ViPNet xFirewall 5

Справочник команд и конфигурационных файлов

Версия продукта: 5.6.1

ViPNet xFirewall xF100
ViPNet xFirewall xF5000
ViPNet xFirewall xF1000 C, D
ViPNet xFirewall xF-VA

infotecs

ФРКЕ.465614.002ИС3

Версия продукта 5.6.1

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Документ содержит описание команд, доступных для выполнения в командном интерпретаторе ViPNet xFirewall. В нем приведены синтаксис команд, руководство по использованию, а также примеры команд. Команды сгруппированы по первому ключевому 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 управляющей службы.
- `iplir.conf-<интерфейс или группа интерфейсов>` — конфигурационные файлы сетевых интерфейсов ViPNet xFirewall.
- `failover.ini` — конфигурационный файл системы защиты от сбоев.
- `mftp.conf` — конфигурационный файл транспортного сервера MFTP.

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

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

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

Обозначения при описании команд в документе:

- Команды, которые участвуют в сценарии администратора, обозначены символом `#`

  ```
  hostname# admin config list
  ```

- Команды, которые участвуют в сценарии пользователя, обозначены символом `>`

  ```
  hostname> firewall local show
  ```

  Все команды, которые доступны пользователю, доступны и администратору.

- Параметры заключены в угловые скобки:

  ```
  inet bonding delete <номер>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки:

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

- Допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:

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

Обратная связь

Контактная информация

- Единый многоканальный телефон:

  +7 (495) 737-6192,

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

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телеграм-канал поддержки: t.me/vhd21

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- О продуктах ViPNet.
- О решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

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

1

Справочник команд

Команды группы admin

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

admin config delete

Удалить копию конфигурации.

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`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе имени работают автодополнение 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

Просмотреть список сохраненных копий конфигурации.

Синтаксис

```
admin config list
```

Режимы командного интерпретатора

Администратор.

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

Загрузить (восстановить) настройки ViPNet xFirewall из копии конфигурации.

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`.

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 введите имя, под которым будет сохранена копия текущей конфигурации.
- Если текущая версия vpn-компонента ниже версии, указанной в команде, то дополнительно подтвердите загрузку настроек из копии конфигурации.

Пример использования

Чтобы загрузить настройки из копии конфигурации с именем Rollback_config, относящейся к версии 5.5.0:

```
hostname# admin config load Rollback_config 5.5.0
```

admin config save

Сохранить копию текущей конфигурации.

Синтаксис

```
admin config save <имя>
```

Параметры и ключевые слова

`<имя>` — имя копии конфигурации.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды рекомендуется остановить службы `iplircfg`, `failoverd` и `mftpd`, выполнив команду:

  ```
  hostname# vpn stop
  ```

- 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

Выйти в системную командную оболочку.

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

Синтаксис

```
admin escape
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе команды автодополнение не работает.
- После выполнения команды требуется ввести пароль администратора сетевого узла ViPNet.
- Для возвращения в командный интерпретатор ViPNet xFirewall введите команду `exit`. После чего командный интерпретатор продолжит свою работу с того момента, в котором он находился перед выходом в системную оболочку.

Пример использования

```
hostname# admin escape
This command is intended only for debugging.
```

```
It should be used only by InfoTeCS support team or people who
 were explicitly advised by InfoTeCS support team to use it.
InfoTeCS does not guarantee normal operation of Platform: ViPNet xFirewall VA
 in case of incorrect user actions in the system shell.
Are you sure you want to exit to the Linux system shell?[Yes,No]:Yes
Type the administrator password:
sh-4.4#
```

admin export-and-clear logs

Экспортировать файлы системного журнала на другой компьютер (по TFTP) или на USB-носитель с последующим удалением их с ViPNet xFirewall.

Синтаксис

```
admin export-and-clear logs {tftp | usb}
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды рекомендуется остановить службы `iplir`, `failoverd` и `mftpd`, выполнив команду:

  ```
  hostname# vpn stop
  ```

- 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 системного журнала можно только на USB-носитель.

Пример использования

```
hostname# admin export-and-clear logs usb
```

```
Are you sure to export and remove logs?. Do you Want to continue? [Yes/No] : Yes
Packing of log files in progress. Press ^+C to abort.
Stopping system log daemon: syslog
```

```
Please insert the USB flash drive and press Yes to continue [Yes/No] : Yes
Put logs.tar.gz file onto USB drive.
Insert USB drive and press Enter
1) JetFlash Transcend 32GB partition 30639Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc1 as vfat
Partition /dev/sdc1 was successfully mounted on /usb.
File logs.tar.gz to be copied onto the USB drive. Press ^+C to abort.
File logs.tar.gz was successfully copied onto the USB drive.
You may remove the USB drive.
Logs exported and removed from ViPNet xFirewall successfully.
Starting system log daemon: syslog
hostname#
```

admin export keys binary-encrypted

Экспортировать справочники, лицензии и настройки 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.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Экспортировать справочники, лицензию и настройки в удаленной SSH-сессии запрещено.
- Перед выполнением команды требуется завершить работу служб `iplircfg` (см. iplir stop) и `mftpd` (см. mftp stop).
- Если вы выбрали экспорт по TFTP и на ViPNet xFirewall запущен DHCP-сервер, 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.
```

admin export logs

Экспортировать файлы системного журнала на другой компьютер (по TFTP) или USB-носитель.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо остановить службы iplircfg (см. iplir stop) и mftpd (см. mftp stop).
- 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.
- В удаленной SSH-сессии экспортировать файлы журнала по протоколу TFTP запрещено.
- Имя файла экспорта — `logs.tar.gz`.
- Если ViPNet xFirewall работает в составе кластера горячего резервирования, экспортировать файлы системного журнала можно только на USB-носитель.
- При просмотре архива журнала в Windows время создания архива может отличаться от реального времени. При этом время событий в журналах будет правильным. Это связано с особенностями работы разных ОС с системным временем.

Пример использования

Пример выполнения команды с параметром `usb`:

```
hostname# admin export logs usb
Stopping system log daemon: syslogd.
tar: Removing leading `/' from member names
/var/log/dmesg.boot
/var/log/everything.log
/var/log/integrity.log
/var/log/iphook.log
/var/log/lastlog
/var/log/vipnet_error.log
/var/log/vmware-vmsvc.log
/var/log/webgui-fcgi-server.log
/var/log/wtmp
/var/log/wtmp.1
/mnt/main/etc/probed_hw.txt
Starting system log daemon: syslogd.
Put logs.tar.gz file onto USB drive.
Insert USB drive and press Enter
1) JetFlash Transcend 32GB partition 30639Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc1 as vfat
Partition /dev/sdc1 was successfully mounted on /usb.
Copying files logs.tar.gz to /dev/sdc1. Press ^+C to abort.
File logs.tar.gz to be copied onto the USB drive.
You may remove the USB drive.
```

admin export packetdb usb

Экспортировать журнал регистрации IP-пакетов на USB-носитель.

Синтаксис

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

Параметры и ключевые слова

`<имя>` — имя файла экспорта.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При удаленном подключении по протоколу SSH установите в настройках SSH-клиента тип терминала VT100+.

- Перед экспортом сохраните журнал IP-пакетов в файл (см. iplir view).
- При вводе имени файла работает автодополнение и подсказка, данные для подсказки берутся из списка существующих файлов экспорта.

Пример использования

Чтобы экспортировать файл `ippacket`, в который сохранены записи журнала IP-пакетов:

```
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.
```

admin kick

Завершить сессию 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 узле, подключенном к ViPNet xFirewall по протоколу SSH.

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).
- Для просмотра информации обо всех запущенных сессиях командного интерпретатора используется команда `who` (см. who).

Пример использования

Чтобы завершить работу командного интерпретатора на компьютере tty1:

```
hostname# admin kick tty1
```

admin passwd

Изменить пароль пользователя ViPNet xFirewall.

Синтаксис

```
admin passwd
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды требуется ввести текущий пароль пользователя или пароль администратора, затем дважды ввести новый пароль для пользователя.
- При вводе пароля на экране не отображаются вводимые символы, а курсор остается неподвижным.
- Минимальная длина пароля — 6 символов.

Совет. Задавайте сложные пароли, содержащие не менее 8 символов.

- Чтобы изменить пароль пользователя на ViPNet xFirewall, работающих в режиме кластера горячего резервирования, выполните команду сначала на узле, функционирующем в пассивном режиме, а затем на узле, функционирующем в активном режиме. Пароли, задаваемые на обоих узлах, должны совпадать.

Пример использования

```
hostname# admin passwd
Enter either the current user password or the current administrator password:
Type the new user password:
Confirm the new user password:
The new password has been successfully set.
Dumping data files...
Data files were dumped successfully
```

admin remove keys

Удалить лицензию и справочники ViPNet xFirewall.

Синтаксис

```
admin remove keys
```

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,
You will need to deploy keys anew after executing this command.
Are you sure you want 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 ssh reset-key

Удалить отпечатки SSH-ключей, хранящиеся локально на ViPNet xFirewall.

Синтаксис

```
admin ssh reset-key {host <адрес> | id <идентификатор>}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сервера, чей отпечаток SSH-ключа необходимо удалить.
- `<идентификатор>` — идентификатор сервера, чей отпечаток SSH-ключа необходимо удалить.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для параметра `id` при двойном нажатии **Tab** выводится подсказка со списком всех идентификаторов серверов, с которыми есть связи.

Пример использования

Чтобы удалить отпечаток SSH-ключа для сервера `ssh.domain.com`:

```
hostname# admin ssh reset-key host ssh.domain.com
```

admin ssh show-key

Просмотреть информацию об SSH-ключах, хранящихся локально на ViPNet xFirewall.

Синтаксис

```
admin ssh show-key {host <адрес> | id <идентификатор> | local}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сервера, чей отпечаток SSH-ключа необходимо просмотреть.
- `<идентификатор>` — идентификатор сервера, чей отпечаток SSH-ключа необходимо просмотреть.
- `local` — просмотр информации о ключах локального SSH-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Для параметра `id` при двойном нажатии **Tab** выводится подсказка со списком всех идентификаторов серверов, с которыми есть связи.
- В результате выполнения команды выводится:
  - `Key type` — тип ключа:
    - `ssh-dsa(ssh2)` — SSH-ключ, сгенерированный с использованием алгоритма dsa;
    - `ssh-rsa(ssh2)` — SSH-ключ, сгенерированный с использованием алгоритма rsa;
  - `Fingerprint` — отпечаток SSH-ключа;

- `Public key` — открытый SSH-ключ.

Пример использования

Чтобы просмотреть информацию о ключах локального SSH-сервера:

```
hostname# admin ssh show-key local

command: admin ssh show key local

Local host ssh public keys:

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

Key type: ssh-dsa(ssh2)

Fingerprint: SHA256:Q5/e7nofhVTre1K72AWf0V0K1FxqUysfVxMQP0PnIuw

Public key:
AAAAB3NzaC1kc3MAAACBAOiitldq9nRVKx72gOR4nVVPotoAdjJvgJRbYs9mLvJdmypb4Y+JvG8GLQZvODJCnI
KzWLJ2eUJi5/iVTOfBwHt9oXo+W+K4JaVwUaQq0uEHj6YbhPk6mIlV+TIBfCbSP5r9quQCFdnn4IKcVng7rVKu
dl8geMKW0GQGrOtZl9pRAAAAFQC2iqrroLE+zS6qmAkM2x/iOCzeiQAAAIEAxBbdKDITOtJDNykwYuCPnCgWZu
jXz0oUUxAOsp+dVYcsnevRN6IiM51gTAUDRR5AKPkY7M5ma3EOXAZTrdKj+Y7NePt4smEQQat93L+nKgoNDjf+
oUnQFh07XkK0eydX3/xCO0M+pn/VvICDjXP6DdpDmXr01Gy389wakaqHZX4AAACBAJYC9XgjKgnLRcKjmSVLuA
/yZ/YFk3P0LJUmSRe4yzV16v2uLlRH8rEfTGVllMWuDX47ZmRhpemoM3QbvkFAFMBkmbqZzrn8nFARLAoP1syS
2CO3gaEFkmeQ/d7rL7HRq05tH2e4gUX2ZxWJQHNYgprj8r5gKPWyN6zBCRJ0GF8U

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

Key type: ssh-rsa(ssh2)

Fingerprint: SHA256:Txn8IloRmfAbD+l/F6/UWah4DfwGu2cKXDGiDE5VXQk

Public key:
AAAAB3NzaC1yc2EAAAADAQABAAABAQDgRfTwzDnmxg3GCofsWFqOlh96opUuTz1zkPA1c70ncnyNtkW6kmaeXx
MU3EM7r/yf3/e/U6JH5Pkc6bWcYbU70tEBy3db9ZDY/QdOBZdijIagUuWyiiHqAEWwC1vCXqQ1/0AZwh71DKTD
PFI0cImTC3ahMJMtvl/X7SnWJVxVz3AMBqXnTqjMXOpHDXQnAgPw4kcTNqZMNT1OOvaYmcCGZ6Tko7HPygy1n+
ZUV/GajAlwTmCfKr0DT/O3ebi9OF7SK6A5eJeGCVBRv2BdOhL/uWzuaMSP6vMk+hiWkX0lNl6iOUIo4PCHW8kH
m6FcaJAmG0MKVw8M2dDo0osTtUhz

----------------------------------------------------------------
```

admin upgrade dpi usb

Обновить модуль DPI вручную с USB-носителя.

Синтаксис

```
admin upgrade dpi usb
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Выполнять команду необходимо только при подключении к ViPNet xFirewall через COM-консоль или обычную консоль. 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

Обновить ПО ViPNet xFirewall вручную с USB-носителя.

Синтаксис

```
admin upgrade software usb
```

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
```

Команды группы alg

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

Внимание! Для команд группы `alg` контекстная справка не поддерживается.

alg module process off

Выключить обработку 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`.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы выключить обработку прикладного протокола `ftp`:

```
hostname# alg module ftp process off
Alg module ftp protocol off operation is successfully
```

alg module process on

Включить обработку прикладного протокола FTP, H.323, SCCP или SIP, либо изменить параметры 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.

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
Alg module ftp protocol on operation for 20-21, 26 port(s) is successfully
```

alg show

Просмотреть текущие параметры обработки прикладных протоколов.

Синтаксис

```
alg show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> alg show
==================================================
```

```
SERVICE    PROTOCOL PORTS        ON/OFF
=================================================
FTP      TCP   21          ON
-------------------------------------------------
DNS      UDP   53          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

Настройка и управление системой защиты от сбоев ViPNet xFirewall.

failover config edit

Редактировать конфигурационный файл системы защиты от сбоев.

Синтаксис

```
failover config edit
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде будет запущен текстовый редактор с конфигурационным файлом failover.ini.
- После изменения файла `failover.ini` перезапустите службу `failoverd` с помощью команд failover stop и failover start.

Пример использования

```
hostname# failover config edit
GNU nano 2.3.6   File: /etc/failover.ini
[network]
checktime = 10
timeout = 2
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes
...

The file failover.ini is changed
Changes will be applied after restart of Failover daemon
```

failover config mode

Изменить режим работы системы защиты от сбоев.

Синтаксис

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

Параметры и ключевые слова

- `single` — одиночный режим.
- `cluster` — режим кластера.

Значения по умолчанию

Установлен одиночный режим (`single`).

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы установить режим кластера:

```
hostname# failover 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
```

failover show config

Просмотреть файл конфигурации системы защиты от сбоев.

Синтаксис

```
failover show config
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Чтобы завершить просмотр файла конфигурации нажмите **Q**.

Пример использования

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

failover show info

Просмотреть информацию о состоянии системы защиты от сбоев.

Синтаксис

```
failover show info
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде отображается следующая информация:

- версия ПО ViPNet xFirewall и версия службы `failoverd`;
- информация о сетевом узле;
- локальное время на узле;

- режим работы системы защиты от сбоев;
- информация об использовании процессора и оперативной памяти;
- информация о текущем состоянии управляющей службы, служб `mftpd`, `failoverd`, веб-интерфейса и управления пользователями.

Пример использования

```
hostname> failover show info
Running failover info

Versions: ViPNet 5.6.1 (95), daemon 1.5 (1)

Workstation configured for ID 16410156 (xf-va-ips)

The workstation works in a single mode of protection against failures

Workstation time (utc: 1560071660) Sun Jan 9 12:14:20 2022


failover mode  * single

failover uptime * 12d 21:23

total cpu    * 0%

total memory   * 4050324 kB

available memory * 119356 kB

failover state  * works

failover cpu   * 0%

iplir state   * works

iplir cpu    * 0%

mftp state    * works

mftp cpu     * 0%

webgui state   * works

webgui cpu    * 0%
  uc state     * stopped
```

failover start

Запустить службу `failoverd`, отвечающую за работу системы защиты от сбоев.

Синтаксис

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

Параметры и ключевые слова

- `active` — запустить службу в активном режиме (в кластере горячего резервирования).
- `passive` — запустить службу в пассивном режиме (в кластере горячего резервирования).

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, служба `failoverd` будет запущена в том режиме, в котором она находилась до завершения работы.
- Перед запуском службы `failoverd` в активном режиме убедитесь, что на другом ViPNet xFirewall кластера служба `failoverd` запущена в пассивном режиме. Запуск службы `failoverd` в активном режиме на обоих узлах кластера приведет к конфликту IP-адресов и другим нежелательным последствиям.

Пример использования

Чтобы запустить службу `failoverd` в пассивном режиме:

```
hostname> failover start passive
```

failover stop

Завершить работу службы `failoverd`, отвечающей за работу системы защиты от сбоев.

Синтаксис

```
failover stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

failover view

Просмотреть журнал 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.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Команда доступна только в режиме кластера горячего резервирования.
- Чтобы завершить просмотр журнала нажмите **Q**.

Пример использования

```
hostname> failover view 09.03.2022.08.00.00 23.03.2022.19.00.00
  View journal of failover switching
  Versions: ViPNet 5.6.1 (204), daemon 1.5 (1)
  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 2022

  09 Mar 2022 12:51:42     <P_START> Start failover daemon in passive mode
  22 Mar 2022 12:27:27     <A_START> Start failover daemon in active mode
  22 Mar 2022 14:10:35     <A_START> Start failover daemon in active mode
  22 Mar 2022 15:30:46     <BOOT> Boot the system
23 Mar 2022 11:09:07       <SWITCH> Switch server from passive mode to active mode
```

Команды группы firewall

Команды группы `firewall` предназначены для работы с сетевыми фильтрами, правилами трансляции адресов и группами объектов.

Внимание! Для команд группы `firewall` контекстная справка не поддерживается.

firewall add

Создать сетевой фильтр или правило трансляции адресов.

Синтаксис

```
firewall <тип> add [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя>
[url <адрес> [type <mime>] [mthd <http-метод>]] [<транспортный протокол>] [<расписание>]
[dpiapp <приложение>] [dpiprotocol <прикладной протокол>] [dpigroup <группа приложений>]
[dnuser <пользователь>] [ssl {decrypt|bypass}] [ips {on|off}] [av {on|off}] <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.
- `<url-адрес>` — url-адрес ресурса (для контентных фильтров).
  - `<mime-тип>` — mime-тип передаваемых данных.
  - `<http-метод>` — метод http-запроса (CONNECT, DELETE, GET, HEAD, OPTIONS, POST, PUT, TRACE).

- `<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).
- `ssl` — расшифровка трафика SSL/TLS-сессий (для транзитных фильтров открытой сети):
  - `decrypt` — расшифровывать трафик;
  - `bypass` — пропускать трафик без расшифровки;
- `ips` — проверка трафика подсистемой IPS (для транзитных фильтров открытой сети):
  - `on` — включить.
  - `off` — выключить.
- `av` — проверка трафика антивирусом (для транзитных фильтров открытой сети):
  - `on` — включить.
  - `off` — выключить.
- `<действие>` — действие с IP-пакетами, соответствующими условиям фильтра (правила трансляции).

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 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>}}
  ```

- Для правил трансляции адресов при задании адреса отправителя или получателя можно указывать, соответственно, входящий (`src`) или исходящий (`dst`) интерфейсы собственного узла в виде:

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

  при этом:

  - в одном правиле трансляции нельзя указывать одновременно и входящий и исходящий интерфейсы;
  - для правил с трансляцией адреса назначения можно указать только входящий интерфейс;
  - для правил с трансляцией адреса источника можно указать только исходящий интерфейс.

- 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 «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 «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 «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.

- `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. Если сессия была открыта до начала действия расписания, то она будет работать до момента ее завершения. Например, в сетевом фильтре, разрешающем работу по протоколу RDP, задано расписание с 9:00 до 20:00. В этом случае пользователь, открывший RDP-сессию до 20:00, сможет работать в ней и после 20:00 до тех пор, пока она не будет завершена. После этого пользователь уже не сможет открыть новую RDP-сессию.

- Действие задается одной из следующих лексем:
  - для сетевых фильтров:
    - `pass` — пропускать IP-пакеты;
    - `drop` — блокировать IP-пакеты.
  - для сетевых фильтров при необходимости отклонить IP-пакеты с отправкой ICMP-сообщения об ошибке:
    - `reject` — отправляет сообщение `Destination port unreachable`;
    - `rej-net-unreachable` — отправляет сообщение `Destination net unreachable`;
    - `rej-host-unreachable` — отправляет сообщение `Destination host unreachable`;
    - `rej-proto-unreachable` — отправляет сообщение `Destination protocol unreachable`;
    - `rej-net-prohibited` — отправляет сообщение `Network administratively prohibited`;
    - `rej-host-prohibited` — отправляет сообщение `Host administratively prohibited`;
    - `rej-admin-prohibited` — отправляет сообщение `Communication administratively prohibited`;
    - `rej-tcp-reset` — отправляет сообщение `TCP reset` (только для TCP-пакетов);

Внимание! При создании сетевых фильтров нельзя задавать блокировку IP-пакетов с отправкой ICMP-сообщения совместно с параметрами, задающими фильтрацию по пользователю, приложению или прикладному протоколу. Такие параметры задаются следующими лексемами: `dpiapp, dpiprotocol, dpigroup, dnuser`.

- 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 «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:

  ```
  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:

  ```
  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:

  ```
  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`:

  ```
  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`:

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

- Чтобы создать локальный фильтр, блокирующий все IP-пакеты, отправляемые на порт 3128 по протоколу TCP/IP с отправкой icmp-уведомления `destination host unreachable`:

  ```
  hostname# firewall local add src @any dst @any tcp dport 3218 rej-host-unreachable
  ```

- Чтобы создать транзитный фильтр, разрешающий отправку трафика с любого узла узлу с адресом 192.168.2.4 без расшифровки трафика SSL/TLS-сессий:

  ```
  hostname# firewall forward add src @any dst 192.168.2.4 pass
  ```

- Чтобы создать транзитный фильтр, разрешающий трафик узла с адресом 192.168.30.1 через порт 2525 на порт 443 узла с адресом 172.16.35.1 по протоколу TCP/IP и применяющий к нему расшифровку SSL/TLS-сессий:

  ```
  hostname# firewall forward add src 192.168.30.1 dst 172.16.35.1 tcp sport 2525 dport 443 ssl decrypt pass
  ```

firewall add name

Создать группу 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;
  - `service-object` — протоколы;
  - `schedule-object` — расписания.
- `<имя>` — имя группы объектов.
- `<состав>` — объекты, входящие в группу.
- `<исключения>` — объекты, не входящие в группу.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Имя группы объектов должно быть уникальным и не должно содержать пробелов и символов «"».
- Сетевые интерфейсы разделяйте пробелом, и перед именем каждого сетевого интерфейса укажите слово `interface`.
- Синтаксис протокола и расписания — тот же, что при создании сетевого фильтра или правила трансляции адресов с помощью команды firewall add.

Примеры использования

- Чтобы создать группу IP-адресов, содержащую сегмент сети за исключением нескольких IP-адресов:

  ```
  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, содержащую выходные дни с 9 до 23 часов:

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

- Чтобы создать группу сетевых интерфейсов, содержащую интерфейсы `eth0` и `eth1`:

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

firewall change append

Добавить адрес отправителя, адрес получателя, протокол или расписание 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>] [<расписание>] [dpiapp <приложение>] [dpiprotocol
<прикладной протокол>] [dpigroup <группа приложений>] [dnuser <пользователь>]
```

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).

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.
- 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 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:

  ```
  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:

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

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

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

firewall change replace

Заменить значения параметров сетевого фильтра: адрес отправителя, адрес получателя, транспортного протокола или расписания. Для транзитных фильтров открытой сети также можно:

- заменить:
  - адрес ресурса и параметры контент-фильтрации;
  - приложение;
  - прикладной протокол;
  - группу приложений;
  - пользователя Active Directory или LDAP-сервера;
- включить или выключить:
  - расшифровку трафика SSL/TLS-сессий;
  - проверку трафика подсистемой ips или антивирусом.

Синтаксис

```
firewall <тип> change replace <номер> [rule <имя>] [src <адрес отправителя>] [dst <адрес получателя>] [url <адрес> [type <mime>] [mthd <метод>]] [<транспортный протокол>] [<расписание>] [dpiapp <приложение>] [dpiprotocol <прикладной протокол>] [dpigroup <группа приложений>] [dnuser <пользователь>] [ssl {decrypt|bypass}] [ips {on|off}] [av {on|off}]
```

Параметры и ключевые слова

- `<тип>` — тип 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>` — адрес отправителя IP-пакетов.
- `<адрес отправителя>` — адрес получателя IP-пакетов.
- `<url-адрес>` — url-адрес ресурса (для контентных фильтров).
  - `<mime-тип>` — mime-тип передаваемых данных.
  - `<http-метод>` — метод http-запроса (CONNECT, DELETE, GET, HEAD, OPTIONS, POST, PUT, TRACE).
- `<транспортный протокол>` — 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).
- `ssl` — расшифровка трафика SSL/TLS-сессий(для транзитных фильтров открытой сети):
  - `decrypt` — расшифровывать трафик;
  - `bypass` — пропускать трафик без расшифровки;
- `ips` — проверка трафика подсистемой IPS (для транзитных фильтров открытой сети):
  - `on` — включить.
  - `off` — выключить.
- `av` — проверка трафика антивирусом (для транзитных фильтров открытой сети):
  - `on` — включить.
  - `off` — выключить.

