УТВЕРЖДЕНО

BY.РТНК.00006-04.1 34 01-21-ЛУ

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1»

Программный продукт «Bel VPN L2 4.1»

Руководство администратора

BY.РТНК.00006-04.1 34 01-21

Листов 19

2016

Содержание

Требования на базовые платформы и совместимость 6
Назначение и функции 7
Инициализация 8
Настройка 9
Запуск и останов 13
Информация о текущем состоянии L2-туннеля 15
Протоколирование 16

Лицензионное Соглашение

о праве пользования программным продуктом «Bel VPN L2 4.1» производства ООО «С-Терра Бел»

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного программного продукта «Bel VPN L2 4.1» (далее – Продукт) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Продукта, являющейся неотъемлемой частью настоящего Лицензионного Соглашения). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Продуктом.

Под Продуктом понимается комплекс материальных объектов (программных, аппаратных средств, носителей информации, кода программных продуктов, документации в печатной и электронной формах), состав которых определяется артикулом из прайс-листа Общества с ограниченной ответственностью «С-Терра Бел», и объекты которого не могут быть использованы отдельно друг от друга.

Продукт может использоваться для защиты трафика на канальном уровне (L2) и не предназначен для использования в других целях. Использование Продукта в прочих системах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.

Продукт может включать компоненты (программные и аппаратные средства, информационные носители и прочее) от третьих поставщиков. Конечный Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих поставщиков, которые являются в совокупности неотъемлемой частью настоящего Лицензионного Соглашения.

Продукт в полном комплекте передается Конечному Пользователю на условиях настоящего Лицензионного Соглашения.

Продукт и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Республики Беларусь об авторском праве на объекты интеллектуальной собственности.

Установка Продукта после предъявления Конечному Пользователю текста Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступление его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 403 Гражданского кодекса Республики Беларусь имеет силу договора между Конечным Пользователем и Производителем Продукта (ООО «С-Терра Бел»).

При наличии компонент третьих поставщиков Производитель является законным и полномочным представителем третьих поставщиков, если обратное не оговорено в Лицензионных Соглашениях третьих поставщиков или в других документах, регламентирующих отношения между Конечным Пользователем и третьими поставщиками.

Все компоненты третьих поставщиков объединяются в программный комплекс в процессе установки Продукта. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Продукта только в составе работ, связанных с эксплуатацией Продукта. Копирование, распространение, установка и эксплуатация отдельных компонент являются нарушением настоящего Лицензионного Соглашения и авторских прав как Производителя, так и третьих поставщиков (если обратное не оговорено в Лицензиях и Лицензионных Соглашениях третьих поставщиков).

Конечный Пользователь может хранить, устанавливать и использовать в рамках Лицензионного Соглашения только один экземпляр Продукта, и не имеет права хранить, устанавливать, использовать большее количество экземпляров Продукта.

Конечный Пользователь не имеет права распространять Продукт в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Продукта путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения.

Конечный Пользователь не имеет права дисассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и другие компоненты Продукта, вносить какие-либо изменения в бинарный код программ и совершать относительно Продукта другие действия, нарушающие белорусское и международное законодательство по авторскому праву и использованию программных средств.

Настоящее Лицензионное Соглашение вступает в силу с момента установки Продукта и действует на протяжении всего срока использования Продукта.

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Республики Беларусь от 17.05.2011 г. "Об авторском праве и смежных правах" и преследуется по закону.

Настоящее Лицензионное Соглашение предоставляет Конечному Пользователю Ограниченные гарантии, состоящие в том, что:

1. На аппаратные платформы в обязательном порядке предоставляются гарантии производителя. Срок действия гарантийных обязательств и адрес точки предоставления гарантийного обслуживания указаны в документации, сопровождающей аппаратную платформу. При этом состав и условия предоставления сервиса гарантийного обслуживания аппаратных платформ определяется производителем аппаратных платформ.

