ViPNet xFirewall

Справочное руководство по командному интерпретатору и конфигурационным файлам

infotecs

© 1991 – 2018 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00217-01 90 17

Версия продукта 4.1.0

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

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

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

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

ОАО «ИнфоТеКС»

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

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

Веб-сайт: https://infotecs.ru/

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Документ содержит описание команд, доступных для выполнения в командном интерпретаторе ViPNet xFirewall (см. глоссарий, стр. 298). В нем приведены синтаксис команд, руководство по использованию, а также примеры команд. Команды сгруппированы по первому слову, список групп и список команд внутри каждой группы упорядочены по алфавиту.

Также в документе приведено подробное описание параметров следующих конфигурационных файлов ViPNet xFirewall:

- `iplir.conf` — конфигурационный файл управляющего демона (см. Файл iplir.conf на стр. 264).
- `iplir.conf-<интерфейс или группа интерфейсов>` — конфигурационные файлы сетевых интерфейсов ViPNet xFirewall.
- `failover.ini` — конфигурационный файл системы защиты от сбоев (см. Файл failover.ini на стр. 277).
- `mftp.conf` — конфигурационный файл транспортного модуля MFTP (см. Файл mftp.conf на стр. 284).

Параметры в конфигурационных файлах используются для настройки ViPNet xFirewall. Некоторые параметры задаются программным обеспечением (далее — ПО) ViPNet® автоматически, они носят информационный характер и служат для того, чтобы администратор в процессе работы мог посмотреть их значения для выполнения каких-либо настроек или подключения к ViPNet xFirewall. Изменять такие параметры вручную не следует, в данном документе они называются нередактируемыми и описаны в специальных подразделах.

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}
  ```

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

Справочник команд

Команды группы admin

Команды группы `admin` предназначены для управления копиями конфигурации, обновления ПО и выполнения других административных задач.

admin config delete

Команда используется для удаления копии конфигурации с заданным именем.

Синтаксис

```
admin config delete <имя> [<версия vpn>]
```

Параметры и ключевые слова

- `<имя>` — имя копии конфигурации.
- `<версия vpn>` — версия VPN-компонента ViPNet, к которой относится копия конфигурации. Указывается в формате `Major.Minor.Subminor`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе имени работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка сохраненных копий конфигурации.
- В имени можно указать символ «*» для обозначения любого количества символов. Это позволяет производить удаление сразу нескольких копий конфигурации.
- Если имя копии конфигурации состоит из нескольких слов либо если для указания имени используется маска, заключите его в кавычки.
- Если версия не указана и при этом имеется несколько копий конфигурации с совпадающими именами, но различными версиями, то выводится список таких копий конфигурации с предложением указать версию для удаления.

Примеры использования

Для удаления всех сохраненных копий конфигурации, у которых имя начинается с «Config_», выполните команду:

```
hostname# admin config delete "Config_*"
```

Для удаления копии конфигурации Config_1, относящейся к версии vpn с номером 4.3.0 выполните команду:

```
hostname# admin config delete Config_1 4.3.0
Configuration 'Config_1' (version 4.3.0) deleted
```

admin config list

Команда предназначена для просмотра текущего списка сохраненных копий конфигурации.

Синтаксис

```
admin config list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# admin config list
"Config_1", version 4.3.0, full, saved on 31.07.2017 at 20:06, never loaded
hostname#
```

Список сохраненных копий конфигурации отображается в следующем формате:

```
"Name", Version, Type, saved on Date at Time, loaded at Date-load at Time-load
```

где:

- `Name` — имя копии конфигурации; имя автоматически сохраненной копии конфигурации начинается со слова `autosave`.
- `Version` — версия VPN-компонента ViPNet, в которой была создана копия конфигурации.
- `Type` — вид копии конфигурации: `full` (полная) или `part` (частичная).
- `Date`, `Time` — дата и время создания копии конфигурации.
- `Date-load`, `Time-load` — дата и время загрузки копии конфигурации. Если копия конфигурации никогда не загружалась, вместо даты и времени загрузки отображается `never loaded`.

admin config load

Команда используется для загрузки (восстановления) настроек ViPNet xFirewall из копии конфигурации с заданным именем.

Синтаксис

```
admin config load <имя> [<версия vpn>]
```

Параметры и ключевые слова

- `<имя>` — имя копии конфигурации.
- `<версия vpn>` — версия VPN-компонента ViPNet, к которой относится копия конфигурации. Указывается в формате `Major.Minor.Subminor`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе имени работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка сохраненных копий конфигурации.
- Если версия не указана и при этом имеется несколько копий конфигурации с совпадающими именами, но различными версиями, то выводится список таких копий конфигурации с предложением указать версию для загрузки.
- Перед загрузкой настроек из копии конфигурации запрашивается подтверждение для сохранения копии текущей конфигурации. В случае подтверждения требуется ввести имя, под которым будет сохранена копия текущей конфигурации.

- Если текущая версия vpn-компонента ниже версии, указанной в команде, то требуется дополнительно подтвердить загрузку настроек из копии конфигурации.

Пример использования

Для загрузки настроек из копии конфигурации с именем Rollback_config, относящейся к версии 4.3.0, выполните команду:

```
hostname# admin config load Rollback_config 4.3.0
```

admin config save

Команда используется для сохранения копии текущей конфигурации с заданным именем.

Синтаксис

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

Параметры и ключевые слова

`<имя>` — имя копии конфигурации.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- В имени можно использовать только символы латинского алфавита, цифры, знаки «дефис» и «подчеркивание».
- Если в списке сохраненных копий конфигурации есть копия конфигурации с указанным именем, то запрашивается подтверждение на перезапись этой копии конфигурации.

Пример использования

Для сохранения копии текущей конфигурации под именем Rollback_config выполните команду:

```
hostname# admin config save Rollback_config
```

admin escape

Команда используется для выхода в системную командную оболочку.

Внимание! Команда предназначена для использования опытными администраторами в целях отладки. ОАО «ИнфоТеКС» не гарантирует нормальную работу ViPNet xFirewall в случае некорректных действий администратора в системной командной оболочке.

Синтаксис

```
admin escape
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе команды автозаполнение не работает.
- После выполнения команды требуется указать пароль администратора сетевого узла ViPNet.
- После выхода из системной командной оболочки интерпретатор продолжит свою работу с того момента, в которой он находился перед запуском системной оболочки.

Пример использования

```
hostname# admin escape
This command is intended solely for the purposes of debugging.
It should only be used by InfoTeCS support team, or people who
 were explicitly advised to use it by InfoTeCS support team.
InfoTeCS does not guarantee normal operation of ViPNet xFirewall
 in case of incorrect user actions in the system shell.
Do you really wish to escape to Linux system shell?[Yes,No]:Yes
Type the administrator password:
sh-4.2#
```

admin export keys binary-encrypted

Команда используется для экспорта справочников, лицензии (см. глоссарий, стр. 301) и настроек ViPNet xFirewall на ноутбук (по TFTP) или на USB-носитель.

Синтаксис

```
admin export keys binary-encrypted {tftp | usb}
```

Параметры и ключевые слова

- `tftp` — экспорт на ноутбук по протоколу TFTP.
- `usb` — экспорт на USB-носитель.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Экспортировать справочники, лицензию и настройки в удаленной SSH-сессии запрещено.
- Перед выполнением команды требуется завершить работу демонов `iplircfg` (см. iplir stop на стр. 155) и `mftpd` (см. mftp stop на стр. 184).
- Если вы выбрали экспорт по TFTP и на ViPNet xFirewall запущен DHCP-сервер (см. глоссарий, стр. 293), то до начала экспорта его работа будет автоматически завершена, а после окончания экспорта — автоматически восстановлена.
- В случае экспорта на USB-носитель необходимо дождаться сообщения с разрешением извлечь устройство прежде, чем извлечь USB-носитель из разъема.

Пример использования

Ниже приведен пример выполнения команды с параметром `usb`:

```
hostname# admin export keys binary-encrypted usb
Configuration file will be saved to /tmp/vipnet/xfva-15ea000b-2016-09-09.vbe
Put xfva-15ea000b-2016-09-09.vbe file onto USB drive.
Insert USB drive and press Enter
1) General USB Flash Disk partition 3839Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc1 was successfully mounted on /usb.
File xfva-15ea000b-2016-09-09.vbe to be copied onto the USB drive.
File xfva-15ea000b-2016-09-09.vbe was successfully copied onto the USB drive.
```

```
You may remove the USB drive.
hostname#
```

admin export logs

Команда используется для экспорта файлов журнала событий, хранящихся на ViPNet xFirewall, на другой компьютер (по TFTP) или на USB-носитель.

Синтаксис

```
admin export logs {tftp | usb}
```

Параметры и ключевые слова

- `tftp` — экспорт на другой компьютер по протоколу TFTP.
- `usb` — экспорт на USB-носитель.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить демоны failoverd, iplir, mftpd (см. vpn stop на стр. 254).
- При выборе метода экспорта файлов журнала по протоколу TFTP внешний IP-адрес интерфейса eth1 изменится на 169.254.241.1, а остальные сетевые интерфейсы будут отключены.
- Экспортировать файлы журнала по протоколу TFTP в удаленной SSH-сессии запрещено.
- Имя файла экспорта — `logs.tar.gz`.
- Если ViPNet xFirewall работает в составе кластера горячего резервирования, экспортировать файлы журнала событий можно только на USB-носитель.

Пример использования

Ниже приведен пример выполнения команды с параметром `usb`:

```
hostname# admin export logs usb
tar: Removing leading `/' from member names
/var/log/atop
/var/log/boot.log
```

```
/var/log/dmesg.boot
/var/log/everything.log
/var/log/lastlog
/var/log/lighttpd/
/var/log/lighttpd/accesss.log
/var/log/lighttpd/error.log
/var/log/news/
/var/log/ntpstats/
/var/log/wtmp
Put logs.tar.gz file onto USB drive.
Insert USB drive and press Enter
1) JetFlash Transcend 4GB partition 3825Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdb1 as is
Partition /dev/sdb1 was successfully mounted on /usb.
File logs.tar.gz to be copied onto the USB drive.
File logs.tar.gz was successfully copied onto the USB drive.
You may remove the USB drive.
hostname#
```

admin export packetdb usb

Команда используется для экспорта журнала регистрации IP-пакетов на USB-носитель.

Синтаксис

```
admin export packetdb usb <имя>
```

Параметры и ключевые слова

`<имя>` — имя файла экспорта.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

При вводе имени файла работает автозаполнение и подсказка, данные для подсказки берутся из списка существующих файлов экспорта.

Пример использования

Чтобы экспортировать журнал регистрации IP-пакетов в файл с именем `ippacket`, выполните команду:

```
hostname# admin export packetdb usb ippacket
Put ippacket.tar.gz file onto USB drive.
Insert USB drive and press Enter
1) JetFlash Transcend 4GB partition 3825Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc as is
Partition /dev/sdc was successfully mounted on /usb.
File ippacket.tar.gz to be copied onto the USB drive.
File ippacket.tar.gz was successfully copied onto the USB drive.
You may remove the USB drive.
hostname#
```

admin kick

Команда используется для завершения сессии командного интерпретатора.

Синтаксис

```
admin kick {tty<N> | ttyS<N> | pts/<N>}
```

Параметры и ключевые слова

- `tty<N>` — номер сессии, запущенной на обычной консоли.
- `ttyS<N>` — номер сессии, запущенной на COM-консоли.
- `pts/<N>` — номер сессии, которая запущена на удаленном рабочем месте, подключенном к ViPNet xFirewall по протоколу SSH.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Нельзя завершить сессию командного интерпретатора, в которой выполняется команда. Для завершения такой сессии следует использовать команду `exit` (см. exit на стр. 259).
- Для просмотра информации обо всех запущенных сессиях командного интерпретатора используется команда `who` (см. who на стр. 261).

Пример использования

Для завершения работы командного интерпретатора на компьютере tty1 выполните команду:

```
hostname# admin kick tty1
```

admin passwd

Команда используется для изменения пароля пользователя ViPNet xFirewall.

Синтаксис

```
admin passwd
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды требуется ввести текущий пароль пользователя или пароль администратора, затем дважды ввести новый пароль.
- При вводе паролей на экране ничего не отображается, введенные символы отредактировать нельзя.
- Минимальная длина нового пароля — 6 символов.
- Чтобы изменить пароль пользователя на ViPNet xFirewall, работающих в режиме кластера горячего резервирования, выполните команду сначала на сервере, функционирующем в пассивном режиме, а затем на сервере, функционирующем в активном режиме. Пароли, задаваемые на обоих серверах, должны совпадать.

 **Совет.** Рекомендуется задавать сложные пароли, содержащие не менее 8 символов.

Пример использования

```
hostname# admin passwd
Enter the user password to be changed or current admin password:
```

```
Type the new user password:
Confirm the new user password:
The new password has been successfully set.
Dumpling data files...
Data files were dumped successfully
hostname#
```

admin remove keys

Команда используется для удаления лицензии и справочников ViPNet xFirewall.

Синтаксис

```
admin remove keys
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда недоступна в удаленной SSH-сессии.
- Если на ViPNet xFirewall запущен DHCP-сервер, то его работа будет автоматически завершена.

Пример использования

```
hostname# admin remove keys
This command removes all ViPNet keys and cannot be reverted,
it will be necessary to deploy new keys after executing this command.
Do you really wish to execute this command?[Yes,No]
Yes
DHCP server is already off. Command ignored.
DNS server is already off. Command ignored.
NTP server is already off. Command ignored.
Stopping all VPN services
...
server login:
```

admin remove logs

Команда используется для удаления файлов журнала событий и журнала транспортных конвертов MFTP.

Синтаксис

```
admin remove logs
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# admin remove logs
ALL SYSTEM LOGS WILL BE REMOVED. ARE YOU SURE? (Yes/No) Yes
All logs are removed
hostname#
```

admin upgrade dpi usb

Команда используется для обновления модуля DPI (см. глоссарий, стр. 294) вручную с USB-носителя.

Синтаксис

```
admin upgrade dpi usb
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Выполнять команду необходимо только при подключении к ViPNet xFirewall через COM-консоль (см. глоссарий, стр. 293) или обычную консоль (см. глоссарий, стр. 299). Выполнение команды в удаленной SSH-сессии невозможно.
- При выполнении команды останавливается работа сетевого экрана и блокируются все сетевые соединения ViPNet xFirewall.
- После обновления модуля DPI потребуется перезагрузка ViPNet xFirewall.

Пример использования

```
hostname# admin upgrade dpi usb

During update, firewall will be stopped and all connections will be blocked. Are you
sure you want to continue? [y/n]: y
Insert USB flash drive into empty USB slot and press <Enter>
Select file to use for DPI upgrade:
1 — /mnt/tmp/sdb1/dpi.lzh
Enter file number [1-1] or [q] to cancel: 1
Check file dpiimg.dat successfully
Check for enough main disk size
Stop network interface eth0
Stop ViPNet
...
Done.
DPI UPGRADE WAS SUCCESSFULL!
Machine will be rebooted. Remove USB disk and press <Enter>
hostname#
```

admin upgrade software usb

Команда используется для обновления ПО ViPNet xFirewall вручную с USB-носителя.

Синтаксис

```
admin upgrade software usb
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды рекомендуется проверить подлинность и целостность файла обновления. Для этого вычислите контрольную сумму файла по алгоритму MD5, а затем сравните ее с контрольной суммой, приведенной в файле с расширением `*.md5`, который поставляется с файлом обновления.

Пример использования

```
hostname# admin upgrade software usb
Insert USB flash drive into empty USB slot and press <Enter>
Select file to use for software upgrade:
1 — /mnt/tmp/sdb1/driv.lzh
Enter file number [1-1] or [q] to cancel: 1
vupgrade    — Melted : o
This is xfva platform
Stop VPN daemons
...
To apply upgrades reboot the computer
hostname#
```

Команды группы alg

Команды группы `alg` предназначены для управления обработкой прикладных протоколов.

alg module process off

Команда используется для выключения обработки прикладного протокола FTP, H.323, SCCP или SIP.

Синтаксис

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

Параметры и ключевые слова

`<прикладной протокол>` — имя прикладного протокола: `ftp`, `h323`, `sccp` или `sip`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для выключения обработки прикладного протокола DNS выполните команду:

```
hostname# alg module ftp process off

Waiting for alg daemon..

hostname#
```

alg module process on

Команда используется для включения обработки прикладного протокола FTP, H.323, SCCP или SIP либо изменения параметров обработки этого протокола.

Синтаксис

```
alg module <прикладной протокол> process {tcp | udp} <порты> on
```

Параметры и ключевые слова

- `<прикладной протокол>` — имя обрабатываемого прикладного протокола: `ftp`, `h323`, `sccp` или `sip`.
- `tcp` — протокол TCP для обработки.
- `udp` — протокол UDP для обработки.
- `<порты>` — номера портов для обработки.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- В качестве портов можно указать один порт, диапазон портов либо список портов и диапазонов портов, перечисленных через запятую.
- Нулевое значение порта означает выключение обработки прикладного протокола указанным сетевым протоколом.

Пример использования

Чтобы включить обработку прикладного протокола FTP по портам 20, 21 и 26 для протокола TCP, выполните команду:

```
hostname# alg module ftp process tcp 20-21,26 on

Waiting for alg daemon..

hostname#
```

alg show

Команда предназначена для просмотра текущих параметров обработки прикладных протоколов.

Синтаксис

```
alg show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> alg show

=================================================
SERVICE       PROTOCOLPORTS                 ON/OFF

=================================================
FTP           TCP     21                    ON

-------------------------------------------------
H323          TCP     1720                  ON

-------------------------------------------------
H323          UDP     1719                  ON

-------------------------------------------------
SCCP          TCP     2000                  ON

-------------------------------------------------
SIP           TCP     5060                  ON
-------------------------------------------------
SIP           UDP     5060                  ON

-------------------------------------------------
hostname>
```

Таблица с параметрами обработки содержит следующие столбцы:

- `SERVICE` — название прикладного протокола.
- `PROTOCOL` — транспортный протокол для обработки.
- `PORTS` — порты для обработки.
- `ON/OFF` — состояние обработки: `ON` (включена) или `OFF` (выключена).

Команды группы failover

Команды группы `failover` предназначены для настройки и управления системой защиты от сбоев ViPNet xFirewall.

failover config edit

Команда используется для редактирования файла конфигурации системы защиты от сбоев.

Синтаксис

```
failover config edit
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

По команде будет запущен текстовый редактор с файлом конфигурации `failover.ini`.

Пример использования

```
hostname# failover config edit
GNU nano 1.3.7     File: /etc/failover.ini
[network]
checktime = 10
timeout = 2
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes
...
hostname#
```

failover config mode

Команда используется для установки режима работы системы защиты от сбоев.

Синтаксис

```
failoverd config mode {single | cluster}
```

Параметры и ключевые слова

- `single` — одиночный режим.
- `cluster` — режим кластера (см. глоссарий, стр. 297).

Значения по умолчанию

По умолчанию установлен одиночный режим (`single`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- При установке режима кластера автоматически будет завершена работа драйверов и демонов, которые не поддерживаются в этом режиме.
- При установке одиночного режима автоматически будет завершена работа всех демонов.

Пример использования

Для установки режима кластера выполните команду:

```
hostname# failoverd config mode cluster
Note: the following services are NOT allowed to run in cluster mode:
        DHCP
        HTTPPROXY
If any of them are currently running, please stop them.
Do you want to stop all services that are not allowed to run in cluster mode
now?[Yes,No]:
Yes
You have approved services stopping. Proceeding...
Switching to cluster mode. Attempt to stop the following services: DHCP
DHCP server is STOPPED. Command is ignored
Switching to cluster mode. Attempt to stop the following services: HTTPPROXY
HTTP Proxy is already stopped
Installing ViPNet failover system
hostname#
```

failover show config

Команда предназначена для просмотра файла конфигурации системы защиты от сбоев.

Синтаксис

```
failover show config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Для завершения просмотра файла конфигурации используется клавиша **Q**.

Пример использования

```
hostname> failover show config
[network]
checktime = 10
timeout = 2
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes
...
hostname>
```

failover show info

Команда предназначена для просмотра информации о текущем состоянии системы защиты от сбоев.

Синтаксис

```
failover show info
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> failover show info
Running failover info
Versions: ViPNet 4.0.6 (329), daemon 1.5 (1)
Workstation configured for ID 2AEE001D (xF)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1495459784) Mon May 22 16:29:44 2017

failover mode   * single
failover uptime * 0d  0:15
total cpu       * 2%
total memory    * 2055396 kB
free memory     * 1773220 kB
failover state  * works
failover cpu    * 1
iplir state     * works
iplir cpu       * 1
mftp state      * works
mftp cpu        * 1
webgui state    * works
webgui cpu      * 0%
dpi state       * works
dpi cpu         * 3%
uc state        * works
uc cpu          * 5%
hostname>
```

По команде отображается следующая информация:

- версия ПО ViPNet xFirewall и версия демона failoverd;
- информация о сетевом узле;
- локальное время на узле;
- режим работы системы защиты от сбоев (одиночный или режим кластера);

- информация об использовании процессора и оперативной памяти;
- информация о текущем состоянии управляющего демона, демонов mftpd, failoverd, веб-интерфейса и модуля DPI.

failover start

Команда используется для запуска демона `failoverd`, отвечающего за функционирование системы защиты от сбоев.

Синтаксис

```
failover start [{active | passive}]
```

Параметры и ключевые слова

- `active` — запуск демона failoverd в активном режиме.
- `passive` — запуск демона failoverd в пассивном режиме.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Параметр можно указать только при работе системы защиты от сбоев в режиме кластера.
- Если в режиме кластера параметр не указан, демон `failoverd` будет запущен в том режиме, в котором он находился до завершения работы.
- Перед запуском демона `failoverd` в активном режиме необходимо убедиться, что на другом ViPNet xFirewall кластера демон `failoverd` запущен в пассивном режиме. Запуск демона `failoverd` в активном режиме на обоих элементах кластера приведет к конфликту IP-адресов и другим нежелательным последствиям.

Пример использования

Чтобы запустить демон `failoverd` в пассивном режиме, выполните команду:

```
hostname> failover start passive
```

failover stop

Команда используется для завершения работы демона `failoverd`, отвечающего за функционирование системы защиты от сбоев.

Синтаксис

```
failover stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> failover stop
Shutting down failover daemon
hostname>
```

failover view

Команда предназначена для просмотра журнала переключений кластера горячего резервирования за заданный период времени.

Синтаксис

```
failover view <начало> <конец>
```

Параметры и ключевые слова

- `<начало>` — начало периода. Указывается в формате `DD.MM.YYYY[.hh.mm.ss]`, где `DD` — день, `MM` — месяц, `YYYY` — год, `hh` — час, `mm` — минуты, `ss` — секунды. Время можно не задавать.

- `<конец>` — конец периода. Указывается в том же формате, что и начало периода.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Команда работает только в том случае, когда ViPNet xFirewall работает в режиме кластера. Если ViPNet xFirewall настроен на работу в одиночном режиме, при выполнении команды появится сообщение об ошибке.
- Для завершения просмотра журнала используется клавиша **Q**.

Пример использования

```
hostname> failover view 09.03.2017.08.00.00 23.03.2017.19.00.00
  Veiw journal of failover switching
  Versions: ViPNet 4.0.6 (475), daemon 1.3 (14)
  Workstation configured for ID 1031F (Cluster for xF1)
  Workstation works in a mode of hot reservation
  Workstation time (utc: 1174916969) Mon Mar 29 17:49:29 2017

  09 Mar 2017 12:51:42     <P_START> Start failover daemon in passive mode
  22 Mar 2017 12:27:27     <A_START> Start failover daemon in active mode
  22 Mar 2017 14:10:35     <A_START> Start failover daemon in active mode
  22 Mar 2017 15:30:46     <BOOT> Boot the system
  23 Mar 2017 11:09:07     <SWITCH> Switch server from passive mode to active mode

hostname>
```

Команды группы firewall

Команды группы `firewall` предназначены для работы с сетевыми фильтрами (см. глоссарий, стр. 300), правилами трансляции адресов (см. глоссарий, стр. 301) и группами объектов.

firewall add

Команда используется для создания сетевого фильтра или правила трансляции адресов.

Синтаксис

```
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>
```

Параметры и ключевые слова

- `<тип>` — тип создаваемого сетевого фильтра или указание на создание правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `vpn` — фильтр защиты канала управления;
  - `nat` — правило трансляции адресов.
- `<номер>` — порядковый номер фильтра (правила трансляции) в таблице, определяющий его приоритет.
- `<имя>` — имя фильтра (правила трансляции).
- `<адрес отправителя>` — адрес отправителя IP-пакетов.
- `<адрес получателя>` — адрес получателя IP-пакетов.
- `<транспортный протокол>` — транспортный протокол, по которому передаются IP-пакеты.
- `<приложение>` — приложение (для транзитных фильтров открытой сети).
- `<прикладной протокол>` — прикладной протокол (для транзитных фильтров открытой сети).
- `<группа приложений>` — группа приложений (для транзитных фильтров открытой сети).
- `<пользователь>` — пользователь Active Directory или LDAP-сервера (для транзитных фильтров открытой сети).
- `<расписание>` — расписание применения фильтра (правила трансляции).
- `<действие>` — действие с IP-пакетами, соответствующими условиям фильтра (правила трансляции).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если номер не указан, фильтр (правило трансляции) добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика (см. глоссарий, стр. 294) в последнюю очередь.
- Если указанный номер меньше последнего номера в таблице, нумерация фильтров (правил трансляции), следующих за новым фильтром (правилом трансляции), будет автоматически изменена (их номера будут увеличены на 1).
- В качестве адреса отправителя или получателя можно указать следующее:
  - для локальных фильтров открытой сети — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, системную группу объектов `any`, `local` или `remote`, одну или несколько пользовательских групп IP-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, системные группы объектов `any`, `allcoordinators`, `allclients`, `local` или `remote` либо пользовательские группы узлов ViPNet, идентификатор сети ViPNet.
  - для правил трансляции адресов — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, одну или несколько пользовательских групп IP-адресов.
- В качестве адреса отправителя для локальных и транзитных фильтров открытой сети также можно указать сетевой интерфейс собственного узла в виде:

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

- В качестве адреса отправителя для локальных и транзитных фильтров открытой сети также одновременно можно указать и системную группу объектов (`local`, `remote`, `multicast`, `broadcast` кроме `any`), и сетевой интерфейс собственного узла:

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

- В качестве адреса получателя для локальных фильтров открытой сети также можно указать системную группу `broadcast` или `multicast`.
- При задании доменного имени в качестве адреса получателя нельзя использовать кириллицу.
- Транспортный протокол можно указать, используя следующее:

- имена протоколов, написанные строчными буквами и разделенные пробелами. При этом можно также задать дополнительные параметры 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`,
  - ICMP: `type` (тип пакета) и/или `code` (код пакета). При использовании обоих этих параметров сначала необходимо указать параметр `type`, затем — параметр `code`;
- номера протоколов. При этом перед номером каждого протокола необходимо указать ключевое слово `proto`;
- пользовательские группы протоколов в виде: `service @<имя группы>`.

При создании правила трансляции с использованием порта назначения указание адреса назначения и транспортного протокола TCP или UDP обязательно.

- Прикладной протокол необходимо указывать по его названию (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», приложение «Поддерживаемые прикладные протоколы»). Вы можете указать несколько протоколов в списке через запятую. При задании протокола, содержащего пробелы, его название необходимо заключить в двойные кавычки:

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

  Если вы задали приложение в фильтре, то вы можете задать только те прикладные протоколы, которые относятся к этому приложению.

- Приложение необходимо указывать по его названию (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», приложение «Поддерживаемые приложения»). 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
  ```

- Группу приложений необходимо указывать по ее названию (см. документ «ViPNet xFirewall. Настройка с помощью командного интерпретатора», приложение «Поддерживаемые группы приложений»). Вы можете указать несколько групп приложений в списке через запятую. При задании группы приложений, содержащей пробелы, ее название необходимо заключить в двойные кавычки:

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

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

- Пользователя необходимо указывать, используя его доменное имя (без указания имени самого домена) или имя, зарегистрированное на Captive portal. Вы можете указать несколько пользователей в списке через запятую:

  ```
  dnuser ivanov_v,petrov_a
  ```

- Расписание можно задать, используя одну 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.

Также для задания расписания можно использовать соответствующие пользовательские группы объектов.

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 задается одной из следующих лексем:
  - для сетевых фильтров:
    - `pass` — пропускать IP-пакеты;
    - `drop` — блокировать IP-пакеты;
  - для правил трансляции адресов:
    - `change src {<адрес отправителя> | auto}` — заменять адрес отправителя пакетов на указанный внешний адрес ViPNet xFirewall или автоматически на публичный адрес внешнего сетевого интерфейса ViPNet xFirewall;
    - `change dst <адрес получателя>:[<порт>]` — перенаправлять пакеты на указанные адрес и порт. Если вы используете параметр `<порт>`, указание транспортного протокола TCP или UDP обязательно.

Подробнее см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», в главах «Настройка сетевых фильтров» и «Настройка правил трансляции IP-адресов».

Пример использования

- 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 при отправке пакета внешним узлом с адресом mydomain.ru узлу с адресом 192.168.20.1 по протоколу TCP/IP через порт 8080 ViPNet xFirewall подменял адрес получателя (публичный

IP-адрес ViPNet xFirewall) 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 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 ViPNet xFirewall, 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 создать транзитный фильтр, 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 с номером 333, запрещающий MPEG и SSL трафик с ресурсов Youtube и Vimeo для пользователей `PetrovPP` и `SidorovKP`, выполните команду:

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

firewall add name

Команда используется для создания группы объектов заданного типа.

Синтаксис

```
firewall <тип> add name @<имя> <состав> [exclude <исключения>]
```

Параметры и ключевые слова

- `<тип>` — тип объектов. Можно указать одно из следующих значений:
  - `ip-object` — IP-адреса;
  - `vpn-object` — сетевые узлы ViPNet;
  - `interface-object` — сетевые интерфейсы (см. глоссарий, стр. 300);
  - `service-object` — протоколы;
  - `schedule-object` — расписания.
- `<имя>` — имя группы объектов.
- `<состав>` — объекты, входящие в группу.

- `<исключения>` — объекты, не входящие в группу.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Имя группы должно быть уникальным в рамках групп объектов одного типа.
- Перед именем группы необходимо указывать символ `@`.
- Сетевые интерфейсы разделяются пробелом, и перед именем каждого сетевого интерфейса необходимо указать слово `interface`;
- Синтаксис протокола и расписания — тот же, что при создании сетевого фильтра или правила трансляции адресов с помощью команды firewall add (на стр. 42).

Примеры использования

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
```

firewall change append

Команда используется для добавления адреса отправителя, адреса получателя, протокола или расписания в сетевой фильтр или правило трансляции адресов. Для транзитных фильтров открытой сети также можно добавить:

- приложение;
- прикладной протокол;
- группу приложений;

- пользователя Active Directory или LDAP-сервера.

Синтаксис

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

Параметры и ключевые слова

- `<тип>` — тип изменяемого сетевого фильтра или указание на изменение правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `vpn` — фильтр защиты канала управления;
  - `nat` — правило трансляции адресов.
- `<номер>` — порядковый номер фильтра (правила трансляции) в таблице.
- `<имя>` — имя фильтра.
- `<адрес отправителя>` — добавляемый адрес отправителя IP-пакетов.
- `<адрес отправителя>` — добавляемый адрес получателя IP-пакетов.
- `<транспортный протокол>` — добавляемый протокол, по которому передаются IP-пакеты.
- `<приложение>` — приложение (для транзитных фильтров открытой сети).
- `<прикладной протокол>` — прикладной протокол (для транзитных фильтров открытой сети).
- `<группа приложений>` — группа приложений (для транзитных фильтров открытой сети).
- `<пользователь>` — пользователь Active Directory или LDAP-сервера (для транзитных фильтров открытой сети).
- `<расписание>` — добавляемое расписание применения фильтра (правила трансляции).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, транспортного протокола, приложения, прикладного протокола, группы приложений, пользователя и расписания — тот же, что при создании сетевого фильтра (правила трансляции) с помощью команды firewall add (на стр. 42).
- Можно указать несколько параметров.

- Для транзитных фильтров открытой сети возможно задание несколько значений параметров `<приложение>`, `<прикладной протокол>`, `<группа приложений>` и `<пользователь>`. Значения в списке разделяются запятой. Значение, содержащее пробелы, заключается в двойные кавычки.

Пример использования

Пусть существует локальный фильтр открытой сети, созданный с помощью следующей команды:

```
hostname# firewall local add 8 rule "Rule8" src 192.168.1.0/24 dst 10.0.0.1 drop
```

Чтобы добавить в этот фильтр еще один адрес отправителя и расписание, по которому фильтр будет применяться только в выходные дни с 9 до 23 часов, выполните команду:

```
hostname# firewall local change append 8 src 192.168.2.2 weekly sa su at 09:00-23:00
```

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

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

Чтобы к транзитному правилу открытой сети с номером 333 добавить запрет игрового трафика (группа приложений Gaming) для пользователей MakarovTP и DeryuginAA, выполните команду:

```
hostname# firewall forward change append 333 dpigroup Gaming dnuser
MakarovTP,DeryuginAA
```

firewall delete

Команда используется для удаления сетевого фильтра или правила трансляции адресов.