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.
- 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

Чтобы в локальном фильтре открытой сети с порядковым номером 8 заменить адрес отправителя и расписание:

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

Чтобы заменить тип трафика с текущего на video/mpeg контент-фильтрации с ресурса facebook.com в фильтре с порядковым номером 12:

```
hostname# firewall forward change replace 12 url facebook.com type video/mpeg
```

Чтобы включить антивирусную проверку трафика фильтром с порядковым номером 10:

```
hostname# firewall forward change replace 10 av on
```

firewall delete

Удалить сетевой фильтр или правило 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.

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.
- 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

Чтобы удалить локальный фильтр открытой сети с номером 7:

```
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? [Yes/No]:
```

firewall move rule

Изменить порядковый номер (приоритет) 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).

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):

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

firewall object delete

Удалить группу объектов с заданным именем.

Синтаксис

```
firewall object delete @<имя>
```

Параметры и ключевые слова

`<имя>` — имя группы объектов.

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 сначала удалите эти фильтры, правила и группы, а затем выполните команду для удаления группы еще раз.
- Для команды не поддерживается автодополнение.

Пример использования

Чтобы удалить группу объектов с именем `IP_group`:

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

firewall object show

Просмотреть все группы объектов.

Синтаксис

```
firewall object show
```

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

Просмотреть все сетевые фильтры и правила трансляции адресов.

Синтаксис

```
firewall rules show [{pass | drop | reject}]
```

Параметры и ключевые слова

- `pass` — будут выведены все сетевые фильтры, для которых в параметре <действие> задано значение `pass`.
- `drop` — будут выведены все сетевые фильтры, для которых в параметре <действие> задано значение `drop`.
- `reject` — будут выведены все сетевые фильтры, для которых в параметре <действие> задано значение `reject`.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Для завершения просмотра используется клавиша **Q**.
- Если параметр не указан, будут выведены все сетевые фильтры и правила трансляции адресов.
- Каждый тип сетевых фильтров и правила трансляции адресов выводятся в отдельной таблице, содержащей следующие столбцы:
  - `Num` — порядковый номер фильтра (правила трансляции) в таблице.
  - `Rule ID-Name` — идентификатор и 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
 Service Local Rules:
Current Rules Set Id: 25
================================================================================
Num  Rule ID-Name                 Option Schedule
Act  Protocol        Source        ->Destination
   DpiProtocol      [G]DpiGroup, DpiApp  DomainUser
================================================================================
1   100001 - Allow DHCP              Generated
pass Service        @any         ->@any
   udp:
    from 67                  @any
    to 68         @any
   @any
--------------------------------------------------------------------------------
2   100002 - ViPNet Service            Generated
drop Common Out       @local        ->@any
   tcp/udp:                  @any
    from 2046       @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 drop
 Service Local Rules:
Current Rules Set Id: 25
================================================================================
Num  Rule ID-Name                 Option Schedule
Act  Protocol        Source        ->Destination
   DpiProtocol      [G]DpiGroup, DpiApp  DomainUser
================================================================================
2   100002 - ViPNet Service            Generated
drop Common Out       @local        ->@any
   tcp/udp:                   @any
    from 2046       @any
   @any
--------------------------------------------------------------------------------
empty rule for Forward Rules:
empty rule for Nat Rules:
hostname>
```

В результате выполнения команды будут показаны только сетевые фильтры и правила трансляции адресов, для которых в параметре <действие> задано значение `drop`.

firewall rules show rule

Просмотреть сетевые фильтры и правила трансляции адресов с заданным именем.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Для завершения просмотра используется клавиша **Q**.
- Если параметр `<имя>` состоит из нескольких слов, разделенных пробелами, то его необходимо заключить в кавычки.

- 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 rule "Allow ICMP Ping"
 Service Vpn Rules:
================================================================================
Num  Rule ID-Name                                    Option Schedule
Act  Protocol        Source         ->Destination
   DpiProtocol      [G]DpiGroup, DpiApp    DomainUser
================================================================================
10  100012 - Allow ICMP                    User
pass Ping
       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:
Current Rules Set Id: 150
================================================================================
Num  Rule ID-Name                                    Option Schedule
Act  Protocol        Source         ->Destination
   DpiProtocol      [G]DpiGroup, DpiApp    DomainUser
```

```
================================================================================
4   40000010 - Allow ICMP              User
pass Ping
       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

Просмотреть конкретные группы объектов, сетевые фильтры заданного типа, а также правила 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.

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.
- Можно указать несколько параметров.
- При просмотре транзитных фильтров открытой сети возможно использование нескольких 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 (см. firewall object show), сетевых фильтров или правил трансляции адресов (см. firewall rules show).

Пример использования

Для просмотра локальных фильтров для протокола UDP:

```
hostname> firewall local show udp
User:
=============================================================================
Num  RuleID - 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
-----------------------------------------------------------------------------
```

Чтобы просмотреть транзитные фильтры открытой сети:

```
hostname> firewall forward show
User:
================================================================================
Num  Name                        Option Schedule
Act  Protocol        Source          ->Destination
   DpiProtocol       [G]DpiGroup, DpiApp    DomainUser
================================================================================
1   [IPS]Production database             User
pass udp: from 67 to 68   @any          ->@DB
   @any          @any           @any
--------------------------------------------------------------------------------
2   [iPS][AV]Mail server               User
pass @any          @any          ->@MailIn
   @any          @any           @any
--------------------------------------------------------------------------------
```

Команды группы firewall inspector

Команды группы `firewall inspector` предназначены для настройки параметров расшифрования трафика SSL/TLS-сессий, а также для настройки антивирусной инспекции.

firewall inspector antivirus bypass

Включить или выключить блокировку трафика, проходящего через ViPNet xFirewall при недоступности ICAP-сервера внешнего антивируса.

Синтаксис

```
hostname# firewall inspector antivirus bypass {on | off}
```

Параметры и ключевые слова

- `on` — при недоступности ICAP-сервера внешнего антивируса ViPNet xFirewall разрешает проходящий через него трафик.
- `off` — при недоступности ICAP-сервера внешнего антивируса ViPNet xFirewall блокирует проходящий через него трафик.

Значения по умолчанию

`on`.

Режимы командного интерпретатора

Администратор.

Особенности использования

В режиме кластера команда работает только на активном узле.

Пример использования

```
hostname# firewall inspector antivirus bypass on
```

firewall inspector antivirus mode

Включить или выключить антивирусную проверку трафика.

Синтаксис

```
hostname# firewall inspector 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

- Чтобы включить антивирусную проверку, необходимо предварительно настроить URL для ICAP-сервера (URL, порт, метод).
- В режиме кластера команда работает только на активном узле.

Пример использования

```
hostname# firewall inspector antivirus mode on
```

firewall inspector antivirus server-url add

Задать адрес и метод подключения к ICAP-серверу внешнего антивируса.

Синтаксис

```
hostname# firewall inspector antivirus server-url add {reqmod | respmod} <URL>
```

Параметры и ключевые слова

- `reqmod` — проверяется исходящий трафик (запросы от пользователей сети);
- `respmod` — проверяется входящий трафик (ответы на запросы пользователей).
- `<URL>` — адрес ICAP-сервера антивируса в формате `icap://адрес[:порт]/[путь]`

Режимы командного интерпретатора

Администратор.

Особенности использования

- 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# firewall inspector antivirus server-url add respmod
icap://192.168.1.45/virus_scan
HTTP proxy antivirus add respmod service success
```

firewall inspector antivirus server-url delete

Удалить параметры подключения к ICAP-серверу внешнего антивируса.

Синтаксис

```
hostname# firewall inspector antivirus server-url delete {reqmod | respmod}
```

Параметры и ключевые слова

- `reqmod` — будет удален адрес доступа к ICAP-серверу для проверки исходящего трафика;
- `respmod` — будет удален адрес доступа к ICAP-серверу для проверки входящего трафика.

Режимы командного интерпретатора

Администратор.

Особенности использования

В режиме кластера команда работает только на активном узле.

Пример использования

```
hostname# firewall inspector antivirus server-url delete respmod
HTTP proxy antivirus delete respmod service success
```

firewall inspector antivirus show-status

Просмотреть текущие настройки и состояние антивирусной защиты.

Синтаксис

```
hostname> firewall inspector antivirus show-status
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

В режиме кластера команда выполняется на обоих узлах.

Пример использования

```
hostname> firewall inspector antivirus show-status
Antivirus mode is enabled.
External antivirus settings
---------------------------
Bypass is on
Reqmod server-url: icap://192.168.1.45:1344/virus_scan
Respmod server-url: icap://192.168.1.45:1344/virus_scan
```

firewall inspector ssl-decryption algorithms

Задать набор алгоритмов аутентификации, обмена ключами и шифрования, которые будут используются в расшифровке трафика SSL/TLS-сессий.

Синтаксис

```
firewall inspector ssl-decryption algorithms {allow-all|<algm> {allow|block}}
```

Параметры и ключевые слова

- `allow-all` — разрешить все алгоритмы.
- `<algm>` — один из алгоритмов `RSA`, `DHE`, `ECDHE`, `3DES`, `RC4`, `AES128-CBC`, `AES128-GCM`, `AES256-CBC`, `AES256-GCM`, `MD5`, `SHA1`, `SHA256`, `SHA384` и действие с ним:
  - `allow` — разрешить.
  - `block` — блокировать.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Для каждой группы алгоритмов набора необходимо разрешить минимум один алгоритм:
  - Обмен ключами: `RSA`, `DHE`, `ECDHE`.
  - Шифрование: `3DES`, `RC4`, `AES128-CBC`, `AES128-GCM`, `AES256-CBC`, `AES256-GCM`.

    - Аутентификация: `MD5`, `SHA1`, `SHA256`, `SHA384`.
- В названиях алгоритмов разрешены строчные и прописные буквы латинского алфавита.

Пример использования

Чтобы использовать в расшифровке трафика SSL/TLS-сессий весь набор алгоритмов:

```
hostname# firewall inspector ssl-decryption algorithms allow-all
All algorithms allowed.
```

Чтобы исключить из текущего набора алгоритм обмена ключами dhe:

```
hostname# firewall inspector ssl-decryption algorithms DHE block
Algorithm DHE blocked
```

firewall inspector ssl-decryption cert

Установить корневой сертификат из локального хранилища сертификатов ViPNet xFirewall, который будет использоваться в расшифровании трафика SSL/TLS-сессий. Этим сертификатом подписываются сертификаты, используемые при встраивании в сессию.

Синтаксис

```
firewall inspector ssl-decryption cert <cert>
```

Параметры и ключевые слова

`<cert>` — имя файла собственного корневого сертификата.

Режимы командного интерпретатора

Администратор.

Особенности использования

- После выполнения команды корневой сертификат ViPNet xFirewall не используется в расшифровке трафика SSL/TLS-сессий.
- Чтобы вернуться к использованию корневого сертификата ViPNet xFirewall, выполните команду `firewall inspector ssl-decryption recreate-cert`

Пример использования

```
hostname# firewall inspector ssl-decryption cert cert_file_name.pem
```

firewall inspector ssl-decryption export-cert

Экспортировать текущий корневой сертификат, используемый в расшифровании трафика SSL/TLS-сессий, на USB-носитель.

Синтаксис

```
firewall inspector ssl-decryption export-cert
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

После запуска команды подключите к ViPNet xFirewall USB-носитель и нажмите **Enter**.

Пример использования

```
hostname> firewall inspector ssl-decryption export-cert
To save ssl_decryption_cert.pem file please insert USB drive and press Enter
...
```

firewall inspector ssl-decryption option

Задать опции расшифровки трафика SSL/TLS-сессий.

Синтаксис

```
firewall inspector ssl-decryption option <option> <value>
```

Параметры и ключевые слова

- `<option>` — опция:
  - `client-auth` — аутентификация клиента (двухсторонний TLS).
  - `compression` — сжатие трафика SSL/TLS-сессий.
- `<value>` — значение:
  - `bypass` — пропустить.
  - `block` — блокировать.
  - `on` — включить сжатие.

- `off` — выключить сжатие.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Значения `bypass` и `block` недоступны для опции `compression`.
- Значения `on` и `off` доступны только для опции `compression`.

Пример использования

Чтобы заблокировать трафик SSL/TLS-сессий, в которых используется двухсторонний TLS:

```
hostname# firewall inspector ssl-decryption option client-auth block
Set to BLOCK sessions with client authentication
```

Чтобы включить сжатие расшифрованного трафика SSL/TLS-сессий:

```
hostname# firewall inspector ssl-decryption option compression on
Compression of decrypted traffic ON
```

firewall inspector ssl-decryption protocols

Задать расшифровываемые протоколы SSL/TLS-сессий.

Синтаксис

```
firewall inspector ssl-decryption protocols {allow-all|<protocol> {allow|block}}
```

Параметры и ключевые слова

- `allow-all` — все протоколы.
- `<protocol>` — один из протоколов: `ssl3`, `tls10`, `tls11`, `tls12` и действие с ним:
  - `allow` — разрешить.
  - `block` — блокировать.

Режимы командного интерпретатора

Администратор.

Особенности использования

Необходимо разрешить минимум один расшифровываемый протокол.

Пример использования

```
hostname# firewall inspector ssl-decryption protocols allow-all

All protocols allowed.
```

firewall inspector ssl-decryption recreate-cert

Перевыпустить и установить корневой сертификат ViPNet xFirewall (не путать с корневым сертификатом, установленным из локального хранилища), который будет использоваться в расшифровке трафика SSL/TLS-сессий. Этим сертификатом подписываются сертификаты, используемые при встраивании в сессию.

Синтаксис

```
firewall inspector ssl-decryption recreate-cert
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# firewall inspector ssl-decryption recreate-cert

ssl-decryption root certificate recreated and set.

Root certificate info:

 Subject:  C = GB, ST = Test State, L = Test Locality, O = JSC InfoTeCS, OU = XF, CN = InfoTeCS SSL inspection, emailAddress = soft@infotecs.ru

 Validity: Dec 6 07:43:36 2026 GMT

 Issuer:  C = GB, ST = Test State, L = Test Locality, O = JSC InfoTeCS, OU = XF, CN = InfoTeCS SSL inspection, emailAddress = soft@infotecs.ru

 Filename: ssl_decryption_cert.pem

 Serial:  F802A3C1E44CAF26
```

firewall inspector ssl-decryption show

Просмотреть параметры расшифрования трафика SSL/TLS-сессий.

Синтаксис

```
firewall inspector ssl-decryption show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде отображаются:

- Статус расшифровки трафика SSL/TLS-сессий: `ON` — включена или `OFF` — выключена.
- Сведения о корневом сертификате (корневом сертификате ViPNet xFirewall или собственном корневом сертификате), которым подписываются сертификаты, используемые при встраивании в SSL/TLS-сессию:
  - `Subject` — для кого создан.
  - `Validity` — срок действия.
  - `Issuer` — издатель.
  - `Filename` — имя файла.
  - `Serial number` — серийный номер.
- Параметры расшифровывания:
  - Протоколы: `ssl3`, `tls10`, `tls11`, `tls12`.
  - Алгоритмы обмена ключами: `RSA`, `DHE`, `ECDHE`.
  - Алгоритмы шифрования: `3DES`, `RC4`, `AES128-CBC`, `AES128-GCM`, `AES256-CBC`, `AES256-GCM`.
  - Алгоритмы аутентификации: `MD5`, `SHA1`, `SHA256`, `SHA384`.
- Действия с расшифрованной SSL/TLS-сессией:
  - Сессия требует аутентификацию и клиента и сервера (двухсторонний TLS): `BYPASS` — пропускать или `BLOCK` — блокировать.
  - Сессия использует сертификат с истекшим сроком действия: `BYPASS` или `BLOCK`.
  - Сессия использует сертификат, не предназначенный для подтверждения подлинности сервера и/или клиента: `BYPASS` или `BLOCK`.
  - Сессия использует самоподписанный сертификат: `BYPASS` или `BLOCK`.
- Сжатие трафика расшифрованной SSL/TLS-сессии: `ON` —включено или `OFF` — выключено.
- ID и срок действия лицензии

Пример использования

```
hostname> firewall inspector ssl-decryption show

SSL-decryption in ON.

Root certificate info:
```

```
 Subject:  C = GB, ST = Test State, L = Test Locality, O = JSC InfoTeCS, OU = XF, CN = InfoTeCS
SSL inspection, emailAddress = soft@infotecs.ru

 Validity: Dec 6 07:43:36 2026 GMT

 Issuer:  C = GB, ST = Test State, L = Test Locality, O = JSC InfoTeCS, OU = XF, CN = InfoTeCS
SSL inspection, emailAddress = soft@infotecs.ru

 Filename: /etc/cert/sslsplit_cert.crt

 Serial:  F802A3C1E44CAF26

Decryption parameters:

 Allowed protocols: tls10 tls11 tls12 ssl3

 Allowed algorithms:

  Key Exchange: RSA ECDHE DHE

  Encryption: 3DES RC4 AES128-CBC AES128-GCM AES256-CBC AES256-GCM

  Authentication: MD5 SHA1 SHA256 SHA384

Decryption options:

 BLOCK sessions with client authentication

 Compression of decrypted traffic OFF

SSL Inspection license ID: 2578618/2:6:1:ssl_va

SSL Inspection license expiration date: 2023-01-28 00:00:00
```

Команды группы healthmond

Команды группы `healthmond` предназначены для настройки и управления службой мониторинга устройства `healthmond`.

healthmond start

Запустить `healthmond`, службу мониторинга состояния ViPNet xFirewall.

Синтаксис

```
healthmond start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

нет

Пример использования

```
hostname# healthmond start
```

healthmond stop

Остановить `healthmond`, службу мониторинга состояния ViPNet xFirewall.

Синтаксис

```
healthmond stop
```

Режимы командного интерпретатора

Администратор.

Особенности использования

нет

Пример использования

```
hostname# healthmond stop
```

healthmond edit

Открыть для редактирования `healthmond.ini`, конфигурационный файл службы мониторинга состояния ViPNet xFirewall.

Синтаксис

```
healthmond edit
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде будет запущен текстовый редактор с конфигурационным файлом `healthmond.ini`.
- После изменения файла `healthmond.ini` перезапустите службу `healthmond` с помощью команд `healthmond stop` и `healthmond start`.

Пример использования

```
hostname# healthmond edit
```

Команды группы inet

Настройка и управление сетевыми интерфейсами, прикладными сервисами, маршрутизацией и мониторингом.

inet bonding add mode slaves

Настроить агрегированный интерфейс.

Синтаксис

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

Параметры и ключевые слова

- `<номер>` — номер добавляемого агрегированного интерфейса. Возможные значения 0, 1, 2.
- `<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. 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;
    - 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);

- с другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью команды inet ifconfig bonding lacp-rate, что позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую (например, через медиаконвертер).

- `active-backup` — режим, при котором один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью команды inet ifconfig bonding primary) и все исходящие пакеты отправляются через него. При этом в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
- `broadcast` — режим, 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).
- 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.
- При добавлении агрегированного интерфейса, а также впоследствии с помощью команды inet ifconfig bonding add, 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 512.

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
```

inet bonding delete

Удалить агрегированный интерфейс.

Синтаксис

```
inet bonding delete <номер>
```

Параметры и ключевые слова

`<номер>` — номер удаляемого агрегированного интерфейса.

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), предварительно удалите все соответствующие ему виртуальные интерфейсы с помощью команды inet ifconfig vlan delete.

Пример использования

```
hostname# inet bonding delete 1
```

inet clear mac-address-table

Очистить ARP-таблицу (таблицу преобразования IP-адресов в MAC-адреса).

Синтаксис

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

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet clear mac-address-table
This command clears the MAC address table.
Are you sure you want to execute this command? [Yes/No]: Yes
```

inet dhcp client route-default-metric

Изменить значение метрики по умолчанию 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.

Пример использования

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

inet dhcp client route-distance

Задать административную дистанцию маршрутам, поступающим от DHCP-сервера (с использованием DHCP-протокола).

Синтаксис

```
inet dhcp client route-distance <административная дистанция> [default-route
<административная дистанция>]
```

Параметры и ключевые слова

- `route-distance <административная дистанция>` — общая административная дистанция для всех маршрутов DHCP-сервера. Возможные значения: 1–255.
- `default-route <административная дистанция>` — административная дистанция для маршрутов по умолчанию. Возможные значения: 1–255.

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
```

inet dhcp relay add backup-interface

Добавить сетевой интерфейс, через который служба DHCP-relay будет связываться с запасным DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] add backup-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задается интерфейс. Возможные значения от 1 до 32.

- `<интерфейс>` — имя интерфейса, со стороны которого находится запасной DHCP-сервер.
- `<адрес>` — IP-адрес запасного DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- 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 для копии 2 службы DHCP-relay использовать интерфейс `eth1` для связи с запасным DHCP-сервером, имеющим IP-адрес 172.16.1.1:

```
hostname# inet dhcp relay 2 add backup-interface eth1 server 172.16.1.1
```

inet dhcp relay add external-interface

Добавить сетевой интерфейс, через который служба DHCP-relay будет связываться с внешним DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] add external-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задается интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса, со стороны которого находится внешний DHCP-сервер.
- `<адрес>` — IP-адрес внешнего DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- 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.
    - В качестве сетевого интерфейса нельзя задать:интерфейс «внутренней петли» (loopback, localhost);
    - виртуальные интерфейсы, созданные после назначения дополнительных IP-адресов физическим интерфейсам (алиасы).

Пример использования

Чтобы для копии 2 службы DHCP-relay использовать интерфейс `eth1` для связи с внешним DHCP-сервером, имеющим адрес 172.16.1.1:

```
hostname# inet dhcp relay 2 add external-interface eth1 server 172.16.1.1
```

inet dhcp relay add listen-interface

Добавить сетевой интерфейс в список интерфейсов, принимающих запросы от DHCP-клиентов для их последующей ретрансляции на внешний DHCP-сервер.

Синтаксис

```
inet dhcp relay [<номер копии>] add listen-interface <интерфейс>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задается интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя сетевого интерфейса.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- 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.
- Добавляемый интерфейс не должен использоваться в других копиях DHCP-relay.
    - В качестве сетевого интерфейса нельзя задать:интерфейс «внутренней петли» (loopback, localhost);
    - виртуальные интерфейсы, созданные после назначения дополнительных IP-адресов физическим интерфейсам (алиасы).

Пример использования

Чтобы для копии DHCP-relay 2 добавить интерфейс `eth0` в список интерфейсов, принимающих запросы от DHCP-клиентов:

```
hostname# inet dhcp relay 2 add listen-interface eth0
```

inet dhcp relay delete backup-interface

Удалить сетевой интерфейс, через который служба DHCP-relay связывается с запасным DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] delete backup-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой удаляется интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса, со стороны которого находится запасной DHCP-сервер.
- `<адрес>` — IP-адрес запасного DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка.

Пример использования

Чтобы для копии 2 службы DHCP-relay удалить интерфейс `eth1`, имеющий связь с запасным DHCP-сервером с IP-адресом 172.16.1.1:

```
hostname# inet dhcp relay 2 delete backup-interface eth1 server 172.16.1.1
```

inet dhcp relay delete external-interface

Удалить сетевой интерфейс, через который служба DHCP-relay связывается с внешним DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] delete external-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой удаляется интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса, со стороны которого находится внешний DHCP-сервер.
- `<адрес>` — IP-адрес внешнего DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка.

Пример использования

Чтобы для копии 2 службы DHCP-relay удалить интерфейс `eth1` для связи с внешним DHCP-сервером, имеющим адрес 172.16.1.1:

```
hostname# inet dhcp relay 2 delete external-interface eth1 server 172.16.1.1
```

inet dhcp relay delete listen-interface

Удалить сетевой интерфейс из списка интерфейсов, принимающих запросы от DHCP-клиентов для их последующей ретрансляции на внешний DHCP-сервер.

Синтаксис

```
inet dhcp relay [<номер копии>] delete listen-interface <интерфейс>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задан интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка.

Пример использования

Чтобы для копии DHCP-relay 2 удалить интерфейс `eth0` из списка интерфейсов, принимающих запросы от DHCP-клиентов:

```
hostname# inet dhcp relay 2 delete listen-interface eth0
```

inet dhcp relay mode

Включить или выключить автоматический запуск службы DHCP-relay при загрузке ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения 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:

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

inet dhcp relay reset

Сбросить настройки службы DHCP-relay, включая настройки автоматического запуска при загрузке ViPNet xFirewall, и завершить её работу.

Синтаксис

```
inet dhcp relay [<номер копии>] reset
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то настройки сбрасываются для всех копий.

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
Are you sure to reset DHCP relay settings? [Yes/No]: Yes
```

inet dhcp relay start

Запустить службу DHCP-relay.

Синтаксис

```
inet dhcp relay [<номер копии>] start
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

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.
- Указан несуществующий номер копии процесса DHCP-relay.

Пример использования

Чтобы запустить копию 2 процесса DHCP-relay:

```
hostname# inet dhcp relay 2 start
```

inet dhcp relay stop

Завершить работу службы DHCP-relay.

Синтаксис

```
inet dhcp relay [<номер копии>] stop
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы завершить работу копии 2 процесса DHCP-relay:

```
hostname# inet dhcp relay 2 stop
```

inet dhcp server add broadcast

Задать широковещательный IP-адрес, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add broadcast <IP-адрес> {interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<IP-адрес>` — широковещательный IP-адрес.

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается широковещательный IP-адрес.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться широковещательный IP-адрес. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается широковещательный IP-адрес (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды необходимо завершить работу DHCP-сервера (см. inet dhcp server stop).
- При добавлении более одного широковещательного IP-адреса выдается сообщение, что предыдущее значение будет перезаписано.

Пример использования

Чтобы задать широковещательный IP-адрес 192.168.1.255 для сетевого интерфейса `eth1`:

```
hostname# inet dhcp server add broadcast 192.168.1.255 interface eth1
```

Чтобы задать широковещательный IP-адрес 172.16.1.255 для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add broadcast 172.16.1.255 remote subnet 192.168.1.0 mask
255.255.255.0
```

Чтобы задать широковещательный IP-адрес 192.168.1.255 для узла сети ViPNet с именем host123:

```
hostname# inet dhcp server add broadcast 192.168.1.255 host host123
```

inet dhcp server add default-lease-time

Задать значение по умолчанию времени аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay). Это значение используется клиентами DHCP-сервера, которые не запрашивают определенное время аренды IP-адресов.

Синтаксис

```
inet dhcp server add default-lease-time <время> [interface <интерфейс> | remote subnet
<подсеть> mask <маска> | host <имя узла>]
```

Параметры и ключевые слова

- `<время>` — время аренды в секундах (от 1 до 4294967294).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается время аренды (лизинга) IP-адресов по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться время аренды IP-адресов по умолчанию. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается время аренды IP-адресов по умолчанию (в параметрах секции `[id]` указанного узла файла `iplir.conf`). Для узла должен быть предварительно зарезервирован IP-адрес с помощью команды inet dhcp server add host.