2. В случае, если в ходе эксплуатации Продукта Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ООО «С-Терра Бел») обеспечивает:

а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения

б) бесплатное предоставление обновлений программного обеспечения Производителя Продукта, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 2 базируется на следующем определении: Критичная Проблема заключается в том, что Продукт, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.2б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

3. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Продукта дефекты в составе информационных носителей или некомплектность Продукта, то информационные носители будут заменены, а комплектность Продукта восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Продукта любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Продукта и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Ввиду того, что Продукт поставляется как законченный продукт, обладающий заявленной в технической документации функциональностью и прошедший цикл выходного контроля и сертификационных испытаний для строго определенной среды функционирования, настоящее Лицензионное Соглашение ограничивает Конечного Пользователя в части несанкционированных изменений Продукта, к которым относятся:

- МОДЕРНИЗАЦИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ, ВКЛЮЧАЯ УСТАНОВКУ ШТАТНЫХ ОБНОВЛЕНИЙ,
- ДОБАВЛЕНИЕ/ОТКЛЮЧЕНИЕ ОТДЕЛЬНЫХ СЕРВИСОВ ОПЕРАЦИОННОЙ СИСТЕМЫ (ПО ОТНОШЕНИЮ К СОСТОЯНИЮ ОПЕРАЦИОННОЙ СИСТЕМЫ НА МОМЕНТ ПОСТАВКИ ПРОДУКТА),
- УСТАНОВКА ДОПОЛНИТЕЛЬНЫХ ПРИЛОЖЕНИЙ,
- САМОСТОЯТЕЛЬНОЕ ДОБАВЛЕНИЕ/УДАЛЕНИЕ АППАРАТНЫХ КОМПОНЕНТ (В ТОМ ЧИСЛЕ СЕТЕВЫХ КАРТ, ЖЕСТКИХ ДИСКОВ И Т.П.).

Нарушение этих ограничений рассматривается как нарушение целостности Продукта и трактуется Производителем Продукта как основание для отказа Конечному Пользователю в сервисе технического сопровождения и поддержки Продукта.

Нарушение условий эксплуатации аппаратной платформы Продукта, заявленных производителем аппаратной платформы, может являться причиной отказа в гарантийном обслуживании аппаратной платформы.

Настоящее Лицензионное Соглашение (в рамках законодательства Республики Беларусь и если противное не оговорено в виде отдельного дополнительного соглашения с Конечным Пользователем) не регламентирует вопросы технических, организационных и прочих возможных проблем, связанных с эксплуатацией Продукта и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Продукта.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Продукта Конечным Пользователем. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие код и прочие информационные компоненты Продукта, включая информацию на внутренних носителях Продукта. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Дистрибутив Debian и включенные в него компоненты является свободно распространяемым Продуктом и используется в составе Изделия без каких-либо модификаций в соответствии с лицензиями (https://www.debian.org/legal/licenses/). Debian является торговой маркой, принадлежащей Software in the Public Interest, Inc.

Cisco, Cisco IOS Router, Cisco Security Manager являются торговыми марками компании Cisco Systems в США и в других странах.

Программный Продукт Системная Библиотека GNU libc является свободно распространяемым Продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (http://www.gnu.org/licenses/licenses.html).

Продукта включает в себя программное обеспечение, написанное Эриком Янгом (Eric Young. eay@cryptsoft.com).

Java является торговой маркой корпорации Oracle.

Другие названия компаний и продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Продукта могут являться зарегистрированными торговыми марками соответствующих им компаний. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является ни поддержкой, рекомендацией либо рекламой. Общество с ограниченной ответственностью «С-Терра Бел» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.

Напечатано в Республике Беларусь

Общество с ограниченной ответственностью «С-Терра Бел»

220012, г. Минск, ул. Чернышевского, д. 10А, пом. 702Б1

Телефон: (+375 17) 280 6000

Факс: (+375 17) 280 78 67

Эл.почта: *info@s-terra.*by

http://www.s-terra.by

Требования на базовые платформы и совместимость

Программный продукт «Bel VPN L2 4.1» (далее - Bel VPN L2) функционирует под управлением операционной системы Debian GNU/Linux 6.