Синтаксис

```
firewall <тип> delete <параметры>
```

Параметры и ключевые слова

- `<тип>` — тип удаляемого сетевого фильтра или указание на удаление правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `vpn` — фильтр защиты канала управления;
  - `nat` — правило трансляции адресов.
- `<параметры>` — параметры фильтра (правила трансляции) для удаления. Можно указать следующие параметры: порядковый номер, имя, адрес отправителя, адрес получателя, протокол, действие фильтра или правила.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании фильтра (правила трансляции) с помощью команды `firewall add` (на стр. 42).
- Можно указать несколько параметров.
- Поиск фильтров (правил трансляции) для удаления осуществляется по строгому совпадению с заданными параметрами.
- Нумерация фильтров (правил трансляции), следующих за удаленным фильтром (правилом трансляции), изменяется автоматически (их номера уменьшаются на 1).

Пример использования

Для удаления локального фильтра открытой сети с номером 7 выполните команду:

```
hostname# firewall local delete 7
+====+=======================+============+==========+
|Num |Name                   |Option      |Schedule  |
+----+---------+-------------+------------+----------+
|Act |Source   |Destination  |Protocol               |
+====+=========+=============+============+==========+
|7   |Allow syslog outgoing  |User        |          |
+----+---------+-------------+------------+----------+
|pass|@local   |@any         |udp: to 514            |
+====+=======================+============+==========+
Do you want to perform the action on the above rule? [y/n]: y
hostname#
```

firewall move rule

Команда используется для изменения порядкового номера (приоритета) сетевого фильтра или правила трансляции адресов в таблице.

Синтаксис

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

Параметры и ключевые слова

- `<тип>` — тип изменяемого сетевого фильтра или указание на изменение правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `vpn` — фильтр защиты канала управления;
  - `nat` — правило трансляции адресов.
- `<текущий номер>` — текущий порядковый номер фильтра (правила трансляции).
- `<новый номер>` — новый порядковый номер фильтра (правила трансляции).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При изменении порядкового номера соответственно изменяется приоритет фильтра (правила трансляции) при обработке трафика.
- Нумерация фильтров (правил трансляции), следующих за перемещенным фильтром (правилом трансляции), изменяется автоматически (их номера увеличиваются на 1).
- Невозможно изменить порядковый номер, если новый номер больше последнего номера в таблице.

Пример использования

Чтобы переместить локальный фильтр с девятого на восьмое место в таблице (то есть сделать его более приоритетным), выполните команду:

```
hostname# firewall local move rule 9 to 8
```

firewall object delete

Команда используется для удаления группы объектов с заданным именем.

Синтаксис

```
firewall object delete @<имя>
```

Параметры и ключевые слова

`<имя>` — имя группы объектов.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если группа используется в каких-либо сетевых фильтрах, правилах трансляции адресов или других группах объектов, то в результате выполнения данной команды появится сообщение об ошибке, содержащее список всех фильтров, правил или групп, которые используют данную группу. В этом случае необходимо сначала удалить эти фильтры, правила и группы, а затем выполнить команду для удаления группы еще раз.

Пример использования

Чтобы удалить группу объектов с именем `IP_group`, выполните команду:

```
hostname# firewall object delete @IP_group
```

firewall object show

Команда предназначена для просмотра всех групп объектов.

Синтаксис

```
firewall object show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Для завершения просмотра используется клавиша **Q**.

Пример использования

```
hostname> firewall object show
Ip Objects
================================================================================
Num Name                                            Creation type
Inclusion                           Exclusion
================================================================================
1   PrivateNetworkIP                                User
10.0.0.0/255.0.0.0, 172.16.0.0/
255.240.0.0, 192.168.0.0/255.255.0.0
--------------------------------------------------------------------------------
hostname>
```

Группы каждого типа объектов выводятся в отдельной таблице, содержащей следующие столбцы:

- `Num` — порядковый номер группы.
- `Name` — имя группы.
- `Creation Type` — вид группы: для групп из программы ViPNet Policy Manager — `Policy`, для пользовательских групп — `User`.
- `Inclusion` — объекты, входящие в группу.
- `Exclusion` — объекты, не входящие в группу.

firewall rules show

Команда предназначена для просмотра всех сетевых фильтров и правил трансляции адресов, заданных в ViPNet xFirewall.

Синтаксис

```
firewall rules show [rule <имя>]
```

Параметры и ключевые слова

`<имя>` — имя сетевого фильтра или правила трансляции адресов.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Для завершения просмотра используется клавиша **Q**.

Каждый тип сетевых фильтров и правила трансляции адресов выводятся в отдельной таблице, содержащей следующие столбцы:

- `Num` — порядковый номер фильтра (правила трансляции) в таблице.
- `Name` — имя фильтра (правила трансляции).
- `Option` — категория фильтра (правила трансляции).
- `Schedule` — расписание применения фильтра (правила трансляции).
- `Act` — действие фильтра (правила трансляции).
- `Source` — адрес отправителя IP-пакетов.
- `Destination` — адрес получателя IP-пакетов.
- `Protocol` — протокол, по которому передаются IP-пакеты.

Пример использования

```
hostname> firewall rules show
 Local Rules:
================================================================================
Num   Name                                        Option  Schedule
Act   Protocol              Source               ->Destination
      DpiProtocol           [G]DpiGroup, DpiApp    DomainUser
================================================================================
1     Allow DHCP Service                          User
pass  udp: from 67 to 68    @any                 ->@any
      @any                  @any                   @any
--------------------------------------------------------------------------------
empty rule for Forward Rules:
empty rule for Nat Rules:
hostname>
```

В результате выполнения команды будут показаны все сетевые фильтры и правила трансляции адресов, заданные на сетевом узле.

```
hostname> firewall rules show rule "Allow ICMP Ping"

 Service Vpn Rules:

================================================================================

Num   Name                                          Option  Schedule

Act   Protocol              Source                ->Destination
```

```
      DpiProtocol            [G]DpiGroup, DpiApp       DomainUser
================================================================================
10    Allow ICMP Ping                                    User
pass  icmp: 8                @any                    ->@any
                                                        @any
      @any                   @any
--------------------------------------------------------------------------------
empty rule for  Vpn Rules:
empty rule for  Nat Rules:
empty rule for  Service Local Rules:
 Local Rules:
================================================================================
Num   Name                                            Option  Schedule
Act   Protocol               Source                  ->Destination
      DpiProtocol            [G]DpiGroup, DpiApp       DomainUser
================================================================================
4     Allow ICMP Ping                                  User
pass  icmp: 8                @local                  ->@any
                                                        @any
      @any                   @any
--------------------------------------------------------------------------------
empty rule for  Forward Rules:
```

В результате выполнения команды будут показаны все сетевые фильтры и правила трансляции адресов с именем Allow ICMP Ping, заданные на сетевом узле.

firewall show

Команда предназначена для просмотра конкретных групп объектов, сетевых фильтров заданного типа, а также правил трансляции адресов.

Синтаксис

```
firewall <тип> show [<параметры>]
```

Параметры и ключевые слова

- `<тип>` — тип групп объектов или сетевых фильтров, правила трансляции адресов:

- `ip-object` — группы IP-адресов;
- `vpn-object` — группы узлов ViPNet;
- `interface-object` — группы интерфейсов;
- `service-object` — группы протоколов;
- `schedule-object` — группы расписаний;
- `local` — локальный фильтр открытой сети;
- `forward` — транзитный фильтр открытой сети;
- `vpn` — фильтр защиты канала управления;
- `nat` — правило трансляции адресов.

- `<параметр>` — параметры фильтров (правил трансляции), отбираемых для просмотра. Можно указать следующие параметры:
  - порядковый номер фильтра или правила трансляции;
  - имя фильтра или правила трансляции;
  - адрес отправителя;
  - адрес получателя;
  - транспортный протокол;
  - прикладной протокол (для транзитных фильтров открытой сети);
  - приложение (для транзитных фильтров открытой сети);
  - группа приложений (для транзитных фильтров открытой сети);
  - пользователь Active Directory или LDAP-сервера (для транзитных фильтров открытой сети);
  - действие фильтра или правила.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Указать параметры для групп объектов нельзя.
- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании фильтра (правила трансляции) с помощью команды firewall add (на стр. 42).
- Можно указать несколько параметров.

- При просмотре транзитных фильтров открытой сети возможно использование несколько значений параметров <прикладной протокол>, <приложение>, <группа приложений> и<пользователь>. Значения в списке разделяются запятой. Значение, содержащее пробелы, заключается в двойные кавычки.
- Поиск фильтров (правил трансляции) осуществляется по строгому совпадению с указанными параметрами.
- В результате выполнения команды отображается таблица, содержащая соответствующие типы групп объектов, сетевых фильтров или правил трансляции адресов.

Пример использования

Для просмотра локальных фильтров для протокола UDP выполните команду:

```
hostname> firewall local show udp
User:
=============================================================================
Num   Name                                        Option  Schedule
Act   Protocol               Source               ->Destination
      DpiProtocol            [G]DpiGroup, DpiApp    DomainUser
=============================================================================
1     Allow DHCP Service                           User
pass  udp: from 67 to 68     @any                 ->@any
      @any                   @any                   @any
-----------------------------------------------------------------------------
hostname>
```

Команды группы inet

Команды группы `inet` предназначены для настройки и управления сетевыми интерфейсами и сервисами ViPNet xFirewall (DHCP-сервером, DNS-сервером и другими).

inet bonding add mode slaves

Команда используется для добавления агрегированного интерфейса, задания подчиненных ему физических интерфейсов, а также для задания режима его работы.

Синтаксис

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

Параметры и ключевые слова

- `<номер>` — номер добавляемого агрегированного интерфейса.
- `<режим>` — режим работы агрегированного интерфейса. Можно указать один из следующих режимов:
  - `balance-rr` — режим, при котором исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.
  - `balance-xor` — режим, при котором подчиненный физический интерфейс, через который отправляется тот или иной пакет, выбирается на основе значения хэш-функции, вычисляемой по алгоритму, задаваемому с помощью команды inet ifconfig bonding xmit-hash-policy (на стр. 91). В результате пакеты от одного и того же отправителя к одному и тому же получателю всегда будут отправляться через один и тот же подчиненный интерфейс.
  - `balance-tlb` — режим, при котором ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных физических интерфейсов, и на основе этого выполняется балансировка исходящего трафика между подчиненными интерфейсами.
  - `802.3ad` — режим динамического агрегирования с использованием протокола LACP. В этом режиме агрегированный интерфейс работает следующим образом:
    - среди подчиненных физических интерфейсов формируются группы — «агрегаторы», скорость передачи данных на интерфейсах которых одинакова;
    - один из агрегаторов выбирается активным в соответствии с алгоритмом, задаваемым с помощью команды inet ifconfig bonding ad-select (на стр. 87);

- внутри агрегатора подчиненный физический интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму `balance-xor`;
- в случае сбоя на физическом интерфейсе, входящем в агрегатор, или при добавлении нового подчиненного физического интерфейса, в качестве активного выбирается другой агрегатор (также в соответствии с алгоритмом, задаваемым с помощью команды inet ifconfig bonding ad-select (на стр. 87));
- с другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью команды inet ifconfig bonding lacp-rate (на стр. 88), что позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую (например, через медиаконвертер).

o `active-backup` — режим, при котором один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью команды inet ifconfig bonding primary (на стр. 90)) и все исходящие пакеты отправляются через него. При этом в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.

o `broadcast` — режим, при котором пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно.

- `<интерфейс 1>`, `<интерфейс 2>`, `<интерфейс 3>` — физические интерфейсы, подчиненные создаваемому агрегированному интерфейсу.

Значения по умолчанию

- По умолчанию агрегированные интерфейсы не заданы.
- По умолчанию используется режим работы агрегированного интерфейса `balance-rr`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- В качестве номера агрегированного интерфейса можно задавать номера 0, 1 или 2. Таким образом, вы можете задать до трех агрегированных интерфейсов.
- В результате выполнения команды создается агрегированный интерфейс с именем `bond<номер>`.
- Задаваемые подчиненные физические интерфейсы должны относиться к классу `slave` (см. inet ifconfig class на стр. 92).
- При добавлении агрегированного интерфейса необходимо задать хотя бы один подчиненный ему физический интерфейс. В дальнейшем вы можете задавать подчиненные физические интерфейсы с помощью команды inet ifconfig bonding add (на стр. 86).

- При добавлении агрегированного интерфейса, а также впоследствии с помощью команды inet ifconfig bonding add (на стр. 86), можно задать до трех подчиненных ему физических интерфейсов.
- Режим `broadcast` требует специальной настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов данных.
- Для работы агрегированного интерфейса в режиме `balance-tlb` необходимо, чтобы все подчиненные физические интерфейсы были подключены к сети через коммутатор.
- Максимальное количество интерфейсов в ViPNet xFirewall (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Пример использования

Чтобы добавить агрегированный интерфейс `bond1`, работающий в режиме `balance-rr`, с подчиненными физическими интерфейсами eth0 и eth1, последовательно выполните следующие команды:

```
hostname# inet ifconfig eth0 class slave

eth0 set to slave class.

hostname# inet ifconfig eth1 class slave

eth1 set to slave class.

hostname# inet bonding add 1 mode balance-rr slaves eth0 eth1

hostname#
```

inet bonding delete

Команда используется для удаления агрегированного интерфейса.

Синтаксис

```
inet bonding delete <номер>
```

Параметры и ключевые слова

`<номер>` — номер удаляемого агрегированного интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Имена агрегированных интерфейсов имеют вид `bond<номер>`.
- Если вы хотите удалить агрегированный интерфейс класса `trunk` (см. inet ifconfig class на стр. 92), предварительно удалите все соответствующие ему виртуальные интерфейсы с помощью команды inet ifconfig vlan delete (на стр. 102).

Пример использования

```
hostname# inet bonding delete 1

hostname#
```

inet clear mac-address-table

Команда используется для очистки ARP-таблицы (таблицы преобразования IP-адресов в MAC-адреса).

Синтаксис

```
inet clear mac-address-table
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet clear mac-address-table
This command clears MAC address table.
Do you really wish to execute this command? [Yes,No]: Yes
hostname#
```

inet dhcp client route-default-metric

Команда используется для изменения значения метрики по умолчанию (см. глоссарий, стр. 299) для маршрутов, поступающих от DHCP-сервера. Эта метрика будет присваиваться маршрутам DHCP-сервера, если для сетевого интерфейса, на который они поступили, не задана специфичная метрика.

Синтаксис

```
inet dhcp client route-default-metric <1-255>
```

Параметры и ключевые слова

`<1—255>` — новое значение метрики по умолчанию.

Значения по умолчанию

`70`

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet dhcp client route-default-metric 60
hostname#
```

inet dhcp client route-distance

Команда используется для задания административной дистанции (см. глоссарий, стр. 296) маршрутам, поступающим от DHCP-сервера (с использованием DHCP-протокола).

Синтаксис

```
inet dhcp client route-distance <1-255> [default-route <1-255>]
```

Параметры и ключевые слова

`<1—255>` — значение общей административной дистанции для всех маршрутов DHCP-сервера.

`default-route <1-255>` — значение административной дистанции для маршрутов по умолчанию (см. глоссарий, стр. 298).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Значение административной дистанции для маршрутов по умолчанию можно задать только вместе с административной дистанцией для всего протокола DHCP.

Пример использования

```
hostname# inet dhcp client route-distance 80 default-route 60
Set distance to 80, default distance to 60
hostname#
```

inet dhcp server add wins

Команда используется для добавления адреса WINS-сервера (см. глоссарий, стр. 295) в список адресов, передаваемых DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server add wins <IP-адрес>
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес WINS-сервера.

Значения по умолчанию

По умолчанию список адресов WINS-серверов содержит адрес 172.16.1.1.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды необходимо завершить работу DHCP-сервера (см. inet dhcp server stop на стр. 69).

Пример использования

Чтобы в список передаваемых адресов WINS-серверов добавить адрес 192.168.10.1, выполните команду:

```
hostname# inet dhcp server add wins 192.168.10.1
```

inet dhcp server delete wins

Команда используется для удаления адреса WINS-сервера из списка адресов, передаваемых DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server delete wins <IP-адрес>
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес WINS-сервера.

Значения по умолчанию

По умолчанию список адресов WINS-серверов содержит адрес 172.16.1.1.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды необходимо завершить работу DHCP-сервера (см. inet dhcp server stop на стр. 69).

Пример использования

Чтобы из списка передаваемых адресов WINS-серверов удалить адрес 172.16.1.1, выполните команду:

```
hostname# inet dhcp server delete wins 172.16.1.1
```

inet dhcp server interface

Команда используется для задания рабочего интерфейса DHCP-сервера (см. глоссарий, стр. 293).

Синтаксис

```
inet dhcp server interface <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Значения по умолчанию

По умолчанию в качестве рабочего интерфейса используется eth0.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу DHCP-сервера (см. inet dhcp server stop на стр. 69).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- В качестве рабочего можно указать Ethernet-, VLAN-интерфейс или агрегированный интерфейс.
- Рабочий интерфейс DHCP-сервера должен иметь статический адрес.
- Адрес рабочего интерфейса DHCP-сервера не должен принадлежать диапазону выделяемых адресов, заданному командой `inet dhcp range` (см. inet dhcp server range на стр. 67).

Пример использования

Чтобы задать интерфейс eth1 в качестве рабочего для DHCP-сервера, выполните команду:

```
hostname# inet dhcp server interface eth1
```

inet dhcp server lease

Команда используется для задания времени аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server lease <время>
```

Параметры и ключевые слова

`<время>` — время аренды в секундах.

Значения по умолчанию

По умолчанию время аренды 864000 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды необходимо завершить работу DHCP-сервера (см. inet dhcp server stop на стр. 69).

Пример использования

Чтобы установить время аренды 5 дней, выполните команду:

```
hostname# inet dhcp server lease 432000
```

inet dhcp server mode

Команда используется для включения или выключения автоматического запуска DHCP-сервера при загрузке ViPNet xFirewall.

Синтаксис

```
inet dhcp server mode {on | off}
```

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

По умолчанию автоматический запуск DHCP-сервера выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска DHCP-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск в следующих случаях:
  - Включен автоматический запуск службы DHCP-relay.
  - Текущие настройки DHCP-сервера некорректны.

Пример использования

Чтобы включить автоматический запуск DHCP-сервера, выполните команду:

```
hostname# inet dhcp server mode on
DHCP server enabled and will be started on next reboot.
You need to start the NTP server manually or reboot to start it.
hostname#
```

inet dhcp server range

Команда используется для задания диапазона IP-адресов, выделяемых DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server range <начало диапазона> <конец диапазона>
```

Параметры и ключевые слова

- `<начало диапазона>` — начальный IP-адрес диапазона.
- `<конец диапазона>` — конечный IP-адрес диапазона.

Значения по умолчанию

- `<начало диапазона>` — 172.16.1.2.
- `<конец диапазона>` — 172.16.1.254.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу DHCP-сервера (см. inet dhcp server stop на стр. 69).
- Конечный адрес диапазона должен быть не меньше начального.
- В локальной сети, маршрутизируемой в сеть Интернет, рекомендуется, чтобы диапазон выделяемых адресов был из числа допустимых для частных сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

Пример использования

Чтобы DHCP-сервер выделял своим клиентам адреса из диапазона 192.168.10.2–192.168.10.254, выполните команду:

```
hostname# inet dhcp server range 192.168.10.2 192.168.10.254
```

inet dhcp server router

Команда используется для задания адреса шлюза по умолчанию, передаваемого DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server router <адрес>
```

Параметры и ключевые слова

`<адрес>` — IP-адрес шлюза по умолчанию.

Значения по умолчанию

`<адрес>` — 172.16.1.1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу DHCP-сервера (см. inet dhcp server stop на стр. 69).
- IP-адрес шлюза должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам.

Пример использования

Чтобы DHCP-сервер передавал своим клиентам адрес шлюза по умолчанию 192.168.10.1, выполните команду:

```
hostname# inet dhcp server router 192.168.10.1
```

inet dhcp server start

Команда используется для запуска DHCP-сервера.

Синтаксис

```
inet dhcp server start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Невозможно запустить DHCP-сервер в следующих случаях:

- Запущена служба DHCP-relay.
- Текущие настройки DHCP-сервера некорректны.

Пример использования

```
hostname# inet dhcp server start
hostname#
```

inet dhcp server stop

Команда используется для завершения работы DHCP-сервера.

Синтаксис

```
inet dhcp server stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet dhcp server stop
stopped /usr/sbin/udhcpd (pid 5831)
hostname#
```

inet dhcp relay add listen-interface

Команда используется для добавления интерфейса в список интерфейсов, принимающих запросы от DHCP-клиентов для их последующей ретрансляции на внешний DHCP-сервер.

Синтаксис

```
inet dhcp relay add listen-interface <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу службы DHCP-relay (см. inet dhcp relay stop на стр. 75).
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из списка интерфейсов, которые имеются в системе, но отсутствуют в списке принимающих DHCP-запросы.
- Добавляемый интерфейс должен иметь статический адрес.

Пример использования

Чтобы добавить интерфейс eth0 в список интерфейсов, принимающих запросы от DHCP-клиентов, выполните команду:

```
hostname# inet dhcp relay add listen-interface eth0
```

inet dhcp relay delete listen-interface

Команда используется для удаления интерфейса из списка интерфейсов, принимающих запросы от DHCP-клиентов.

Синтаксис

```
inet dhcp relay delete listen-interface <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу службы DHCP-relay (см. inet dhcp relay stop на стр. 75).
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из текущего списка интерфейсов, принимающих DHCP-запросы.

Пример использования

Чтобы удалить интерфейс `eth0` из списка интерфейсов, принимающих запросы от DHCP-клиентов, выполните команду:

```
hostname# inet dhcp relay delete listen-interface eth0
```

inet dhcp relay external-interface

Команда используется для установки параметров связи службы DHCP-relay с внешним DHCP-сервером.

Синтаксис

```
inet dhcp relay external-interface <интерфейс> server {<адрес> | <DNS-имя>}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса, со стороны которого находится внешний DHCP-сервер.
- `<адрес>` — IP-адрес внешнего DHCP-сервера.
- `<DNS-имя>` — DNS-имя внешнего DHCP-сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу службы DHCP-relay (см. inet dhcp relay stop на стр. 75).
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из списка интерфейсов, которые имеются в системе, но отсутствуют в списке принимающих DHCP-запросы.
- Указанный в команде интерфейс должен иметь статический адрес.

Пример использования

Чтобы использовать интерфейс `eth1` для связи с внешним DHCP-сервером, имеющим адрес 172.16.1.1, выполните команду:

```
hostname# inet dhcp relay external-interface eth1 server 172.16.1.1
```

inet dhcp relay mode

Команда используется для включения или выключения автоматического запуска службы DHCP-relay при загрузке ViPNet xFirewall.

Синтаксис

```
inet dhcp relay mode {on | off}
```

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

По умолчанию автоматический запуск службы DHCP-relay выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска службы DHCP-relay, ее текущее состояние не изменяется.
- Невозможно включить автоматический запуск в следующих случаях:
  - Включен автоматический запуск DHCP-сервера.
  - Не заданы какие-либо настройки службы DHCP-relay.

Пример использования

Чтобы включить автоматический запуск службы DHCP-relay, выполните команду:

```
hostname# inet dhcp relay mode on
```

inet dhcp relay reset

Команда завершает работу службы DHCP-relay, сбрасывает все ее настройки и выключает автоматический запуск службы при загрузке ViPNet xFirewall.

Синтаксис

```
inet dhcp relay reset
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда используется в случае, если требуется сбросить настройки службы DHCP-relay для последующего задания новых параметров.

Пример использования

```
hostname# inet dhcp relay reset
The factory default settings of DHCP-relay will be restored. Continue? [Yes,No]: Yes
DHCP relay settings successfully restored to factory defaults.
hostname#
```

inet dhcp relay start

Команда используется для запуска службы DHCP-relay.

Синтаксис

```
inet dhcp relay start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Невозможно запустить службу DHCP-relay в следующих случаях:

- Запущен DHCP-сервер.
- Не заданы какие-либо настройки службы DHCP-relay.

Пример использования

```
hostname# inet dhcp relay start
```

inet dhcp relay stop

Команда используется для завершения работы службы DHCP-relay.

Синтаксис

```
inet dhcp relay stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet dhcp relay stop
```

inet dns clients add

Команда используется для добавления заданного адреса или подсети в список клиентов DNS-сервера (см. глоссарий, стр. 293), развернутого на ViPNet xFirewall.

Синтаксис

```
inet dns clients add {<адрес>[/<длина маски>] | any}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес отдельного узла или подсети.
- `<длина маски>` — длина маски подсети.
- `any` — любые узлы.

Значения по умолчанию

По умолчанию список клиентов DNS-сервера содержит ключевое слово `any`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы в список клиентов DNS-сервера добавить узлы из подсети 192.168.10.0/16, выполните команду:

```
hostname# inet dns clients add 192.168.10.0/16
```

inet dns clients delete

Команда используется для удаления заданного адреса или подсети из списка клиентов DNS-сервера (см. глоссарий, стр. 293), развернутого на ViPNet xFirewall.

Синтаксис

```
inet dns clients delete {<адрес>[/<длина маски>] | any}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес отдельного узла или подсети.
- `<длина маски>` — длина маски подсети.
- `any` — любые узлы.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

При вводе адреса работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка клиентов DNS-сервера.

Пример использования

Чтобы из списка клиентов DNS-сервера удалить ключевое слово `any`, по умолчанию присутствующее в списке, выполните команду:

```
hostname# inet dns clients delete any
```

inet dns clients list

Команда предназначена для просмотра текущего списка DNS-клиентов, которым разрешена передача запросов DNS-серверу.

Синтаксис

```
inet dns clients list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

В примере ниже список содержит только ключевое слово `any` (любые узлы), по умолчанию присутствующее в списке:

```
hostname> inet dns clients list
Allow DNS requests from the following client(s):
any
hostname>
```

inet dns forwarders add

Команда используется для добавления сервера с заданным адресом в список DNS-серверов (forwarder), которые передают запросы DNS-серверу внешней сети. Дополнительно можно указать имя зоны, для которой осуществляется перенаправление запросов.

Синтаксис

```
inet dns forwarders add <адрес> [for-zone <имя зоны>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес DNS-сервера.
- `<имя зоны>` — имя зоны (окончание доменного имени сетевых узлов, запросы от которых перенаправляются на DNS-сервер).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если зона не указана, то DNS-серверу перенаправляются все запросы.
- Если IP-адрес DNS-сервера задается без зоны, то независимо от его предыдущего состояния (с зоной или без зоны), все запросы перенаправляются на DNS-сервер без зоны. При этом выводится сообщение:

  ```
  Forward DNS address <адрес> resolves both named zone and all requests
  ```

- Если IP-адрес DNS-сервера задается с зоной, то независимо от его предыдущего состояния (с зоной или без зоны), все запросы перенаправляются на DNS-сервер с зоной. При этом выводится сообщение:

  ```
  Forward DNS address <адрес> resolves both named zone and all requests
  ```

Примеры использования

Чтобы в список DNS-серверов пересылки добавить сервер с адресом 10.0.2.3, выполните команду:

```
hostname# inet dns forwarders add 10.0.2.3
```

Чтобы в список DNS-серверов пересылки добавить сервер с адресом 10.0.2.4, который перенаправляет запросы от сетевых узлов зоны gov.ru, выполните команду:

```
hostname# inet dns forwarders add 10.0.2.4 for-zone gov.ru
```

inet dns forwarders delete

Команда используется для удаления сервера с заданным адресом из списка DNS-серверов (forwarder), которые передают запросы DNS-серверу внешней сети.

Синтаксис

```
inet dns forwarders delete <адрес> [for-zone <имя зоны>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес удаляемого DNS-сервера.
- `<имя зоны>` — имя зоны, связанное с удаляемым DNS-сервера (окончание доменного имени сетевых узлов, запросы от которых перенаправляются на DNS-сервер).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе адреса работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка DNS-серверов пересылки.
- Если удаляемый DNS-сервер был ранее связан с зоной, то в команде на удаление DNS-сервера эта зона должна быть указана.

Примеры использования

Чтобы из списка DNS-серверов пересылки удалить сервер с адресом 10.0.2.3, выполните команду:

```
hostname# inet dns forwarders delete 10.0.2.3
```

Чтобы из списка DNS-серверов пересылки удалить сервер с адресом 10.0.2.4 и зоной gov.ru, выполните команду:

```
hostname# inet dns forwarders delete 10.0.2.4 for-zone gov.ru
```

inet dns forwarders list

Команда предназначена для просмотра текущего списка DNS-серверов пересылки (forwarder).

Синтаксис

```
inet dns forwarders list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если адреса DNS-серверов пересылки не заданы (список пустой), то выводится информация о том, что используются корневые DNS-серверы.

Пример использования

```
hostname> inet dns forwarders list
Forward DNS requests to servers:
10.0.2.3

10.0.2.4 from USERS for-zone gov.ru
hostname>
```

inet dns mode

Команда используется для включения или выключения автоматического запуска DNS-сервера при загрузке ViPNet xFirewall.

Синтаксис

```
inet dns mode {on | off}
```

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

Задается при установке справочников и ключей (см. глоссарий, стр. 301).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска DNS-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск, если DNS-сервер не запущен.
- Невозможно выключить автоматический запуск, если DNS-сервер запущен.

Пример использования

Чтобы выключить автоматический запуск DNS-сервера, выполните команду:

```
hostname# inet dns mode off
```

inet dns start

Команда используется для запуска DNS-сервера.

Синтаксис

```
inet dns start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet dns start
Starting domain name service...: bind9.
hostname#
```

inet dns stop

Команда используется для завершения работы DNS-сервера.

Синтаксис

```
inet dns stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet dns stop
Stopping domain name service...: bind9 waiting for pid 2902 to die
hostname#
```

inet ifconfig address

Команда используется для установки параметров заданного интерфейса (см. глоссарий, стр. 300).

Синтаксис

```
inet ifconfig <интерфейс> address <IP-адрес> netmask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<IP-адрес>` — IP-адрес.
- `<маска>` — маска подсети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен относиться к классу `access` (см. inet ifconfig class на стр. 92).
- Если указанный интерфейс является рабочим для DHCP-сервера, то перед изменением его параметров требуется завершить работу DHCP-сервера (см. inet dhcp server stop на стр. 69).
- При изменении адреса интерфейса в таблице маршрутизации (см. глоссарий, стр. 301) автоматически изменяются все маршруты, связанные с этим интерфейсом. Необходимо скорректировать маршрут по умолчанию и статические маршруты так, чтобы они стали удовлетворять новой адресации.
- Если ранее на указанном интерфейсе был установлен режим DHCP, то после установки параметров будет потеряна информация о DNS- и NTP-серверах, полученная от DHCP-сервера.
- Не рекомендуется в качестве маски подсети использовать маски 255.255.255.254 и 255.255.255.255.

Пример использования

Чтобы на интерфейсе `eth1` установить IP-адрес 192.168.10.1 и маску подсети 255.255.255.0, выполните команду:

```
hostname# inet ifconfig eth1 address 192.168.10.1 netmask 255.255.255.0
```

inet ifconfig address add

Команда используется для добавления дополнительного IP-адреса на заданный интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> address add <IP-адрес> netmask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<IP-адрес>` — IP-адрес.
- `<маска>` — маска подсети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен быть включен и относиться к классу `access` (см. inet ifconfig class на стр. 92).
- Нельзя добавить IP-адрес, если на указанном интерфейсе установлен режим DHCP.
- По команде создается виртуальный интерфейс с именем `<интерфейс>:номер`, где `номер` — очередной свободный номер (нумерация дополнительных адресов начинается с 0). На созданном виртуальном интерфейсе задаются указанные IP-адрес и маска.

Пример использования

Чтобы на интерфейсе eth1 установить дополнительный IP-адрес 192.168.10.2 с маской подсети 255.255.255.0, выполните команду:

```
hostname# inet ifconfig eth1 address add 192.168.10.2 netmask 255.255.255.0
Alias eth1:0 has been created.
hostname#
```

В результате появится новый виртуальный интерфейс с именем `eth1:0`, адресом 192.168.10.2 и маской подсети 255.255.255.0.

inet ifconfig address delete

Команда используется для удаления дополнительного IP-адреса с заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> address delete <IP-адрес> netmask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<IP-адрес>` — IP-адрес.
- `<маска>` — маска подсети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен быть включен и относиться к классу `access` (см. inet ifconfig class на стр. 92).
- Нельзя удалить дополнительный IP-адрес, если на указанном интерфейсе установлен режим DHCP.
- Если дополнительный IP-адрес с указанными параметрами существует, то удаляется соответствующий виртуальный интерфейс.

Пример использования

Чтобы с интерфейса `eth1` удалить дополнительный IP-адрес 192.168.10.2 с маской подсети 255.255.255.0, выполните команду:

```
hostname# inet ifconfig eth1 address delete 192.168.10.2 netmask 255.255.255.0
```

inet ifconfig bonding add

Команда используется для добавления подчиненного физического интерфейса к уже имеющемуся агрегированному.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding add <подчиненный интерфейс>
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Задаваемый подчиненный физический интерфейс должен относиться к классу `slave` (см. inet ifconfig class на стр. 92).
- Задаваемый подчиненный физический интерфейс не должен быть привязан ни к одному агрегированному интерфейсу.
- Для каждого агрегированного интерфейса можно добавить не более трех подчиненных физических интерфейсов.
- Максимальное количество интерфейсов в ViPNet xFirewall (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Пример использования

Чтобы для агрегированного интерфейса `bond1` добавить физический интерфейс `eth2`, выполните следующую команду:

```
hostname# inet ifconfig bond1 bonding add eth2

hostname#
```

inet ifconfig bonding ad-select

Команда используется для задания режима выбора активного агрегатора на агрегированном интерфейсе, работающем в режиме 802.3ad.

Синтаксис

```
inet ifconfig <интерфейс> bonding ad-select <режим>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `<режим>` — режим выбора активного агрегатора на агрегированном интерфейсе, работающем в режиме 802.3ad. Можно задать следующие значения этого параметра:
  - `stable` — режим, при котором первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора.
  - `bandwidth` — режим, при котором первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.
  - `count` — режим, при котором первоначально выбирается агрегатор с наибольшим количеством подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.

