (например, `rule "number one"`).

Примечание. Порядковый номер и имя не являются обязательными параметрами правила фильтрации содержимого трафика. При создании правила без указания номера ему будет присвоен номер, следующий за номером последнего правила в соответствующей таблице, и оно будет иметь самый низкий приоритет. При создании правила без указания имени будет создано правило без имени.

- Параметры, определяющие процесс обработки трафика этим правилом. Подробное описание этих параметров см. в соответствующих разделах:
  - Адрес отправителя (на стр. 118).
  - Адрес получателя (на стр. 119).
  - HTTP-метод (на стр. 120).
  - Тип содержимого (на стр. 119).
  - Действие (на стр. 89).

6 Чтобы удалить правило фильтрации из таблицы правил, выполните команду:

`hostname# service http-proxy content-filter delete {num <номер> | rule <имя>},`

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет;
- `<имя>` — имя правила.

7 Чтобы изменить порядок правила фильтрации в таблице правил, выполните команду:

`hostname# service http-proxy content-filter move {num <номер> | rule <имя>} to <новый номер>`,

где:

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет;
- `<имя>` — имя правила;
- `<новый номер>` — новый порядковый номер правила в таблице.

Примечание. Если при вводе команды была допущена синтаксическая ошибка, то в результате выполнения такой команды появится сообщение с указанием слова, содержащего ошибку. Исправьте ошибку и выполните команду еще раз.

Адрес отправителя

Адрес отправителя является обязательным параметром правила фильтрации содержимого трафика и описывается лексемой:

`src <адрес отправителя>`

Возможные значения адреса отправителя:

- IP-адрес, например:

```
src 192.168.1.36
```

- адрес подсети в формате классовой адресации, например:

  ```
  src 192.168.1.0/24
  ```

- системная группа объектов `any`, например:

  ```
  src @any
  ```

Примечание. В качестве отправителя всегда необходимо указывать клиента прокси-сервера. Использование доменных имен не допускается.

Адрес получателя

Адрес получателя является обязательным параметром правила фильтрации содержимого трафика и описывается лексемой:

```
dst <адрес получателя>
```

Возможные значения адреса получателя:

- IP-адрес или доменное имя узла;
- системная группа объектов `any`, например:

  ```
  dst @any
  ```

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

Тип содержимого

Тип содержимого не является обязательным параметром правила фильтрации содержимого трафика.

Тип содержимого описывается лексемой:

```
mime-type <тип содержимого>
```

Вы можете указать любой тип содержимого из поддерживаемых (см. Поддерживаемые типы содержимого на стр. 265), но только один.

Внимание! Вы можете указать тип содержимого только в том случае, если в правиле фильтрации содержимого трафика не был задан HTTP-метод.

Правило с заданным типом содержимого будет блокировать трафик, передающий этот тип содержимого. Например, следующее правило будет блокировать загрузку изображений формата PNG:

```
hostname# service http-proxy content-filter add src @any dst @any mime-type image/png drop
```

Примечание. MIME-тип файла может зависеть от настроек удаленного HTTP-сервера, с которого этот файл был загружен. То есть, файл будет иметь тот MIME-тип, который был назначен ему HTTP-сервером.

HTTP-метод

HTTP-метод не является обязательным параметром правила фильтрации содержимого трафика.

HTTP-метод описывается лексемой:

```
command <HTTP-метод>
```

Вы можете указать любой из методов протокола HTTP/1.0 (но только один):

- GET
- HEAD
- POST
- PUT
- DELETE
- PATCH
- CONNECT
- OPTIONS
- TRACE

Внимание! Вы можете указать HTTP-метод только в том случае, если в правиле фильтрации содержимого трафика не был задан тип содержимого.

Правило с заданным HTTP-методом будет действовать в тех случаях, когда прокси-сервер ViPNet xFirewall получит от клиента запрос к удаленному HTTP-серверу с этим методом. Например, необходимо запретить заполнение и отправку форм на веб-портал `example.com`, доступный по протоколу HTTP. Для этого необходимо создать правило, которое будет блокировать метод POST для `example.com`:

```
hostname# service http-proxy content-filter add src @any dst example.com command POST drop
```

Чтобы полностью запретить доступ к этому порталу, создайте правило с методом GET:

```
hostname# service http-proxy content-filter add src @any dst example.com command GET drop
```

Действие

Действие является обязательным параметром сетевого фильтра и определяет, что делает фильтр с IP-пакетом, соответствующим его условию.

Действие описывается одной из следующих лексем:

- `pass` — пропускать IP-пакет;
- `drop` — блокировать IP-пакет.

Редактирование правил фильтрации трафика

Вы можете редактировать существующие правила фильтрации трафика. Для этого войдите в режим администратора и остановите прокси-сервер. Далее выполните следующую команду:

```
service http-proxy content-filter change num <номер>[ rule <имя>] src <адрес отправителя> dst <адрес получателя>{ command <HTTP-метод>| mime-type <тип содержимого>}<действие>,
```

где:

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет;
- `<имя>` — имя правила. Если имя состоит из нескольких слов, разделенных пробелом, заключите его в кавычки (например, `rule "number one"`);
- параметры, определяющие процесс обработки трафика этим правилом. Подробное описание этих параметров см. в разделах:
  - Адрес отправителя (на стр. 118).
  - Адрес получателя (на стр. 119).
  - HTTP-метод (на стр. 120).
  - Тип содержимого (на стр. 119).
  - Действие (на стр. 89).

После внесения изменений в правила фильтрации трафика запустите прокси-сервер.

Пример настройки фильтрации содержимого трафика

Чтобы настроить фильтрацию трафика с помощью прокси-сервера и запретить загрузку исполняемых файлов Windows с расширением `.exe`, выполните следующие действия:

1 Остановите работу прокси-сервера с помощью команды:

```
hostname# service http-proxy stop
```

2 Создайте правило фильтрации содержимого трафика прокси-сервера, которое будет блокировать загрузку исполняемых файлов Windows (например, файлов с расширением `.exe`), с помощью команды:

```
hostname# service http-proxy content-filter add src @any dst @any mime-type
application/octet-stream drop
```

3 Запустите прокси-сервер с помощью команды:

```
hostname# service http-proxy start
```

После выполнения действий загрузка исполняемых файлов Windows с расширением `.exe` будет заблокирована.

Настройка антивирусной проверки

Если ViPNet xFirewall используется в качестве прокси-сервера, вы можете настроить антивирусную проверку трафика, передаваемого через прокси-сервер по протоколу HTTP в обоих направлениях: из Интернета к пользователю и от пользователя в Интернет.

Антивирусная проверка осуществляется либо с помощью встроенного антивируса KAV4Proxy, либо с помощью внешнего антивируса по протоколу ICAP (см. глоссарий, стр. 271).

Настройка встроенного антивируса KAV4Proxy

Вы можете настроить фильтрацию трафика, проходящего через прокси-сервер ViPNet xFirewall, встроенным антивирусом KAV4Proxy.

Для настройки фильтрации трафика выполните следующие действия:

1 Остановите работу прокси-сервера с помощью команды:

```
hostname# service http-proxy stop
```

2 Остановите работу антивируса:

```
hostname# service http-proxy antivirus mode off
```

3 Выберите режим фильтрации трафика встроенным антивирусом KAV4Proxy:

```
hostname# service http-proxy antivirus select internal
```

4 Создайте разрешающие правила:

```
hostname# service http-proxy fw-rules apply
```

5 Установите лицензионный ключ антивируса KAV4Proxy:

```
hostname# service http-proxy antivirus internal key install
```

6 Задайте расписание обновления антивирусной базы:

```
hostname# service http-proxy antivirus internal schedule-fetch
```

7 Запустите антивирусную проверку трафика:

```
hostname# service http-proxy antivirus mode on
```

8 Запустите прокси-сервер с помощью команды:

```
hostname# service http-proxy start
```

9 Запустите принудительное обновление антивирусной базы:

```
hostname# service http-proxy antivirus internal fetch
```

В результате выполнения действий прокси-сервер ViPNet xFirewall будет выполнять фильтрацию трафика встроенным антивирусом KAV4Proxy.

Настройка внешнего антивируса

Предположим, вам необходимо настроить фильтрацию трафика внешним антивирусом, работающим на ICAP-сервере (см. глоссарий, стр. 271) с IP-адресом 192.168.0.250 и портом по умолчанию 1344. В случае недоступности ICAP-сервера трафик должен пропускаться через прокси-сервер.

Для настройки фильтрации трафика выполните следующие действия:

1 Остановите работу прокси-сервера:

```
hostname# service http-proxy stop
```

2 Остановите работу антивируса:

```
hostname# service http-proxy antivirus mode off
```

3 Выберите режим фильтрации трафика внешним антивирусом:

```
hostname# service http-proxy antivirus select external
```

4 Задайте адрес ICAP-сервера внешнего антивируса для проверки входящего трафика:

```
hostname# service http-proxy antivirus external server-url add respmod
icap://192.168.0.250/
```

5 Задайте адрес ICAP-сервера внешнего антивируса для проверки исходящего трафика:

```
hostname# service http-proxy antivirus external server-url add reqmod
icap://192.168.0.250/
```

6 Создайте разрешающие правила:

```
hostname# service http-proxy fw-rules apply
```

7 Задайте режим пропуска трафика при недоступности ICAP-сервера внешнего антивируса:

```
hostname# service http-proxy antivirus external bypass on
```

8 Запустите антивирусную проверку трафика:

```
hostname# service http-proxy antivirus mode on
```

9 Запустите прокси-сервер:

```
hostname# service http-proxy start
```

В результате выполнения действий прокси-сервер ViPNet xFirewall будет выполнять фильтрацию трафика внешним антивирусом, работающем на ICAP-сервере с IP-адресом 192.168.0.250.

Настройка взаимодействия с Active Directory

Если вы хотите использовать имена пользователей при создании транзитных фильтров открытой сети (см. Создание сетевого фильтра на стр. 81) и данные пользователей хранятся на контроллере домена Active Directory (см. глоссарий, стр. 270) 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. 124) на контроллере домена.

2 На ViPNet xFirewall настройте взаимодействие с контроллером домена (см. Настройка ViPNet xFirewall для взаимодействия с контроллером домена на стр. 125).

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 ViPNet xFirewall для взаимодействия с контроллером домена

Чтобы настроить ViPNet xFirewall для взаимодействия с контроллером домена, выполните следующие действия:

1 Задайте адрес подключения к контроллеру домена с помощью команды:

`hostname# service user-control ad set controller <адрес контроллера домена> user <имя пользователя>`, указав следующие параметры:

- `<адрес контроллера домена>` — IP-адрес или доменное имя сетевого узла, выполняющего роль контроллера домена. Доменное имя может содержать символы A-z, 0-9, «-» и «.».
- `<имя пользователя>` — имя учетной записи технологического пользователя для соединения с контроллером домена (см. Настройка учетной записи технологического пользователя на контроллере домена на стр. 124). В имени пользователя вы можете использовать любые символы, кроме:

  `" / \ [ ] : ; | = , + * ? < >`

  В имени пользователя не учитывается регистр.

  После выполнения команды введите пароль пользователя для соединения с контроллером домена.

- Задайте время жизни кэша пользовательских сессий. 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;
  - транзитные фильтры открытой сети, в которых задан хотя бы один из пользователей Active Directory, будут показываться как активные, но не будут применяться.

  Чтобы задать время жизни кэша пользовательских сессий в секундах, выполните команду:

  `hostname# service user-control ad set connection-timeout <время жизни кэша пользовательских сессий>`

  По умолчанию значение параметра равно 1800 секундам.

2 Задайте период получения журнала контроллера домена. От значения этого параметра зависит, как часто ViPNet xFirewall будет запрашивать список активных пользователей домена.

   Чтобы задать период получения журнала контроллера домена, выполните команду:

   ```
   hostname# service user-control ad set sync-delay <период>
   ```

   По умолчанию период равен 5 секундам. Период должен быть меньше времени жизни кэша пользовательских сессий.

3 Чтобы просмотреть информацию о текущих настройках взаимодействия с контроллером домена, выполните команду:

   ```
   hostname> service user-control ad show
   ```

4 После изменения настроек взаимодействия с контроллером домена необходимо создать разрешающие сетевые фильтры. Для этого выполните команду:

   ```
   hostname# service user-control fw-rules apply
   ```

5 Чтобы сбросить настройки взаимодействия с контроллером домена, выполните команду:

   ```
   hostname# service user-control ad reset
   ```

6 Чтобы просмотреть список активных пользователей (Active Directory и Captive portal), выполните команду:

   ```
   hostname# service user-control active-users
   ```

Пример настройки взаимодействия с контроллером домена

Предположим вам необходимо настроить взаимодействие с AD, используя параметры:

- адрес контроллера домена — `dc.corp`;
- пользователь домена с правами чтения журналов — `admin`.

Для настройки выполните следующие действия:

1 Остановите демон управления учетными записями пользователей с помощью команды:

   ```
   hostname# service user-control stop
   ```

2 Задайте адрес подключения к контроллеру домена с помощью команды:

   ```
   hostname# service user-control ad set controller dc.corp user admin
   ```

   После выполнения команды введите пароль пользователя для соединения с контроллером домена.

3 Создайте разрешающие сетевые фильтры для соединения с контроллером домена с помощью команды:

   ```
   hostname# service user-control fw-rules apply
   ```

4 При необходимости измените заданное по умолчанию время жизни кэша пользовательских сессий (1800 секунд) с помощью команды:

```
hostname# service user-control ad set connection-timeout <время жизни кэша
пользовательских сессий>
```

5 При необходимости измените заданный по умолчанию период получения журнала контроллера домена (5 секунд) с помощью команды:

```
hostname# service user-control ad set sync-delay <период>
```

6 Убедитесь в правильности настроек взаимодействия с контроллером домена с помощью команды:

```
hostname> service user-control ad show
```

При правильных настройках подключения к контроллеру домена команда должна иметь следующий вывод:

```
Active Directory authentication information:

    Domain Controller dc.corp connection is available

    OS version: Microsoft Windows Server 2008 R2 Enterprise  Locale: English - United
States

    Domain user: admin

    DC synchronization delay: 5 sec

    Allowed connection timeout: 1800 sec
```

7 Запустите демон управления учетными записями пользователей с помощью команды:

```
hostname# service user-control start
```

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:

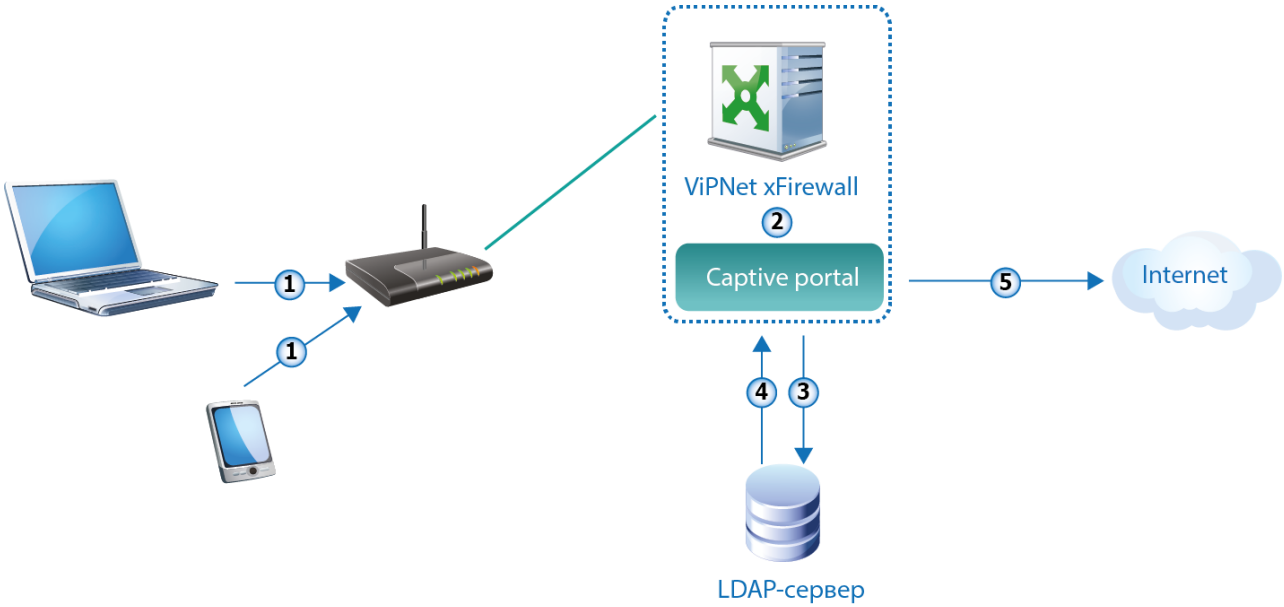


Рисунок 15. Схема аутентификации пользователей с помощью Captive portal

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.

Получение и импорт сертификатов

Перед тем как настроить Captive portal (см. Настройка параметров Captive portal на стр. 131), вам необходимо импортировать в локальное хранилище сертификатов ViPNet xFirewall следующие объекты:

- Корневой сертификат удостоверяющего центра, выпустившего сертификат LDAP-сервера (см. глоссарий, стр. 272). 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. 272) и передайте его в удостоверяющий центр (см. глоссарий, стр. 276). 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 3.

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 Создайте запрос на сертификат Captive portal с помощью команды:

```
hostname# service cert request create name <имя> bits <длина ключа> digest {md5 | sha1},
```

указав следующие параметры:

- `<имя>` — имя сертификата.
- `<длина ключа>` — размер создаваемого RSA-ключа в битах, можно задавать следующие значения: 1024, 1536, 2048, 3072, 4096.
- `md5` — алгоритм хэширования MD5.

- `sha1` — алгоритм хэширования SHA1.

Например:

```
hostname# service cert request create name Cert_1 bits 1024 digest md5
```

2 Чтобы на основе созданного запроса сформировать сертификат, воспользуйтесь одним из вариантов действий:

- Экспортируйте файл запроса на сертификат на USB-носитель. Для этого выполните команду:

  ```
  hostname# service cert request export <имя файла запроса на сертификат>,
  ```

  Например:

  ```
  hostname# service cert request export Cert1_req.pem
  ```

  В ответ на запрос командного интерпретатора подключите USB-носитель и нажмите клавишу **Enter**. Вы сможете использовать полученный файл запроса для формирования сертификата.

- Откройте содержимое запроса на сертификат с помощью команды:

  ```
  hostname> service cert request show <имя файла запроса на сертификат>,
  ```

  Например:

  ```
  hostname> service cert request show Cert1_req.pem
  ```

  После выполнения команды на экране отобразится содержимое запроса на сертификат. Вы можете скопировать его (например, если вы выполнили команду в SSH-сессии) и использовать для формирования сертификата.

3 Обратитесь в удостоверяющий центр и получите сертификат веб-сервера Captive portal. Captive portal поддерживает только сертификаты, подписанные с помощью алгоритма RSA.

4 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 с помощью команды:

```
hostname# service cert import
```

В ответ на запрос командного интерпретатора подключите USB-носитель и нажмите клавишу **Enter**. Далее введите номер файла сертификата и нажмите клавишу **Enter**.

Примечание. Вы можете импортировать сертификаты как в кодировке DER (см. глоссарий, стр. 276), так и в Base64 (см. глоссарий, стр. 270).

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. 131).

Настройка параметров Captive portal

После того, как вы импортировали необходимые сертификата в локальное хранилище ViPNet xFirewall (см. Получение и импорт сертификатов на стр. 129), вы можете настроить аутентификацию пользователей Captive portal на ViPNet xFirewall. Для этого выполните следующие действия:

1 Выберите корневой сертификат удостоверяющего центра, выдавшего сертификат LDAP-сервера из локального хранилища сертификатов ViPNet xFirewall с помощью команды:

```
hostname# service user-control cp set ldap cacert <сертификат>,
```

где `<сертификат>` — имя файла корневого сертификата, установленного в локальное хранилище ViPNet xFirewall.

Например:

```
hostname# service user-control cp set ldap cacert ldap_cert.pem
```

Совет. Чтобы командный интерпретатор автоматически подставил имя корневого сертификата, подходящего для установки (или вывел список сертификатов, если вы импортировали несколько корневых сертификатов), нажмите клавишу **Tab**.

2 Задайте параметры соединения Captive portal с LDAP-сервером с помощью команды:

```
hostname# service user-control cp set ldap <адрес LDAP-сервера> identity <имя служебной учетной записи> basedn <база поиска>,
```

указав следующие параметры:

- `<адрес LDAP-сервера>` — IP-адрес или доменное имя LDAP-сервера. Доменное имя может иметь длину до 253 символов и содержать латинские буквы (`A-z`), цифры (`0-9`), знаки «минус» и «точка».
- `<имя служебной учетной записи>` — выделенное имя (DN, Distinguished Name) (см. RFC 4514) (https://tools.ietf.org/html/rfc4514) служебной учетной записи LDAP-сервера, которая обладает правами на чтение записей LDAP-сервера. Выделенное имя служебной учетной записи может иметь длину до 256 любых символов, кроме:

  ```
  " / \ [ ] : ; | + * ? < >
  ```

  Выделенное имя служебной учетной записи должно быть заключено в двойные кавычки ("").
- `<база поиска>` — выделенное имя (DN, Distinguished Name) (см. RFC 4514) (https://tools.ietf.org/html/rfc4514) базы поиска, от которой начинаются операции поиска в LDAP-каталоге. Выделенное имя базы поиска может иметь длину до 128 любых символов, кроме:

  ```
  " / \ [ ] : ; | + * ? < >
  ```

Выделенное имя базы должно быть заключено в двойные кавычки ("").

Например:

```
hostname# service user-control cp set ldap example.com identity
"uid=admin,ou=People,dc=example" basedn "example"
```

После выполнения команды в ответ на запрос командного интерпретатора введите пароль служебной учетной записи LDAP-сервера.

Внимание! Если вы введете неверный пароль служебной учетной записи LDAP-сервера, то это может стать причиной следующих ситуаций:

- Статус LDAP-сервера будет отображаться неверно.
- Если на LDAP-сервере выключен прием анонимных запросов, то на веб-портале Captive portal не будет работать аутентификация пользователей. При этом в случае, если на LDAP-сервере включен прием анонимных запросов, то на веб-портале Captive portal будет работать аутентификация пользователей независимо от того, верно ли указан пароль к служебной учетной записи LDAP-сервера или нет.

---

3 Выберите сертификат веб-сервера Captive portal из локального хранилища сертификатов ViPNet xFirewall с помощью команды:

```
hostname# service user-control cp set hostcert <имя файла сертификата> hostkey <имя
файла закрытого ключа>
```

Например:

```
hostname# service user-control cp set hostcert certificate.pem hostkey private.key
```

Совет. Чтобы командный интерпретатор автоматически подставил имя сертификата, подходящего для установки (локального сертификата, для которого есть закрытый ключ), или вывел список сертификатов, если их несколько, нажмите клавишу **Tab**.

Внимание! Если вы выбрали сертификат веб-сервера Captive portal и хотите отказаться от его использования, то вам необходимо сбросить настройки Captive portal с помощью команды (см. документ «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам»):

```
hostname# service user-control cp reset
```

Сброс настроек Captive portal необходимо выполнить также в том случае, если вы удалили сертификат веб-сервера Captive portal и не хотите использовать вместо него другой сертификат.