«Bel VPN L2» является самостоятельным Продуктом, но поставляется и работает только совместно с программно-аппаратным комплексом «Шлюз безопасности Bel VPN Gate 4.1» (далее, ПАК Шлюз) или программным комплексом «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1» (далее, ПК Шлюз-В).

Назначение и функции

Программный продукт «Bel VPN L2» предназначен для:

- передачи кадров протокола канального уровня между географически распределенными сегментами ЛВС;
- передачи данных между локальными сетями не по IP-протоколам, интеграции приложений, использующих широковещательные механизмы передачи данных;
- построения географически распределенных виртуальных локальных сетей VLAN, работающих по стандарту IEEE 802.1q.

Программный продукт «Bel VPN L2» позволяет объединить удаленные сегменты локальной Ethernet сети посредством WAN соединений. Передача данных между удаленными сегментами Ethernet сети через общедоступную сеть осуществляется по протоколу UDP. Для организации передачи пакетов между сетями с различными протоколами используется туннелирование – Ethernet-кадр инкапсулируется в UDP-пакет (получаем L2-туннель). А для защиты UDP-трафика используется программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1» или программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1» – выполняется IPsec-инкапсуляция (VPN-туннель).

Программный продукт «Bel VPN L2» реализован в виде usermode-демон – l2svc. Используя драйвер TUN/TAP, для каждого L2-туннеля на шлюзе создаётся виртуальный TAP-интерфейс, соединенный мостом с физическим Ethernet-интерфейсом (внутренним интерфейсом шлюза, на котором осуществляется захват Ethernet-кадров). Эти интерфейсы работают в режиме прослушивания (promiscuous mode). Продукт запоминает mac-адреса захватываемых Ethernet-кадров. Захваченные на внутреннем интерфейсе Ethernet-кадры подлежат инкапсуляции в UDP-пакеты и последующей отправке, только если их destination mac-адрес не является локальным для данного сегмента сети. Это позволяет избежать передачи лишнего трафика. ПАК Шлюз / ПК Шлюз-В, при необходимости создает IPsec-туннель и передает данные в удаленную сеть на шлюз назначения. На шлюзе назначения производится сначала IPsec-декапсуляция, а затем – UDP-декапсуляция и полученные Ethernet-кадры передаются в защищаемую сеть через внутренний интерфейс. Встречный трафик между сетями идёт аналогичным образом.

Примеры сценариев, иллюстрирующих построение защищенного соединения между сегментами одной сети, приведены на сайте http://www.s-terra.by/ в разделе «Решения – Типовые сценарии применения продуктов S-Terra Bel».

Инициализация

Программный продукт «Bel VPN L2» поставляется предварительно инсталлированным.

Перед запуском Bel VPN L2 необходимо создать файл с лицензией и конфигурационный файл с настройками.

В случае запуска без предварительной настройки будет выдано сообщение «`No configuration files found. Exiting`», после чего процесс завершится.

Описание конфигурационного файла приведено в разделе «Настройка».

Создание лицензионного файла описано ниже, в соответствующем подразделе.

Создание лицензионного файла

Для нормальной работы Bel VPN L2 необходимо создать файл с лицензией `l2.lic` в директории `/opt/l2svc/etc`.

При запуске без лицензии будет произведена проверка конфигураций с выдачей ошибок при их наличии, но туннели строиться не будут.

Пример лицензии (недопустимы пробелы между названием поля, знаком “=” и значением поля):

```
[license]
CustomerCode=test
ProductCode=L2VPN
LicenseNumber=1
LicenseCode=1234567890ABCDEF
```

Лицензионный файл можно создать вручную или с помощью скрипта ввести значения запрашиваемых полей:

```
/opt/l2svc/bin/license.sh
```

При запуске скрипта, проверяется наличие уже существующего файла с лицензией, и , в случае его обнаружения, пользователь может использовать лицензионную информацию либо ввести новую лицензию.