Значения по умолчанию

По умолчанию используется режим `stable`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы на агрегированном интерфейсе bond1, работающем в режиме 802.3ad, активный агрегатор выбирался в соответствии с режимом `count`, выполните команду:

```
hostname# inet ifconfig bond1 bonding ad-select count
```

inet ifconfig bonding delete

Команда используется для удаления подчиненного интерфейса из агрегированного.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding delete <подчиненный интерфейс>
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если агрегированному интерфейсу подчинен только один физический интерфейс, то его удалить нельзя.

Пример использования

Чтобы удалить подчиненный физический интерфейс eth2 из агрегированного интерфейса bond1, выполните команду:

```
hostname# inet ifconfig bond1 bonding delete eth2
hostname#
```

inet ifconfig bonding lacp-rate

Команда используется для задания частоты обмена пакетами по протоколу LACP для агрегированных интерфейсов, работающих в режиме 802.3ad.

Синтаксис

```
inet ifconfig <интерфейс> bonding lacp-rate <slow | fast>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `slow` — обмен пакетами по протоколу LACP выполняется каждые 30 секунд.
- `fast` — обмен пакетами по протоколу LACP выполняется каждую секунду.

Значения по умолчанию

По умолчанию обмен пакетами по протоколу LACP выполняется каждые 30 секунд (`slow`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме 802.3ad обмен пакетами по протоколу LACP выполнялся каждую секунду, выполните команду:

```
hostname# inet ifconfig bond1 bonding lacp-rate fast
```

inet ifconfig bonding miimon

Команда используется для задания частоты проверки соединения на подчиненных физических интерфейсах.

Синтаксис

```
inet ifconfig <интерфейс> bonding miimon <интервал>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `<интервал>` — время в миллисекундах, через которое производится проверка соединения на подчиненных физических интерфейсах.

Значения по умолчанию

По умолчанию соединение проверяется каждые 100 миллисекунд (0,1 секунды).

Режимы командного интерпретатора

Администратор.

Особенности использования

Для параметра `<интервал>` можно задавать значения от 1 до 1000 миллисекунд.

Пример использования

Чтобы на подчиненных интерфейсах агрегированного интерфейса bond1 соединение проверялось каждые 0,5 секунды, выполните команду:

```
hostname# inet ifconfig bond1 bonding miimon 500
```

inet ifconfig bonding primary

Команда используется для настройки агрегированных интерфейсов, работающих в режиме `balance-tlb` или `active-backup`. Команда используется для принудительного выбора одного из подчиненных физических интерфейсов в качестве основного.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding primary {<подчиненный интерфейс> | none}
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.
- `none` — отмена принудительного выбора основного интерфейса.

Значения по умолчанию

По умолчанию основной интерфейс выбирается в соответствии с выбранным режимом работы агрегированного канала (`none`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы на агрегированном интерфейсе bond1, работающем в режиме `active-backup`, принудительно выбрать в качестве основного интерфейса подчиненный интерфейс eth1, выполните команду:

```
hostname# inet ifconfig bond1 bonding primary eth1
```

inet ifconfig bonding xmit-hash-policy

Команда используется для настройки агрегированных интерфейсов, работающих в режиме `balance-xor` или `802.3ad`. Команда задает алгоритм вычисления хэш-функции, используемой при выборе подчиненного интерфейса, через который будет отправляться исходящий пакет.

Синтаксис

```
inet ifconfig <интерфейс> bonding xmit-hash-policy <layer2 | layer2+3 | layer3+4>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `layer2` — алгоритм, при котором для хеширования используются MAC-адреса отправителя и получателя пакета.
- `layer2+3` — алгоритм, при котором для хеширования используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протоколов IPv4 или IPv6).
- `layer3+4` — алгоритм, при котором для хеширования используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии).

Значения по умолчанию

По умолчанию используется алгоритм `layer2`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы на агрегированном интерфейсе bond1, работающем в режиме `balance-xor`, при выборе подчиненного интерфейса, через который будет отправляться исходящий пакет, использовался алгоритм `layer2+3`, выполните команду:

```
hostname# inet ifconfig bond1 bonding xmit-hash-policy layer2+3
```

inet ifconfig class

Команда используется для установки класса заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> class {access | trunk | slave}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `trunk` — класс интерфейсов, предназначенных для передачи трафика из нескольких VLAN (см. глоссарий, стр. 295).
- `slave` — класс интерфейсов, предназначенных для использования в составе агрегированных интерфейсов.
- `access` — класс интерфейсов, предназначенных для использования во всех остальных случаях.

Значения по умолчанию

По умолчанию все физические интерфейсы ViPNet xFirewall относятся к классу `access`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Класс `trunk` можно установить только для физических и агрегированных интерфейсов. Виртуальные интерфейсы всегда относятся к классу `access`.
- Для агрегированных и виртуальных интерфейсов нельзя установить класс `slave`.
- Нельзя установить класс `trunk`, если на указанном интерфейсе запущен или настроен на автоматический запуск DHCP-сервер или служба DHCP-relay.
- Если на указанном интерфейсе задан один или несколько IP-адресов, то для установки класса `trunk` требуется дополнительное подтверждение. После установки класса `trunk` все адреса будут потеряны.
- Перед установкой класса `access` или `slave` требуется удалить все виртуальные интерфейсы, созданные на базе указанного интерфейса.
- Перед тем как изменить класс интерфейса `slave` на `access` или `trunk`, необходимо, чтобы он не был подчинен ни одному агрегированному интерфейсу.

Пример использования

Чтобы установить класс `trunk` на интерфейсе eth1 для возможности создавать на его базе виртуальные интерфейсы, выполните команду:

```
hostname# inet ifconfig eth1 class trunk
```

inet ifconfig dhcp

Команда используется для установки режима DHCP на заданном интерфейсе.

Синтаксис

```
inet ifconfig <интерфейс> dhcp [<настройка> {on | off}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<настройка>` — название настройки, передаваемой с помощью DHCP. Можно указать одно из следующих значений:
  - `dns` — адреса DNS-серверов;
  - `route` — маршруты;
  - `ntp` — адреса NTP-серверов.
- `on` — включение автоматического приема указанной настройки.
- `off` — выключение автоматического приема указанной настройки.

Значения по умолчанию

По умолчанию для всех настроек, передаваемых с помощью DHCP, автоматический прием включен (`on`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен быть включен.
- Параметр `<настройка>` при вводе команды может не задаваться. В этом случае на интерфейсе будет просто включен режим DHCP.

- Указанный интерфейс может относиться к классу `access` (см. inet ifconfig class на стр. 92) или являться агрегированным интерфейсом.
- Если на интерфейсе заданы дополнительные адреса, они будут потеряны после установки режима DHCP.

Пример использования

Чтобы только установить на интерфейсе eth1 режим DHCP, выполните команду:

```
hostname# inet ifconfig eth1 dhcp route off
```

Чтобы установить на интерфейсе eth2 режим DHCP и выключить автоматический прием маршрута по умолчанию, выполните команду:

```
hostname# inet ifconfig eth2 dhcp route off
```

inet ifconfig dhcp route-metric

Команда используется для задания специфичной метрики (см. глоссарий, стр. 299) маршрутам, поступающим от DHCP-сервера, на конкретном сетевом интерфейсе ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `<1—255>` — значение метрики.
- `none` — удаляет метрику на сетевом интерфейсе.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если на сетевом интерфейсе не установлен режим DHCP, то заданная метрика будет сохранена. Но метрика начнет учитываться только после того, как режим DHCP будет установлен.
- Указанный интерфейс может относиться к классу `access` (см. inet ifconfig class на стр. 92) или являться агрегированным интерфейсом.
- При удалении специфичной метрики будет использоваться метрика по умолчанию для маршрутов DHCP-сервера (см. inet dhcp client route-default-metric на стр. 62).

Пример использования

Чтобы назначить на сетевом интерфейсе eth0 метрику 50, выполните команду:

```
hostname# inet ifconfig eth0 dhcp route-metric 50
```

Чтобы удалить метрику на сетевом интерфейсе eth0, выполните команду:

```
hostname# inet ifconfig eth0 dhcp route-metric none
```

inet ifconfig down

Команда используется для выключения заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> down
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если существуют виртуальные интерфейсы, созданные на базе указанного интерфейса, то требуется дополнительно подтвердить выключение интерфейса. Вместе с интерфейсом автоматически будут выключены все его виртуальные интерфейсы независимо от их текущего состояния.
- Если указанный интерфейс является рабочим для DHCP-сервера, то его нельзя выключить в следующих случаях:
  - DHCP-сервер запущен.
  - DHCP-сервер не запущен, но включен его автоматический запуск при загрузке ViPNet xFirewall.

Пример использования

Чтобы выключить виртуальный интерфейс eth1.2, выполните команду:

```
hostname# inet ifconfig eth1.2 down
```

inet ifconfig reset

Команда используется для сброса настроек заданного сетевого интерфейса либо всех интерфейсов.

Синтаксис

```
inet ifconfig {<интерфейс> | all} reset
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `all` — все интерфейсы.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды с параметром `all` происходит сброс настроек всех физических интерфейсов. Все виртуальные интерфейсы при этом удаляются.
- Команда используется для подготовки указанного интерфейса к установке новых параметров.
- По команде будут выполнены следующие изменения в настройках указанного физического интерфейса:
  - Удалены все существующие дополнительные адреса интерфейса и виртуальные интерфейсы, созданные на его базе.
  - Удалена информация об IP-адресе и маске подсети.
  - Установлен режим автоматического определения параметров скорости интерфейса (см. inet ifconfig speed auto на стр. 99).
  - Будет установлено значение MTU (см. глоссарий, стр. 295) по умолчанию (1500 байт).
  - Интерфейс будет выключен.
- Для виртуальных интерфейсов класса `slave` команда не выполняется.
- Для виртуальных интерфейсов VLAN по команде не сбрасываются следующие настройки:
  - Имя соответствующего физического интерфейса.
  - Номер виртуального интерфейса VLAN.

- Для агрегированных интерфейсов по команде не сбрасываются следующие настройки:
  - Имя агрегированного интерфейса.
  - Режим работы агрегированного интерфейса.
  - Частота проверки соединения на подчиненных физических интерфейсах.

Пример использования

Чтобы сбросить настройки интерфейса `eth1`, выполните команду:

```
hostname# inet ifconfig eth1 reset
This command will reset eth1 interface settings to default
Continue? [Yes,No]: Yes
done.
hostname#
```

inet ifconfig mtu

Команда используется для изменения значения MTU (см. глоссарий, стр. 295) для заданного сетевого интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> mtu {<значение MTU> | auto}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<значение MTU>` — размер MTU в байтах. Допустимые значения: 1280–9000.
- `auto` — задает значение MTU по умолчанию (1500 байт).

Значения по умолчанию

По умолчанию используется значение MTU 1500 байт.

Режимы командного интерпретатора

Администратор.

Особенности использования

- 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.
- Команда не может быть использована для сетевых интерфейсов классов `vlan` и `slave`.
- Значение MTU, заданное для интерфейса класса `trunk`, автоматически применяется ко всем виртуальным интерфейсам класса `vlan`, созданным на этом физическом интерфейсе.
- Значение MTU, заданное для интерфейса класса `bond`, будет использоваться на всех подчиненных физических интерфейсах класса `slave`.
- При создании агрегированного интерфейса с помощью командного интерпретатора для всех подчиненных физических интерфейсов автоматически задается значение MTU 1500 байт.
- Если вы исключаете подчиненный физический интерфейс из агрегированного, для исключенного интерфейса устанавливается значение MTU 1500 байт.

Пример использования

Чтобы для интерфейса `eht0` задать размер MTU, равный 3000 байт, выполните команду:

```
hostname# inet ifconfig eth0 mtu 3000
```

inet ifconfig speed

Команда используется для установки параметров скорости заданного интерфейса.

Примечание. Использование данной команды возможно только для аппаратных исполнений ViPNet xFirewall. Для исполнения ViPNet xFirewall xF-VA команда выполняться не будет.

Синтаксис

```
inet ifconfig <интерфейс> speed <скорость> duplex {half | full}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.

`<скорость>` — скорость в Мбит/с. Можно указать одно из следующих значений: `10`, `100`, `1000`, `10000` (для исполнений, оборудованных соответствующими интерфейсами).

- `half` — полудуплекс (см. глоссарий, стр. 299).
- `full` — полный дуплекс (см. глоссарий, стр. 297).

Значения по умолчанию

По умолчанию на интерфейсе устанавливаются автоматические параметры (определяются исходя из характеристик интерфейса).

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Нельзя установить параметры скорости виртуального интерфейса, так как он наследует эти параметры от соответствующего физического интерфейса.
- Команда неприменима к интерфейсам класса slave (см. inet ifconfig class на стр. 92).
- Установку параметров скорости интерфейса следует использовать с осторожностью и только в тех случаях, когда это действительно необходимо — например, для согласования работы внешнего интерфейса ViPNet xFirewall и коммутационного оборудования, подключенного к данному интерфейсу.

Пример использования

Чтобы на интерфейсе eth1 установить скорость 100 Мбит/с и режим полудуплекса, выполните команду:

```
hostname# inet ifconfig eth1 speed 100 duplex half
```

inet ifconfig speed auto

Команда используется для установки на заданном интерфейсе режима автоматического определения параметров скорости.

Примечание. Использование данной команды возможно только для аппаратных исполнений ViPNet xFirewall. Для исполнения ViPNet xFirewall xF-VA команда выполняться не будет.

Синтаксис

```
inet ifconfig <интерфейс> speed auto
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Нельзя установить параметры скорости виртуального интерфейса, так как он наследует эти параметры от соответствующего физического интерфейса.
- Команда неприменима к интерфейсам класса slave (см. inet ifconfig class на стр. 92).

Пример использования

Чтобы на интерфейсе eth1 установить режим автоматического определения параметров скорости, выполните команду:

```
hostname# inet ifconfig eth1 speed auto
```

inet ifconfig up

Команда используется для включения заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> up
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если существуют виртуальные интерфейсы, созданные на базе указанного интерфейса, то требуется дополнительно подтвердить включение интерфейса. Вместе с интерфейсом автоматически будут включены все его виртуальные интерфейсы независимо от их текущего состояния.
- Нельзя включить виртуальный интерфейс, если выключен соответствующий физический интерфейс.

Пример использования

Чтобы включить виртуальный интерфейс `eth1.2`, выполните команду:

```
hostname# inet ifconfig eth1.2 up
```

inet ifconfig vlan add

Команда используется для создания интерфейса для виртуальной сети (см. глоссарий, стр. 295) с заданным номером.

Синтаксис

```
inet ifconfig <интерфейс> vlan add <номер>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<номер>` — номер виртуальной сети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Физический интерфейс должен относиться к классу trunk (см. inet ifconfig class на стр. 92).
- По команде будет создан виртуальный интерфейс с именем `<интерфейс>.<номер>`. Созданный интерфейс будет иметь то же состояние (включен или выключен), что и физический интерфейс.
- Максимальное количество интерфейсов в ViPNet xFirewall (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

- Номер виртуальной сети `<номер>` должен находиться в диапазоне от 1 до 4094. Значения 0 и 4095 зарезервированы.

Пример использования

Чтобы на базе интерфейса `eth1` создать интерфейс для виртуальной сети с номером 2, выполните команду:

```
hostname# inet ifconfig eth1 vlan add 2
```

inet ifconfig vlan delete

Команда используется для удаления заданного виртуального интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> vlan delete <номер>
```

Параметры и ключевые слова

- `<интерфейс>` — имя физического интерфейса.
- `<номер>` — номер виртуальной сети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе номера работают автозаполнение и подсказка, данные для подсказки берутся из списка существующих виртуальных интерфейсов.

Пример использования

Чтобы удалить виртуальный интерфейс eth1.2, выполните команду:

```
hostname# inet ifconfig eth1 vlan delete 2
```

inet ntp add

Команда предназначена для добавления сервера с заданным адресом в список NTP-серверов (см. глоссарий, стр. 295), используемых для синхронизации времени.

Синтаксис

```
inet ntp add {<адрес> | <DNS-имя>}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес сервера.
- `<DNS-имя>` — DNS-имя сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы в список NTP-серверов добавить сервер `ntp.psn.ru`, выполните команду:

```
hostname# inet ntp add ntp.psn.ru
```

inet ntp delete

Команда предназначена для удаления сервера с заданным адресом из списка NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp delete {<адрес> | <DNS-имя>}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес удаляемого сервера.
- `<DNS-имя>` — DNS-имя удаляемого сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

При вводе адреса или DNS-имени работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка NTP-серверов.

Пример использования

Чтобы из списка NTP-серверов удалить сервер `ntp.psn.ru`, выполните команду:

```
hostname# inet ntp delete ntp.psn.ru
```

inet ntp list

Команда предназначена для просмотра текущего списка NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet ntp list
NTP servers list:
10.0.2.1 from USER
10.0.2.4 from USER
hostname>
```

inet ntp mode

Команда используется для включения или выключения автоматического запуска NTP-сервера при загрузке ViPNet xFirewall.

Синтаксис

```
inet ntp mode {on | off}
```

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

Задается при установке справочников и лицензии (см. глоссарий, стр. 301).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска NTP-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск, если NTP-сервер не запущен.
- Невозможно выключить автоматический запуск, если NTP-сервер запущен.

Пример использования

Чтобы выключить автоматический запуск NTP-сервера, выполните команду:

```
hostname# inet ntp mode off
```

inet ntp start

Команда используется для запуска NTP-сервера.

Синтаксис

```
inet ntp start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet ntp start
```

inet ntp stop

Команда используется для завершения работы NTP-сервера.

Синтаксис

```
inet ntp stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet ntp stop
Stopping NTP server: ntpd.
hostname#
```

inet ospf mode

Команда предназначена для включения или выключения использования протокола OSPF (см. глоссарий, стр. 295).

Синтаксис

```
inet ospf mode {on | off}
```

Параметры и ключевые слова

- `on` — включение использования протокола OSPF;
- `off` — выключение использования протокола OSPF.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet ospf mode on
Loading capability module if not yet done.
Starting Quagga daemons (prio:10): ospfd.
```

```
Stopping Quagga monitor daemons: watchquagga.

Loading capability module if not yet done.

Stopping Quagga monitor daemons: watchquagga.
```

inet ospf network add

Команда используется для добавления сети, в которой должна осуществляться маршрутизация по протоколу OSPF (см. глоссарий, стр. 295).

Синтаксис

```
inet ospf network add <IP-адрес назначения> netmask <маска сети> area <0-4294967295>
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес сети.
- `<маска сети>` — маска сети.
- `area <0-4294967295>` — область маршрутизации (см. глоссарий, стр. 299).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если использование протокола OSPF (см. глоссарий, стр. 295) не включено, задать сеть невозможно.

Пример использования

```
hostname# inet ospf network add 10.0.5.0 netmask 255.255.255.0 area 1

The following OSPF network has been added:

Destination    Netmask          OSPF Area

-----------    -------          ---------

10.0.5.0       255.255.255.0    1

hostname#
```

inet ospf network delete

Команда используется для удаления сети, которая была указана как маршрутизируемая по протоколу OSPF (см. глоссарий, стр. 295).

Синтаксис

```
inet ospf network delete <IP-адрес назначения> netmask <маска сети> area <0-4294967295>
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес сети.
- `<маска сети>` — маска сети.
- `area <0-4294967295>` — область маршрутизации (см. глоссарий, стр. 299).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если использование протокола OSPF (см. глоссарий, стр. 295) не включено, удалить сеть невозможно.
- Если в конфигурации протокола OSPF указанная сеть не будет найдена, ее удаление будет невозможно.

Пример использования

```
hostname# inet ospf network delete 10.0.5.0 netmask 255.255.255.0 area 1

The following OSPF network has been deleted:

Destination    Netmask          OSPF Area

-----------    -------          ---------

10.0.5.0       255.255.255.0    1

hostname#
```

inet ospf redistribute add

Команда используется для включения перераспределения (см. глоссарий, стр. 299) статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF (см. глоссарий, стр. 295).

Синтаксис

```
hostname# inet ospf redistribute add {static | dhcp}
```

Параметры и ключевые слова

- `static` — включение перераспределения статических маршрутов;
- `dhcp` — включение перераспределения маршрутов DHCP-сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. inet ospf mode на стр. 107).
- Перераспределение указанного типа маршрутов было включено ранее.

Пример использования

```
hostname# inet ospf redistribute add static
Redistribution of static routes has been enabled.
hostname#
```

inet ospf redistribute delete

Команда используется для выключения перераспределения (см. глоссарий, стр. 299) статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF (см. глоссарий, стр. 295).

Синтаксис

```
hostname# inet ospf redistribute delete {static | dhcp}
```

Параметры и ключевые слова

- `static` — выключение перераспределения статических маршрутов;
- `dhcp` — выключение перераспределения маршрутов DHCP-сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. inet ospf mode на стр. 107).
- Перераспределение указанного типа маршрутов не было включено ранее.

Пример использования

```
hostname# inet ospf redistribute delete static
Redistribution of static routes has been disabled.
hostname#
```

inet ping

Команда используется для проверки соединения с заданным IP-адресом.

Синтаксис

```
inet ping <IP-адрес>
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес, с которым необходимо проверить соединение.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Для завершения проверки соединения используется сочетание клавиш **Ctrl+C**.

Пример использования

Чтобы проверить соединение с адресом 10.0.2.1, выполните команду:

```
hostname> inet ping 10.0.2.1
Pinging 10.0.2.1, press Ctrl+C to cancel.
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_req=1 ttl=255 time=2.98 ms
64 bytes from 10.0.2.1: icmp_req=2 ttl=255 time=1.60 ms
64 bytes from 10.0.2.1: icmp_req=3 ttl=255 time=1.14 ms
64 bytes from 10.0.2.1: icmp_req=4 ttl=255 time=1.71 ms
^C
--- 10.0.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packets loss, time 3004ms
rtt min/avg/max/mdev = 1.144/1.862/2.983/0.683 ms
hostname>
```

inet route add

Команда используется для добавления статического маршрута (см. глоссарий, стр. 298).

Синтаксис

```
inet route add {<IP-адрес назначения> | default} next-hop <IP-адрес шлюза> [netmask
<маска> [distance <1-255> [weight <1-255>]]]
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес назначения создаваемого маршрута.
- `default` — маршрут по умолчанию, по которому будут пересылаться IP-пакеты с адресом назначения в случае, если для них нет других маршрутов.
- `<IP-адрес шлюза>` — IP-адрес шлюза для доступа к IP-адресу назначения.
- `<маска>` — маска подсети.
- `[distance <1-255>]` — административная дистанция (см. глоссарий, стр. 296).
- `[weight <1-255>]` — вес (см. глоссарий, стр. 296).

Значения по умолчанию

- Если маска не указана, то она принимает следующие значения:
  - 0.0.0.0 — если указано ключевое слово `default`;
  - 255.255.255.255 — в остальных случаях.
- Если административная дистанция не указана, то она принимает значение 10.
- Если вес не указан, то он принимает значение 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Можно добавить несколько маршрутов по умолчанию.
- Если при добавлении нескольких маршрутов в одну и ту же сеть (включая и маршруты по умолчанию) не указывается их вес, то он назначается автоматически.
- Для маршрута по умолчанию не указывается маска подсети.
- Вес маршруту требуется задавать в том случае, если наряду с этим маршрутом будет присутствовать другой маршрут в ту же самую сеть через другой шлюз, и административная дистанция этих маршрутов совпадает. Нельзя задать вес равный 0.
- Добавленный маршрут можно удалить только с помощью команды `inet route delete` (см. inet route delete на стр. 114).

Пример использования

Чтобы добавить маршрут с адресом назначения 10.10.0.0, адресом шлюза 172.16.5.1, маской 255.255.0.0 и дистанцией 15, выполните команду:

```
hostname# inet route add 10.10.0.0 next-hop 172.16.5.1 netmask 255.255.0.0 distance 15
```

Чтобы добавить маршрут по умолчанию, для которого IP-пакеты будут передаваться на шлюз 172.16.5.2, выполните команду:

```
hostname# inet route add default next-hop 172.16.5.2
```

Чтобы добавить несколько маршрутов в одну сеть с разными шлюзами и настроить на них балансировку IP-трафика: в среднем по 50% от всего объема передаваемого IP-трафика на каждый маршрут, выполните команды:

```
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
```

В результате последние два маршрута будут просуммированы — объединены в один маршрут с двумя шлюзами.

inet route clear

Команда используется для удаления всех маршрутов, в том числе маршрута по умолчанию.

Синтаксис

```
inet route clear
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы удалить все маршруты, выполните команду:

```
hostname# inet route clear
```

inet route delete

Команда используется для удаления маршрута.

Синтаксис

```
inet route delete {<IP-адрес назначения> | default} [netmask <маска> [next-hop <IP-адрес шлюза>]]
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес назначения.
- `default` — маршрут по умолчанию.
- `<маска>` — маска подсети.
- `<IP-адрес шлюза>` — IP-адрес шлюза.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Для маршрута по умолчанию не указывается маска подсети.
- Если в удаляемом маршруте не указаны маска сети и IP-адрес шлюза, то производится поиск всех маршрутов в указанный IP-адрес назначения. Если будет найдено несколько маршрутов в указанный IP-адрес назначения, то в результате выполнения команды будет выдан список этих маршрутов. Вы можете подтвердить удаление всех маршрутов, для этого введите символ **y** и нажмите клавишу **Enter**. Аналогичная ситуация возникнет при удалении маршрута с несколькими шлюзами.

Пример использования

Чтобы удалить маршрут с адресом назначения 10.0.14.0, выполните команду:

```
hostname# inet route delete 10.0.14.0
You are going to delete the following static routes:
Destination    Netmask          Next hop     Distance   Weight
-----------    -------          ---------    --------   ------
10.0.14.0      255.255.255.0    10.0.1.1     10         1
10.0.14.0      255.255.255.0    10.0.2.1     10         1
Continue? (y/n): y
Routes deleted.
hostname#
```

inet show dhcp client

Команда предназначена для просмотра настроек DHCP на сетевых интерфейсах (настроек DHCP-клиента).

Синтаксис

```
inet show dhcp client
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show dhcp client

Administrative distance for DHCP routes: 80

Default metric for DHCP routes: 60

Interface    DHCP       Routes     Metric      DNS         NTP

---------    ----       ------     ------      ---         ---

eth0         no         yes        default     yes         yes

eth1         yes        yes        50          yes         yes

eth2         no         yes        default     yes         yes

eth3         no         yes        default     yes         yes

hostname>
```

По команде выводится следующая информация:

- административная дистанция, которая задана для маршрутов, поступающих от DHCP-сервера;
- метрика по умолчанию;
- список сетевых интерфейсов со следующими параметрами:
  - статус режима DHCP: включен (`yes`) или выключен (`no`);
  - разрешение на автоматическое получение IP-адресов;
  - специфичные метрики на сетевых интерфейсах, если такие заданы;
  - разрешение на автоматическое получение адресов DNS-серверов;
  - разрешение на автоматическое получение адресов NTP-серверов.

inet show dhcp relay

Команда предназначена для просмотра настроек службы DHCP-relay и ее текущего состояния.

Синтаксис

```
inet show dhcp relay
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show dhcp relay
Mode of dhcp relay is set to off
The server for forwarding dhcp relay requests is set in 172.16.1.1
The interface on which side is dhcp the server is eth1
The list of interfaces on which will listen dhcp requests: eth2
Service dhcp relay is running
hostname>
```

inet show dhcp server

Команда предназначена для просмотра настроек DHCP-сервера и его текущего состояния.

Синтаксис

```
inet show dhcp server
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show dhcp server
DHCP server is off
DHCP server is RUNNING
start   172.16.1.2
end     172.16.1.254
interface       eth0
option subnet  255.255.255.0
option router  172.16.1.1
option wins    172.16.1.1
option lease   864000
max_leases 65533
hostname>
```

inet show dns

Команда предназначена для просмотра текущего состояния DNS-сервера.

Синтаксис

```
inet show dns
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.

- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show dns
DNS server is on
DNS server is RUNNING
hostname>
```

inet show interface

Команда предназначена для просмотра параметров заданного интерфейса и его текущего состояния.

Синтаксис

```
inet show interface [<имя интерфейса> | <имя интерфейса>:<номер>]
```

Параметры и ключевые слова

- `<имя интерфейса>` — имя физического или виртуального интерфейса.
- `<имя интерфейса>:<номер>` — имя виртуального интерфейса, если основной интерфейс имеет дополнительный IP-адрес (alias).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Если параметр не указан, то выводится информация обо всех интерфейсах, включая существующие дополнительные IP-адреса интерфейсов.

- Если в качестве параметра вы указали имя виртуального интерфейса, созданного при добавлении на основной интерфейс дополнительного IP-адреса, то будет выдана краткая информация по основному интерфейсу.
- Если в качестве параметра вы указали имя агрегированного интерфейса, помимо приведенной ниже информации будет выведено следующее:
  - режим работы агрегированного канала;
  - частоту проверки соединения для подчиненных интерфейсов в миллисекундах;
  - в режиме `802.3ad` — режим выбора активного агрегатора и частоту обмена пакетами LACP;
  - в режиме `802.3ad` и `balance-xor` — алгоритм хэширования пакетов;
  - в режимах `active-backup`, `balance-tlb` — основной подчиненный интерфейс;
  - список подчиненных физических интерфейсов.

Пример использования

Чтобы просмотреть информацию об интерфейсе eth0, выполните команду:

```
hostname> inet show interface eth0

eth0      Link encap:Ethernet  HWaddr 00:15:17:e4:6c:5a
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

          Configured by DHCP: yes
          Information requested from DHCP server: IP address, routes, DNS
          servers, NTP servers
          DHCP route metric: default (70)
          Class: access

          Speed: 1000Mb/s
          Duplex: Full
          Auto-negotiation: off
          Link detected: yes
```

По команде выводится следующая информация:

- IP-адрес.
- Маска подсети.
- Настройки получения информации от DHCP-сервера и заданная метрика для маршрутов DHCP-сервера, если на интерфейсе включен соответствующий режим.
- Класс интерфейса (access, trunk или slave) (см. inet ifconfig class на стр. 92). В зависимости от класса интерфейса также выводится следующая информация:

- Для класса trunk — список существующих дочерних виртуальных интерфейсов.
- Для класса access— информация о родительском интерфейсе данного виртуального интерфейса.
- Для класса slave— информация о том, какому агрегированному интерфейсу подчинен данный интерфейс либо информация о том, что интерфейс пока не подчинен ни одному из агрегированных интерфейсов.

- Состояние интерфейса (включен или выключен).
- Если вы выполняете команду на ViPNet xFirewall в исполнении xF-VA, для всех сетевых интерфейсов по команде выводится максимальная возможная скорость 10000 Мбит/с. Реальная скорость передачи данных через интерфейс зависит от характеристик аппаратного обеспечения, назначенного для виртуальной машины.

inet show mac-address-table

Команда предназначена для просмотра ARP-таблицы (таблицы преобразования IP-адресов в MAC-адреса).

Синтаксис

```
inet show mac-address-table
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show mac-address-table
Address         HWtype  HWaddress           Flags Mask  Iface
172.16.5.1      ether   4c:02:89:0c:53:a2   C           eth3
172.23.221.11   ether   00:0c:29:09:1a:98   C           eth0
```

```
172.23.221.99  ether   54:04:a6:d0:f7:1a  C           eth0
172.16.5.3     ether   4c:02:89:08:ef:24  C           eth3
hostname>
```

inet show ntp

Команда предназначена для просмотра настроек NTP-сервера и его текущего состояния.