---

4 Задайте режим соединения с LDAP-сервером с помощью команды:

```
hostname# service user-control cp set connection-secure <режим соединения>,
```

где `<режим соединения>` может принимать следующие значения:

- `stls` — режим соединения Start TLS, устанавливает соединения на порт LDAP 389;
- `ldaps` — режим соединения на порт LDAP 636;

- `none` — режим открытого соединения. Используется по умолчанию.

Например:

```
hostname# service user-control cp set connection-secure stls
```

5 Проверьте работу Captive portal с помощью команды:

```
hostname> service user-control cp show
```

6 После изменения настроек взаимодействия с LDAP-сервером необходимо создать разрешающие сетевые фильтры. Для этого выполните команду:

```
hostname# service user-control fw-rules apply
```

7 Чтобы просмотреть список активных пользователей (Active Directory и Captive portal), выполните команду:

```
hostname# service user-control active-users
```

8 При необходимости вы можете настроить остальные параметры Captive portal (см. документ «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам»).

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.

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 параметры взаимодействия Captive portal с LDAP-сервером, выполните следующие действия:

1 Импортируйте сертификат веб-сервера Captive portal и сертификат LDAP-сервера (см. Получение и импорт сертификатов на стр. 129).

2 Остановите демон управления учетными записями пользователей с помощью команды:

```
hostname# service user-control stop
```

3 Задайте параметры соединения Captive portal с LDAP-сервером с помощью команды:

```
hostname# service user-control cp set ldap 192.168.203.155 identity
"uid=admin,ou=People,dc=example" basedn "example"
```

4 Задайте режим соединения с LDAP-сервером с помощью команды:

```
hostname# service user-control cp set connection-secure stls
```

5 Создайте разрешающие сетевые фильтры для соединения с LDAP-сервером с помощью команды:

```
hostname# service user-control fw-rules apply
```

6 Задайте время жизни сессии пользователя с помощью команды:

```
hostname# service user-control cp set connection-timeout 43200
```

7 Задайте время неактивности пользователя с помощью команды:

```
hostname# service user-control cp set idle-timeout 1800
```

8 Задайте название сети, отображаемое на веб-странице Captive portal с помощью команды:

```
hostname# service user-control cp set custom-login-form "Guest Network"
```

9 Убедитесь в правильности настроек Captive portal с помощью команды:

```
hostname> service user-control cp show
```

При правильных настройках Captive portal и доступном LDAP-сервере команда должна иметь примерно следующий вывод:

```
Captive Portal authentication information:
LDAP server 192.168.203.155 is available
LDAP identity: "uid=admin,ou=People,dc=example"
LDAP basedn: "example"
LDAP connection secured: stls
LDAP server CA certificate: xF_cacert.pem
CP server CA certificate: xF_hostcert.pem
Allowed connection timeout: 43200 sec
Allowed idle timeout: 1800 sec
Custom login phrase: Guest Network
```

10 Запустите демон управления учетными записями пользователей с помощью команды:

```
hostname# service user-control start
```

После выполнения описанных действий на вашем ViPNet xFirewall будет работать авторизация пользователей с помощью Captive portal, и вы сможете задавать имена пользователей при создании транзитных фильтров открытой сети (см. Создание сетевого фильтра на стр. 81).

Тонкая настройка межсетевого экрана

Настройка антиспуфинга

В ViPNet xFirewall реализована функция антиспуфинга, то есть блокирования входящих IP-пакетов от отправителей, IP-адреса которых недопустимы на данном сетевом интерфейсе узла. Антиспуфинг работает только для открытого трафика, поскольку для трафика защиты канала управления IP-адрес отправителя не имеет значения. Открытые пакеты сначала проверяются посредством антиспуфинга, а затем уже обрабатываются сетевыми фильтрами (см. Общие сведения о сетевых фильтрах на стр. 74).

Основная задача антиспуфинга — это защита от сетевых атак, называемых спуфингом. При спуфинге злоумышленник посылает на какой-либо компьютер IP-пакет, в котором в качестве адреса отправителя указан не адрес злоумышленника, а адрес какого-либо другого узла, которому разрешено соединение с данным координатором. Например, таким образом можно отправить открытый пакет из Интернета через координатор, задав в качестве адреса отправителя адрес частной внутренней сети, которая также подключена к данному координатору. Антиспуфинг позволяет исключить такую возможность.

По умолчанию антиспуфинг в ViPNet xFirewall выключен. Для повышения уровня безопасности сети рекомендуется включить его.

Чтобы просмотреть текущее состояние антиспуфинга, в интерпретаторе ViPNet выполните команду:

```
hostname> iplir option get antispoofing
```

Чтобы включить (`on`) или выключить (`off`) антиспуфинг в ViPNet xFirewall, выполните команду:

```
hostname# iplir option set antispoofing {on | off}
```

Внимание! В случае использования сложных схем маршрутизации на узле (с метриками маршрутов или асимметричными маршрутами) включать функцию антиспуфинга не рекомендуется, так как она может работать некорректно.

Антиспуфинг работает следующим образом:

- Для всех сетевых интерфейсов, кроме интерфейса, соответствующего маршруту по умолчанию, блокируются IP-пакеты, адреса отправителей которых не совпадают с адресами, маршрутизируемыми через данный интерфейс.
- Для сетевого интерфейса, соответствующего маршруту по умолчанию, блокируются IP-пакеты, адреса отправителей которых совпадают с зарегистрированными маршрутами других интерфейсов.

Пример настройки антиспуфинга

Пусть на сетевом узле используется следующая таблица маршрутизации:

Таблица 8. Пример таблицы маршрутизации на узле

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	10.0.8.1	10.0.8.54	20
10.0.8.0	255.255.255.0	On-link	10.0.8.54	276
10.0.8.54	255.255.255.255	On-link	10.0.8.54	276
10.0.8.255	255.255.255.255	On-link	10.0.8.54	276
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.48.0	255.255.255.0	On-link	192.168.48.1	276
192.168.48.1	255.255.255.255	On-link	192.168.48.1	276
192.168.48.255	255.255.255.255	On-link	192.168.48.1	276
192.168.59.0	255.255.255.0	On-link	192.168.59.1	276
192.168.59.1	255.255.255.255	On-link	192.168.59.1	276
192.168.59.255	255.255.255.255	On-link	192.168.59.1	276
224.0.0.0	224.0.0.0	On-link	127.0.0.1	306
224.0.0.0	224.0.0.0	On-link	10.0.8.54	276
224.0.0.0	224.0.0.0	On-link	192.168.48.1	276
224.0.0.0	224.0.0.0	On-link	192.168.59.1	276
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	10.0.8.54	276
255.255.255.255	255.255.255.255	On-link	192.168.48.1	276
255.255.255.255	255.255.255.255	On-link	192.168.59.1	276

Рассматриваемый узел имеет четыре сетевых интерфейса. Сетевой интерфейс с адресом 127.0.0.1 является интерфейсом «внутренней петли» (loopback), поэтому не будем его учитывать.

При включении антиспуфинга на основе приведенной таблицы маршрутизации будут выполнены следующие действия:

- На сетевом интерфейсе с адресом 192.168.48.1 разрешены входящие пакеты только от узлов с IP-адресами 192.168.48.0/24.
- На сетевом интерфейсе с адресом 192.168.59.1 разрешены входящие пакеты только от узлов с IP-адресами 192.168.59.0/24.

- На сетевом интерфейсе с адресом 10.0.8.54 разрешены все входящие пакеты, кроме пакетов от узла с IP-адресами 192.168.48.0/24, 192.168.59.0/24.

Настройка дополнительных параметров межсетевого экрана

Чтобы посмотреть текущие настройки дополнительных параметров межсетевого экрана, выполните команду:

```
hostname> iplir option get <параметр>,
```

указав один из следующих параметров:

- `antispoofing` — включение или выключение антиспуфинга. Возможные значения:
  - `off` (по умолчанию) — антиспуфинг выключен.
  - `on` — антиспуфинг включен.
- `block-fragmented-packets` — включение или выключение блокирования входящих фрагментированных IP-пакетов, принимаемых по всем сетевым интерфейсам. Возможные значения:
  - `off` (по умолчанию) — фрагментированные пакеты пропускаются.
  - `on` — фрагментированные пакеты блокируются, в журнал регистрации IP-пакетов вносится соответствующая запись (см. Просмотр журнала регистрации IP-пакетов на стр. 202).
- `connection-ttl-ip` — время жизни соединений по протоколу IP при отсутствии активности в нем. Указывается в секундах, по умолчанию — 300 (5 минут).
- `connection-ttl-tcp` — время жизни соединений по протоколу TCP при отсутствии активности в нем. Указывается в секундах, по умолчанию — 1800 (30 минут).
- `connection-ttl-udp` — время жизни соединений по протоколу UDP при отсутствии активности в нем. Указывается в секундах, по умолчанию — 300 (5 минут).
- `max-connections` — максимальное количество параллельно установленных соединений. Значение данного параметра зависит от исполнения ViPNet xFirewall.

Таблица 9. Значения параметра max-connections для исполнений ViPNet xFirewall

Исполнение ViPNet xFirewall	Объем оперативной памяти	Значение по умолчанию	Максимальное значение
ViPNet xFirewall xF100	2 Гбайт	150000	150000
ViPNet xFirewall xF1000	2 Гбайт	1000000	1000000
ViPNet xFirewall xF5000	8 Гбайт	8000000	10000000
ViPNet xFirewall xF-VA	2 Гбайт	150000	150000

Для изменения настройки какого-либо параметра межсетевого экрана в ViPNet xFirewall выполните команду:

```
hostname# iplir option set <параметр> <значение>
```

8

Настройка сетевых служб

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 Укажите сетевой интерфейс Ethernet, на котором будет работать DHCP-сервер, с помощью команды:

```
hostname# inet dhcp server interface <имя интерфейса>
```

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

2 Задайте диапазон IP-адресов для распределения сервером с помощью команды:

```
hostname# inet dhcp server range <начальный IP-адрес> <конечный IP-адрес>
```

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`.

3 Чтобы задать IP-адрес шлюза по умолчанию, выполните команду:

```
hostname# inet dhcp server router <IP-адрес>
```

IP-адрес шлюза должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам.

4 Чтобы включить или выключить автоматический запуск DHCP-сервера при загрузке ViPNet xFirewall, выполните команду:

```
hostname# inet dhcp server mode {on | off}
```

По умолчанию автоматический запуск DHCP-сервера выключен.

Примечание. Перед тем как вы включаете или запускаете DHCP-сервер, убедитесь, что служба DHCP-relay выключена (см. Настройка DHCP-relay на стр. 142).

5 Чтобы запустить DHCP-сервер или завершить его работу, выполните команду:

```
hostname# inet dhcp server {start | stop}
```

6 Чтобы просмотреть текущие параметры DHCP-сервера, выполните команду:

```
hostname> inet show dhcp server
```

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.

При настройке службы DHCP-relay следует учитывать следующие рекомендации и ограничения:

- На ViPNet xFirewall требуется дополнительно задать правило фильтрации транзитного трафика, разрешающее UDP-трафик по портам 67 и 68. Аналогичные правила для локального открытого и широковещательного трафика заданы по умолчанию.
- Использование ViPNet xFirewall в качестве агента DHCP-relay возможно только при работе ViPNet xFirewall в одиночном режиме. Работа службы DHCP-relay в режиме кластера горячего резервирования не поддерживается.

Чтобы запустить службу DHCP-relay на сетевом интерфейсе Ethernet, выполните следующие действия:

1. Задайте список сетевых интерфейсов Ethernet, через которые DHCP-relay должен получать DHCP-запросы от клиентов:
   - Чтобы добавить сетевой интерфейс в список, выполните команду:

     ```
     hostname# inet dhcp relay add listen-interface <имя интерфейса>
     ```

     На каждом добавляемом сетевом интерфейсе должен быть задан статический IP-адрес, принадлежащий адресному пространству соответствующей подсети. Сетевой интерфейс, который используется для соединения с удаленным сервером, может также получать IP-адрес по DHCP.
   - Чтобы удалить сетевой интерфейс из списка, выполните команду:

     ```
     hostname# inet dhcp relay delete listen-interface <имя интерфейса>
     ```
2. Задайте внешний DHCP-сервер, на который необходимо перенаправлять DHCP-запросы клиентов, а также сетевой интерфейс ViPNet xFirewall, который должен использоваться для доступа к удаленному серверу, с помощью следующей команды:

   ```
   hostname# inet dhcp relay external-interface <имя интерфейса> server {<IP-адрес сервера> | <DNS-имя сервера>}
   ```

3 Чтобы включить или выключить автоматический запуск службы DHCP-relay при загрузке ViPNet xFirewall, выполните команду:

```
hostname# inet dhcp relay mode {on | off}
```

По умолчанию автоматический запуск DHCP-relay выключен.

Примечание. Перед тем как вы включаете или запускаете службу DHCP-relay, убедитесь, что работа DHCP-сервера завершена (см. Настройка параметров DHCP-сервера на стр. 140).

4 Чтобы запустить службу DHCP-relay или завершить ее работу, выполните команду:

```
hostname# inet dhcp relay {start | stop}
```

Примечание. Чтобы впоследствии завершить работу службы DHCP-relay и одновременно сбросить все ее настройки, а также выключить автоматический запуск службы при загрузке ViPNet xFirewall, выполните команду:

```
hostname# inet dhcp relay reset
```

Пример настройки работы клиентов с локальным DHCP-сервером

Чтобы настроить работу клиентов с локальным DHCP-сервером, выполните следующие действия:

1. Выполните команду `enable` для перехода в режим администратора. В ответ на приглашение введите пароль администратора.
2. Задайте интерфейс, на котором будет работать DHCP-сервер, с помощью команды:

   ```
   hostname# inet dhcp server interface <имя интерфейса>
   ```

   В качестве параметра укажите имя интерфейса, подключенного к локальной сети.
3. Задайте диапазон IP-адресов, выделяемых клиентам, с помощью команды:

   ```
   hostname# inet dhcp server range <начальный IP-адрес> <конечный IP-адрес>
   ```

   IP-адрес интерфейса ViPNet xFirewall, подключенного к локальной сети, не должен входить в этот диапазон.
4. Задайте срок (время аренды), на который клиентам предоставляются IP-адреса, с помощью команды:

   ```
   hostname# inet dhcp server lease <время аренды>
   ```
5. Задайте IP-адрес шлюза по умолчанию, если его необходимо передавать клиентам, с помощью команды:

   ```
   hostname# inet dhcp server router <IP-адрес>
   ```
6. Проверьте текущие параметры DHCP-сервера с помощью команды:

   ```
   hostname# inet show dhcp server
   ```

   При необходимости откорректируйте параметры с помощью приведенных выше команд.
7. Включите интерфейс, на котором будет работать DHCP-сервер, с помощью команды:

   ```
   hostname# inet ifconfig <имя интерфейса> up
   ```
8. Включите автоматический запуск DHCP-сервера, чтобы не запускать его вручную при каждой загрузке ViPNet xFirewall. Для этого выполните команду:

   ```
   hostname# inet dhcp server mode on
   ```
9. Запустите DHCP-сервер, если это необходимо сделать в текущем сеансе работы, с помощью команды:

   ```
   hostname# inet dhcp server start
   ```

   При следующей загрузке ViPNet xFirewall DHCP-сервер будет запущен автоматически (если автоматический запуск включен).

Внимание! Вместе с IP-адресом DHCP-сервер, функционирующий на ViPNet xFirewall, всегда предоставляет клиентам свой адрес в качестве адресов DNS-сервера и NTP-сервера. Поэтому клиенты будут отправлять запросы на разрешение имен и синхронизацию времени через соответствующие сервисы, запущенные на ViPNet xFirewall. Если на ViPNet xFirewall эти сервисы не запущены, то клиенты не смогут работать с DNS-именами и синхронизировать свое время.

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 лицензии (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 (см. Настройка параметров DHCP-сервера на стр. 140). 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 По умолчанию DNS-запросы к серверу разрешены для любых узлов. Если необходимо явно указать IP-адреса узлов и подсетей, узлам которых разрешены запросы к DNS-серверу, задайте их с помощью команды:

```
hostname# inet dns clients add {<IP-адрес> | <IP-адрес/длина маски>}
```

Для проверки текущего списка IP-адресов, которым разрешены DNS-запросы к серверу, используйте команду:

```
hostname# inet dns clients list
```

Для удаления IP-адресов из списка используйте команду:

```
hostname# inet dns clients delete {<IP-адрес> | <IP-адрес/длина маски>}
```

2 Добавьте IP-адреса DNS-серверов, на которые ViPNet xFirewall будет перенаправлять DNS-запросы, с помощью команды:

```
hostname# inet dns forwarders add <IP-адрес>
```

По умолчанию DNS-запросы перенаправляются на корневые DNS-серверы из домена root-servers.net.

Для проверки текущего списка DNS-серверов пересылки используйте команду:

```
hostname# inet dns forwarders list
```

Для удаления DNS-серверов из списка используйте команду:

```
hostname# inet dns forwarders delete <IP-адрес>
```

3 Чтобы включить или выключить автоматический запуск DNS-сервера при загрузке ViPNet xFirewall, выполните команду:

```
hostname# inet dns mode {on | off}
```

По умолчанию автоматический запуск DNS-сервера включен.

4 Чтобы запустить DNS-сервер или завершить его работу, выполните команду:

```
hostname# inet dns {start | stop}
```

5 Чтобы просмотреть текущие параметры DNS-сервера, выполните команду:

```
hostname> inet show dns
```

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 в файле `iplir.conf` в секции `[id]` для этого узла установить параметр `visibility` в значение `real`. Описание секции и параметра см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», в разделе «Файл iplir.conf».

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 Чтобы добавить IP-адрес NTP-сервера для синхронизации системного времени ViPNet xFirewall, выполните команду:

```
hostname# inet ntp add {IP-адрес | DNS-имя}
```

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.

2 Чтобы удалить адрес NTP-сервера из списка, выполните команду:

```
hostname# inet ntp delete {IP-адрес | DNS-имя}
```

3 Чтобы включить или выключить автоматический запуск NTP-сервера при загрузке ViPNet xFirewall, выполните команду:

```
hostname# inet ntp mode {on | off}
```

По умолчанию автоматический запуск NTP-сервера включен.

4 Чтобы запустить NTP-сервер или завершить его работу, выполните следующую команду:

```
hostname# inet ntp {start | stop}
```

Внимание! NTP-серверы, указанные по доменному имени, будут доступны, только если запущен DNS-сервер.

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 просмотреть текущие параметры и состояние NTP-сервера, выполните команду:

```
hostname> inet show ntp
```

Пример настройки доступа клиентов удаленных офисов к DNS- и NTP-серверам, расположенным в центральном офисе

Предположим, вам надо настроить работу клиентов (сетевых узлов) удаленных офисов с корпоративными DNS- и NTP-серверами, расположенными в центральном офисе, выполните следующие действия:

1. Выполните команду `enable` для перехода в режим администратора. В ответ на приглашение введите пароль администратора.
2. Включите автоматический запуск DNS-сервера, чтобы не запускать его вручную при каждой загрузке ViPNet xFirewall. Для этого выполните команду:

   ```
   hostname# inet dns mode on
   ```

   Если при установке справочников и лицензии вы уже включили автоматический запуск DNS-сервера при загрузке (см. документ «ViPNet xFirewall. Подготовка к работе», раздел «Настройка DNS-сервера»), эту команду можно не выполнять.
3. Включите автоматический запуск NTP-сервера, чтобы не запускать его вручную при каждой загрузке ViPNet xFirewall. Для этого выполните команду:

   ```
   hostname# inet ntp mode on
   ```

   Если при установке справочников и лицензии вы уже включили автоматический запуск DNS-сервера при загрузке (см. документ «ViPNet xFirewall. Подготовка к работе», раздел «Настройка NTP-сервера»), эту команду можно не выполнять.
4. Добавьте IP-адрес корпоративного NTP-сервера, который необходимо использовать для синхронизации времени, с помощью команды:

   ```
   hostname# inet ntp add <IP-адрес>
   ```

   По умолчанию для синхронизации времени используются публичные NTP-серверы из кластера `pool.ntp.org`.

   Для проверки текущего списка NTP-серверов используйте команду:

   ```
   hostname# inet ntp list
   ```

   Для удаления NTP-серверов из списка используйте команду:

   ```
   hostname# inet ntp delete <IP-адрес>
   ```
5. Проверьте текущие параметры NTP-сервера с помощью команды:

```
hostname# inet show ntp
```

При необходимости откорректируйте параметры с помощью соответствующих команд.

6 Запустите NTP-сервер, если это необходимо сделать в текущем сеансе работы, с помощью команды:

```
hostname# inet ntp start
```

При следующей загрузке ViPNet xFirewall NTP-сервер будет запущен автоматически (если автоматический запуск включен).

7 Запустите DNS-сервер, если это необходимо сделать в текущем сеансе работы, с помощью команды:

```
hostname# inet dns start
```

При следующей загрузке ViPNet xFirewall DNS-сервер будет запущен автоматически (если автоматический запуск включен).

8 Создайте локальные фильтры открытой сети, разрешающие доступ клиентов филиалов к DNS- и NTP-серверу:

```
hostname# firewall local add src @PrivateNetworkIP dst @local service @DNS pass
hostname# firewall local add src @PrivateNetworkIP dst @local service @NTP pass
```

В результате произведенных настроек клиенты филиала смогут отправлять запросы на корпоративные DNS- и NTP-сервера.

9

Настройка маршрутизации

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, 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 (см. глоссарий, стр. 271);
- динамических маршрутов, формируемых протоколом OSPF (см. глоссарий, стр. 272).

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 (см. Настройка балансировки IP-трафика на стр. 161). 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

В процессе или после настройки маршрутизации вы можете просмотреть список всех существующих маршрутов (содержимое RIB). Для этого выполните команду:

```
hostname> inet show routing
```

В результате выполнения команды будет выдана информация в следующем виде:

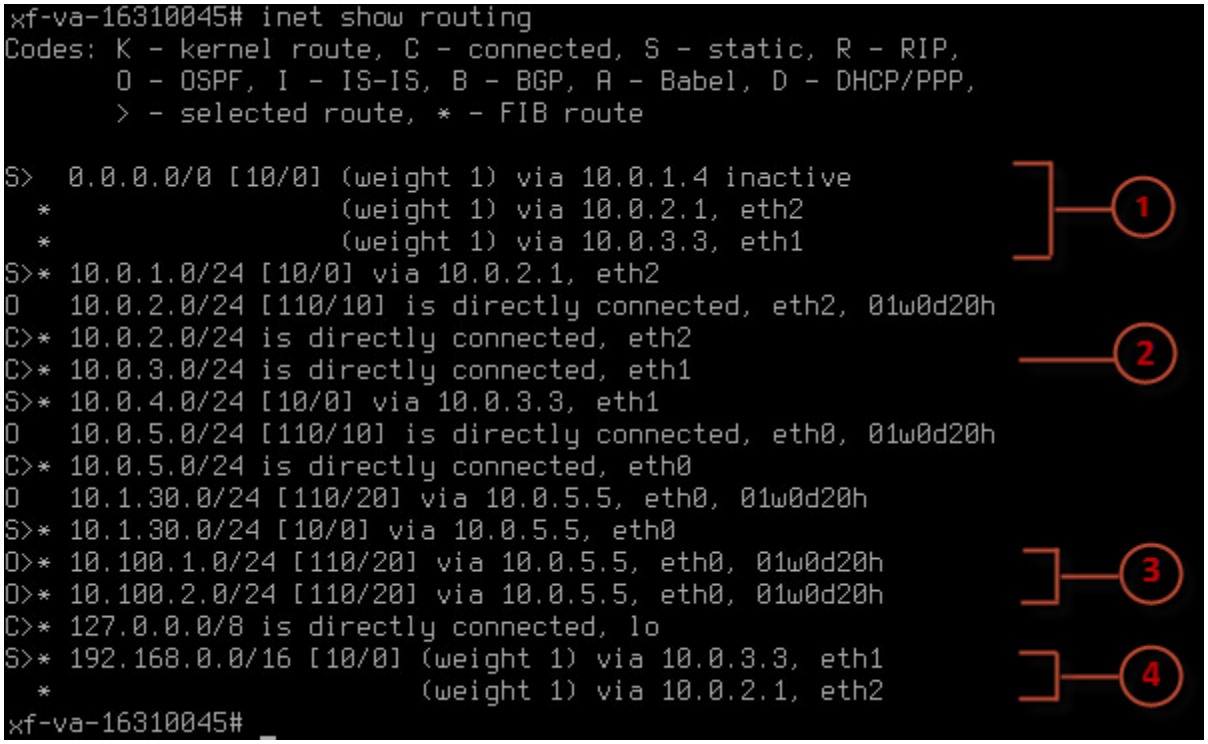


Рисунок 16. Просмотр таблицы маршрутизации

Цифрами на рисунке обозначены:

1 Статический маршрут по умолчанию. Выбран как наилучший. Объединяет три маршрута, поэтому включает в себя три шлюза. Каждому шлюзу назначен вес, поэтому в процессе маршрутизации будет осуществляться балансировка нагрузки.