Значения по умолчанию

По умолчанию время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы установить время аренды по умолчанию 5 дней для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add default-lease-time 432000 remote subnet 192.168.1.0 mask
255.255.255.0
```

inet dhcp server add dns

Задать IP-адрес DNS-сервера для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add dns <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть> mask
<маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес DNS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес DNS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес DNS-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес DNS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 10 IP-адресов DNS-серверов.

Пример использования

- Чтобы добавить IP-адрес DNS-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server add dns 192.168.15.41 interface eth1
  ```

- Чтобы задать IP-адрес DNS-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server add dns 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы задать IP-адрес DNS-сервера 192.168.15.41 для узла сети ViPNet с именем host123:

  ```
  hostname# inet dhcp server add dns 192.168.15.41 host host123
  ```

inet dhcp server add domain

Задать имя домена для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add domain <имя домена> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<имя домена>` — имя домена, соответствующее формату FQDN.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается имя домена.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться имя домена. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается имя домена (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При добавлении более одного имени домена выдается сообщение, что предыдущее значение будет перезаписано.

Пример использования

- Чтобы добавить доменное имя dc.corp для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server add domain dc.corp interface eth1
  ```

- Чтобы задать доменное имя dc.corp для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server add domain dc.corp remote subnet 192.168.1.0 mask
  255.255.255.0
  ```

- Чтобы задать доменное имя dc.corp для узла сети ViPNet с именем host123:

  ```
  hostname# inet dhcp server add domain dc.corp host host123
  ```

inet dhcp server add host

Зарезервировать в DHCP-сервере IP-адрес сетевого узла с заданными доменным именем и MAC-адресом. Информацию об этом DHCP-сервер передает своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add host <имя узла> hardware <MAC-адрес> address <IP-адрес> {interface
<интерфейс> | remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<имя узла>` — доменное имя сетевого узла, для которого резервируется IP-адрес. Может содержать символы латинского алфавита, цифры и знак дефиса («-»). Максимальная длина 32 символа.
- `<MAC-адрес>` — MAC-адрес сетевого узла, для которого резервируется IP-адрес.
- `<IP-адрес>` — IP-адрес, который резервируется DHCP-сервером для данного узла.
- `<интерфейс>` — название сетевого интерфейса в системе, на котором резервируется IP-адрес узла.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться информация о резервировании IP-адреса. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы зарезервировать IP-адрес 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 на сетевом интерфейсе `eth1`:

```
hostname# inet dhcp server add host host123 hardware 00:50:56:C0:00:08 address
192.168.15.41 interface eth1
```

- Чтобы зарезервировать IP-адрес 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add host host123 hardware 00:50:56:C0:00:08 address
192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
```

inet dhcp server add interface

Задать рабочий интерфейс DHCP-сервера.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- В качестве рабочего можно указать физический, VLAN- или агрегированный сетевой интерфейс.
- Рабочий интерфейс DHCP-сервера должен иметь статический IP-адрес.
- IP-адрес рабочего интерфейса DHCP-сервера не должен принадлежать диапазону выделяемых IP-адресов, заданному командой inet dhcp server add range.

Пример использования

Чтобы задать интерфейс `eth1` в качестве рабочего для DHCP-сервера:

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

inet dhcp server add max-lease-time

Задать время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add max-lease-time <время> [{interface <интерфейс> | remote subnet
<подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<время>` — время аренды в секундах (от 1 до 4294967294).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться время аренды IP-адресов. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

- `<имя узла>` — имя узла сети ViPNet, для которого задается время аренды IP-адресов (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Значения по умолчанию

Время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы установить время аренды 5 дней для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add max-lease-time 432000 remote subnet 192.168.1.0 mask
255.255.255.0
```

inet dhcp server add ntp

Задать IP-адрес NTP-сервера для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add ntp <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть> mask
<маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес NTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес NTP-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес NTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 10 IP-адресов NTP-серверов.

Пример использования

- Чтобы добавить IP-адрес NTP-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server add ntp 192.168.15.41 interface eth1
  ```

- Чтобы задать IP-адрес NTP-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server add ntp 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы задать IP-адрес NTP-сервера 192.168.15.41 для узла сети ViPNet с именем `host123`:

  ```
  hostname# inet dhcp server add ntp 192.168.15.41 host host123
  ```

inet dhcp server add option

Добавить опцию DHCP-сервера в соответствии с RFC 2132.

Синтаксис

```
inet dhcp server add option <номер> {ip | ascii | hex} <значение> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<номер>` — номер опции DHCP-сервера (от 1 до 254).
- `ip` — опция содержит IP-адрес.
- `ascii` — опция содержит текст в кодировке ASCII.
- `hex` — опция содержит разрядное шестнадцатеричное число (с точками разрядов, без учета регистра).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается опция DHCP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться опция DHCP-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.

- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается опция DHCP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При выполнении команды выдается предупреждение, что значения опций не проверяются на соответствие RFC 2132.

Пример использования

Чтобы добавить опцию DHCP-сервера 69 (сервер SMTP по умолчанию) со значением 10.0.0.25 для сетевого интерфейса `eth1`:

```
hostname# inet dhcp server add option 69 ip 10.0.0.25 interface eth1
```

inet dhcp server add range

Задать диапазон IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add range <начало диапазона> <конец диапазона> {interface <интерфейс> |
remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<начало диапазона>` — начальный IP-адрес диапазона.
- `<конец диапазона>` — конечный IP-адрес диапазона.
- `<интерфейс>` — название сетевого интерфейса в системе, на котором задается диапазон IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться информация о диапазоне IP-адресов. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- Конечный адрес диапазона должен быть не меньше начального.
- В локальной сети, маршрутизируемой в 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 клиентам сети 192.168.10.0/24 адреса из диапазона 192.168.10.2–192.168.10.254:

```
hostname# inet dhcp server add range 192.168.10.2 192.168.10.254 remote subnet 192.168.10.0
mask 255.255.255.0
```

inet dhcp server add relay-interface

Задать сетевой интерфейс DHCP-сервера, на котором он будет обрабатывать запросы от агента DHCP-relay, работающего в удаленной подсети.

Синтаксис

```
inet dhcp server add relay-interface <интерфейс> remote subnet <подсеть> mask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса. Сетевой интерфейс должен быть предварительно задан в качестве рабочего интерфейса DHCP-сервера (см. inet dhcp server add interface).
- `<подсеть>` — IP-адрес удаленной подсети, в которой работает агент DHCP-relay.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- Максимально возможное количество удаленных подсетей —128.
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов, заданных командой inet dhcp server add interface.

- В качестве рабочего можно указать физический, VLAN- или агрегированный сетевой интерфейс.
- Задаваемый интерфейс DHCP-сервера должен иметь статический IP-адрес.
- IP-адрес задаваемого интерфейса DHCP-сервера не должен принадлежать диапазону выделяемых IP-адресов, заданному командой inet dhcp server add range.

Пример использования

Чтобы задать интерфейс `eth1` в качестве сетевого интерфейса DHCP-сервера, на котором он будет обрабатывать запросы от агента DHCP-relay, работающего в удаленной подсети с адресом 192.168.10.0/24:

```
hostname# inet dhcp server add relay-interface eth1 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add router

Задать IP-адрес шлюза по умолчанию для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add router <IP-адрес> {interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес шлюза по умолчанию.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес шлюза по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес шлюза по умолчанию. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес шлюза по умолчанию (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

- IP-адрес шлюза должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам.
- С помощью последовательного выполнения команд можно добавить до 10 IP-адресов шлюзов по умолчанию.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 адрес шлюза по умолчанию 192.168.10.1:

```
hostname# inet dhcp server add router 192.168.10.1 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add subnet-mask

Задать маску подсети для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add subnet-mask <маска подсети> {interface <интерфейс> | remote subnet
<подсеть> mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<маска подсети>` — маска подсети, передаваемая DHCP-сервером.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается маска подсети.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться маска подсети. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается маска подсети (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При добавлении более одной маски подсети выдается сообщение, что предыдущее значение будет перезаписано.

- На основе указанной маски подсети будет автоматически задан широковещательный IP-адрес, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP-relay).

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 маску подсети 255.255.255.0:

```
hostname# inet dhcp server add subnet-mask 255.255.255.0 remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server add tftp

Задать IP-адрес или имя TFTP-сервера, а также имя передаваемого файла. Данная информация передается DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add tftp {<имя сервера> | <адрес сервера>} [file <путь к файлу>] [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<имя сервера>` — доменное имя TFTP-сервера, соответствующее формату FQDN.
- `<адрес сервера>` — IP-адрес TFTP-сервера.
- `<путь к файлу>` — путь к файлу, загружаемому по протоколу TFTP.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задаются параметры TFTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будут передаваться параметры TFTP-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задаются параметры TFTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

- При добавлении более одного адреса TFTP-сервера выдается сообщение, что предыдущее значение будет перезаписано.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 IP-адрес TFTP-сервера 192.168.10.65:

```
hostname# inet dhcp server add tftp 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add voip

Задать IP-адрес TFTP-сервера Cisco VoIP. Данная информация передается DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add voip <адрес сервера> [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес TFTP-сервера Cisco VoIP.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задаются параметры TFTP-сервера Cisco VoIP.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будут передаваться параметры TFTP-сервера Cisco VoIP. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задаются параметры TFTP-сервера Cisco VoIP (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 2 IP-адресов TFTP-сервера Cisco VoIP.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 IP-адрес TFTP-сервера Cisco VoIP 192.168.10.65:

```
hostname# inet dhcp server add voip 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add wins

Добавить адрес WINS-сервера в список адресов, передаваемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add wins <адрес сервера> [interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес WINS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес WINS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес WINS-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес WINS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 2 IP-адресов WINS-сервера.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 IP-адрес WINS-сервера 192.168.10.65:

```
hostname# inet dhcp server add wins 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server delete broadcast

Удалить широковещательный IP-адрес, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete broadcast {interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан широковещательный IP-адрес.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается широковещательный IP-адрес.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан широковещательный IP-адрес (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить широковещательный IP-адрес для сетевого интерфейса eth1, выполните команду:

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

Чтобы удалить широковещательный IP-адрес для клиентов удаленной подсети с адресом 192.168.1.0/24, выполните команду:

```
hostname# inet dhcp server delete broadcast remote subnet 192.168.1.0 mask 255.255.255.0
```

Чтобы удалить широковещательный IP-адрес для узла сети ViPNet с именем host123, выполните команду:

```
hostname# inet dhcp server delete broadcast host host123
```

inet dhcp server delete default-lease-time

Удалить значение по умолчанию времени аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete default-lease-time {interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого удаляется время аренды (лизинга) IP-адресов по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается время аренды IP-адресов по умолчанию.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задано время аренды IP-адресов по умолчанию (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить заданное время аренды по умолчанию для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server delete default-lease-time remote subnet 192.168.1.0 mask 255.255.255.0
```

inet dhcp server delete dns

Удалить IP-адрес DNS-сервера, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete dns <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес DNS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес DNS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес DNS-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес DNS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить IP-адрес DNS-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server delete dns 192.168.15.41 interface eth1
  ```

- Чтобы удалить IP-адрес DNS-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete dns 192.168.15.41 remote subnet 192.168.1.0 mask
  255.255.255.0
  ```

- Чтобы удалить IP-адрес DNS-сервера 192.168.15.41 для узла сети ViPNet с именем `host123`:

  ```
  hostname# inet dhcp server delete dns 192.168.15.41 host host123
  ```

inet dhcp server delete domain

Удалить доменное имя, передаваемое DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete domain [{interface <интерфейс> | remote subnet <подсеть> mask
<маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задано имя домена.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается имя домена.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задано имя домена (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить доменное имя для сетевого интерфейса `eth1`:

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

- Чтобы удалить доменное имя для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete domain remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы удалить доменное имя для узла сети ViPNet с именем `host123`:

  ```
  hostname# inet dhcp server delete domain host host123
  ```

inet dhcp server delete host

Удалить зарезервированный DHCP-сервером IP-адрес сетевого узла с заданными доменным именем и MAC-адресом.

Синтаксис

```
inet dhcp server delete host <имя узла> hardware <MAC-адрес> address <IP-адрес> {interface <интерфейс> | remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<имя узла>` — доменное имя сетевого узла, для которого зарезервирован IP-адрес. Может содержать символы латинского алфавита, цифры и знак дефиса («-»). Максимальная длина 32 символа.
- `<MAC-адрес>` — MAC-адрес сетевого узла, для которого зарезервирован IP-адрес.
- `<IP-адрес>` — IP-адрес, который зарезервирован DHCP-сервером для данного узла.

- `<интерфейс>` — название сетевого интерфейса в системе, на котором зарезервирован IP-адрес узла.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается информация о резервировании IP-адреса.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить резервирование IP-адреса 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 на сетевом интерфейсе `eth1`:

  ```
  hostname# inet dhcp server delete host host123 hardware 00:50:56:C0:00:08 address 192.168.15.41 interface eth1
  ```

- Чтобы удалить резервирование IP-адреса 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete host host123 hardware 00:50:56:C0:00:08 address 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

inet dhcp server delete interface

Удалить рабочий интерфейс DHCP-сервера.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- В качестве рабочего можно указать физический, VLAN- или агрегированный сетевой интерфейс.

Пример использования

Чтобы удалить интерфейс `eth1` как рабочий интерфейс DHCP-сервера:

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

inet dhcp server delete max-lease-time

Удалить ранее заданное время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete max-lease-time [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задано время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задано время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Значения по умолчанию

После выполнения команды время аренды сбрасывается на значение по умолчанию (864000 секунд).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить заданное время аренды для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server delete max-lease-time remote subnet 192.168.1.0 mask
255.255.255.0
```

inet dhcp server delete ntp

Удалить IP-адрес NTP-сервера, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete ntp <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес NTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес NTP-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес NTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server delete ntp 192.168.15.41 interface eth1
  ```

- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete ntp 192.168.15.41 remote subnet 192.168.1.0 mask
  255.255.255.0
  ```

- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для узла сети ViPNet с именем `host123`:

```
hostname# inet dhcp server delete ntp 192.168.15.41 host host123
```

inet dhcp server delete option

Удалить опцию DHCP-сервера в соответствии с RFC 2132.

Синтаксис

```
inet dhcp server delete option <номер> [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<номер>` — номер опции DHCP-сервера (от 1 до 254).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого удаляется опция DHCP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается опция DHCP-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задана опция DHCP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить опцию DHCP-сервера 69 (сервер SMTP по умолчанию) для сетевого интерфейса `eth1`:

```
hostname# inet dhcp server delete option 69 interface eth1
```

inet dhcp server delete range

Удалить диапазон IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete range <начало диапазона> <конец диапазона> {interface <интерфейс>
| remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<начало диапазона>` — начальный IP-адрес диапазона.
- `<конец диапазона>` — конечный IP-адрес диапазона.
- `<интерфейс>` — название сетевого интерфейса в системе, на котором задан диапазон IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается информация о диапазоне IP-адресов.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить выделяемый DHCP-сервером клиентам сети 192.168.10.0/24 диапазон 192.168.10.2–192.168.10.254:

```
hostname# inet dhcp server delete range 192.168.10.2 192.168.10.254 remote subnet
192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete relay-interface

Удалить сетевой интерфейс DHCP-сервера, на котором обрабатываются запросы от агента DHCP-relay, работающего в удаленной подсети.

Синтаксис

```
inet dhcp server delete relay-interface <интерфейс> remote subnet <подсеть> mask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса. Сетевой интерфейс должен быть предварительно задан в качестве рабочего интерфейса DHCP-сервера (см. inet dhcp server add interface).

- `<подсеть>` — IP-адрес удаленной подсети, в которой работает агент DHCP-relay. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов, заданных командой inet dhcp server add interface.

Пример использования

Чтобы удалить интерфейс `eth1`, на котором DHCP-сервер обрабатывает запросы от агента DHCP-relay, работающего в удаленной подсети с адресом 192.168.10.0/24:

```
hostname# inet dhcp server delete relay-interface eth1 remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete router

Удалить IP-адрес шлюза по умолчанию, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete router <адрес> {interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес шлюза по умолчанию.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес шлюза по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес шлюза по умолчанию.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес шлюза по умолчанию.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить адрес шлюза по умолчанию 192.168.10.1, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete router 192.168.10.1 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server delete subnet-mask

Удалить маску подсети, передаваемую DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete subnet-mask {interface <интерфейс> | remote subnet <подсеть> mask
<маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задана маска подсети.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается маска подсети.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задана маска подсети (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- По команде будет автоматически удален широковещательный IP-адрес, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP-relay).

Пример использования

Чтобы удалить маску подсети, передаваемую DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete subnet-mask remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete tftp

Удалить настройки TFTP-сервера, передаваемые DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete tftp [{interface <интерфейс> | remote subnet <подсеть> mask <маска>
| host <имя узла>}]
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого заданы параметры TFTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передаются параметры TFTP-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого заданы параметры TFTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить IP-адрес TFTP-сервера 192.168.10.65, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete tftp remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete voip

Удалить IP-адрес TFTP-сервера Cisco VoIP. Данная информация передается DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete voip <адрес сервера> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес TFTP-сервера Cisco VoIP.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого заданы параметры TFTP-сервера Cisco VoIP.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передаются параметры TFTP-сервера Cisco VoIP.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого заданы параметры TFTP-сервера Cisco VoIP (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить IP-адрес TFTP-сервера Cisco VoIP 192.168.10.65, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete voip 192.168.10.65 remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete wins

Удалить адрес WINS-сервера из списка адресов, передаваемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete wins <адрес сервера> [interface <интерфейс> | remote subnet
<подсеть> mask <маска> | host <имя узла>]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес WINS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес WINS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес WINS-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес WINS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Удалить IP-адрес WINS-сервера 192.168.10.65, передаваемый DHCP-сервером клиентам удаленной подсети 192.168.10.0/24:

```
hostname# inet dhcp server delete wins 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server lease show

Просмотреть список клиентов DHCP-сервера.

Синтаксис

```
inet dhcp server lease show [{last | all | full}]
```

Параметры и ключевые слова

- `last` — вывести текущий список клиентов DHCP-сервера (по умолчанию).
- `all` — вывести полный список клиентов DHCP-сервера с историей аренды IP-адресов.

- `full` — вывести полный список клиентов DHCP-сервера без форматирования вывода (см. пример ниже).

Значения по умолчанию

По умолчанию команда без параметров выводит текущий список клиентов DHCP-сервера (`last`).

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если среди клиентов DHCP-сервера присутствуют клиенты, подключенные к разным интерфейсам VLAN, у который один MAC-адрес, то по умолчанию в выводе команды отображаются IP-адреса клиентов только одного интерфейса VLAN. Для отображения информации о клиентах всех интерфейсов VLAN выполните команду с параметром `all` (`inet show dhcp server lease all`).

Пример использования

- Чтобы просмотреть текущий список клиентов DHCP-сервера:

```
hostname> inet dhcp server lease show
MAC        IP       hostname    valid until
===========================================================================
90:27:e4:f9:9d:d7 192.168.0.182  iMac-de-mac  2018-12-12 01:37:06
d8:a2:5e:94:40:81 192.168.0.178  foo-2     2018-12-12 01:04:56
e8:9a:8f:6e:0f:60 192.168.0.127  angela     2018-12-11 23:55:32
ec:55:f9:c5:f2:55 192.168.0.179  angela     2018-12-11 23:54:56
f0:4f:7c:3f:9e:dc 192.168.0.183  kindle-1234567 2018-12-11 23:54:31
f4:ec:38:e2:f9:67 192.168.0.185  -NA-      2018-12-11 23:55:40
f8:d1:11:b7:5a:62 192.168.0.184  -NA-      2018-12-11 23:57:34
```

- Чтобы просмотреть полный список клиентов DHCP-сервера без форматирования вывода:

```
hostname> inet dhcp server lease show full
lease 192.168.42.1 {
starts 0 2018/01/30 08:02:54;
ends 5 2018/02/04 08:02:54;
hardware ethernet
00:50:04:53:D5:57;
uid 01:00:50:04:53:D5:57;
client-hostname "PC0097";
}
...
```

inet dhcp server lease clear

Удалить записи об арендованных адресах DHCP-сервера.

Синтаксис

```
inet dhcp server lease clear [address <значение>]
```

Параметры и ключевые слова

- `<значение>` — IP-адрес, который необходимо удалить из списка аренды. Вы можете одновременно удалить до 5 IP-адресов, указав для каждого удаляемого IP-адреса пару `address <значение>`, разделив их пробелами.

Значения по умолчанию

По умолчанию команда без параметров полностью очищает список аренды адресов DHCP-сервера.

Режимы командного интерпретатора

- Администратор.

Особенности использования

Если среди клиентов DHCP-сервера присутствуют клиенты, подключенные к разным интерфейсам VLAN, у который один MAC-адрес, то по умолчанию в выводе команды отображаются IP-адреса клиентов только одного интерфейса VLAN. Для отображения информации о клиентах всех интерфейсов VLAN выполните команду с параметром `all` (`inet show dhcp server lease all`).

Пример использования

- Чтобы полностью очистить список аренды DHCP-сервера:

```
hostname> inet dhcp server lease clear
3 lease entries have been deleted.
```

- Чтобы удалить из списка аренды адрес 192.168.1.1:

```
hostname> inet dhcp server lease clear address 192.168.1.1
1 lease entries have been deleted.
```

inet dhcp server mode

Включить или выключить автоматический запуск DHCP-сервера при загрузке ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения 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:

```
hostname# inet dhcp server mode on
```

inet dhcp server reset

Сбросить настройки DHCP-сервера, включая настройки автоматического запуска при загрузке ViPNet xFirewall, и завершить работу DHCP-сервера.

Синтаксис

```
inet dhcp server reset
```

Режимы командного интерпретатора

Администратор.

Особенности использования

После выполнения команды настройте параметры DHCP-сервера, иначе его запуск будет невозможен.

Пример использования

```
hostname# inet dhcp server reset

Are you sure to reset DHCP server settings to default values? [Yes/No]: Yes
```

inet dhcp server start

Запустить DHCP-сервер.

Синтаксис

```
inet dhcp server start
```

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

Starting DHCP server ...
```

inet dhcp server stop

Завершить работу DHCP-сервера.

Синтаксис

```
inet dhcp server stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet dhcp server stop
Stopping DHCP server ...
```

inet dns clients add

Добавить адрес или подсеть в список клиентов DNS-сервера, 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.

Пример использования

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

```
hostname# inet dns clients add 192.168.10.0/16
Client '192.168.10.0/16' appended to the list of allowed clients
```

inet dns clients delete

Удалить адрес или подсеть из списка клиентов DNS-сервера, 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.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

```
hostname# inet dns clients delete 192.168.0.7
Client '192.168.0.7' removed from the list of allowed clients
Reloading domain name service...: bind9.
```

inet dns clients list

Просмотреть список DNS-клиентов, которым разрешена передача запросов DNS-серверу.

Синтаксис

```
inet dns clients list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet dns clients list
Allow DNS requests from the following client(s):
any
192.168.0.4
192.168.0.3
```

```
192.168.0.5
```

inet dns filter add

Добавить DNS-фильтр, блокирующий доступ к указанному поддомену. Поддомен задается в виде шаблона, дополнительно можно указать IP-адрес перенаправления, который будет возвращаться при DNS-запросах к заблокированному поддомену.

Синтаксис

```
inet dns filter add <DNS-шаблон> [subst-with <адрес>]
```

Параметры и ключевые слова

- `<DNS-шаблон>` — шаблон поддомена, например `*.mail.ru`.
- `<адрес>` — IPv4-адрес перенаправления, который будет возвращаться при DNS-запросах к заблокированному поддомену.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Шаблон, задающий блокируемый поддомен, всегда должен начинаться с `*`.
- Блокировка поддомена начнет действовать после следующего перезапуска DNS-сервера.
- Блокировка поддомена будет работать только для клиентов, для которых ViPNet xFirewall задан в качестве DNS-сервера.

Примеры использования

Чтобы заблокировать доступ ко всем поддоменам домена `MAIL.RU`:

```
hostname# inet dns filter add *.mail.ru
```

inet dns filter delete

Удалить DNS-фильтр, блокирующий доступ к указанному поддомену. Поддомен задается в виде шаблона.

Синтаксис

```
inet dns filter delete <DNS-шаблон>
```

Параметры и ключевые слова

`<DNS-шаблон>` — шаблон поддомена, например `*.mail.ru`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Поддомен должен быть указан в том же виде, что при добавлении DNS-фильтра командой `inet dns filter add`.
- Изменения начнут действовать после следующего перезапуска DNS-сервера.

Примеры использования

Чтобы из списка DNS-фильтров удалить фильтр, блокирующий доступ к `*.mail.ru`:

```
hostname# inet dns filter delete *.mail.ru
```

inet dns filter list

Просмотреть список заблокированных DNS-поддоменов.

Синтаксис

```
inet dns dns filter list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet dns filter list

Blocked subdomain           Alt. IP-address

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

*.MAIL.RU

hostname>
```

inet dns filter refresh

Обновить список IPv4-адресов заблокированных поддоменов.

Синтаксис

```
inet dns filter refresh
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Обновление списка IPv4-адресов не применяет изменения в составе DNS-фильтров. Для применения изменений следует перезапустить DNS-сервер.

Примеры использования

Чтобы обновить список IPv4-адресов заблокированных доменов, заданных шаблонами DNS-фильтров:

```
hostname# inet dns filter refresh
```

inet dns forwarders add

Добавить сервер в список DNS-серверов перенаправления (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).

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
  ```

- Если DNS-сервер перенаправления не может разрешить доменное имя для указанной зоны, то для разрешения этого имени будут использоваться корневые DNS-серверы.

Примеры использования

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

  ```
  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:

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

inet dns forwarders delete

Удалить сервер 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-сервером (окончание доменного имени сетевых узлов, запросы от которых перенаправляются на DNS-сервер).

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе адреса работают автодополнение 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:

  ```
  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:

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

inet dns forwarders list

Просмотреть список DNS-серверов пересылки (forwarder).