Синтаксис

```
inet show ntp
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если NTP-сервер запущен, дополнительно выводятся параметры NTP-серверов, используемых для синхронизации. Эта информация выводится в виде таблицы аналогично выводу команды `ntpq -pn`.

Пример использования

```
hostname> inet show ntp
NTP server is off
NTP server is RUNNING
   remote       refid     st t when poll reach  delay  offset jitter
==============================================================================
 10.0.2.1       10.0.2.4    5 u  36    64     1  3.893  0.708  0.000
 10.0.2.1       10.0.6.100 4 u  35    64     1  0.702 25.706  0.000
 194.149.67.129  .INIT.   16 u   -    64     0  0.000 0.000   0.000
hostname>
```

Возможны следующие состояния NTP-сервера:

- `NTP server is INITIALIZING` — NTP-сервер в процессе запуска с проверкой доступности публичных или корпоративных NTP-серверов.
- `NTP server is RUNNING` — NTP-сервер запущен, доступен хотя бы один NTP-сервер.

- `NTP server is TERMINATING` — работа NTP-сервера в процессе завершения.
- `NTP server is STOPPED` — NTP-сервер не запущен.

В зависимости от столбца, в нем содержится следующая информация:

- `remote` — IP-адреса внешних NTP-серверов, с которыми синхронизируется время.
- `refid` — сервер, с которым синхронизируется данный NTP-сервер.
- `st` — уровень сервера, с которым синхронизируется данный NTP-сервер.
- `t` — тип соединения, принимает следующие значения:
  - `u` — unicast или manycast;
  - `o`— broadcast или multicast;
  - `l` — local reference clock;
  - s — симметричный узел;
  - `A` — manycast NTP-сервер;
  - `B` — broadcast NTP-сервер;
  - `M` — multicast NTP-сервер.
- `when` — время, соответствующее последнему ответу NTP-сервера.
- `poll` — частота опроса.
- `reach` — восьмой бит октета, показывающий статус общения с внешним NTP-сервером.
- `delay` — время в миллисекундах между отправкой и получения ответа.
- `offset` — смещение в миллисекундах между ViPNet xFirewall и NTP-серверами.
- `jitter` — абсолютное значение в миллисекундах с указанием среднеквадратичного отклонения смещения относительно ViPNet xFirewall.
- `refid` — код ошибки или идентификатор NTP-сервера.

inet show ospf configuration

Команда предназначена для просмотра настроек протокола OSPF.

Синтаксис

```
inet show ospf configuration
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show ospf configuration

OSPF protocol is enabled

OSPF networks defined:

Destination    Netmask          OSPF Area

-----------    -------          ---------

10.0.2.0       255.255.255.0    1

10.0.5.0       255.255.255.0    0

Redistribution of DHCP routes is enabled.

hostname>
```

По команде выводится следующая информация:

- включено или выключено использование протокола OSPF;
- список сетей, в которых ViPNet xFirewall осуществляет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
- включено или выключено перераспределения маршрутов (статических или от DHCP-сервера).

inet show ospf database

Команда предназначена для просмотра информации о состоянии каналов связей между всеми OSPF-маршрутизаторами в базе данных (link state database).

Синтаксис

```
inet show ospf database
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show ospf database

       OSPF Router with ID (10.0.5.2)

              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]
```

```
hostname>
```

inet show ospf neighbour

Команда предназначена для просмотра сведений о соседних OSPF-маршрутизаторах, работающих в вашей сети по протоколу OSPF.

Синтаксис

```
inet show ospf neighbour
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show ospf neighbour

Neighbor ID    Pri    State     Dead Time   Address    Interface       RXmtl   Rqstl   DBsml

10.1.30.5      1      Full/DR   33.310s     10.0.5.5   eth0:10.0.5.2   0       0       0

hostname>
```

По команде выводится следующая информация для каждого маршрутизатора:

- IP-адрес активного сетевого интерфейса, по которому доступен маршрутизатор для обмена информацией по протоколу OSPF;
- порядковый номер маршрутизатора, под которым он известен другим маршрутизаторам при работе по протоколу OSPF;
- тип маршрутизатора (в приведенном примере маршрутизатор-сосед является назначенным, что показывает значение `DR` в поле `State`);

- интервал простоя маршрутизатора, по истечении которого он будет считаться неактивным (выключенным);
- другие параметры.

inet show routing

Команда предназначена для просмотра содержимого общей таблицы маршрутизации или списков маршрутов от конкретного источника (Static, DHCP, OSPF).

Синтаксис

```
inet show routing {static | dhcp | ospf}
```

Параметры и ключевые слова

- `static` — для просмотра статических маршрутов;
- `dhcp` — для просмотра динамических маршрутов, получаемых от DHCP-сервера;
- `ospf` — для просмотра динамических маршрутов передаваемых по протоколу OSPF.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Если параметр не указан, то выводится список со всеми маршрутами.
- Если указан параметр, для которого не существует маршрутов, вывод команды будет пустой.
- Маршруты в одну и ту же сеть, полученные от одного источника и с одинаковой метрикой (или административной дистанцией в случае статических маршрутов), отображаются в виде одного маршрута с несколькими шлюзами.
- Если маршрут по умолчанию не задан и отсутствует в таблице маршрутизации, выводится соответствующее предупреждение.

Пример использования

```
hostname> inet show routing
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel, D - DHCP,
```

```
        > - selected route, * - FIB route
D       0.0.0.0/0 [35/23] via 10.1.30.5, eth1
S>      0.0.0.0/0 [10/0] (weight 1) via 10.0.1.4 inactive
                         (weight 1) via 10.0.2.1 inactive
  *                      (weight 1) via 10.0.5.2, eth0
S>*     10.0.1.0/24 [10/0] via 10.0.5.2, eth0
S>*     10.0.2.0/24 [10/0] via 10.0.5.2, eth0
O       10.0.5.0/24 [110/10] is directly connected, eth0, 5d22h18m
C>*     10.0.5.0/24 is directly connected, eth0
S       10.1.1.1/32 [10/0] (weight 1) via 10.2.2.2 inactive
                           (weight 1) via 10.3.3.2 inactive
D>*     10.100.2.0/24 [30/23] (weight 1) via 10.1.30.202, eth1
  *                         (weight 1) via 10.1.30.202, eth1
hostname>
```

Пояснения по атрибутам, которые выводятся перед списком маршрутов, приведены в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», в разделе «Просмотр таблицы маршрутизации».

inet show snmp

Команда используется для просмотра информации о текущем состоянии SNMP-агента, IP-адресе удаленного узла, на который отправляются оповещения SNMP Traps, а также о заданном уровне протоколирования.

Синтаксис

```
inet show snmp
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show snmp

VPN SNMP agent mode is ON.

VPN SNMP agent is RUNNING.

debug-level = info

trapsink = 192.168.0.1

hostname>
```

inet show snmp community

Команда используется для просмотра следующих паролей:

1. Пароль для авторизации на удаленной станции сетевого менеджмента, заданный с помощью команды inet snmp community trap (на стр. 131).
2. Текущий пароль доступа к SNMP-параметрам ViPNet xFirewall, заданный с помощью команды inet snmp community ro (на стр. 131).

Синтаксис

```
inet show snmp community
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show snmp community

community ro = public

community trap = public

hostname>
```

inet show vlan

Команда предназначена для просмотра списка существующих виртуальных интерфейсов.

Синтаксис

```
inet show vlan
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> inet show vlan
VLAN interfaces
Id    | Name      | IP           | Parent| Comment
11    | eth2.11   | 172.16.11.2  | eth2  | VLAN11
12    | eth2.12   | 172.16.12.2  | eth2  | VLAN12
13    | eth2.13   | 172.16.13.2  | eth2  | VLAN13
14    | eth2.14   | 172.16.14.2  | eth2  | VLAN14
hostname>
```

Таблица со списком виртуальных интерфейсов содержит следующие столбцы:

- `Id` — номер виртуальной сети.

- `Name` — имя виртуального интерфейса.
- `IP` — IP-адрес виртуального интерфейса.
- `Parent` — имя родительского физического интерфейса.
- `Comment` — комментарий к виртуальной сети.

inet snmp community ro

Команда используется для задания пароля доступа к SNMP-параметрам вашего ViPNet xFirewall.

Синтаксис

```
inet snmp community ro <пароль>
```

Параметры и ключевые слова

`<пароль>` — последовательность, содержащая от 6 до 18 символов.

Значения по умолчанию

По умолчанию задан пароль `public`.

Режимы командного интерпретатора

Администратор.

Особенности использования

В паролях вы можете использовать символы латинского алфавита, цифры, а также следующие специальные символы: «.», «*», «/», «-», «:», «_», «?», «=», «@», «&».

Пример использования

Чтобы задать пароль `Aa1234567`, выполните команду:

```
hostname# inet snmp community ro Aa1234567

hostname#
```

inet snmp community trap

Команда используется для задания пароля, используемого при авторизации на удаленной станции сетевого менеджмента, принимающей оповещения SNMP Traps.

Синтаксис

```
inet snmp community trap <пароль>
```

Параметры и ключевые слова

`<пароль>` — последовательность, содержащая от 6 до 18 символов

Значения по умолчанию

По умолчанию задан пароль `public`.

Режимы командного интерпретатора

Администратор.

Особенности использования

В паролях вы можете использовать символы латинского алфавита, цифры, а также следующие специальные символы: «.», «*», «/», «-», «:», «_», «?», «=», «@», «&».

Пример использования

Чтобы задать пароль `Aa1234567`, выполните команду:

```
hostname# inet snmp community trap Aa1234567
hostname#
```

inet snmp debug-level

Команда используется для задания событий SNMP-агента, которые будут записываться в журнал событий.

Синтаксис

```
inet snmp debug-level <уровень детализации>
```

Параметры и ключевые слова

`<уровень детализации>` — может принимать одно из следующих значений:

- `off` — протоколирование выключено.
- `info` — протоколируется только информация, касающаяся инициализации SNMP-агента.
- `debug` — протоколируется служебная информация, используемая при отладке.
- `error` — протоколируются ошибки, после которых SNMP-агент может продолжать работу.

- `critical` — протоколируются критические ошибки, после которых SNMP-агент не может продолжить работу.

Значения по умолчанию

По умолчанию используется уровень `info`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы выключить протоколирование событий SNMP-агента, выполните команду:

```
hostname# inet snmp debug-level off
hostname#
```

inet snmp mode

Команда предназначена для включения или выключения запуска SNMP-агента при загрузке ViPNet xFirewall.

Синтаксис

```
inet snmp mode {on | off}
```

Параметры и ключевые слова

- `on` — включение запуска SNMP-агента при загрузке ViPNet xFirewall.
- `off` — выключение запуска SNMP-агента при загрузке ViPNet xFirewall.

Значения по умолчанию

По умолчанию запуск SNMP-агента при загрузке ViPNet xFirewall включен (`on`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы включить запуск SNMP-агента при загрузке ViPNet xFirewall, выполните команду:

```
hostname# inet snmp mode on
VPN SNMP agent enabled and will be started during next boot.
You have to start VPN SNMP agent manually or reboot to have it running.
hostname#
```

inet snmp start

Команда используется для запуска встроенного SNMP-агента.

Синтаксис

```
inet snmp start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet snmp start
Starting VPN SNMP agent: vpn-snmpd.
hostname#
```

inet snmp stop

Команда используется для завершения работы встроенного SNMP-агента.

Синтаксис

```
inet snmp stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# inet snmp stop
Stopping VPN SNMP agent: vpn-snmpd.
hostname#
```

inet snmp trapsink

Команда используется для задания сетевого узла, на который будут направляться оповещения по протоколу `SNMP`.

Синтаксис

```
inet snmp trapsink {<IP-адрес> | null}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес удаленного сетевого узла.
- `null` — выключить оповещения.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Сетевой узел, на который будут отправляться оповещения по протоколу `SNMP`, должен быть доступен для ViPNet xFirewall.

Пример использования

Для направления оповещений по протоколу `SNMP` на узел с адресом 192.168.10.10 выполните команду:

```
hostname# inet snmp trapsink 192.168.10.10
```

inet ssh

Команда используется для удаленного доступа по SSH к заданному компьютеру.

Синтаксис

```
inet ssh {host <компьютер> | id <идентификатор>} [user <пользователь>] [port <порт>]
```

Параметры и ключевые слова

- `<компьютер>` — имя или IP-адрес удаленного компьютера.
- `<идентификатор>` — идентификатор сетевого узла ViPNet в шестнадцатеричном формате. Используется для доступа к узлу сети ViPNet.
- `<пользователь>` — имя пользователя удаленного компьютера.
- `<порт>` — номер порта доступа.

Значения по умолчанию

- `<пользователь>` — user.
- `<порт>` — 22.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе идентификатора работают автозаполнение и подсказка, данные для подсказки берутся из списка связей ViPNet xFirewall.
- На время установления соединения с удаленным компьютером блокируется доступ к консоли. Максимальное время ожидания — 90 секунд. По истечении этого времени удаленный компьютер считается недоступным и соединение разрывается.
- 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 консоли символов нелатинского алфавита.

Пример использования

Чтобы подключиться к узлу ViPNet с идентификатором 0x270e000a, выполните команду:

```
hostname# inet ssh id 0x270e000a
```

inet vlan comment add

Команда используется для добавления комментария к виртуальной сети с заданным номером.

Синтаксис

```
inet vlan <номер> comment add <комментарий>
```

Параметры и ключевые слова

- `<номер>` — номер виртуальной сети.
- `<комментарий>` — комментарий. Комментарий, содержащий пробелы, должен быть указан в двойных кавычках.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы добавить комментарий «This is VLAN number 10» к виртуальной сети с номером 10, выполните команду:

```
hostname# inet vlan 10 comment add "This is VLAN number 10"
```

inet vlan comment delete

Команда используется для удаления комментария к виртуальной сети с заданным номером.

Синтаксис

```
inet vlan <номер> comment delete
```

Параметры и ключевые слова

`<номер>` — номер виртуальной сети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы удалить комментарий к виртуальной сети с номером 10, выполните команду:

```
hostname# inet vlan 10 comment delete
```

Команды группы iplir

Команды группы `iplir` предназначены для настройки параметров работы в сети ViPNet (см. глоссарий, стр. 300).

iplir config

Команда используется для редактирования одного из файлов конфигурации: основного файла конфигурации, файла конфигурации заданного интерфейса.

Синтаксис

```
iplir config {<интерфейс>}
```

Параметры и ключевые слова

`<интерфейс>` — имя статического интерфейса (см. глоссарий, стр. 301), для которого требуется редактировать файл конфигурации.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если в команде не указан параметр, то будет запущен текстовый редактор с основным файлом конфигурации `iplir.conf`.
- Если в команде указан интерфейс, то будет запущен текстовый редактор с файлом конфигурации этого интерфейса `iplir.conf-<интерфейс`.
- Перед редактированием файла `iplir.conf` или файла `iplir.conf-<интерфейс` требуется завершить работу демона `iplircfg` (см. iplir stop на стр. 155).

Пример использования

Чтобы отредактировать файл конфигурации интерфейса eth0, выполните команду:

```
hostname# iplir config eth0
```

iplir info

Команда предназначена для просмотра информации о своем узле, а также для просмотра статистики фильтрации IP-пакетов по заданному интерфейсу.

Синтаксис

```
iplir info {<интерфейс>}
```

Параметры и ключевые слова

`<интерфейс>` — имя статического интерфейса (см. глоссарий, стр. 301), для которого требуется просмотреть статистику фильтрации IP-пакетов.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Если в команде не указан параметр, то выводится информация об узле (имя узла, имя сети, версия установленного ПО, активные сетевые интерфейсы и другие параметры) и статистика фильтрации IP-пакетов по всем интерфейсам.
- Если в команде указан интерфейс, то выводится только статистика фильтрации IP-пакетов по этому интерфейсу.
- Для выполнения команды требуется, чтобы был запущен демон iplircfg.

Пример использования

Для просмотра статистики по интерфейсу eth0 выполните команду:

```
hostname> iplir info eth0
Interface:              eth0

Category                                        Received            Sent

Non-encrypted packets passed:                          0               0
Non-encrypted packets dropped:                         0               0
Non-encrypted bytes passed:                            0               0
Non-encrypted bytes dropped:                           0               0
```

```
Encrypted packets passed:                          0                0
Encrypted packets dropped:                         0                0
Encrypted bytes passed:                            0                0
Encrypted bytes dropped:                           0                0

Non-encrypted broadcast packets passed:            0                0
Non-encrypted broadcast packets dropped:           2                0
Non-encrypted broadcast bytes passed:              0                0
Non-encrypted broadcast bytes dropped:           271                0


Encrypted broadcast packets passed:                0                2
Encrypted broadcast packets dropped:               0                0
Encrypted broadcast bytes passed:                  0              271
Encrypted broadcast bytes dropped:                 0                0
hostname>
```

iplir option get

Команда предназначена для просмотра текущего состояния или значения одного из параметров межсетевого экрана (см. глоссарий, стр. 298).

Синтаксис

```
iplir option get <параметр>
```

Параметры и ключевые слова

`<параметр>` — имя параметра межсетевого экрана. Можно указать один из следующих параметров:

- `antispoofing` — состояние функции антиспуфинга (см. глоссарий, стр. 296);
- `block-fragmented-packets` — состояние функции блокирования фрагментированных IP-пакетов, передаваемых по всем сетевым интерфейсам;
- `max-connections` — максимальное количество параллельно установленных соединений;
- `connection-ttl-ip` — время жизни соединений по протоколу IP;
- `connection-ttl-tcp` — время жизни соединений по протоколу TCP;
- `connection-ttl-udp` — время жизни соединений по протоколу UDP.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.

- Администратор.

Особенности использования

Нет.

Пример использования

Для просмотра максимального количества параллельно установленных соединений выполните команду:

```
hostname> iplir option get max-connections
Option: Max-connections State: 15000
hostname> _
```

iplir option set antispoofing

Команда используется для включения или выключения антиспуфинга (см. глоссарий, стр. 296).

Синтаксис

```
iplir option set antispoofing {on | off}
```

Параметры и ключевые слова

- `on` — включение антиспуфинга.
- `off` — выключение антиспуфинга.

Значения по умолчанию

По умолчанию антиспуфинг выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для включения антиспуфинга выполните команду:

```
hostname# iplir option set antispoofing on
```

iplir option set block-fragmented-packets

Команда используется для включения или выключения блокирования входящих фрагментированных IP-пакетов, которые принимаются по всем сетевым интерфейсам.

Синтаксис

```
iplir option set block-fragmented-packets {on | off}
```

Параметры и ключевые слова

- `on` — включение блокирования.
- `off` — выключение блокирования.

Значения по умолчанию

По умолчанию блокирование выключено (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для включения блокирования выполните команду:

```
hostname# iplir option set block-fragmented-packets on
```

iplir option set connection-ttl-ip

Команда используется для задания времени жизни соединения по протоколу IP при отсутствии активности в нем.

Синтаксис

```
iplir option set connection-ttl-ip <значение>
```

Параметры и ключевые слова

`<значение>` — время жизни в секундах.

Значения по умолчанию

60 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы задать время жизни соединений по протоколу IP равным 150 секунд, выполните команду:

```
hostname# iplir option set connection-ttl-ip 150
```

iplir option set connection-ttl-tcp

Команда используется для задания времени жизни соединения по протоколу TCP при отсутствии активности в нем.

Синтаксис

```
iplir option set connection-ttl-tcp <значение>
```

Параметры и ключевые слова

`<значение>` — время в секундах.

Значения по умолчанию

3600 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы задать время жизни соединений по протоколу TCP равным 1500 секунд, выполните команду:

```
hostname# iplir option set connection-ttl-tcp 1500
```

iplir option set connection-ttl-udp

Команда используется для задания времени жизни соединения по протоколу UDP при отсутствии активности в нем.

Синтаксис

```
iplir option set connection-ttl-udp <значение>
```

Параметры и ключевые слова

`<значение>` — время в секундах.

Значения по умолчанию

300 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы задать время жизни соединений по протоколу UDP равным 150 секунд, выполните команду:

```
hostname# iplir option set connection-ttl-udp 150
```

iplir option set max-connections

Команда используется для задания максимального количества параллельно установленных соединений.

Синтаксис

```
iplir option set max-connections <количество>
```

Параметры и ключевые слова

`<количество>` — количество соединений.

Значения по умолчанию

Значение по умолчанию, а также максимально возможное значение параметра зависят от используемого исполнения ViPNet xFirewall.

Таблица 3. 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

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы установить максимальное количество одновременных соединений равным 200000, выполните команду:

```
hostname# iplir option set max-connections 200000
```

iplir ping

Команда используется для проверки соединения с заданным сетевым узлом ViPNet.

Синтаксис

```
iplir ping <идентификатор>
```

Параметры и ключевые слова

`<идентификатор>` — шестнадцатеричный идентификатор сетевого узла ViPNet, соединение с которым необходимо проверить.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- При вводе идентификатора работают автозаполнение и подсказка, данные для подсказки берутся из списка связей ViPNet xFirewall с другими узлами.
- Для выполнения команды требуется, чтобы был запущен демон `iplircfg`.

Пример использования

Для проверки связи ViPNet xFirewall с узлом, который имеет идентификатор `0x15ea000d`, выполните команду:

```
hostname> iplir ping 0x15ea000d
```

iplir set cipher-mode

Команда используется для установки режима шифрования.

Синтаксис

```
iplir set cipher-mode {gost-ctr | gost-cfb| aes}
```

Параметры и ключевые слова

- `gost-ctr` — режим гаммирования GOST-CTR (Counter mode).
- `gost-cfb` — режим гаммирования с обратной связью GOST-CFB (Cipher Feedback mode).
- `aes` — режим гаммирования AES.

Значения по умолчанию

По умолчанию используется режим гаммирования GOST-CTR (`gost-ctr`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- После смены режима шифрования требуется перезагрузить компьютер. Если при выполнении команды вы откажетесь от перезагрузки, новый режим шифрования не будет установлен.
- При работе ViPNet xFirewall в режиме кластера горячего резервирования (см. глоссарий, стр. 297) устанавливать режим шифрования требуется не только на активном, но и на пассивом сервере кластера, так как данная настройка не может передаваться с активного сервера на пассивный в ходе резервирования.

Пример использования

Для установки режима шифрования GOST-CFB выполните команду:

```
hostname# iplir set cipher-mode gost-cfb
The GOST-CFB mode is set. It is necessary to reboot system to changes become
effective.
Would you like to reboot now? [y/n]: y
```

iplir show adapters

Команда предназначена для просмотра всех активных статических интерфейсов ViPNet xFirewall (см. глоссарий, стр. 301) . При просмотре для каждого интерфейса в списке указан параметр `allowtraffic`, который показывает, разрешено или заблокировано прохождения IP-трафика через интерфейс.

Синтаксис

```
iplir show adapters
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

Для просмотра списка активных сетевых интерфейсов выполните команду:

```
hostname> iplir show adapters

Active interface    Allowtraffic

eth0                on

eth1                on

eth2                off

eth3                on
```

iplir show cipher-mode

Команда предназначена для просмотра информации о текущем режиме шифрования.

Синтаксис

```
iplir show cipher-mode
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> iplir show cipher-mode
GOST - CTR: Counter Mode
hostname>
```

iplir show config

Команда предназначена для просмотра одного из файлов конфигурации — основного файла конфигурации или файла конфигурации заданного интерфейса.

Синтаксис

```
iplir show config {<интерфейс>}
```

Параметры и ключевые слова

`<интерфейс>` — имя статического интерфейса (см. глоссарий, стр. 301), файл конфигурации которого требуется просмотреть.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Если в команде не указан параметр, то выводится основной файл конфигурации `iplir.conf`.
- Если в команде указан интерфейс, то выводится файл конфигурации этого интерфейса `iplir.conf-<интерфейс>`.
- Для завершения просмотра файла конфигурации используется клавиша **Q**.

Пример использования

Чтобы просмотреть основной файл конфигурации, выполните команду:

```
hostname> iplir show config
[id]
id= 0x15ea000b
name= xFirewall 2
ip= 10.0.14.101
...
hostname>
```

iplir show firewall status

Команда предназначена для просмотра статистики работы межсетевого экрана.

Синтаксис

```
iplir show firewall status
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> iplir show firewall status
Max connections   150000
TCP SYN timeout   120
Connection ttl TCP   1800
Connection ttl UDP   300
ICMP timeout   30
Connection ttl IP   300
Total connections count   39
Public connections count   28
VPN connections count   11
hostname>
```

По команде выводится следующая информация:

- `Max connections` — максимальное количество одновременных соединений (см. iplir option set max-connections на стр. 145).
- `TCP SYN timeout` — таймаут установления TCP-соединения в секундах.
- `Connection ttl TCP` — таймаут разрыва TCP-соединения в секундах.
- `Connection ttl UDP` — время жизни UDP-соединения.
- `ICMP timeout` — время жизни ICMP-соединения.
- `Connection ttl IP` — время жизни соединения для протоколов, отличных от TCP, UDP, ICMP.
- `Total connections count` — текущее количество открытых соединений и соединений с узлами сети ViPNet по всем протоколам.

- `Public connections count` — текущее количество открытых соединений по всем протоколам.
- `VPN connections count` — текущее количество соединений с узлами сети ViPNet по всем протоколам.

iplir show key-info

Команда используется для получения информации о ключах, входящих в состав лицензии, установленной на ViPNet xFirewall. Предоставляется информация о следующих ключах:

- персональный ключ пользователя (см. глоссарий, стр. 299);
- резервный набор персональных ключей (РНПК) (см. глоссарий, стр. 300);
- ключи узла.

Синтаксис

```
iplir show key-info
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Получение информации о ключах может требоваться в следующих случаях:

- Администратору ViPNet xFirewall — чтобы убедиться в наличии или отсутствии файла РНПК на узле.
- Сотрудникам технического сопровождения «ИнфоТеКС» — для выяснения причин возникновения проблем с ключевой системой ViPNet xFirewall (например, после обновления справочников и лицензии).

Пример использования

```
hostname# iplir show key-info

Current personal key info:                              //Информация о персональном
ключе

  User ID: 0x16310029
```

```
  Key variant: 0
  Master key date: 2014-06-23 13:44:57 MSK
  Master key number: 1
  Key update date: 2015-05-25 15:40:24 MSK
Spare key set info:                                    //Информация о РНПК
  User ID: 0x16310029
  Key variants: from 0 to 19
  Master key date: 2014-06-23 13:44:57 MSK
Lck key info:                                          //Информация о ключах узла
  User ID: 0x16310029
  Master key date: 2014-06-23 13:44:57 MSK
Current defense key info:
  AP ID: 0x1631002a
  Current defense key variant: 0
  Master defense key date: 2014-06-23 13:44:57 MSK
  Master defense key number: 1
  Current defense key update date: 2015-05-25 15:40:24 MSK
Cck key info:
  Ap ID: AP ID: 0x1631002a
  Master cck key date: 2014-06-23 13:44:57 MSK
hostname#
```

iplir show keys-upgrade-log

Команда предназначена для просмотра журнала, в котором содержится информация о принятых обновлениях справочников и лицензии (см. глоссарий, стр. 301).

Синтаксис

```
iplir show keys-upgrade-log
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# iplir show keys-upgrade-log
19/05/2016 16:37:34.896  Starting upgrade process ...
19/05/2016 16:37:34.896  try find /opt/vipnet/ccc/ap*.dtm
...
hostname#
```

iplir start

Команда используется для запуска управляющего демона iplircfg.

Синтаксис

```
iplir start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> iplir start
Loading DPI modules
Loading Kernel Interface driver
Loading Iplir Watchdog driver
```

```
Loading IpLir Crypto driver
Loading IpLir driver
Loading IPCLS driver
Loading IpLir
hostname>
```

iplir stop

Команда используется для завершения работы управляющего демона `iplircfg`.

Синтаксис

```
iplir stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> iplir stop
Shutting down IpLir
hostname>
```

iplir view

Команда предназначена для просмотра журнала регистрации IP-пакетов.

Синтаксис

```
iplir view
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- После ввода команды будет запущена программа просмотра с эмуляцией графического интерфейса, на экране появится окно для задания параметров поиска в журнале IP-пакетов. После ввода параметров и поиска нужных записей появится окно с результатом поиска.
- Для выполнения команды требуется, чтобы был запущен демон `iplircfg`.
- При работе ViPNet xFirewall в режиме кластера горячего резервирования (см. глоссарий, стр. 297) на пассивном сервере кластера нельзя просмотреть журнал IP-пакетов.

Пример использования

```
hostname# iplir view
```

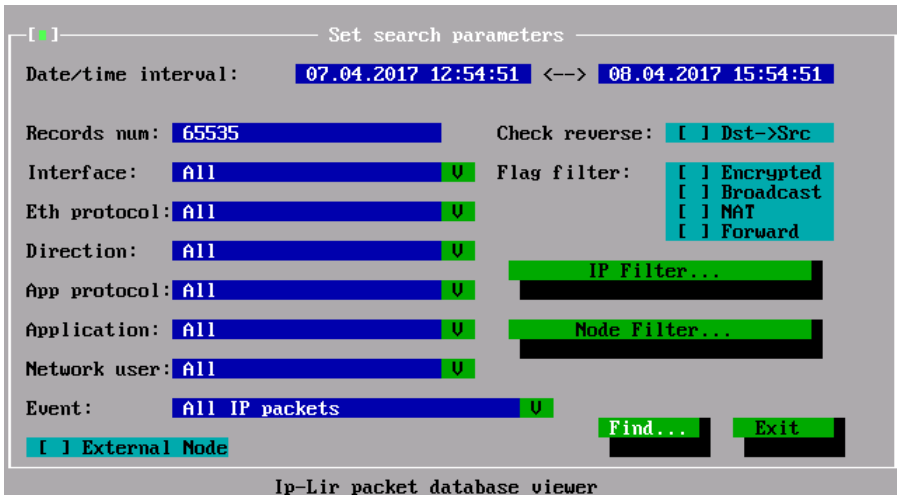

Рисунок 1. Задание параметров поиска записей в журнале регистрации IP-пакетов

Команды группы machine

Команды группы `machine` предназначены для выключения и перезагрузки компьютера, установки имени компьютера и системного времени, работы с журналом событий, а также для регламентного тестирования ViPNet xFirewall.

machine halt

Команда используется для выключения компьютера.

Синтаксис

```
machine halt
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine halt
Shutting down failover daemon
Shutting down MFTP daemon
Shutting down IpLir
hostname> The session has been forced to close.
```

machine reboot

Команда используется для перезагрузки компьютера.

Синтаксис

```
machine reboot
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine reboot
Shutting down failover daemon
Shutting down MFTP daemon
Shutting down IpLir
hostname> The session has been forced to close.
...
hostname login:
```

machine self-test

Команда используется для запуска регламентного тестирования ViPNet xFirewall.

Синтаксис

```
machine self-test
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команду нельзя использовать при удаленном администрировании с помощью SSH.
- До начала тестирования работа всех демонов будет автоматически завершена, а после успешного окончания тестирования — автоматически восстановлена.
- В процессе регламентного тестирования производится проверка целостности модулей и файлов конфигурации, проверка файловых систем на первом и втором разделах загрузочного носителя, проверка контрольных сумм ядра и образа ПО и так далее.
- При успешной проверке на экран выводятся имена проверенных файлов и шестнадцатеричные значения их контрольных сумм.
- При обнаружении ошибок компьютер попытается восстановить искаженные файлы из резервных копий.
- Если резервная копия искаженного файла не найдена, ViPNet xFirewall загрузится, однако демоны, отвечающие за работу в сети ViPNet, не будут запущены. Если у вас есть файл экспорта справочников, лицензии и настроек с расширением `*.vbe`, попробуйте восстановить систему, импортировав этот файл. Если восстановить работу ViPNet xFirewall не удалось, обратитесь в службу поддержки ОАО «ИнфоТеКС».
- После успешной проверки в ViPNet xFirewall автоматически создается резервная копия конфигурационных и исполняемых файлов ПО, а также справочников и лицензии.

Пример использования

```
hostname# machine self-test
If you run selftest, then all daemons will be stopped.
Continue?[y/n]: y
>> Stop Daemons...
stopped /usr/sbin/crond (pid 6021)
Stopping Advanced Configuration and Power Interface daemon: acpid.
Shutting down IpLir
...
hostname#
```

machine set dailyreboot mode

Команда используется для включения или выключения ежедневной перезагрузки ViPNet xFirewall.

Синтаксис

```
machine set dailyreboot mode {on | off}
```

Параметры и ключевые слова

- `on` — включение ежедневной перезагрузки.
- `off` — выключение ежедневной перезагрузки.

Значения по умолчанию

По умолчанию ежедневная перезагрузка выключена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед перезагрузкой завершается работа всех демонов и драйверов ViPNet xFirewall.

Пример использования

Чтобы включить ежедневную перезагрузку, выполните команду:

```
hostname# machine set dailyreboot mode on
```

machine set cef loghost

Команда используется для задания сетевого узла для экспорта записей из журнала регистрации IP-пакетов в формате CEF (см. глоссарий, стр. 293). С помощью этой команды также можно выключить экспорт записей журнала регистрации IP-пакетов.

Синтаксис

```
machine set cef loghost {<доменное имя>| <IP-адрес> | none}
```

Параметры и ключевые слова

- `<доменное имя>` — доменное имя сетевого узла;
- `<IP-адрес>` — IP-адрес сетевого узла;
- `none` — выключение экспорта записей журнала регистрации IP-пакетов.

Значения по умолчанию

`none`

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить работу демона iplircfg (см. iplir stop на стр. 155).
- В качестве сетевого узла нельзя указывать локальный узел localhost, собственные адреса и алиасы интерфейсов.
- При работе в открытой сети необходимо создать разрешающее исходящее правило для протокола syslog на заданный сетевой узел:

  ```
  hostname# firewall local add src @local dst <IP-адрес> service @syslog pass
  ```

  В сети ViPNet разрешающее исходящее правило для протокола syslog создается автоматически.
- Экспорт записей из журнала регистрации IP-пакетов в формате CEF работает только на активном узле кластера или в одиночном режиме. Настройки синхронизируются в кластере.

Примеры использования

Для экспорта записей журнала регистрации IP-пакетов на сетевой узел с адресом `10.0.112.126`, выполните команду:

```
hostname# machine set cef loghost 10.0.112.126
Reloading system log daemon configuration files...done.
hostname#
```

Если вы хотите выключить экспорт записей журнала регистрации IP-пакетов, выполните команду:

```
hostname# machine set cef loghost none
hostname#
```

machine show cef loghost

Команда предназначена для просмотра IP-адреса текущего сетевого узла, на который выполняется экспорт записей журнала регистрации IP-пакетов в формате CEF (см. глоссарий, стр. 293).