Если создается новая лицензия, то после ввода всей необходимой информации будет создан файл лицензии – `l2.lic`, а уже имеющаяся лицензия будет помещена в файл `l2.lic.old`. Далее будет произведена проверка лицензионной информации.

Если лицензия верна, будет выдано сообщение `License OK` и скрипт завершит работу. Иначе будет выдано сообщение об ошибке, восстановлен старый файл лицензии (если он существовал), и потребуется заново ввести лицензионную информацию.

Настройка

Настройка Bel VPN L2 выполняется в текстовом конфигурационном файле и заключается в описании параметров создаваемого L2-туннеля.

Конфигурационный файл должен иметь расширение `.conf` и располагаться в каталоге `/opt/l2svc/etc`. В этом же каталоге размещается пример конфигурационного файла – `sample_conf.txt`.

Для каждого создаваемого туннеля необходимо подготовить отдельный файл с конфигурацией. При этом разные туннели могут использовать один сетевой мост (bridge) и сетевой интерфейс (capture), с которого будет осуществляться захват ethernet-фреймов, но у каждого туннеля должен быть свой виртуальный интерфейс. Причем как сетевой интерфейс (capture), так и виртуальный интерфейс могут входить только в один мост (bridge). Включать один и тот же интерфейс в разные мосты не допускается.

При использовании нескольких туннелей, необходимо прописать для них разные локальные порты.

Примечание: на удаленном шлюзе, с которым устанавливается соединение, тоже должен быть описан соответствующий туннель.

Рекомендуется не использовать Bel VPN L2 на всех интерфейсах ПАК Шлюз / ПК Шлюз-В, поскольку хотя бы один интерфейс необходим для передачи трафика на удаленный шлюз безопасности (WAN-интерфейс).

Настройки «Bel VPN L2 » считываются из конфигурационного файла при запуске, поэтому после внесения изменений следует перезапустить демон или операционную систему (при этом демон запустится автоматически).

Настройка L2-туннелей

Все параметры в одном конфигурационном файле могут быть заданы только однократно.

Текст, начинающийся с '#' и до конца строки, считается комментарием и игнорируется Продуктом.

Опции конфигурационного файла также можно задать в командной строке при прямом запуске бинарного файла `/opt/l2svc/bin/l2svc`, указав перед ними «--».

Опишем возможные параметры конфигурационного файла:

Обязательные параметры

- *vif* <*name*> – имя виртуального интерфейса (TAP). Рекомендуется tapN, где N – цифра.
- *capture* <*name*> – имя сетевого интерфейса, с которого будет осуществляться захват ethernet-фреймов. Этому интерфейсу не рекомендуется назначать IP-адрес.
- *bridge* <*name*> – имя виртуального интерфейса моста. Рекомендуется brN, где N – цифра.

Опциональные параметры

- *local* <*host*> – ip-адрес или символьное имя локального хоста.
- *remote* <*host*> *[port]* – ip-адрес или символьное имя и порт удалённого хоста.
- *port* <*port*> – номер используемого UDP-порта, используемый и для локального и для удалённого хостов. Значение по-умолчанию – 1194 (порт протокола Openvpn).
- *local_port* <*port*> – номер порта на локальном хосте. Значение по-умолчанию – 1194 (порт протокола Openvpn).
- *hwaddr* <*hw*> – MAC-адрес виртуального интерфейса.

- *bonding [name]* – включение bonding-режима. В данном режиме трафик с одного физического интерфейса разделяется на два l2-туннеля. При этом возможно увеличение производительности tcp трафика либо многопоточного трафика. Имя bond-интерфейса – bond0. Дополнительный параметр *name* может использоваться для использования другого bond-интерфейса, но только совместно с дополнительной настройкой bond-драйвера.