Синтаксис

```
inet dns forwarders list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Если адреса DNS-серверов пересылки не заданы (список пустой), выводится информация о том, что используются корневые DNS-серверы.
- DNS-серверы, полученные по DHCP, отмечены как `from DHCP`.
- DNS-серверы, заданные пользователем, отмечены как `from USER`.

Пример использования

```
hostname> inet dns forwarders list
Forward DNS requests to servers:
10.0.2.3 from USERS
10.0.2.4 from USERS for-zone gov.ru
```

inet dns mode

Включить или выключить автоматический запуск DNS-сервера при загрузке ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Задается при установке справочников и ключей.

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска DNS-сервера, его текущее состояние не изменяется.
- Изменение настройки автоматического запуска не зависит от текущего состояния DNS-сервер (остановлен или запущен).

Пример использования

```
hostname# inet dns mode on

DNS server will be activated on next reboot

You need to start DNS server manually or reboot to have it running
```

inet dns start

Запустить DNS-сервер.

Синтаксис

```
inet dns start
```

Режимы командного интерпретатора

Администратор.

Пример использования

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

inet dns stop

Завершить работу DNS-сервера.

Синтаксис

```
inet dns stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet dns stop
Stopping domain name service...: bind9.
```

inet ifconfig address

Настроить параметры сетевого интерфейса.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе имени интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен относиться к классу `access` (см. inet ifconfig class).
- Если указанный интерфейс является рабочим для DHCP-сервера, то перед изменением его параметров завершите работу DHCP-сервера (см. inet dhcp server stop).
- При изменении адреса интерфейса в таблице маршрутизации автоматически изменяются все маршруты, связанные с этим интерфейсом. Скорректируйте 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.
- В качестве IP-адреса нельзя использовать 0.0.0.0.
- В качестве маски подсети нельзя использовать маски 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов нельзя задавать IP-адреса, относящиеся к одной подсети.
- Не изменяйте параметры сетевых интерфейсов, задействованных в работе кластера, если система защиты от сбоев запущена в режиме кластера горячего резервирования (см. failover show info). Иначе это может вызвать сбои в работе кластера.

Пример использования

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

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

inet ifconfig address add

Добавить дополнительный IP-адрес на сетевой 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.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автодополнение 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).
- 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

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

inet ifconfig address delete

Удалить дополнительный IP-адрес с сетевого 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.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автодополнение 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).

- 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:

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

inet ifconfig bonding ad-select

Задать режим 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

Используется режим `stable`.

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

inet ifconfig bonding add

Добавить подчиненный физический интерфейс к агрегированному.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Задаваемый подчиненный физический интерфейс должен относиться к классу `slave` (см. inet ifconfig class).
- 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 512.

Пример использования

Чтобы для агрегированного интерфейса `bond1` добавить физический интерфейс `eth2`:

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

inet ifconfig bonding delete

Удалить подчиненный интерфейс 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.

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`:

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

inet ifconfig bonding lacp-rate

Задать частоту 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

Обмен пакетами по протоколу LACP выполняется каждые 30 секунд (`slow`).

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

inet ifconfig bonding miimon

Задать частоту 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 (от 1 до 1000 миллисекунд).

Значения по умолчанию

Соединение проверяется каждые 100 миллисекунд (0,1 секунды).

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

inet ifconfig bonding primary

Настроить агрегированный интерфейс, работающий в режиме `balance-tlb` или `active-backup` (см. inet bonding add mode slaves). 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

Основной интерфейс выбирается в соответствии с выбранным режимом работы агрегированного канала (`none`).

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

inet ifconfig bonding xmit-hash-policy

Настроить агрегированный интерфейс, работающий в режиме `balance-xor` или `802.3ad` (см. inet bonding add mode slaves). 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 хэширования используются MAC-адреса отправителя и получателя пакета.
- `layer2+3` — алгоритм, при котором для хэширования используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протоколов IPv4 или IPv6).
- `layer3+4` — алгоритм, при котором для хэширования 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.

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`:

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

inet ifconfig class

Выбрать класс для сетевого 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.
- `slave` — класс интерфейсов, предназначенных для использования в составе агрегированных интерфейсов.
- `access` — класс интерфейсов, предназначенных для использования во всех остальных случаях.

Значения по умолчанию

Все физические интерфейсы ViPNet xFirewall относятся к классу `access`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если для указанного интерфейса смена класса выполняется впервые, то будет запрошено подтверждение операции.
- 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:

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

inet ifconfig dhcp

Установить режим DHCP на сетевом 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` — включить автоматический приём указанной настройки.
- `off` — выключить автоматический приём указанной настройки.

Значения по умолчанию

Для всех настроек, передаваемых с помощью DHCP, автоматический прием включен (`on`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Интерфейс должен относиться к классу `access` (см. inet ifconfig class) 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:

  ```
  hostname# inet ifconfig eth1 dhcp
  ```

- Чтобы установить на интерфейсе `eth2` режим DHCP и выключить автоматический прием маршрута по умолчанию:

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

inet ifconfig dhcp route-metric

Задать специфичную метрику маршрутам, поступающим от DHCP-сервера, на сетевом интерфейсе ViPNet xFirewall.

Синтаксис

```
inet ifconfig <интерфейс> dhcp route-metric {<метрика> | none}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<метрика>` — метрика. Возможные значения: 1–255.
- `none` — удаляет метрику на сетевом интерфейсе.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

- Чтобы назначить на сетевом интерфейсе `eth0` метрику 50:

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

- Чтобы удалить метрику на сетевом интерфейсе `eth0`:

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

inet ifconfig down

Выключить сетевой интерфейс.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

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`:

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

inet ifconfig reset

Сбросить настройки одного сетевого интерфейса либо всех интерфейсов.

Синтаксис

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

Параметры и ключевые слова

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

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 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).
  - Интерфейс будет выключен.
- Для виртуальных интерфейсов класса `slave` команда не выполняется.

- Для виртуальных интерфейсов VLAN по команде не сбрасываются настройки:
  - Имя соответствующего физического интерфейса.
  - Номер виртуального интерфейса VLAN.
- Для агрегированных интерфейсов по команде не сбрасываются настройки:
  - Имя агрегированного интерфейса.
  - Режим работы агрегированного интерфейса.
  - Частота проверки соединения на подчиненных физических интерфейсах.

Пример использования

Чтобы сбросить настройки интерфейса `eth1`:

```
hostname# inet ifconfig eth1 reset
This command will reset eth1 interface settings to default. Are you sure? [Yes/No]: Yes
done.
```

inet ifconfig mtu

Изменить значение MTU 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 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

Задать размер MTU, равный 3000 байт, для интерфейса `eth0`:

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

inet ifconfig speed

Задать параметры скорости сетевого интерфейса.

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

Синтаксис

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

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<скорость>` — скорость в Мбит/с. Возможные значения: `10`, `100`, `1000`, `10000` (для исполнений, оборудованных соответствующими интерфейсами).
- `duplex` — режим передачи данных:
    - `half` — полудуплекс;
    - `full` — полный дуплекс.
- `autoneg` — режим автосогласования скорости интерфейса (autonegotiation):

- `on` — включен;
- `off` — выключен.

Значения по умолчанию

На интерфейсе установлены автоматические параметры (определяются, исходя из характеристик интерфейса).

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автодополнение 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).
- 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.
- Нельзя изменить параметры скорости оптических интерфейсов (для исполнений, оборудованных соответствующими разъемами).

Пример использования

На интерфейсе `eth1` установить скорость 100 Мбит/с, режим полудуплекса и отключить режим автосогласования:

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

inet ifconfig speed auto

Установить режим автоматического определения параметров скорости на сетевом интерфейсе.

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.

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).

Пример использования

Установить режим автоматического определения параметров скорости на интерфейсе `eth1`:

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

inet ifconfig up

Включить сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> up
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

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`:

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

inet ifconfig vlan add

Создать интерфейс для виртуальной сети с заданным номером.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Физический интерфейс должен относиться к классу `trunk` (см. inet ifconfig class).
- 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 512.
- 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:

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

inet ifconfig vlan delete

Удалить виртуальный интерфейс.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить виртуальный интерфейс `eth1.2`:

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

inet ntp add

Добавить сервер в список NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp add {server | peer} {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- `server` — добавить NTP-сервер, работающий в одностороннем режиме (рассылка данных времени).
- `peer` — добавить NTP-сервер, работающий в двустороннем режиме (рассылка и получение данных времени).
- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<доменное имя>` — доменное имя NTP-сервера.

Режимы командного интерпретатора

Администратор.

Пример использования

Добавить сервер `ntp.psn.ru`, работающий в одностороннем режиме:

```
hostname# inet ntp add server ntp.psn.ru
NTP server ntp.psn.ru has been inserted successfully
```

inet ntp delete

Удалить сервер из списка NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp delete {server | peer} {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- `server` — удалить NTP-сервер, работающий в одностороннем режиме (рассылка данных времени).
- `peer` — удалить NTP-сервер, работающий в двустороннем режиме (рассылка и получение данных времени).
- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<доменное имя>` — доменное имя NTP-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы из списка NTP-серверов удалить сервер `ntp.psn.ru`, работающий в одностороннем режиме:

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

inet ntp list

Просмотреть список NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- NTP-серверы, полученные по DHCP, отмечены как `from DHCP`.
- NTP-серверы, заданные пользователем, отмечены как `from USER`.

Пример использования

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

inet ntp mode

Включить или выключить автоматический запуск NTP-сервера при загрузке ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Задается при установке справочников и ключей.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда изменяет только настройку автоматического запуска NTP-сервера, его текущее состояние не изменяется.

Пример использования

Выключить автоматический запуск NTP-сервера:

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

inet ntp orphan

Включить или выключить переход локального NTP-сервера в изолированный (orphan) режим при потере соединения с внешними NTP-серверами.

Синтаксис

```
inet ntp orphan {on <stratum> | off}
```

Параметры и ключевые слова

`<stratum>` — используется для задания уровня внешнего NTP-сервера. Если со всеми внешними NTP-серверами меньше указанного уровня не удается установить соединение в течение 5 минут, то локальный NTP-сервер переходит в изолированный режим. Допустимы значения 1—10, рекомендуемое значение 5.

Значения по умолчанию

По умолчанию установлено значение параметра `<stratum>` 5.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы настроить переход локального NTP-сервера в изолированный режим при потере соединения с внешними NTP-серверами 5го уровня:

```
hostname# inet ntp orphan on 5
```

inet ntp start

Запустить NTP-сервер.

Синтаксис

```
inet ntp start
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet ntp start
Starting NTP server...
```

inet ntp stop

Завершить работу NTP-сервера.

Синтаксис

```
inet ntp stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

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

inet ospf mode

Включить или выключить использование протокола OSPF.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить использование протокола OSPF;
- `off` — выключить использование протокола OSPF.

Режимы командного интерпретатора

Администратор.

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

Добавить сеть, в которой должна выполняться маршрутизация по протоколу OSPF.

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.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если использование протокола OSPF 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
```

inet ospf network delete

Удалить сеть, которая была указана как маршрутизируемая по протоколу OSPF.

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.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если использование протокола OSPF 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
```

inet ospf redistribute add

Включить перераспределение статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF.

Синтаксис

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

Параметры и ключевые слова

- `static` — включить перераспределение статических маршрутов;
- `dhcp` — включить перераспределение маршрутов DHCP-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда не будет выполнена в следующих случаях:

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

Пример использования

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

inet ospf redistribute delete

Выключить перераспределение статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF.

Синтаксис

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

Параметры и ключевые слова

- `static` — выключить перераспределение статических маршрутов;
- `dhcp` — выключить перераспределение маршрутов DHCP-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда не будет выполнена в следующих случаях:

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

Пример использования

```
hostname# inet ospf redistribute delete static

Redistribution of static routes has been disabled.
```

inet ospf priority

Задать приоритет ViPNet xFirewall.

Синтаксис

```
inet ospf priority <приоритет> [interface <интерфейс>]
```

Параметры и ключевые слова

- `<приоритет>` — целое число из диапазона 0 — 255.
- `<интерфейс>` — имя интерфейса.

Значения по умолчанию

Значение приоритета по умолчанию — 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Использование команды `inet ospf priority` разрешено, если на ViPNet xFirewall включен протокол маршрутизации OSPF (см. inet ospf mode).
- Чем больше значение приоритета, тем выше вероятность того, что ViPNet xFirewall будет выбран назначенным маршрутизатором DR или резервным назначенным маршрутизатором BDR.
- Если приоритет равен нулю, то ViPNet xFirewall не участвует в выборе DR или BDR.

- Если ключевое слово `interface` не задано, то значение приоритета для всех интерфейсов ViPNet xFirewall устанавливается равным параметру `<приоритет>`.

Пример использования

```
hostname# inet ospf priority 10

OSPF priority 10 has been set for this router.
```

inet ospf router-id

Задать идентификатор ViPNet xFirewall в формате адреса протокола IPv4.

Синтаксис

```
inet ospf router-id {<идентификатор> | auto}
```

Параметры и ключевые слова

- `<идентификатор>` — идентификатор ViPNet xFirewall в формате адреса протокола IPv4.
- `auto` — автоматический выбор идентификатора ViPNet xFirewall исходя из максимального значения IP-адреса, назначенного на интерфейсах ViPNet xFirewall.

Значения по умолчанию

Максимальное значение IP-адреса из назначенных на интерфейсах ViPNet xFirewall.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Использование команды разрешено, если на ViPNet xFirewall включен протокол маршрутизации OSPF (см. inet ospf mode).
- Если в сети со множественным доступом у двух маршрутизаторов будут одинаковые идентификаторы, то такие маршрутизаторы не смогут установить отношения соседства.

Пример использования

```
hostname# inet ospf router-id 172.16.12.1

Stopping Quagga monitor daemon: (waiting) .. watchquagga.

Loading capability module if not yet done.

Starting Quagga daemons (prio:10): (waiting)..
```

```
Stopping Quagga monitor daemon: (waiting) .. watchquagga.
Loading capability module if not yet done.
Starting Quagga monitor daemon: watchquagga.
OSPF router-id 172.16.12.1 has been set for this router.
```

inet ping

Проверить соединение с сетевым узлом.

Синтаксис

```
inet ping {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес узла (в виде октетов или шестнадцатеричного числа), с которым необходимо проверить соединение.
- `<доменное имя>` — доменное имя узла, с которым необходимо проверить соединение.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- IP-адрес в виде шестнадцатеричного числа перед выполнением опроса преобразовывается в корректный IPv4 адрес.
- Чтобы завершить проверку соединения нажмите **Ctrl+C**.

Пример использования

Чтобы проверить соединение с адресом 10.0.2.1:

```
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
```

inet route add

Добавить статический маршрут.

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.
- `[weight <1-255>]` — вес.

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).

- Параметры `distance` и `weight` можно задавать, только если задан параметр `netmask`.

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:

```
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

Удалить все маршруты, в том числе маршрут по умолчанию.

Синтаксис

```
inet route clear
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet route clear
```

inet route delete

Удалить маршрут.

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.

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.
```

inet show dhcp client

Просмотреть настройки DHCP на сетевых интерфейсах (настройки DHCP-клиента).

Синтаксис

```
inet show dhcp client
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде выводится следующая информация:

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

Пример использования

```
hostname> inet show dhcp client

Administrative distance for DHCP/PPP routes: 80

Default metric for DHCP/PPP routes: 60

Interface    DHCP       Routes     Metric      DNS         NTP

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

eth0         no         yes        default     yes         yes

eth1         yes        yes        50          yes         yes

...
```

inet show dhcp relay

Просмотреть настройки службы DHCP-relay и ее текущее состояние.

Синтаксис

```
inet show dhcp relay [<номер копии>]
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть настройки 2-ой копии службы DHCP-relay:

```
hostname> inet show dhcp relay 2
DHCP relay 2 started
External DHCP server X.X.X.X
External DHCP server interface eth2
Backup DHCP server Y.Y.Y.Y
Backup DHCP server interface eth2
Internal listen interfaces eth3.1 eth3.2
```

inet show dhcp server

Просмотреть настройки DHCP-сервера и его текущее состояние.

Синтаксис

```
inet show dhcp server
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

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
```

inet show dns

Просмотреть информацию о состоянии DNS-сервера.

Синтаксис

```
inet show dns
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

inet show interface

Просмотреть параметры и состояние сетевого интерфейса.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Если интерфейс не указан, выводится информация обо всех интерфейсах, включая дополнительные IP-адреса интерфейсов.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- При вводе интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- 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.
- 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 (см. inet ifconfig class). 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.
- Если в качестве параметра вы указали имя агрегированного интерфейса, дополнительно будет выведена информация:
  - режим работы агрегированного канала (см. inet bonding add mode slaves);
  - частота 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

Просмотреть информацию об интерфейсе `eth0`:

```
hostname> inet show interface eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
               inet 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
               ether 00:0c:29:51:3c:c7 txqueuelen 1000 (Ethernet)
               RX packets 352 bytes 57400 (56.0 KiB)
               RX errors 0 dropped 0 overruns:0 frame:0
               TX packets 118bytes 13001 (12.7 KiB)
               TX errors 0 dropped 0 overruns 0 frame 0 collisions 0

               Configured by DHCP: no
               Class: access

               Speed: 10000Mb/s
               Duplex: Full
               Auto-negotiation: off
               Link detected: yes
```

inet show mac-address-table

Просмотреть ARP-таблицу (таблицу, содержащую записи о преобразованиях IP-адресов в MAC-адреса).

Синтаксис

```
inet show mac-address-table [{interface <интерфейс> | address <IP-адрес> | hwaddress
<MAC-адрес> | vlan <интерфейс VLAN>}]
```

Параметры и ключевые слова

- `<интерфейс>` — фильтрация по имени сетевого интерфейса ViPNet xFirewall (физического или виртуального):
  - Если вы укажете физический сетевой интерфейс (например, `eth0`), для которого настроены виртуальные сетевые интерфейсы, то в выводе команды будут содержаться записи как для физического сетевого интерфейса, так и для всех виртуальных сетевых интерфейсов, настроенных на нем.
  - Если вы укажете виртуальный сетевой интерфейс (например, `eth0.1`), то в выводе команды будут содержаться записи только для указанного виртуального сетевого интерфейса

- `<IP-адрес>` — фильтрация по IP-адресу в формате X.X.X.X. В случае указания части IP-адреса будут выведены все записи, содержащие в подстроке указанную часть (октеты) IP-адреса.
- `<MAC-адрес>` — фильтрация по MAC-адресу в формате XX:XX:XX:XX:XX:XX. В случае указания только части MAC-адреса будут выведены все записи, содержащие в подстроке указанную часть MAC-адреса.
- `<интерфейс VLAN>` — фильтрация по номеру сетевого интерфейса VLAN ViPNet xFirewall (например, `vlan 1`).

Значения по умолчанию

Если параметр не указан, выводится вся ARP-таблица.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

- Просмотреть всю ARP-таблицу:

```
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
Found: 4
```

- Просмотреть ARP-таблицу с фильтрацией по сетевому интерфейсу `eth0`:

```
hostname> inet show mac-address-table interface eth0
Address     HWtype  HWaddress     Flags Iface
---------------------------------------------------------------
81.30.192.131  ether   1c:74:0d:10:16:3d C   eth0.1
81.30.192.132  ether   b4:b5:2f:89:bb:0d C   eth0.1
81.30.192.129  ether   00:1f:ca:b3:6c:c0 C   eth0.2
81.30.192.133  ether   64:d1:54:14:c5:53 C   eth0.2
Found: 4
```

- Просмотреть записи ARP-таблицы, содержащие часть IP-адреса 30.192:

```
hostname> inet show mac-address-table address 30.192
Address     HWtype  HWaddress     Flags Iface
---------------------------------------------------------------
81.30.192.131  ether   1c:74:0d:10:16:3d C   eth0.1
```

```
86.30.192.132  ether   b4:b5:2f:89:bb:0d C   eth0.1
218.15.30.192  ether   00:1f:ca:b3:6c:c0 C   eth0.2
81.30.192.133  ether   64:d1:54:14:c5:53 C   eth0.2
Found: 4
```

- Просмотреть записи ARP-таблицы, содержащие часть MAC-адреса `b4:b5:2f`:

```
hostname> inet show mac-address-table hwaddress b4:b5:2f
Address     HWtype  HWaddress     Flags Iface
-----------------------------------------------------------
81.30.192.132  ether   b4:b5:2f:89:bb:0d C   eth0.1
81.30.192.133  ether   14:c5:b4:b5:2f:53 C   eth0.2
10.0.0.1     ether   b4:b5:2f:b4:b5:2f C   eth1.1
Found: 3
```

inet show ntp

Просмотреть настройки и состояние NTP-сервера.

Синтаксис

```
inet show ntp
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- 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.
- Если NTP-сервер запущен, выводятся следующие параметры NTP-серверов, используемых для синхронизации:
  - `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.

Пример использования

```
hostname> inet show ntp
NTP server autostart 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
```

inet show ospf configuration

Просмотреть настройки протокола OSPF.

Синтаксис

```
inet show ospf configuration
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если протокол OSPF выключен, то при попытке выполнения команды выводится сообщение об ошибке: `error: OSPF protocol has not been enable`.

Пример использования

```
hostname> inet show ospf configuration

OSPF protocol has been enabled

OSPF protocol autostart is on

OSPF router id is 172.20.20.100

Redistribution of static routes is enabled.

Redistribution of DHCP routes is enabled.

Destination         Netmask             OSPF Area

172.20.20.0         255.255.255.0       0

172.20.21.0         255.255.255.0       1

Interface: OSPF priority

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

eth0: 1

eth1: 20

hostname>
```

По команде выводится следующая информация:

- состояние протокола OSPF: включен/выключен;
- состояние автоматического запуска протокола OSPF при старте ViPNet xFirewall: включен/выключен;
- идентификатор ViPNet xFirewall;
- состояние перераспределения статических маршрутов: включены/выключены;
- состояние перераспределения DHCP маршрутов: включены/выключены;
- список сетей, в которых ViPNet xFirewall осуществляет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
- приоритеты ViPNet xFirewall на интерфейсах.

inet show ospf database

Просмотреть информацию о состоянии каналов связей между всеми OSPF-маршрутизаторами в базе данных (link state database).

Синтаксис

```
inet show ospf database
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

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]
```

inet show ospf neighbour

Просмотреть сведения о соседних OSPF-маршрутизаторах, работающих в вашей сети по протоколу OSPF.

Синтаксис

```
inet show ospf neighbour
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

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
```

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

Просмотреть общую таблицу маршрутизации или списки маршрутов от конкретного источника (Static, DHCP, OSPF).

Синтаксис

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

Параметры и ключевые слова

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

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, P - PIM A - Babel, D - DHCP/PPP,
       > - 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
```

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

inet show vlan

Просмотреть список виртуальных интерфейсов.

Синтаксис

```
inet show vlan
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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.

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
```

inet snmp autostart

Включить или выключить запуск SNMP-агента при загрузке ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить запуск SNMP-агента при загрузке ViPNet xFirewall.
- `off` — выключить запуск SNMP-агента при загрузке ViPNet xFirewall.

Значения по умолчанию

Запуск SNMP-агента при загрузке ViPNet xFirewall выключен (`off`).

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы включить запуск SNMP-агента при загрузке ViPNet xFirewall:

```
hostname# inet snmp autostart on

SNMP agent is enabled and will be activated on next reboot.

You need to start the SNMP agent server manually or reboot to start it
```

inet snmp cluster node community

Задать community string, который используется для мониторинга узла кластера горячего резервирования по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp cluster node <IP-адрес> community
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда доступна только в режиме кластера горячего резервирования и только на активном узле кластера.
- При выполнении команды требуется ввести community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

Пример использования

```
hostname# inet snmp cluster node 172.168.0.1 community

Type community for 172.168.0.1: public1

Restarting SNMP Agent

New community for 172.168.0.1: public1
```

inet snmp cluster node context

Изменить контекст, назначенный узлу кластера горячего резервирования.

Синтаксис

```
inet snmp cluster node <IP-адрес> context <контекст>
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера (без маски).
- `<контекст>` — новое значение контекста для узла кластера. Допустимая длина — от 1 до 32 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита и цифры.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда доступна только в режиме кластера горячего резервирования и только на активном узле кластера.

Пример использования

```
hostname# inet snmp cluster node 172.168.0.1 context Node1
Restarting SNMP Agent
New context for 172.168.0.1: Node1
```

inet snmp cluster show

Просмотреть конфигурацию мониторинга кластера по протоколу SNMP.

Синтаксис

```
inet snmp cluster show [community]
```

Параметры и ключевые слова

`community` — показывать список community string для мониторинга кластера.

Режимы командного интерпретатора

- Пользователь (параметр `community` недоступен).
- Администратор.

Особенности использования

- Команда доступна только в режиме кластера горячего резервирования, на активном и пассивном узлах кластера.
- По команде отображается следующая информация:
  - разрешено или запрещено чтение SNMP-параметров по протоколам SNMPv1 и SNMPv2c;
  - IP-адреса интерфейсов синхронизации узлов кластера;
  - контексты, назначенные узлам кластера;
  - community string, заданные на узлах кластера (если не задано, отображается `Not set`). Данный параметр отображается, если указана лексема `community`.

Пример использования

```
hostname# inet snmp cluster show

RO communities for cluster nodes are OFF

IP-address   Context   Community

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

172.168.0.1   Node1    Not set

172.168.0.2   Node2    public2
```

inet snmp cluster v2

Разрешить или запретить чтение SNMP-параметров узлов кластера горячего резервирования по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp cluster v2 {on | off}
```

Параметры и ключевые слова

- `on` — разрешить.
- `off` — запретить.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда доступна только в режиме кластера горячего резервирования и только на активном узле кластера.
- Если чтение параметров по протоколам SNMPv1 и SNMPv2c запрещено с помощью команды inet snmp v2, команда не выполняется.
- Если при включении мониторинга кластера хотя бы на одном из узлов кластера не задано community string, выводится соответствующее сообщение.

Пример использования

```
hostname# inet snmp cluster v2 on

Restarting SNMP Agent

RO communities for cluster nodes is ON
```

inet snmp community add

Добавить community string (пароль) для чтения SNMP-параметров ViPNet xFirewall.