Синтаксис

```
machine show cef loghost
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show cef loghost

The cef loghost set to `10.0.112.126`
hostname>
```

machine set dailyreboot time

Команда используется для задания времени ежедневной перезагрузки ViPNet xFirewall.

Синтаксис

```
machine set dailyreboot time <время>
```

Параметры и ключевые слова

`<время>` — время перезагрузки. Указывается в формате `hh:mm`, где `hh` — час (24-часовой формат), `mm` — минуты.

Значения по умолчанию

Время перезагрузки по умолчанию — `00:00`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- В режиме кластера необходимо устанавливать время перезагрузки на каждом узле, настройки не синхронизируются.
- Рекомендуется устанавливать разное время перезагрузки на узлах кластера с интервалом в 30 минут.

Пример использования

Чтобы настроить ежедневную перезагрузку в 6 часов утра, выполните команду:

```
hostname# machine set dailyreboot 06:00
```

machine set date

Команда используется для установки даты и времени.

Синтаксис

```
machine set date <дата> <время>
```

Параметры и ключевые слова

- `<дата>` — дата. Указывается в формате `YYYY-MM-DD`, где `YYYY` — год, `MM` — месяц, `DD` — день.
- `<время>` — время. Указывается в формате `hh:mm:ss`, где `hh` — час, `mm` — минуты, `ss` — секунды.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед установкой даты и времени требуется остановить демоны `iplircfg` (см. iplir stop на стр. 155), `failoverd` (см. failover stop на стр. 40) и `mftpd` (см. mftp stop на стр. 184), а после установки восстановить их работу с помощью соответствующих команд.

Пример использования

Чтобы установить дату 22 июля 2014 года и время, равное 12 часам, выполните команду:

```
hostname# machine set date 2014-07-22 12:00:00
```

machine set hostname

Команда используется для установки имени компьютера.

Синтаксис

```
machine set hostname <имя>
```

Параметры и ключевые слова

`<имя>` — имя компьютера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию имя компьютера сформировано по шаблону `<название>-<идентификатор>`, где `название` — наименование исполнения ViPNet xFirewall, `идентификатор` — идентификатор сетевого узла. Например: xF`1000-270E033A`.
- Имя компьютера используется в качестве приглашения командного интерпретатора, а также указывается в начале сообщений, записываемых в протоколы работы при их хранении на жестком диске.

Пример использования

Чтобы установить имя компьютера xF1000, выполните команду:

```
hostname# machine set hostname xF1000
```

machine set log invalid-packet

Команда используется для включения и отключения записи нарушений параметров таблицы соединений в журнал устранения неполадок.

Синтаксис

```
machine set log invalid-packet {on | off}
```

Параметры и ключевые слова

- `on` — нарушения параметров таблицы соединений записываются в журнал;
- `off` — нарушения параметров таблицы соединений не записываются в журнал.

Значения по умолчанию

`on`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для включения записи нарушений параметров таблицы соединений в журнал устранения неполадок выполните команду:

```
hostname# machine set log invalid-packet on

hostname#
```

machine set log queue

Команда используется для включения и отключения записи в журнал устранения неполадок событий о входящих IP-пакетах, обработка которых была отклонена в рамках приоритетной обработки трафика.

Синтаксис

```
machine set log queue {on | off}
```

Параметры и ключевые слова

- `on` — события об отклоненных IP-пакетах записываются в журнал;
- `off` — события об отклоненных IP-пакетах не записываются в журнал.

Значения по умолчанию

`on`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для включения записи в журнал устранения неполадок событий об отклоненных IP-пакетах выполните команду:

```
hostname# machine set log queue on

hostname#
```

machine set loghost

Команда используется для задания места хранения журнала событий. С помощью этой команды также можно выключить запись событий в журнал.

Синтаксис

```
machine set loghost {<IP-адрес> | local | null}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес удаленного сетевого узла, на который должен отправляться журнал событий (удаленное протоколирование).
- `local` — журнал событий хранится на самом ViPNet xFirewall (локальное протоколирование).
- `null` — выключение протоколирования.

Значения по умолчанию

По умолчанию во всех исполнениях ViPNet xFirewall включено локальное протоколирование (`local`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если протоколы работы будут направляться на удаленный сетевой узел, то этот узел должен быть доступен для ViPNet xFirewall. Если этот узел является открытым, то на ViPNet xFirewall должен быть создан 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 потеряна. Если все же необходимо настроить удаленное протоколирование на кластере, то параметры протоколирования должны быть заданы не только на активном, но и на пассивом

сервере кластера, так как данные настройки не передаются с активного сервера на пассивный в ходе резервирования.

Пример использования

Для отправки журнала событий на узел с адресом 192.168.10.10 выполните команду:

```
hostname# machine set loghost 192.168.10.10

hostname#
```

machine set session-timeout

Команда используется для установки допустимого времени неактивности сессии при удаленном подключении к ViPNet xFirewall по протоколу SSH.

Синтаксис

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

Параметры и ключевые слова

`<время>` — время неактивности в минутах. Допустимые значения: 0–65535.

Значения по умолчанию

По умолчанию время неактивности удаленной сессии 30 минут.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы установить допустимое время неактивности удаленной сессии 1 час, выполните команду:

```
hostname# machine set session-timeout 60
```

machine set timezone

Команда используется для установки временной зоны (часового пояса).

Синтаксис

```
machine set timezone <временная зона>
```

Параметры и ключевые слова

`<временная зона>` — временная зона, заданная в формате `Континент/Зона`, или значение `UTC` для установки времени UTC.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Название континента и зоны должны начинаться с прописной буквы.
- При вводе континента или зоны работает подсказка.
- Если временная зона не указана, выводится список всех существующих временных зон.

Примеры использования

Чтобы просмотреть список временных зон в Антарктике, выполните команду:

```
hostname# machine set timezone Antarc?
Antarctica/Casey
Antarctica/Davis
...
hostname# machine set timezone Antarc
```

Чтобы установить часовой пояс Москвы, выполните команду:

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

machine show dailyreboot

Команда предназначена для просмотра настройки ежедневной перезагрузки ViPNet xFirewall.

Синтаксис

```
machine show dailyreboot
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show dailyreboot
Daily reboot is on
Daily reboot at 6:00
hostname>
```

machine show date

Команда предназначена для просмотра текущих даты и времени.

Синтаксис

```
machine show date
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show date
Втр Июл 22 18:31:17 SAMT 2016
hostname>
```

machine show hostname

Команда предназначена для просмотра имени компьютера.

Синтаксис

```
machine show hostname
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show hostname
hostname
hostname>
```

machine show log invalid-packet

Команда используется для отображения статуса записи нарушений параметров таблицы соединений в журнал устранения неполадок (см. machine set log invalid-packet на стр. 164).

Синтаксис

```
machine show log invalid-packet
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show log invalid-packet
Invalid-packet option is ON
hostname>
```

machine show log queue

Команда используется для отображения статуса записи событий об отклоненных IP-пакетах в журнал устранения неполадок (см. machine set log queue на стр. 165).

Синтаксис

```
machine show log queue
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show log queue

Option is: ON

hostname>
```

machine show loghost

Команда предназначена для просмотра места хранения журнала событий.

Синтаксис

```
machine show loghost
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show loghost
The log host set to `local`
hostname>
```

По команде выводится одно из следующих значений:

- `null` — протоколирование выключено.
- `local` — журнал событий хранится локально на сетевом узле ViPNet xFirewall.
- IP-адрес удаленного сетевого узла, заданный с помощью команды `machine set loghost` (см. machine set loghost на стр. 166).

machine show logs

Команда предназначена для просмотра журнала событий.

Синтаксис

```
machine show logs [reversed] [since <время>] [filtered {<демон> | string <строка>}]
```

Параметры и ключевые слова

- `reversed` — вывод списка записей в обратном хронологическом порядке.
- `<время>` — вывод записей, начиная с указанного момента времени.
- `<демон>` — вывод записей только для указанного демона в составе ПО ViPNet xFirewall.
- `<строка>` — поиск записей журнала по части строки.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Для завершения просмотра используется клавиша **Q**.
- Параметр `<время>` задается в формате `YYYY-MM-DD hh:mm:ss`
- В параметре `<демон>` можно указать один из демонов в составе ПО ViPNet xFirewall. Полный список демонов см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», разделе «Список демонов в составе ViPNet xFirewall».
- Для параметра `<строка>` 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 ("").

- В одной команде `machine show logs` можно одновременно указать только один из параметров `since` или `filtered`. При указании параметра `filtered` можно указать только один из его вариантов `<демон>` или `string <строка>`.

Пример использования

Чтобы найти все записи журнала событий за все время для всех демонов, выполните команду:

```
hostname# machine show logs
```

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
```

Чтобы найти все записи журнала событий для демона `vmunix`, выполните команду:

```
hostname# machine show logs filtered vmunix
```

Чтобы найти записи журнала событий за все время его ведения, для всех демонов и где есть строка `command 3001`, выполните команду:

```
hostname# machine show logs filtered string "command 3001"
```

machine show memory

Команда предназначена для просмотра информации об использовании оперативной памяти, файла подкачки (см. глоссарий, стр. 301) и файловой системы.

Синтаксис

```
machine show memory
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show memory
       total    used    free    shared    buffers    cached
Mem:    2007     522    1485         0        102       362
-/+ buffers/cache:
Swap:      0       0       0

Filesystem    Size  Used  Avail  Use%  Mounted on
rootfs       1004M  3,3M  1001M    1%  /
tmpfs        1004M   60M   944M    6%  /mnt/root
...
hostname>
```

machine show session-timeout

Команда предназначена для просмотра текущего допустимого времени неактивности сессии.

Синтаксис

```
machine show session-timeout
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show session-timeout
shell session timeout:  30 minute(s)
hostname>
```

machine show timezone

Команда предназначена для просмотра текущей временной зоны (часового пояса).

Синтаксис

```
machine show timezone
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show timezone
Europe/Samara
hostname>
```

machine show uptime

Команда предназначена для просмотра времени работы ViPNet xFirewall после загрузки, а также среднего числа процессов в очереди за ближайшее время.

Синтаксис

```
machine show uptime
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> machine show uptime
 18:04:29 up 44 min, 1 user, load average: 2.19, 2.18, 2.06
hostname>
```

По команде отображается следующая информация:

- текущее время;
- время работы ViPNet xFirewall после загрузки;
- текущее число пользователей;
- среднее число процессов в очереди за последние 1, 5 и 15 минут. Выводимые значения следует интерпретировать в зависимости от количества процессорных ядер исполнения ViPNet xFirewall. Для исполнений с многоядерными процессорами (в том числе с двумя процессорами) критическими являются значения, превышающие общее количество ядер. Например, для исполнений с 4-мя процессорными ядрами значения не должны превышать 4.00 — такие значения говорят о том, что ViPNet xFirewall перегружен.

Внимание! Для исполнений с одноядерными процессорами не стоит ориентироваться на эти значения, так как количество запущенных процессов на ViPNet xFirewall многократно больше 1. Вместо этого используйте значение `total cpu` в выводе команды failover show info.

machine swap mode

Команда предназначена для включения или выключения использования файла подкачки (см. глоссарий, стр. 301).

Синтаксис

```
machine swap mode {on | off}
```

Параметры и ключевые слова

`on` — включает использование файла подкачки.

`off` — выключает использование файла подкачки.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Невозможно включить использование файла подкачки, если не был задан его размер с помощью команды machine swap set (на стр. 178).
- После выключения использования файл подкачки удаляется.

Пример использования

```
hostname# machine swap mode on
SWAP is enabled and will be enabled after reboot.
hostname#
```

machine swap set

Команда предназначена для задания размера файла подкачки (см. глоссарий, стр. 301), если такой будет использоваться в процессе работы ViPNet xFirewall.

Синтаксис

```
machine swap set <size>
```

Параметры и ключевые слова

`<size>` — размер файла подкачки в мегабайтах.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При задании размера файла подкачки на диске должно остаться не менее 256 Мбайт свободного пространства. Если будет задан размер файла подкачки, превышающий размер доступного пространства на диске, появится соответствующее сообщение.
- Просмотреть сведения об использовании оперативной памяти и файле подкачки можно с помощью команды machine show memory (на стр. 174).

Пример использования

```
hostname# machine swap set 2048

Creating swap. Please, wait...Setting up swapspace version 1, size 2097148 KiB

no label, UUID=of389079-f9f5-4abb-ac2e-a26848eca54c

 done.

Activating swap...

 done.

hostname#
```

Команды группы mftp

Команды группы `mftp` предназначены для настройки параметров транспортного модуля MFTP (см. глоссарий, стр. 301) и каналов обмена ViPNet xFirewall с другими узлами сети ViPNet.

mftp config

Команда используется для редактирования конфигурационного файла демона mftpd.

Синтаксис

```
mftp config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе команды работают автозаполнение и подсказка, данные для подсказки берутся из списка команд ViPNet xFirewall.
- Перед редактированием конфигурационного файла требуется завершить работу демона `mftpd` (см. mftp stop на стр. 184). Перед выполнением команды проверяется, завершена ли работа демона mftpd. Если демон запущен, то выдается ошибка.
- При выполнении команды запускается текстовый редактор, и в него загружается файл `mftp.conf`.
- При сохранении файла происходит проверка его корректности, и в случае ошибки предлагается отказаться от изменений или продолжить редактирование. Если проверка прошла успешно, файл применяется для работы демона mftpd, а информации об изменении конфигурации сохраняется в журнал событий.

Пример использования

Чтобы включить режим немедленной передачи конвертов по каналу обмена с узлом 0x270e000a, выполните команду:

```
hostname# mftp config
```

В открывшемся файле в секции `[channel]` для узла 0x270e000a присвойте параметру `call_flag` значение `yes`:

```
[channel]
id = 0x270e000a
name = Client-1
off_flag = no
call_flag = yes
type = MFTP
...
```

mftp info

Команда предназначена для просмотра очереди исходящих транспортных конвертов.

Синтаксис

```
mftp info
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды на ViPNet xFirewall xF100 в консоль выводится не более 10000 записей о конвертах. При выполнении команды на остальных исполнениях ViPNet xFirewall число выводимых записей о конвертах ограничено временем ожидания ответа (30 секунд), но не превышает 400000 записей.
- Для просмотра очереди исходящих конвертов используйте навигационные клавиши.
- Для завершения просмотра используйте клавишу **Q**.

Пример использования

```
hostname# mftp info
Name   Size   Type   Date         Time       Sender Id    Sender Name
@M1~   1390   Mail   15-10-2016   10:40:05   0x1639001b   Client-11
0x1639001a    Client-10
@M2~   3639   Mail   15-10-2016   10:42:50   0x1639001b   Client-11
0x1639001c    Client-12
...
hostname#
```

Очередь исходящих конвертов отображается в следующем формате:

```
Name  Size  Type  Date  Time  Sender ID  Sender Name

Receiver ID  Receiver Name
```

где:

- `Name` — имя конверта.
- `Size` — размер конверта в килобайтах.
- `Type` — тип конверта:
  - `Mail` — прикладной конверт (см. глоссарий, стр. 299);
  - `Control request` — управляющий запрос;
  - `Control request answer` — ответ на управляющий запрос;
  - `Task receipt` — прикладная квитанция (см. глоссарий, стр. 299);
  - `Transport receipt` — транспортная квитанция (см. глоссарий, стр. 301).
- `Date`, `Time` — дата и время создания конверта (первого его появления в очереди).
- `Sender ID` — идентификатор узла-отправителя конверта.
- `Sender Name` — имя узла-отправителя конверта.
- `Receiver ID` — идентификатор узла-получателя конверта.
- `Receiver Name` — имя узла-получателя конверта.

В случае отсутствия конвертов в очереди выводится сообщение `queue is empty`.

mftp show config

Команда предназначена для просмотра файла конфигурации транспортного модуля.

Синтаксис

```
mftp show config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Для завершения просмотра файла конфигурации используется клавиша **Q**.

Пример использования

```
hostname> mftp show config
[channel]
id = 0x15ea0011
name = Client-1
off_flag = no
call_flag = no
type = MFTP
...
hostname>
```

mftp start

Команда используется для запуска транспортного модуля MFTP.

Синтаксис

```
mftp start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# mftp start
Loading MFTP daemon
No mftp running. Starting it
Daemonizing...
hostname#
```

mftp stop

Команда используется для завершения работы транспортного модуля MFTP.

Синтаксис

```
mftp stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# mftp stop
Shutting down MFTP daemon
```

```
hostname#
```

mftp view

Команда используется для просмотра журнала конвертов транспортного модуля MFTP.

Синтаксис

```
mftp view
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если вы выполняете команду на одном из серверов кластера горячего резервирования, отображается только информация о конвертах транспортного модуля, обработанных за периоды, когда этот сервер был активным.

Пример использования

```
hostname# mftp view
Name  Sender Id  Sender Name  Receiver ID  Receiver Name  Date         Time ...
@M1~  0x1639001b Client-11    0x1639001a   Client-10      15-10-2016   10:40:05 ...
@M2~  0x1639001b Client-11    0x1639001c   Client-12      15-10-2016   10:42:50 ...
...
hostname#
```

Журнал отображается в следующем формате:

- `Name` — имя конверта.
- `Sender ID` — идентификатор узла-отправителя конверта.
- `Sender Name` — имя узла-отправителя конверта.
- `Receiver ID` — идентификатор узла-получателя конверта.
- `Receiver Name` — имя узла-получателя конверта.

- `Date`, `Time` — дата и время события.
- `Event` — событие. Событие может иметь следующие значения:
  - `Received` — конверт получен;
  - `Sent` — конверт отправлен;
  - `Deleted` — конверт удален;
- `Size` — размер конверта в килобайтах.
- `Task` — прикладная задача, в которой создан конверт.

Команды группы service

Команды группы `service` предназначены для управления сертификатами, прокси-сервером и пользователями.

service cert delete cert

Команда используется для удаления сертификата с заданным именем.

Синтаксис

```
service cert delete cert <сертификат>
```

Параметры и ключевые слова

`<сертификат>` — имя файла сертификата.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

После удаления сертификата веб-сервера Captive portal необходимо сбросить настройки Captive portal (см. service user-control cp reset на стр. 232) в том случае, если вы не будете устанавливать другой сертификат веб-сервера Captive portal.

Пример использования

Чтобы удалить сертификат с именем Cert1.pem, выполните команду:

```
hostname# service cert delete cert Cert1.pem
Certificate Cert1.pem is deleted
hostname#
```

service cert delete crl

Команда используется для удаления списка аннулированных сертификатов (CRL) с заданным именем.

Синтаксис

```
service cert delete crl <CRL>
```

Параметры и ключевые слова

`<CRL>` — имя файла списка аннулированных сертификатов.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы удалить CRL с именем CRL1.pem, выполните команду:

```
hostname# service cert delete crl CRL1.pem
CRL CRL1.pem is deleted
hostname#
```

service cert delete private

Команда используется для удаления файла с закрытым ключом с заданным именем.

Синтаксис

```
service cert delete private <ключ>
```

Параметры и ключевые слова

`<ключ>` — имя файла закрытого ключа.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы удалить закрытый ключ с именем файла Cert1_key.pem, выполните команду:

```
hostname# service cert delete private Cert1_key.pem
Private key Cert1_key.pem is deleted
hostname#
```

service cert import

Команда используется для импорта в локальное хранилище ViPNet xFirewall сертификатов и списков аннулированных сертификатов (CRL) (см. глоссарий, стр. 301) с USB-накопителя.

Синтаксис

```
service cert import
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Поддерживает импорт только сертификатов, подписанных с использованием алгоритма RSA.
- Поддерживает импорт сертификатов в кодировке DER и Base64.

- По команде выполняется поиск на USB-накопителе файлов с расширениями `*.pem`, `*.cer` и `*.crl` и предлагается выбрать нужный сертификат или CRL.
- При импорте сертификата с расширением `*.cer` выполняется его конвертация в формат PEM.

Пример использования

```
hostname# service cert import
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#
```

service cert list

Команда используется для просмотра установленных закрытых ключей, сертификатов и списков аннулированных сертификатов (CRL) (см. глоссарий, стр. 301).

Синтаксис

```
service cert list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> service cert list

Certificates:

...

Certificate revocation list:


Private keys:

...

hostname>
```

service cert request create

Команда используется для создания закрытого ключа и запроса на сертификат в формате PKCS#12.

Синтаксис

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

Параметры и ключевые слова

- `<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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- В процессе выполнения команды у вас будут запрошены личные данные, необходимые для создания сертификата. Не все поля обязательны к заполнению. Чтобы отказаться от заполнения тех или иных сведений, нажмите клавишу **Enter**.
- По команде создается файл запроса на сертификат с именем `<имя сертификата>_req.pem` и файл с закрытым ключом с именем `<имя сертификата>_key.pem`.

Пример использования

Чтобы создать запрос на сертификат с длиной ключа 1024 бита, используя алгоритм шифрования MD5, выполните команду:

```
hostname# service cert request create name Cert1 bits 1024 digest md5
Generating a 1024 bit RSA private key
    ++++
writing new private key to '/etc/cert/Cert1_key.pem'
----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value
If you enter '.', the field will be left blank.
----
Country name (2 letter code) [AU]:RU
State or province Name (full name) [Some-State]:
...
Creating request Cert1_req.pem is completed
hostname#
```

service cert request delete

Команда используется для удаления запроса на сертификат с заданным именем.

Синтаксис

```
service cert request delete <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы удалить запрос на сертификат с именем Cert1_req.pem, выполните команду:

```
hostname# service cert request delete Cert1_req.pem
Certificate request Cert1_req.pem is deleted
hostname#
```

service cert request export

Команда используется для экспорта запроса на сертификат на USB-накопитель.

Синтаксис

```
service cert request export <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы экспортировать запрос на сертификат с именем Cert1_req.pem, выполните команду:

```
hostname# service cert request export Cert1_req.pem
Insert USB flash drive into empty USB slot and press <Enter>
Try to mount /dev/sdc1 as vfat
/dev/sdc1 mounted
Cert1_req.pem was exported
hostname#
```

service cert request list

Команда используется для просмотра списка созданных запросов на сертификаты.

Синтаксис

```
service cert request list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

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

```
hostname>
```

service cert request show

Команда используется для просмотра содержимого запроса на сертификат с заданным именем или всех запросов на сертификаты, созданных в ViPNet xFirewall.

Синтаксис

```
service cert request show <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат. Если вместо имени запроса на сертификат указать `all`, то будет отображено содержимое всех запросов на сертификаты, созданных вViPNet xFirewall.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

Чтобы просмотреть содержимое файла запроса на сертификат с именем Cert1_req.pem, выполните команду:

```
hostname> service cert request show Cert1_req.pem
----BEGIN CERTIFICATE REQUEST----
...
----END CERTIFICATE REQUEST----
hostname>
```

service cert show cert

Команда используется для просмотра содержимого сертификата с заданным именем или всех сертификатов, установленных в локальное хранилище ViPNet xFirewall.

Синтаксис

```
service cert show cert <сертификат>
```

Параметры и ключевые слова

`<сертификат>` — имя файла сертификата. Если вместо имени сертификата указать `all`, то будет отображено содержимое всех сертификатов, установленных в локальное хранилище ViPNet xFirewall.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

Чтобы просмотреть содержимое сертификата с именем Cert1.pem, выполните 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>
```

service cert show crl

Команда используется для просмотра содержимого списка аннулированных сертификатов (CRL) с заданным именем или всех списков аннулированных сертификатов, установленных в локальное хранилище ViPNet xFirewall.

Синтаксис

```
service cert show crl <CRL>
```

Параметры и ключевые слова

`<CRL>` — имя файла списка аннулированных сертификатов CRL). Если вместо имени CRL указать `all`, то будет отображено содержимое всех списков аннулированных сертификатов, установленных в локальное хранилище ViPNet xFirewall.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

Чтобы просмотреть содержимое списка аннулированных сертификатов с именем CRL.pem, выполните команду:

```
hostname> service cert show cert CRL.pem
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
...
hostname>
```

service http-proxy antivirus external bypass

Команда предназначена для включения и выключения блокировки трафика, проходящего через прокси-сервер при недоступности ICAP-сервера (см. глоссарий, стр. 294) внешнего антивируса.

Синтаксис

```
hostname# service http-proxy antivirus external bypass {on | off}
```

Параметры и ключевые слова

- `on` — при недоступности ICAP-сервера внешнего антивируса прокси-сервер разрешает проходящий через него трафик.
- `off` — при недоступности ICAP-сервера внешнего антивируса прокси-сервер блокирует проходящий через него трафик.

Значения по умолчанию

`on`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо:
  - выключить антивирусную проверку `service http-proxy antivirus mode off` (см. service http-proxy antivirus mode на стр. 204);
  - остановить прокси-сервер service http-proxy stop (на стр. 226).
- В режиме кластера команда работает только на активном узле.

Пример использования

```
hostname# service http-proxy antivirus bypass on
HTTP proxy antivirus set bypass option: on
hostname#
```

service http-proxy antivirus external server-url add

Команда предназначена для задания адреса и метода подключения к ICAP-серверу (см. глоссарий, стр. 294) внешнего антивируса.

Синтаксис

```
hostname# service http-proxy antivirus external server-url add {reqmod | respmod}
<URL>
```

Параметры и ключевые слова

- `reqmod` — проверяется исходящий трафик (запросы от пользователей сети к прокси-серверу);
- `respmod` — проверяется входящий трафик (ответы прокси-сервера на запросы пользователей).
- `<URL>` — адрес ICAP-сервера антивируса в формате `icap://адрес[:порт]/[путь]`

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить прокси-сервер server http-proxy stop (см. service http-proxy stop на стр. 226).
- В режиме кластера команда работает только на активном узле.
- В конце адреса ICAP-сервера необходимо указать символ «/».
- Если в адресе ICAP-сервера не указан порт, будет использоваться порт по умолчанию 1344.

Пример использования

```
hostname# service http-proxy antivirus external server-url add respmod
icap://192.168.1.45/
HTTP proxy antivirus add respmod service success
hostname#
```

service http-proxy antivirus external server-url delete

Команда предназначена для удаления параметров подключения к ICAP-серверу внешнего антивируса.

Синтаксис

```
hostname# service http-proxy antivirus external server-url delete {reqmod | respmod}
```

Параметры и ключевые слова

- `reqmod` — будет удален адрес доступа к ICAP-серверу для проверки исходящего трафика (запросы от пользователей сети к прокси-серверу);
- `respmod` — будет удален адрес доступа к ICAP-серверу для проверки входящего трафика (ответы прокси-сервера на запросы пользователей).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо:
  - выключить антивирусную проверку `service http-proxy antivirus mode off` (см. service http-proxy antivirus mode на стр. 204);
  - остановить прокси-сервер service http-proxy stop (на стр. 226).
- В режиме кластера команда работает только на активном узле.

Пример использования

```
hostname# service http-proxy antivirus external server-url delete respmod
HTTP proxy antivirus delete respmod service success
hostname#
```

service http-proxy antivirus internal key

Команда предназначена для управления лицензионными ключами встроенного антивируса KAV4Proxy.

Синтаксис

```
hostname# service http-proxy antivirus internal key {install | show | delete}
```

Параметры и ключевые слова

- `install` — установка лицензионного ключа антивируса KAV4Proxy;
- `show` — вывод информации об установленной лицензии антивируса KAV4Proxy;
- `delete` — удаления лицензионного ключа антивируса KAV4Proxy.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо:
  - выключить антивирусную проверку `service http-proxy antivirus mode off` (см. service http-proxy antivirus mode на стр. 204);
  - остановить прокси-сервер service http-proxy stop (на стр. 226).
- В режиме кластера команда работает только на активном узле.

Примеры использования

Установка лицензионного ключа:

```
hostname# service http-proxy antivirus internal key install
Insert USB flash drive into empty USB slot and press <Enter>
Try to mount /dev/sdc1 as vfat
/dev/sdc1 mounted
Select file to use for antivirus license install:
0 - 5720059C.key
Enter file number [0-0] or [q] to cancel: 0
Kaspersky license manager for Linux. Version 5.5.85/RELEASE #59
(C) 1997-2012 Kaspersky Lab ZAO. All Rights Reserved.
Registered trademarks and service marks are the property of their respective owners.
Key file /usb/5720059C.key has been successfully registered
hostname#
```

Просмотр параметров лицензионного ключа:

```
hostname# service http-proxy antivirus internal key show
Kaspersky license manager for Linux. Version 5.5.85/RELEASE #59
(C) 1997-2012 Kaspersky Lab ZAO. All Rights Reserved.
Registered trademarks and service marks are the property of their respective owners.


License info:
```

```
Product name: Kaspersky Security for Internet Gateway International Edition. 50-99
User 1 month Trial License: Kaspersky Anti-Virus Suite for Gateway

Expiration date: 17-12-2016 UTC, expires in 29 days


Active key info:

Key file: 50CC9FEB.key

Install date: 17-11-2016 UTC

Product name: Kaspersky Security for Internet Gateway International Edition. 50-99
User 1 month Trial License: Kaspersky Anti-Virus Suite for Gateway

Creation date: 28-10-2016 UTC

Expiration date: 27-12-2016 UTC

Serial: 13CE-0004C6-50CC9FEB

Type: Trial

Count: 50

Lifespan: 30

Objs: 1:50

hostname#
```

Удаление лицензионного ключа:

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

Kaspersky license manager for Linux. Version 5.5.85/RELEASE #59

(C) 1997-2012 Kaspersky Lab ZAO. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

License key was successfully removed

hostname#
```

service http-proxy antivirus internal fetch

Команда предназначена для принудительного обновления базы данных встроенного антивируса KAV4Proxy.

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо:
  - включить антивирусную проверку `service http-proxy antivirus mode on` (см. service http-proxy mode на стр. 223);
  - запустить прокси-сервер `service http-proxy start` (на стр. 225);
  - создать разрешающие правила service http-proxy fw-rules apply (на стр. 218).
- В режиме кластера команда работает только на активном узле.
- При выполнении команды проверяется наличие лицензионного ключа.

Пример использования

```
hostname# service http-proxy antivirus internal fetch
Database update was started in the background
hostname#
```

service http-proxy antivirus internal schedule-fetch

Команда используется для настройки автоматического обновления базы данных встроенного антивируса KAV4Proxy.

Синтаксис

```
hostname# service http-proxy antivirus internal schedule-fetch {1 | 2 | 3 | 4 | 5 |
none}
```

Параметры и ключевые слова

- `1, 2, 3, 4, 5` — количество обновлений за сутки;
- `none` — отключить автоматическое обновление.

Значения по умолчанию

`none`

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо:
  - выключить антивирусную проверку `service http-proxy antivirus mode off` (см. service http-proxy antivirus mode на стр. 204);
  - остановить прокси-сервер service http-proxy stop (на стр. 226).
- В режиме кластера команда работает только на активном узле.
- При выполнении команды проверяется наличие лицензионного ключа.

Пример использования

```
hostname# service http-proxy antivirus internal schedule-fetch 5
hostname#
```

service http-proxy antivirus mode

Команда предназначена для включения или выключения антивирусной проверки трафика, проходящего через прокси-сервер.

Синтаксис

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

Параметры и ключевые слова

- `on` — антивирусная проверка трафика включена.
- `off` — антивирусная проверка трафика выключена.

Значения по умолчанию

`off`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо:
  - выключить антивирусную проверку `service http-proxy antivirus mode off` (см. service http-proxy antivirus mode на стр. 204);

    - остановить прокси-сервер service http-proxy stop (на стр. 226).
- В режиме кластера команда работает только на активном узле.
- Режим антивирусной проверки трафика предварительно задается командой service http-proxy antivirus select (на стр. 205).
- Для режима internal проверяется наличие лицензионного ключа и настроенного расписания.
- Для режима external проверяется настроенные URL для ICAP-сервера (см. глоссарий, стр. 294) (URL, порт, метод).

Пример использования

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

hostname#
```

service http-proxy antivirus select

Команда предназначена для выбора режима антивирусной проверки трафика:

- встроенный антивирус KAV4Proxy;
- внешний антивирус, доступный по протоколу ICAP (см. глоссарий, стр. 294).

Синтаксис

```
hostname# service http-proxy antivirus select {internal | external}
```

Параметры и ключевые слова

- `internal` — антивирусная проверка трафика выполняется встроенным антивирусом.
- `external` — антивирусная проверка трафика выполняется внешним антивирусом.

Значения по умолчанию

```
internal
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо:
    - выключить антивирусную проверку `service http-proxy antivirus mode off` (см. service http-proxy antivirus mode на стр. 204);
    - остановить прокси-сервер service http-proxy stop (на стр. 226).

- В режиме кластера команда работает только на активном узле.
- Значение выбранного режима синхронизируется в конфигурационном файле кластера.

Примеры использования

Выбор внешнего антивируса:

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

You have chosen the external antivirus for traffic processing.

Before starting the proxy server, make sure that external ICAP server addresses are
specified.

hostname#
```

Выбор встроенного антивируса:

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

You have chosen the internal antivirus for traffic processing.

Before starting the proxy server, make sure that keys for KAV4proxy antivirus are
installed and database update schedule is configured.

hostname#
```

service http-proxy antivirus show-status

Команда предназначена для просмотра текущих настроек и состояния антивирусной защиты.

Синтаксис

```
hostname> service http-proxy antivirus show-status
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- В режиме кластера команда выполняется на обоих узлах.