  При использовании bonding-режима нужно создать два конфигурационных файла (по одному на туннель), отличающихся портами и tap-интерфейсами. Настройка должна быть произведена с обеих сторон туннеля.

  При распределении пакетов между tap-интерфейсами используется режим balance xor с политикой хеширования (xmit_hash_policy) layer2+3. В этом случае, на какой из tap-интерфейсов направить пакет, вычисляется по полям: source mac, destination mac, source ip, destination ip.

  Возможно использование политики хэширования layer3+4, в этом режиме для вычисления хэша будут учитываться поля: source ip, destination ip, source port, destination port. Для этого надо отредактировать скрипт `/opt/l2svc/bin/up`, а именно строку:

  ```
  modprobe bonding mode=2 xmit_hash_policy=layer2+3 >/dev/null 2>&1
  ```

- *nobind* – использовать случайный локальный порт. Применимо для автоматического назначения локальных портов при поднятии нескольких туннелей. Может быть использован только вместе с *remote*.
- *log* <*file*> – писать логи в файл вместо протоколирования в syslog.
- *verb* <*n*> – уровень подробности протоколирования.

  Уровни:

  0 – только критические ошибки,

  1 – информация о старте продукта и построении соединений, а также не критические сетевые ошибки;

  2 – показ информации об измеренном MTU, открытии/закрытии TAP-интерфейсов, рестартах продукта и соответствии опций туннеля на локальном и удалённом хостах;

  3 – на каждый входящий/исходящий UDP-пакет в лог будет писаться R/W, на каждый прочитанный/записанный TAP-интерфейсом пакет – r/w.

  Значение по-умолчанию – 1.

- *mute [n]* – не повторять более n однотипных сообщений подряд. Если *n* не указано, оно считается равным 1. По-умолчанию в Продукте выставлено mute=1000.
- *nice* <*n*> – изменить приоритет процесса.
- *status* <*file*> *[n]* – писать в <*file*> каждые *n* секунд информацию о текущем состоянии туннеля. Если *n* не указано, обновление раз в минуту. В файл пишется информация о количестве переданных и полученных байт по udp-туннелю, а также количество байт, записанных и прочитанных TAP-интерфейсом.
- *compression [always|adaptive]* – использование сжатия библиотекой LZO. *Adaptive* – использование адаптивного алгоритма, позволяющее избежать проблем при передаче уже сжатого трафика. При этом регулярно проводится проверка, насколько удалось сжать пакет. Если выигрыш составляет менее 5%, то сжатие выключается до следующей проверки (на 1 минуту). Если не указано *always* либо *adaptive*, используется *adaptive*. Пакеты размером 100 байт и меньше не сжимаются. По-умолчанию отключено.
- *tun_mtu* <*n*> – MTU туннеля (туннельного интерфейса). Значение по-умолчанию – 1500.

- *mtu_test* – при выставлении данного параметра Продукт попытается определить mtu соединения, посылая служебные пакеты (собственного формата, не icmp) различного размера. Результат будет записан в лог. Длительность процедуры – до нескольких минут. Полученное значение (минимальное) можно применить в *mssfix*, *fragment*, *tun_mtu*. При использовании данной опции необходимо отключить *fragment* и *mssfix* Данная опция автоматически выставляет использование path mtu discovery. После получения эмпирического значения mtu данный параметр нужно убрать из конфигурации. По-умолчанию отключено.
- *pmtud <do|dont|want>* использование path mtu discovery для автоматического выяснения размера mtu udp-канала, по которому будет пересылаться захваченный трафик:

  do – использовать pmtud, при этом всегда будут выставляться DF(don't fragment) флаги;

  dont – не использовать pmtud, DF-флаги выставляться не будут;

  w*ant* – использовать индивидуальные настройки маршрутов.

