Справочное руководство по конфигурационным файлам

Приложение к руководству администратора ViPNet Terminal 4

infotecs

ФРКЕ.00154-01 90 03

Версия продукта 4.1.8

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В данном документе приведено подробное описание параметров следующих конфигурационных файлов ViPNet Terminal:

- `iplir.conf` — конфигурационный файл управляющего демона.
- `iplir.conf-ethall` — конфигурационный файл сетевого интерфейса eth0.

В перечисленных конфигурационных файлах содержатся параметры, которые можно использовать для настройки ViPNet Terminal, и параметры, задаваемые ПО ViPNet автоматически и приведенные в документе в ознакомительных целях.

Остальные параметры, необходимые для настройки ViPNet Terminal, задаются с помощью команд. Подробнее о настройке с помощью команд см. документ «ViPNet Terminal. Руководство администратора». Описание всех команд содержится в документе «Справочное руководство по командному интерпретатору. Приложение к руководству администратора ViPNet Terminal».

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.

- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.

Контактная информация

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

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

Файл iplir.conf

Параметры защищенной сети содержатся в файле `iplir.conf`. Для редактирования этого файла используется команда `iplir config`. Перед редактированием файла необходимо остановить управляющий демон с помощью команды `iplir stop`, а после окончания редактирования вновь запустить его с помощью команды `iplir start`, чтобы все изменения вступили в силу.

Файл `iplir.conf` содержит секции, описанные ниже.

Секция [adapter]

Секции `[adapter]` описывают статические сетевые интерфейсы компьютера (на стр. 21). Каждому интерфейсу соответствует своя секция `[adapter]`. Если интерфейс не описан секцией `[adapter]`, то все проходящие через него IP-пакеты (на стр. 19) блокируются. Если в файле `iplir.conf` нет ни одной секции `[adapter]`, то управляющий демон при запуске получает от системы список сетевых интерфейсов и автоматически создает соответствующие секции `[adapter]`.

В процессе работы управляющий демон и драйвер ViPNet периодически получают информацию о параметрах известных им интерфейсов с интервалом времени, заданным параметром `ifcheck_timeout` секции `[misc]` (см. «Секция [misc]» на стр. 13). Если обнаруживается, что интерфейс выключен в системе, то он выключается и в драйвере ViPNet. После включения или изменения IP-адреса интерфейса эти изменения автоматически загружаются в драйвер ViPNet.

В секции `[adapter]` указываются следующие параметры:

- `allowtraffic` — разрешение или блокирование прохождения IP-трафика через интерфейс. Возможные значения:
  - `on` (по умолчанию) — IP-пакеты пропускаются или блокируются в соответствии с сетевыми фильтрами, заданными на узле.
  - `off` – IP-пакеты блокируются независимо от остальных настроек.

Нередактируемые параметры

- `ip` — IP-адрес интерфейса.
- `name` — системное имя интерфейса (например, eth0).

Адаптеру eth0, описанному в секции `[adapter]`, соответствует файл конфигурации `iplir.conf-ethall`. Настройка этого файла конфигурации описана в разделе Файл iplir.conf-ethall (на стр. 17).

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала устранения неполадок управляющего демона. Она содержит следующие параметры:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от `-1` до `5` (по умолчанию — `3`). Чем выше уровень детализации, тем более подробная информация выводится в журнал. Значение параметра `-1` выключает ведение журнала.
- `debuglogfile` — место хранения журнала, заданное в виде `syslog:<facility.level>`. Значение 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 координатор, выбранный в параметре `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 координатора, который находится во внешней сети (на стр. 20) и используется для организации входящих соединений с ViPNet Terminal, работающим в режиме **С динамической трансляцией адресов**. Указывается в шестнадцатеричном формате с префиксом `0x`, например: `0x15c8000a`.
- `timeout` — период отправки сообщений внешнему координатору для поддержания активного соединения с ним и пропуска входящего трафика через межсетевой экран. Указывается в секундах, значение по умолчанию — `25`.