Пример использования

```
hostname> service http-proxy antivirus show-status
HTTP-proxy antivirus client service is stopped.
Antivirus mode is disabled.
Antivirus service is set to external.

Internal antivirus settings
---------------------------
Version: KAV4Proxy 5.5.86/RELEASE build #80, compiled Jun 19 2012, 20:15:45
Service: stopped
Key: installed
Database: None
Database updates per day: 5

External antivirus settings
---------------------------
Bypass is on
Reqmod server-url: unspecified
Respmod server-url: icap://192.168.1.45:1344/ is n/a
hostname>
```

service http-proxy cache

Команда используется для задания размера кэша прокси-сервера.

Синтаксис

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

Параметры и ключевые слова

`<размер>` — размер кэша в мегабайтах.

Значения по умолчанию

По умолчанию размер кэша 256 Мбайт.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Кэш используется для хранения копии данных, к которым часто обращаются пользователи.
- Перед выполнением команды необходимо завершить работу прокси-сервера (см. service http-proxy stop на стр. 226).

- Невозможно задать размер кэша, превышающий 80% от объема свободного места на диске.

Пример использования

Чтобы задать размер кэша 512 мегабайт, выполните команду:

```
hostname# service http-proxy cache 512
```

service http-proxy content-filter change num

Команда используется для редактирования существующего правила фильтрации трафика, передаваемого через прокси-сервер.

Синтаксис

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

Параметры и ключевые слова

- `<номер правила>` — номер редактируемого правила фильтрации трафика в таблице;
- `<имя правила>` — имя редактируемого правила фильтрации трафика;
- `<адрес отправителя>` — адрес отправителя IP-пакетов;
- `<адрес отправителя>` — адрес получателя IP-пакетов;
- `<HTTP-метод>` — метод протокола HTTP;
- `<тип содержимого>` — MIME-тип (см. глоссарий, стр. 294) содержимого трафика;
- `<действие>` — действие с HTTP-трафиком, соответствующим условиям правила фильтрации содержимого трафика. Действие задается одной из следующих лексем:
  - `pass` — пропускать HTTP-трафик;
  - `drop` — блокировать HTTP-трафик.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить прокси-сервер (см. service http-proxy stop на стр. 226).
- В качестве адреса отправителя необходимо задать адрес клиента прокси-сервера, в качестве получателя — адрес удаленного HTTP-сервера.
- Если номер не указан, правило добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика (см. глоссарий, стр. 294) в последнюю очередь.
- 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.
- Если указанный номер правила больше последнего номера в таблице, то правило будет добавлено с номером на 1 больше последнего номера в таблице. Например: последний номер правила в таблице — 5, вы добавили правило с номером 8. В этом случае правило добавится с номером 6.
- Если имя правила не задано, будет создано правило без имени.
- В качестве адреса отправителя можно задать IP-адрес узла, маску адресов подсети, системную группу объектов `any`.
- В качестве адреса получателя можно задать IP-адрес или доменное имя узла, системную группу объектов `any`.

  Контентный фильтр прокси-сервера работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса назначения доменного имени узла фильтрация будет осуществляться только по доменному имени, а при использовании IP-адреса узла, только по IP-адресу, без взаимного разрешения доменное имя — IP-адрес.
- Можно задать только один из параметров: `<HTTP-метод>` или `<тип содержимого>`. При указании HTTP-метода нельзя указать тип содержимого, и наоборот.
- При неверном указании значения параметра `<тип содержимого>` выводится полный список поддерживаемых значений.
- Для блокировки веб-сайта задайте HTTP-метод GET.

Пример использования

Предположим, в таблице существует правило без имени с номером 15, которое полностью блокирует доступ к сайту yandex.ru для всех пользователей сети. Вы можете изменить имя блокируемого ресурса, например на google.ru, выполнив команду:

```
hostname# service http-proxy content-filter change num 15 @any dst google.ru command
get drop
```

service http-proxy content-filter add

Команда используется для добавления правила фильтрации содержимого трафика, передаваемого через прокси-сервер.

Синтаксис

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

Параметры и ключевые слова

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет.
- `<имя>` — имя правила.
- `<адрес отправителя>` — адрес отправителя IP-пакетов.
- `<адрес получателя>` — адрес получателя IP-пакетов.
- `<HTTP-метод>` — метод протокола HTTP.
- `<тип содержимого>` — MIME-тип (см. глоссарий, стр. 294) содержимого трафика.
- `<действие>` — действие с HTTP-трафиком, соответствующим условиям правила фильтрации содержимого трафика. Действие задается одной из следующих лексем:
  - `pass` — пропускать HTTP-трафик;
  - `drop` — блокировать HTTP-трафик.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить прокси-сервер (см. service http-proxy stop на стр. 226).
- В качестве адреса отправителя необходимо задать адрес клиента прокси-сервера, в качестве получателя — адрес удаленного HTTP-сервера.
- Если номер не указан, правило добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика (см. глоссарий, стр. 294) в последнюю очередь.
- 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.

- Если указанный номер правила больше последнего номера в таблице, то правило будет добавлено с номером на 1 больше последнего номера в таблице. Например: последний номер правила в таблице — 5, вы добавили правило с номером 8. В этом случае правило добавится с номером 6.
- Если имя правила не задано, будет создано правило без имени.
- В качестве адреса отправителя можно задать IP-адрес узла, маску адресов подсети, системную группу объектов `any`.
- В качестве адреса получателя можно IP-адрес или доменное имя узла, системную группу объектов `any`.

  Контентный фильтр прокси-сервера работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса назначения доменного имени узла фильтрация будет осуществляться только по доменному имени, а при использовании IP-адреса узла — только по IP-адресу (без взаимного разрешения доменное имя — IP-адрес).
- Можно задать только один из параметров: `<HTTP-метод>` или `<тип содержимого>`. При указании HTTP-метода нельзя указать тип содержимого, и наоборот.
- При неверном указании значения параметра `<тип содержимого>` выводится полный список поддерживаемых значений.
- Для блокировки веб-сайта задайте HTTP-метод GET.

Пример использования

Чтобы заблокировать просмотр видео на сайте youtube.com для сети 192.168.1.1/24, выполните команду:

```
hostname# service http-proxy content-filter add rule deny_youtube src 192.168.1.1/24
dst youtube.com mime-type video/mp4 drop
```

Чтобы заблокировать использование поисковой формы на сайте yandex.ru для всех пользователей, выполните команду:

```
hostname# service http-proxy content-filter add rule deny_post_yandex src @any dst
yandex.ru command post drop
```

Чтобы полностью заблокировать доступ к сайту yandex.ru, выполните команду:

```
hostname# service http-proxy content-filter add rule deny_yandex src @any dst
yandex.ru command get drop
```

service http-proxy content-filter delete

Команда используется для удаления правила фильтрации содержимого трафика, передаваемого через прокси-сервер.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить прокси-сервер (см. service http-proxy stop на стр. 226).
- Для имени правила работает автодополнение.

Пример использования

Чтобы удалить правило с именем `deny_youtube`, выполните команду:

```
hostname# service http-proxy content-filter delete rule deny_youtube
```

Чтобы удалить правило с порядковым номером 5, выполните команду:

```
hostname# service http-proxy content-filter delete rule 5
```

service http-proxy content-filter list

Команда используется для вывода списка правил фильтрации содержимого трафика, передаваемого через прокси-сервер.

Синтаксис

```
service http-proxy content-filter list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> service http-proxy content-filter list

Content filter rules

============================

       num           1

       act           drop

       name          rule1

       src           @any

       dst           @any

       mime-type     image/jpeg


       num           2

       act           drop

       name          rule2

       src           @any

       dst           @any

       mime-type     image/png

hostname>
```

service http-proxy content-filter mode

Команда используется для включения или выключения фильтрации содержимого трафика, передаваемого через прокси-сервер.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение фильтрации содержимого.
- `off` — выключение фильтрации содержимого.

Значения по умолчанию

По умолчанию фильтрация содержимого выключена (`on`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить прокси-сервер (см. service http-proxy stop на стр. 226).
- Фильтрация содержимого трафика работает при запущенном прокси-сервере (см. service http-proxy start на стр. 225).

Пример использования

Чтобы включить фильтрацию содержимого трафика, выполните команду:

```
hostname# service http-proxy content-filter mode on
```

service http-proxy content-filter move

Команда используется для назначения нового порядкового номера правилу контроля фильтрации трафика, передаваемого через прокси-сервер.

Синтаксис

```
service http-proxy content-filter move rule {<текущий номер> | <имя>} to <новый номер>
```

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить прокси-сервер (см. service http-proxy stop на стр. 226).
- Для имени правила работает автодополнение.

Пример использования

Чтобы назначить новый порядковый номер правилу с именем `deny_youtube`, выполните команду:

```
hostname# service http-proxy content-filter move rule deny_youtube to 7
```

Чтобы назначить новый порядковый номер правилу с порядковым номером 5, выполните команду:

```
hostname# service http-proxy content-filter move rule 5 to 7
```

service http-proxy content-filter show-status

Команда используется для вывода информации о статусе фильтрации содержимого трафика, передаваемого через прокси-сервер.

Синтаксис

```
service http-proxy content-filter show-status
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> service http-proxy content-filter show-status
HTTP-proxy content-filter is enabled with 4 rules
HTTP-proxy content-filter default-action is pass
HTTP-proxy service is stopped
hostname>
```

service http-proxy external-address set

Команда используется для задания внешнего IP-адреса прокси-сервера.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса, подключенного к Интернету.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу прокси-сервера (см. service http-proxy stop на стр. 226).
- При вводе интерфейса работает подсказка, данные для подсказки берутся из списка интерфейсов в системе (включая виртуальные интерфейсы, созданные при назначении дополнительных IP-адресов основным интерфейсам).
- На указанном интерфейсе должен быть задан IP-адрес.

Пример использования

Чтобы задать IP-адрес интерфейса eth1 в качестве внешнего адреса прокси-сервера, выполните команду:

```
hostname# service http-proxy external-address set eth1
```

service http-proxy external-address show

Команда предназначена для просмотра внешнего IP-адреса прокси-сервера.

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> service http-proxy external-address show
External address: 10.0.14.110 (eth0)
hostname>
```

service http-proxy fw-rules apply

Команда используется для автоматического создания сетевых фильтров и правил трансляции адресов, соответствующих текущим настройкам прокси-сервера.

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Невозможно создать сетевые фильтры и правила трансляции, если заданы не все параметры прокси-сервера.
- Автоматически созданные фильтры и правила трансляции добавляются в конец соответствующих таблиц и имеют зарезервированное название HTTP-Proxy auto.
- Редактировать созданные сетевые фильтры и правила трансляции не рекомендуется.
- Предыдущие сетевые фильтры и правила трансляции, соответствующие измененным настройкам прокси-сервера, будут удалены.

Пример использования

Чтобы после настройки прокси-сервера создать необходимые сетевые фильтры и правила трансляции, выполните команду:

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

service http-proxy fw-rules delete

Команда используется для удаления сетевых фильтров и правил трансляции адресов, необходимых для работы прокси-сервера.

Синтаксис

```
service http-proxy fw-rules delete
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

По команде из соответствующих таблиц будут удалены сетевые фильтры и правила трансляции с названием HTTP-Proxy auto, автоматически созданные с помощью команды service http-proxy fw-rules apply (на стр. 218).

Пример использования

Чтобы удалить имеющиеся сетевые фильтры и правила трансляции, автоматически созданные для работы прокси-сервера, выполните команду:

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

service http-proxy fw-rules show

Команда предназначена для просмотра существующих сетевых фильтров и правил трансляции адресов, необходимых для работы прокси-сервера.

Синтаксис

```
service http-proxy fw-rules show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> service http-proxy fw-rules show
Local:
empty rule for  Service:
================================================================================
Num   Name                                      Option  Schedule
Act   Protocol              Source              ->Destination
      DpiProtocol           DpiApp                DomainUser
================================================================================
7     HTTP-Proxy auto                           User
pass  tcp: to 1024          @HttpProxyUsers     ->192.168.203.174
      @any                  @any                  @any
--------------------------------------------------------------------------------
8     HTTP-Proxy auto                           User
pass  tcp: to 80, tcp: to 21 192.168.203.174    ->@InternetIP
      @any                  @any                  @any
--------------------------------------------------------------------------------
...
any_word_2>
```

service http-proxy listen-address add

Команда используется для добавления интерфейса и порта, через которые будут приниматься запросы от клиентов прокси-сервера.

Синтаксис

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

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<порт>` — номер порта.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу прокси-сервера (см. service http-proxy stop на стр. 226).
- При вводе интерфейса работает подсказка, данные для подсказки берутся из списка интерфейсов в системе (включая виртуальные интерфейсы, созданные при назначении дополнительных IP-адресов основным интерфейсам).
- На указанном интерфейсе должен быть задан IP-адрес.

Пример использования

Чтобы указать интерфейс eth1 и номер порта 6789 для приема запросов от клиентов прокси-сервера, выполните команду:

```
hostname# service http-proxy listen-address add eth1 6789
```

service http-proxy listen-address delete

Команда используется для удаления из списка интерфейса и порта, через которые не должны приниматься запросы от клиентов прокси-сервера.

Синтаксис

```
service http-proxy listen-address delete <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу прокси-сервера (см. service http-proxy stop на стр. 226).

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка для прослушивания.

Пример использования

Чтобы удалить интерфейс eth1 из списка интерфейсов, по которым принимаются запросы от клиентов прокси-сервера, выполните команду:

```
hostname# service http-proxy listen-address delete eth1
```

service http-proxy listen-address list

Команда предназначена для просмотра текущего списка адресов интерфейсов и портов, через которые принимаются запросы от клиентов прокси-сервера.

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> service http-proxy listen-address list
Listen:
10.0.14.110:6789 (eth0)
hostname>
```

service http-proxy mode

Команда используется для включения или выключения автоматического запуска прокси-сервера при загрузке ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

По умолчанию автоматический запуск прокси-сервера выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска прокси-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск, если заданы не все параметры, необходимые для работы прокси-сервера.

Пример использования

Чтобы выключить автоматический запуск прокси-сервера, выполните команду:

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

service http-proxy reset

Команда предназначена для очистки текущих настроек прокси-сервера.

Синтаксис

```
service http-proxy reset
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды запрашивается подтверждение очистки всех настроек прокси-сервера.
- При выполнении команды не удаляются сетевые фильтры и правила трансляции адресов, если такие создавались в соответствии с текущими настройками прокси-сервера с помощью команды service http-proxy fw-rules apply (на стр. 218). После очистки настроек прокси-сервера данные фильтры и правила трансляции можно удалить вручную с помощью команды service http-proxy fw-rules delete (на стр. 218).

Пример использования

Для очистки настроек прокси-сервера выполните следующую команду:

```
hostname# service http-proxy reset
```

service http-proxy show

Команда предназначена для просмотра текущих настроек прокси-сервера и его состояния.

Синтаксис

```
service http-proxy show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> service http-proxy show
HTTP PROXY is enabled
Service is running
Transparent: on
Cache size: 256
Listen:
169.254.241.1:6789 (eth1)
External address: 10.0.14.110 (eth0)
hostname>
```

service http-proxy start

Команда используется для запуска прокси-сервера.

Синтаксис

```
service http-proxy start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Невозможно запустить прокси-сервер, если заданы не все параметры, необходимые для его работы.

Пример использования

```
hostname# service http-proxy start
HTTP Proxy started
hostname#
```

service http-proxy stop

Команда используется для завершения работы прокси-сервера.

Синтаксис

```
service http-proxy stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# service http-proxy stop
Stopping HTTP Proxy: Waiting......
........
HTTP Proxy stopped
hostname#
```

service user-control active-users

Команда используется для вывода информации о текущих сессиях пользователей Active Directory и Captive portal.

Синтаксис

```
service user-control active-users
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

В результате выполнения команды отображается список пользователей в формате:

`<имя пользователя> <ip-адрес> {<метка времени>| 0 }`, где:

- `<имя пользователя>` — имя зарегистрированного пользователя Active Directory и Captive portal.
- `<ip-адрес>` — IP-адрес зарегистрированного пользователя Active Directory и Captive portal.
- `<метка времени>` — метка времени последнего IP-пакета от пользователя, если в Captive portal включены ограничения продолжительности сессии для IP-адресов пользователей. Если в Captive portal ограничения не включены, то вместо метки времени будет выводиться значение «0».

Примечание. ViPNet xFirewall не отслеживает выход пользователей из сети (logout). Например, если пользователь Active Directory вышел из сети, то он будет отображаться в списке пользователей до тех пор, пока не истечет время жизни кэша пользовательских сессий (см. service user-control ad set connection-timeout на стр. 229) или пока с этого IP-адреса в сеть не войдет другой пользователь.

Пример использования

```
hostname# service user-control active-users
User name     Session IP-address  Type   Start time    Lifetime left
-----------------------------------------------------------------
JohnSmith     13.34.152.12        AD     10:11:42
Admin         78.54.24.16         CP     12:24:45      15m (Idle)
User-123      82.12.33.212        CP     11:03:36      1h 3m
hostname#
```

service user-control ad reset

Команда используется для удаления параметров соединения ViPNet xFirewall с контроллером домена Active Directory.

Синтаксис

```
service user-control ad reset
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

После выполнения команды также останавливается работа демона управления пользователями (uc).

Пример использования

```
hostname# service user-control ad reset
Stopping uc.sh: uc.
hostname#
```

service user-control ad show

Команда используется для просмотра информации о текущих параметрах аутентификации с помощью Active Directory.

Синтаксис

```
service user-control ad show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

В результате выполнения команды выводится следующая информация о параметрах аутентификации с помощью Active Directory:

- Адрес и доступность контроллера домена (или сообщение об отсутствии этого параметра).
- Версия операционной системы и локаль контроллера домена.
- Имя пользователя, используемое для соединения с контроллером домена.
- Время задержки до следующего обновления статуса соединения.
- Допустимое время отсутствия связи (время до очистки кэша пользовательских сессий).

Пример использования

Выполнение команды при настроенном подключении к Active Directory имеет следующий вывод:

```
hostname# service user-control ad show

Active Directory authentication information:

    Domain Controller domain.local connection is available

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

    Domain user: admin

    DC synchronization delay: 100 sec

    Allowed connection timeout: 1800 sec

hostname#
```

service user-control ad set connection-timeout

Команда используется для задания времени жизни пользовательских сессий Active Directory.

Синтаксис

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

Параметры и ключевые слова

`<время жизни кэша пользовательских сессий>` — целое число в секундах.

Значения по умолчанию

По умолчанию время жизни кэша пользовательских сессий составляет 1800 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Значение параметра `<время жизни кэша пользовательских сессий>` должно быть больше или равно значению периода получения журнала контроллера домена (см. service user-control ad set sync-delay на стр. 231).

Пример использования

Для задания времени жизни пользовательских сессий Active Directory 60 секунд выполните команду:

```
hostname# service user-control ad set connection-timeout 60
hostname#
```

service user-control ad set controller

Команда используется для задания параметров соединения с контроллером домена Active Directory.

Синтаксис

```
service user-control ad set controller <адрес контроллера домена> user <имя пользователя>
```

Параметры и ключевые слова

- `<адрес контроллера домена>` — IP-адрес или доменное имя узла контроллера домена. Доменные имена не зависят от регистра и могут содержать латинские буквы (A-z), цифры (0-9), знак «минус» (-) и «точка» (.). Максимальная длина доменного имени — 253 символа.

- `<имя пользователя>` — имя пользователя домена, обладающего правами на чтение журналов системы контроллера домена. Имя пользователя не зависит от регистра и может содержать любые символы, кроме:

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

  Максимальная длина имени пользователя — 20 символов.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

После успешного выполнения команды в ответ на приглашение командного интерпретатора введите пароль пользователя Active Directory, после чего нажмите клавишу **Enter**. Длина пароля должна быть от 1 до 128 символов. Если пароль не введен, нажатие клавиши **Enter** не сработает.

Пример использования

Для задания параметров соединения с контроллером по адресу 192.168.1.23 и пользователем домена user23 выполните команду:

```
hostname# service user-control ad set controller 192.168.1.23 user user23
Enter user23 password:
hostname#
```

service user-control ad set sync-delay

Команда используется для задания периода получения журнала контроллера домена.

Синтаксис

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

Параметры и ключевые слова

`<период>` — целое число секунд от 0 и больше, значение по умолчанию 5.

Значения по умолчанию

По умолчанию период получения журнала контроллера домена равен 5 секундам.

Режимы командного интерпретатора

Администратор.

Особенности использования

Значение параметра `<период>` должно быть меньше или равно значению времени жизни кэша пользовательских сессий (см. service user-control ad set connection-timeout на стр. 229).

Пример использования

Для задания периода получения журнала контроллера домена 10 секунд выполните команду:

```
hostname# service user-control ad set sync-delay 10
hostname#
```

service user-control cp reset

Команда используется для сброса настроек Captive portal (см. глоссарий, стр. 293).

Синтаксис

```
service user-control cp reset
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

После выполнения команды также останавливается работа демона управления пользователями (uc).

Пример использования

Для сброса настроек Captive portal выполните команду:

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

```
Stopping uc.sh: uc.
hostname#
```

service user-control cp set connection-secure

Команда используется для задания режима соединения Captive portal (см. глоссарий, стр. 294) с LDAP-сервером (см. глоссарий, стр. 294).

Синтаксис

```
service user-control cp set connection-secure <режим соединения>
```

Параметры и ключевые слова

`<режим соединения>` — параметр 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.

Значения по умолчанию

По умолчанию установлен режим открытого соединения (`none`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для задания режима соединения с LDAP-сервером Start TLS выполните команду:

```
hostname# service user-control cp set connection-secure stls
hostname#
```

service user-control cp set connection-timeout

Команда используется для задания времени жизни сессии пользователя Captive portal (см. глоссарий, стр. 293), по истечении которого сессия будет принудительно сброшена.

Синтаксис

```
service user-control cp set connection-timeout <полное время жизни сессии пользователя>
```

Параметры и ключевые слова

`<полное время жизни сессии пользователя>` — целое число в секундах. Если задано значение 0, то длительность пользовательских сессий не ограничена.

Значения по умолчанию

По умолчанию для параметра `<полное время жизни сессии пользователя>` задано значение 43200 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для задания времени жизни сессии пользователя 1 час выполните команду:

```
hostname# service user-control cp set connection-timeout 3600
hostname#
```

service user-control cp set custom-login-form

Команда используется для задания произвольного текстового сообщения на странице авторизации пользователей Captive portal (см. глоссарий, стр. 293).

Синтаксис

```
service user-control cp set custom-login-form <текстовое сообщение>
```

Параметры и ключевые слова

`<текстовое сообщение>` — от 0 до 32 символов, при использовании пробелов необходимо заключить текстовое сообщение в двойные кавычки (`""`).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для задания текстового сообщения «Welcome to Guest Network!» на странице авторизации пользователей Captive portal выполните команду:

```
hostname# service user-control cp set custom-login-form "Welcome to Guest Network!"
hostname#
```

service user-control cp set hostcert

Команда используется для выбора сертификата веб-сервера Captive portal (см. глоссарий, стр. 293) из локального хранилища сертификатов ViPNet xFirewall.

Синтаксис

```
service user-control cp set hostcert <имя файла сертификата> hostkey <имя файла закрытого ключа>
```

Параметры и ключевые слова

- `<имя файла сертификата>` — имя файла сертификата;
- `<имя файла закрытого ключа>` — имя файла закрытого ключа.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды импортируйте сертификат и его закрытый ключ в корневое хранилище сертификатов ViPNet xFirewall (см. service cert import на стр. 189).
- Если вы выбрали сертификат веб-сервера Captive portal и хотите отказаться от его использования, то вам необходимо сбросить настройки Captive portal (см. service user-control cp reset на стр. 232).

Пример использования

Для выбора сертификата с именем `certificate.pem` и его закрытого ключа с именем `private.pem` выполните команду:

```
hostname# service user-control cp set hostcert certificate.pem hostkey private.pem
hostname#
```

service user-control cp set idle-timeout

Команда используется для задания времени неактивности (отсутствия передачи данных) пользователя Captive portal (см. глоссарий, стр. 293), по истечении которого сессия будет сброшена.

Синтаксис

```
service user-control cp set idle-timeout <время бездействия пользователя>
```

Параметры и ключевые слова

`<время бездействия пользователя>` — целое число в секундах. Если задано значение 0, то время бездействия не ограничено.

Значения по умолчанию

По умолчанию для параметра `<время бездействия пользователя>` задано значение 1800 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для задания времени бездействия пользователя 10 минут выполните команду:

```
hostname# service user-control cp set idle-timeout 600

hostname#
```

service user-control cp set ldap

Команда используется для задания параметров соединения Captive portal (см. глоссарий, стр. 293) с LDAP-сервером (см. глоссарий, стр. 294).

Синтаксис

```
service user-control cp set ldap <адрес LDAP-сервера> identity <имя администратора>
basedn <база поиска>
```

Параметры и ключевые слова

- `<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 «-» и «.».
- `<имя администратора>` — выделенное имя (DN, Distinguished Name) учетной записи администратора LDAP-сервера, которая обладает правами на чтение записей LDAP-сервера. Выделенное имя администратора может иметь длину до 256 любых символов, кроме:

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

  Выделенное имя администратора должно быть заключено в двойные кавычки (`""`).
- `<база поиска>` — выделенное имя (DN, Distinguished Name) 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 (`""`).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

После успешного выполнения команды в ответ на запрос командного интерпретатора введите пароль учетной записи администратора LDAP-сервера.

Пример использования

Предположим, для подключения к LDAP-серверу необходимо указать:

- адрес LDAP-сервера example.com;
- учетную запись администратора admin, которая находится в организации People и домене example;
- базу поиска example.

Для подключения к LDAP-серверу с указанными параметрами выполните команду:

```
hostname# service user-control cp set ldap example.com identity
"uid=admin,ou=People,dc=example" basedn "example"

Enter password for LDAP identity:

hostname#
```

service user-control cp set ldap cacert

Команда используется для выбора корневого сертификата LDAP-сервера (см. глоссарий, стр. 294) из локального хранилища сертификатов ViPNet xFirewall.

Синтаксис

```
service user-control cp set ldap cacert <имя файла сертификата>
```

Параметры и ключевые слова

`<имя файла сертификата>` — имя файла корневого сертификата в локальном хранилище ViPNet xFirewall.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды необходимо импортировать корневой сертификат LDAP-сервера в локальное хранилище сертификатов ViPNet xFirewall (см. service cert import на стр. 189).

Пример использования

Для выбора сертификата с именем `ldap_cert.pem` выполните команду:

```
hostname# service user-control cp set ldap cacert ldap_cert.pem

hostname#
```

service user-control cp show

Команда используется для вывода текущих настроек Captive portal (см. глоссарий, стр. 293).

Синтаксис

```
service user-control cp show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Администратор.
- Пользователь.

Особенности использования

Нет.

Пример использования

```
hostname> service user-control cp show
Captive Portal authentication information:
LDAP server 10.254.252.214 is available
LDAP identity: "uid=admin,ou=People,dc=test,dc=local"
LDAP basedn: "dc=test,dc=local"
LDAP connection secured: stls
LDAP server CA certificate: cacert.pem
CP server CA certificate:
Allowed connection timeout: 3600 sec
Allowed idle timeout: 600 sec
Custom login phrase: Guest Network
hostname>
```

service user-control fw-rules apply

Команда используется для создания разрешающих сетевых фильтров после изменения параметров соединения с сервером Active Directory или Captive portal.

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# service user-control fw-rules apply
Applying rules for Active Directory... Please wait.
hostname#
```

service user-control fw-rules delete

Команда используется для удаления разрешающих сетевых фильтров, созданных после выполнения команды `service user-control fw-rules apply` (на стр. 240).

Синтаксис

```
service user-control fw-rules delete
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

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

service user-control fw-rules show

Команда используется для просмотра сетевых фильтров, разрешающих соединение ViPNet xFirewall с сервером Active Directory и Captive portal.

Синтаксис

```
service user-control fw-rules show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

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

```
empty rule for  Service:
+======+=================+=============+==================+
|Num   |Name         |                   |Option Schedule    |
|Act   |Protocol           |Source       ->|Destination      |
|      |DpiProtocol        |DpiApp             |DomainUser   |
+======+=================+=============+=================+
|8     |user-control auto |                  |User         |
|pass  |@any       |@local       ->|10.10.10.10            |
|      |@any       |@any         |@any                      |
+======+=================+=============+=================+
hostname#
```

service user-control mode off

Команда используется для отключения автозапуска демона управления пользователями (uc) при загрузке ViPNet xFirewall.

Синтаксис

```
service user-control mode off
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для отключения автозапуска демона управления пользователями (uc) при загрузке ViPNet xFirewall выполните команду:

```
hostname# service user-control mode off
hostname#
```

service user-control mode on

Команда используется для включения автозапуска демона управления пользователями (uc) при загрузке ViPNet xFirewall.

Синтаксис

```
service user-control mode on
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Для включения автозапуска демона управления пользователями (uc) при загрузке ViPNet xFirewall выполните команду:

```
hostname# service user-control mode on
hostname#
```

service user-control show

Команда используется для просмотра информации о текущем статусе работы демона управления пользователями (uc).

Синтаксис

```
service user-control show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

В результате выполнения команды выводится следующая информация о статусе работы демона uc:

- Статус демона uc (включен или выключен) и режим его автозапуска.
- Текущий уровень событий, добавляемых в системный журнал (см. service user-control syslog-level на стр. 246).
- Статус настройки и доступность сервера Active Directory и Captive portal.
- Количество активных сессий пользователей (если демон uc запущен).

Пример использования

Выполнение команды при запущенном демоне uc имеет следующий вывод:

```
hostname# service user-control show
User Control service is ON and will NOT restart automatically
Current syslog level is warning and higher
Active Directory authentication is configured and available
Captive Portal authentication is is configured and available
No active network users.
hostname#
```

service user-control start

Команда используется для запуска демона управления пользователями (uc).

Синтаксис

```
service user-control start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# service user-control start
Starting uc.sh: uc.
hostname#
```

service user-control stop

Команда используется для остановки демона управления пользователями (uc).

Синтаксис

```
service user-control stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

```
hostname# service user-control stop

Stopping uc.sh: uc.

hostname#
```

service user-control syslog-level

Команда используется для задания уровня событий демона управления пользователями (uc), которые будут попадать в системный журнал.

Синтаксис

```
service user-control syslog-level <уровень событий>
```

Параметры и ключевые слова

`<уровень событий>` — число от 0 до 5, соответствующее уровням событий:

- 0 — критические события;
- 1 — ошибки;
- 2 — извещения;
- 3 — информационные события;
- 4 — отладочные события;
- 5 — детализированные отладочные события.

Значения по умолчанию

По умолчанию задан уровень событий 3 (информационные события).

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы в системный журнал записывались события демона uc уровня 4, выполните команду:

```
hostname# service user-control syslog-level 4

hostname#
```

Команды группы ups

Команды группы `ups` предназначены для настройки взаимодействия ViPNet xFirewall с источником бесперебойного питания (UPS) (см. глоссарий, стр. 297).

Примечание. Использование группы команд ups возможно только для аппаратных исполнений ViPNet xFirewall. Для исполнения ViPNet xFirewall xF-VA эти команды выполняться не будут.

ups set driver

Команда используется для выбора драйвера `UPS`.

Синтаксис

```
ups set driver <драйвер>
```

Параметры и ключевые слова

`<драйвер>` — название драйвера. В текущей версии ViPNet xFirewall можно указать только значение `usbhid-ups`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Нет.

Пример использования

Чтобы выбрать драйвер `UPS`, выполните команду:

```
hostname# ups set driver usbhid-ups
```

ups set mode

Команда используется для установки режима взаимодействия ViPNet xFirewall с UPS.

Синтаксис

```
ups set mode {master | slave <IP-адрес мастера>}
```

Параметры и ключевые слова

- `master` — взаимодействие в режиме главного компьютера. Главным является компьютер, к которому подключен интерфейсный кабель UPS и который непосредственно взаимодействует с UPS.
- `slave` — взаимодействие в режиме подчиненного компьютера. Подчиненный компьютер взаимодействует с UPS через главный компьютер.
- `<IP-адрес мастера>` — IP-адрес главного компьютера, находящегося в режиме `master`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды требуется вручную завершить работу демонов пакета NUT (Network UPS Tools) (см. глоссарий, стр. 295) с помощью команды ups stop (на стр. 252).

Пример использования

Для установки режима главного компьютера выполните команду:

```
hostname# ups set mode master
```

ups set monitoring

Команда используется для включения или выключения мониторинга состояния UPS.

Синтаксис

```
ups set monitoring {on | off}
```

Параметры и ключевые слова

- `on` — включение мониторинга.
- `off` — выключение мониторинга.

Значения по умолчанию

По умолчанию мониторинг состояния UPS выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- После включения мониторинга необходимо вручную запустить демоны пакета NUT с помощью команды ups start (на стр. 251).
- При выключении мониторинга будет автоматически завершена работа демонов пакета NUT.

Пример использования

Чтобы включить мониторинг состояния UPS, выполните команду:

```
hostname# ups set monitoring on
```

ups show config

Команда предназначена для просмотра текущих настроек взаимодействия ViPNet xFirewall с UPS.

Синтаксис

```
ups show config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> ups show config
UPS service mode is Master. Driver: usbhid-ups
UPS service is RUNNING
hostname>
```

По команде отображается следующая информация:

- Включен или выключен мониторинг состояния UPS. Остальная информация выводится только в случае, если мониторинг включен.
- Режим взаимодействия ViPNet xFirewall с UPS (`master` или `slave`).
- Используемый драйвер `UPS` (только в режиме `master`).
- IP-адрес мастера (только в режиме `slave`).
- Состояние демонов пакета `NUT` (запущены или работа демонов завершена).

ups show status

Команда предназначена для просмотра текущего состояния UPS.