  Работа механизма path mtu discovery зависит от icmp-пакетов, и в реальных сетях могут быть проблемы (блокирование icpm трафика на промежуточных хостах). В таком случае рекомендуется использовать опции *mssfix* и *fragment*. По умолчанию path mtu discovery не используется.
- *mssfix [n] [force]* – при включении данной опции поле MSS всех проходящих через туннель tcp-пакетов будет выставлено в *n*, если текущее значение mss в пакете больше *n*. Также, если определены *tun_mtu* либо *fragment*, и их значения меньше указанного в *mssfix*, в пакет будет прописано минимальное из них. При указанной опции *force* будет прописано именно указанное в конфигурационном файле значение *mssfix*, даже если оно больше имеющегося в пакете. При этом tcp/ip стек отправителя и получателя сам уменьшит максимальный размер пакета, не прибегая к использованию icmp. Это позволит избежать фрагментации. Если параметр *n* отсутствует, будет взято значение параметра *fragment*, если оно определено. Работает только для tcp-трафика. Значение по-умолчанию – 1380.
- *fragment n* – если задано, то все пакеты, большие *n* байт, будут фрагментированы самим продуктом (а не ip-стеком). Это происходит в usermode-режиме, поэтому выполняется медленнее, чем фрагментация IP-стеком. Однако фрагментация ip-стеком завязана на path mtu discovery и в реальных условиях может не работать. Фрагментирование производится после сжатия, если оно включено. Опции добавляет 4 байта к размеру пакета. Включение данной опции может искажать результаты *mtu_test*. По-умолчанию отключено.
- *passtos* – выставить ToS-поле отправляемого UDP-пакета такое же, как у захваченного пакета. По-умолчанию отключено.
- *txqueuelen <n>* – длина очереди отправки пакетов виртуального (TAP) интерфейса. Значение по-умолчанию – 1000.
- *sndbuf <n>* – размер буфера отправки UDP-сокета. Значение по-умолчанию – 65536 байт.
- *rcvbuf <n>* – размер буфера приёма UDP-сокета. Значение по-умолчанию – 65536 байт.
- *keepalive <n> <m>* – при указании данного параметра Продукт будет посылать по туннелю keepalive-пакеты собственного формата раз в *n* секунд. Если на отправленный пакет не будет ответа в течение *m* секунд либо от партнёра не придёт любого другого пакета – будет произведён частичный перезапуск продукта (будут пересозданы сокеты и виртуальный интерфейс, произойдёт пересоздание моста. Конфигурационные файлы перезачитываться не будут). Так как происходт пересоздание моста (bridge), использование keepalive невозможно при построении топологии «звезда». Рекомендуется выставлять *keepalive* на обоих концах туннеля и с одинаковыми значениями параметров. По-умолчанию отключено.
- *no_timestamps* – не писать время в логи. По-умолчанию время пишется.
- *no_paging* – запретить использование файла подкачки. По-умолчанию отключено.

Пример описания туннеля:

```
#just another l2-tunnel
vif tap0
capture eth0
bridge br0

remote 1.2.3.4 2345
tun_mtu 6000
mssfix 1380
```

Настройка Bel VPN Gate / Bel VPN Gate-V

В политике безопасности ПАК Шлюз / ПК Шлюз-В, на котором установлен Bel VPN L2, должны быть указаны правила шифрования UDP-трафика, проходящего по L2-туннелю, а также правила, запрещающие поступление UDP-пакетов на внешний интерфейс шлюза с остальных хостов WAN.

Запуск и останов

Запуск

Для запуска программного продукта «Bel VPN L2» следует выполнить команду:

```
/etc/init.d/l2svc start
```

или

```
service l2svc start.
```

При запуске демона `l2svc` на консоль выдается сообщение о версии Bel VPN L2.

В дальнейшем, после выполнения первоначальных настроек и первого запуска, Продукт будет автоматически запускаться при загрузке операционной системы.

В случае запуска Продукта без предварительной настройки (отсутствуют конфигурационные файлы) будет выдано сообщение «`No configuration files found. Exiting`», после чего процесс завершится.