Синтаксис

```
inet snmp community add
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type new community string:` введите значение community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.
- Максимальное количество community string — 16.

Пример использования

Чтобы задать community string со значением `Mycommunity`:

```
hostname# inet snmp community add

Type new community string: Mycommunity

Restarting SNMP Agent
```

```
RO community Mycommunity created
```

inet snmp community change

Изменить community string для чтения SNMP-параметров ViPNet xFirewall.

Синтаксис

```
inet snmp community change
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- При выполнении команды требуется ввести текущее community string и новое значение community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

Пример использования

Чтобы изменить текущее community string со значения `MyCommunity` на значение `MyCommunity1`:

```
hostname# inet snmp community change
Type current community string: MyCommunity
Type new community string: MyCommunity1
Restarting SNMP Agent
RO community MyCommunity changed to MyCommunity1
```

inet snmp community delete

Удалить community string, используемый для чтения SNMP-параметров ViPNet xFirewall.

Синтаксис

```
inet snmp community delete
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type community string to delete:` введите значение community string.
- При вводе команды не поддерживается контекстная подсказка.

Пример использования

Чтобы удалить community string со значением `MyCommunity`:

```
hostname# inet snmp community delete
Type community string to delete: MyCommunity
Restarting SNMP Agent
RO community MyCommunity deleted
```

inet snmp community list

Просмотреть список community string для чтения SNMP-параметров ViPNet xFirewall.

Синтаксис

```
inet snmp community list
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1 и SNMPv2c.

Пример использования

```
hostname# inet snmp community list
community ro = private
```

inet snmp logging

Изменить уровень важности событий SNMP-агента, которые будут записываться в системный журнал ViPNet xFirewall.

Синтаксис

```
inet snmp logging <уровень важности>
```

Параметры и ключевые слова

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

- `off` — запись событий в журнал выключена.
- `critical` — в журнал записываются критические ошибки, после которых SNMP-агент не может продолжить работу.
- `error` — в журнал записываются ошибки, после которых SNMP-агент может продолжать работу.
- `info` — в журнал записывается полная информация о работе SNMP-агента.
- `debug` — в журнал записывается служебная информация, используемая при отладке.

Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

В системный журнал записываются критические ошибки и ошибки, после которых SNMP-агент может продолжать работу (`error`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

- Чтобы выключить регистрацию событий SNMP-агента в системном журнале ViPNet xFirewall:

  ```
  hostname# inet snmp logging off
  SNMP Agent logging is off
  ```

- Чтобы протоколировать полную информацию о работе SNMP-агента:

  ```
  hostname# inet snmp logging info
  New SNMP Agent syslog level is info
  ```

inet snmp port

Задать UDP-порт, на котором SNMP-агент будет принимать запросы.

Синтаксис

```
inet snmp port <порт>
```

Параметры и ключевые слова

`<порт>` — номер UDP-порта.

Значения по умолчанию

По умолчанию SNMP-агент использует UDP-порт 161.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- Если UDP-порт используется другой службой ViPNet xFirewall — выводится сообщение `UDP port already in use. Please choose another port.`

Пример использования

Чтобы SNMP-агент принимал запросы на UDP-порт 5252:

```
hostname# inet snmp port 5252

Restarting SNMP Agent

SNMP agent port set to 5252 UDP
```

inet snmp reset-engineid

Сгенерировать новый идентификатор `engineID` SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp reset-engineid
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Команду рекомендуется использовать для устранения проблем, связанных с получением сообщений от SNMP-агентов ViPNet xFirewall по протоколу SNMPv3, одной из причин которых может быть одинаковый `engineID` у SNMP-агентов. Не следует генерировать новый идентификатор `engineID` при нормальной работе системы мониторинга SNMP-агентов.
- В режиме кластера горячего резервирования команда генерирует новый `engineID` только на том узле кластера, на котором она вызвана.

Пример использования

Чтобы сгенерировать новый идентификатор `engineID`:

```
hostname# inet snmp reset-engineid

Restarting SNMP Agent

New EngineID = 0x80002A3C800D992556F6C6745E00000000
```

inet snmp show

Просмотреть информацию о текущем состоянии и настройках SNMP-агента.

Синтаксис

```
inet snmp show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname> inet snmp show

Net-SNMP agent is RUNNING.

ViPNet SNMP plugin is RUNNING.

SNMP agent autostart is ON.

Reading OIDs via SNMPv1 and SNMPv2c is OFF and sending traps is OFF

Reading OIDs via SNMPv3 is ON and sending traps is ON
```

```
Device info:
   Name = MyCoordinator
   Location = Branch_Office
   Contact = admin@infotecs.ru
   engineID = 0x80002A3C800D992556F6C6745E00000000

Current syslog level is error
SNMP agent use UDP port 161.
```

По команде выводится следующая информация:

- Статус SNMP-агента — запущен (`RUNNING`) или остановлен (`STOPPED`).
- Статус плагина ViPNet SNMP — запущен (`RUNNING`) или остановлен (`STOPPED`).
- Статус запуска SNMP-агента при перезагрузке ViPNet xFirewall — запуск включен (`ON`) или выключен (`OFF`).
- Статус работы по протоколам SNMPv1 и SNMPv2c и статус отправки SNMP-оповещений по протоколам SNMPv1 и SNMPv2c — разрешена (`ON`) или запрещена (`OFF`).
- Статус работы по протоколу SNMPv3 и статус отправки SNMP-оповещений по протоколу SNMPv3 — разрешена (`ON`) или запрещена (`OFF`).
- Информация о ViPNet xFirewall, доступная по SNMP: имя устройства, месторасположение, контактная информация, идентификатор устройства. Если имя устройства, месторасположение или контактная информация не заданы — выводится сообщение `Not set`.
- UDP-порт, используемый SNMP-агентом.

inet snmp start

Запустить встроенный SNMP-агент ViPNet xFirewall.

Синтаксис

```
inet snmp start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname# inet snmp start

Starting SNMP agent... done.
```

inet snmp stop

Завершить работу встроенного SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp stop
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname# inet snmp stop

Stopping SNMP agent... done.
```

inet snmp system contact

Задать параметр `mib-2.system.sysContact` («Контактное лицо») SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp system contact
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new syscontact:` введите значение параметра mib-2.system.sysContact.

- Допустимая длина строки параметра `mib-2.system.sysContact` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysContact` SNMP-агента ViPNet xFirewall сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.4.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysContact`).
- В режиме кластера горячего резервирования команда используется только на активном узле кластера.

Пример использования

Чтобы задать параметр `mib-2.system.sysContact`:

```
hostname# inet snmp system contact
Type new syscontact: admin@mycompany.ru
Restarting SNMP Agent
Syscontact set successfully. New syscontact = admin@mycompany.ru
```

inet snmp system location

Задать параметр `mib-2.system.sysLocation` («Местоположение») SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp system location
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new syslocation:` введите значение параметра `mib-2.system.sysLocation`.
- Допустимая длина строки параметра `mib-2.system.sysLocation` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysLocation` SNMP-агента ViPNet xFirewall сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.6.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysLocation`).
- В режиме кластера горячего резервирования команда задает параметр `mib-2.system.sysLocation` только на том узле кластера, на котором она вызвана.

Пример использования

Чтобы задать параметр `mib-2.system.sysLocation` SNMP-агента ViPNet xFirewall:

```
hostname# inet snmp system location
Type new syslocation: Branch_Office
Restarting SNMP Agent
Syslocation set successfully. New syslocation = Branch_Office
```

inet snmp system name

Задать параметр `mib-2.system.sysName` («Имя устройства») SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp system name
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new sysname:` введите значение параметра `mib-2.system.sysName`.
- Допустимая длина строки параметра `mib-2.system.sysName` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysName` SNMP-агента ViPNet xFirewall сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.5.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysName`).
- В режиме кластера горячего резервирования команда задает параметр `mib-2.system.sysName` только на том узле кластера, на котором она вызвана.

Пример использования

Чтобы задать параметр `mib-2.system.sysName` SNMP-агента ViPNet xFirewall:

```
hostname# inet snmp system name
Type new sysname: MyCoordintor
Restarting SNMP Agent
Sysname set successfully. New sysname = MyCoordinator
```

inet snmp trapsink add

Добавить адрес сетевого узла, на который SNMP-агент ViPNet xFirewall будет отправлять оповещения.

Синтаксис

```
inet snmp trapsink add <адрес> [port <номер>] [{v1 | inform}]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта, на который отправлять оповещения.
- `v1` — отправлять оповещения типа TRAP по протоколу SNMPv1.
- `inform` — отправлять оповещения типа INFORM по протоколу SNMPv2c.

Значения по умолчанию

- Если порт не задан, используется порт UDP 162.
- Если тип оповещений не задан, используется тип TRAP по протоколу SNMPv2c.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type community string for sending traps:` введите значение community string, которое задано на сетевом узле, получающем SNMP-оповещения (community-trap string).
- Максимальное количество сетевых узлов для SNMP-агента ViPNet xFirewall — 16.
- Допустимая длина community-trap string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `. * / - : _ ? = @ , &`.
- При указании параметра `v1`, отправка оповещений INFORM невозможна.
- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт (см. firewall add).

Пример использования

Чтобы SNMP-агент ViPNet xFirewall отправлял оповещения INFORM на UDP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp trapsink add 10.0.0.1 port 162 inform
```

```
Type community string for sending traps: trapcommynity1

Restarting SNMP Agent

Inform -> 10.0.0.1:162 UDP Community = trapcommynity1 added
```

inet snmp trapsink delete

Удалить адрес сетевого узла, на который SNMP-агент ViPNet xFirewall отправляет оповещения.

Синтаксис

```
inet snmp trapsink delete <адрес> [port <номер>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- Если на SNMP-агенте ViPNet xFirewall заданы сетевые узлы с одинаковым IP-адресом и портом, но с разными community-trap string — удаляются все такие сетевые узлы.

Пример использования

Чтобы удалить сетевой узел с IP-адресом 10.0.0.1, принимающий SNMP-оповещения на UDP-порт 162:

```
hostname# inet snmp trapsink delete 10.0.0.1 port 162

Restarting SNMP Agent

Trap -> 10.0.0.1:162 UDP Community = trapcommynity1 deleted
```

inet snmp trapsink list

Просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения.

Синтаксис

```
inet snmp trapsink list [secure]
```

Параметры и ключевые слова

`secure` — отображать community-trap string.

Примечание. Ключевое слово `secure` доступно только в режиме Администратор.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1 и SNMPv2c.

Пример использования

- Чтобы просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения:

```
hostname> inet snmp trapsink list
Trap {v1|v2c} -> 101.101.101.211:162 UDP

Trap {v1|v2c} -> my-domain.org:162 UDP

Inform -> 10.10.10.3:162 UDP
```

- Чтобы просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения, включая community-trap string:

```
hostname# inet snmp trapsink list secure
Trap {v1|v2c} -> 101.101.101.211:162 UDP
Community = trapcommunity2

Trap {v1|v2c} -> my-domain.org:162 UDP
Community = trapcommunity3

Inform -> 10.10.10.3:162 UDP
Community = trapcommunity2
```

inet snmp user add

Добавить пользователя SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp user add <имя пользователя> [{md5 | sha}]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `md5` или `sha` — алгоритм хэширования пароля пользователя.

Значения по умолчанию

Алгоритм хэширования пароля пользователя — MD5.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Допустимая длина имени пользователя — от 1 до 32 символов. Разрешенные символы имени пользователя — прописные и строчные буквы латинского алфавита и цифры.
- При выполнении команды требуется дважды ввести пароль пользователя. При вводе паролей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешенные символы пароля — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- Максимальное количество пользователей на SNMP-агенте ViPNet xFirewall — 32.
- Пользователь создается с правом на чтение SNMP-параметров.

Пример использования

Чтобы добавить нового пользователя `user1` и задать алгоритм хэширования пароля `sha`:

```
hostname# inet snmp user add user1 sha

Type the new user1 password:

Confirm the new user1 password:

Restarting SNMP Agent

User1 created
```

inet snmp user delete

Удалить пользователя SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp user delete <имя пользователя>
```

Параметры и ключевые слова

`<имя пользователя>` — имя пользователя SNMP.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы удалить пользователя `user1`:

```
hostname# inet snmp user delete user1
Restarting SNMP Agent
user1 deleted
```

inet snmp user list

Просмотреть список пользователей SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp user list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

```
hostname> inet snmp user list
user1:
```

```
  hash=MD5 encryption=OFF
  read = ON
  trapsess = OFF
user2:
  hash=SHA encryption=off
  read = OFF
  trapsess = ON
  Trap -> 101.101.101.211:162 UDP
user3:
  hash=SHA encryption=AES
  read = ON view = all
  trapsess = ON
  Trap -> my-domain.org:162 UDP
  Inform -> 10.10.10.3:162 UDP
user4:
  certname=user4
  read = ON view = all
```

По команде выводится список пользователей и настройки каждого из них:

- имя пользователя;
- настройка хэширования пароля;
- настройка шифрования данных;
- право чтения SNMP-параметров;
- право отправки SNMP-оповещений;
- параметры отправки SNMP-оповещений.

Примечание. Если пользователь использует TLS, вместо информации о хэшировании и шифровании выводится имя используемого сертификата.

inet snmp user set key

Создать, изменить или удалить ключ шифрования пользователя SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp user set <имя пользователя> key [off]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `off` — удалить ключ шифрования пользователя.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- При выполнении команды требуется дважды ввести ключ шифрования пользователя. При вводе ключей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина ключа шифрования — от 8 до 32 символов. Разрешенные символы ключа — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

Внимание! Не используйте повторяющиеся последовательности символов в ключе шифрования. Иначе его хэш может совпасть с хэшем другого ключа. Например, ключи AbcdAbcd и AbcdAbcdAbcd будут иметь одинаковые хэши. Подробнее см. RFC 3414.

- Для шифрования данных используется алгоритм AES-128.

Пример использования

- Чтобы создать ключ шифрования пользователя `user1`, для которого ключ не создавался или был удален:

```
hostname# inet snmp user set user1 key
Type the privacy key for user1:
Confirm the privacy key for user1:
Restarting SNMP Agent
Privacy key for User1 created
```

- Чтобы изменить ключ шифрования пользователя:

```
hostname# inet snmp user set user1 key
Type the privacy key for user1:
Confirm the privacy key for user1:
Restarting SNMP Agent
Privacy key for User1 changed
```

- Чтобы удалить ключ шифрования пользователя `user1`:

```
hostname# inet snmp user set user1 key off
Restarting SNMP Agent
Privacy key for User1 deleted
```

inet snmp user set name

Изменить имя пользователя SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp user set <имя пользователя> name <новое имя пользователя>
```

Параметры и ключевые слова

- `<имя пользователя>` — текущее имя пользователя SNMP.
- `<новое имя пользователя>` — новое имя пользователя SNMP.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Допустимая длина имени пользователя — до 32 символов. Разрешенные символы имени пользователя — прописные и строчные буквы латинского алфавита и цифры.
- При успешном выполнении команды:
  - Пароль пользователя остается без изменений.
  - Если для пользователя настроено шифрование данных (см. inet snmp user set key), ключ шифрования остается без изменений.
  - Если для пользователя выполнены настройки отправки оповещений, имя пользователя в них будет изменено.

Пример использования

Чтобы изменить имя пользователя с `user1` на `user2`:

```
hostname# inet snmp user set user1 name user2
Username for user1 changed to user2
Restarting SNMP Agent
```

inet snmp user set passwd

Изменить пароль пользователя SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp user set <имя пользователя> passwd [{md5 | sha}]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `md5` или `sha` — алгоритм хэширования пароля.

Значения по умолчанию

Алгоритм хэширования пароля пользователя — MD5.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- При выполнении команды требуется дважды ввести новый пароль пользователя. При вводе паролей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешенные символы пароля — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

Внимание! Не используйте повторяющиеся последовательности символов в пароле. Иначе его хэш может совпасть с хэшем другого пароля. Например, пароли AbcdAbcd и AbcdAbcdAbcd будут иметь одинаковые хэши. Подробнее см. RFC 3414.

Пример использования

Чтобы изменить пароль пользователя `user1` и задать алгоритм хэширования пароля `sha`:

```
hostname# inet snmp user set user1 passwd sha

Type the new user1 password:

Confirm the new user1 password:

Restarting SNMP Agent

Password for User1 changed
```

inet snmp user set read

Разрешить или запретить чтение SNMP-параметров (OID) для пользователя SNMP-агента ViPNet xFirewall.

Синтаксис

```
inet snmp user set <имя пользователя> read {on | off}
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `on` — разрешить чтение.
- `off` — запретить чтение.

Значения по умолчанию

При добавлении пользователя (см. inet snmp user add) чтение по умолчанию разрешено.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы запретить пользователю `user1` чтение SNMP-параметров:

```
hostname# inet snmp user set user1 read off
Restarting SNMP Agent
Reading OID for user1 is off
```

inet snmp user set trapsess

Разрешить или запретить отправку SNMP-оповещений для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess {on | off}
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `on` — разрешить отправку.
- `off` — запретить отправку.

Значения по умолчанию

Отправка оповещений запрещена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы разрешить отправку оповещений для пользователя `user1`:

```
hostname# inet snmp user set user1 trapsess on

Restarting SNMP Agent

Sending traps for user1 is on
```

inet snmp user set trapsess add

Добавить адрес сетевого узла, на который SNMP-агент ViPNet xFirewall будет отправлять оповещения для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess add <адрес> [port <номер>] [inform]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта, на который отправлять оповещения.
- `inform` — отправлять оповещения типа INFORM.

Значения по умолчанию

- Если порт не задан, используется порт UDP 162.
- Если лексема `inform` не указана, используется тип TRAP.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Максимальное количество сетевых узлов для всех пользователей SNMP-агента ViPNet xFirewall — 16.
- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт (см. firewall add).

Пример использования

Чтобы SNMP-агент ViPNet xFirewall отправлял оповещения TRAP для пользователя `user1` на UDP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp user set user1 trapsess add 10.0.0.1
Restarting SNMP Agent
Trap -> 10.0.0.1:162 UDP for user1 added
```

inet snmp user set trapsess delete

Удалить адрес сетевого узла, на который SNMP-агент ViPNet xFirewall отправляет оповещения для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess delete <адрес> [port <номер>]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы SNMP-агент ViPNet xFirewall перестал отправлять сообщения для пользователя `user1` на TCP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp user set user1 trapsess delete 10.0.0.1 port 162

Restarting SNMP Agent

Trap -> 10.0.0.1:162 UDP for user1 deleted
```

inet snmp v2

Разрешить или запретить чтение SNMP-параметров (OID) и отправку SNMP-оповещений по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp v2 {ro | traps} {on | off}
```

Параметры и ключевые слова

- `ro` — чтение SNMP-параметров:
  - `on` — разрешить.
  - `off` — запретить.
- `traps` — отправка SNMP-оповещений:
  - `on` — разрешить.
  - `off` — запретить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-оповещений запрещена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

До выполнения команды `inet snmp v2 traps on`, которая разрешает отправку SNMP-оповещений, добавьте хотя бы один сетевой узел (см. inet snmp trapsink add).

Пример использования

- Чтобы разрешить чтение SNMP-параметров:

```
hostname# inet snmp v2 ro on
Restarting SNMP Agent
Reading OIDs via SNMPv1 and SNMPv2c is ON
```

- Чтобы разрешить отправку SNMP-оповещений:

```
hostname# inet snmp v2 traps on
Restarting SNMP Agent
Sending traps via SNMPv1 and SNMPv2c is ON
```

inet snmp v3

Разрешить или запретить чтение SNMP-параметров (OID) и отправку SNMP-оповещений по протоколу SNMPv3.

Синтаксис

```
inet snmp v3 {ro | traps} {on | off}
```

Параметры и ключевые слова

- `ro` — чтение SNMP-параметров:
  - `on` — разрешить.
  - `off` — запретить.
- `traps` — отправка SNMP-оповещений:
  - `on` — разрешить.
  - `off` — запретить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-оповещений запрещена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

До выполнения команды `inet snmp v3 traps on`, которая разрешает отправку SNMP-оповещений, добавьте хотя бы один сетевой узел (см. inet snmp user set trapsess add).

Пример использования

- Чтобы разрешить чтение SNMP-параметров:

```
hostname# inet snmp v3 ro on
Restarting SNMP Agent
Reading OIDs via SNMPv3 is ON
```

- Чтобы разрешить отправку SNMP-оповещений:

```
hostname# inet snmp v3 traps on
Restarting SNMP Agent
Sending traps via SNMPv3 is ON
```

inet ssh

Подключиться к удаленному узлу по протоколу SSH.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе идентификатора работают автодополнение 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`:

```
hostname# inet ssh id 0x270e000a
user password:
```

inet vlan comment add

Добавить комментарий к виртуальной сети.

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.

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

inet vlan comment delete

Удалить комментарий к виртуальной сети.

Синтаксис

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

Параметры и ключевые слова

`<номер>` — номер виртуальной сети.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы удалить комментарий к виртуальной сети с номером 10:

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

Команды группы iplir

Команды группы `iplir` предназначены для настройки параметров работы в сети ViPNet.

Внимание! Для команд подгруппы `iplir option` контекстная справка не поддерживается.

iplir config

Редактировать один из файлов конфигурации: основной файл конфигурации или файл конфигурации заданного интерфейса.

Синтаксис

```
iplir config [<интерфейс>]
```

Параметры и ключевые слова

`<интерфейс>` — имя статического интерфейса, для которого требуется редактировать файл конфигурации.

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 службы `iplircfg` (см. iplir stop).

Пример использования

Чтобы отредактировать файл конфигурации интерфейса `eth0`:

```
hostname# iplir config eth0
```

iplir info

Просмотреть информацию о своем узле, а также статистику фильтрации IP-пакетов по сетевому интерфейсу.

Синтаксис

```
iplir info [<интерфейс>]
```

Параметры и ключевые слова

`<интерфейс>` — имя статического интерфейса, для которого требуется просмотреть статистику фильтрации IP-пакетов.

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.
- Служба `iplircfg` должна быть запущена.

Пример использования

Чтобы просмотреть статистку по интерфейсу `eth0`:

```
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
```

iplir option get

Просмотреть состояние или значение одного из параметров межсетевого экрана.

Синтаксис

```
iplir option get <параметр>
```

Параметры и ключевые слова

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

- `antispoofing` — состояние функции антиспуфинга.
- `block-fragmented-packets` — состояние функции блокирования фрагментированных IP-пакетов, передаваемых по всем сетевым интерфейсам.
- `connection-ttl-ip` — время жизни соединений по протоколу IP (для транспортных протоколов, отличных от TCP или UDP).
- `connection-ttl-tcp` — время жизни соединений по протоколу TCP.
- `connection-ttl-udp` — время жизни соединений по протоколу UDP.
- `max-connections` — максимальное количество параллельно установленных соединений.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть состояние функции блокирования фрагментированных IP-пакетов:

```
hostname> iplir option get block-fragmented-packets
Option: Block-fragmented-packets State: On
```

iplir option set antispoofing

Включить или выключить антиспуфинг.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить антиспуфинг;
- `off` — выключить антиспуфинг.

Значения по умолчанию

Антиспуфинг выключен (`off`).

Режимы командного интерпретатора

Администратор.

Пример использования

Включить антиспуфинг:

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

iplir option set block-fragmented-packets

Включить или выключить блокирование входящих фрагментированных IP-пакетов, которые принимаются по всем сетевым интерфейсам.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить блокирование;
- `off` — отключить блокирование.

Значения по умолчанию

По умолчанию блокирование выключено (`off`).

Режимы командного интерпретатора

Администратор.

Пример использования

Включить блокирование:

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

iplir option set connection-ttl-ip

Задать время жизни соединений по протоколу IP при отсутствии активности в нем.

Синтаксис

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

Параметры и ключевые слова

`<интервал>` — время жизни в секундах. Возможные значения: 0-65535.

Значения по умолчанию

300 секунд (`300`).

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

iplir option set connection-ttl-tcp

Задать время жизни соединений по протоколу TCP при отсутствии активности в нем.

Синтаксис

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

Параметры и ключевые слова

`<интервал>` — время жизни в секундах. Возможные значения: 0–65535.

Значения по умолчанию

1800 секунд (`1800`).

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

iplir option set connection-ttl-udp

Задать время жизни соединений по протоколу UDP при отсутствии активности в нем.

Синтаксис

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

Параметры и ключевые слова

`<интервал>` — время жизни в секундах. Возможные значения: 0–65535.

Значения по умолчанию

300 секунд (`300`).

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

iplir option set max-connections

Задать максимальное количество параллельно установленных соединений.

Синтаксис

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

Параметры и ключевые слова

`<количество>` — количество соединений. Допустимый диапазон: 1-1000000.

Значения по умолчанию

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

Таблица 1. Значения параметра max-connection для исполнений ViPNet xFirewall

Исполнение	Максимальное значение	Значение по умолчанию
xF100 N1	150000	150000
xF1000 Q5, Q6	1000000	500000
xF1000 Q7, Q8	20000000	5000000
xF5000 Q1	10000000	5500000
xF5000 Q2	30000000	10000000
xF-VA	2000000	1000000
xF-VA100	300000	150000
xF-VA500	2000000	1000000
xF-VA1000	5000000	2500000
xF-VA2000	8000000	4000000
xF-VA5000	10000000	5000000

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы установить максимальное количество одновременных соединений равным 200000:

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

iplir ping

Проверить соединение с сетевым узлом ViPNet.

Синтаксис

```
iplir ping <идентификатор>
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- При вводе идентификатора работают автодополнение и подсказка, данные для подсказки берутся из списка связей ViPNet xFirewall с другими узлами.
- Служба `iplircfg` должна быть запущена.

Пример использования

Чтобы проверить связь ViPNet xFirewall с узлом, который имеет идентификатор `0x15ea000d`:

```
hostname> iplir ping 0x15ea000d

Check connection with 0x15ea000d...

Connection successful
```

iplir show adapters

Просмотреть все активные статические интерфейсы ViPNet xFirewall. При просмотре для каждого интерфейса в списке указан параметр `allowtraffic`, который показывает, разрешено или заблокировано прохождения IP-трафика через интерфейс.

Синтаксис

```
iplir show adapters
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть список активных сетевых интерфейсов:

```
hostname> iplir show adapters

Active interface    Allowtraffic

eth0                on

eth1                on

eth2                off

eth3                on
```

iplir show cipher-mode

Просмотреть информацию о текущем режиме шифрования.