Нередактируемые параметры секции [dynamic]

- `firewallip` — внешний IP-адрес доступа (на стр. 19) к ViPNet Terminal, работающему в режиме **С динамической трансляцией адресов**, со стороны других сетевых узлов.
- `port` — порт назначения, на который следует посылать пакеты для ViPNet Terminal, работающего в режиме **С динамической трансляцией адресов**.

Секция [id]

Секция `[id]` используется для описания адресных настроек защищенных узлов (на стр. 20), связанных с ViPNet Terminal. Каждому узлу, с которым у ViPNet Terminal есть связь, соответствует

своя секция [id]. Первая секция [id] соответствует собственным настройкам ViPNet Terminal (собственная секция).

Секция `[id]` содержит следующие параметры:

- `accessiplist` — определяет IP-адреса доступа (на стр. 19) 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 Terminal.

  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 при запуске управляющего демона.

  - `<IP-адрес доступа>` — IP-адрес доступа к узлу. Принимает значение `0.0.0.0`, когда данный узел не находится за межсетевым экраном.
  - `<метрика>` — метрика (на стр. 21) 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]` (см. «Секция [misc]» на стр. 13)). Возможные значения: от `0` до `9999`. По умолчанию метрика имеет значение `auto`, то есть определяется автоматически. Принципы выбора адреса доступа и назначения метрик описаны в документе «ViPNet Terminal. Настройка с помощью командной строки», в главе «Настройка VPN», в разделе «Настройка IP-адресов доступа к узлу и их приоритета».
  - `<реальный IP-адрес узла>` — реальный IP-адрес узла, соответствующий сетевому интерфейсу (на стр. 21), 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 Terminal.
    - `manual` — адрес задан администратором вручную (редактированием файла `iplir.conf`).
    - `addrdoc` — адрес взят из справочников, полученных из программы ViPNet Центр управления сетью (на стр. 19).

    - `other` — адрес добавлен другим способом (например, в качестве адреса доступа добавлен координатор, выбранный внешним межсетевым экраном).

- `blockforward` — включение или выключение блокировки транзитных пакетов, идущих от данного узла либо к нему. По умолчанию этот параметр отсутствует для всех узлов. Может использоваться в секциях для всех узлов, кроме собственного. Принимает значение `on` или `off` (`off` равнозначно отсутствию этого параметра в секции). При включении параметра все транзитные пакеты для данного узла блокируются с кодом 70.
- `fixfirewall` — определяет режим фиксации настроек работы собственного узла через внешний межсетевой экран. Возможные значения:
    - `off` (по умолчанию) — внешний IP-адрес и порт доступа к ViPNet Terminal определяются автоматически по информации от узлов внешней сети;
    - `on` — внешний IP-адрес и порт доступа к ViPNet Terminal жестко заданы администратором в параметрах `firewallip` и `port` данной секции.
- `ip` — содержит реальный адрес (на стр. 21) и соответствующий ему виртуальный адрес (на стр. 20) узла. Причем первым указывается реальный адрес, затем после запятой — виртуальный адрес (например: `ip = 192.168.201.10,10.1.0.5)`. Если указан только реальный адрес, то считается, что ему еще не сопоставлен виртуальный.

Внимание! Виртуальный адрес назначается автоматически, изменять его вручную не следует.

Если узел имеет несколько сетевых интерфейсов или несколько IP-адресов на интерфейсе, в каждой секции `[id]` может быть несколько параметров `ip`. При этом первым должен быть указан параметр, содержащий наиболее приоритетный IP-адрес доступа к данному узлу. При автоматическом обновлении адресов наиболее приоритетный IP-адрес доступа становится первым автоматически. Причем в случае изменения порядка следования IP-адресов виртуальный адрес всегда перемещается вместе с соответствующим реальным.