Примечание. Если маршрут по умолчанию не задан, отображается соответствующее предупреждение. В этом случае создайте статический маршрут по умолчанию (см. Создание статических маршрутов на стр. 160).

---

2 Маршрут в подсеть 10.0.3.0 с маской 255.255.255.0, к которой подключен один из интерфейсов ViPNet xFirewall. Выбран как наилучший.

3 Маршруты в подсети 10.100.1.0 и 10.100.2.0 с маской 255.255.255.0, полученные по протоколу OSPF (см. глоссарий, стр. 272). Выбраны как наилучшие.

4 Статический маршрут в подсеть 192.168.0.0 с маской 255.255.0.0. Выбран как наилучший. Объединяет два маршрута, поэтому включает в себя два шлюза. Каждому шлюзу назначен вес, поэтому в процессе маршрутизации будет осуществляться балансировка нагрузки.

Каждый раз перед списком маршрутов выводится список возможных атрибутов, которые могут присваиваться для маршрутов, и их расшифровка. В таблице ниже приведены пояснения по данным атрибутам.

Таблица 10. Атрибуты маршрутов

Атрибут	Расшифровка в командном интерпретаторе	Пояснение
C	connected	Маршрут в подсеть, к которой подключен один из интерфейсов ViPNet xFirewall.
S	static	Статический маршрут.
O	OSPF	Маршрут протокола динамической маршрутизации OSPF.
B	BGP	Маршрут протокола динамической маршрутизации BGP. В текущей версии ViPNet xFirewall не поддерживается работа по данному протоколу.
D	DHCP	Маршрут, предоставленный DHCP-сервером.
>	selected route	Наилучший маршрут. Отображается в том случае, если в таблице есть несколько маршрутов в одну и ту же сеть с разной административной дистанцией (см. глоссарий, стр. 273).
*	FIB route	Маршрут, загруженный в таблицу FIB и используемый для маршрутизации.

Примечание. В таблице маршрутизации могут присутствовать другие атрибуты, кроме описанных в таблице выше. Эти атрибуты зарезервированы для других протоколов маршрутизации и в текущей версии ViPNet xFirewall не используются.

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. 273).

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. После заполнения базы данных на каждом маршрутизаторе по алгоритму Дейкстры вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость. 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, 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.

Создание статических маршрутов

Вы можете создать маршрут по умолчанию или ряд статических маршрутов следующим образом:

- Чтобы добавить маршрут по умолчанию, выполните команду:

  ```
  hostname# inet route add default next-hop <IP-адрес шлюза> [distance <1-255> [weight <1-255>]]
  ```

- Чтобы добавить статический маршрут, выполните команду:

  ```
  hostname# inet route add <IP-адрес назначения> next-hop <IP-адрес шлюза> [netmask <маска сети> [distance <1-255> [weight <1-255>]]]
  ```

Совет. Если вам требуется добавить 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. ниже).

В обеих командах вы можете задать необязательные параметры `distance` — административную дистанцию маршрута (см. глоссарий, стр. 273) и `weight` — вес шлюза (см. глоссарий, стр. 273).

Административная дистанция задается, чтобы назначить приоритет маршруту. Если вы не укажете значение административной дистанции, то оно будет задано автоматически: `distance=10`. Если вы укажете административную дистанцию, и ее значение будет совпадать со значением

административной дистанции, заданной протоколам динамической маршрутизации (см. Настройка административной дистанции для маршрутов DHCP-протокола на стр. 165), появится сообщение, что маршрут не может быть добавлен. В этом случае создайте маршрут с другим значением административной дистанции.

Вес задается в маршруте для шлюза. Его требуется задавать в том случае, если создается несколько маршрутов в одну сеть с разными шлюзами, между которыми требуется производить балансировку нагрузки. Подробнее см. раздел Настройка балансировки IP-трафика (на стр. 161).

В результате маршрут будет добавлен в RIB. Если маршрут будет определен как наилучший, то он также будет загружен в FIB, после чего начнет использоваться при маршрутизации IP-трафика.

При необходимости вы можете удалить созданные маршруты. Подробнее см. раздел Удаление статического маршрута (на стр. 161).

Удаление статического маршрута

При необходимости вы можете удалить маршрут по умолчанию или статический маршрут следующим образом:

- Чтобы удалить маршрут по умолчанию, выполните команду:

  ```
  hostname# inet route delete default [next-hop <IP-адрес шлюза>]
  ```

- Чтобы удалить статический маршрут, выполните команду:

  ```
  hostname# inet route delete <IP-адрес назначения> [netmask <маска сети> next-hop
  <IP-адрес шлюза>]
  ```

Если при вводе команды вы не указали маску сети или IP-адрес шлюза, и в процессе проверки будет установлено, что в таблице RIB есть несколько маршрутов в указанную сеть, то будет выдан список всех маршрутов. Если вы согласны на удаление всех этих маршрутов, введите символ **y** и нажмите клавишу **Enter**. Аналогичная ситуация возникнет при удалении маршрута с несколькими шлюзами.

В результате маршрут или все маршруты с указанными параметрами будут удалены из RIB. Если маршруты присутствуют в таблице FIB, то из нее они также будут удалены.

Примечание. Если требуется удалить все статические маршруты, включая все маршруты по умолчанию, воспользуйтесь командой:

```
hostname# inet route clear
```

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. 273) (`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. Создание статических маршрутов на стр. 160) 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 команд для создания статических маршрутов с весом шлюзов равным 1:

```
hostname# inet route add 10.0.5.0 next-hop 10.0.1.1 netmask 255.255.255.0 distance 20
weight 1

hostname# inet route add 10.0.5.0 next-hop 10.0.4.3 netmask 255.255.255.0 distance 20
weight 1
```

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.

Просмотр статических маршрутов

Если вы хотите просмотреть список всех статических маршрутов, которые были созданы и присутствуют в RIB, выполните команду:

```
hostname> inet show routing static
```

В результате выполнения команды появится список маршрутов в следующем виде:

```
xf-va-16310045# inet show routing static
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------
0.0.0.0          0.0.0.0          10.0.1.4         10       1
0.0.0.0          0.0.0.0          10.0.2.1         10       1
0.0.0.0          0.0.0.0          10.0.3.3         10       1
10.0.1.0         255.255.255.0    10.0.2.1         10       1
10.0.4.0         255.255.255.0    10.0.3.3         10       1
10.1.30.0        255.255.255.0    10.0.5.5         10       1
192.168.0.0      255.255.0.0      10.0.2.1         10       1
192.168.0.0      255.255.0.0      10.0.3.3         10       1
xf-va-16310045#
```

Рисунок 17. Просмотр статических маршрутов

В списке для каждого маршрута указаны: IP-адрес назначения, маска сети, шлюз, административная дистанция маршрута (см. глоссарий, стр. 273) и вес шлюза (см. глоссарий, стр. 273).

Настройка динамической маршрутизации

Если в вашей сети поддерживается работа по протоколу DHCP (см. глоссарий, стр. 271) или OSPF (см. глоссарий, стр. 272), 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 (см. Настройка административной дистанции для маршрутов DHCP-протокола на стр. 165). 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-протокола на стр. 165). Это позволит определить приоритет среди маршрутов DHCP-сервера в одну и ту же сеть, полученных с разных сетевых интерфейсов.

Просмотр информации базы данных состояний каналов связи по протоколу OSPF

Кроме настроек протокола OSPF вы также можете просмотреть информацию о состоянии каналов связей между всеми маршрутизаторами, работающими по протоколу OSPF. Данная информация содержится в базе данных (link state database) (см. Общие сведения о протоколе OSPF на стр. 158) и синхронизируется на всех OSPF-маршрутизаторах. Именно на ее основе вычисляются динамические маршруты протокола OSPF. Для просмотра информации базы данных состояний каналов связи, выполните команду:

```
hostname> inet show ospf database
```

В результате выполнения команды отобразится содержимое базы данных в следующем виде:

```
xf-16310045# inet show ospf database

       OSPF Router with ID (10.0.3.2)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.0.3.2        10.0.3.2        155 0x8000017d 0x590a 2
10.1.30.5       10.1.30.5       220 0x8000029f 0x3fa0 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.0.5.5        10.1.30.5       751 0x80000263 0x3541

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
10.0.1.0        10.1.30.5      1551 0x80000182 0x9061 E2 10.0.1.0/24 [0x0]
10.0.2.0        10.1.30.5      1001 0x80000183 0x836c E2 10.0.2.0/24 [0x0]
10.0.3.0        10.1.30.5       210 0x80000182 0x7a75 E2 10.0.3.0/24 [0x0]
10.0.4.0        10.1.30.5       341 0x80000182 0x6f7f E2 10.0.4.0/24 [0x0]
10.100.1.0      10.1.30.5       911 0x8000029d 0xe1ad E2 10.100.1.0/24 [0x0]
10.100.2.0      10.1.30.5       180 0x8000029f 0xe0aa E2 10.100.2.0/24 [0x0]
192.168.0.0     10.1.30.5       821 0x80000182 0x6c27 E2 192.168.0.0/16 [0x0]


xf-16310045# _
```

Рисунок 18. Просмотр базы данных состояний связи

Настройка административной дистанции для маршрутов DHCP-протокола

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. 160) 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. 273), тем выше приоритет маршрута.

В настройках ViPNet xFirewall вы можете выполнить следующие действия:

- Задать административную дистанцию для маршрутов, поступающих от DHCP-сервера. Эта дистанция будет определять приоритет всех маршрутов DHCP-сервера, независимо от того, на какой сетевой интерфейс они поступили.

  Чтобы задать административную дистанцию для маршрутов от DHCP-сервера, выполните команду:

  ```
  hostname# inet dhcp client route-distance <1-255>
  ```

- Задать административную дистанцию для маршрутов по умолчанию вместе с общей административной дистанцией для всех маршрутов DHCP-сервера. Эта дистанция будет определять приоритет только маршрутов по умолчанию. Если эта дистанция не задана, то у маршрутов по умолчанию дистанция и приоритет соответственно будет таким же, как и у других маршрутов DHCP-сервера.

  Чтобы задать административную дистанцию для маршрутов по умолчанию от DHCP-сервера, выполните команду:

  `hostname# inet dhcp client route-distance <1-255> [default-route <1-255>]`, где `default-route <1-255>` — значение административной дистанции для маршрутов по умолчанию.

При необходимости перед или после настройки административной дистанции вы можете посмотреть, на каких сетевых интерфейсах включен режим DHCP и какая административная дистанция задана. Подробнее см. раздел Просмотр настроек DHCP в режиме клиента (на стр. 166).

Настройка метрики для маршрутов DHCP-протокола

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. 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.

- Чтобы добавить специфичную метрику на сетевом интерфейсе, выполните команду:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp route-metric <1-255>
  ```

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

- Ethernet.
- VLAN (см. Организация обработки трафика из нескольких VLAN на стр. 46).
- Агрегированный интерфейс (см. Использование агрегированных сетевых интерфейсов на стр. 50).

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 удалить метрику, заданную на сетевом интерфейсе, выполните команду:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp route-metric none
  ```

  После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

При необходимости перед или после настройки метрик вы можете посмотреть, на каких сетевых интерфейсах включен режим DHCP и какие метрики заданы. Подробнее см. раздел Просмотр настроек DHCP в режиме клиента (на стр. 166).

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 команду:

```
hostname# inet dhcp client route-default-metric <1-255>
```

Просмотр настроек DHCP в режиме клиента

Вы можете просмотреть следующие параметры DHCP в режиме клиента:

- административная дистанция, которая задана для маршрутов, поступающих от DHCP-сервера (см. Настройка административной дистанции для маршрутов DHCP-протокола на стр. 165);

- метрика по умолчанию (см. Настройка метрики для маршрутов DHCP-протокола на стр. 165);
- сетевые интерфейсы, на которых включен режим DHCP;
- специфичные метрики на сетевых интерфейсах, если такие заданы;
- разрешение на автоматическое получение IP-адресов, адресов DNS- и NTP-серверов.

Чтобы посмотреть указанные настройки, выполните команду:

```
hostname> inet show dhcp client
```

В результате выполнения команды указанные настройки будут отражены в следующем виде:

```
xf-va-15ea000a# inet show dhcp client
Administrative distance for DHCP/PPP routes: 80
Default metric for DHCP/PPP routes: 60

Interface  DHCP  Routes  Metric   DNS  NTP
---------  ----  ------  ------   ---  ---
     eth0   yes     yes  default  yes  yes
     eth1   yes     yes       50  yes  yes
     eth2    no     yes  default  yes  yes
     eth3   yes      no  default  yes  yes
xf-va-15ea000a#
```

Рисунок 19. Просмотр настроек DHCP-режима

Просмотр маршрутов DHCP-протокола

Если вы хотите просмотреть список маршрутов, полученных от DHCP-сервера и добавленных в RIB, выполните команду:

```
hostname> inet show routing dhcp
```

В результате выполнения команды появится список маршрутов в следующем виде:

```
xf-va-16310046# inet show routing dhcp
DHCP routes currently available: (* = RIB route)
>* 0.0.0.0/0 [35/23] via 10.1.30.5, eth1
>* 10.100.1.0/24 [30/23] via 10.1.30.201, eth1
>* 10.100.2.0/24 [30/23] via 10.1.30.202, eth1
 *                      via 10.1.30.202, eth1
xf-va-16310046#
```

Рисунок 20. Просмотр маршрутов DHCP-сервера

В списке для каждого маршрута указаны: атрибут, IP-адрес назначения, маска сети, шлюз и имя сетевого интерфейса, на который поступил маршрут. Если маршрут добавлен в таблицу RIB, то перед ним стоит атрибут «*».

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;
- 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 по протоколу OSPF.

Настройка протокола OSPF

Для настройки протокола OSPF выполните следующие действия:

1 Включите использование протокола с помощью команды:

```
hostname# inet ospf mode on
```

2 Укажите сеть, в которой осуществляется обмен информацией по протоколу OSPF, с помощью команды:

```
hostname# inet ospf network add <IP-адрес назначения> netmask <маска сети> area <0-4294967295>,
```

К данной сети должен быть подключен сетевой интерфейс ViPNet xFirewall.

С помощью параметра `area` задайте область маршрутизации, в которую входит ViPNet xFirewall (см. Общие сведения о протоколе OSPF на стр. 158).

Примечание. Вы можете указать не более 128 сетей, в которых осуществляется обмен информацией по протоколу OSPF.

---

3 Создайте на ViPNet xFirewall следующие сетевые фильтры открытой сети:

- Фильтры, разрешающие входящий однонаправленный (unicast) IP-трафик и многоадресный (multicast) IP-трафик по протоколу OSPF от всех соседних OSPF-маршрутизаторов, с которыми взаимодействует ViPNet xFirewall:

  ```
  hostname# firewall local add 1 rule "Rule 1" src <IP-адрес OSPF-маршрутизатора> dst @local service @OSPF pass
  ```

  ```
  hostname# firewall local add 2 rule "Rule 2" src <IP-адрес OSPF-маршрутизатора> dst @multicast service @OSPF 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 на любой IP-адрес назначения:

  ```
  hostname# firewall local add 3 rule "Rule 3" src @local dst @any service @OSPF pass
  ```

4 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:

  ```
  hostname# firewall vpn add 1 rule "Rule 1" src @any dst @any service @OSPF pass
  ```

- Между двумя и более ViPNet xFirewall установлены связи на уровне пользователей — фильтры добавляются на этих (двух и более) ViPNet xFirewall:

  ```
  hostname# firewall vpn add 1 rule "Rule 1" src @any dst @any service @OSPF pass
  ```

Подробнее о создании сетевых фильтров см. в разделе Создание сетевого фильтра (на стр. 81).

Внимание! Если вы не настроите указанные фильтры, то ViPNet xFirewall не сможет работать по протоколу OSPF (см. Общие сведения о протоколе OSPF на стр. 158).

Если впоследствии потребуется отказаться от использования протокола OSPF для маршрутизации, выполните команду:

```
hostname# inet ospf mode off
```

Если в подсети прекращено использование протокола OSPF, удалите ее. Для этого выполните команду:

```
hostname# inet ospf network delete <IP-адрес назначения> netmask <маска сети> area
<0-4294967295>
```

При необходимости вы можете посмотреть параметры настройки протокола OSPF, а также информацию о маршрутизаторах, работающих по протоколу OSPF и связях между ними. Подробнее см. раздел Просмотр настроек протокола OSPF (на стр. 172).

Настройка перераспределения маршрутов

Протокол OSPF позволяет осуществлять перераспределение (redistribute) маршрутов. В каких случаях это может требоваться?

В одной разветвленной сети может быть образовано нескольких автономных систем (см. глоссарий, стр. 273) 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 21. 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. 158), 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 включить перераспределение маршрутов на ViPNet xFirewall, выполните команду:

```
hostname# inet ospf redistribute add {static | dhcp}
```

указав один из параметров:

- `static` — включение перераспределения статических маршрутов;
- `dhcp` — включение перераспределения маршрутов от DHCP-сервера.

Если перераспределение указанного типа маршрутов было включено ранее, появится соответствующее сообщение.

Чтобы выключить перераспределение маршрутов, выполните команду:

```
hostname# inet ospf redistribute delete {static | dhcp}
```

В параметрах протокола OSPF указывается, настроено перераспределение маршрутов или нет. Подробнее см. раздел Просмотр настроек протокола OSPF (на стр. 172).

Просмотр настроек протокола OSPF

Вы можете просмотреть следующие параметры протокола OSPF:

- статус использования протокола OSPF: включен или выключен;
- список сетей, в которых ViPNet xFirewall осуществляет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
- статус перераспределения маршрутов: доступно или недоступно.

Чтобы посмотреть указанные настройки, выполните команду:

```
hostname> inet show ospf configuration
```

В результате выполнения команды указанные настройки будут отображены в следующем виде:

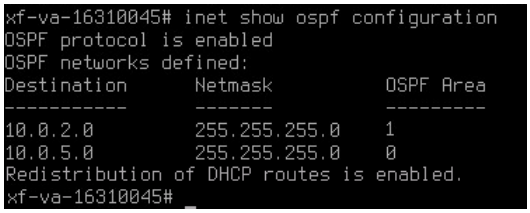


Рисунок 22. Просмотр настроек протокола OSPF

Просмотр информации о соседних маршрутизаторах

При составлении маршрутов по протоколу OSPF участвуют все OSPF-маршрутизаторы, находящиеся в области маршрутизации ViPNet xFirewall. При необходимости вы можете

просмотреть сведения об OSPF-маршрутизаторах, которые являются соседними для ViPNet xFirewall. Для этого выполните команду:

```
hostname> inet show ospf neighbour
```

В результате выполнения команды отобразится информация обо всех соседних OSPF-маршрутизаторах:

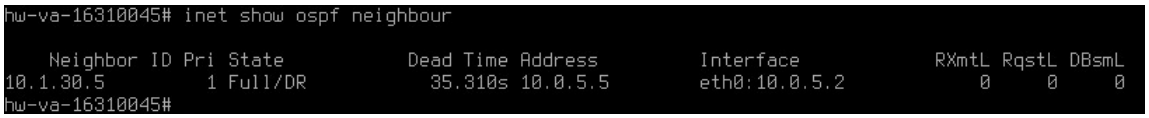


Рисунок 23. Просмотр информации о соседних OSPF-маршрутизаторах

По каждому маршрутизатору отображается следующая информация:

- уникальный идентификатор OSPF-маршрутизатора, под которым он известен другим маршрутизаторам при работе по протоколу OSPF;
- приоритет маршрутизатора;
- тип маршрутизатора (см. Общие сведения о протоколе OSPF на стр. 158) (в случае, приведенном на рисунке, маршрутизатор-сосед является назначенным, на что указывает значение `DR` в поле `State`);
- интервал простоя маршрутизатора, по истечении которого он будет считаться неактивным (выключенным);
- IP-адрес маршрутизатора, по которому он доступен для обмена информацией по протоколу OSPF;
- IP-адрес активного сетевого интерфейса маршрутизатора;
- другие параметры.

Просмотр маршрутов, сформированных по протоколу OSPF

Если вы хотите просмотреть список динамических маршрутов, сформированных по протоколу OSPF и присутствующих в RIB, выполните команду:

```
hostname> inet show routing ospf
```

В результате выполнения команды появится списки маршрутов в трех разделах:

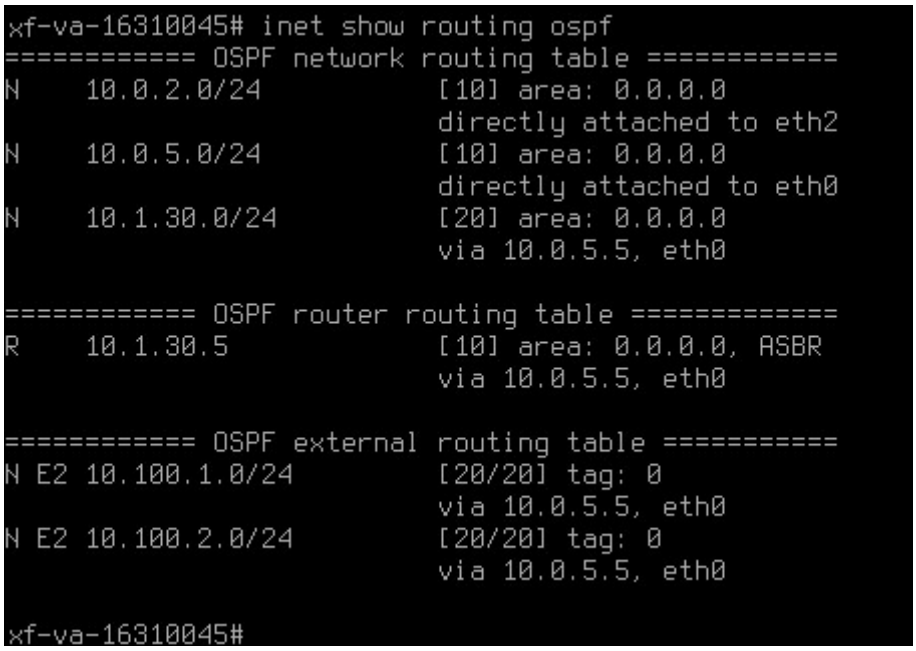


Рисунок 24. Просмотр маршрутов протокола OSPF

В каждом из разделов отображаются следующие маршруты:

- `OSPF network routing table` — маршруты, которые были сформированы по OSPF-протоколу в той области маршрутизации, к которой подключен ViPNet xFirewall. Если ViPNet xFirewall является межобластным маршрутизатором (ABR) (см. Общие сведения о протоколе OSPF на стр. 158), то в этом разделе будут присутствовать маршруты из всех областей, которые он объединяет.
- `OSPF router routing table` — маршруты до соседних OSPF-маршрутизаторов, которые находятся в области маршрутизации ViPNet xFirewall и выполняют перераспределение маршрутов.
- `OSPF external routing table` — маршруты в другие автономные системы, поступившие при перераспределении от соседних OSPF-маршрутизаторов.

10

Настройка транспортного модуля

Назначение и функциональность транспортного модуля

Транспортный модуль (см. глоссарий, стр. 276) предназначен для надежной и безопасной передачи транспортных конвертов между ViPNet xFirewall и сетевыми узлами с установленным административным ПО (ViPNet Центр управления сетью (см. глоссарий, стр. 272), ViPNet Policy Manager (см. глоссарий, стр. 272)) посредством протоколов TCP (этот канал передачи называется MFTP) и SMTP/POP3. Транспортный модуль входит в состав ViPNet xFirewall в виде демона mftpd и программы mailtrans.

Транспортные конверты представляют собой файлы с данными, которыми обмениваются между собой приложения, входящие в состав ПО ViPNet. Размер конверта, передаваемый транспортным модулем, не может превышать 2 Гбайт (2 097 151 Кбайт). Транспортный модуль передает конверты в соответствии с адресами получателей, прописанными в заголовках этих конвертов.

Для обмена транспортными конвертами на узлах сети ViPNet могут использоваться каналы следующих типов:

- MFTP — при связи по такому каналу узел-отправитель конвертов устанавливает TCP-соединение с узлом-получателем конвертов, проводится взаимная аутентификация узлов и осуществляется передача конвертов между узлами через транспортные серверы. Данный тип канала по умолчанию устанавливается для узлов сети ViPNet.
- SMTP/POP3 — при связи по такому каналу транспортный модуль переадресует конверты для отправки модулю почтового обмена MailTrans, который передает их через сервер SMTP, а также забирает с сервера POP3 конверты, предназначенные для данного узла. То есть канал SMTP/POP3 позволяет использовать для обмена транспортными конвертами почтовые серверы, что удобно, например, в случае передачи конвертов между сетевыми узлами разных организаций, в которых по каким-либо причинам затруднен выход в Интернет по TCP-каналам (см. Настройка взаимодействия с модулем почтового обмена на стр. 178).
- Viaserv — такой канал используется для связи с узлами доверенной сети (см. глоссарий, стр. 274), если настроено межсетевое взаимодействие. При этом транспортный модуль передает и получает конверты от узлов доверенной сети через шлюзовой координатор. Данный тип канала по умолчанию задается для координаторов доверенной сети при установлении межсетевого взаимодействия.

Настройка транспортного модуля выполняется путем редактирования конфигурационного файла `mftp.conf`. Подробнее о параметрах, содержащихся в файле `mftp.conf`, см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».

Выбор канала передачи конвертов

По умолчанию для обмена конвертами с защищенными узлами, связанными с ViPNet xFirewall, используется канал MFTP. Чтобы изменить тип канала на SMTP/POP3, выполните следующие действия:

1. Завершите работу демона mftpd с помощью команды:

   ```
   hostname> mftp stop
   ```

2. Откройте конфигурационный файл `mftp.conf` для редактирования с помощью команды:

   ```
   hostname# mftp config
   ```

3. В секции `[channel]` нужного узла измените следующие параметры:

   - установите параметр `type` в значение `smtp`;
   - в параметре `reportaddress` укажите адрес электронной почты для отправки исходящих конвертов в формате:

     ```
     <имя пользователя>@<сервер>.<домен>
     ```

4. Чтобы сохранить изменения в файле `mftp.conf`, нажмите сочетание клавиш **Ctrl+O**. Затем нажмите клавишу **Enter**.
5. Чтобы закрыть файл, нажмите сочетание клавиш **Ctrl+X**.
6. Запустите демон mftpd с помощью команды:

   ```
   hostname> mftp start
   ```

Настройка взаимодействия с модулем почтового обмена

Если для каких-либо узлов в вашей организации предполагается использование каналов SMTP/POP3, настройте параметры взаимодействия транспортного модуля с модулем почтового обмена MailTrans. Для этого выполните следующие действия:

1. Завершите работу демона mftpd с помощью команды:

   ```
   hostname> mftp stop
   ```

2. Откройте конфигурационный файл `mftp.conf` для редактирования с помощью команды:

   ```
   hostname# mftp config
   ```

3. В секции `[mailtrans]` укажите значения следующих параметров:

   - `frommailbox` —адрес электронной почты отправителя SMTP-конвертов в формате: `<имя пользователя>@<сервер>.<домен>`
   - `inputmailbox` — адрес электронной почты, по которому модуль почтового обмена будет забирать конверты по протоколу POP3, в формате: `<имя пользователя>:<пароль>@<IP-адрес POP3-сервера>`
   - `outputmailbox` — IP-адрес SMTP-сервера, на который модуль почтового обмена будет отправлять конверты по протоколу SMTP.

4. Чтобы сохранить изменения в файле `mftp.conf`, нажмите сочетание клавиш **Ctrl+O**. Затем нажмите клавишу **Enter**.

5. Чтобы закрыть файл, нажмите сочетание клавиш **Ctrl+X**.

6. Запустите демон mftpd с помощью команды:

   ```
   hostname> mftp start
   ```

Настройка протоколирования событий транспортного модуля

Демон mftpd записывает информацию о событиях, происходящих в процессе работы транспортного модуля, в журнал событий.

Чтобы изменить параметры записи событий в журнал событий транспортного модуля, выполните следующие действия:

1 Завершите работу демона mftpd с помощью команды:

```
hostname> mftp stop
```

2 Откройте файл `mftp.conf` для редактирования с помощью команды:

```
hostname# mftp config
```

3 В секции `[debug]` при необходимости измените значения следующих параметров:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от `1` до `5` (по умолчанию `3`). Чем выше уровень детализации, тем более подробная информация выводится в журнал. Значение параметра `-1` выключает ведение журнала.

  Не рекомендуется задавать уровень детализации выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ОАО «ИнфоТеКС».

  - `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:

    - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы), `mail` (почтовая система) или `daemon` (демоны).
    - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

    Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

1 Запустите демон mftpd с помощью команды:

```
hostname> mftp start
```

11

Обеспечение отказоустойчивости

Настройка системы защиты от сбоев

Назначение и принципы работы системы защиты от сбоев

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNet xFirewall и создания отказоустойчивого решения на базе узлов ViPNet xFirewall. Данная система может работать в одиночном режиме (см. Работа системы защиты от сбоев в одиночном режиме на стр. 181) или в режиме кластера горячего резервирования.

Настройка системы защиты от сбоев выполняется путем редактирования конфигурационного файла `failover.ini`. Подробнее о параметрах, содержащихся в этом файле см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».

Работа системы защиты от сбоев в одиночном режиме

По умолчанию после установки программы ViPNet xFirewall система защиты от сбоев работает в одиночном режиме. При этом данная система обеспечивает постоянную работоспособность программы, выполняя следующие функции:

- контроль собственной работоспособности;
- контроль работоспособности демонов и драйверов ViPNet xFirewall, ведение статистики использования системных ресурсов;
- контроль сбоев при обработке пакетов драйвером ViPNet.

Данные функции реализуются watchdog-драйвером itcswd и демоном failoverd. При загрузке системы сначала запускается watchdog-драйвер, а затем демон failoverd, который запускает остальные демоны и драйверы ViPNet xFirewall. Watchdog-драйвер и демон failoverd работают постоянно в фоновом режиме.

Watchdog-драйвер отвечает за контроль собственной работоспособности системы защиты от сбоев, то есть работоспособности демона failoverd. В зависимости от настроек (подробнее см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», описании секции `[misc]` файла `failover.ini`) при запуске демон failoverd может регистрироваться watchdog-драйвером. В этом случае в процессе своей работы он периодически посылает драйверу сообщения для подтверждения своей работоспособности. Если по истечении определенного времени от демона не будет получено ни одного сообщения, драйвер инициирует перезагрузку системы.

Демон failoverd отвечает за контроль работоспособности остальных демонов и драйверов ViPNet xFirewall. В зависимости от настроек (подробнее см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», описании секции `[misc]` файла `failover.ini`) при запуске демоны ViPNet xFirewall могут регистрироваться демоном failoverd. В этом случае в процессе своей работы каждый из них периодически посылает демону failoverd сообщения для подтверждения своей работоспособности. Если по истечении определенного времени от какого-либо демона не будет получено ни одного сообщения или от драйвера ViPNet будет получено сообщение с кодом ошибки обработки пакетов, демон failoverd считает, что произошел сбой и пытается завершить работу этого демона. Если завершить работу корректно не удается, демон failoverd производит принудительный перезапуск. Если после пяти перезапусков подряд, работу контролируемого демона восстановить не удалось, он считается неработоспособным, и демон failoverd инициирует перезапуск системы.

Примечание. Система защиты от сбоев контролирует работоспособность только запущенных демонов и драйверов ViPNet xFirewall.

Работа системы защиты от сбоев в режиме кластера горячего резервирования

Помимо контроля работоспособности программы ViPNet xFirewall (см. Работа системы защиты от сбоев в одиночном режиме на стр. 181), в режиме кластера горячего резервирования система защиты от сбоев позволяет передавать функции вышедшего из строя сервера другому (резервному) серверу. Кластер горячего резервирования состоит из двух взаимосвязанных серверов ViPNet xFirewall:

- активного сервера, который работает в активном режиме;
- пассивного сервера, который работает в пассивном режиме, то есть в режиме ожидания.

В случае сбоев, критичных для работоспособности ViPNet xFirewall на активном сервере, пассивный сервер переключается в активный режим и выполняет функции сбойного сервера, который после перезагрузки переходит в пассивный режим.

При работе в режиме кластера горячего резервирования некоторые функции ViPNet xFirewall недоступны.

Внимание! На обоих серверах кластера горячего резервирования должна быть установлена одна и та же версия ПО ViPNet xFirewall, а также справочники одного и того же узла. Оба сервера должны иметь одинаковую аппаратную платформу.

Если вы развертываете кластер на базе ViPNet xFirewall xF-VA, оба сервера должны иметь одинаковые параметры эмулируемого аппаратного обеспечения: количество процессоров, ОЗУ и сетевых интерфейсов.

Каждый сетевой интерфейс кластера горячего резервирования имеет один IP-адрес, по которому кластер доступен для других узлов. Этот IP-адрес всегда принадлежит серверу, работающему в данный момент в активном режиме. Сетевые интерфейсы сервера, работающего в пассивном

режиме, имеют другие IP-адреса, которые не используются другими узлами для установления соединения с кластером. Причем каждый сетевой интерфейс пассивного сервера имеет индивидуальный IP-адрес и, чтобы после перезагрузки каждый интерфейс сервера получал свой IP-адрес для работы в пассивном режиме, администратор сети ViPNet должен соответствующим образом настроить стек IP на серверах кластера.

Внимание! При работе с типовой схемой кластера горячего резервирования все используемые IP-адреса (IP-адрес активного сервера и два IP-адреса пассивного сервера) должны быть статическими и находиться в одном адресном пространстве. Если возможности по выделению IP-адресов в сети ограничены, может применяться схема, рассчитанная на выделение одного реального IP-адреса для активного сервера (подробнее см. раздел (см. Схема организации кластера в условиях ограничений по выделению IP-адресов на стр. 195) настоящего документа).

При запуске кластера активным становится тот сервер, который запускается быстрее. После загрузки пассивный сервер периодически посылает в сеть запросы на IP-адреса активного сервера. Если ни один из IP-адресов недоступен в течение заданного времени (то есть активный сервер не найден в сети), пассивный сервер переходит в активный режим. При этом ему назначается IP-адрес активного сервера.

Активный сервер в процессе работы периодически контролирует работоспособность своих интерфейсов, анализируя IP-трафик, проходящий через каждый из них. Если количество IP-пакетов, зарегистрированных по истечении определенного интервала времени, больше количества IP-пакетов, которое было зарегистрировано к моменту начала этого интервала времени, то считается, что интерфейс работает нормально, и счетчик отказов для этого интерфейса сбрасывается. Если в течение этого интервала времени не было ни отправлено, ни принято ни одного пакета, то производится дополнительная проверка — через каждый интерфейс посылаются эхо-запросы стабильным объектам сети (например, маршрутизатору). Если на какой-либо из интерфейсов в течение заданного времени не пришло ответа ни на один эхо-запрос, счетчик отказов для этого интерфейса увеличивается на единицу. При достижении счетчиком определенного значения интерфейс считается неработоспособным, и активный сервер перезагружается. Во время перезагрузки активный сервер становится недоступен, при этом пассивный сервер переходит в активный режим. После перезагрузки сервер, работавший в активном режиме, переходит в пассивный режим.

Примечание. Если стабильные объекты сети находятся в открытой сети, то для отправки эхо-запросов и получения ответов на серверах ViPNet xFirewall автоматически создаются соответствующие разрешающие фильтры открытой сети для протокола ICMP.

При работе сервера в активном режиме эхо-запросы для контроля работоспособности его интерфейсов могут посылаться постоянно (подробнее см. в описании файла `failover.ini` в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам»).

Для поддержания справочников, конфигурационных файлов и журналов на обоих серверах ViPNet xFirewall в актуальном состоянии между серверами должен быть создан и настроен выделенный Ethernet-канал (резервный канал), по которому копии файлов с активного сервера будут периодически передаваться на пассивный. Кроме того, по резервному каналу активный сервер

передает пассивному копии принятых и готовых к отправке MFTP-конвертов, и серверы обмениваются пакетами синхронизации, содержащими информацию о текущем режиме работы каждого из них. Обмен пакетами синхронизации позволяет избежать ситуации, когда оба сервера кластера работают в активном режиме (например, в случае практически одновременного запуска). Резервный канал используется только для передачи файлов и пакетов с целью резервирования, данные передаются по резервному каналу в открытом виде. Система защиты от сбоев не контролирует работоспособность резервного канала.

Внимание! Адреса резервного канала на серверах кластера не должны совпадать с адресами узлов сети ViPNet, иначе трафик, идущий на эти адреса, будет блокироваться. Если необходимо использовать одинаковые адреса, для разрешения конфликта рекомендуется настроить видимость соответствующих узлов сети ViPNet по виртуальным адресам.

На пассивном сервере кластера блокируется любой защищенный трафик, а также любой открытый трафик, кроме обмена данными по резервному каналу и периодического опроса адресов активного сервера. Сетевые фильтры, разрешающие такой открытый трафик между соответствующими интерфейсами серверов, создаются в ViPNet xFirewall автоматически.

Функции ViPNet xFirewall, недоступные в режиме кластера горячего резервирования

В режиме кластера недоступны следующие сетевые службы ViPNet xFirewall:

- DHCP-сервер.
- Служба DHCP-relay.

Перед переключением в режим кластера горячего резервирования необходимо отключить перечисленные функции.

Развертывание кластера горячего резервирования

Перед развертыванием кластера горячего резервирования:

1. Убедитесь в наличии двух серверов, каждый из которых имеет минимум три сетевых интерфейса: для доступа во внешнюю сеть, для доступа во внутреннюю сеть и для организации резервного канала.
2. На обоих серверах установите одинаковую версию программного обеспечения ViPNet xFirewall, одинаковые справочники и лицензия (подробнее см. в документе «ViPNet xFirewall. Подготовка к работе»).
3. Настройте параметры сетевых интерфейсов, соблюдая следующие ограничения:

- Для сетевых интерфейсов, задействованных в работе кластера горячего резервирования, должны быть заданы статические IP-адреса. Назначение IP-адресов по протоколу DHCP не допускается.

Примечание. В качестве резервируемых сетевых интерфейсов вы можете задать как физические, так и виртуальные или VLAN интерфейсы. В данном сценарии используются только физические сетевые интерфейсы.

- Во избежание конфликтов при копировании конфигурационных файлов с активного сервера на пассивный требуется, чтобы имена интерфейсов, используемых для доступа к соответствующим сетям, совпадали.
- В соответствующих секциях файла `failover.ini` должны быть указаны все сетевые интерфейсы класса `access`, описанные секциями `[adapter]` в файле `iplir.conf`.

Примечание. В качестве резервируемых сетевых интерфейсов можно задать только интерфейсы класса `access`. Указывать в файле `failover.ini` сетевые интерфейсы классов `trunk` и `slave` не следует.

4. Между ViPNet xFirewall создайте резервный канал для передачи файлов с целью резервирования. Необходимо настроить систему так, чтобы при ее перезапуске связь по резервному каналу устанавливалась автоматически.
5. Выберите один или несколько стабильных объектов сети (например, маршрутизатор), которые будут использоваться для проверки работоспособности интерфейсов активного ViPNet xFirewall.

Для развертывания кластера на каждом из ViPNet xFirewall выполните следующие действия:

1. Завершите работу демона системы защиты от сбоев командой:

```
hostname> failover stop
```

2. Откройте файл `failover.ini` для редактирования с помощью команды:

```
hostname# failover config edit
```

3. В файле `failover.ini` для сетевых интерфейсов класса `access`, которые используются для взаимодействия с узлами внутренней и внешней сетей, в соответствующих секциях `[channel]` укажите значения следующих параметров:
   - `device` — имя интерфейса.
   - `activeip` — IP-адрес и маска, которые интерфейс будет иметь в активном режиме.
   - `passiveip` — IP-адрес и маска, которые интерфейс будет иметь в пассивном режиме.
   - `testip` — IP-адрес маршрутизатора или другого стабильного объекта сети, которому будут посылаться эхо-запросы для проверки работоспособности интерфейса.

     При необходимости можно для каждого из интерфейсов указать несколько параметров `testip`. В этом случае сбоем интерфейса будет считаться ситуация, когда ни от одного из заданных IP-адресов не будет получено ответа.

Например, чтобы эхо-запросы отправлялись на IP-адреса 192.168.100.34 и 192.168.100.25, добавьте следующие строки:

```
testip = 192.168.100.34
testip = 192.168.100.25
```

- `ident` — текстовая строка, идентифицирующая интерфейс. Для интерфейсов, подключенных к одинаковым сетям, параметры `ident` должны совпадать.

Внимание! На серверах кластера значения параметров `ident`, `activeip` и `testip` должны быть одинаковыми, а значения параметров `passiveip` — разными. IP-адрес, указанный в параметре `passiveip` каждого сервера, должен совпадать с IP-адресом, который установлен для соответствующего интерфейса в системе.

В качестве параметра `testip` не рекомендуется задавать адрес интерфейса «внутренней петли» (loopback), например `127.0.0.1` или `localhost`, так как в этом случае реальной проверки работоспособности сетевого интерфейса не производится.

- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов. Возможные значения: `yes` (по умолчанию) — активный сервер посылает эхо-запросы на интерфейсы, адреса которых указаны в параметрах `testip`, только если за период опроса IP-адресов на данных интерфейсах не было или входящих, или исходящих пакетов; `no` — эхо-запросы на интерфейсы, адреса которых указаны в параметрах `testip`, посылаются всегда.

4 В файле `failover.ini` в секции `[sendconfig]` задайте следующие параметры, контролирующие пересылку файлов с активного сервера на пассивный с целью резервирования:

- `device` — системное имя интерфейса, который используется для организации резервного канала.
- `activeip` — адрес резервного канала другого сервера кластера (который работает в режиме, противоположном режиму данного сервера).

5 При необходимости измените другие параметры секции `[sendconfig]` и параметры работы системы защиты от сбоев, относящиеся к посылке пакетов в сеть, в секции `[network]` файла `failover.ini`.

6 Чтобы сохранить изменения в файле `failover.ini`, нажмите сочетание клавиш **Ctrl+O**. Затем нажмите клавишу **Enter**.

7 Чтобы закрыть файл, нажмите сочетание клавиш **Ctrl+X**.

8 Переведите систему защиты от сбоев в режим кластера горячего резервирования с помощью команды:

```
hostname# failover config mode cluster
```

Примечание. При переключении в режим кластера горячего резервирования проверяется текущее состояние локального DHCP-сервера. Если DHCP-сервер запущен или в настройках включен его автоматический запуск, то появляется предупреждение о необходимости предварительно завершить работу DHCP-сервера или выключить его автоматический запуск.

9 Запустите демон системы защиты от сбоев командой:

```
hostname> failover start
```

В результате кластер начнет свою работу, и на серверах ViPNet xFirewall будут автоматически созданы нередактируемые сетевые фильтры, необходимые для корректной работы системы защиты от сбоев с выбранными параметрами.

Примеры настройки кластера горячего см. в разделе (см. Пример использования кластера горячего резервирования на стр. 192) настоящего документа.

Запуск и завершение работы демона системы защиты от сбоев

Чтобы запустить демон системы защиты от сбоев failoverd на одиночном сервере, выполните команду:

```
hostname> failover start
```

Чтобы запустить демон failoverd на сервере кластера горячего резервирования, выполните одну из команд:

- Для запуска в активном режиме:

  ```
  hostname> failover start active
  ```

- Для запуска в пассивном режиме:

  ```
  hostname> failover start passive
  ```

Внимание! Если при запуске демона failoverd на сервере кластера горячего резервирования вы не укажете параметр `active` или `passive`, то демон будет запущен в том режиме, в котором он находился до завершения работы.

Перед запуском демона системы защиты от сбоев на сервере кластера горячего резервирования в активном или пассивном режиме убедитесь в том, что второй сервер кластера работает в противоположном режиме. Запуск обоих серверов кластера в активном режиме вызовет конфликт IP-адресов и другие неполадки.

Чтобы завершить работу демона failoverd, выполните команду:

```
hostname> failover stop
```

Просмотр информации о работе системы защиты от сбоев

Просмотр текущего состояния системы защиты от сбоев

Для просмотра информации о текущем состоянии системы защиты от сбоев узла:

```
hostname> failover show info
```

В результате выводится следующая информация об узле:

- версии ПО ViPNet xFirewall и демона failoverd, установленных на узле (`versions`);
- идентификатор и имя узла (`ID`);
- локальное время на узле (`workstation time`);
- режим работы системы защиты от сбоев узла (`failover mode`):
  - `single` — одиночный режим работы;
  - `active` — активный режим работы в составе кластера горячего резервирования;
  - `passive` — пассивный режим работы в составе кластера горячего резервирования;
- время непрерывной работы демона failoverd (`failover uptime`);
- общая загруженность процессора в процентах (`total cpu`);
- общий объем памяти в килобайтах (`total memory`);
- общий объем свободной памяти в килобайтах (`free memory`);
- сведения о текущем состоянии демонов ViPNet xFirewall:
  - `initializing` – загружается;
  - `works` — работает;
  - `stopped` — работа завершена;
  - `unknown` — неизвестно (например, если произошел сбой в работе демона, была произведена попытка его перезапуска, и данных о его состоянии пока нет);
- сведения о ресурсах процессора, используемых каждым из этих демонов, в процентах (`failover cpu`, `iplir cpu` и так далее).

Примечание. В случае просмотра информации о текущем состоянии системы защиты от сбоев на узле, работающем в составе кластера горячего резервирования, статистика использования системных ресурсов и текущее состояние демонов ViPNet xFirewall отображаются для обоих серверов кластера (в столбце `local` — для сервера, на котором выполнена команда, в столбце `remote` — для второго сервера кластера, см. пример ниже).

Например, если демон failoverd работает в одиночном режиме, выводится следующая информация:

```
Versions: ViPNet 4.1.0 (570), daemon 1.5 (1)
Workstation configured for ID 29A0022 (xF)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1479217050) Thu May 8 16:37:30 2018

failover mode     * single
failover uptime   * 6d  0:23
total cpu         * 11%
total memory      * 2055840 kB
free memory       * 1883540 kB
failover state    * works
failover cpu      * 0%
iplir state       * works
iplir cpu         * 46%
mftp state        * works
mftp cpu          * 40%
webgui state      * works
webgui cpu        * 0%
dpi state         * works
dpi cpu           * 3%
uc state          * works
uc cpu            * 5%
```

Если демон failoverd работает в режиме кластера горячего резервирования, выводится следующая информация:

```
Versions: ViPNet 4.1.0 (570), daemon 1.5 (1)
Workstation configured for ID 29A0022 (xF)
Workstation works in a cluster mode of protection against failures
Workstation time (utc: 1479217050) Thu May 8 16:37:30 2018
                        * local      * remote
failover mode           * active     * passive
failover uptime         * 3d  5:26   * 0d  0:00
total cpu               * 80%        * 0%
total memory            * 2044104 kB * 2044104 kB
free memory             * 1672360 kB * 1672360 kB
failover state          * works      * works
failover cpu            * 7%         * 0%
iplir state             * works      * works
iplir cpu               * 0%         * 0%
mftp state              * works      * works
mftp cpu                * 66%        * 0%
webgui state            * works      * stopped
webgui cpu              * 0%         * 0%
dpi state               * works      * works
dpi cpu                 * 3%         * 3%
```

Если демон failoverd не работает, выводится только информация о его режиме. Например:

```
Failover is in single mode
```

Просмотр журнала переключений

События о работе системы защиты от сбоев в режиме кластера горячего резервирования, записываются демоном failoverd в журнал переключений. Среди таких событий:

- <BOOT> — запуск демона failoverd при загрузке операционной системы;
- <P_START> — ручной запуск демона failoverd в пассивном режиме;
- <A_START> — ручной запуск демона failoverd в активном режиме;
- <SWITCH> — переход сервера из пассивного режима работы в активный (или наоборот).

Для просмотра записей в журнале переключений сервера, выполните команду:

```
hostname> failover view <дд.мм.гггг[.чч.мм.сс]> <дд.мм.гггг[.чч.мм.сс]>,
```

указав начало и конец интервала времени, записи за который вас интересуют. Например:

```
failover view 08.11.2016.00.00.00 23.11.2016.16.37.00
```

В результате выполнения команды выводится следующая информация:

- версии ПО ViPNet xFirewall и демона failoverd;
- идентификатор и имя сервера;
- указание на работу системы защиты от сбоев в режиме кластера горячего резервирования;
- локальные дата и время на сервере;
- список записей за выбранный интервал времени (дата, время, идентификатор и описание события).

Данная информация выводится в следующем формате:

```
View journal of failover switching
Versions: ViPNet 4.1.0 (570), daemon 1.5 (1)
Workstation configured for ID 29A0022 (xF)
The workstation works in a cluster mode of protection against failures
Workstation time (utc: 1479217050) Thu May 8 16:37:30 2018

09 Nov 2016 12:51:42    <P_START> Start failover daemon in passive mode
22 Nov 2016 12:27:27    <A_START> Start failover daemon in active mode
22 Nov 2016 14:10:35    <A_START> Start failover daemon in active mode
22 Nov 2016 15:30:46    <BOOT> Boot the system
23 Nov 2016 11:09:07    <SWITCH> Switch server from passive mode to active mode
```

Если за указанный интервал времени не произошло ни одного события, выводится следующее сообщение:

```
There are no records in journal of switchings
```

Работа кластера горячего резервирования совместно с коммутационным оборудованием

На практике часто применяются схемы подключения кластера горячего резервирования к коммутаторам, маршрутизаторам и другому коммутационному оборудованию. Настройки данного оборудования могут влиять на работу кластера горячего резервирования. В частности, администратор такого оборудования может настроить блокирование тех или иных сетевых пакетов, среди которых могут оказаться служебные пакеты, необходимые для корректного функционирования ViPNet xFirewall в режиме кластера горячего резервирования.

В связи с этим при использовании коммутационного оборудования с кластером горячего резервирования необходимо убедиться в следующем:

- На оборудовании пропускаются эхо-запросы ICMP с IP-адресов активного сервера до всех узлов с IP-адресами, заданными в параметрах `testip` секции `[channel]` файла `failover.ini`, и ответы на них.
- На оборудовании отключена функция Proxy ARP и пропускаются ARP-запросы с IP-адресов пассивного сервера до IP-адресов активного сервера и ответы на них.

Данные рекомендации касаются всех сетевых интерфейсов ViPNet xFirewall, для которых в файле `failover.ini` существует секция `[channel]`.

Пример использования кластера горячего резервирования

Типовая схема организации кластера

Пример типовой схемы организации кластера горячего резервирования приведен ниже. Интерфейсы eth0 используются для организации резервного канала.

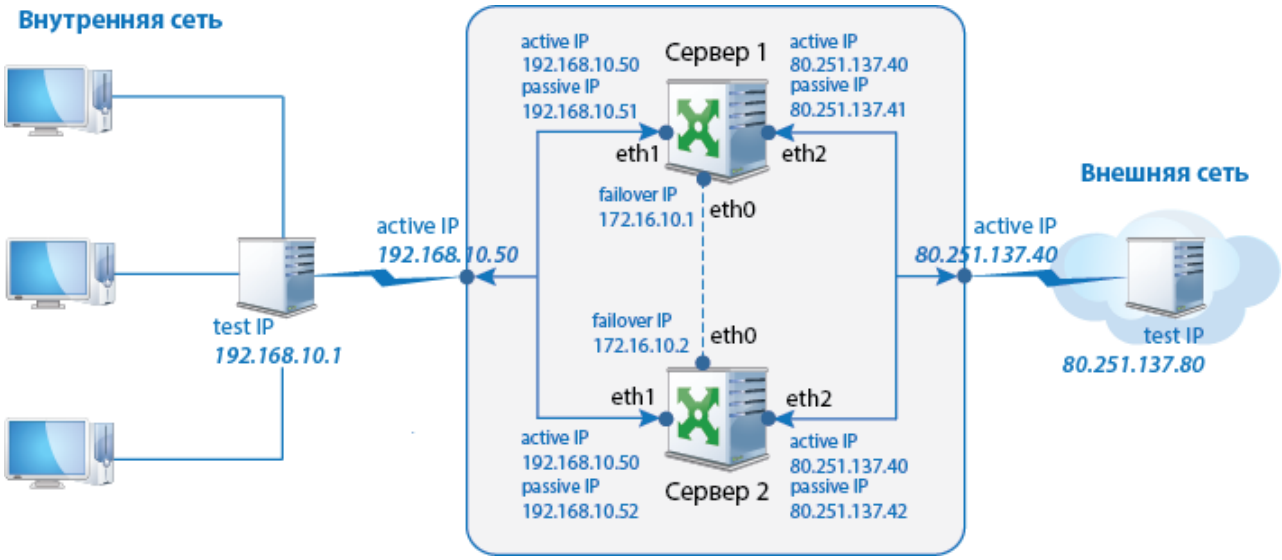


Рисунок 25. Типовая схема организации кластера горячего резервирования

Параметры работы системы защиты от сбоев настраиваются в конфигурационном файле `failover.ini`, содержащем несколько секций. Для настройки кластера предназначены параметры секций `[channel]`, `[network]` и `[sendconfig]`. Подробнее см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».

В случае использования типовой схемы необходимо соблюдать следующие требования:

- На сетевых интерфейсах, которые задействованы в работе кластера горячего резервирования, должны быть заданы статические IP-адреса. Назначение IP-адресов по протоколу DHCP не допускается.

Примечание. В качестве резервируемых сетевых интерфейсов вы можете задать как физические, так и виртуальные или VLAN интерфейсы. В данном сценарии используются только физические сетевые интерфейсы.

- При настройке параметров в секциях `[channel]` IP-адреса, указанные в параметрах `activeip` и `passiveip` для внутреннего (eth1) и внешнего (eth2) интерфейсов, должны находиться в одной подсети. При этом маску подсети указывать необязательно.

- Значения параметров `ident`, `activeip` и `testip` должны быть одинаковыми на обоих серверах кластера, а параметры `passiveip` должны различаться. Таким образом, в типовой схеме в каждой из сетей, к которым подключены контролируемые интерфейсы кластера, должны быть выделены три IP-адреса: один для `activeip` и два для `passiveip`. IP-адрес, указанный в параметре `passiveip`, должен совпадать с адресом, который установлен для данного интерфейса в системе (командой `inet ifconfig <интерфейс>`).
- Для интерфейсов, подключенных к одинаковым сетям, параметры `ident` должны совпадать на обоих серверах кластера — именно по этим параметрам система защиты от сбоев определяет интерфейсы, которые выполняют одинаковые функции на серверах кластера.

Внимание! Настоятельно рекомендуем назначать одинаковые имена интерфейсам, выполняющим одинаковые функции на серверах кластера. В следующих версиях ViPNet xFirewall параметр `ident` не будет использоваться, и отличающиеся имена интерфейсов приведут к нарушению работоспособности сети ViPNet.

Таблица ниже содержит настройки параметров системы защиты от сбоев для типовой схемы организации кластера.

Таблица 11. Настройки параметров системы защиты от сбоев для типовой схемы организации кластера

Настройки на первом сервере	Настройки на втором сервере
[channel]	**[channel]**
`device = eth1`	`device = eth1`
`activeip = 192.168.10.50`	`activeip = 192.168.10.50`
`passiveip = 192.168.10.51`	`passiveip = 192.168.10.52`
`testip = 192.168.10.1`	`testip = 192.168.10.1`
`ident = if-1`	`ident = if-1`
`checkonlyidle = yes`	`checkonlyidle = yes`
[channel]	**[channel]**
`device = eth2`	`device = eth2`
`activeip = 80.251.137.40`	`activeip = 80.251.137.40`
`passiveip = 80.251.137.41`	`passiveip = 80.251.137.42`
`testip = 80.251.137.80`	`testip = 80.251.137.80`
`ident = if-2`	`ident = if-2`
`checkonlyidle = yes`	`checkonlyidle = yes`
[network]	**[network]**
`checktime = 10`	`checktime = 10`
`timeout = 2`	`timeout = 2`
`activeretries = 3`	`activeretries = 3`

Настройки на первом сервере	Настройки на втором сервере
`channelretries = 3`	`channelretries = 3`
`synctime = 5`	`synctime = 5`
`fastdown = yes`	`fastdown = yes`
[sendconfig]	**[sendconfig]**
`device = eth0`	`device = eth0`
`activeip = 172.16.10.2` (соответствует failover IP второго сервера)	`activeip = 172.16.10.1` (соответствует failover IP первого сервера)

К такой схеме применяется следующий алгоритм работы активного сервера:

1. Каждые `checktime` секунд проверяется работоспособность каждого из указанных в конфигурационном файле интерфейсов.
2. Если параметр `checkonlyidle` установлен в значение `yes`, то анализируется весь сетевой трафик, проходящий через интерфейс.
3. Если в течение `checktime` через интерфейс не прошло ни одного пакета, через этот интерфейс посылаются эхо-запросы на узел с адресом `testip`, и в течение `timeout` ожидаются ответы на эти запросы.
4. Если ни одного ответа не приходит, то счетчик сбоев этого интерфейса увеличивается на единицу, и посылаются новые эхо-запросы. Если на эхо-запрос приходит хотя бы один ответ, то счетчик сбоев интерфейса обнуляется. В случае обнуления счетчиков сбоев всех интерфейсов происходит возврат к началу цикла проверки (ожидание в течение `checktime` и так далее). При достижении счетчиком сбоев какого-либо интерфейса значения `channelretries` интерфейс считается неработоспособным, и система перезагружается.

Примечание. Чтобы эхо-запросы на узел с адресом `testip` посылались каждые `checktime` секунд, установите параметр `checkonlyidle` в значение `no`.

Таким образом, максимальное время, которое нужно системе защиты от сбоев для того, чтобы определить неработоспособность интерфейса, равно:

```
checktime + (timeout * channelretries)
```

К такой схеме применяется следующий алгоритм работы пассивного сервера:

1. Каждые `checktime` секунд из системной ARP-таблицы удаляются записи для `activeip`.
2. Затем со всех интерфейсов посылаются UDP-запросы на узел с адресом `activeip`, точнее система сначала посылает ARP-запрос и только в случае получения ответа на него посылает UDP-запрос.
3. По истечении `timeout` проверяется наличие ARP-записи для каждого `activeip` в системной ARP-таблице и делается вывод о работоспособности соответствующего интерфейса активного сервера.

4 Если ни от одного интерфейса не был получен ответ, счетчик сбоев (один для всех интерфейсов) увеличивается. Если хотя бы от одного интерфейса был получен ответ, счетчик сбоев обнуляется. В случае достижения счетчиком сбоев значения `activeretries`, производится переход сервера в активный режим.

Таким образом, максимальное время, проходящее с момента начала перезагрузки активного сервера до обнаружения пассивным сервером этого факта, равно:

```
checktime + (timeout * activeretries)
```

Минимальное общее время неработоспособности системы при сбое равно:

```
checktime * 2 + timeout * (channelretries + activeretries)
```

Реальное время неработоспособности системы при сбое будет несколько больше. Это связано с тем, что после начала перезагрузки сбойного сервера система переводит его интерфейсы в нерабочее состояние не сразу, а через некоторое время, после завершения работы других подсистем (обычно около 30 секунд).

Схема организации кластера в условиях ограничений по выделению IP-адресов

При отсутствии возможности выделения трех IP-адресов в одной сети для реализации типовой схемы организации кластера горячего резервирования (например, при использовании публичных IP-адресов или в условиях ограниченного адресного пространства сети), можно организовать кластер по схеме, в которой требуется только один IP-адрес для активного сервера. Пример такой схемы приведен ниже.

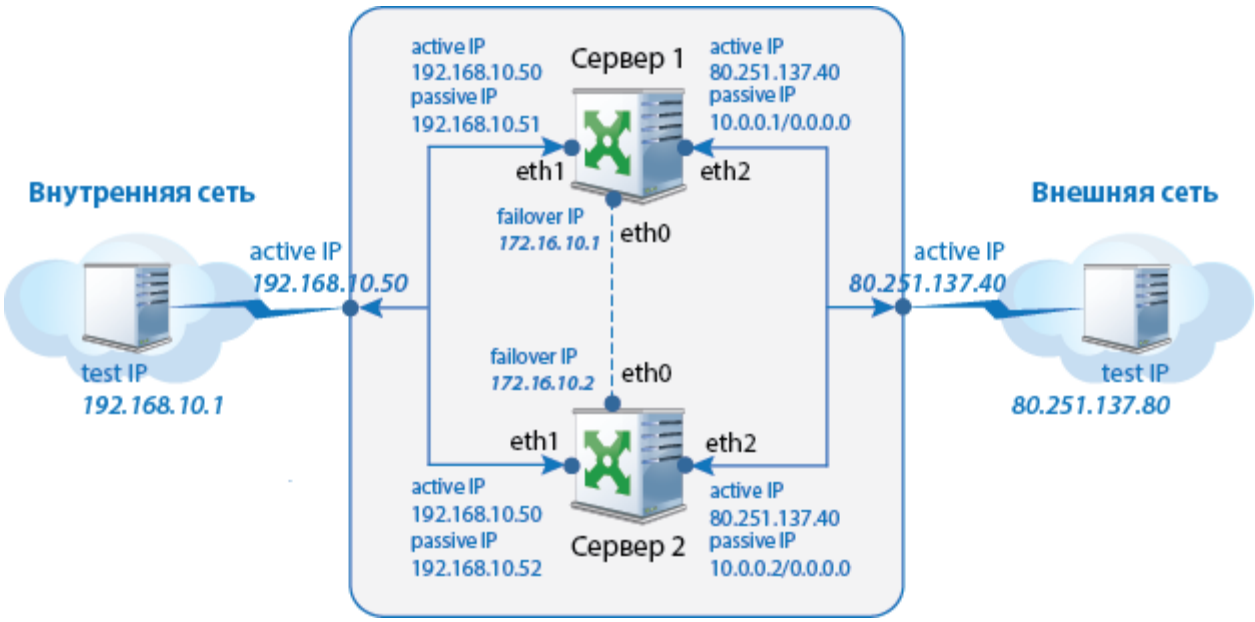


Рисунок 26. Схема организации кластера горячего резервирования в условиях ограничений по выделению IP-адресов

В отличие от типовой схемы в этом случае для внешних интерфейсов (на схеме eth2) вместо трех публичных IP-адресов выделен только один, а адреса пассивных интерфейсов выбраны из диапазона частной сети. Общий принцип работы состоит в том, чтобы использовать на пассивном сервере адреса из другой подсети (например, частной). Чтобы при этом пассивный сервер мог контролировать работоспособность активного путем посылки ARP-запросов, на соответствующих интерфейсах пассивного сервера необходимо установить маску подсети 0.0.0.0 и широковещательный адрес 255.255.255.255.

Примечание. Если на интерфейсе, для которого вы хотите установить маску 0.0.0.0, уже был задан IP-адрес, нужно предварительно очистить настройки адреса интерфейса с помощью команды:

```
hostname# ifconfig <имя интерфейса> reset,
```

Затем вы можете задать нужные IP-адрес и маску с помощью команды:

```
hostname# ifconfig <имя интерфейса> address <IP-адрес> netmask 0.0.0.0
```

Таким образом, при настройке схемы, использующей только один публичный IP-адрес, важно явно задать маски подсети в параметрах `activeip` и `passiveip` файла `failover.ini`. Причем для `activeip` необходимо использовать реальную маску подсети, а для `passiveip` — нулевую маску. При настройке маршрутизации на адреса интерфейсов активного сервера через интерфейсы с маской 0.0.0.0, пассивный сервер всегда будет сначала запрашивать MAC-адреса этих интерфейсов, а затем отправлять по этим адресам пакеты (независимо от того, к каким подсетям принадлежат адреса активного и пассивного серверов).

Внимание! Маршрутизацию через интерфейсы с маской 0.0.0.0 нужно настроить только на адреса интерфейсов активного сервера. В противном случае эти настройки могут нарушить работу других интерфейсов.

Настраивать маски рекомендуется только в файле `failover.ini`, использование других методов крайне нежелательно и может привести к неработоспособности кластера горячего резервирования.

Для настройки маршрутизации предназначен специальный сценарий (shell-скрипт), входящий в комплект поставки ViPNet xFirewall. Этот скрипт задает маршруты на сервере при работе в активном и пассивном режимах. Вызов данного скрипта необходимо прописать в параметрах `afterifconf` и `beforeifconf` секции `[network]` в файле `failover.ini` (см. таблицу ниже). В результате демон failoverd будет вызывать shell-скрипт в двух случаях:

- после конфигурирования сетевых интерфейсов — на пассивном сервере этот скрипт будет устанавливать в системе маршруты на IP-адреса активного сервера, при переходе сервера в активный режим работы этот скрипт будет устанавливать статические маршруты (в том числе маршруты по умолчанию).
- до конфигурирования сетевых интерфейсов — на активном сервере этот скрипт будет удалять из системы маршруты, установленные при работе в пассивном режиме.

Необходимая служебная информация передается скрипту через набор переменных окружения.

Таблица 12. Настройки параметров системы защиты от сбоев в условиях ограничений по выделению IP-адресов

Настройки на первом сервере	Настройки на втором сервере
[channel]	**[channel]**
`device = eth1`	`device = eth1`
`activeip = 192.168.10.50`	`activeip = 192.168.10.50`
`passiveip = 192.168.10.51`	`passiveip = 192.168.10.52`
`testip = 192.168.10.1`	`testip = 192.168.10.1`
`ident = if-1`	`ident = if-1`
`checkonlyidle = yes`	`checkonlyidle = yes`
[channel]	**[channel]**
`device = eth2`	`device = eth2`
`activeip = 80.251.137.40/24`	`activeip = 80.251.137.40/24`
`passiveip = 10.0.0.1/0.0.0.0`	`passiveip = 10.0.0.2/0.0.0.0`
`testip = 80.251.137.80`	`testip = 80.251.137.80`
`ident = if-2`	`ident = if-2`
`checkonlyidle = yes`	`checkonlyidle = yes`
[network]	**[network]**
`checktime = 10`	`checktime = 10`
`timeout = 2`	`timeout = 2`
`activeretries = 3`	`activeretries = 3`
`channelretries = 3`	`channelretries = 3`
`synctime = 5`	`synctime = 5`
`fastdown = yes`	`fastdown = yes`
`afterifconf = /sbin/change_route.sh after`	`afterifconf = /sbin/change_route.sh after`
`beforeifconf = /sbin/change_route.sh before`	`beforeifconf = /sbin/change_route.sh before`
[sendconfig]	**[sendconfig]**
`device = eth0`	`device = eth0`
`activeip = 172.16.10.2` (соответствует failover IP второго сервера)	`activeip = 172.16.10.1` (соответствует failover IP первого сервера)

Организация обеспечения электропитания от UPS

Примечание. Приведенные в разделе настройки справедливы только для аппаратных исполнений ViPNet xFirewall. Для исполнения ViPNet xFirewall xF-VA данная функция не поддерживается.

Чтобы обеспечить электропитание ViPNet xFirewall в случае отключения электроэнергии или перебоев в электросети, рекомендуется подключить его к источнику бесперебойного питания (см. глоссарий, стр. 274).

Внимание! В настоящее время поддерживаются только UPS фирмы APC, подключаемые через USB-порт (например, APC Smart-UPS).

Если ViPNet xFirewall подключен к UPS, при отключении электроэнергии выполняются следующие действия:

1. ViPNet xFirewall начинает питаться от аккумуляторной батареи UPS.
2. Если заряд аккумуляторной батареи достигает критически низкого уровня (этот уровень зависит от следующих параметров, заданных на UPS: `battery.charge`, `battery.charge.low`, `battery.runtime` и `battery.runtime.low`), выполняются следующие действия:
   - **2.1** UPS взаимодействует с компьютером по интерфейсному кабелю и посылает сигнал об истощении батареи.
   - **2.2** ViPNet xFirewall получает сигнал и начинает выключаться. При этом на UPS передается информация о том, что для выключения ViPNet xFirewall потребуется не менее 180 секунд. Получив эти данные, UPS корректирует расход оставшегося заряда батареи таким образом, чтобы ViPNet xFirewall успел штатно завершить работу.

     В результате ViPNet xFirewall успевает выключиться до полного разряда батареи и потери данных не происходит.
3. Если подача электроэнергии восстанавливается до достижения батареей критически низкого уровня заряда, ViPNet xFirewall снова начинает питаться от электросети.

В общем случае от одного UPS могут питаться несколько компьютеров. Компьютер, к которому подключен интерфейсный кабель UPS, является главным (master), остальные компьютеры — подчиненными (slave). Главный компьютер взаимодействует непосредственно с UPS и отвечает за своевременное оповещение по сети подчиненных компьютеров. Главный компьютер должен быть доступен подчиненным по одному из своих IP-адресов. На рисунке ниже представлена схема подключения нескольких компьютеров к одному UPS.

Рисунок 27. Схема подключения компьютеров к UPS

В частном случае, когда к UPS подключен только один компьютер, подчиненные компьютеры отсутствуют.

Если к UPS подключается кластер горячего резервирования, состоящий из двух ViPNet xFirewall, то один ViPNet xFirewall будет главным, а другой — подчиненным. При этом никакие другие компьютеры к UPS подключать нельзя. Для связи между двумя ViPNet xFirewall кластера можно использовать только резервный канал, так как на нем IP-адреса неизменны при переходе ViPNet xFirewall из активного режима кластера в пассивный и наоборот.

Чтобы настроить взаимодействие нескольких ViPNet xFirewall с UPS, необходимо на каждом ViPNet xFirewall выполнить ряд команд, соответствующих его роли (master или slave).

На ViPNet xFirewall, который будет выступать в роли master, выполните следующие действия:

1. Подключите к ViPNet xFirewall интерфейсный кабель UPS.
2. Выполните команду `enable` для перехода в режим администратора. В ответ на приглашение введите пароль администратора.
3. Включите взаимодействие ViPNet xFirewall с UPS с помощью команды:

   ```
   hostname# ups set monitoring on
   ```
4. Установите на ViPNet xFirewall режим master с помощью команды:

   ```
   hostname# ups set mode master
   ```
5. Запустите взаимодействие ViPNet xFirewall с UPS с помощью команды:

   ```
   hostname# ups start
   ```
6. Проверьте взаимодействие ViPNet xFirewall с UPS с помощью команды:

   ```
   hostname# ups show status
   ```

   Если взаимодействие установлено, отобразится информация о текущем состоянии UPS.

Внимание! Если вы переподключили интерфейсный кабель UPS (то есть отсоединили его от ViPNet xFirewall, а затем снова подключили), то для восстановления взаимодействия ViPNet xFirewall с UPS выполните последовательно команды `ups stop` и `ups start`.

На ViPNet xFirewall, который будет выступать в роли slave, выполните следующие действия:

1. Выполните команду `enable` для перехода в режим администратора. В ответ на приглашение введите пароль администратора.
2. Включите взаимодействие ViPNet xFirewall с UPS с помощью команды:

   ```
   hostname# ups set monitoring on
   ```

3 Установите на ViPNet xFirewall режим slave с помощью команды:

```
hostname# ups set mode slave <master_IP>
```

ViPNet xFirewall, выступающий в роли master, должен быть доступен с данного ViPNet xFirewall по этому IP-адресу.

При подключении к UPS кластера горячего резервирования в качестве IP-адреса мастера укажите адрес первого ViPNet xFirewall на резервном канале.

4 Запустите взаимодействие ViPNet xFirewall с UPS с помощью команды:

```
hostname# ups start
```

5 Проверьте взаимодействие ViPNet xFirewall с UPS с помощью команды:

```
hostname# ups show status
```

Если взаимодействие установлено, отобразится информация о текущем состоянии UPS, подключенного к ViPNet xFirewall в роли master.

Также вы можете настроить автоматическое включение ViPNet xFirewall после появления электропитания. Это может понадобиться в случае долговременного отключения электроэнергии. Чтобы выполнить такую настройку для исполнений xF1000 и xF5000 задайте в BIOS следующие параметры:

1 Пункт меню/подменю: **Advanced** > **APM**

2 Параметр: **Restore AC Power Loss**

3 Значение: **Power On**

Примечание. Для аппаратной платформы ViPNet xFirewall xF100 N1 автоматическое включение после появления электропитания настроить нельзя.

12

Ведение и просмотр журналов

Просмотр журнала регистрации IP-пакетов

Управляющий демон ведет журнал регистрации IP-пакетов, в который заносится информация обо всех IP-пакетах (зашифрованных и открытых), проходящих через сетевые интерфейсы узла.

В журнал заносится информация не о соединениях, а об IP-пакетах, которые проходят через сетевые интерфейсы, поэтому:

- каждый пропущенный и заблокированный локальный IP-пакет отображается в журнале один раз — на том интерфейсе, через который он прошел, или на том интерфейсе, на котором он был заблокирован, соответственно;
- каждый пропущенный транзитный IP-пакет отображается в журнале дважды: первый раз — на интерфейсе, через который он пришел, второй раз — на интерфейсе, через который он ушел.

Чтобы просмотреть записи из журнала регистрации IP-пакетов, выполните команду:

```
hostname# iplir view
```

В результате откроется окно **Set search parameters** для задания параметров поиска записей в журнале.

Внимание! При работе ViPNet xFirewall в режиме кластера горячего резервирования журнал IP-пакетов можно просмотреть только на активном сервере кластера.

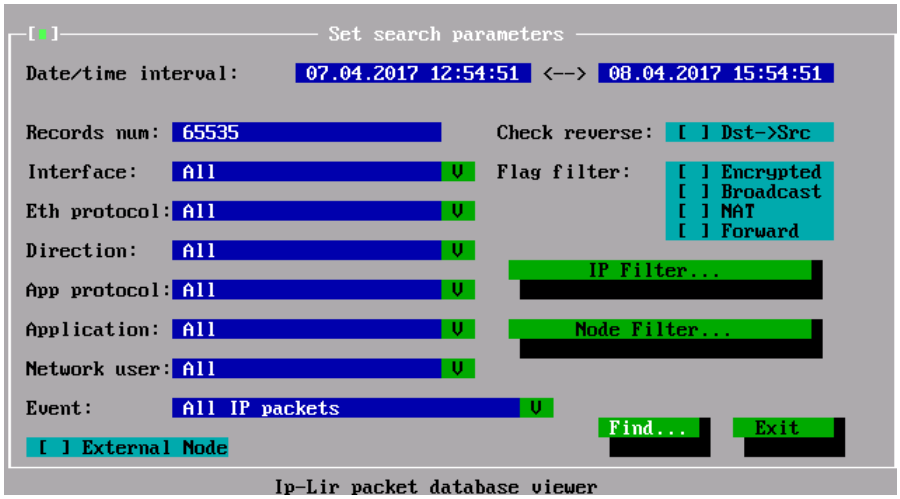


Рисунок 28. Задание параметров поиска записей в журнале регистрации IP-пакетов

По умолчанию предполагается просмотр записей обо всех пакетах, прошедших через сетевые интерфейсы собственного узла за последние сутки. Чтобы просмотреть такие записи, нажмите кнопку **Find**.

Чтобы выбрать записи из журнала регистрации IP-пакетов для просмотра, выполните следующие действия:

1 Укажите параметры пакетов:

- **Date/time interval** — период времени, в который были зарегистрированы пакеты в формате: `дд.мм.гггг чч:мм:сс <--> дд.мм.гггг чч:мм:сс`

  По умолчанию — текущие сутки.

- **Records num** — количество записей о зарегистрированных пакетах, которое будет отображено (по умолчанию — 65535).
- **Interface** — сетевой интерфейс, на котором были обработаны пакеты. По умолчанию — все доступные интерфейсы (**All**).
- **Protocol** — IP-протокол, по которому были переданы пакеты. Возможные значения:
  - **All** (по умолчанию) — любой протокол;
  - **ICMP** — только протокол ICMP;
  - **TCP** — только протокол TCP;
  - **UDP** — только протокол UDP.
  - **Except TCP, UDP, ICMP** — любой протокол, кроме TCP, UDP и ICMP.
- **Direction** — направление пакетов:
  - **All** (по умолчанию) — входящие и исходящие пакеты;
  - **Incoming** — входящие пакеты;
  - **Outgoing** — исходящие пакеты.
- **App protocol —** прикладной протокол (на стр. 87). По умолчанию — все прикладные протоколы (**All**).
- **Application** — приложение (на стр. 86). По умолчанию — все приложения (**All**).

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)».

- **Network user** — имя пользователя сети (см. Пользователь на стр. 88), аутентифицированного с помощью Active Directory или Captive portal. По умолчанию — все пользователи (**All**).
- **Event** — тип события, которому соответствует IP-пакет. По умолчанию — события всех типов (**All**).
- **Check reverse** — включение в журнал ответных пакетов от получателя отправителю (**Dst -> Src**). Устанавливать этот флажок имеет смысл только, если в качестве отправителя и/или получателя пакетов указаны конкретные IP-адреса (**IP Filter**) или узлы (**Node Filter**).
- **Flag filter** — вид пакетов:
  - **Encrypted** — зашифрованные пакеты;
  - **Broadcast** — широковещательные пакеты;
  - **NAT** — транслированные пакеты;
  - **Forward** — транзитные пакеты.

  Вы можете выбрать один или несколько видов пакетов, установив соответствующие флажки. Транслированные (**NAT**) и транзитные (**Forward**) пакеты имеет смысл выбирать только для просмотра записей об IP-пакетах на маршрутизаторе.

2 Чтобы задать IP-адреса или порты отправителя или получателя пакетов, нажмите кнопку **IP Filter** и в открывшемся окне:

- если в списке **Protocol** вы выбрали все протоколы или все протоколы, кроме TCP, UDP и ICMP, укажите:
  - **Source IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) отправителей пакетов. По умолчанию — любой адрес (**All**);
  - **Destination IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) получателей пакетов. По умолчанию — любой адрес (**All**);
- если в списке **Protocol** вы выбрали протокол TCP или UDP, помимо IP-адресов отправителя и получателя, укажите:
  - **Source port** — порт (**Value**) или диапазон портов (**Range**) отправителей. По умолчанию — все порты (**All**);
  - **Destination port** — порт (**Value**) или диапазон портов (**Range**) получателей. По умолчанию — все порты (**All**);
- если в списке **Protocol** вы выбрали протокол ICMP, помимо IP-адресов отправителя и получателя, укажите:
  - **ICMP type** — тип (**Value**) или диапазон типов (**Range**) ICMP-пакетов.
  - **ICMP code** — код (**Value**) или диапазон кодов (**Range**) ICMP-пакетов.

3 Чтобы выбрать узел отправителя или получателя, нажмите кнопку **Node Filter** и в открывшемся окне:

3.1 Для выбора узла отправителя нажмите кнопку **Select source Node**, для выбора узла получателя — кнопку **Select destination Node**.

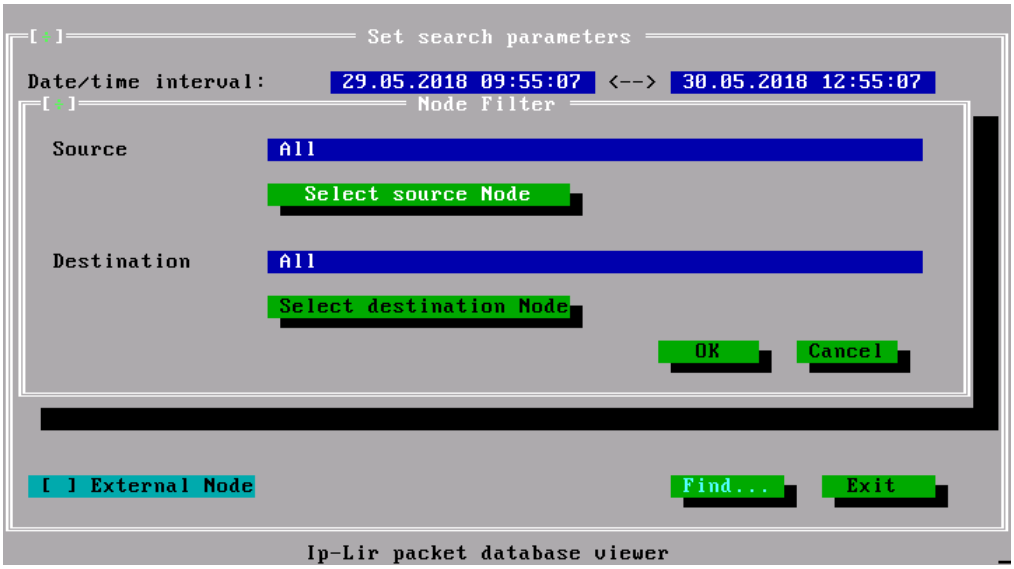


Рисунок 29. Выбор узла отправителя и получателя

В результате откроется таблица со списком узлов ViPNet, с которыми у данного узла есть связь. В левом столбце таблицы указан шестнадцатеричный идентификатор узла (**ID**), в правом — имя узла (**Name**).

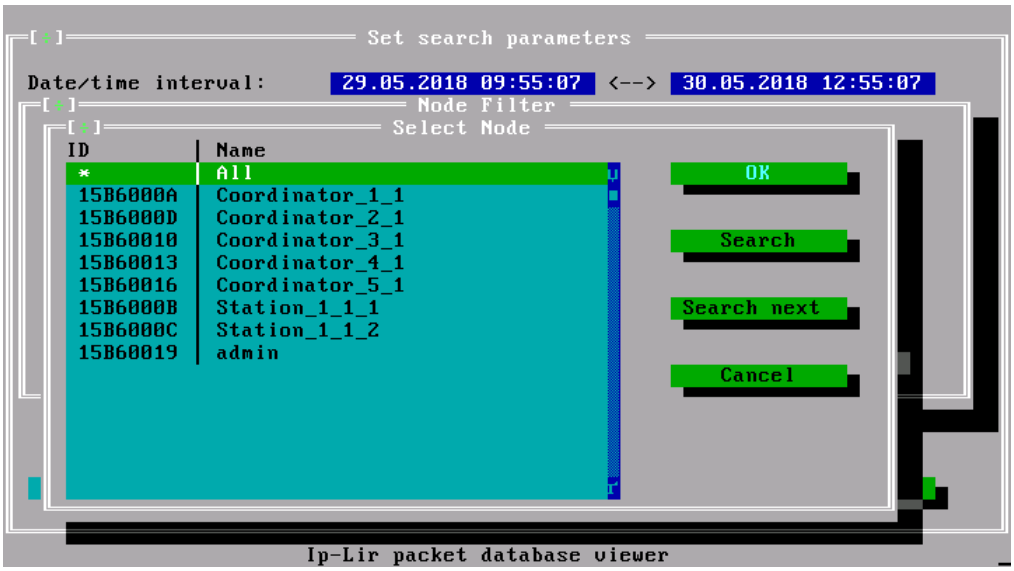


Рисунок 30. Выбор узла отправителя и получателя

3.2 Выберите нужный узел и нажмите кнопку **OK**.

Совет. Чтобы быстро найти нужный узел в списке, нажмите кнопку **Search**. В открывшемся окне введите часть идентификатора или имени узла и нажмите кнопку **OK**. В результате курсор будет переведен на строку первого узла, идентификатор или имя которого удовлетворяют условиям поиска. Для перехода к следующему такому узлу нажмите кнопку **Search next**.

---

4 Чтобы просмотреть журнал регистрации IP-пакетов удаленного узла:

Внимание! Для просмотра журнала регистрации IP-пакетов удаленного узла необходимо, чтобы этот узел был доступен.

4.1 Установите флажок **External Node** и введите пароль администратора узла ViPNet.

4.2 С помощью кнопки **Select** откройте окно со списком узлов ViPNet и выберите нужный узел.

5 Нажмите кнопку **Find**.

В результате откроется окно **View results**, содержащее таблицу со списком записей о пакетах, которые удовлетворяют выбранным параметрам. Записи упорядочены по времени регистрации. Таблица включает следующие столбцы:

- **Date/time** — дата и время регистрации пакета;
- **Dev** — интерфейс, на котором был обработан пакет;
- **Flags** — направление и флаги пакетов:
  - **<** — исходящий пакет;
  - **>** — входящий пакет;
  - **C** — шифрованный пакет;
  - **B** — широковещательный пакет;
  - **D** — заблокированный пакет;
  - **T** — транзитный пакет;
  - **R** — пакет, который будет обработан правилами NAT открытой сети;
  - **N** — пакет, который был обработан правилами NAT открытой сети;
- **Prot** — протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — локальный порт для TCP- и UDP-пакетов или тип для ICMP-пакетов;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт удаленного компьютера для TCP- и UDP-пакетов или код для ICMP-пакетов.

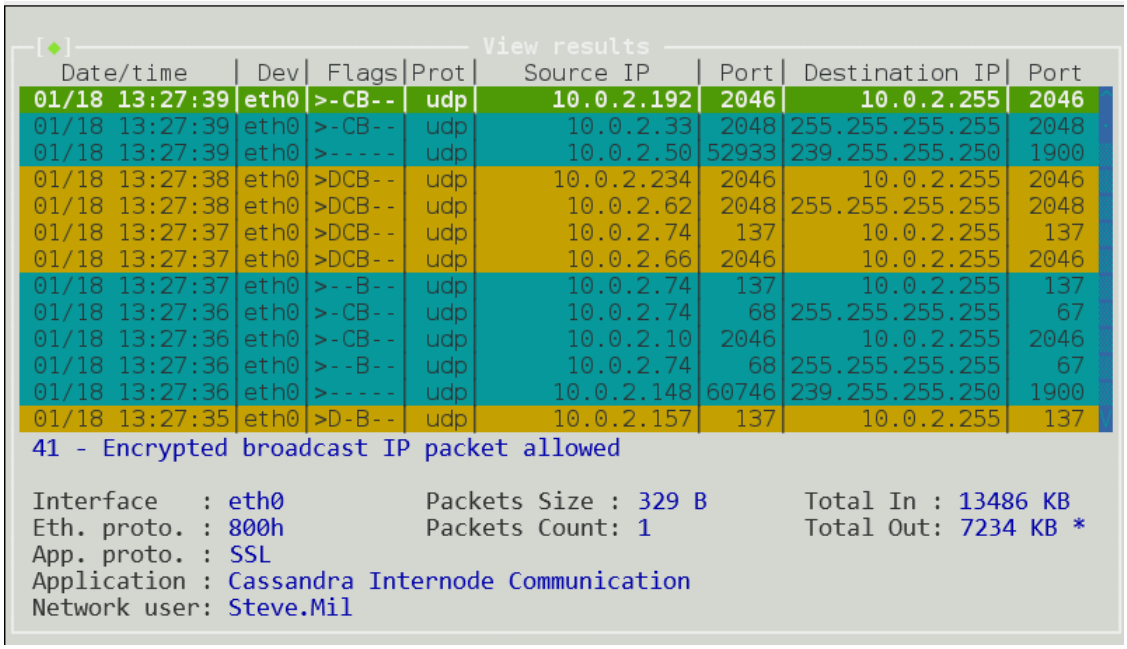


Рисунок 31. Просмотр записей из журнала регистрации IP-пакетов

Вы можете выполнить следующие действия:

- Экспортировать список записей в текстовый файл (например, для последующего анализа). Для этого в окне **View Results** нажмите клавишу **F2** и укажите файл для экспорта.
- Просмотреть краткую информацию о пакете, выбрав его в списке. В результате под списком отобразится следующая дополнительная информация:
  - тип события, которому соответствует IP-пакет;
  - **Eth. proto** — шестнадцатеричный идентификатор протокола Ethernet;
  - **Packet Size** — размер пакетов, соответствующих данному типу события;

Примечание. Для зашифрованных пакетов в параметре **Packet size** отображается размер пакетов со всеми служебными заголовками.

  - **Packet Count** — число пакетов, соответствующих выбранному типу события;
  - **Total In** — суммарный размер всех входящих пакетов, соответствующих выбранному типу события;
  - **Total Out** — суммарный размер всех исходящих пакетов, соответствующих выбранному типу события;

Примечание. Единицы изменения суммарного размера пакетов: **B** — байты, **KB** — килобайты, **MB** — мегабайты.

Символ «*» в поле **Total In** или **Total Out** пакета означает, что этот пакет не учтен в общем объеме входящего или исходящего трафика. Символ «N/A» — означает отсутствие информации о размере пакетов, соответствующих выбранному типу события.

- **App. proto** — тип прикладного протокола (см. Поддерживаемые прикладные протоколы на стр. 253);
- **Application** — тип приложения (см. Поддерживаемые приложения на стр. 251);
- **Network user** — пользователь сети (см. Пользователь на стр. 88);
- имена узла отправителя и узла получателя.

- Просмотреть подробную информацию о записи журнала, выбрав его в списке и нажав клавишу **Enter**. Подробная информация о записи журнала откроется в отдельном окне **Record details**.

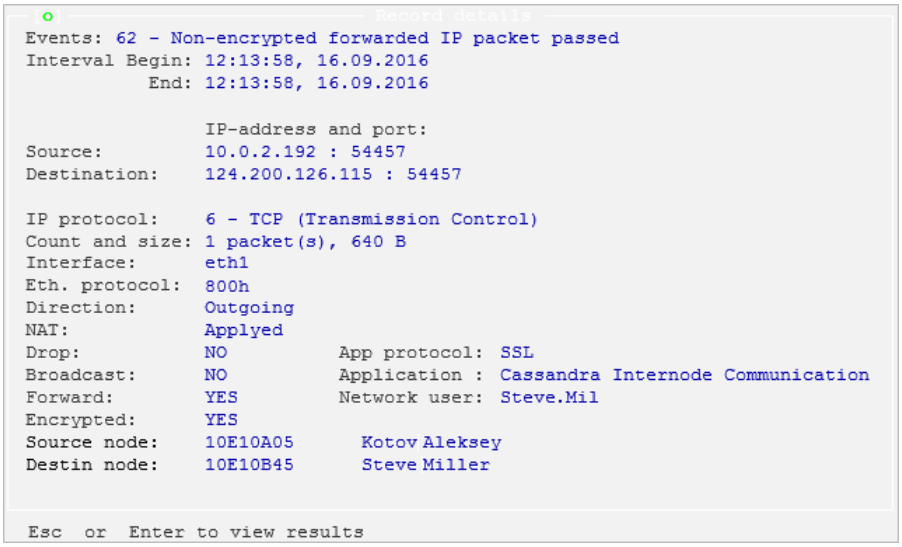


Рисунок 32. Просмотр подробной информации о пакете

Для каждой записи журнала отображается следующая информация:

- **Events** — номер и тип событий, объединенных в одну запись журнала (см. Типы событий в журнале регистрации IP-пакетов на стр. 235);
- **Interval Begin, End** — начало и конец интервала времени, в течение которого несколько событий были объединены в одну запись журнала IP-пакетов;
- **Source** — IP-адрес и порт отправителя пакетов;
- **Destination** — IP-адрес и порт получателя пакетов;
- **IP protocol** — тип транспортного протокола (TCP/UDP);
- **Count and size** — число и размер пакетов, соответствующих выбранному типу события;
- **Interface** — имя сетевого интерфейса, на котором были зарегистрированы события;
- **Eth. protocol** — шестнадцатеричный идентификатор протокола Ethernet;
- **Direction** — направление пакета (входящий, исходящий);
- **NAT** — флаг транслированного пакета;
- **Drop** — флаг блокировки пакета;
- **Broadcast** — флаг широковещательного пакета;

- **Forward** — флаг транзитного пакета;
- **Encrypted** — флаг зашифрованного пакета;
- **App protocol** — тип прикладного протокола (см. Поддерживаемые прикладные протоколы на стр. 253);
- **Application** — тип приложения (см. Поддерживаемые приложения на стр. 251);
- **Network user** — пользователь сети (см. Пользователь на стр. 88);
- **Source node** — номер и имя сетевого узла ViPNet (отправителя пакетов);
- **Destination node** — номер и имя сетевого узла ViPNet (получателя пакетов).

- Для завершения просмотра журнала регистрации IP-пакетов или изменения параметров поиска пакетов в журнале нажмите клавишу **Esc**.

Экспорт журнала регистрации IP-пакетов на USB-носитель

Чтобы экспортировать список записей из журнала регистрации IP-пакетов на USB-носитель, выполните следующие действия:

Внимание! Если вы используете удаленное подключение по SSH, то для корректного экспорта установите в настройках используемого ПО SSH-клиента тип терминала VT100+.

1. Выполните команду:

   ```
   hostname# iplir view
   ```

2. В окне **Set search parameters** задайте параметры для выбора из журнала регистрации IP-пакетов нужных записей и нажмите кнопку **Find** (см. Рисунок 28 на стр. 202).

3. В окне **View results** со списком найденных записей нажмите клавишу **F2** (см. Рисунок 31 на стр. 207).

4. В открывшемся окне введите имя файла, в который вы хотите сохранить журнал, или выберите из списка существующий файл. Затем нажмите клавишу **Enter**.

5. Чтобы завершить просмотр журнала, нажмите клавишу **Esc**. Затем нажмите кнопку **Exit**.

6. Выполните команду:

   ```
   hostname# admin export packetdb usb <имя файла>,
   ```

   указав имя файла с журналом.

7. Подключите USB-носитель к одному из USB-разъемов ViPNet xFirewall и нажмите клавишу **Enter**.

8. В списке подключенных к ViPNet xFirewall USB-носителей и имеющихся на них разделов найдите нужный, введите его номер, нажмите клавишу **Enter** и дождитесь завершения экспорта.

В результате журнал регистрации IP-пакетов будет экспортирован в корневой каталог выбранного USB-носителя в виде архива `*.tar.gz`, содержащего текстовый файл. Данные в этом текстовом файле разделены символом «|».

Чтобы преобразовать журнал в удобный для чтения вид, распакуйте архив, откройте его с помощью программы Microsoft Excel и выполните импорт данных, указав в качестве разделителя символ «|». В результате данные отобразятся в таблице, содержащей следующие столбцы:

- **Time begin** — дата и время начала регистрации пакета;
- **Time end** — дата и время окончания регистрации пакета;

- **Dev** — интерфейс, на котором был обработан пакет;
- **Eth** — шестнадцатеричный идентификатор протокола Ethernet;
- **Flags** — направление и флаги пакета;
- **Prot** — протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — локальный порт TCP- и UDP-пакетов или тип для ICMP-пакетов;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт удаленного компьютера для TCP- и UDP-пакетов или код для ICMP-пакетов.
- **Size** — размер пакета (или суммарный размер пакетов, если количество пакетов больше единицы);
- **Cnt** — количество пакетов, относящихся к данному событию;
- **SourceNode** — узел отправителя;
- **DestinNode** — узел получателя;
- **Event** — код и название события, присвоенного пакету;
- **App. protocol** — прикладной протокол;
- **Application** — приложение;
- **Network user** — пользователь сети.

Экспорт журнала регистрации IP-пакетов по сети в формате CEF

Вы можете экспортировать записи из журнала регистрации IP-пакетов по сети в формате CEF (см. глоссарий, стр. 270). Для настройки экспорта записей выполните следующие действия:

1 Остановите работу демона iplircfg:

```
hostname# iplir stop
```

2 Укажите параметры формирования сообщений CEF для интерфейса, записи журнала регистрации IP-пакетов которого вы хотите экспортировать:

```
hostname# iplir config ethX
```

где `X` — номер интерфейса.

Отредактируйте секцию `[cef]` файла конфигурации интерфейса `iplir.conf-ethX`. Вы можете задать следующие параметры:

- `event` — формирование сообщений CEF при регистрации IP-пакетов, проходящих через интерфейс:
  - `all` — для всех IP-пакетов;
  - `blocked` — только для блокированных IP-пакетов (значение по умолчанию);
- `exclude` — формирование сообщений CEF, заданных в `event`, за исключением типов событий в журнале регистрации IP-пакетов (см. Типы событий в журнале регистрации IP-пакетов на стр. 235). Допускается перечисление номеров типов событий в любом порядке через запятую.

Примечание. При необходимости вы можете изменить значение параметра `timedif` секции `[db]` в файле конфигурации интерфейса `iplir.conf-ethX`. Параметр `timedif` задает:

- интервал времени, в течение которого одинаковые события объединяются в одну запись журнала регистрации IP-пакетов;
- периодичность отправки записей журнала регистрации IP-пакетов в формате CEF по сети.

Подробнее см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», раздел «Файл iplir.conf-<интерфейс или группа интерфейсов>».

---

3 Задайте адрес сетевого узла, на который будут посылаться сообщения CEF:

```
hostname# machine set cef loghost <имя|адрес>
```

где `<имя|адрес>` — доменное имя или IP-адрес сетевого узла. При задании корректного доменного имени или IP-адреса сетевого узла включается механизм экспорта.

Внимание! В качестве сетевого узла нельзя указывать локальный узел localhost, собственные адреса и алиса интерфейсов.

4 Запустите демон iplircfg:

```
hostname# iplir start
```

5 При работе в открытой сети создайте разрешающее исходящее правило для протокола syslog на заданный сетевой узел:

```
hostname# firewall local add src @local dst <имя|адрес> service @syslog pass
```

Примечание. В сети ViPNet разрешающее исходящее правило для протокола syslog создается автоматически.

Для просмотра текущего сетевого узла, на который экспортируются записи из журнала регистрации IP-пакетов в формате CEF, выполните команду:

```
hostname# machine show cef loghost
```

Если вы хотите остановить экспорт записей журнала регистрации IP-пакетов в формате CEF, выполните команды:

```
hostname# iplir stop
```

```
hostname# machine set cef loghost none
```

```
hostname# iplir start
```

Пример записи журнала регистрации IP-пакетов в формате CEF

Ниже приведен пример записи журнала регистрации IP-пакетов в формате CEF:

```
Sep 19 08:26:10 xfva-2936003e CEF:0|infotecs|xf|4.1|20|unencrypted IP packet
blocked|10|start=08:26:10<space>19.09.2017 end=08:26:10<space>19.09.2017 src=10.0.0.1
dst=2.1.2.2 spt=1232 dpt=80 proto=tcp cnt=5 in=20 deviceInboundInterface=eth0 cn1=800h
cnLabel=Eth<space>protocol<space>hex cs1=NAT<space>yes cs2=Drop<space>yes
cs3=Broadcast<space>no cs4=Forward<space>no cs5=Encrypted<space>no cs1Label=Flags
cs6=Facebook cs6Label=Application<space>name deviceDirection=inbound app=http
suser=admin
```

Вы можете посмотреть структуру записи журнала регистрации IP-пакетов в формате CEF в приложении (см. Структура записи журнала регистрации IP-пакетов в формате CEF на стр. 240) к настоящему документу.

Просмотр журнала транспортных конвертов MFTP

В процессе работы транспортный модуль MFTP записывает информацию о полностью принятых, отправленных, удаленных и поврежденных конвертах в специальный журнал.

Алгоритм работы с журналом конвертов основан на использовании ротации. В настройках транспортного модуля задается максимальный размер файла журнала в мегабайтах. При превышении данного размера наиболее ранние записи перезаписываются новыми. Таким образом, задавая максимальный размер журнала конвертов, вы можете регулировать число хранимых записей на текущий момент. При изменении максимального размера журнала в процессе работы происходит реконструкция журнала конвертов — в случае уменьшения размера журнала наиболее ранние записи удаляются из него.

Для просмотра журнала транспортных конвертов выполните команду:

```
hostname# mftp view
```

При экспорте информации из журнала конвертов в текстовый файл выводится следующая информация:

- имя конверта;
- размер конверта;
- имя узла-отправителя;
- имя узла-получателя;
- название события;
- имя прикладной задачи (роли) или тип узла-отправителя;
- описание конверта;
- дата и время события.

Работа с журналом событий

В ViPNet xFirewall все демоны записывают информацию о событиях, происходящих в процессе их работы, в журнал событий. Этот журнал позволяет контролировать работоспособность ViPNet xFirewall, своевременно выявлять и устранять причины сбоев в его работе.

Запись информации в журнал событий осуществляется системными средствами с использованием протокола syslog. Этот журнал может храниться в системном журнале syslog на самом сервере ViPNet xFirewall (локальное протоколирование) или на удаленном сетевом узле (удаленное протоколирование).

Внимание! Во всех исполнениях ViPNet xFirewall по умолчанию настроено локальное протоколирование третьего уровня детализации. Подробнее об уровнях детализации см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам», в описании секций `[debug]` конфигурационных файлов демонов iplircfg, mftpd, failoverd.

- В случае локального хранения журнала предусмотрена автоматическая ротация файла журнала с целью экономии места на ViPNet xFirewall. Ротация выполняется, когда размер файла журнала достигает размера 1 Гбайт.

В процессе ротации заполненный файл журнала переименовывается, при этом другой файл журнала, который был переименован раньше остальных, удаляется. Это делается для того, чтобы на ViPNet xFirewall всегда было не более 10 заполненных файлов и 1 текущего файла.

При локальном хранении журнала вы можете выполнить с ним следующие действия:

- Просмотреть содержимое журнала. Для этого выполните команду:

  ```
  hostname# machine show logs
  ```

- Экспортировать файлы журнала на другой компьютер (см. Экспорт журнала событий на компьютер на стр. 218) или на USB-носитель (см. Экспорт журнала событий на USB-носитель на стр. 220). Файлы журнала экспортируются в виде архива `logs.tar.gz`.
- Вручную удалить все имеющиеся файлы журнала. Для этого выполните команду:

  ```
  hostname# admin remove logs
  ```

Внимание! Удаление файлов журнала требуется при завершении эксплуатации ViPNet xFirewall. В других случаях удалять файлы журнала настоятельно не рекомендуется.

Вы также можете настроить ряд параметров ведения журнала (см. Настройка параметров ведения журнала событий на стр. 216).

Перечень протоколируемых событий, связанных с аутентификацией и настройкой оборудования, приведен в приложении (см. Записи в журнале событий, связанные с аутентификацией и настройкой оборудования на стр. 243).

Просмотр журнала событий

Чтобы просмотреть записи журнала событий, выполните команду:

```
hostname# machine show logs [reversed] [since <время>] [filtered {<демон> | string <строка>}],
```

указав следующие параметры:

- `reversed` — вывод списка записей в обратном хронологическом порядке.
- `<время>` — вывод списка записей, начиная с указанного момента времени. Момент времени задается в формате `YYYY-MM-DD hh:mm:ss`.
- `<демон>` — вывод записей только для указанного демона в составе ПО ViPNet xFirewall (см. Список демонов в составе ПО ViPNet xFirewall на стр. 249).
- `<строка>` — вывод записей журнала по части строки. При поиске по части строки можно использовать символы `A-Z, a-z, 0-9`, а также следующие символы:

  ```
  !# $ % & ( ) * + , - . / : ; < = > @ [ ] _ { | } ~
  ```

  Также можно использовать пробел, в этом случае необходимо взять часть строки в двойные кавычки (`""`).

Внимание! В одной команде `machine show logs` можно одновременно использовать только одну из лексем: `since` или `filtered`. При использовании лексемы `filtered` можно указать только один из ее параметров: `<демон>` или `<строка>`.

Например, чтобы найти все записи журнала событий, начиная с 14:50 22 ноября 2016 года, и отобразить их в обратном порядке, выполните команду:

```
hostname# machine show logs reversed since 2016-11-22 14:50:00
```

Настройка параметров ведения журнала событий

Вы можете выполнить следующие настройки параметров ведения журнала событий:

- Чтобы выбрать место хранения журнала событий, выполните команду:

  ```
  hostname# machine set loghost {<IP-адрес> | local},
  ```

указав IP-адрес удаленного сетевого узла, на котором будет храниться журнал, или параметр `local` для локального протоколирования.

Внимание! Если для удаленного протоколирования будет использоваться открытый узел, на ViPNet xFirewall вручную задайте фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на 514-й порт этого открытого узла.

Не рекомендуется использовать удаленное протоколирование на ViPNet xFirewall в режиме кластера горячего резервирования, так как на удаленный сетевой узел не будут передаваться журналы с пассивного сервера (то есть часть информации о работе ViPNet xFirewall будет утеряна).

Если все же необходимо настроить удаленное протоколирование при работе в режиме кластера горячего резервирования, задайте параметры протоколирования на обоих серверах кластера, так как эти параметры не передаются с активного сервера на пассивный по каналу резервирования.

- Чтобы отключить ведение журнала событий, выполните команду:

  ```
  hostname# machine set loghost null
  ```

Внимание! Отключать ведение журнала не рекомендуется.

- Чтобы изменить уровень детализации информации, выводимой в журнал, выполните настройку параметра `debuglevel` в секции `[debug]` конфигурационных файлов `iplir.conf`, `failover.ini`, `mftp.conf`. Описание параметров секции `[debug]` в данных файлах см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».

Совет. В большинстве случаев изменять уровень детализации, выбранный по умолчанию, не рекомендуется. При повышении уровня детализации необходимо учитывать, что размер файла журнала будет быстро расти, вследствие чего, будет чаще производиться его ротация при достижении максимального размера.

- Чтобы сообщения о работе демона выводились на консоль командного интерпретатора, выполните команду:

  ```
  hostname# debug on <facility.level>,
  ```

  указав выбранные значения параметров `facility` и `level`.

  Параметры `facility` и `level` должны быть заданы в секции `[debug]` конфигурационных файлов `iplir.conf`, `failover.ini`, `mftp.conf`. Описание параметров секции `[debug]` в данных файлах см. в документе «ViPNet xFirewall. Справочное руководство по командному интерпретатору и конфигурационным файлам».

- Чтобы выключить вывод сообщений на консоль командного интерпретатора, выполните команду `debug off`. С помощью этой команды вы можете выключить как вывод всех сообщений, так и вывод только тех сообщений, которые соответствуют конкретным значениям параметров `facility` и `level`.

  Например, вы можете настроить протоколирование так, чтобы следить за работой разных демонов на разных терминалах. Для этого выполните следующее:

  - В конфигурационном файле одного из демонов в секции `[debug]` задайте нужные параметры, например:

    ```
    [debug]
    debuglogfile = syslog:daemon.debug
    debuglevel = 3
    ```

    И на одном из терминалов выполнить команду:

    ```
    hostname# debug on daemon.debug
    ```

  - В конфигурационном файле другого демона в секции `[debug]` задайте параметры протоколирования, указав другое значение `facility`, например:

    ```
    [debug]
    debuglogfile = syslog:local0.debug
    debuglevel = 3
    ```

    И на другом терминале выполнить команду:

    ```
    hostname# debug on local0.debug
    ```

  В результате на первый терминал будут поступать сообщения только от первого демона, на второй терминал — только от второго демона. Чтобы на первом терминале можно было следить за работой обоих демонов, на нем в дополнение к первой команде выполните команду:

  ```
  hostname# debug on local0.debug
  ```

Примечание. Выводимые на консоль командного интерпретатора сообщения о работе демонов могут смешиваться с сообщениями самого интерпретатора и командами, набираемыми на консоли. Для просмотра набранной к данному моменту части команды и продолжения ее ввода используйте комбинацию клавиш **Ctrl+L**.

Экспорт журнала событий на компьютер

Внимание! Во время экспорта журналов на другой компьютер завершается работа всех демонов и выгружаются все драйверы ViPNet, то есть ViPNet xFirewall будет незащищенным.

При экспорте журналов событий с ViPNet xFirewall на другой компьютер используется стандартная служба TFTP. В ОС Windows XP эта служба по умолчанию включена. В ОС Windows 10 эта служба по

умолчанию выключена и ее необходимо включить вручную. Для включения службы в ОС Windows 10 выполните следующее:

1 Выберите **Пуск** (**Start**) > **Панель управления** (**Control Panel**) > **Программы и компоненты** (**Programs and Features**).

2 Зайдите в меню **Включение или отключение компонентов Windows** (**Turn Windows features on or off**) и установите флажки рядом с названием служб **Клиент TFTP** (**TFTP Client**) и **Простые службы TCPIP** (**Simple TCPIP services**).

На время выполнения экспорта автоматически изменяются настройки сетевых интерфейсов ViPNet xFirewall: на интерфейсе Ethernet1 устанавливается IP-адрес `169.254.241.1`, все остальные интерфейсы выключаются. После успешного завершения экспорта настройки интерфейсов ViPNet xFirewall автоматически восстанавливаются.

Внимание! Во избежание потери удаленного доступа к ViPNet xFirewall запрещается выполнять экспорт журналов на другой компьютер в удаленной SSH-сессии.

Чтобы экспортировать журналы событий на компьютер, выполните следующие действия:

1 Подключите ноутбук к порту Ethernet1 ViPNet xFirewall с помощью кросс-кабеля Ethernet.

2 Установите вручную на сетевом интерфейсе ноутбука IP-адрес 169.254.241.5.

3 Подключите к ViPNet xFirewall обычную консоль (монитор и клавиатуру) или COM-консоль.

4 Завершите работу демонов iplircfg, failoverd и mftpd, выполнив команду:

```
hostname# vpn stop
```

5 Выполните команду:

```
hostname# admin export logs tftp
```

При выполнении команды производится архивирование журналов событий в файл экспорта `logs.tar.gz`.

Примечание. Чтобы прервать экспорт во время архивирования, нажмите сочетание клавиш **Ctrl+C**.

После завершения архивирования появится сообщение, содержащее предложение скачать полученный файл.

6 Перенесите файл `logs.tar.gz` на ноутбук по TFTP. Для этого выполните на ноутбуке команду:

```
tftp -i 169.254.241.1 get logs.tar.gz
```

7 Нажмите клавишу **Enter**.

8 Запустите демоны iplircfg, failoverd и mftpd, выполнив команду:

```
hostname# vpn start
```

В результате архив с журналами событий будет скопирован на компьютер.

Экспорт журнала событий на USB-носитель

Чтобы экспортировать журналы событий на USB-носитель, выполните следующие действия:

1 На ViPNet xFirewall выполните команду:

```
hostname# admin export logs usb
```

При выполнении команды производится архивирование журналов событий в файл экспорта `logs.tar.gz`.

Примечание. Чтобы прервать экспорт во время архивирования, нажмите сочетание клавиш **Ctrl+C**.

После завершения архивирования появляется предложение подключить USB-носитель и подтвердить выполнение экспорта.

2 Подключите USB-носитель к USB-разъему ViPNet xFirewall (или к компьютеру, на котором развернут виртуальный образ ViPNet xFirewall).

3 По запросу командного интерпретатора введите номер USB-носителя и нажмите клавишу **Enter**.

В результате архив с журналами событий будет скопирован на USB-носитель.

13

Мониторинг ViPNet xFirewall

Мониторинг с помощью ПК ViPNet StateWatcher

Вы можете осуществлять мониторинг работы ViPNet xFirewall с помощью программного комплекса ViPNet StateWatcher. Данный комплекс предназначен для наблюдения за состоянием узлов сети ViPNet (в том числе ViPNet xFirewall). ПК ViPNet StateWatcher также собирает информацию о состоянии установленных на узлах компонентов ПО ViPNet, о текущей загруженности аппаратного обеспечения узлов, о состоянии сетевых интерфейсов, о статусе связей между узлами.

В случае возникновения сбоев или неполадок на узлах, вы будете оперативно проинформированы об этом. Вы можете настроить удобный вам способ оповещения о событиях: непосредственно в веб-интерфейсе ПК ViPNet StateWatcher (визуальные и звуковые оповещения, оповещения на карте и информационной панели), по электронной почте (в том числе ViPNet Деловая почта), по SMS, по протоколу Syslog. События на узлах выявляются на основе анализа их состояния специальными правилами. Вы можете использовать встроенные правила анализа или создать собственные правила, с помощью которых будут анализироваться важные для вас параметры узлов.

Подробнее о работе с ПК ViPNet StateWatcher см. в документе «Программный комплекс ViPNet StateWatcher. Сервер мониторинга. Руководство администратора».

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. Параметры протокола `rocommunity` и `trapcommunity` по умолчанию имеют значение `public`.

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.

Примечание. Чтобы SNMP-запросы обрабатывались корректно, необходимо отправлять их на IP-адрес ViPNet xFirewall, который доступен с опрашивающего узла по кратчайшему маршруту.

ViPNet xFirewall поддерживает базу управляющей информации (MIB) для ПО ViPNet и некоторые стандартные базы управляющей информации (см. Поддерживаемые базы управляющей информации SNMP на стр. 226).

По умолчанию SNMP-агент выключен и не запускается автоматически при загрузке ViPNet xFirewall. При необходимости вы можете изменить параметры запуска SNMP-агента:

- Чтобы включить автоматический запуск SNMP-агента, выполните команду:

  ```
  hostname# inet snmp mode {on | off}
  ```

- Чтобы запустить или остановить SNMP-агент, выполните команду:

  ```
  hostname# inet snmp {start | stop}
  ```

Чтобы использовать оповещения (SNMP Traps), выполните настройку следующих параметров:

- Настройте IP-адрес удаленного узла, на который будут отправляться асинхронные оповещения о различных событиях при работе ПО ViPNet, с помощью команды:

  ```
  hostname# inet snmp trapsink <IP-адрес>
  ```

Примечание. Выключить использование оповещений SNMP Traps вы можете с помощью команды:

```
hostname# inet snmp trapsink none
```

- Чтобы на удаленной станции управления сетью при приеме оповещений SNMP Traps проводилась авторизация, задайте пароль с помощью команды:

  ```
  hostname# inet snmp community trap <пароль>
  ```

- При необходимости задайте пароль доступа к SNMP-параметрам вашего ViPNet xFirewall с помощью команды:

  ```
  hostname# inet snmp community ro <пароль>
  ```

Примечание. Пароли должны содержать от 6 до 18 символов. В паролях вы можете использовать символы латинского алфавита, цифры, а также следующие специальные символы: «.», «*», «/», «-», «:», «_», «=», «@», «&».

Просмотреть текущие значения паролей вы можете с помощью команды:

```
hostname> inet show snmp community
```

Информация о работе SNMP-агента записывается в системный журнал. Чтобы настроить уровень детализации записываемой информации, выполните команду:

```
hostname# inet snmp debug-level <уровень детализации>
```

В качестве уровня детализации вы можете задать следующие значения:

- `info` (по умолчанию) — записывается только информация, касающаяся инициализации SNMP-агента. Этот уровень задан .
- `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.
- `off` — запись выключена.

Чтобы получить информацию о текущем состоянии SNMP-агента, IP-адресе удаленного узла, на который отправляются оповещения (SNMP Traps), а также о заданном уровне детализации, выполните команду:

```
hostname> inet show snmp
```

Описание SNMP-параметров для ПО ViPNet xFirewall

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

- .1.3.6.1.4.1.10812.1.1.1 — шестнадцатеричный идентификатор сети ViPNet.
- .1.3.6.1.4.1.10812.1.1.2 — шестнадцатеричный идентификатор сетевого узла ViPNet.
- .1.3.6.1.4.1.10812.1.1.3 — имя пользователя узла ViPNet.
- .1.3.6.1.4.1.10812.1.1.4 — время работы ViPNet xFirewall (обнуляется каждый раз при перезапуске управляющего демона).
- .1.3.6.1.4.1.10812.1.1.5 — шестнадцатеричный идентификатор, включающий в себя идентификаторы узла ViPNet и сети ViPNet.
- .1.3.6.1.4.1.10812.1.1.7 — имя узла ViPNet.
- .1.3.6.1.4.1.10812.1.2.1 — количество сетевых интерфейсов.
- .1.3.6.1.4.1.10812.1.2.2 — последовательность объектов, описывающих сетевые интерфейсы.
- .1.3.6.1.4.1.10812.1.2.2.1 — объекты, описывающие сетевые интерфейсы:
  - .1.3.6.1.4.1.10812.1.2.2.1.1 — номер интерфейса;
  - .1.3.6.1.4.1.10812.1.2.2.1.2 — системное имя интерфейса;
  - .1.3.6.1.4.1.10812.1.2.2.1.3 — устаревший параметр, всегда равен 0;
  - .1.3.6.1.4.1.10812.1.2.2.1.4 — число пропущенных входящих нешифрованных пакетов;
  - .1.3.6.1.4.1.10812.1.2.2.1.5 — число блокированных входящих нешифрованных пакетов;
  - .1.3.6.1.4.1.10812.1.2.2.1.6 — число пропущенных исходящих нешифрованных пакетов;
  - .1.3.6.1.4.1.10812.1.2.2.1.7 — число блокированных исходящих нешифрованных пакетов;
  - .1.3.6.1.4.1.10812.1.2.2.1.8 — число пропущенных входящих шифрованных пакетов;
  - .1.3.6.1.4.1.10812.1.2.2.1.9 — число блокированных входящих шифрованных пакетов;
  - .1.3.6.1.4.1.10812.1.2.2.1.10 — число пропущенных исходящих шифрованных пакетов;
  - .1.3.6.1.4.1.10812.1.2.2.1.11 — число блокированных исходящих шифрованных пакетов.
- .1.3.6.1.4.1.10812.1.7 — последовательность объектов, описывающих состояние демонов iplircfg, failoverd, mftpd, webgui-fcgi-server (подробнее о демонах ViPNet xFirewall см. в приложении Список демонов в составе ПО ViPNet xFirewall (на стр. 249)).
- .1.3.6.1.4.1.10812.1.7.1 — объекты, описывающие состояние демонов ViPNet xFirewall:
  - .1.3.6.1.4.1.10812.1.7.1.1 — индекс демона;
  - .1.3.6.1.4.1.10812.1.7.1.2 — имя демона:
    - `Failover` — демон failoverd,

        - `Iplir` — демон iplircfg,
        - `Mftp` — демон mftpd,
        - `Webgui` — демон webgui-fcgi-server;
    - .1.3.6.1.4.1.10812.1.7.1.3 — состояние демона:
        - `unknown(0)` — состояние неизвестно,
        - `shutdown(1)` — работа демона завершена,
        - `running(2)` — демон работает;
    - .1.3.6.1.4.1.10812.1.7.1.4 — время работы демона.
- .1.3.6.1.4.1.10812.4.3.1 — версия агента мониторинга.
- .1.3.6.1.4.1.10812.4.3.2 — уникальный идентификатор установки агента мониторинга.
- .1.3.6.1.4.1.10812.4.4 — таблица плагинов агента мониторинга.
- .1.3.6.1.4.1.10812.4.5 — таблица функциональных возможностей агента мониторинга.
- .1.3.6.1.4.1.10812.4.20.5 — уникальный идентификатор устройства.

ПО ViPNet использует следующие оповещения SNMP (SNMP Traps):

- .1.3.6.1.4.1.10812.1.0.1 — запуск управляющего демона.
- .1.3.6.1.4.1.10812.1.0.2 — завершение работы управляющего демона.
- .1.3.6.1.4.1.10812.1.0.3 — запуск демона mftpd.
- .1.3.6.1.4.1.10812.1.0.4 — завершение работы демона mftpd.
- .1.3.6.1.4.1.10812.1.0.7 — запуск демона failoverd (только в активном режиме).
- .1.3.6.1.4.1.10812.1.0.8 — завершение работы демона failoverd (только в активном режиме).

Примечание. Как правило, NMS позволяет настроить ответное действие при возникновении каждого из этих оповещений (например, отправка письма). Подробнее см. в документации по используемой NMS.

Поддерживаемые базы управляющей информации SNMP

ViPNet xFirewall частично поддерживает следующие стандартные базы управляющей информации (MIB):

- MIB-II System (.1.3.6.1.2.1.1) — база управляющей информации для системных параметров. Включает в себя объекты, предназначенные для получения информации о различных системных параметрах компьютера и операционной системы ViPNet xFirewall (например, имя сетевого узла, название ОС, название аппаратной платформы, количество и параметры сетевых интерфейсов). Подробнее см. в RFC 1213 (https://tools.ietf.org/html/rfc1213).

- IF-MIB (.1.3.6.1.2.1.2) — база управляющей информации для сетевых интерфейсов ViPNet xFirewall. Включает в себя объекты, предназначенные для получения информации о различных параметрах сетевых интерфейсов ViPNet xFirewall (например, тип интерфейса, физический адрес, скорость). Подробнее см. в RFC 2863 (https://tools.ietf.org/html/rfc2863).
- IP-MIB (.1.3.6.1.2.1.4) — база управляющей информации для протокола IP. Включает в себя объекты, предназначенные для получения информации о различных характеристиках работы ViPNet xFirewall по протоколу IP (например, параметры сетевых интерфейсов, статистика для IP-трафика, таблица адресов). Подробнее см. в RFC 4293 (https://tools.ietf.org/html/rfc4293).
- TCP-MIB (.1.3.6.1.2.1.6) — база управляющей информации для протокола TCP. Включает в себя объекты, предназначенные для получения информации о различных характеристиках работы ViPNet xFirewall по протоколу TCP (например, максимальный размер сегмента, количество активных соединений). Подробнее см. в RFC 4022 (https://tools.ietf.org/html/rfc4022).
- UDP-MIB (.1.3.6.1.2.1.7) — база управляющей информации для протокола UDP. Включает в себя объекты, предназначенные для получения информации о различных характеристиках работы ViPNet xFirewall по протоколу UDP (например, общее количество полученных и отправленных датаграмм). Подробнее см. в RFC 4113 (https://tools.ietf.org/html/rfc4113).
- HOST-RESOURCES-MIB (.1.3.6.1.2.1.25) — база управляющей информации, которая включает в себя объекты, предназначенные для получения информации о системных параметрах ViPNet xFirewall. Подробнее см. RFC 2790 (https://tools.ietf.org/html/rfc2790). На данный момент поддерживаются следующие системные параметры:
    - HOST-RESOURCES-MIB (.1.3.6.1.2.1.25.1.1.0) hrSystemUptime — длительность работы ViPNet xFirewall с момента последнего запуска.
- UCD-SNMP-MIB (.1.3.6.1.4.1.2021) — база управляющей информации для протокола SNMP. Включает в себя объекты, предназначенные для получения информации о состоянии компьютера и операционной системы (например, состояние оперативной памяти и жесткого диска). Подробнее см. на веб-ресурсе http://www.net-snmp.org/docs/mibs/UCD-SNMP-MIB.txt.
- SNMP-FRAMEWORK-MIB (.1.3.6.1.6.3.10) — база управляющей информации, которая включает в себя параметры для получения информации о динамически загружаемых модулях SNMP в ViPNet xFirewall. Подробнее см. на веб-ресурсе http://www.net-snmp.org/docs/mibs/snmpFrameworkMIB.html.

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 13. 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 14. 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 15. 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. 76), перечисленные в таблице ниже.

Таблица 16. 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 33. Классификация событий в журнале IP-пакетов

Описание типов событий каждой подгруппы приведено в таблицах.

*Таблица 17. 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 18. 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 19. 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 20. 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 21. 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 22. 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

Структура записи журнала регистрации IP-пакетов в формате CEF

Запись журнала регистрации IP-пакетов в формате CEF (см. CEF (Common Event Format) на стр. 270) состоит из полей заголовка CEF и полей записи журнала регистрации IP пакетов ViPNet xFirewall:

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

где:

- `Version` — номер версии CEF-нотации. Значение равно 0;
- `Device Vendor, Device Product, Device Version` — идентификатор устройства (производитель, продукт, версия);
- `Signature ID` — номер события (см. Типы событий в журнале регистрации IP-пакетов на стр. 235) в журнале регистрации IP-пакетов;
- `Name` — описание события (см. Типы событий в журнале регистрации IP-пакетов на стр. 235) в журнале регистрации IP-пакетов;
- `Severity` — число, показывающее важность IP-пакета. Допустимый диапазон 1 — 10;
- `Extension` — набор пар ключ-значение, разделенных пробелом, из словаря CEF.

Таблица 23. Соответствие имен ViPNet xFirewall именам словаря CEF

Описание в ViPNet xFirewall	Имя в ViPNet xFirewall	Короткое имя словаря CEF
Начало интервала времени UTC, в течение которого несколько	Interval Begin	start

Описание в ViPNet xFirewall	Имя в ViPNet xFirewall	Короткое имя словаря CEF
событий были объединены в одну запись журнала IP-пакетов		
Конец интервала времени UTC, в течение которого несколько событий были объединены в одну запись журнала IP-пакетов	Interval End	end
IP-адрес отправителя пакетов	Source IP	src
Порт отправителя пакетов	Source port	spt
IP-адрес получателя пакетов	Destination IP	dst
Порт получателя пакетов	Destination port	dpt
Тип транспортного протокола (TCP/UDP)	IP protocol	proto
Число пакетов, соответствующих выбранному типу события	Count	cnt
Размер входящих пакетов, соответствующих выбранному типу события	size in	in
Размер исходящих пакетов, соответствующих выбранному типу события	size out	out
Имя сетевого интерфейса, на котором были зарегистрированы события	Interface	deviceInboundInterface deviceOutboundInterface
Шестнадцатеричный идентификатор протокола Ethernet	Eth. protocol	cn1 cn1Label=Eth<space>protocol<space>hex
Направление пакета (входящий, исходящий)	Direction	deviceDirection
• NAT — флаг транслированного пакета; • Drop — флаг блокировки пакета; • Broadcast — флаг широковещательного пакета; • Forward — флаг транзитного пакета; • Encrypted — флаг зашифрованного пакета		• cs1=NAT<space>{yes|no} • cs2=Drop<space>{yes|no} • cs3=Broadcast<space>{yes|no} • cs4=Forward<space>{yes|no} • cs5=Encrypted<space>{yes|no}

Описание в ViPNet xFirewall	Имя в ViPNet xFirewall	Короткое имя словаря CEF
		cs1Label=Flags
Название прикладного протокола	App protocol	app
Название приложения	Application	cs6 cs6Label=Application<space>name
Имя пользователя сети	Network user	suser
Номер и имя сетевого узла ViPNet	Source node	shost
Номер и имя сетевого узла ViPNet	Destination node	dhost

E

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 24. 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 25. 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 26. 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 27. 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 28. 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`

F

Список демонов в составе ПО ViPNet xFirewall

Ниже приведен список демонов в составе ПО ViPNet xFirewall, для которых можно настроить фильтрацию вывода записей журнала событий (см. Настройка параметров ведения журнала событий на стр. 216):

Демоны ViPNet:

- failover, failoverd — демон слежения за основными службами ViPNet и организации кластера;
- iplircfg — демон, управляющий настройками драйвера перехвата сетевого трафика, ведения журнала IP пакетов, обновления справочно-ключевой информации;
- iplirpasswd — утилита проверки паролей пользователя и администратора ViPNet;
- logQos — демон, управляющий сбором статистики приоритетной обработки трафика;
- mftp, mftpd — демон транспортного сервиса ViPNet;
- pace2_nfq_smp5 — демон модуля DPI;
- rvpn_shell — командный интерпретатор ViPNet;
- scripts — скрипты первичной инициализации ViPNet xFirewall;
- session_watcher — демон, отслеживающий сессии пользователей ViPNet;
- uc — демон управления пользователями сети;
- unmerge — утилита распаковки дистрибутива справочников и лицензии;
- vpncmd — демон, командного интерпретатора, отвечающий за изменение правил межсетевого экрана;
- vpn-snmpd — демон SNMP;

- vupgrade — утилита обновления ПО ViPNet xFirewall;
- webgui (webgui_captive_portal, webgui-fcgi-server, webgui_php, webgui_frontend) — демон веб-интерфейса ViPNet xFirewall.

Демоны Linux:

- acpid (ACPI event daemon) — демон для реакции на ACPI события, например, реакция на нажатие кнопки питания;
- crond — демон для запуска задач по расписанию;
- freeradius — демон RADIUS-серверf для поддержки Captive Portal;
- login — демон для аутентификации пользователя и открытия его сессии;
- named — демон DNS;
- ntpd — демон NTP;
- pcscd — демон pcsc для работы с токенами;
- sshd — демон SSH;
- squid3 — демон прокси-сервера squid, фильтрации содержимого трафика и антивирусной проверки по протоколу ICAP;
- syslogd — демон системного журнала;
- udhcpcd — демон DHCP-клиента;
- udhcpd — демон DHCP-сервера;
- upsd — демон UPS;
- upsmon — демон монитора UPS;
- vmunix — ядро системы;
- watchquagga — демон слежения за службой динамической маршрутизации;
- xinetd — демон, запускающий сетевые серверные процессы;
- zebra — демон динамической маршрутизации;
- zdhcpd — демон протокола DHCP службы динамической маршрутизации;
- zospfd — демон протокола OSPF службы динамической маршрутизации.

Модули ядра ViPNet:

- bonding (bonding_helper) — скрипт управления модуля ядра, реализующего функционал агрегированных каналов;
- drviplir — драйвер перехвата сетевого трафика (модуль ядра);
- itcscrpt — крипто-драйвер шифрования IP-пакетов (модуль ядра) для защиты канала управления;
- itcskrniface — интерфейс-драйвер перехвата сетевого трафика;
- itcswd — драйвер демона Watch dog.

G

Поддерживаемые приложения

Ниже приведен список приложений, которые можно указать в параметре `dpiapp <название приложение>` при создании транзитного фильтра открытой сети (см. Приложение на стр. 86).

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

Поддерживаемые прикладные протоколы

Ниже приведен список прикладных протоколов, которые можно указать в параметре `dpiprotocol <название протокола>` при создании транзитного фильтра открытой сети (см. Прикладной протокол на стр. 87).

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

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 (см. Прикладной протокол на стр. 87).

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

J

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. 96). 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.

- **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.

Поддерживаемые типы содержимого

Ниже приведен список MIME-типов, которые можно указать в параметре `<тип содержимого>` при настройке правил фильтрации содержимого трафика (см. Настройка фильтрации содержимого трафика на стр. 116).

- **Application — Внутренний формат прикладной программы**
  - application/atom+xml: Atom
  - application/EDI-X12: EDI X12 (RFC 1767)
  - application/EDIFACT: EDI EDIFACT (RFC 1767)
  - application/json: JavaScript Object Notation JSON (RFC 4627)
  - application/javascript: JavaScript (RFC 4329)
  - application/octet-stream: двоичный файл без указания формата (RFC 2046)
  - application/ogg: Ogg (RFC 5334)
  - application/pdf: Portable Document Format, PDF (RFC 3778)
  - application/postscript: PostScript (RFC 2046)
  - application/soap+xml: SOAP (RFC 3902)
  - application/font-woff: Web Open Font Format
  - application/xhtml+xml: XHTML (RFC 3236)
  - application/xml-dtd: DTD (RFC 3023)
  - application/xop+xml:XOP
  - application/zip: ZIP

- application/gzip: Gzip
- application/x-bittorrent: BitTorrent
- application/x-tex: TeX

- **audio — Аудио**
  - audio/basic: mulaw аудио, 8 кГц, 1 канал (RFC 2046)
  - audio/L24: 24bit Linear PCM аудио, 8-48 кГц, 1-N каналов (RFC 3190)
  - audio/mp4: MP4
  - audio/aac: AAC
  - audio/mpeg: MP3 или др. MPEG (RFC 3003)
  - audio/ogg: Ogg Vorbis, Speex, Flac или др. аудио (RFC 5334)
  - audio/vorbis: Vorbis (RFC 5215)
  - audio/x-ms-wma: Windows Media Audio
  - audio/x-ms-wax: Windows Media Audio перенаправление
  - audio/vnd.rn-realaudio: RealAudio
  - audio/vnd.wave: WAV(RFC 2361)
  - audio/webm: WebM
- **image — Изображение**
  - image/gif: GIF(RFC 2045 и RFC 2046)
  - image/jpeg: JPEG (RFC 2045 и RFC 2046)
  - image/pjpeg: JPEG
  - image/png: Portable Network Graphics[9](RFC 2083)
  - image/svg+xml: SVG
  - image/tiff: TIFF(RFC 3302)
  - image/vnd.microsoft.icon: ICO
  - image/vnd.wap.wbmp: WBMP
- **message — Сообщение**
  - message/http (RFC 2616)
  - message/imdn+xml: IMDN (RFC 5438)
  - message/partial: E-mail (RFC 2045 и RFC 2046)
  - message/rfc822: E-mail; EML файлы, MIME файлы, MHT файлы, MHTML файлы (RFC 2045 и RFC 2046)
- **model — Для 3D моделей**
  - model/example: (RFC 4735)

- model/iges: IGS файлы, IGES файлы (RFC 2077)
- model/mesh: MSH файлы, MESH файлы (RFC 2077), SILO файлы
- model/vrml: WRL файлы, VRML файлы (RFC 2077)
- model/x3d+binary: X3D ISO стандарт для 3D компьютерной графики, X3DB файлы
- model/x3d+vrml: X3D ISO стандарт для 3D компьютерной графики, X3DV VRML файлы
- model/x3d+xml: X3D ISO стандарт для 3D компьютерной графики, X3D XML файлы
- multipart
- multipart/mixed: MIME E-mail (RFC 2045 и RFC 2046)
- multipart/alternative: MIME E-mail (RFC 2045 и RFC 2046)
- multipart/related: MIME E-mail (RFC 2387 и используемое MHTML (HTML mail))

- **multipart — составные файлы**
  - multipart/form-data: MIME Webform (RFC 2388)
  - multipart/signed: (RFC 1847)
  - multipart/encrypted: (RFC 1847)
- **text — Текст**
  - text/cmd: команды
  - text/css: Cascading Style Sheets (RFC 2318)
  - text/csv: CSV (RFC 4180)
  - text/html: HTML (RFC 2854)
  - text/javascript (Obsolete): JavaScript(RFC 4329)
  - text/plain: текстовые данные (RFC 2046 и RFC 3676)
  - text/php: Скрипт языка PHP
  - text/xml: Extensible Markup Language (RFC 3023)
- **video — Видео**
  - video/mpeg: MPEG-1 (RFC 2045 и RFC 2046)
  - video/mp4: MP4 (RFC 4337)
  - video/ogg: Ogg Theora или другое видео (RFC 5334)
  - video/quicktime: QuickTime
  - video/webm: WebM
  - video/x-ms-wmv: Windows Media Video
  - video/x-flv: FLV
  - video/3gpp: .3gpp .3gp
  - video/3gpp2: .3gpp2 .3g2

- **vnd — Вендорные файлы**
  - application/vnd.oasis.opendocument.text: OpenDocument
  - application/vnd.oasis.opendocument.spreadsheet: OpenDocument
  - application/vnd.oasis.opendocument.presentation: OpenDocument
  - application/vnd.oasis.opendocument.graphics: OpenDocument
  - application/vnd.ms-excel: Microsoft Excel файлы
  - application/vnd.openxmlformats-officedocument.spreadsheetml.sheet: Microsoft Excel 2007 файлы
  - application/vnd.ms-powerpoint: Microsoft Powerpoint файлы
  - application/vnd.openxmlformats-officedocument.presentationml.presentation: Microsoft Powerpoint 2007 файлы
  - application/msword: Microsoft Word файлы
  - application/vnd.openxmlformats-officedocument.wordprocessingml.document: Microsoft Word 2007 файлы
  - application/vnd.mozilla.xul+xml: Mozilla XUL файлы
  - application/vnd.google-earth.kml+xml: KML файлы (например, для Google Earth)
- **x — Нестандартные файлы**
  - application/x-www-form-urlencoded Form Encoded Data
  - application/x-dvi: DVI
  - application/x-latex: LaTeX файлы
  - application/x-font-ttf: TrueType (не зарегистрированный MIME-тип, но наиболее часто используемый)
  - application/x-shockwave-flash: Adobe Flash
  - application/x-stuffit: StuffIt
  - application/x-rar-compressed: RAR
  - application/x-tar: Tarball
  - text/x-jquery-tmpl: jQuery
  - application/x-javascript:
- **x-pks — PKCS**
  - application/x-pkcs12: p12 файлы
  - application/x-pkcs12: pfx файлы
  - application/x-pkcs7-certificates: p7b файлы
  - application/x-pkcs7-certificates: spc файлы
  - application/x-pkcs7-certreqresp: p7r файлы

- application/x-pkcs7-mime: p7c файлы
- application/x-pkcs7-mime: p7m файлы
- application/x-pkcs7-signature: p7s файлы

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.

CEF (Common Event Format)

Открытый текстовый формат описания событий. Позволяет агрегировать события различных типов сетевых устройств и приложений в едином формате.

COM-консоль

Ноутбук, подключенный к COM-порту, который используется для локальной настройки ViPNet xFirewall.

DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса серверов DNS, IP-адреса серверов WINS.

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. 271).

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. 271).

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, образованный из нескольких физических интерфейсов Ethernet, объединенных на канальном уровне сетевой модели OSI.

Административная дистанция

Характеристика маршрута. Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

Вариант персонального ключа пользователя

Номер персонального ключа пользователя из резервного набора персональных ключей (РНПК). Изменение варианта персонального ключа пользователя означает, что номер персонального ключа был увеличен на единицу и для создания новых ключей пользователя будет использоваться следующий персональный ключ из РНПК.

Вес

Параметр, который задается для шлюза в статическом маршруте 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.

Виртуальная защищенная сеть

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

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Дистрибутив лицензии

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы ПО ViPNet xFirewall.

Доверенная сеть

Сеть ViPNet, с узлами которой узлы своей сети ViPNet осуществляют защищенное взаимодействие.

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.

Источник бесперебойного питания (UPS)

Автоматическое электронное устройство с аккумуляторной батареей, предназначенное для бесперебойного кратковременного снабжения электрической энергией компьютера и его

компонентов с целью корректного завершения работы и сохранения данных в случае резкого падения или отсутствия входного питающего напряжения системы.

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. Клиент должен быть зарегистрирован на координаторе. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключи узла ViPNet xFirewall

Совокупность ключей, с использованием которых производится шифрование служебной информации, передаваемой между ViPNet xFirewall и узлами сети ViPNet. Шифрование трафика клиентов сети ViPNet на ключах узла ViPNet xFirewall не производится.

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.

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.

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.

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Файлы в DER-кодировке X.509

DER (Distinguished Encoding Rules) для ASN.1, как определено в рекомендации ITU-T Recommendation X.509, – более ограниченный стандарт кодирования, чем альтернативный BER (Basic Encoding Rules) для ASN.1, определенный в рекомендации ITU-T Recommendation X.209, на котором основан DER. И BER, и DER обеспечивают независимый от платформы метод кодирования объектов, таких как сертификаты и сообщения, для передачи между устройствами и приложениями.

При кодировании сертификата большинство приложений используют стандарт DER, так как сертификат (сведения о запросе на сертификат) должен быть закодирован с помощью DER и подписан. Файлы сертификатов DER имеют расширение .cer.

Более подробное описание изложено в документе «ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework» на веб-узле International Telecommunication Union (ITU http://www.itu.int/ru/Pages/default.aspx).