Синтаксис

```
ups show status [extended]
```

Параметры и ключевые слова

`extended` — просмотр всех параметров состояния UPS в формате утилиты `upsc`, входящей в состав пакета `NUT`. Эта возможность предназначена для квалифицированных системных администраторов, которые могут самостоятельно интерпретировать результат вывода утилиты `upsc`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> ups show status
Manufacturer:   American Power Conversion
Model:          Smart-UPS 750 RM
Load:           24.0%
Power status:   OL
Battery charge: 100%
Runtime:        2520
Runtime to low: 1380
hostname>
```

По команде отображается следующая информация:

- Производитель UPS.
- Модель UPS.
- Текущая нагрузка по мощности (в процентах от максимальной нагрузки).
- Текущий режим питания (`OL` — питание от сети, `OB` — питание от батареи).
- Текущий уровень заряда батареи (в процентах от максимального уровня).
- Расчетное время работы от батареи при текущих нагрузке и уровне заряда (в секундах).
- Максимальное время работы от батареи, по истечении которого UPS посылает сигнал о необходимости выключения компьютера (задается производителем UPS).

ups start

Команда используется для запуска демонов пакета `NUT`, обеспечивающих взаимодействие ViPNet xFirewall с UPS.

Синтаксис

```
ups start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

Чтобы запустить демоны пакета `NUT`, выполните команду:

```
hostname> ups start
```

ups stop

Команда используется для завершения работы демонов пакета `NUT`, обеспечивающих взаимодействие ViPNet xFirewall с UPS.

Синтаксис

```
ups stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

Чтобы завершить работу демонов пакета `NUT`, выполните команду:

```
hostname> ups stop
```

Команды группы vpn

Команды группы `vpn` предназначены для загрузки и выгрузки драйверов и служб ViPNet.

vpn start

Команда используется для загрузки всех драйверов и запуска всех демонов ViPNet xFirewall.

Синтаксис

```
vpn start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда выполняется только в том случае, если перед этим была выполнена команда `vpn stop` или если демоны и драйверы не были запущены при загрузке ViPNet xFirewall (например, если вы не выбрали запуск сервисов VPN после разворачивания дистрибутива ключей). Если некоторые демоны были остановлены с помощью соответствующих команд, то команда `vpn start` не будет выполнена (отобразится сообщение `Failover daemon is already running (PID XXXX). Exit.`). Вместо нее используйте команды запуска демонов. Например, после выполнения команд `iplir stop` и `mftp stop` для запуска демонов `iplir` и `mftp` выполните команды `iplir start` и `mftp start`.

Пример использования

Для загрузки драйверов и запуска демонов ViPNet xFirewall выполните команду:

```
hostname# vpn start
```

vpn stop

Команда используется для выгрузки драйверов и завершения работы демонов ViPNet xFirewall.

Синтаксис

```
vpn stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Администратор.

Особенности использования

Нет.

Пример использования

Для выгрузки драйверов и завершения работы демонов ViPNet xFirewall выполните команду:

```
hostname# vpn stop
```

Команды группы webui

Команды группы `webui` предназначены для управления веб-сервером ViPNet xFirewall, на основе которого функционирует веб-интерфейс.

webui restart

Команда используется для перезапуска веб-сервера ViPNet xFirewall.

Синтаксис

```
webui restart
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Невозможно перезапустить веб-сервер, если он не был запущен.

Пример использования

```
hostname> webui restart
Shutting down ViPNet Web GUI service
Loading ViPNet Web GUI service
spawn-fcgi: child spawned successfully: PID: 22996
hostname>
```

webui status

Команда используется для просмотра текущего состояния веб-сервера ViPNet xFirewall.

Синтаксис

```
webui status
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> webui status
 WebUI server is enabled and is running.
hostname>
```

Прочие команды

К прочим относятся команды, которые не входят ни в одну из групп команд, описанных выше.

debug off

Команда используется для выключения вывода сообщений о событиях.

Синтаксис

```
debug off [<источник> <важность>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого требуется выключить вывод сообщений.
- `<важность>` — уровень серьезности выключаемых сообщений.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если в команде не указаны параметры, то будет выключен вывод всех сообщений.

Пример использования

Чтобы выключить вывод сообщений об ошибках демонов, выполните команду:

```
hostname# debug off daemon err
```

debug on

Команда используется для включения вывода сообщений о событиях.

Синтаксис

```
debug on [<источник> <важность>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого должны выводиться сообщения. Например:
    - `kern` (ядро);
    - `user` (пользовательские программы);
    - `mail` (почтовая система);
    - `daemon` (демоны).
- `<важность>` — уровень серьезности выводимых сообщений. Например:
    - `err` (ошибка);
    - `info` (информационное сообщение);
    - `debug` (отладочное сообщение).

Значения по умолчанию

- `<источник>` — `daemon`.
- `<важность>` — `debug`.

Режимы командного интерпретатора

- Администратор.

Особенности использования

Для демонов сообщения будут выводиться только в случае, если в их файлах конфигураций в секции `[debug]` задано протоколирование для указанных источника и важности сообщений.

Пример использования

Чтобы включить вывод сообщений об ошибках демонов, выполните команду:

```
hostname# debug on daemon err
```

enable

Команда используется для перехода в режим администратора.

Синтаксис

```
enable
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Пользователь.

Особенности использования

- После выполнения команды требуется указать пароль администратора сетевого узла ViPNet или пароль администратора группы сетевых узлов ViPNet.
- При вводе пароля на экране ничего не отображается, введенные символы отредактировать нельзя.
- Если пароль администратора введен верно, то выполняется переход в режим администратора, в журнале событий создается запись об успешном переходе в режим администратора, содержащая хэш-сумму пароля администратора, который был введен.

Пример использования

```
hostname> enable
Enter administrator password:
hostname# _
```

exit

Команда используется для выхода из текущего режима командного интерпретатора.

Синтаксис

```
exit
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- В результате выполнения команды в режиме администратора происходит переход в режим пользователя.
- В результате выполнения команды в режиме пользователя происходит завершение работы командного интерпретатора. При этом отображается приглашение ввести имя пользователя и пароль для запуска командного интерпретатора.

Пример использования

```
hostname# exit
hostname>
```

version

Команда предназначена для просмотра текущей версии ViPNet xFirewall и его компонентов.

Синтаксис

```
version [full]
```

Параметры и ключевые слова

`full` — просмотр текущей версии всех компонентов, а также других параметров (набор функционала для текущего исполнения, архитектура процессора).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> version
Product: ViPNet xFirewall VA
Platform: XFVA
License: XF-VA
Software version: 4.0.6-157
```

```
hostname>
```

По команде выводится название и версия исполнения ViPNet xFirewall, версия ПО ViPNet xFirewall. При указании ключевого слова `full` выводятся дополнительные параметры.

version features list

Команда предназначена для просмотра списка функциональных модулей, входящих в состав текущей версии ViPNet xFirewall.

Синтаксис

```
version features list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> version features list
dhcp-client
dhcp-relay
dhcp-server
...
hostname>
```

who

Команда предназначена для просмотра информации о запущенных сессиях командного интерпретатора (локальной и всех удаленных).

Синтаксис

```
who
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Нет.

Пример использования

```
hostname> who
LINE  HOST           IDLE      MODE  COMMENTS
tty1  local console  00:00:06  user  current
hostname>
```

Информация отображается в следующем формате:

```
LINE HOST IDLE MODE COMMENTS
```

где:

- `LINE` — имя консоли.
- `HOST` — адрес подключения (для своего узла — `local console`).
- `IDLE` — время неактивности (отсутствие нажатия каких-либо клавиш).
- `MODE` — командный режим: `user` (Пользователь) или `admin` (Администратор).
- `COMMENTS` — комментарий, содержащий информацию о консоли (обычно информация о местонахождении).

2

Справочник по конфигурационным файлам

Файл iplir.conf

Параметры защищенной сети ViPNet (см. глоссарий, стр. 300) содержатся в файле `iplir.conf`. Для редактирования этого файла используется команда `iplir config`. Перед редактированием файла `iplir.conf` необходимо завершить работу управляющего демона командой `iplir stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его командой `iplir start`.

Файл `iplir.conf` содержит секции с параметрами, описанные ниже.

Секция [adapter]

Секции `[adapter]` описывают статические сетевые интерфейсы компьютера (см. глоссарий, стр. 301). Каждому интерфейсу соответствует своя секция `[adapter]`. Если статический интерфейс не описан секцией `[adapter]`, то все проходящие через него IP-пакеты (см. глоссарий, стр. 294) блокируются.

Если в файле `iplir.conf` нет ни одной секции `[adapter]`, то управляющий демон при запуске получает от системы список сетевых интерфейсов и автоматически создает соответствующие секции `[adapter]`.

В процессе работы управляющий демон и драйвер ViPNet периодически получают информацию о параметрах известных им интерфейсов с интервалом времени, заданным параметром `ifcheck_timeout` секции `[misc]`. Если обнаруживается, что интерфейс выключен в системе, то он выключается и в драйвере ViPNet. После включения или изменения IP-адреса интерфейса эти изменения автоматически загружаются в драйвер ViPNet.

В секции `[adapter]` указываются следующие параметры:

- `allowtraffic` — разрешение или блокирование прохождения IP-трафика через интерфейс. Возможные значения:
  - `on` (по умолчанию) — IP-пакеты пропускаются или блокируются в соответствии с сетевыми фильтрами, заданными на узле.
  - `off` – IP-пакеты блокируются независимо от остальных настроек.
- `type` — тип интерфейса для драйвера ViPNet. Возможные значения: `internal` (внутренний) или `external` (внешний).

  Тип интерфейса выбирается, исходя из следующего:
  - Если ViPNet xFirewall работает в режиме «Без использования межсетевого экрана» или «С динамической трансляцией адресов», то все интерфейсы должны иметь тип `internal`.
  - Если ViPNet xFirewall работает в режиме «Координатор» или «Со статической трансляцией адресов» (с фиксированным внешним адресом (см. глоссарий, стр. 297)), то интерфейсу, посредством которого ViPNet xFirewall будет связываться с узлом, выполняющим функции

межсетевого экрана (см. глоссарий, стр. 298), следует назначить тип `external`, остальным интерфейсам ViPNet xFirewall — тип `internal`.

Нередактируемые параметры секции [adapter]

- `name` — системное имя интерфейса (например, eth0). Если в системе задано несколько IP-адресов на одном интерфейсе и присутствуют один или несколько виртуальных интерфейсов (eth0:0, eth0:1 и так далее), то для управляющего демона и драйвера ViPNet все они будут представлять одно физическое устройство с базовым именем (eth0).

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала устранения неполадок управляющего демона. Она содержит следующие параметры:

- `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`.

Секция [dynamic]

Секция `[dynamic]` содержит параметры для настройки режима подключения к внешней сети через межсетевой экран с динамической трансляцией адресов:

- `always_use_server` — включение или выключение режима, при котором весь трафик с внешними узлами направляется через сервер соединений, указанный в `forward_id` данной секции. Возможные значения: `off` (по умолчанию) или `on`.
- `dynamic_proxy` — включение или выключение режима «С динамической трансляцией адресов». Возможные значения: `off` (по умолчанию) или `on`. Если этот параметр установлен в значение `off`, то остальные параметры в данной секции игнорируются.

- `forward_id` — идентификатор сервера соединений для ViPNet xFirewall. С помощью сервера соединений ViPNet xFirewall будет устанавливать соединения с другими узлами — всегда, если включен режим в `always_use_server`, либо до тех пор, пока соединение с другими узлами не будет установлено напрямую. Указывается в шестнадцатеричном формате с префиксом `0x`, например: `0x15c8000a`.

Внимание! Указанный сервер соединений должен быть доступен из внешней сети по публичному IP-адресу.

- `timeout` — интервал отправки IP-пакетов серверу соединений для поддержания активного соединения с ним и пропуска входящего трафика через межсетевой экран. Указывается в секундах, значение по умолчанию — `25`. Как правило, интервала, заданного по умолчанию, достаточно для поддержки связи с сервером соединений при работе через большинство межсетевых экранов.

Секция [id]

Секция `[id]` используется для описания адресных настроек узлов сети ViPNet, связанных с ViPNet xFirewall. Каждому узлу, с которым у ViPNet xFirewall есть связь, соответствует своя секция `[id]`. Первая секция `[id]` соответствует собственным настройкам ViPNet xFirewall (собственная секция).

Секция `[id]` содержит следующие параметры:

- `accessiplist` — определяет IP-адреса доступа (см. глоссарий, стр. 296) к узлу и их приоритет, если узел имеет множественные адреса доступа. В каждой секции `[id]` может быть указано любое количество параметров `accessiplist` — по количеству адресов доступа к узлу. Причем в первом параметре `accessiplist` каждой секции в качестве адреса доступа должен быть указан тот же адрес, что и в параметре `firewallip` данной секции. Если в секции не будет параметров `accessiplist`, то параметр `firewallip` тоже будет отсутствовать. Остальные параметры `accessiplist` в секции используются для формирования списка адресов доступа к узлу с узла ViPNet xFirewall.

  Параметр `accessiplist` может быть указан во всех секциях `[id]`, кроме собственной, в виде:

  `accessiplist = <IP-адрес доступа>, <метрика>, <реальный IP-адрес узла>, <номер интерфейса>, <тип регистрации>`, где:

Примечание. Вручную в параметре `accessiplist` можно указать только IP-адрес узла или IP-адрес узла и метрику, остальные значения определяются системой автоматически в процессе работы управляющего демона.

  - `<IP-адрес доступа>` — IP-адрес доступа к узлу. Принимает значение `0.0.0.0`, когда данный узел не находится за межсетевым экраном.
  - `<метрика>` — метрика (см. глоссарий, стр. 299) указанного адреса доступа. Метрика определяет задержку (в миллисекундах) отправки служебных сообщений при выполнении

процедуры определения адреса доступа узла. Опросы осуществляются периодически (см. параметры `server_pollinterval` и `client_pollinterval` секции `[misc]`). Возможные значения: от `0` до `9999`. По умолчанию метрика имеет значение `auto`, то есть определяется автоматически.

- `<реальный IP-адрес узла>` — реальный IP-адрес узла, соответствующий сетевому интерфейсу (см. глоссарий, стр. 300), через который будут передаваться IP-пакеты для выбранного IP-адреса доступа.
- `<номер интерфейса>` — условный номер сетевого интерфейса. Возможные значения: от `0` до `255`.
- `<тип регистрации>` — тип регистрации данного IP-адреса доступа узла. Возможные значения:
  - `auto` — адрес задан ViPNet xFirewall.
  - `manual` — адрес задан администратором вручную (редактированием файла `iplir.conf`).
  - `addrdoc` — адрес взят из справочников, полученных из программы ViPNet Центр управления сетью (см. глоссарий, стр. 295).

- `fixfirewall` — определяет режим фиксации настроек работы собственного узла через внешний межсетевой экран. Возможные значения:
  - `off` (по умолчанию) — внешний IP-адрес и порт доступа к ViPNet xFirewall определяются автоматически по информации от узлов внешней сети;
  - `on` — внешний IP-адрес и порт доступа к ViPNet xFirewall жестко заданы администратором в параметрах `firewallip` и `port` данной секции.
- `ip` — содержит реальный IP-адрес (см. глоссарий, стр. 300) и соответствующий ему виртуальный IP-адрес (см. глоссарий, стр. 296) узла. Причем первым указывается реальный адрес, затем после запятой — виртуальный (например: `ip = 192.168.201.10, 10.1.0.5)`. Если указан только реальный адрес, то считается, что ему еще не сопоставлен виртуальный.

  Если узел имеет несколько сетевых интерфейсов или несколько IP-адресов на интерфейсе, в каждой секции `[id]` может быть несколько параметров `ip`. При этом первым должен быть указан параметр, содержащий наиболее приоритетный IP-адрес доступа к данному узлу. При автоматическом обновлении адресов наиболее приоритетный IP-адрес доступа становится первым автоматически. Причем в случае изменения порядка следования реальных IP-адресов, порядок следования виртуальных адресов не меняется.
- `port` — определяет порт назначения, на который следует посылать пакеты для узла, если этот узел находится за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр.
- `proxyid` — определяет режим работы узла, находящегося за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр. Возможные значения:
  - в собственной секции `[id]`:

- `0xfffffffe` — при работе в режиме «С динамической трансляцией адресов» (если в секции `[dynamic]` параметр `dynamic_proxy` установлен в `on` (см. Секция [dynamic] на стр. 265));
- `0x00000000` — при работе в режиме «Со статической трансляцией адресов» (если в собственной секции `[id]` параметр `usefirewall` установлен в `on`);
- идентификатор координатора, через который осуществляется обмен информацией с другими узлами — при работе в режиме «Координатор» (если в соответствующей секции `[id]` параметр `usefirewall` установлен в `on`). Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`;
- идентификатор собственного координатора — при работе в режиме «Без использования межсетевого экрана» (если в собственной секции `[id]` параметр `usefirewall` установлен в `off`). Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.

o в любой секции `[id]`, кроме собственной:

- `0xfffffffe` — при работе в режимах «Со статической трансляцией адресов» или «С динамической трансляцией адресов», если узел является сервером соединений для ViPNet xFirewall;
- `0x00000000` — при работе в режиме «Без использования межсетевого экрана»;
- идентификатор координатора — при работе в режимах «Координатор» или «С динамической трансляцией адресов». Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.

- `usefirewall` — может принимать значение `on` или `off` и используется в секциях `[id]` в следующих целях:
  - Во всех секциях `[id]`, кроме собственной, — указывает на использование настроек работы через межсетевой экран с данным узлом. Если этот параметр имеет значение `off`, то параметры `firewallip`, `port` и `proxyid` в этой секции игнорируются, и работа с данным узлом будет возможна только по одному из его реальных IP-адресов.
  - В собственной секции `[id]` — указывает на использование внешнего межсетевого экрана. В случае если межсетевой экран использоваться не будет, он установлен в значение `off`, в остальных случаях — в значение `on` (см. описание параметра `proxyid` данной секции).
- `visibility` — позволяет настроить тип видимости узла. Возможные значения:
  - `auto` — автоматически определять тип видимости узла, в зависимости от текущего адреса видимости узла (см. глоссарий, стр. 296).
  - `real` — всегда обращаться к данному узлу по его реальному адресу.
  - `virtual` — всегда обращаться к данному узлу по его виртуальному адресу.

Внимание! Для узлов ViPNet, расположенных на мобильных устройствах, параметру `visibility` всегда автоматически присваивается значение `virtual`.

Этот параметр не является обязательным и используется, только если для данного узла необходимо индивидуально задать тип видимости. В случае отсутствия параметра `visibility` видимость узла определяется параметрами секции `[visibility]`, то есть параметрами видимости всей сети, к которой этот узел принадлежит, либо параметрами видимости узлов по умолчанию.

Примечание. Использовать параметр `visibility` нужно осторожно, так как у сетевых узлов, которые видны по виртуальным адресам, могут совпадать реальные адреса (если эти узлы находятся в частных сетях).

Нередактируемые параметры секции [id]

- `accessip` — текущий IP-адрес доступа к узлу (см. глоссарий, стр. 296) со стороны ViPNet xFirewall. Может принимать значение одного из реальных или виртуальных IP-адресов, в зависимости от физической топологии сети, режимов подключения к внешней сети ViPNet xFirewall и данного узла.
- `always_use_server` — признак работы узла в режиме использования межсетевого экрана с динамической трансляцией адресов с направлением трафика через выбранный координатор. Параметр присутствует только в случае работы данного узла в указанном режиме и принимает значение `on`.
- `dynamic_timeout` — период опроса (в секундах) ViPNet-координатора, выбранного в качестве межсетевого экрана для данного узла, с целью обеспечения пропуска входящего трафика через межсетевой экран. Данный параметр присутствует во всех секциях `[id]`, кроме собственной.
- `id` — уникальный идентификатор узла. По этому параметру управляющий демон отличает одну секцию `[id]` от другой. Идентификатор присваивается сетевому узлу ViPNet при его создании в программе ViPNet Центр управления сетью (см. глоссарий, стр. 295). В каждой секции `[id]` может быть только один такой параметр.
- `firewallip` — определяет внешний IP-адрес доступа к узлу в случае, если этот узел находится за межсетевым экраном. При работе с узлом, установленным за межсетевым экраном, все направленные к нему зашифрованные пакеты инкапсулируются (см. глоссарий, стр. 297) в единый UDP-пакет с адресом назначения, указанным в данном параметре, и портом назначения, указанным в параметре `port` данной секции. Если узел не находится за межсетевым экраном, то параметр `firewallip` отсутствует или установлено его значение `0.0.0.0`. В каждой секции `[id]` может быть только один такой параметр.
- `name` — имя узла. Задается администратором сети ViPNet в программе ViPNet Центр управления сетью и предназначен для удобства настройки. Данный параметр записывается в файл конфигурации автоматически при его сохранении. В каждой секции `[id]` может быть только один такой параметр.
- `virtualip` — базовый виртуальный адрес узла. В каждой секции `[id]` может быть только один такой параметр.

- `version` — версия протокола обмена служебной информацией между узлами сети ViPNet.

Секция [misc]

Секция `[misc]` содержит различные дополнительные параметры:

- `config_version` — версия конфигурационного файла (совпадает с версией ViPNet xFirewall, с помощью которой файл последний раз был сохранен).
- `ifcheck_timeout` — период опроса параметров сетевых интерфейсов, известных управляющему демону. Указывается в секундах, значение по умолчанию — `5`.
- `msg_compress_level` — степень сжатия служебных межсерверных сообщений. Возможные значения: от 1 (минимальное сжатие, максимальная скорость) до 9 (максимальное сжатие, минимальный объем служебного трафика). Значение по умолчанию — 3.

Примечание. На высоконагруженных узлах не рекомендуется устанавливать значение параметра `msg_compress_level` больше 5.

- `mssdecrease` — число байт, на которое будет уменьшен параметр MSS (максимальный размер сегмента) протокола TCP. Значение по умолчанию — `0`.

  Уменьшать параметр MSS рекомендуется только, если между вашим и другими узлами сети ViPNet успешно проходит проверка соединения (ping), но не устанавливается TCP-соединение. Причиной блокирования шифрованных управляющих IP-пакетов, передаваемых в рамках TCP-соединения, может быть фрагментация этих IP-пакетов на устройствах, стоящих на пути от отправителя к получателю.

  Во избежание фрагментации рекомендуется уменьшить размер IP-пакетов, принимаемых на узле, присвоив параметру `mssdecrease` значение от 20 до 40 байт. Чтобы уменьшить размер исходящих IP-пакетов узла, значение параметра `mssdecrease` следует изменить на узле получателя этих IP-пакетов. Для установления TCP-соединения достаточно изменить параметр `mssdecrease` на одном из взаимодействующих узлов.

Внимание! Параметр `mssdecrease` не следует изменять без крайней необходимости.

- `packettype` — формат шифрованных управляющих пакетов. Возможные значения: `4.1` (по умолчанию) или `4.0`. Определяет только формат пакетов, отправляемых данным сетевым узлом. Формат входящих пакетов определяется автоматически, и их расшифрование производится независимо от установленного значения параметра `packettype`. Формат пакетов 4.0 рекомендуется использовать только, если необходимо связываться с узлами, на которых установлены старые версии ПО ViPNet.
- `timediff` — максимально допустимая разница между временем отправки и временем приема IP-пакетов. Из соображений безопасности драйвер ViPNet блокирует входящие IP-пакеты, если

время их отправки отличается от времени их приема более чем на число секунд, указанное в этом параметре. Значение параметра должно быть больше либо равно 1 секунде и меньше либо равно 7200 секунд. Значение по умолчанию — `7200` (2 часа).

- `timesync` — включение или выключение автоматической установки времени на ViPNet xFirewall в соответствии со временем на координаторе ViPNet, который служит сервером IP-адресов для ViPNet xFirewall. На ViPNet xFirewall этот параметр по умолчанию установлен в значение on, изменять его не следует.
- `warnoldautosave` — параметр, включающий или выключающий предупреждения о наличии конфигураций, содержащих настройки ПО ViPNet, которые были автоматически сохранены более месяца назад. Возможные значения: `on` (по умолчанию) или `off`. Если параметр установлен в значение `on`, то предупреждения выводятся каждый раз при запуске управляющего демона.

Секция [servers]

Секция `[servers]` содержит список координаторов ViPNet (см. глоссарий, стр. 298), известных данному сетевому узлу. Каждому координатору соответствует один параметр `server`, в котором через запятую указаны идентификатор координатора и его имя.

Для координатора, выбранного в качестве сервера IP-адресов, вместо параметра `server` используется параметр `active`.

Секция [virtualip]

Секция `[virtualip]` описывает настройки виртуальных IP-адресов (см. глоссарий, стр. 296) и содержит следующие параметры:

- `endvirtualip` — служебный параметр, в котором хранится следующий за последним назначенным базовый виртуальный адрес (см. глоссарий, стр. 296). Используется в качестве точки отсчета при поиске и назначении базовых виртуальных адресов для новых узлов сети ViPNet. При назначении базовых виртуальных адресов сначала проверяется, есть ли свободный виртуальный адрес в диапазоне от `startvirtualip` до `endvirtualip`, оказавшийся таковым в результате удаления одного из узлов и, если такой есть, то назначается этот свободный виртуальный адрес. Если – нет, то производится поиск первого свободного адреса в диапазоне от `endvirtualip` до `maxvirtualip`.

Внимание! Параметр `endvirtualip` не следует изменять (особенно увеличивать) без крайней необходимости.

- `maxvirtualip` — максимальный адрес для формирования базовых виртуальных адресов узлов сети ViPNet (по умолчанию — `11.0.255.255`). Используется для ограничения диапазона назначаемых базовых виртуальных адресов. По умолчанию параметр `maxvirtualip`

соответствует максимально возможному адресу, то есть адресу, у которого два старших октета совпадают с этими же октетами стартового адреса `startvirtualip`, а два младших октета равны 255. Данное значение можно уменьшить, при этом необходимо следить за тем, чтобы оно было больше значения параметра `endvirtualip`.

- `startvirtualip` — стартовый адрес для формирования базовых виртуальных адресов узлов сети ViPNet (по умолчанию — `11.0.0.1`). При изменении данного параметра назначение всех базовых виртуальных адресов узлов производится заново, как при начальном формировании файлов конфигурации. Кроме того, для узлов производится назначение виртуальных адресов в параметрах `ip` (см. Секция [id] на стр. 266).

Секция [visibility]

Секция `[visibility]` содержит настройки видимости узлов сети ViPNet, с которыми связан ViPNet xFirewall. В отличие от параметра `visibility`, с помощью которого в секциях [id] (см. Секция [id] на стр. 266) задается видимость отдельных узлов, в этой секции можно задать видимость сразу для всех узлов сетей или подсетей ViPNet. Настройки, заданные в секции `[visibility]`, учитываются при определении видимости узлов со стороны собственного узла.

Секция может содержать следующие параметры:

- `default` — видимость узлов по умолчанию. Возможные значения:
  - `auto` (по умолчанию) — автоматическое определение видимости узлов;
  - `real` — доступ к узлам по их реальным IP-адресам (см. глоссарий, стр. 300);
  - `virtual` — доступ к узлам по их виртуальным IP-адресам (см. глоссарий, стр. 296).
- `subnet_real` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по реальным IP-адресам.

  Идентификатор сети вы можете посмотреть в управляющем ПО ViPNet, например в ViPNet Центр управления сетью, или с помощью команды `iplir info`. Идентификаторы сетей указываются в шестнадцатеричном формате с префиксом `0x`. В одной секции `[visibility]` можно задать несколько параметров `subnet_real`. При этом в каждом параметре можно указать либо один идентификатор, либо несколько идентификаторов через запятую. Например:

  ```
  subnet_real = 0x5155
  subnet_real = 0x5156,0x5157,0x5158
  ```

- `subnet_virtual` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по виртуальным IP-адресам. Задается так же, как параметр `subnet_real`.

Внимание! Один и тот же идентификатор сети ViPNet можно указать только в одном из параметров `subnet_real` или `subnet_virtual`.

При старте управляющего демона идентификаторы, заданные в параметрах `subnet_real` и `subnet_virtual`, автоматически сортируются в порядке возрастания и группируются в строки, каждая из которых содержит максимум 8 идентификаторов.

Параметры `subnet_real` и `subnet_virtual` являются необязательными и по умолчанию отсутствуют в секции `[visibility]`.

Файл iplir.conf-<интерфейс или группа интерфейсов>

Параметры журнала прохождения трафика через любой активный сетевой интерфейс настраиваются в конфигурационных файлах `iplir.conf-<интерфейс или группа интерфейсов>`. Для каждого статического интерфейса, описанного секцией [adapter] в файле `iplir.conf`, а также для каждой группы динамических интерфейсов управляющий демон при запуске автоматически создает такой файл с параметрами по умолчанию.

Для редактирования этих файлов используется команда:

```
iplir config <интерфейс или группа интерфейсов>
```

Перед редактированием файла `iplir.conf-<имя интерфейса или группа интерфейсов>` необходимо завершить работу управляющего демона командой `iplir stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его командой `iplir start`.

Внимание! Конфигурационный файл `iplir.conf-<интерфейс или группа интерфейсов>` может отсутствовать для статического интерфейса, если соответствующая секция `[adapter]` была добавлена в файл `iplir.conf` вручную и после этого управляющий демон не перезапускался. Поэтому после добавления секций `[adapter]` в файл `iplir.conf` вручную рекомендуется сначала запустить управляющий демон командой `iplir start`, затем завершить его работу командой `iplir stop`, после чего отредактировать нужный файл `iplir.conf-<интерфейс или группа интерфейсов>` и снова запустить управляющий демон.

Каждый файл `iplir.conf-<интерфейс или группа интерфейсов>` содержит секции `[db]` и `[cef]`.

Для каждого статического интерфейса и группы динамических интерфейсов ведется свой журнал, который хранится в файле `iplir.db-<интерфейс или группа интерфейсов>`, расположенном в подкаталоге `iplirdb` каталога, содержащего файлы `iplir.conf-<имя интерфейса или группа интерфейсов>`.

Записи о пакетах накапливаются в журнале регистрации IP-пакетов до тех пор, пока не будет достигнут максимальный размер журнала, после чего самые ранние записи стираются и на их место записываются новые. Для уменьшения размера журнала, а также для удобства его просмотра одинаковые записи о пакетах, зарегистрированные в течение заданного времени, объединяются в одну запись, и затем при просмотре журнала можно узнать, сколько раз было зафиксировано событие, описываемое этой записью.

Секция `[db]`

Секция `[db]` содержит следующие параметры:

- `maxsize` — максимальный размер журнала в мегабайтах (по умолчанию — `50 MBytes`).

  В исполнении xF100 максимальный размер журнала не должен превышать 50 Мбайт. Значение по умолчанию — 50 Мбайт. При указании большего размера журнала он автоматически устанавливается равным 50 Мбайт.

  В исполнениях xF1000, xF5000 и xF-VA ограничений на размер журнала не установлено. Значение по умолчанию — 50 Мбайт.

  Реальный размер журнала из-за наличия в нем служебного заголовка получается примерно на 1 Кбайт больше. Каждый раз при запуске управляющего демона после размера журнала автоматически дописывается слово `MBytes`, если оно отсутствует. Поэтому при изменении значения этого параметра его можно не писать. Значение параметра `0` выключает ведение журнала. При этом если до выключения журнала в нем были записи, то просмотреть их будет невозможно.

- `timedif` — интервал времени, в течение которого одинаковые события объединяются в журнале в одну запись. Диапазон разрешенных значений в секундах `0` — `86400`, значение по умолчанию — `60`. При включенном экспорте событий в формате CEF параметр `timedif` определяет периодичность отправки объединенных записей журнала регистрации IP-пакетов. Если параметр `timedif` установлен в `0`, то объединение событий не происходит, а период экспорта записей журнала регистрации IP-пакетов в формате CEF составит 1 секунду.

- `registerall` — включение или выключение регистрации записей обо всех пакетах, проходящих через интерфейс. Возможные значения: `off` (по умолчанию) или `on`. То есть по умолчанию регистрируются только записи о блокированных пакетах и изменении адресов сетевых узлов.

- `registerbroadcast` — включение или выключение регистрации записей о широковещательных пакетах. Возможные значения: `off` (по умолчанию) или `on`.

- `registertcpserverport` — включение или выключение скрытия информации о порте ViPNet xFirewall при соединении TCP. Возможные значения: `off` (по умолчанию) или `on`.

  Обычно порт клиента при TCP-соединении выделяется динамически и никакой полезной информации не несет. Если с какого-либо сетевого ресурса производятся попытки подключиться к какому-либо порту на компьютере, а соединение по каким-то причинам не будет установлено, то при следующей попытке установить соединение с того же ресурса будет использоваться другой порт. При использовании сканеров портов или каких-либо сетевых атаках число таких попыток может достигать нескольких сотен в секунду. Поскольку клиент использует каждый раз разные порты, то такие пакеты не считаются одинаковыми и для каждого из них создается своя запись в журнале, что засоряет его и затрудняет последующий анализ. Если параметр `registertcpserverport` установлен в значение `on`, порт клиента при TCP-соединении не регистрируется и не учитывается, что позволяет объединить события о попытках подключения к какому-либо порту на компьютере с определенного адреса в одну запись. Это часто бывает удобно.