- `port` — определяет порт назначения, на который следует посылать пакеты для узла, если этот узел находится за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр.
- `proxyid` — определяет режим работы узла, находящегося за межсетевым экраном. Используется во всех секциях `[id]`, кроме собственной, и может принимать различные значения в зависимости от установленного режима. Для удобства идентификаторы записываются в шестнадцатеричном формате с префиксом `0x` (как в параметре `id`). В каждой секции `[id]` может быть только один параметр `proxyid`.
- `tunnel` — содержит адреса незащищенных компьютеров, туннелируемых координатором (на стр. 22), в виде: `ip1-ip2 to ip3-ip4`, где:
    - `ip1` и `ip2` – начальный и конечный адреса диапазона туннелирования;
    - `ip3-ip4` — диапазон, адреса из которого предназначены для замены адресов туннелируемых узлов в случае, когда адреса из диапазона `ip1-ip2` относятся к частной сети и уже используются в локальной сети данного координатора. Этот диапазон может

совпадать с диапазоном `ip1-ip2`. Значение `ip4` формируется автоматически путем прибавления к `ip3` разницы между `ip2` и `ip1`.

Например, чтобы указать, что координатор туннелирует адреса с 192.168.201.5 по 192.168.201.10, которые при необходимости заменяются на адреса из диапазона 192.168.202.5 – 192.168.202.10, следует сделать следующую запись:

```
tunnel= 192.168.201.5-192.168.201.10 to 192.168.202.5-192.168.202.10
```

Примечание. Обычно значения параметров `tunnel` рассылаются в составе справочников и ключей. То есть если туннелируемые адреса координатора заданы в программе ViPNet Центр управления сетью, то другие узлы получат информацию об этом автоматически. Если туннелируемые адреса заданы на координаторе вручную, эти адреса также необходимо указать вручную на каждом узле ViPNet, который будет работать с этими туннелируемыми узлами.

- `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, установлен в значение `off`, в остальных случаях — в значение `on` (см. описание параметра `proxyid` данной секции).

Внимание! Для всех секций параметр `usefirewall` определяется автоматически, изменять его вручную не следует.

- `visibility` — позволяет настроить тип видимости узла. Возможные значения:
  - `auto` — автоматически определять тип видимости узла, в зависимости от текущего адреса видимости узла (на стр. 19).
  - `real` — всегда обращаться к данному узлу по его реальному адресу.
  - `virtual` — всегда обращаться к данному узлу по его виртуальному адресу.

Этот параметр не является обязательным и используется, только если для данного узла необходимо индивидуально задать тип видимости. В случае отсутствия параметра `visibility` видимость узла определяется параметрами секции `[visibility]`, то есть параметрами видимости всей сети, к которой этот узел принадлежит, либо параметрами видимости узлов по умолчанию.

Примечание. Использовать параметр `visibility` нужно осторожно, так как у сетевых узлов, которые видны по виртуальным адресам, могут совпадать реальные адреса (если эти узлы находятся в частных сетях).

Нередактируемые параметры секции [id]

В секции `[id]` кроме параметров, предназначенных для настройки ViPNet Terminal и связанных с ним узлов, также содержатся параметры, значения которых определяются автоматически. Эти параметры носят информативный характер.

Секция `[id]` содержит следующие нередактируемые параметры:

- `accessip` — текущий IP-адрес доступа (на стр. 19) к узлу со стороны ViPNet Terminal. Может принимать значение одного из реальных или виртуальных IP-адресов, в зависимости от физической топологии сети и режимов функционирования ViPNet Terminal и данного узла.
- `always_use_server` — признак работы узла в режиме использования межсетевого экрана с динамической трансляцией адресов с направлением трафика через выбранный координатор. Параметр присутствует только в случае работы данного узла в указанном режиме и принимает значение `on`.
- `dynamic_timeout` — период опроса (в секундах) ViPNet-координатора, выбранного в качестве межсетевого экрана для данного узла, с целью обеспечения пропуска входящего трафика через межсетевой экран. Данный параметр присутствует во всех секциях `[id]`, кроме собственной.
- `id` — уникальный идентификатор узла. По этому параметру управляющий демон отличает одну секцию `[id]` от другой. Идентификатор присваивается сетевому узлу ViPNet при его создании в программе ViPNet Центр управления сетью (ЦУС) (на стр. 19). В каждой секции `[id]` может быть только один такой параметр.
- `firewallip` — определяет внешний IP-адрес доступа к узлу в случае, если этот узел находится за межсетевым экраном. При работе с узлом, установленным за межсетевым экраном, все направленные к нему зашифрованные пакеты инкапсулируются (на стр. 20) в единый тип (UDP) 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 имеет значение `0.0.0.0`. В каждой секции `[id]` может быть только один такой параметр.
- `name` — имя узла. Задается администратором сети ViPNet в программе ViPNet Центр управления сетью (ЦУС) (на стр. 19) и предназначен для удобства настройки. Данный параметр записывается в файл конфигурации автоматически при его сохранении. В каждой секции `[id]` может быть только один такой параметр.
- `virtualip` — базовый виртуальный адрес узла. В каждой секции `[id]` может быть только один такой параметр.