Синтаксис

```
iplir show cipher-mode
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

iplir show config

Просмотреть один из файлов конфигурации: основной файл конфигурации или файл конфигурации заданного интерфейса.

Синтаксис

```
iplir show config [<интерфейс>]
```

Параметры и ключевые слова

`<интерфейс>` — имя статического интерфейса, файл конфигурации которого требуется просмотреть.

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>`.
- Чтобы завершить просмотр файла конфигурации нажмите **Q**.

Пример использования

Чтобы просмотреть основной файл конфигурации:

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

iplir show firewall status

Просмотреть статистику работы межсетевого экрана.

Синтаксис

```
iplir show firewall status
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> iplir show firewall status
Max connections  150000
TCP SYN SENT timeout  30
```

```
TCP SYN RECV timeout  30
TCP WAIT timeout  15
Connection ttl TCP  3600
Connection ttl UDP  40
Connection stream ttl UDP  180
ICMP timeout  10
Connection ttl IP  300
Total connections count  172
Public connections count  171
VPN connections count  1
hostname>
```

По команде выводится следующая информация:

- `Max connections` — максимальное количество одновременных соединений (см. iplir option set max-connections).
- `TCP SYN SENT timeout` — таймаут установления TCP-соединения в режиме ожидания в секундах.
- `TCP SYN RECV timeout` — таймаут установления TCP-соединения в режиме запроса в секундах.
- `Connection ttl TCP` — время жизни TCP-соединения в секундах.
- `Connection ttl UDP` — время жизни UDP-соединения.
- `Connection stream ttl UDP` — время жизни потокового 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

Просмотреть информацию о ключах, входящих в состав лицензии, установленной на ViPNet xFirewall:

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

Синтаксис

```
iplir show key-info
```

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).
- После смены варианта персонального ключа в строке `Current personal key update date` может отображаться дата предыдущего обновления персонального ключа.

Пример использования

```
hostname> iplir show key-info
Current personal key info:                //Информация о персональном ключе
 User ID: 0x16310029
 Current personal key variant: 0
 Master personal key date: 2022-04-23 13:44:57 MSK
 Master personal key number: 1
 Current personal key update date: 2022-05-25 15:40:24 MSK
Spare personals keys set info:                    //Информация о РНПК
 User ID: 0x3307000e
 Personals keys variants: from 0 to 19
 Master personal key date : 2022-06-07 17:52:50 +05
Lck key info:                        //Информация о ключах узла
 User ID: 0x3307000e
 Master defense key date : 2022-06-07 17:52:50 +05
Current defense key info:
 AP ID: 0x1631002a
 Current defense key variant: 0
 Master defense key date: 2022-04-23 13:44:57 MSK
 Master defense key number: 1
 Current defense key update date: 2022-05-25 15:40:24 MSK
Cck key info:
```

```
Ap ID: AP ID: 0x1631002a
Master cck key date: 2022-06-23 13:44:57 MSK
```

iplir show keys-upgrade-log

Просмотреть журнал, в котором содержится информация о принятых обновлениях справочников и лицензии.

Синтаксис

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

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# iplir show keys-upgrade-log
19/01/2022 16:37:34.896 Starting upgrade process ...
19/01/2022 16:37:34.896 try find /opt/vipnet/ccc/ap*.dtm
...
```

iplir start

Запустить управляющую службу `iplircfg`.

Синтаксис

```
iplir start
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> iplir start
Loading DPI modules
Loading Kernel Interface driver
Loading stream helper module
Loading Iplir Watchdog driver
Loading IpLir Crypto driver
Loading IpLir driver
```

```
Loading IPCLS driver
Loading IpLir
```

iplir stop

Завершить работу управляющей службы `iplircfg`.

Синтаксис

```
iplir stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

iplir view

Просмотреть журнал регистрации IP-пакетов.

Синтаксис

```
iplir view
```

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.
- Служба `iplircfg` должна быть запущена.
- При работе ViPNet xFirewall в режиме кластера горячего резервирования на пассивном узле кластера нельзя просмотреть журнал IP-пакетов.

Пример использования

```
hostname# iplir view
```

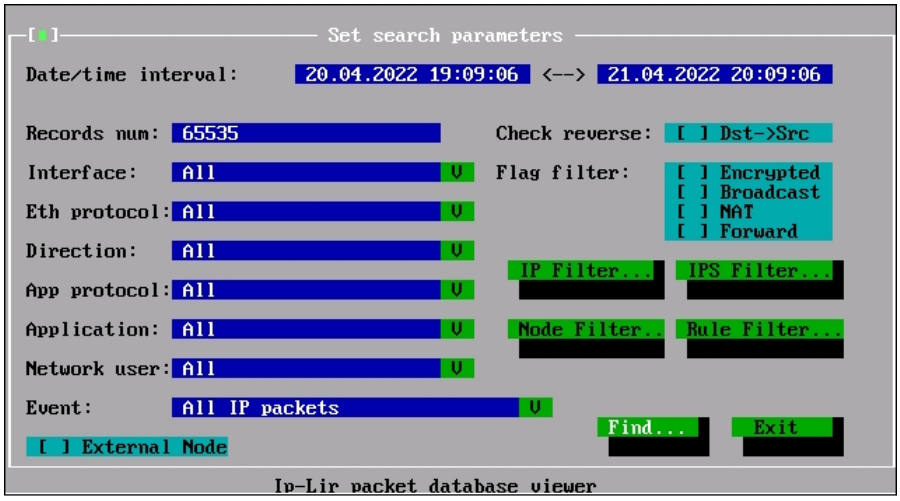

Рисунок 1. Задание параметров поиска записей в журнале регистрации IP-пакетов

Команды группы machine

Выключение и перезагрузка ViPNet xFirewall, установка имени компьютера и системного времени, работа с системным журналом, а также регламентное тестирование ViPNet xFirewall.

machine halt

Выключить ViPNet xFirewall.

Синтаксис

```
machine halt
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> machine halt
Shutting down failover daemon
Shutting down ViPNet Web GUI service
Shutting down MFTP daemon
..
Shutting down IpLir
```

machine reboot

Перезагрузить ViPNet xFirewall.

Синтаксис

```
machine reboot
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> machine reboot

Shutting down failover daemon

Shutting down ViPNet Web GUI service

Shutting down MFTP daemon

..

Shutting down IpLir
...
```

machine self-test

Запустить регламентное тестирование ViPNet xFirewall.

Синтаксис

```
machine self-test
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команду нельзя использовать при удаленном администрировании с помощью SSH.
- До начала тестирования работа всех служб 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 службы, 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 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?[Yes/No]: y
>> Stop Daemons...
stopped /usr/sbin/crond (pid 6021)
Stopping Advanced Configuration and Power Interface daemon: acpid.
Shutting down IpLir
...
```

machine set dailyreboot mode

Включить или выключить ежедневную перезагрузку ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить ежедневную перезагрузку.
- `off` — выключить ежедневную перезагрузку.

Значения по умолчанию

Ежедневная перезагрузка выключена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед перезагрузкой завершается работа всех служб и драйверов ViPNet xFirewall.

Пример использования

Чтобы включить ежедневную перезагрузку:

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

machine set dailyreboot time

Задать время ежедневной перезагрузки ViPNet xFirewall.

Синтаксис

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

Параметры и ключевые слова

`<время>` — время перезагрузки в формате `hh:mm`, где `hh` — часы (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:

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

machine set date

Изменить дату и время.

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` — часы, `mm` — минуты, `ss` — секунды.

Режимы командного интерпретатора

Администратор.

Особенности использования

- После ввода даты и времени необходимо подтвердить действие — ввести `Yes` и нажать **Enter**.
- Дата и время на ViPNet xFirewall не должны отличаться от даты и времени узлов сети ViPNet более чем на величину `timediff`. Иначе текущие управляющие соединения с ViPNet xFirewall будут разорваны, а новые управляющие соединения невозможно будет установить.

Пример использования

Чтобы установить дату 15 апреля 2022 года и время, равное 12 часам:

```
hostname# machine set date 2022-04-15 12:00:00
warning: changing date-time process requires VPN services to be restarted
warning: incorrect date and time settings may lead to appliance malfunction
Change current time?
Continue? [Yes No]: Yes
SSLsplit process stopped
Shutting down failover daemon
Shutting down ViPNet Web GUI service
Shutting down MFTP daemon
...
```

machine set hostname

Изменить имя узла.

Синтаксис

```
machine set hostname <имя>
```

Параметры и ключевые слова

`<имя>` — имя узла.

Значения по умолчанию

Имя узла сформировано по шаблону `<название>-<идентификатор>`, где `название` — наименование исполнения ViPNet xFirewall, `идентификатор` — идентификатор сетевого узла. Например: `xF1000-270E033A`

Режимы командного интерпретатора

Администратор.

Особенности использования

Имя узла 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 узла `xF1000`:

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

machine set log invalid-packet

Включить и отключить запись нарушений параметров таблицы соединений в системный журнал.

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

Нарушения параметров таблицы соединений записываются в журнал (`on`).

Режимы командного интерпретатора

Администратор.

Пример использования

Для включения записи нарушений параметров таблицы соединений в системный журнал:

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

machine set log queue

Включить или выключить запись событий о входящих IP-пакетах, обработка которых была отклонена в рамках приоритетной обработки трафика, в системный журнал.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

События об отклоненных IP-пакетах записываются в журнал (`on`).

Режимы командного интерпретатора

Администратор.

Пример использования

Для включения записи в системный журнал событий об отклоненных IP-пакетах:

```
hostname# machine set log queue on
```

machine set loghost

Задать место хранения системного журнала. 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 котором будет храниться системный журнал (удаленное ведение журнала).
- `local` — хранить системный журнал на ViPNet xFirewall (локальное ведение журнала).
- `null` — выключить ведение журнала.

Значения по умолчанию

Системный журнал хранится на ViPNet xFirewall (`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 узла, 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 пассивном узле кластера, так как данные настройки не передаются с активного узла на пассивный в ходе резервирования.

Пример использования

Для отправки системного журнала на узел с адресом 192.168.10.10:

```
hostname# machine set loghost 192.168.10.10
```

machine set session-timeout

Задать допустимое время 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, кратное 10 (10, 20, 30 и так далее). Допустимые значения: `0-65530`. При значении равном `0` параметр отключен (сессия не будет завершена при неактивности).

Значения по умолчанию

Время неактивности удаленной сессии 30 минут.

Режимы командного интерпретатора

Администратор.

Особенности использования

SSH-сессия будет завершена через время неактивности, заданное в параметре `<время>`, плюс до 5 минут погрешности.

Пример использования

Чтобы установить допустимое время неактивности удаленной сессии 1 час:

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

machine set timezone

Задать временную зону (часовой пояс).

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.

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:

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

```
hostname# machine set timezone Antarc
```

- Чтобы установить часовой пояс Москвы:

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

machine show dailyreboot

Просмотреть настройки ежедневной перезагрузки ViPNet xFirewall.

Синтаксис

```
machine show dailyreboot
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show date

Просмотреть дату и время, установленные на ViPNet xFirewall.

Синтаксис

```
machine show date
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> machine show date
Thu Jan 27 19:11:56 MSK +7 2022
```

machine show hostname

Просмотреть имя ViPNet xFirewall.

Синтаксис

```
machine show hostname
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show log invalid-packet

Просмотреть настройку записи нарушений параметров таблицы соединений в системный журнал (см. machine set log invalid-packet).

Синтаксис

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show log queue

Просмотреть настройку записи событий об отклоненных IP-пакетах в системный журнал (см. machine set log queue).

Синтаксис

```
machine show log queue
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> machine show log queue
Option is: ON
```

machine show loghost

Просмотреть настройки хранения системного журнала.

Синтаксис

```
machine show loghost
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде выводится одно из следующих значений:

- `null` — ведение журнала выключено.
- `local` — системный журнал хранится локально на ViPNet xFirewall.
- IP-адрес удаленного сетевого узла, заданный с помощью команды `machine set loghost` (см. machine set loghost).

Пример использования

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

machine show logs

Просмотреть системный журнал.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Чтобы завершить просмотр нажмите **Q**.
- Параметр `<время>` задается в формате `YYYY-MM-DD hh:mm:ss`
- В параметре `<служба>` можно указать одну из служб в составе ПО ViPNet xFirewall. Полный список служб см. в документе «ViPNet xFirewall. Настройка с помощью командного интерпретатора», в разделе «Список системных служб в составе ПО 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 `<служба>` или `string <строка>`.

Пример использования

- Чтобы найти все записи системного журнала за все время для всех служб:

  ```
  hostname# machine show logs
  ```
- Чтобы найти все записи системного журнала, начиная с 14:50 22 февраля 2022 года, и отобразить их в обратном порядке:

  ```
  hostname# machine show logs reversed since 2022-02-22 14:50:00
  ```
- Чтобы найти все записи системного журнала для службы `vmunix`:

  ```
  hostname# machine show logs filtered vmunix
  ```
- Чтобы найти записи системного журнала за все время его ведения для всех служб, где есть строка `command 3001`:

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

machine show memory

Просмотреть информацию об использовании оперативной памяти, файла подкачки и дискового пространства.

Синтаксис

```
machine show memory
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Информация об использовании оперативной памяти и файла подкачки (в Мбайт) выводится в виде таблицы, где строки соответствуют видам физической памяти:
  - `Mem` — оперативная память ОЗУ;
  - `Swap` — использование файла подкачки.

  Столбцы таблицы соответствует категориям выделенной или используемой памяти:
  - `total` — суммарный объем памяти;
  - `used` — объем используемой памяти без учета буферов ядра;
  - `free` — объем неиспользуемой памяти;
  - `shared` — объем разделяемой (shared) памяти
  - `buff/cache` — суммарное количество памяти, занятое операционной системой под буферы ядра и под страничный кэш;
  - `available` — объем памяти, доступный приложениям без использования файла подкачки.
- Информация об использовании дискового пространства выводится в виде таблицы, где строки соответствуют подключенным разделам файловой системы ViPNet xFirewall:
  - `tmpfs` — раздел, выделенный под файл подкачки;
  - `overlay` — объединенная файловая система ViPNet xFirewall.

  Таблица включает следующие столбцы:

  `Filesystem` — имя раздела файловой системы;

  `Size` — размер раздела файловой системы;

  `Used` — объем использованного пространства;

`Avail` — объем доступного пространства;

`Use%` — процент использования раздела файловой системы;

`Mounted on` — точка монтирования раздела файловой системы.

По умолчанию значения доступного и используемого дискового пространства выводятся в Кбайт. Для сокращенного вывода некоторых величин используются модификаторы размера:

- M — Мбайт;
- G — Гбайт.

Например, значение `2.0G` означает 2 Гбайт.

Пример использования

```
hostname> machine show memory
    total  used  free  shared  buff/cached  available
Mem:  2007   420    1485     0    102    362
Swap:   0    0    0

Filesystem  Size Used Avail Use% Mounted on
tmpfs    1004M  60M  944M  6% /mnt/root
overlay   2.0G  93M  1.9G  5% /
...
```

machine show session-timeout

Просмотреть допустимое время неактивности сессии.

Синтаксис

```
machine show session-timeout
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show timezone

Просмотреть информацию о временной зоне (часовом поясе), настроенной на ViPNet xFirewall.

Синтаксис

```
machine show timezone
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show uptime

Просмотреть время работы ViPNet xFirewall после загрузки, а также среднее число процессов в очереди за ближайшее время.

Синтаксис

```
machine show uptime
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде отображается следующая информация:

- текущее время;
- время работы ViPNet xFirewall после загрузки;
- текущее количество пользователей;
- среднее количество процессов в очереди ожидания процессора 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` (ddd).

Пример использования

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

machine swap mode

Включить или выключить использование файла подкачки.

Синтаксис

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

Параметры и ключевые слова

- `on` — использовать файл подкачки;
- `off` — не использовать файл подкачки.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

```
hostname# machine swap mode on

SWAP is enabled and will be enabled after reboot.
```

machine swap set

Задать размер файла подкачки, если такой будет использоваться в процессе работы ViPNet xFirewall.

Синтаксис

```
machine swap set <размер>
```

Параметры и ключевые слова

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

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.

Пример использования

```
hostname# machine swap set 2048

Creating swap. Please, wait...

 done.

Activating swap...

 done.
```

Команды группы mftp

Настройка параметров транспортного сервера MFTP и каналов обмена ViPNet xFirewall с другими узлами сети ViPNet.

mftp config

Редактировать конфигурационный файл службы `mftpd`.

Синтаксис

```
mftp config
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед редактированием конфигурационного файла завершите работу службы `mftpd`.
- 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 службы `mftpd`, а информации об изменении конфигурации сохраняется в системный журнал.

Пример использования

Чтобы включить режим немедленной передачи конвертов по каналу обмена с узлом `0x270e000a`:

```
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

Просмотреть очередь исходящих транспортных конвертов MFTP.

Синтаксис

```
mftp info
```

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.
- Чтобы завершить просмотр нажмите **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;
  - `Control request` — управляющий запрос;
  - `Control request answer` — ответ на управляющий запрос;

    - `Task receipt` — прикладная квитанция;
    - `Transport receipt` — транспортная квитанция.
- `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 `No data match query`.

mftp show config

Просмотреть конфигурационный файл транспортного сервера MFTP.

Синтаксис

```
mftp show config
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Чтобы завершить просмотр конфигурационного файла нажмите **Q**.

Пример использования

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

mftp start

Запустить службу `mftpd` (транспортный сервер MFTP).

Синтаксис

```
mftp start
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> mftp start
Loading MFTP daemon
..
```

mftp stop

Завершить работу службы `mftpd` (транспортный сервер MFTP).

Синтаксис

```
mftp stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

mftp view

Просмотреть журнал конвертов транспортного сервера MFTP.

Синтаксис

```
mftp view
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если вы выполняете команду на одном из узлов кластера горячего резервирования, отображается только информация о конвертах транспортного сервера, обработанных за периоды, когда этот узел был активным.
- Если имеется несколько файлов журнала транспортных конвертов, то они выводятся по порядку, начиная с последней даты. Чтобы после просмотра одного файла журнала открыть следующий, нажмите клавишу `q` и на запрос командного интерпретатора `Do you want to view the next mftp log file?` ответьте `Yes`.

Пример использования

```
hostname# mftp view
=== MFTP envelopes journal dump at Tue Feb 11 16:45:48 2022
-------------------------------------------------------------------------------
-----------------------------------------------------------------
| Envelope filename | Personal envelope name | Sender| Receiver           |Date-Time
 |     Event         |      Size   |      Description   |      Task          |
-----------------------------------------------------------------
| ~OJ)(#(A.RJ9      | ~OJ)(#(A.RJ9               | Admin     | xfva | 11.02.2022 16:45:48
 |     Received      |      19090  |                    | File exchange      |
-------------------------------------------------------------------------------
-----------------------------------------------------------------
hostname#
```

Журнал отображается в следующем формате:

- `Envelope filename, Personal envelope name` — имя конверта.
- `Sender` — имя узла-отправителя конверта.
- `Receiver` — 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.
- `Description` — описание конверта.
- `Task` — прикладная задача, в которой создан конверт.

Команды группы service

Команды группы `service` предназначены для управления пользователями, сертификатами, и системой предотвращения вторжений (IPS).

service cert delete cert

Удалить сертификат.

Синтаксис

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

Параметры и ключевые слова

`<сертификат>` — имя файла сертификата.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить сертификат с именем `Cert1.pem`:

```
hostname# service cert delete cert Cert1.pem
Certificate Cert1.pem is deleted
```

service cert delete crl

Удалить список аннулированных сертификатов (CRL).

Синтаксис

```
service cert delete crl <CRL>
```

Параметры и ключевые слова

`<CRL>` — имя файла списка аннулированных сертификатов.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы удалить CRL с именем `CRL1.pem`:

```
hostname# service cert delete crl CRL1.pem
CRL CRL1.pem is deleted
```

service cert delete private

Удалить закрытый ключ.

Синтаксис

```
service cert delete private <ключ>
```

Параметры и ключевые слова

`<ключ>` — имя файла закрытого ключа.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы удалить закрытый ключ с именем файла `Cert1_key.pem`:

```
hostname# service cert delete private Cert1_key.pem
Private key Cert1_key.pem is deleted
```

service cert import

Импортировать в локальное хранилище ViPNet xFirewall закрытый ключ сертификата, сертификат или список аннулированных сертификатов (CRL) с USB-накопителя.

Синтаксис

```
service cert import
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Поддерживает импорт только сертификатов, подписанных с использованием алгоритма RSA.
- Поддерживает импорт сертификатов в кодировке DER и Base64.
- В контейнере PEM (`.pem`) используется стандарт PKCS#12 (`.p12`).
- По команде выполняется поиск на USB-накопителе файлов с расширениями `*.pem`, `*.cer` и `*.crl` и предлагается выбрать нужный сертификат, закрытый ключ сертификата или CRL.
- При импорте файлов с расширением `*.cer` и `*.crl` выполняется их конвертация в формат PEM.
- При импорте проверяется уникальность сертификата по содержимому и по имени:
  - Если имя и содержимое уникальны — сертификат импортируется, имя остается без изменения.
  - Если содержимое уникально, а имя нет — сертификат импортируется, к имени добавляется уникальный индекс (`<filename>_yyyy-mm-dd-hhmmss.<ext>`), об изменении имени файла выводится сообщение.
  - Если содержимое сертификата дублируется — сертификат не импортируется, выводится предупреждение о дублировании.

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
```

service cert list

Просмотреть установленные закрытые ключи, сертификаты и списки аннулированных сертификатов (CRL).

Синтаксис

```
service cert list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service cert list

Certificates:

...

Certificate revocation list:


Private keys:

...
```

service cert request create

Создать закрытый ключ и запрос на сертификат в формате PKCS#12.

Синтаксис

```
service cert request create name <имя> bits <длина ключа> digest {md5 | sha1} subj [subj]
```

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;
- `subj` — дополнительные параметры запроса:

- `/C` — страна;
- `/ST` — область;
- `/L` — город;
- `/O` — организация;
- `/OU` — отдел организации;
- `/CN` — доменное имя сайта;
- `/emailAddress` — электронный адрес;
- `/subjectAltName` — альтернативные адреса ресурса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды в стандартном режиме учитывайте:
  - Параметры запроса `subj` записываются единой строкой в двойных кавычках.
  - Названия полей параметров запроса отделяются от значений знаком `=`.
  - Пробелы между параметрами запроса не ставятся.
- Дополнительные параметры `subj` можно задавать в интерактивном режиме.
- 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 **Enter**.
- В контейнере PEM (`.pem`) используется стандарт PKCS#12 (`.p12`).
- 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:

```
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.
If you want to create a certificate for the VPN network, fill in the CommonName and
AlternativeNames parameters.
----
Country name (2 letter code) [AU]:RU
State or province Name (full name) [Some-State]:
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgets Pty Ltd]:Infotecs
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or IP-address or *.vipnet name, one value) []:infotecs.biz
Email Address []:post@infotecs.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
An optional company name (e.g. server FQDN or IP-address or *.vipnet name, several
value)[]:127.50.50.50
Creating request Cert1_req.pem is completed
```

- Чтобы создать запрос на сертификат с длиной ключа 1024 бита, используя алгоритм шифрования MD5 и дополнительные параметры запроса:

```
hostname# service cert request create name Cert1 bits 1024 digest md5 subj
"/C=RU/ST=Moscow/L=Moscow/O=Infotecs/OU=IT/CN=infotecs.ru/emailAddress=post@infote
cs.ru/subjectAltName=DNS:infotecs.biz,IP:127.50.50.50"
Creating request Cert1_req.pem is completed
```

service cert request delete

Удалить запрос на сертификат.

Синтаксис

```
service cert request delete <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Режимы командного интерпретатора

Администратор.

Особенности использования

Признак запроса на сертификат в PEM файле: `-----BEGIN CERTIFICATE REQUEST-----`.

Пример использования

Чтобы удалить запрос на сертификат с именем `Cert1_req.pem`:

```
hostname# service cert request delete Cert1_req.pem
Certificate request Cert1_req.pem is deleted
```

service cert request export

Экспортировать запрос на сертификат на USB-накопитель.

Синтаксис

```
service cert request export <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Режимы командного интерпретатора

Администратор.

Особенности использования

Признак запроса на сертификат в PEM файле: `-----BEGIN CERTIFICATE REQUEST-----`.

Пример использования

Чтобы экспортировать запрос на сертификат с именем `Cert1_req.pem`:

```
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
```

service cert request list

Просмотреть список созданных запросов на сертификат.

Синтаксис

```
service cert request list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

service cert request show

Просмотреть содержимое 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 указать `all`, будет отображено содержимое всех запросов на сертификаты, созданных в ViPNet xFirewall.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть содержимое файла запроса на сертификат с именем `Cert1_req.pem`:

```
hostname> service cert request show Cert1_req.pem
Certificate request:
  Data:
```

```
    ..
  Signature algorithm: md5WithRSAEncryption
    ..
...
(END)
```

service cert show cert

Просмотреть содержимое 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.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть содержимое сертификата с именем `Cert1.pem`:

```
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
...
```

service cert show crl

Просмотреть содержимое 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.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть содержимое списка аннулированных сертификатов с именем `CRL.pem`:

```
hostname> service cert show cert CRL.pem
Certificate Revocation List (CRL):
    Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
...
```

service ips start

Включить предотвращение вторжений (IPS).

Синтаксис

```
service ips start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

На время выполнения команды трафик блокируется межсетевым экраном ViPNet xFirewall, активные соединения принудительно закрываются.

Пример использования

Чтобы включить предотвращение вторжений:

```
hostname# service ips start
```

service ips stop

Выключить предотвращение вторжений (IPS).

Синтаксис

```
service ips stop
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- На время выполнения команды трафик блокируется межсетевым экраном ViPNet xFirewall, активные соединения принудительно закрываются.
- После выполнения команды ранее настроенные параметры предотвращения вторжений (IPS) сохраняются и будут применены при повторном включении предотвращения вторжений.

Пример использования

Чтобы выключить предотвращение вторжений:

```
hostname# service ips stop
```

service ips mode

Включить или выключить автоматический запуск предотвращения вторжений (IPS) при загрузке ViPNet xFirewall.

Синтаксис

```
service ips mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Автоматический запуск предотвращения вторжений включен (`on`).

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы автоматически включать предотвращение вторжений (IPS) при загрузке ViPNet xFirewall:

```
hostname# service ips mode on
```

service ips rule restore-default

Восстановить базу правил IPS до версии, поставляемой в составе дистрибутива ViPNet xFirewall.

Синтаксис

```
service ips rule restore-default
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды запрашивается подтверждение восстановления базы правил IPS.
- После выполнения команды:
  - Будут сохранены ранее сделанные настройки обновления с сервера (адрес сервера обновлений, имя и пароль пользователя, расписание).
  - Автоматическое обновление базы правил IPS с сервера будет выключено.
  - Ранее сделанные настройки правил IPS (действие правила, комментарии и параметры правил) устанавливаются в состояние по умолчанию.