Примечание. Если параметр `registertcpserverport` установлен в значение `on`, то значение клиентского порта, отображаемого в журнале пакетов, будет равно 0.

- `registerevents` — включение или выключение регистрации служебных событий. Список служебных событий см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», в приложении «Типы событий в журнале регистрации IP-пакетов». Возможные значения: `off` или `on` (по умолчанию).

Секция `[cef]`

Секция `[cef]` содержит следующие параметры:

- `event` — формирование сообщений CEF (см. глоссарий, стр. 293) 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. Допускается перечисление номеров типов событий в любом порядке через запятую.

Файл failover.ini

Настройка параметров работы системы защиты от сбоев осуществляется путем редактирования файла конфигурации `failover.ini`. Для редактирования файла конфигурации используется команда `failover config edit`. Перед редактированием файла необходимо завершить работу демона failoverd командой `failover stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его с помощью команды `failover start`.

Файл `failover.ini` содержит секции с параметрами, описанные ниже.

Секция [channel]

Каждый сетевой интерфейс активного сервера, работоспособность которого должна контролироваться системой защиты от сбоев при работе в режиме кластера горячего резервирования (см. глоссарий, стр. 297), должен быть описан секцией `[channel]`.

Примечание. Параметры секций `[channel]` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

Чтобы выключить контроль работоспособности какого-либо интерфейса, необходимо удалить из файла `failover.ini` соответствующую секцию `[channel]`.

Секция `[channel]` содержит следующие параметры:

- `activeip` — IP-адрес и маска, которые будет иметь интерфейс активного сервера кластера. Если маска не указана, то будет использовано значение маски, установленное в системе. Маска может быть указана после IP-адреса через символ «/» в нотации CIDR или в прямой нотации. Например:
  - в нотации CIDR: `activeip = 192.168.201.1/24`
  - в прямой нотации: `activeip = 68.21.12.34/255.255.252.0`

Примечание. Указывать маску необходимо при организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов (подробнее см. в документе «ViPNet xFirewall. Сценарии работы»).

Независимо от того, в какой нотации была указана маска, после сохранения файла `failover.ini` и запуска демона `failoverd` маска будет перезаписана в нотации CIDR.

- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов. Возможные значения:

- `yes` (по умолчанию) — активный сервер посылает echo-запросы на интерфейсы, адреса которых указаны в соответствующих параметрах `testip`, только если за период опроса IP-адресов, указанный в параметре `checktime` в секции `[network]`, на данных интерфейсах не было или входящих, или исходящих пакетов.
- `no` — echo-запросы на интерфейсы, адреса которых указаны в соответствующих параметрах `testip`, посылаются постоянно.

- `device` — имя интерфейса (`eth0`, `eth1` и так далее).
- `ident` — текстовая строка, идентифицирующая интерфейс. Для интерфейсов, подключенных к одинаковым сетям, параметры `ident` должны совпадать.

Примечание. Не рекомендуется использовать разные имена (несимметричные конфигурации) интерфейсов кластера горячего резервирования.

- `passiveip` — IP-адрес и маска, которые будет иметь интерфейс пассивного сервера кластера. Если маска не указана, то будет использовано значение маски, установленное в системе. Маска может быть указана в таком же формате как в параметре `activeip`.
- `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
  ```

Внимание! Для каждого интерфейса, описанного секцией `[channel]`, в параметре `testip` должен быть задан свой адрес, принадлежащий подсети данного интерфейса.

Если в параметре `testip` один и тот же адрес указан для нескольких интерфейсов, будет проверяться работоспособность только сетевого интерфейса, указанного в конфигурационном файле первым.

Если в параметре `testip` задан адрес, не принадлежащий подсети данного интерфейса, то для этого адреса должен быть задан статический маршрут или шлюз по умолчанию.

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.

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала устранения неполадок демона failoverd и содержит следующие параметры:

- `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`.

Секция [misc]

Секция `[misc]` содержит дополнительные параметры работы системы защиты от сбоев в режиме кластера горячего резервирования и в одиночном режиме:

- `maxjournal` — максимальное количество дней, за которое необходимо хранить записи в журнале переключений кластера горячего резервирования. По умолчанию это ограничение отсутствует.
- `reboot` — задает действия системы в случае обнаружения полной неработоспособности какого-либо демона или драйвера ViPNet xFirewall. Возможные значения:
  - `yes` (по умолчанию) — включить механизм регистрации в watchdog-драйвере и перезагружать систему, если какой-либо демон или драйвер не может восстановить свою работу;
  - `no` — выключить механизм регистрации в watchdog-драйвере и не перезагружать систему, если какой-либо демон или драйвер не может восстановить свою работу.

Нередактируемые параметры секции [misc]

- `activeconfig` — абсолютный путь к файлу конфигурации управляющего демона, который будет использоваться на активном сервере кластера. Значение по умолчанию — `/etc/iplirpsw`.

- `passiveconfig` — абсолютный путь к файлу конфигурации управляющего демона, который будет использоваться на пассивном сервере кластера. Значение по умолчанию — `/etc/iplirpsw`.

Примечание. Параметры `activeconfig`, `passiveconfig` и `maxjournal` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

Секция [network]

Секция `[network]` описывает различные параметры работы системы защиты от сбоев, относящиеся к посылке пакетов в сеть в режиме кластера горячего резервирования.

Примечание. Все параметры секции `[network]` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

Все параметры этой секции рекомендуется настроить одинаково на обоих серверах кластера.

Секция `[network]` содержит следующие параметры:

- `activeretries` — количество неуспешных попыток опроса пассивным сервером активного сервера, после которых делается вывод об отсутствии активного сервера с опрашиваемым IP-адресом. По умолчанию — `3`.
- `afterifconf` — имя скрипта, содержащего команды, которые выполняются непосредственно после конфигурирования всех интерфейсов при смене активного сервера.
- `beforeifconf` — имя скрипта, содержащего команды, которые выполняются перед конфигурированием всех интерфейсов при смене активного сервера.

Примечание. Параметры `afterifconfig` и `beforeifconfig` используются для организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов (подробнее см. в документе «ViPNet xFirewall. Сценарии работы»). Они не являются обязательными и могут отсутствовать в секции.

- `channelretries` — количество неуспешных попыток опроса интерфейса тестового узла, после которых этот интерфейс считается неработоспособным. По умолчанию — `3`.
- `checktime` — период опроса:
  - на активном сервере — для проверки работоспособности интерфейса;
  - на пассивном сервере — для поиска IP-адресов активного сервера.

  Указывается в секундах, по умолчанию — `10`.

- `fastdown` — указывает на принудительное выключение сетевых интерфейсов перед перезагрузкой сервера. Возможные значения: `yes` (по умолчанию) или `no`. Значение, выбранное по умолчанию, позволяет быстрее установить отсутствие активного сервера в сети и дать возможность второму серверу перейти в активный режим, однако при этом завершение работы сетевых сервисов происходит уже при выключенных интерфейсах и может быть некорректным.
- `synctime` — период отправки пакетов синхронизации по резервному каналу. Указывается в секундах, значение по умолчанию — `5`.
- `timeout` — время ожидания ответа на запрос (эхо-запрос или запрос IP-адресов активного сервера), по истечении которого делается вывод о неуспешности этого запроса. Указывается в секундах, по умолчанию — `2`.

Секция [sendconfig]

В секции `[sendconfig]` задаются параметры, контролирующие отправку конфигурационных файлов с активного сервера на пассивный с целью резервирования.

Примечание. Все параметры секции `[sendconfig]` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования серверов.

Секция `[sendconfig]` содержит следующие параметры:

- `activeip` — адрес резервного канала другого сервера кластера (который работает в режиме, противоположном режиму данного сервера).
- `config` — включение или выключение резервирования группы конфигурационных файлов. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят следующие конфигурационные файлы:
  - файл `iplir.conf`;
  - файлы `iplir.conf-<интерфейс или группа интерфейсов>`, кроме файла для интерфейса резервного канала;
  - файл `mftp.conf` (см. Файл mftp.conf на стр. 284);
  - файлы, содержащие сетевые фильтры и правила трансляции (заданные пользователем и полученные из программы ViPNet Policy Manager);
  - файлы `*.crg` с контрольными суммами конфигурационных файлов;
  - файлы с настройками маршрутизации (см. глоссарий, стр. 298) и статическими маршрутами (если такие создавались);
  - другие служебные конфигурационные файлы.
- `connectport` — номер порта, используя который данный пассивный сервер кластера соединяется с активным сервером и принимает от него файлы для резервирования. По умолчанию этот параметр отсутствует и равен значению параметра `port` данной секции.

Внимание! Номер порта, заданный в параметре `connectport`, по умолчанию используется пассивным сервером кластера для проверки доступности сетевых интерфейсов активного сервера, поэтому изменять значение этого параметра без явной необходимости не рекомендуется.

- `device` — системное имя интерфейса, который используется для организации резервного канала.
- `file` — абсолютный путь к файлу для резервирования. По умолчанию отсутствует. В секции может быть несколько таких параметров, в каждом из которых может быть указан любой файл, который требуется резервировать и который не входит в группы конфигурационных файлов (`config`), файлов справочников и лицензии (`keys`) и файлов журналов (`journals`). Размер указанного файла не должен превышать 1 Мбайт, и для пересылки этого файла должно быть достаточно времени, указанного в параметре `sendtime` данной секции.

Примечание. Чтобы выбрать для резервирования не все, а один или несколько файлов, входящих в группы конфигурационных файлов или файлов журналов, необходимо установить параметр `config` или `journal` в значение `no` и указать нужные файлы в параметрах `file`.

- `journals` — включение или выключение резервирования группы файлов журналов ПО ViPNet. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят следующие файлы:
  - файлы журналов IP-пакетов сетевых интерфейсов, кроме интерфейса резервного канала;
  - файлы журнала конвертов транспортного модуля MFTP;
  - другие служебные файлы журналов.
- `keys` — включение или выключение резервирования группы файлов справочников и лицензии (см. глоссарий, стр. 301). Возможные значения: `yes` (по умолчанию) или `no`.

Внимание! Набор файлов, входящих в группы конфигурационных файлов (`config`), файлов справочников и лицензии (`keys`) и файлов журналов (`journals`), определяется демоном failoverd автоматически на активном сервере. Пассивный сервер в каждом цикле резервирования запрашивает сначала список файлов, входящих в каждую группу, для которой включено резервирование, и другие файлы для резервирования (`file`), а затем инициирует передачу этих файлов.

Резервирование групп файлов производится только при запущенных на активном сервере демонах `iplircfg` и `mftpd`, а также если параметры `config`, `keys` и `journal` установлены в значение `yes`. Установка параметра `config`, `keys` или `journal` в значение `no` означает выключение резервирования соответствующей группы. Не рекомендуется устанавливать параметры `config` и `keys` в значение `no`, так как это может привести к некорректной работе ПО ViPNet.

- `port` — номер порта, на котором данный активный сервер кластера ожидает соединения от пассивного сервера для передачи ему файлов для резервирования. По умолчанию — `10090`.
- `sendtime` — период резервирования файлов, то есть период между попытками пересылки файлов. Указывается в секундах, по умолчанию — `60`.

Файл mftp.conf

Параметры работы транспортного модуля MFTP (см. глоссарий, стр. 301) содержатся в файле `mftp.conf`. Для редактирования этого файла используется команда `mftp config`. Перед редактированием файла необходимо завершить работу демона `mftpd` командой `mftp stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его с помощью команды `mftp start`.

Файл `mftp.conf` содержит секции с параметрами, описанные ниже.

Секция [channel]

Секции `[channel]` содержат настройки каналов, по которым может обмениваться данными с другими узлами. Каждому узлу, с которым у есть связь, соответствует своя секция `[channel]`. Набор параметров в каждой секции зависит от типа выбранного канала. По умолчанию при создании файла конфигурации для всех каналов устанавливается тип `mftp`.

Внимание! Добавление и удаление секций `[channel]` осуществляется автоматически, делать это вручную не следует.

Секции `[channel]` для каналов любого типа содержат следующие параметры:

- `type` — тип канала. Возможные значения: `mftp` (по умолчанию), `smtp`, `viaserv` (подробнее см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», в главе «Настройка транспортного модуля»).
- `off_flag` — признак выключения канала. Возможные значения:
  - `no` (по умолчанию) — канал включен. В этом случае попытка передачи конверта по каналу производится немедленно.
  - `yes` — канал выключен. В этом случае исходящие конверты, передаваемые по каналу, остаются в очереди до тех пор, пока канал не будет включен или инициатором соединения по данному каналу не станет удаленный транспортный сервер (координатор). Если инициатором соединения станет удаленный клиент, то предназначенные ему конверты не отправляются, а этому клиенту передается специальная команда, которая выключает соответствующий канал в настройках его транспортного модуля (см. глоссарий, стр. 301).
- `call_flag` — признак немедленной передачи конвертов по каналам MFTP и SMTP. Возможные значения:
  - `yes` — попытка передачи конверта по каналу производится немедленно (по умолчанию для каналов обмена с координаторами).

- `no` — конверт остается в очереди до тех пор, пока в случае использования канала MFTP инициатором соединения не станет удаленный узел или в случае использования канала SMTP не будет вызван модуль MailTrans (по умолчанию для каналов обмена с клиентами).

Примечание. Если параметры `type`, `off_flag`, `call_flag` отсутствуют в секции, то используются их значения по умолчанию.

Нередактируемые параметры секции [channel] для каналов любого типа

- `id` — уникальный идентификатор сетевого узла ViPNet, с которым происходит обмен данными по каналу. Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`, например: `id = 0x270e000a`.
- `name` — имя сетевого узла ViPNet, с которым происходит обмен данными по каналу.

Кроме того, для каждого из типов каналов существуют специфические параметры, описанные ниже.

Специфические параметры для канала MFTP

Для канала MFTP в секции `[channel]` дополнительно задаются следующие параметры:

- `ip` — IP-адрес удаленного сетевого узла. Определяется управляющим демоном. Если значение этого параметра по каким-либо причинам не было получено от управляющего демона, то оно будет установлено в `0.0.0.0`. В этом случае его можно задать вручную, а затем перезапустить транспортный модуль. Данный параметр может изменяться в процессе работы.
- `call_timeout` — период опроса удаленного сетевого узла в секундах (время следующего опроса узла отсчитывается с момента разрыва последнего соединения с этим узлом). По умолчанию имеет значение 300, то есть опрос производится каждые 300 секунд. Если параметр `call_timeout` отсутствует, то используется его значение по умолчанию.

Нередактируемые параметры для канала MFTP

- `last_port` — порт, по которому осуществлялось последнее удачное MFTP-соединение. Этот порт будет использоваться при следующей попытке соединения с этим узлом.
- `last_call` — время последней попытки опроса канала.
- `last_err` — время, когда произошла последняя ошибка при попытке соединения или в процессе передачи данных.

Специфические параметры для канала SMTP

Для канала SMTP в секции `[channel]` дополнительно задаются следующие параметры:

- `maxsize` — максимальный размер почтового SMTP-конверта при отправке (в килобайтах). Используется в случае, если в параметре `version` данной секции установлена версия протокола `2.0`. При отправке MFTP-конверт разбивается на несколько SMTP-конвертов, размер каждого из которых не превышает заданный параметром `maxsize`. Возможные значения: от 100 до 2048000 (2 Гбайт). Значение `0` означает, что ограничение на размер SMTP-конвертов отсутствует.
- `reportaddress` — адрес электронной почты, на который будут отправляться исходящие конверты, в формате: `reportaddress = <имя пользователя>@<сервер>.<домен>`. Например: `reportaddress = user@example.com`
- `version` — версия протокола инкапсуляции конверта MFTP в почтовый конверт RFC-822, передаваемый по данному каналу. Возможные значения: `1.0` и `2.0`.

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала устранения неполадок транспортного модуля и содержит следующие параметры:

- `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`.

Секция [journal]

Секция `[journal]` содержит параметры настройки журнала MFTP-конвертов, обрабатываемых транспортным модулем. В процессе работы транспортный модуль записывает в этот журнал информацию о полностью принятых, отправленных, удаленных и поврежденных конвертах.

Просмотр журнала конвертов осуществляется с помощью команды `mftp view`.

Секция `[journal]` содержит следующие параметры:

- `dump_interval` — период выгрузки информации из журнала конвертов в днях. В процессе работы транспортный модуль записывает информацию об обработанных конвертах в текущий файл дампа. По истечении периода времени, заданного данным параметром, создается новый файл дампа, в имени которого содержится текущая дата. По умолчанию каждый день создается новый файл дампа (`dump_interval = 1`).
- `max_size` — максимальный размер файла журнала конвертов в мегабайтах (по умолчанию — `1`). Если размер текущего файла журнала превышает значение этого параметра, то новая информация будет записываться в этот файл на место информации, которая была записана раньше остальной. В случае изменения значения этого параметра, если размер этого файла превышает новое значение, то из него удаляется информация, которая была записана раньше остальной.
- `use_journal` — включение или выключение ведения журнала работы транспортного модуля. Возможные значения: `yes` (по умолчанию) или `no`.

Примечание. Если параметры `dump_interval`, `max_size`, `use_journal` отсутствуют в секции, то используются их значения по умолчанию.

Нередактируемые параметры секции [journal]

- `dump_filename` — префикс имени текстового файла, в который регулярно выгружается информация из журнала конвертов (файла дампа). Значение по умолчанию — `/var/log/mftpenv.log`.

  Постфикс имени этого файла определяется текущей датой и зависит от периода выгрузки информации (см. параметр `dump_interval` данной секции). Пример имени файла дампа: `/var/log/mftpenv.log.2015.09.23`.
- `last_dump` — время последней выгрузки информации из журнала конвертов.

Секция [mailtrans]

Секция `[mailtrans]` содержит параметры, отвечающие за взаимодействие транспортного модуля с модулем почтового обмена MailTrans.

Секция `[mailtrans]` содержит следующие параметры:

- `frommailbox` — адрес электронной почты отправителя SMTP-конвертов в формате:

  `frommailbox = <имя пользователя>@<сервер>.<домен>`
- `inputmailbox` — адрес электронной почты, по которому модуль почтового обмена будет забирать конверты по протоколу POP3, в формате:

  `inputmailbox = <имя пользователя>:<пароль>@<IP-адрес POP3-сервера>`
- `mailtrans_bin` — абсолютный путь к исполняемому файлу модуля почтового обмена (по умолчанию — `/sbin/mailtrans`).

- `mail_call_timeout` — период вызова модуля почтового обмена, то есть период опроса адреса электронной почты для входящих и исходящих конвертов по каналу SMTP. По умолчанию вызов не производится (`mail_call_timeout = -1`). Однако при наличии в очереди исходящих конвертов, предназначенных для отправки по каналу SMTP, вызов будет производиться, если это не запрещено параметром `call_flag` соответствующего канала.
- `mail_in_chunks_path` — абсолютный путь к каталогу, в который модуль почтового обмена помещает принятые фрагменты SMTP-конвертов в случае использования протокола версии 2.0 (см. Специфические параметры для канала SMTP на стр. 285). По умолчанию — `/opt/vipnet/smtpin/chunks`.
- `mail_in_path` — абсолютный путь к каталогу, в который модуль почтового обмена помещает принятые конверты. По умолчанию — `/opt/vipnet/smtpin`.
- `mail_out_path` — абсолютный путь к каталогу, в котором транспортный модуль формирует заголовочные файлы на отправляемые конверты. По умолчанию — `/opt/vipnet/smtpout`.
- `outputmailbox` — IP-адрес SMTP-сервера, на который модуль почтового обмена будет отправлять конверты по протоколу SMTP.
- maxsmtpsize — максимальный размер почтового SMTP-конверта при отправке (в мегабайтах). Если размер исходящего конверта превышает заданное значение, то конверт не отправляется и удаляется с записью в журнал устранения неполадок. Возможные значения: не ограничены. Отсутствие параметра означает, что ограничение на размер SMTP-конвертов отсутствует (по умолчанию).

Примечание. При отправке MFTP-конверт может разбиваться на несколько SMTP-конвертов, размер каждого из которых не превышает значение параметра `maxsize` из секции `[channel]`.

Секция [misc]

Секция `[misc]` содержит различные параметры, определяющие работу транспортного модуля в целом:

- `connect_timeout` — интервал времени в секундах, в течение которого клиент будет пытаться установить соединение с удаленным узлом по каналу MFTP (по умолчанию — `5`). Если по истечении этого времени соединение не установлено, то повторные попытки соединения будут производиться по истечении времени, указанного в параметре `outenv_timeout` данной секции.
- `max_connections` — максимальное количество входящих и исходящих соединений по каналам MFTP (по умолчанию — `900`).
- `max_listen_ports` — диапазон значений перебора портов для соединений по каналу MFTP с удаленным узлом в случае неудачи (по умолчанию — `3`). Транспортный модуль циклично перебирает порты в диапазоне от `port` до `port+max_listen_ports-1`. Ожидая входящие соединения, транспортный модуль прослушивает все порты указанного диапазона.

- `num_attempts` — количество последовательных попыток соединения, после которых устанавливается тайм-аут, если соединиться так и не удалось (по умолчанию — `3`).
- `outenv_timeout` — интервал времени в секундах, в течение которого исходящие конверты для канала, на котором произошла ошибка передачи, не могут быть повторно отправлены (по умолчанию — `300`). Если на каком-либо канале произошла ошибка передачи (например, из-за разрыва соединения) и для этого канала существуют исходящие конверты, то следующая попытка передачи произойдет по истечении времени, указанного в параметре `outenv_timeout`.
- `pingpong` — включение или выключение режима поочередного обмена конвертами по каналу MFTP. Возможные значения:
  - `yes` (по умолчанию) — сторона, передавшая конверт, позволяет передать конверт другой стороне, то есть узлы обмениваются конвертами поочередно.
  - `no` — сторона, начавшая передавать конверты, будет их передавать, пока они не закончатся, и только после этого позволит передавать конверты другой стороне.
- `port` — порт, на котором демон mftpd ожидает соединения по каналу MFTP от удаленных сетевых узлов (по умолчанию — `5000`).
- `recv_buff_size` — размер буфера приема в байтах. Значение по умолчанию — `65500`, минимально допустимое значение — `1024`.
- `send_buff_size` — размер буфера передачи в байтах. Значение по умолчанию — `65500`, минимально допустимое значение — `1024`.

Примечание. Обычно значение `65500` параметров `send_buff_size` и `recv_buff_size` оптимально для обеспечения максимальной скорости приема и передачи конвертов транспортным модулем.

- `save_sent` — включение или выключение хранения имен отправленных прикладных конвертов. Возможные значения:
  - `no` (по умолчанию) — имена отправленных конвертов не сохраняются;
  - `yes` — при успешной отправке конверта в подкаталоге `sent` каталога, указанного в параметре `out_path` секции `[transport]`, создается файл нулевой длины с именем отправленного конверта.
- `ttl_ctl` — время жизни конвертов, содержащих управляющие запросы, в исходящей очереди. Указывается в днях, значение по умолчанию — `10`. Если по истечении времени, указанного в параметре `ttl_ctl`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `ttl_out` — время хранения конвертов в исходящей очереди в днях. Значение по умолчанию — `30`. Если по истечении времени, указанного в параметре `ttl_out`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `ttl_trash` — время хранения конвертов в корзине в днях. Значение по умолчанию — `90`. Если время хранения конверта в корзине превышает указанное в параметре `ttl_trash`, то он удаляется.

- `wait_timeout` — время ожидания активности в установленном MFTP-соединении. Указывается в секундах, значение по умолчанию — `30`. Если в течение этого времени узлы, установившие соединение, не обменялись никакой информацией, то данное соединение закрывается. Если в процессе обмена исходящие конверты для удаленного узла были переданы не полностью, то повторные попытки соединения будут происходить по истечении времени, указанного в параметре `outenv_timeout`.

Секция [reserv]

Секция `[reserv]` содержит параметры настройки транспортного модуля на ViPNet xFirewall, работающем в составе кластера горячего резервирования:

- `cmd_port` — порт, на котором демон mftpd пассивного сервера ожидает соединений с активным сервером по резервному каналу для приема управляющих команд (по умолчанию — `6084`). Данный параметр должен иметь одинаковое значение в файлах конфигурации транспортного модуля на «активном» и «пассивном» серверах ViPNet xFirewall.
- `unpack_timeout` — период времени в секундах, в течение которого активный сервер будет ожидать ответы на команды от пассивного сервера, и в случае отсутствия ответов повторять команды (по умолчанию — `60`). Этот параметр используется системой удаленного обновления ПО. Он также определяет период сканирования каталога, заданного параметром `upgrade_path` секции `[upgrade]` (см. Секция [upgrade] на стр. 291), для анализа состояния процесса обновления ПО.
- `transfer_timeout` — период времени в секундах, в течение которого активный сервер будет пытаться передавать копии MFTP-конверта пассивному серверу в случае неполного дублирования данного конверта (по умолчанию — `60`). В течение этого времени обработка конверта на активном сервере блокируется. Если по истечении этого времени конверт не будет передан на пассивный сервер, то его обработка продолжится.
- `use_reserv` — включение или выключение режима резервирования конвертов в кластере горячего резервирования. Возможные значения:
  - `yes` (по умолчанию) — конверты резервируются.
  - `no` — резервирование конвертов не производится. В этом случае синхронизировать данные и обновление ПО на серверах кластера необходимо вручную. Кроме того, для корректной работы кластера настройки серверов кластера должны быть одинаковы.

Секция [transport]

Секция `[transport]` содержит ряд параметров, определяющих пути к транспортным каталогам, то есть к каталогам, участвующим в обмене конвертами и их обработке. Эти параметры задают лишь основные каталоги. Вспомогательные каталоги создаются транспортным модулем в процессе работы как подкаталоги основных. При создании конфигурационного файла значения параметров

этой секции определены по умолчанию относительно каталога, содержащего справочники и ключи.

Примечание. Транспортный модуль при каждом запуске проверяет наличие каталогов, заданных параметрами секции `[transport]`, и при необходимости создает их.

Секция `[transport]` содержит следующие параметры:

- `in_path` — абсолютный путь к каталогу, в который помещаются полностью принятые конверты (по умолчанию — `/opt/vipnet/in`).
- `out_path` — абсолютный путь к каталогу, в который внешние приложения помещают сформированные конверты для отправки (по умолчанию — `/opt/vipnet/out`).
- `trash_path` — абсолютный путь к каталогу, в который помещаются устаревшие конверты из очереди исходящих конвертов — так называемая «корзина» (по умолчанию — `/opt/vipnet/trash`).
- `local_path` — абсолютный путь к каталогу, в который помещаются прикладные конверты, предназначенные для передачи по локальному каналу другим узлам сети ViPNet (по умолчанию — /`opt/vipnet/local`). Данный параметр не используется в ViPNet xFirewall.
- `app_in_path` — абсолютный путь к каталогу, в который помещаются файлы, полученные от других узлов сети ViPNet (по умолчанию — /`opt/vipnet/in/app`). Данный параметр не используется в ViPNet xFirewall.

Секция [upgrade]

Данная секция содержит параметры, которые определяют поведение транспортного модуля при приеме обновлений ПО ViPNet из программы ViPNet Центр управления сетью:

- `confsave` — тип конфигурации, автоматически создаваемой перед обновлением. Возможные значения:
  - `partial` (по умолчанию) — частичная конфигурация, включающая только конфигурационные файлы (без справочников и лицензии).
  - `full` — полная конфигурация, включающая конфигурационные файлы, справочники и лицензию.
  - `off` — конфигурация не создается автоматически.
- `maxautosaves` — максимальное число автоматически сохраненных конфигураций. Возможные значения: от 1 до 10. Значение по умолчанию — `10`. Перед автоматическим созданием очередной конфигурации проверяется число ранее сохраненных конфигураций. Если это число равно значению `maxautosaves`, то конфигурация, созданная раньше остальных, удаляется, после чего сохраняется текущая конфигурация.
- `upgrade_checktimeout` — период проверки транспортного каталога, заданного параметром `upgrade_path`, на наличие файлов обновления программного обеспечения. Указывается в

секундах, значение по умолчанию — `300`. В случае соответствия обнаруженных файлов обновления (время обновления и так далее) вызывается модуль обновления.

- `upgrade_for_kc_path` — абсолютный путь к каталогу, в который внешние приложения помещают файлы `*.sok` с запросами на сертификаты (по умолчанию — `/opt/vipnet/ccc/for_kc`).
- `upgrade_ini` — имя конфигурационного файла для процесса обновления (по умолчанию — `/opt/vipnet/user/upgrade.conf`).
- `upgrade_path` — абсолютный путь к каталогу, в который помещаются файлы обновления программного обеспечения после распаковки соответствующих конвертов (по умолчанию — `/opt/vipnet/ccc`).

A

Глоссарий

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-сервер

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

DNS-сервер

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

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

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. 294).

IP-пакет

Форматированный блок информации, передаваемый в сети по протоколу IP.

IP-трафик

Поток данных, передаваемых в сети по протоколу IP.

IP-форвардинг

IP-форвардинг или маршрутизация транзитных IP-пакетов (не предназначенных для этого компьютера), является опциональной возможностью стека протоколов TCP/IP в операционной системе GNU/Linux. Данная функция обеспечивает пересылку транзитных IP-пакетов через сетевые интерфейсы компьютера.

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. 294).

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.

NUT (Network UPS Tools)

Пакет программ для управления и мониторинга работы источника бесперебойного питания (UPS).

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.

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.

WINS-сервер

Сервер, выполняющий сопоставление NetBIOS-имен компьютеров с IP-адресами узлов.

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.

Административная дистанция

Характеристика маршрута (см. глоссарий, стр. 298). Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

Адреса доступа

IP-адреса, по которым узел доступен в сети (например, адреса межсетевого экрана, за которым он находится).

Антиспуфинг

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

Базовый виртуальный адрес

Базовый виртуальный адрес является точкой отсчета при назначении виртуальных адресов для каждого из реальных адресов узла. Если в данный момент узел виден по виртуальному адресу, то его адресом доступа считается либо базовый виртуальный адрес, либо вторичный виртуальный адрес, соответствующий первому в списке реальному адресу.

Вес

Параметр, который задается для шлюза в статическом маршруте (см. глоссарий, стр. 298) 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.

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.

Внешние IP-адреса

Адреса внешней сети.

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Дуплекс

Способ связи, при котором сетевой интерфейс может одновременно и передавать, и принимать информацию.

Инкапсуляция пакетов

Принцип передачи данных, при котором данные в формате одного протокола упаковываются в формат другого протокола.

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 свои функции (маршрутизатора, прокси-сервера и так далее), а другой сервер (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet 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.

Командный интерпретатор

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

Координатор (ViPNet-координатор)

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

Маршрут

Путь следования IP-трафика при передаче в сети от одного узла другому.

Маршрут по умолчанию

Путь следования IP-пакетов, для которых не был найден подходящий маршрут в таблице маршрутизации.

Маршрутизатор-сосед

OSPF-маршрутизатор, находящиеся в одной области маршрутизации с другими маршрутизаторами этого типа.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Метрика адреса доступа

Определяет задержку (в миллисекундах) отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса. Предназначена для задания приоритета использования каналов связи.

Метрика маршрута

Предназначена для задания приоритета маршрута передачи IP-трафика.

Область маршрутизации

Одна или несколько IP-сетей, в которых осуществляется обмен информацией по определенному протоколу, в частности, по протоколу OSPF (см. глоссарий, стр. 295).

Протокол OSPF рассматривает межсетевую среду как множество областей, соединенных друг с другом через некоторую базовую область (backbone area). Для идентификации областей каждой из них выделяется специальный идентификатор (area ID), представляющий собой 32-разрядное число, которое записывается так же, как и IP-адрес — в десятично-точечном формате (в виде четырех однобайтовых чисел, разделенных точками).

Обычная консоль

Монитор и клавиатура, которые используются для локальной настройки ViPNet xFirewall.

Перераспределение маршрутов

Обмен маршрутной информацией между двумя различными маршрутизирующими протоколами.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

Полудуплекс

Способ связи, при котором сетевой интерфейс в один момент времени может только передавать или только принимать информацию.

Прикладная квитанция

Файл, оповещающий отправителя о доставке и (или) прочтении прикладного конверта.

Прикладной конверт

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

Прозрачный режим работы прокси-сервера

Режим работы, при котором не требуется выполнять настройку программного обеспечения на рабочих местах пользователей, подключающихся к Интернету через прокси-сервер.

Прокси-сервер

Программа, транслирующая соединения по некоторым протоколам из внутренней сети во внешнюю и выступающая при этом как посредник между клиентами и сервером.

Реальный IP-адрес

IP-адрес, назначенный сетевому интерфейсу компьютера в локальной сети или Интернете.

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN (см. глоссарий, стр. 295).

Сетевой узел ViPNet

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

Сетевой фильтр

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

Сеть ViPNet

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

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

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники и лицензия

Справочники, ключи узла и ключи пользователя.

Статический сетевой интерфейс

Сетевой интерфейс (см. глоссарий, стр. 300), для работы которого требуется задать секцию `[adapter]` в файле `iplir.conf` с описанием параметров этого интерфейса. К таким интерфейсам относятся физические (Ethernet) и виртуальные (VLAN) интерфейсы.

Стоимость маршрута

Количество издержек, которые возникнут при отправке IP-пакета в сеть назначения через тот или иной шлюз. Стоимость маршрута обратно пропорциональна его пропускной способности канала связи.

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных в сети.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки конверта.

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.

Файл подкачки

Файл подкачки представляет собой дополнительную виртуальную память, которая позволяет увеличить объем памяти, доступной для использования на компьютере.