Секция [misc]

Секция `[misc]` содержит различные дополнительные параметры:

- `ciphertype` — алгоритм шифрования для исходящих пакетов, адресованных сетевым узлам ViPNet. Параметр может принимать следующие значения:
  - `gost` — шифрование с помощью алгоритма ГОСТ;
  - `aes` — шифрование с помощью алгоритма AES.

  По умолчанию используется значение `gost`.

  

  Примечание. Установка параметра `ciphertype` влияет только на шифрование исходящего трафика.

- `ifcheck_timeout` — интервал опроса (в секундах) параметров адаптеров, известных управляющему демону. По умолчанию значение данного параметра 30 секунд.
- `msg_compress_level` — степень сжатия служебных межсерверных сообщений. Возможные значения: от 1 (минимальная компрессия, максимальная скорость) до 9 (максимальная компрессия, минимальный объем служебного трафика). Значение по умолчанию — 3.

  

  Примечание. На высоконагруженных узлах не рекомендуется устанавливать значение параметра `msg_compress_level` больше 5.

- `mssdecrease` — число байт, на которое будет уменьшен параметр MSS (максимальный размер сегмента) протокола TCP для исключения фрагментации шифрованных ViPNet-пакетов. Значение по умолчанию — `0`.

  В случае если проверка соединения между узлами (ping) или туннелируемыми узлами проходит нормально, но TCP-соединения не устанавливаются, то, скорее всего, по пути следования пакетов на каких-то устройствах производится фрагментация пакетов и их блокировка. Для устранения таких проблем рекомендуется уменьшить значение MSS, например, на 20–40. Уменьшение параметра MSS достаточно произвести только с одной стороны. Данная настройка на координаторе обеспечивает работоспособность как для узлов, взаимодействующих с координатором, так и для туннелируемых устройств, стоящих за ним. Настройка на координаторе не действует на узлы, стоящие за ним. Для таких узлов данный параметр следует изменять непосредственно на самих этих узлах или на других узлах, взаимодействующих с ними.

  

  Внимание! Параметр `mssdecrease` не следует изменять без крайней необходимости.

- `omnnumthreads` — количество ядер процессора, используемое для обработки служебных сообщений (по умолчанию — 1).

- `packettype` — формат шифрованных пакетов. Возможные значения: `4.0` или `4.1`. По умолчанию установлен формат `4.1`.

  Данный параметр влияет только на формат пакетов, посылаемых данным сетевым узлом. Формат входящих пакетов определяется автоматически, и их расшифрование производится вне зависимости от установленного значения параметра `packettype`. Рекомендуется использовать формат `4.1`, однако если необходимо связываться с узлами, на которых установлены старые версии ПО ViPNet, не поддерживающие формат `4.1`, то необходимо использовать формат `4.0`.

Примечание. Установка формата 4.0 совместно с алгоритмом шифрования AES не допускается (см. описание параметра `ciphertype`).