Пример использования

Чтобы восстановить базу правил IPS до версии, поставляемой в составе дистрибутива ViPNet xFirewall:

```
hostname# service ips rule restore-default
All IPS settings will be reset. Continue? [Yes,No]:Y
Shutting down ViPNet Web GUI service
Shutting down IpLir
..
Loading DPI modules
Loading Kernel Interface driver
Loading stream helper module
Loading Iplir Watchdog driver
Loading IpLir Crypto driver
Loading IpLir driver
Loading IPCLS driver
Loading IpLir
Loading ViPNet Web GUI service
```

service ips rule update

Включить или выключить автоматическое обновление базы правил предотвращения вторжения (правил IPS) по расписанию.

Синтаксис

```
service ips rule update {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматическое обновление базы правил IPS.
- `off` — выключить автоматическое обновление базы правил IPS.

Значения по умолчанию

Автоматическое обновление базы правил IPS выключено (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- До включения автоматического обновления базы правил IPS необходимо настроить имя пользователя (см. service ips rule update server login) и пароль пользователя (см. service ips rule update server password) для доступа на сервер обновлений. В случае, если имя пользователя и пароль пользователя не заданы, выводится сообщение о невозможности включить автоматическое обновление правил IPS.
- При обновлении базы правил IPS обработка трафика не прерывается.

Пример использования

Чтобы включить автоматическое обновление базы правил IPS по расписанию:

```
hostname# service ips rule update on
```

service ips rule update fetch

Обновить вручную базу правил предотвращения вторжений (правил IPS) с сервера обновлений.

Синтаксис

```
service ips rule update fetch
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- До выполнения обновления базы правил IPS необходимо настроить имя пользователя (см. service ips rule update server login) и пароль пользователя (см. service ips rule update server password) для доступа к серверу обновлений и проверить доступность сервера обновлений (см. inet ping). В случае, если имя пользователя и пароль пользователя не заданы или сервер обновлений недоступен, выводится сообщение о невозможности выполнить обновление базы правил IPS.
- При обновлении базы правил IPS обработка трафика не прерывается.

Пример использования

Чтобы обновить базу правил IPS, не дожидаясь обновления по расписанию:

```
hostname# service ips rule update fetch

Check file remote_update_ips.conf successfully
Snort configs successfully loaded from database.

IPS updated successfully.
```

service ips rule update proxy address

Задать адрес прокси-сервера, используемого при подключении к серверу обновлений базы правил IPS.

Синтаксис

```
service ips rule update proxy address <адрес прокси-сервера | none>
```

Параметры и ключевые слова

- `<адрес прокси-сервера>` — IP-адрес или доменное имя прокси-сервера.
- `<none>` — не использовать прокси-сервер.

Значения по умолчанию

Прокси-сервер не используется (`none`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Для связи с прокси-сервером необходимо добавить разрешающее правило межсетевого экрана.

Пример использования

Чтобы использовать прокси-сервер `proxy.company.org`:

```
hostname# service ips rule update proxy address proxy.company.org
```

service ips rule update proxy port

Задать TCP-порт прокси-сервера, используемого при подключении к серверу обновлений базы правил IPS.

Синтаксис

```
service ips rule update proxy port <порт>
```

Параметры и ключевые слова

`<порт>` — TCP-порт прокси-сервера.

Значения по умолчанию

Используется TCP-порт 3128.

Режимы командного интерпретатора

Администратор

Пример использования

Чтобы задать TCP-порт 8000:

```
hostname# service ips rule update proxy port 8000
```

service ips rule update schedule

Настроить расписание автоматического обновления базы правил предотвращения вторжений (правил IPS).

Синтаксис

```
service ips rule update schedule {daily at <время> | weekly on <день> at <время>}
```

Параметры и ключевые слова

- `daily at <время>` — ежедневное обновление в указанное время. Параметр `<время>` задается в формате `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты.
- `weekly on <день> at <время>` — еженедельное обновление в указанные день и время. Параметры `<день>` и `<время>` задаются в форматах:
  - `<день>: sunday`, `monday`, `tuesday`, `wednesday`, `thursday`, `friday`, `saturday`.
  - `<время>`: `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты.

Значения по умолчанию

Периодичность обновления базы правил IPS — ежедневно, время обновления выбирается случайным образом.

Режимы командного интерпретатора

Администратор.

Примеры использования

Чтобы настроить ежедневное обновление базы правил IPS в 8 часов 15 минут:

```
hostname# service ips rule update schedule daily at 8:15
```

Чтобы настроить еженедельное обновление базы правил IPS по понедельникам, в 8 часов 15 минут:

```
hostname# service ips rule update schedule weekly on monday at 8:15
```

service ips rule update server address

Задать адрес сервера обновлений базы правил IPS.

Синтаксис

```
service ips rule update server address <адрес сервера>
```

Параметры и ключевые слова

`<адрес сервера>` — IP-адрес или доменное имя сервера обновлений базы правил IPS.

Значения по умолчанию

DNS-имя

Режимы командного интерпретатора

Администратор.

Особенности использования

В доменном имени сервера обновлений разрешено использовать только символы латинского алфавита.

Пример использования

Чтобы использовать для обновления базы правил IPS сервер `10.0.7.72`:

```
hostname# service ips rule update proxy address 10.0.7.72
```

service ips rule update server login

Задать имя пользователя для доступа к серверу обновлений базы правил предотвращения вторжений (правил IPS).

Синтаксис

```
service ips rule update server login <имя пользователя>
```

Параметры и ключевые слова

`<имя пользователя>` — имя пользователя для доступа к серверу обновлений базы правил IPS. Файл с именем и паролем пользователя для доступа к серверу обновлений входит в комплект поставки ViPNet xFirewall.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы задать имя пользователя `User2019` для доступа к серверу обновлений базы правил IPS:

```
hostname# service ips rule update server login User2019
```

service ips rule update server password

Задать пароль пользователя для доступа к серверу обновлений базы правил предотвращения вторжений (правил IPS).

Синтаксис

```
service ips rule update server password
```

Параметры и ключевые слова

`<пароль>` — пароль пользователя для доступа к серверу обновлений базы правил IPS. Файл с именем и паролем пользователя для доступа к серверу обновлений входит в комплект поставки ViPNet xFirewall.

Режимы командного интерпретатора

Администратор.

Особенности использования

Пароль задается в интерактивном режиме, символы при вводе не отображаются.

Пример использования

Чтобы задать пароль пользователя для доступа к серверу обновлений базы правил IPS:

```
hostname# service ips rule update server password
Enter password for ips remote server:
```

service ips rule update usb

Обновить базу правил предотвращения вторжений (правил IPS) с USB-носителя.

Синтаксис

```
hostname# service ips rule update usb
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед обновлением подготовьте USB-носитель:
  - отформатируйте USB-носитель в одной из файловых систем: `FAT32`, `ext2`, `ext3` или `ext4`;
  - загрузите на USB-носитель с сервера обновлений файл обновления базы правил IPS (файл с именем в формате `rules_ГГГГММДД_ЧЧММСС_eac_ver.xfirewall-5.6.1.pem`). Подробнее см. «Настройка с помощью веб-интерфейса», раздел «Обновления базы правил IPS вручную».
- При обновлении базы правил IPS обработка трафика не прерывается.

Пример использования

Чтобы обновить базу правил IPS с USB-носителя, на который предварительно записан файл обновления `rules_2022_1203_eac_ver.xfirewall-5.6.1.pem`, выполните следующие действия:

1. Подключите USB-носитель к ViPNet xFirewall.
2. Выполните команду:

```
hostname# service ips rule update usb
Insert USB flash drive into empty USB slot and press <Enter>


Select file to use for updating IPS rules:
1 - /sdc1/rules_2022_1203_eac_ver.xfirewall-5.6.1.pem
Enter file number [1-1] or [q] to cancel: 1
IPS updated successfully.
```

service ips show status

Просмотреть параметры системы предотвращения вторжений IPS.

Синтаксис

```
service ips show status
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

При выполнении команды отображается следующая информация:

- состояние системы предотвращения вторжений:
  - `IPS subsystem is in service mode` — технологический режим;
  - `IPS subsystem is off` — выключено;
  - `IPS subsystem is on` — включено;
  - `IPS subsystem is on and updating` — включено и выполняется обновление базы правил IPS;
- автоматический запуск системы предотвращения вторжений при перезапуске ViPNet xFirewall:
  - `autostart is on` — разрешено;
  - `autostart is off` — запрещено;
- ошибки системы предотвращения вторжений (строка выводится, если есть ошибки в работе предотвращения вторжений);
- уровень важности событий предотвращения вторжений, регистрируемых в системном журнале ViPNet xFirewall;
- дата и время создания текущей базы правил IPS;
- статус (успешно или не успешно), дата и время последнего обновления текущей базы правил IPS.

Пример использования

Чтобы просмотреть параметры предотвращения вторжений:

```
hostname> service ips show status

IPS subsystem is on

IPS subsystem autostart is on

Current syslog level is 3-info and higher

Current IPS rules database 2022-02-10 16:35:22

IPS rules database updated 2022-02-25 13:13:47
```

service ips show update-settings

Просмотреть параметры обновления базы правил предотвращения вторжений (правил IPS).

Синтаксис

```
service ips show update-settings
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

При выполнении команды отображается следующая информация:

- автоматическое обновление базы правил IPS (включено или выключено);
- расписание обновления базы правил IPS (периодичность и время обновления);
- адрес сервера обновлений базы правил IPS (DNS-имя или IP-адрес);
- имя пользователя для доступа к серверу обновлений базы правил IPS;
- статус пароля пользователя (установлен или не установлен).

Пример использования

Чтобы просмотреть текущие параметры обновления базы правил правил IPS:

```
hostname> service ips show update-settings
IPS rules database remote update: on
Database updates daily at 01:01
Update server:
 Address: updateids.infotecs.ru
 Login: user2021
 Password: specified
Update proxy-server:
 Address: proxy.gov.ru
 Port: 3128
 Status: available/unavailable
IPS rules update license expiration date: 2022-10-14 13:12:11
IPS license ID: 746k-l3s2
```

service ips syslog-level

Задать уровень важности событий предотвращения вторжений (IPS), записываемых в системный журнал ViPNet xFirewall.

Синтаксис

```
service ips syslog-level <уровень важности>
```

Параметры и ключевые слова

`<уровень важности>` — число от 0 до 5 по убыванию степени важности, соответствующее уровням событий:

- 0 — критические события;
- 1 — ошибки;
- 2 — предупреждения;
- 3 — информационные события;
- 4 — отладочные события;
- 5 — детализированные отладочные события.

Значения по умолчанию

Задан уровень событий — 3. При этом в системном журнале ViPNet xFirewall регистрируются:

- 0 — критические события;
- 1 — ошибки;
- 2 — предупреждения;
- 3 — информационные события.

Режимы командного интерпретатора

Администратор.

Особенности использования

Уровни важности событий IPS, записываемых в системный журнал ViPNet xFirewall, входят в три группы, включающие следующие уровни важности:

- 0, 1, 2;
- 3;
- 4, 5.

Если уровень изменяется на значение из другой группы событий, необходимо перезапустить IPS. При этом будет выведено сообщение с предложением немедленного перезапуска IPS:

```
IPS logging level will change upon IPS restart. IPS will restart now. [y/n]
```

- `y` — выполняется немедленный перезапуск IPS, устанавливается новый уровень важности;
- `n` — текущий уровень важности сохраняется до перезапуска IPS, после которого будет установлен новый уровень важности.

При изменении уровня важности на значение из той же группы, перезапуск IPS не требуется.

Пример использования

Предположим, что в ViPNet xFirewall установлен уровень важности событий IPS по умолчанию (`3`). Чтобы в системный журнал ViPNet xFirewall записывались события до 4-го уровня включительно (критические, ошибки, предупреждения, информационные и отладочные), установите уровень важности `4` и выполните немедленный перезапуск IPS:

```
hostname# service ips syslog-level 4
IPS logging level will change upon IPS restart. IPS will restart now. Continue? [y/n]: y
```

service user-control active-users

Просмотреть информацию о текущих сессиях пользователей Active Directory и Captive portal.

Синтаксис

```
service user-control active-users
```

Режимы командного интерпретатора

- Пользователь.
- 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 или пока с этого IP-адреса в сеть не войдет другой пользователь.

Пример использования

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

 5 active network user session(s)

 User name            Session IP-address  Source    Start time Lifetime left
 /AD Domain Controller                    AD Group Name

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

 Smith.John       13.34.152.12    AD      10:11:42
 /dc1.infotecs.int
 BrownPaul       78.54.24.16     CP      12:24:45  15m
 NelsonNeil       12.34.154.12    AD      10:04:23
 /Longdomaincontrollername.infotecs.int   Administrators
 superadmin       12.34.154.68    AD      10:22:57
 /dc2.infotecs.int
 superadmin       82.12.33.212    CP      11:03:36  1h 3m
```

service user-control ad reset

Удалить параметры соединения ViPNet xFirewall с контроллером домена Active Directory.

Синтаксис

```
service user-control ad reset [controller <адрес контроллера домена>]
```

Параметры и ключевые слова

`<адрес контроллера домена>` — IP-адрес или доменное имя узла контроллера домена.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если параметр `<адрес контроллера домена>` не задан, то сбрасываются настройки для всех настроенных контроллеров домена.
- Команда выполняется только при включенной службе UC.

Пример использования

Чтобы сбросить настройки параметров соединения контроллера домена `domain.local`:

```
hostname# service user-control ad reset controller domain.local

User-authentication service is stopped and mode is switched to off, as no authentication
method is currently configured.
```

service user-control ad show

Просмотреть информацию о параметрах аутентификации с помощью Active Directory.

Синтаксис

```
service user-control ad show [controller <адрес>]
```

Параметры и ключевые слова

`<адрес>` — IP-адрес или имя контроллера домена.

Режимы командного интерпретатора

- Пользователь.
- 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 локализацию 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).

Если адрес или имя контроллера не задано, то выводится информация по всем настроенным контроллерам.

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 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

       Log-file name: syslog.log

   Domain Controller secondary.local is available

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

       Domain user: Administrator

       DC synchronization delay: 100 sec

       Allowed connection timeout: 1800 sec

       Log-file name: syslog.log
```

service user-control ad set controller

Настроить соединение 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 латинские буквы (A-z), цифры (0-9), знак «минус» (-) и «точка» (.), кроме:

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

  Максимальная длина имени пользователя — 20 символов.

  Имя пользователя указывается без домена.

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`:

```
hostname# service user-control ad set controller 192.168.1.23 user user23
Enter user23 password:
```

service user-control ad set controller connection-timeout

Задать допустимое время отсутствия связи с контроллером домена Active Directory.

Синтаксис

```
service user-control ad set controller <адрес контроллера> connection-timeout <время>
```

Параметры и ключевые слова

- `<адрес контроллера>` — IP-адрес или имя контроллера домена.
- `<время>` — допустимое время отсутствия связи с контроллером домена Active Directory, целое число в секундах.

Значения по умолчанию

Допустимое время отсутствия связи с контроллером домена составляет 1800 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

Значение параметра `<время>` должно быть больше или равно значению периода получения журнала контроллера домена.

Пример использования

Для задания допустимого времени отсутствия связи с контроллером домена `domain.local` Active Directory 60 секунд:

```
hostname# service user-control ad set controller domain.local connection-timeout 60
```

service user-control cp reset

Сбросить настройки Captive portal.

Синтаксис

```
service user-control cp reset
```

Режимы командного интерпретатора

Администратор.

Особенности использования

После выполнения команды также останавливается работа службы `uc`.

Пример использования

```
hostname# service user-control cp reset
Stopping uc.sh: uc.
```

service user-control cp set connection-secure

Задать режим соединения Captive portal с LDAP-сервером.

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

Установлен режим открытого соединения (`none`).

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы задать режим соединения с LDAP-сервером Start TLS:

```
hostname# service user-control cp set connection-secure stls
```

service user-control cp set connection-timeout

Задать время жизни сессии пользователя Captive portal, 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.

Пример использования

Чтобы задать время жизни сессии пользователя 1 час:

```
hostname# service user-control cp set connection-timeout 3600
```

service user-control cp set custom-login-form

Задать произвольное текстовое сообщение на странице аутентификации пользователей Captive portal.

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.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы задать текстовое сообщение «Welcome to Guest Network!» на странице аутентификации пользователей Captive portal:

```
hostname# service user-control cp set custom-login-form "Welcome to Guest Network!"
```

service user-control cp set hostcert

Выбрать сертификат веб-сервера Captive portal 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.

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).
- 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).

Пример использования

Чтобы выбрать сертификат с именем `certificate.pem` и соответствующий ему закрытый ключ с именем `private.pem`:

```
hostname# service user-control cp set hostcert certificate.pem hostkey private.pem
```

service user-control cp set idle-timeout

Задать время бездействия (отсутствия передачи данных) пользователя Captive portal, 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

Время бездействия пользователя — 1800 секунд.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы задать время бездействия пользователя 10 минут:

```
hostname# service user-control cp set idle-timeout 600
```

service user-control cp set ldap

Настроить соединение Captive portal с LDAP-сервером.

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 253 символов и содержать латинские буквы (`A-z`), цифры (`0-9`), знаки «-» и «.», 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 символов и содержать латинские буквы (`A-z`), цифры (`0-9`), знаки «-» и «.», кроме:

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

  Выделенное имя базы должно быть заключено в двойные кавычки.

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:

```
hostname# service user-control cp set ldap example.com identity
"uid=admin,ou=People,dc=example" basedn "example"

Enter password for LDAP identity:
```

service user-control cp set ldap cacert

Выбрать корневой сертификат LDAP-сервера 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.

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).

Пример использования

Чтобы выбрать сертификат с именем `ldap_cert.pem`:

```
hostname# service user-control cp set ldap cacert ldap_cert.pem
```

service user-control cp show

Просмотреть настройки Captive portal.

Синтаксис

```
service user-control cp show
```

Режимы командного интерпретатора

- Администратор.

- Пользователь.

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 Web certificate:
Allowed connection timeout: 3600 sec
Allowed idle timeout: 600 sec
Custom login phrase: Guest Network
```

service user-control fw-rules apply

Создать разрешающие сетевые фильтры после изменения параметров соединения с сервером Active Directory или Captive portal.

Синтаксис

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

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# service user-control fw-rules apply
Applying rules for Active Directory... Please wait.
```

service user-control fw-rules delete

Удалить разрешающие сетевые фильтры, созданные после выполнения команды `service user-control fw-rules apply` (ddd).

Синтаксис

```
service user-control fw-rules delete
```

Режимы командного интерпретатора

Администратор.

Пример использования

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

service user-control fw-rules show

Просмотреть сетевые фильтры, разрешающие соединение ViPNet xFirewall с сервером Active Directory и Captive portal.

Синтаксис

```
service user-control fw-rules show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

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                     |
+======+=================+=============+=================+
```

service user-control mode off

Выключить автозапуск службы управления пользователями (`uc`) при загрузке ViPNet xFirewall.

Синтаксис

```
service user-control mode off
```

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы выключить автозапуск службы управления пользователями при загрузке ViPNet xFirewall:

```
hostname# service user-control mode off
```

service user-control mode on

Включить автозапуск службы управления пользователями (`uc`) при загрузке ViPNet xFirewall.

Синтаксис

```
service user-control mode on
```

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы включить автозапуск службы управления пользователями при загрузке ViPNet xFirewall:

```
hostname# service user-control mode on
```

service user-control show

Просмотреть информацию о состоянии работы службы управления пользователями (`uc`).

Синтаксис

```
service user-control show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

В результате выполнения команды выводится следующая информация о статусе работы службы `uc`:

- Состояние службы `uc` и режим ее автозапуска.
- Уровень важности событий, добавляемых в системный журнал (см. service user-control syslog-level).
- Статус настройки и доступность сервера Active Directory и Captive portal.
- Количество активных сессий пользователей (если служба `uc` запущена).

Пример использования

Выполнение команды при запущенной службе `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
Active Directory Domain Controller PDC authentication is configured and available
Captive Portal authentication is configured and available
No active network users.
```

service user-control start

Запустить службу управления пользователями (`uc`).

Синтаксис

```
service user-control start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

После запуска службы управления пользователями все сетевые пакеты неавторизованных пользователей будут блокироваться, даже если созданы разрешающие сетевые фильтры.

Пример использования

```
hostname# service user-control start

Starting uc.sh: uc.
```

service user-control stop

Остановить работу службы управления пользователями (`uc`).

Синтаксис

```
service user-control stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# service user-control stop

Stopping uc.sh: uc.
```

service user-control syslog-level

Задать уровень важности событий службы управления пользователями (`uc`), которые будут попадать в системный журнал.

Синтаксис

```
service user-control syslog-level <уровень важности>
```

Параметры и ключевые слова

`<уровень важности>` — число от 0 до 5, соответствующее уровням важности событий:

- 0 — критические события;
- 1 — ошибки;
- 2 — извещения;
- 3 — информационные события;
- 4 — отладочные события;
- 5 — детализированные отладочные события.

Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

Задан уровень важности 3 (информационные события).

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы в системный журнал записывались события службы `uc` уровня 4:

```
hostname# service user-control syslog-level 4
```

Команды группы ups

Команды группы `ups` предназначены для настройки взаимодействия ViPNet xFirewall с источником бесперебойного питания (UPS).

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

Выбрать драйвер `UPS`.

Синтаксис

```
ups set driver <драйвер>
```

Параметры и ключевые слова

`<драйвер>` — название драйвера. В текущей версии ViPNet xFirewall можно указать только значение `usbhid-ups`.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы выбрать драйвер `UPS`:

```
hostname# ups set driver usbhid-ups
```

ups set mode

Настроить режим взаимодействия ViPNet xFirewall с ИБП.

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 ИБП и который непосредственно взаимодействует с ИБП.
- `slave` — взаимодействие в режиме подчиненного компьютера. Подчиненный компьютер взаимодействует с ИБП через главный компьютер.
- `<IP-адрес мастера>` — IP-адрес главного компьютера, находящегося в режиме `master`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды требуется вручную завершить работу служб пакета NUT (Network UPS Tools) с помощью команды ups stop.

Пример использования

```
hostname# ups set mode master
```

ups set monitoring

Включить или выключить мониторинг состояния ИБП.

Синтаксис

```
ups set monitoring {on | off}
```

Параметры и ключевые слова

- `on` — включить мониторинг;
- `off` — выключить мониторинг.

Значения по умолчанию

Мониторинг состояния ИБП выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- После включения мониторинга запустите службы пакета NUT с помощью команды ups start.
- При выключении мониторинга будет автоматически завершена работа служб пакета NUT.

Пример использования

```
hostname# ups set monitoring on
```

ups show config

Просмотреть текущие настройки взаимодействия ViPNet xFirewall с ИБП.

Синтаксис

```
ups show config
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Команда выводит следующую информацию:

- Включен или выключен мониторинг состояния ИБП. Остальная информация выводится только в случае, если мониторинг включен.
- Режим взаимодействия ViPNet xFirewall с ИБП (`master` или `slave`).
- Используемый драйвер `UPS` (только в режиме `master`).
- IP-адрес мастера (только в режиме `slave`).
- Состояние служб пакета `NUT` (запущены или работа служб завершена).

Пример использования

```
hostname> ups show config
UPS service mode is Master. Driver: usbhid-ups
UPS service is RUNNING
```

ups show status

Просмотреть информацию о состоянии ИБП.

Синтаксис

```
ups show status [extended]
```

Параметры и ключевые слова

`extended` — просмотр всех параметров состояния ИБП в формате утилиты `upsc`, входящей в состав пакета `NUT`. Эта возможность предназначена для квалифицированных системных администраторов, которые могут самостоятельно интерпретировать результат вывода утилиты `upsc`.

Особенности использования

Команда выводит следующую информацию:

- производитель ИБП;
- модель ИБП;
- 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 ИБП посылает сигнал о необходимости выключения компьютера (задается производителем ИБП).

Режимы командного интерпретатора

- Пользователь.
- Администратор.

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
```

ups start

Запустить службы пакета `NUT`, обеспечивающие взаимодействие ViPNet xFirewall с ИБП.

Синтаксис

```
ups start
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> ups start
```

ups stop

Завершить работу служб пакета `NUT`, обеспечивающих взаимодействие ViPNet xFirewall с ИБП.

Синтаксис

```
ups stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> ups stop
```

Команды группы vpn

Загрузка и выгрузка драйверов и служб ViPNet.

vpn start

Загрузить все драйверы и запустить все службы ViPNet xFirewall.

Синтаксис

```
vpn start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда выполняется только в том случае, если перед этим была выполнена команда `vpn stop` или если службы и драйверы не были запущены при загрузке ViPNet xFirewall (например, если вы не выбрали запуск служб VPN после разворачивания дистрибутива ключей). Если некоторые службы 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 служб. Например, после выполнения команд `iplir stop` и `mftp stop` для запуска служб `iplircfg` и `mftpd` выполните команды `iplir start` и `mftp start`.

Пример использования

```
hostname# vpn start
```

vpn stop

Выгрузить драйверы и завершить работу служб ViPNet xFirewall.

Синтаксис

```
vpn stop
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Выгружаемые командой `vpn stop` драйверы и службы необходимы для нормальной работы системы обнаружения вторжений (IPS) и службы глубокого исследования пакетов (DPI). После выполнения команды запуск указанных служб будет невозможен.

Пример использования

Для выгрузки драйверов и завершения работы служб ViPNet xFirewall:

```
hostname# vpn stop
Shutting down failover daemon
Shutting down ViPNet Web GUI service
Shutting down MFTP daemon
Shutting down Alg daemon
Shutting down IpLir
Unloading IpLir driver
```

Команды группы webui

Команды группы `webui` предназначены для управления веб-сервером ViPNet xFirewall, на основе которого функционирует веб-интерфейс.

webui info

Просмотреть состояние службы `WebUI`:

- Статус службы — запущена или остановлена.
- Протокол для доступа к ViPNet xFirewall с помощью веб-интерфейса.

Синтаксис

```
webui info
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> webui info
WebUI server is running
Protocol HTTP
Port 8080
```

webui restart

Перезапустить веб-сервер ViPNet xFirewall.