- `timediff` — максимально допустимая разница во времени между сетевыми узлами (в секундах). Из соображений безопасности ViPNet запрещает прохождение пакетов от сетевого узла, если его время отличается от времени собственного узла более, чем на число секунд, указанное в параметре `timediff`. Значение параметра должно быть больше 1 секунды и меньше 7200 секунд включительно. По умолчанию его значение равно 7200 (то есть два часа).
- `tunnel_local_network` — параметр, который позволяет не туннелировать IP-адреса, входящие в локальную подсеть ViPNet Terminal. Возможные значения:
  - `off` (по умолчанию) — обращаться к туннелируемым узлам, находящимся в локальной подсети, минуя туннелирующий координатор;
  - `on` — обращаться к туннелируемым узлам, находящимся в локальной подсети, через координатор, который туннелирует данные узлы. В этом случае доступ к туннелируемым узлам в локальной подсети может быть затруднен.
- `warnoldautosave` — включение или выключение предупреждения о наличии старых автосохраненных конфигураций ViPNet. Может принимать значение `on` или `off`. Если значение параметра `on`, то при старте управляющего демона будут выдаваться предупреждения о наличии автоматически сохраненных конфигураций, дата сохранения которых меньше текущей даты более чем на один месяц.

Секция [servers]

Секция `[servers]` содержит список координаторов, известных ViPNet Terminal. Изменять параметры этой секции не рекомендуется.

Секция `[servers]` содержит следующие параметры:

- `server` — идентификатор и имя координатора, указанные через запятую. Каждому координатору соответствует один параметр `server`.
- `active` — идентификатор координатора, который является сервером IP-адресов для ViPNet Terminal.

Секция [virtualip]

Секция `[virtualip]` описывает настройки виртуальных IP-адресов (на стр. 20) и содержит следующие параметры:

- `endvirtualip` — служебный параметр, в котором хранится следующий за последним назначенным базовый виртуальный адрес (на стр. 20). Используется в качестве точки отсчета при поиске и назначении базовых виртуальных адресов для новых защищенных узлов. При назначении базовых виртуальных адресов сначала производится поиск первого свободного адреса в диапазоне от `endvirtualip` до `maxvirtualip`. Если в этом диапазоне свободных адресов нет, то производится поиск в диапазоне от `startvirtualip` до `endvirtualip`.

Внимание! Параметр `endvirtualip` не следует изменять (особенно увеличивать) без крайней необходимости.

- `maxvirtualip` — максимальный адрес для формирования базовых виртуальных адресов защищенных узлов (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 защищенных узлов (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` секций `[id]` (см. «Секция [id]» на стр. 8).
- `startvirtualiphash` — служебный параметр, который используется для ручного переназначения виртуальных адресов узлов. С помощью данного параметра управляющий демон при запуске определяет, был ли изменен стартовый виртуальный адрес, и в случае, если стартовый виртуальный адрес был изменен, производит переназначение виртуальных адресов для всех узлов. Подробнее см. в документе «ViPNet Terminal. Руководство администратора», в главе «Настройка VPN», в разделе «Принципы назначения виртуальных адресов».

Примечание. Параметр `startvirtualiphash` не следует изменять, кроме случая, когда это необходимо для тонкой настройки с целью переназначения виртуальных адресов узлов.

- `starttunnelvirtualip` — стартовый адрес для формирования виртуальных адресов туннелируемых узлов в автоматическом режиме (по умолчанию для диапазонов адресов туннелируемых узлов — `12.0.0.1`, для адресов одиночных туннелируемых узлов — `11.0.0.1`).

Секция [visibility]

Секция `[visibility]` содержит настройки видимости защищенных сетевых узлов, с которыми связан ViPNet Terminal. В отличие от параметра `visibility`, с помощью которого в секциях `[id]` (см. «Секция [id]» на стр. 8) 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 (на стр. 21);
  - `virtual` — доступ к узлам по их виртуальным IP-адресам (на стр. 20).
- `subnet_real` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по реальным IP-адресам.

  Идентификаторы сетей указываются в шестнадцатеричном формате с префиксом `0x`. В одной секции `[visibility]` можно задать несколько параметров `subnet_real`. При этом в каждом параметре можно указать либо один идентификатор, либо несколько идентификаторов через запятую. Например:

  ```
  subnet_real = 0x5155
  subnet_real = 0x5156,0x5157,0x5158
  ```

- `subnet_virtual` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по виртуальным IP-адресам. Задается так же, как параметр `subnet_real`.

Внимание! Один и тот же идентификатор сети ViPNet можно указать только в одном из параметров `subnet_real` или `subnet_virtual`.

При старте управляющего демона идентификаторы, заданные в параметрах `subnet_real` и `subnet_virtual`, автоматически сортируются в порядке возрастания и группируются в строки, каждая из которых содержит максимум 8 идентификаторов.

Параметры `subnet_real` и `subnet_virtual` являются необязательными и по умолчанию отсутствуют в секции `[visibility]`

Файл iplir.conf-ethall

Параметры настройки сетевого интерфейса eth0 содержатся в файле `iplir.conf-ethall`. Для редактирования этого файла используется команда `iplir config ethall`. Перед редактированием файла необходимо остановить управляющий демон с помощью команды `iplir stop`, а после окончания редактирования вновь запустить его с помощью команды `iplir start`, чтобы все изменения вступили в силу.

Файл конфигурации для интерфейса eth0 содержит только секцию `[db]`. Секция `[db]` используется для задания параметров журнала трафика. Журнал хранится в том же каталоге, где находятся файлы конфигурации, в файле с именем `iplir.db-ethall`. Максимальный размер журнала устанавливается пользователем.

Записи о пакетах накапливаются в журнале 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]` содержит следующие параметры:

- `maxsize` — максимальный размер журнала в мегабайтах (1 мегабайт = 1048576 байт).

  

  Внимание! Максимальный размер журнала должен быть не более 10 Мбайт. При указании большего размера он принудительно устанавливается в 10 Мбайт.

  Реальный размер журнала из-за наличия в нем служебного заголовка получается примерно на 1 Кбайт больше. Каждый раз при запуске управляющего демона после размера журнала автоматически дописывается слово `MBytes`, если оно отсутствует. Поэтому при изменении значения этого параметра его можно не писать. Значение параметра `0` отключает ведение журнала. При этом если до отключения журнала в нем были записи, то просмотреть их будет невозможно.

- `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 регистрации информации о порте клиента 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 `off`, 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.

- `timedif` — интервал времени, в течение которого одинаковые события объединяются в журнале в одну запись. Задается в секундах, значение по умолчанию — `60`. Если это параметр установлен в `0`, то объединение событий не используется. В этом случае при интенсивном трафике в журнале могут регистрироваться не все пакеты.

Глоссарий

IP-пакет

Форматированный блок информации, передаваемый в сети по протоколу IP.

IP-форвардинг

IP-форвардинг или маршрутизация транзитных IP-пакетов (не предназначенных для этого компьютера), является опциональной возможностью стека протоколов TCP/IP в операционной системе Linux. Данная функция обеспечивает пересылку транзитных IP-пакетов через сетевые интерфейсы компьютера.

ViPNet Network Manager

Программа, которая входит в состав программного комплекса ViPNet VPN. Предназначена для создания, конфигурирования и управления малыми и средними сетями ViPNet.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

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).

Базовый виртуальный адрес

Базовый виртуальный адрес является точкой отсчета при назначении виртуальных адресов для каждого из реальных адресов узла. Если в данный момент узел виден по виртуальному адресу, то его адресом доступа считается либо базовый виртуальный адрес, либо вторичный виртуальный адрес, соответствующий первому в списке реальному адресу.

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet Б назначаются непосредственно на узле А. На других узлах узлу ViPNet Б могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Внешние IP-адреса

Адреса внешней сети.

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Инкапсуляция пакетов

Принцип передачи данных, при котором данные в формате одного протокола упаковываются в формат другого протокола.

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, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Метрика

Используется в маршрутизации и при задании нескольких IP-адресов доступа. В первом случае определяет приоритет маршрута передачи IP-трафика, сформированного по протоколу DHCP, во втором — приоритет использования каналов связи (задержку в миллисекундах отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса).

Реальный IP-адрес

IP-адрес, назначенный сетевому интерфейсу компьютера в локальной сети или Интернете.

Сетевой интерфейс

Устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. Сетевым интерфейсом может служить сетевая плата, модем и другие подобные устройства.

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 сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Туннелирование

Технология, позволяющая защитить соединение с участием открытых узлов при передаче данных через Интернет и другие публичные сети. Туннелирование заключается в шифровании трафика открытых узлов координаторами.

Указатель