Синтаксис

```
webui restart
```

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
```

webui status

Просмотреть информацию о состоянии службы `webui`, отвечающей за работу веб-интерфейса ViPNet xFirewall.

Синтаксис

```
webui status
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> webui status
 WebUI server is enabled and is running.
```

Прочие команды

К прочим относятся команды, которые не входят ни в одну из групп команд, описанных выше.

debug off

Выключить вывод сообщений о событиях.

Синтаксис

```
debug off [<источник> <важность>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого требуется выключить вывод сообщений.
- `<важность>` — уровень важности выключаемых сообщений.

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 служб:

```
hostname# debug off daemon err
```

debug on

Включить вывод 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` — службы.
- `<важность>` — уровень важности 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 служб 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 служб:

```
hostname# debug on daemon err
```

enable

Перейти в режим администратора.

Синтаксис

```
enable
```

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 системном журнале создается запись об успешном переходе в режим администратора.

Пример использования

```
hostname> enable

Type the administrator password:
```

exit

Выйти из текущего режима командного интерпретатора.

Синтаксис

```
exit
```

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
```

version

Просмотреть текущую версию ViPNet xFirewall и его компонентов.

Синтаксис

```
version [full]
```

Параметры и ключевые слова

`full` — просмотр текущей версии всех компонентов, а также других параметров (набор функций, архитектура процессора).

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

По команде выводится название и версия продукта. При указании ключевого слова `full` выводятся дополнительные параметры:

```
hostname> version
Product: ViPNet xFirewall
Platform: XFVA
License: xFVA
Software version: 5.6.1-123
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

Просмотреть список функциональных модулей, входящих в состав текущей версии ViPNet xFirewall.

Синтаксис

```
version features list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> version features list
bonding
dhcp-client
```

```
dhcp-relay
dhcp-server
...
```

who

Просмотреть информацию о запущенных сессиях командного интерпретатора (локальной и удаленных).

Синтаксис

```
who
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Информация о запущенных сессиях командного интерпретатора обновляется каждые 7 секунд.

Пример использования

```
hostname> who
LINE HOST      IDLE   MODE COMMENTS
tty1 local console 00:00:06 user current
```

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 healthmond.ini

Настройки системы мониторинга системной нагрузки Protection Tools задаются в конфигурационном файле `healthmond.ini`.

Чтобы отредактировать файл `healthmond.ini`:

1. Завершите работу Protection Tools:

   ```
   hostname# healthmond stop
   ```

2. Откройте файл для редактирования

   ```
   hostname# healthmond edit
   ```

3. Внесите изменения.

4. Запустите Protection Tools:

   ```
   hostname# healthmond start
   ```

Ниже приводится описание секций конфигурационного файла `healthmond.ini` и входящих в них параметров. Для удобства интерпретации значения загруженности ViPNet xFirewall по каждому из контролируемых параметров разделены на зоны:

- green — «зеленая зона», означает штатную нагрузку по контролируемому параметру. В этом случае вмешательства не требуется;
- yellow — «желтая зона», означает повышенную нагрузку. При попадании контролируемого параметра в желтую зону следует обратить внимание на возможные источники повышенной нагрузки.
- red — «красная зона», означает критические значения контролируемого параметра, существенно влияющие на производительность и стабильность работы ViPNet xFirewall. Попадание контролируемого параметра в красную зону также может сигнализировать об осуществлении распределенных сетевых атак типа DDoS. При обнаружении контролируемых параметров в красной зоне следует незамедлительно принять меры по обнаружению и блокировке источников повышенной нагрузки.

Секция `[CPU]`

Параметры секции `[CPU]` описывают значения загрузки ядер центрального процессора и границы зон нормальной, повышенной и критической загрузки:

- `core_yellow` — загрузка ядер процессора (в процентах), порог перехода из зеленой зоны в желтую;
- `core_red` — загрузка ядер процессора (в процентах), порог перехода из желтой зоны в красную;
- `loadavg_yellow` — средняя загрузка процессора (параметр LoadAverage), порог перехода из зеленой зоны в желтую;

- `loadavg_red` — средняя загрузка процессора (параметр LoadAverage), порог перехода из желтой зоны в красную;
- `crit_loadavg_load` — время нахождения средней загрузки процессора (параметр LoadAverage) в зоне критических значений, после которого Protection Tools регистрирует перегрузку. Время определяется как % от временного периода, заданного параметром `times_per_day`;
- `crit_cpu_cores_load` — время нахождения загрузки ядер процессора (в процентах) в зоне критических значений, после которого Protection Tools регистрирует перегрузку. Время определяется как % от временного периода, заданного параметром `times_per_day`;
- `snmp_enable` — определяет отправку SNMP-уведомлений о нагрузке на CPU. Возможные значения:
  - `0` — не отправлять оповещения о загрузке CPU;
  - `1` — отправлять оповещения о загрузке CPU.

Секция `[Memory]`

Параметры секции `[Memory]` описывают значения потребляемой памяти и границы зон нормального, повышенного и критического потребления:

- `mem_free_yellow` — количество свободной памяти (в процентах), порог перехода из зеленой зоны в желтую;
- `mem_free_red` — количество свободной памяти (в процентах), порог перехода из желтой зоны в красную;
- `mem_available_yellow` — количество доступной памяти (в процентах), порог перехода из зеленой зоны в желтую;
- `mem_available_red` — количество доступной памяти (в процентах), порог перехода из желтой зоны в красную;
- `mem_swapped_free_yellow` — количество свободной памяти файла подкачки (в процентах), порог перехода из зеленой зоны в желтую;
- `mem_swapped_free_red` — количество свободной памяти файла подкачки (в процентах), порог перехода из желтой зоны в красную.

Секция `[Netdev]`

Параметры секции `[Netdev]` описывают утилизацию сетевых интерфейсов и границы зон нормальных, повышенных и критических значений:

- `pps_yellow` — количество IP-пакетов в секунду, порог перехода из зеленой зоны в желтую;
- `pps_red` — количество IP-пакетов в секунду, порог перехода из желтой зоны в красную;
- `throughput_yellow` — битрейт (bps), порог перехода из зеленой зоны в желтую;
- `throughput_red` — битрейт (bps), порог перехода из желтой зоны в красную;

- `errps_yellow` — количество ошибок на сетевых интерфейсах, порог перехода из зеленой зоны в желтую;
- `errps_red` — количество ошибок на сетевых интерфейсах, порог перехода из желтой зоны в красную;
- `snmp_enable` — определяет отправку SNMP-уведомлений об утилизации сетевых интерфейсов. Возможные значения:
  - `0` — не отправлять оповещения об утилизации сетевых интерфейсов;
  - `1` — отправлять оповещения об утилизации сетевых интерфейсов.

Секция `[Netfilter queue]`

Параметры секции `[Netfilter queue]` описывают утилизацию очередей Netfilter:

- `threshold` — порог размера очереди Netfilter, при превышении которого она считается перегруженной.

Секция `[Disk]`

Параметры секции `[Disk]` описывают утилизацию дисковой подсистемы и границы зон нормальных, повышенных и критических значений:

- `iopsps_yellow` — количество I/O операций в секунду, порог перехода из зеленой зоны в желтую;
- `iopsps_red` — количество I/O операций в секунду, порог перехода из желтой зоны в красную.

Секция `[Conntrack]`

Параметры секции `[Conntrack]` описывают утилизацию таблицы соединений:

- `cps_yellow` — количество новых соединений в секунду, порог перехода из зеленой зоны в желтую;
- `cps_red` — количество новых соединений в секунду, порог перехода из желтой зоны в красную.

Секция `[Iplirdb]`

Секция `[Iplirdb]` задает настройки механизма блокировки источников повышенной сетевой нагрузки (Штрафной бокс):

- `drops` — количество срабатываний запрещающего правила в журнале IP-пакетов за период, заданный в параметре `db_time_delta`, после которого источник пакетов блокируется на время, заданное в параметре `ipset_timeout`.
- `ipset_timeout` — время автоматической блокировки, секунд. По истечении данного времени источник повышенной нагрузки разблокируется;
- `db_time_delta` — период времени, за который выполняется поиск записей о блокировке в журнале пакетов, секунд.

Значение по умолчанию: 65

- `ifname` — системное имя интерфейса, для которого используется механизм блокировки источников повышенной сетевой нагрузки (как правило, интерфейс, подключенный к публичной сети).

Секция `[SNMP]`

Секция `[SNMP]` содержит параметры настройки SNMP-уведомлений:

- `snmp_ip` — IP-адрес сервера мониторинга для отправки SNMP-уведомлений;

Секция `[Load check]`

Секция `[Load check]` задает общие настройки системы определения повышенной нагрузки:

- `enable — Включить`
- `times_per_day` — определяет период для вычислениях средних значений нагрузки (параметр задает количество проверок в течение суток).

  Значение по умолчанию: 1

Секция `[Rate Limiting]`

Секция `[Rate Limiting]` задает ограничения сетевого трафика:

- `connlimit` — ограничивает количество параллельных TCP-соединений с одного IP-адреса или блока адресов.

Файл failover.ini

Настройка параметров работы системы защиты от сбоев осуществляется путем редактирования конфигурационного файла `failover.ini`.

Чтобы отредактировать файл `failover.ini`:

1. Завершите работу службы `failoverd`:

   ```
   hostname# failover stop
   ```

2. Откройте файл для редактирования

   ```
   hostname# failover config edit
   ```

3. Внесите изменения.

4. Запустите службу `failoverd`:

   ```
   hostname# failover start
   ```

Секция [channel]

Каждый сетевой интерфейс активного узла, работоспособность которого должна контролироваться системой защиты от сбоев при работе в режиме кластера горячего резервирования, 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 узла 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. Независимо от того, в какой нотации была указана маска, после сохранения файла `failover.ini` маска будет перезаписана в нотации CIDR.

- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов. Возможные значения:
  - `yes` (по умолчанию) — активный узел 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 узла 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. Рекомендуется использовать не более 50 параметров `testip` для одного физического интерфейса.

  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
  ```

  При настройке параметра `testip` учитывайте следующие особенности:
  - Рекомендуется использовать не более 32 параметров `testip` для одного физического сетевого интерфейса.
  - В качестве параметра `testip` не рекомендуется использовать адрес 127.0.0.1, потому что в этом случае контроль работоспособности интерфейса активного узла кластера фактически не будет проводиться: интерфейс активного узла кластера будет считаться работоспособным, так как ответы на эхо-запросы по адресу 127.0.0.1 будут приходить всегда. Использование других адресов из подсети 127.0.0.0/8 запрещено.
  - 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.

Секция [debug]

Секция `[debug]` определяет параметры ведения системного журнала службы failoverd и содержит следующие параметры:

- `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `1` до `5` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение `-1` выключает ведение журнала.
- Не рекомендуется задавать уровень важности выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ИнфоТеКС.
- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `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 установлено значение — `30`. Чтобы снять ограничение на время хранения записей, установите значение `0`.
- `reboot` — задает действия системы в случае обнаружения полной неработоспособности какой-либо службы или драйвера ViPNet xFirewall. Возможные значения:
  - `yes` (по умолчанию) — включить механизм регистрации в watchdog-драйвере и перезагружать систему, если какая-либо служба или драйвер не может восстановить свою работу;

- `no` — выключить механизм регистрации в watchdog-драйвере и не перезагружать систему, если какая-либо служба или драйвер не может восстановить свою работу.

Нередактируемые параметры секции [misc]

- `activeconfig` — абсолютный путь к файлу конфигурации управляющей службы, который будет использоваться на активном узле кластера. Значение по умолчанию — `/etc/iplirpsw`.
- `passiveconfig` — абсолютный путь к файлу конфигурации управляющей службы, который будет использоваться на пассивном узле 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 узлах кластера.

Секция `[network]` содержит следующие параметры:

- `activeretries` — количество неуспешных попыток опроса пассивным узлом активного узла, после которых делается вывод об отсутствии активного узла с опрашиваемым IP-адресом. По умолчанию — `3`.
- `afterifconf` — имя скрипта, содержащего команды, которые выполняются непосредственно после конфигурирования всех интерфейсов при смене активного узла.
- `beforeifconf` — имя скрипта, содержащего команды, которые выполняются перед конфигурированием всех интерфейсов при смене активного узла.

Примечание. Параметры `afterifconf` и `beforeifconf` используются для организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов (подробнее см. в документе «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 узле — для проверки работоспособности интерфейса;
- на пассивном узле — для поиска IP-адресов активного узла.

Указывается в секундах, по умолчанию — `10`.

- `fastdown` — указывает на принудительное выключение сетевых интерфейсов перед перезагрузкой узла. Возможные значения: `yes` (по умолчанию) или `no`. Значение, выбранное по умолчанию, позволяет быстрее установить отсутствие активного узла в сети и дать возможность второму узлу 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 узла), 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 узла на пассивный с целью резервирования.

Примечание. Все параметры секции `[sendconfig]` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

Секция `[sendconfig]` содержит следующие параметры:

- `activeip` — адрес резервного канала другого узла кластера (который работает в режиме, противоположном режиму данного узла).
- `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);
  - 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 и статическими маршрутами (если такие создавались);
- другие служебные конфигурационные файлы.

- `connectport` — номер порта, используя который данный пассивный узел кластера соединяется с активным узлом и принимает от него файлы для резервирования. По умолчанию значение параметра — `10090`. Если параметр отсутствует, то его значение равно значению параметра `port` данной секции.
- `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 сервера MFTP;
  - другие служебные файлы журналов.
- `keys` — включение или выключение резервирования группы файлов справочников и лицензии. 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 службой `failoverd` автоматически на активном узле. Пассивный узел 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 узле 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 узел кластера ожидает соединения от пассивного узла 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 iplir.conf

Параметры защищенной сети ViPNet содержатся в файле `iplir.conf`. Чтобы их настроить:

1. Остановите управляющую службу:

   ```
   hostname# iplir stop
   ```

2. Откройте файл:

   ```
   hostname# iplir config
   ```

3. Настройте параметры, используя описание секций.

4. Запустите управляющую службу:

   ```
   hostname# iplir start
   ```

Секция [adapter]

Секции `[adapter]` описывают статические сетевые интерфейсы компьютера. Каждому интерфейсу соответствует своя секция `[adapter]`. Если статический интерфейс не описан секцией `[adapter]`, то все проходящие через него IP-пакеты блокируются.

Если в файле `iplir.conf` нет ни одной секции `[adapter]`, то управляющая служба при запуске получает от системы список сетевых интерфейсов и автоматически создает соответствующие секции.

В процессе работы управляющая служба 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, он выключается и в драйвере ViPNet. После включения или изменения IP-адреса интерфейса эти изменения автоматически загружаются в драйвер ViPNet.

В секции `[adapter]` указываются параметры:

- `allowtraffic` — разрешение или блокирование прохождения IP-трафика через интерфейс:
  - `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), то интерфейсу, посредством которого

ViPNet xFirewall будет связываться с узлом, выполняющим функции межсетевого экрана, следует назначить тип `external`, остальным интерфейсам ViPNet xFirewall — тип `internal`.

Нередактируемые параметры

- `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 управляющей службы и драйвера ViPNet все они будут представлять одно физическое устройство с базовым именем (`eth0`).

Секция [debug]

Секция `[debug]` определяет параметры ведения системного журнала управляющей службы. Она содержит следующие параметры:

- `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `1` до `5` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение `-1` выключает ведение журнала.
- Не рекомендуется задавать уровень важности выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ИнфоТеКС.
- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `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 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 управляющей службы.

  - `<IP-адрес доступа>` — IP-адрес доступа к узлу. Принимает значение `0.0.0.0`, когда данный узел не находится за межсетевым экраном.

- `<метрика>` — метрика 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, 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.

- `fixfirewall` — режим фиксации настроек работы собственного узла через внешний межсетевой экран:
  - `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 заданы администратором в параметрах `firewallip` и `port` данной секции.
- `ip` — реальный IP-адрес и соответствующий ему виртуальный IP-адрес узла. 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. При изменении порядка следования реальных IP-адресов, порядок следования виртуальных адресов не меняется.
- `port` — 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`);
        - `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`.
    - 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` — тип видимости узла:
    - `auto` — автоматически определять тип видимости узла, в зависимости от текущего адреса видимости узла.
    - `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

- `accessip` — текущий IP-адрес доступа к узлу 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 управляющая служба отличает одну секцию `[id]` от другой. Идентификатор присваивается сетевому узлу ViPNet при его создании в ViPNet ЦУС или Prime. В каждой секции `[id]` может быть только один такой параметр.
- `firewallip` — 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 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 ViPNet ЦУС или Prime и предназначен для удобства настройки. Данный параметр записывается в конфигурационный файл 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:

- `cef_enabled` — разрешение экспорта записей журнала регистрации IP-пакетов по сети:
  - `yes` — запустить экспорт;
  - `no` — остановить экспорт.
- `cef_ip` — IP-адрес сетевого узла, на который будут отправляться сообщения CEF.

Внимание! В качестве сетевого узла нельзя указывать локальный узел localhost, собственные IP-адреса и дополнительные IP-адреса (алиасы) интерфейсов.

- `cef_port` — порт UDP для передачи сообщений CEF. Значение по умолчанию — 514.
- `cef_format` — режим формирования сообщений CEF:
  - `xf` — формирование полных сообщений CEF.
  - `ips` — формирование сообщений CEF только по событиям IPS 67 и 142 для совместимости с ViPNet TIAS.
- `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 управляющей службе. 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 устанавливайте значение `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 управляющей службы.
- `netflow_enabled` - включение/выключение сенсора Netflow:
  - `yes` — включить.
  - `no` — выключить.
- `netflow_ip` — IP-адрес коллектора Netflow.
- `netflow_port` — UDP-порт коллектора Netflow. Значение по умолчанию 500.
- `netflow_send_interval` — период отправки статистики Netflow.

Секция [servers]

Секция `[servers]` содержит список координаторов ViPNet, 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`.

Внимание! При редактировании секции `[servers]` всегда убеждайтесь, что координатор, задаваемый с помощью параметра `active`, существует в сети ViPNet и доступен. Неправильно заданная конфигурация может привести к нестабильной работе ViPNet xFirewall.

Секция [virtualip]

Секция `[virtualip]` описывает настройки виртуальных IP-адресов и содержит следующие параметры:

- `endvirtualip` — служебный параметр, в котором хранится следующий за последним назначенным базовый виртуальный адрес. 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 — `11.0.254.254`). 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 254. 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`.

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] 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;
  - `virtual` — доступ к узлам по их виртуальным IP-адресам.
- `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 управляющей службы 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 управляющая служба 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 управляющей службы командой `iplir stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить ее 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 управляющая служба не перезапускалась. Поэтому после добавления секций `[adapter]` в файл `iplir.conf` вручную рекомендуется сначала запустить управляющую службу командой `iplir start`, затем завершить ее работу командой `iplir stop`, после чего отредактировать нужный файл `iplir.conf-<интерфейс или группа интерфейсов>` и снова запустить управляющую службу.

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 максимальный размер журнала не должен превышать 200 Мбайт. Значение по умолчанию — 50 Мбайт. При указании большего размера журнала он автоматически устанавливается равным 200 Мбайт.

  Реальный размер журнала из-за наличия в нем служебного заголовка получается примерно на 1 Кбайт больше. Каждый раз при запуске управляющей службы 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 (в этом случае при интенсивном трафике в журнале могут регистрироваться не все пакеты).

- `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 «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 при регистрации IP-пакетов, проходящих через интерфейс:
  - `all` — для всех IP-пакетов;
  - `blocked` — для блокированных IP-пакетов или с предупреждением о вторжении (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 mftp.conf

Параметры работы транспортного сервера MFTP содержатся в файле `mftp.conf`.

Чтобы отредактировать файл `mftp.conf`:

1. Завершите работу службы `mftpd`:

   ```
   hostname# mftp stop
   ```

2. Откройте файл для редактирования

   ```
   hostname# mftp config
   ```

3. Внесите изменения.

4. Запустите службу `mftpd`:

   ```
   hostname# mftp start
   ```

Секция [channel]

Секции `[channel]` содержат настройки каналов, по которым ViPNet xFirewall может обмениваться данными с другими узлами. Каждому узлу, зарегистрированному за ViPNet xFirewall в ЦУС (координатор является сервером IP-адресов), а также каждому координатору, с которым есть межсерверный канал связи, соответствует своя секция `[channel]`.

Внимание! Добавление и удаление секций `[channel]` осуществляется автоматически, делать это вручную не следует.

Секции `[channel]` содержат следующие параметры:

- `type` — тип канала. Возможные значения: `mftp` (по умолчанию), `smtp`, `viaroute` (подробнее см. в документе «Настройка с помощью командного интерпретатора», в главе «Настройка транспортного сервера MFTP).
- `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 сервера.
- `call_flag` — признак немедленной передачи конвертов по MFTP. 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.

Примечание. Если параметры `type`, `off_flag`, `call_flag` отсутствуют в секции, то используются их значения по умолчанию.

Нередактируемые параметры

- `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.
- `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.

Секция [debug]

Секция `[debug]` определяет параметры ведения системного журнала транспортного сервера и содержит следующие параметры:

- `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `1` до `5` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение `-1` выключает ведение журнала.
- Не рекомендуется задавать уровень важности выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ИнфоТеКС.
- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `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 сервером. В процессе работы транспортный сервер записывает в этот журнал информацию о полностью принятых, отправленных, удаленных и поврежденных конвертах.

Секция `[journal]` содержит следующие параметры:

- `dump_interval` — период выгрузки информации из журнала конвертов в днях. В процессе работы транспортный сервер 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.

Внимание! Не рекомендуется задавать размер журнала более чем 200 мегабайт, так как при превышении этого значения могут возникнуть проблемы с просмотром журнала конвертов в веб-интерфейсе.

- `use_journal` — включение или выключение ведения журнала работы транспортного сервера. 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

- `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.2018.09.23`.

- `last_dump` — время последней выгрузки информации из журнала конвертов.

Секция [misc]

Секция `[misc]` содержит различные параметры, определяющие работу транспортного сервера MFTP в целом:

- `connect_timeout` — интервал времени в секундах, в течение которого клиент будет пытаться установить соединение с удаленным узлом по каналу MFTP (от `2` до `300`, 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 (от `1` до `1000`, по умолчанию — `900`).
- `max_listen_ports` — диапазон значений перебора портов для соединений по каналу MFTP с удаленным узлом в случае неудачи (от `1` до `10`, по умолчанию — `3`). Транспортный сервер циклично перебирает порты в диапазоне от `port` до `port+max_listen_ports-1`. Ожидая входящие соединения, транспортный сервер прослушивает все порты указанного диапазона.
- `num_attempts` — количество последовательных попыток соединения, после которых устанавливается тайм-аут, если соединиться так и не удалось (от `1` до `10`, 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 (от `5` до `600`, 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:
  - `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 служба `mftpd` ожидает соединения по каналу MFTP от удаленных сетевых узлов (от `1` до `65535`, по умолчанию — `5000`).
- `recv_buff_size` — размер буфера приема в байтах. Параметр имеет нередактируемое значение `65500`.
- `send_buff_size` — размер буфера передачи в байтах. Параметр имеет нередактируемое значение `65500`.

Примечание. Обычно значение `65500` параметров `send_buff_size` и `recv_buff_size` оптимально для обеспечения максимальной скорости приема и передачи конвертов транспортным сервером.

- `save_sent` — включение или выключение хранения имен отправленных прикладных конвертов:
  - `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, возможные значения от `10` до `90`, 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, возможные значения от `10` до `90`, 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, возможные значения от `10` до `90`, 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, возможные значения от `3` до `300`, 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 сервера на ViPNet xFirewall, работающем в составе кластера горячего резервирования:

- `cmd_port` — порт, на котором служба `mftpd` пассивного узла ожидает соединений с активным узлом по резервному каналу для приема управляющих команд (по умолчанию — `6084`). Данный параметр должен иметь одинаковое значение в файлах конфигурации транспортного сервера на активном и пассивном узлах кластера.
- `unpack_timeout` — период времени в секундах, в течение которого активный узел будет ожидать ответы на команды от пассивного узла, 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]), для анализа состояния процесса обновления ПО.
- `transfer_timeout` — период времени в секундах, в течение которого активный узел будет пытаться передавать копии MFTP-конверта пассивному узлу в случае неполного дублирования данного конверта (по умолчанию — `60`). В течение этого времени обработка конверта на активном узле блокируется. Если по истечении этого времени конверт не будет передан на пассивный узел, то его обработка продолжится.

- `use_reserv` — включение или выключение режима резервирования конвертов в кластере горячего резервирования:
  - `yes` (по умолчанию) — конверты резервируются.
  - `no` — резервирование конвертов не производится. В этом случае синхронизировать данные и обновление ПО на узлах кластера необходимо вручную. Кроме того, для корректной работы кластера настройки узлов кластера должны быть одинаковы.
  - При частом переключении режимов на кластере горячего резервирования на пассивном узле могут сохранятся файлы устаревших обновлений. Файлы будут удалены при переключении узла кластера в активный режим или через промежуток времени, указанный в параметре `ttl_ctl` секции `[misc]`.

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 сервером MFTP 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 сервер MFTP 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 сервера 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

Термины и сокращения

Captive portal

Портал аутентификации, предоставляющий пользователям внутренней сети доступ в интернет. Чаще всего Captive portal используется в местах общего доступа в интернет, например, оборудованных точками доступа Wi-Fi.

DPI (Deep Packet Inspection)

Технология расширенной инспекции содержимого сетевого трафика на уровнях 2 — 7 модели OSI и накопления статистики. На основании анализа полученных данных идентифицируются приложения и прикладные протоколы.

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задает связи между ними.
- ViPNet Rollout Center — модуль быстрого развертывания защищенных устройств ViPNet в больших распределенных сетях.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet Центр управления сетью (ЦУС)

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 Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

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).

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) 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. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet 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.

Инкапсуляция пакетов

Принцип передачи данных, при котором данные в формате одного протокола упаковываются в формат другого протокола.

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 ViPNet xFirewall, один из которых (активный) выполняет анализ и фильтрацию трафика, а другой (пассивный) находится в режиме ожидания. В случае сбоев на активном ViPNet xFirewall, пассивный узел становится активным и продолжает выполнять фильтрацию трафика. При этом сбойный ViPNet xFirewall перезагружается и переходит в пассивный режим.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

Предотвращение вторжений (IPS)

Программная или программно-аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

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.

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 узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сеть ViPNet

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

Справочники и лицензия

Справочники, ключи узла и ключи пользователя.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки транспортного конверта MFTP.

Транспортный сервер MFTP

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.