При повторном запуске одновременно двух и более копий Продукта (двух демонов) будут перезачитаны файлы конфигураций.

Запуск с указанием параметров

При прямом запуске бинарного файла `/opt/l2svc/bin/l2svc` можно задать параметры, указав перед ними «--». Параметры могут быть как общими, так и относящиеся к создаваемому туннелю. Общие параметры описаны ниже, а параметры туннеля описаны в подразделе «Настройка L2-туннелей».

Общие параметры:

`config <file>` – имя конфигурационного файла, из которого будут прочитаны параметры;

`help` – выводится на консоль краткая информация о параметрах Продукта. Затем данная копия Продукта завершит свою работу;

`version` – вывод на консоль информации о версии Продукта, эту же информацию можно получить если запустить бинарный файл без опций командной строки. После выдачи сообщения данная копия Продукта завершит свою работу;

`license` – проверка текущей лицензии. Будет выдано сообщение `License OK` либо сообщение об ошибке, и Продукт завершит работу.

Останов

Остановить работу Продукта можно командой:

```
/etc/init.d/l2svc stop
```

либо

```
service l2svc stop.
```


Перезапуск

Для перезапуска демона остановите его и запустите снова, используя описанные выше команды `stop` и `start`. Можно воспользоваться командой:

```
/etc/init.d/l2svc restart
```

или

```
service l2svc restart.
```

Перезапуск отдельных L2-туннелей

При необходимости можно перезапускать отдельные туннели. Для этого нужно узнать PID (идентификатор) процесса используя команду `netstat`.

Пример выполнения команды:

```
$netstat –lpn | grep l2
udp    0    0 0.0.0.0:1194    0.0.0.0:*    16700/l2svc
```

Здесь `0.0.0.0:1194` – локальный ip и port туннеля, `16700` – PID процесса для данного туннеля.

Чтобы перезапустить отдельный туннель нужно выполнить команду:

```
Kill –HUP <PID>,
```

где `<PID>` – PID нужного процесса.

При этом будет заново прочитан конфигурационный файл данного туннеля и произойдёт перестроение соединения. В это время другие туннели продолжают работать.

Информация о текущем состоянии L2-туннеля

Получить информацию о текущем состоянии туннеля можно выполнив команду:

```
/etc/init.d/l2svc status
```

или

```
service l2svc status.
```

По этой команде осуществляется запись текущего состояния созданных соединений (информация о переданных/полученных туннелями байтах и пакетах) в файл:

- Если в конфигурационном файле был задан параметр `status <filename>`, то данные будут записаны в указанный файл.
- Если параметр `status` отсутствует – данные пишутся в файл `/tmp/l2svc_<N>_status`, где N – номер локального порта.
  Если имеется два туннеля, локальные ip-адреса которых отличаются, а локальные порты одинаковы, то при выполнении команды `status` в файл с указанным портом будет записана информация только по одному из них.

Протоколирование

Протоколирование событий происходит по протоколу Syslog. Сообщения от источника (facility) LOG_LOCAL7 направляется в файл cspvpngate.log, что является настройками по умолчанию для «Bel VPN L2 » и Bel VPN Gate.

По умолчанию для Bel VPN L2 задан уровень важности 1, в соответствии с которым протоколируются критические ошибки, информация о старте продукта и построении соединений, а также не критические сетевые ошибки.

При описании параметров L2-туннеля можно указать другой файл для записи логов и изменить уровень протоколирования.

Протоколируемые события

Сообщение	Описание события
Interface <ifname>: starting incoming transfer	Начало передачи пакетов с интерфейса <ifname> в туннель
Interface <ifname>: starting outgoing transfer	Начало передачи пакетов из туннеля на интерфейс <ifname>
l2svc needs cspvpngate running	Не запущен cspvnpgate
Configuration successfully loaded from <filename>	Конфигурация успешно загружена из конфигурационного файла <filename>
Can't load configuration loaded from <filename>	Не получилось загрузить конфигурацию из файла <filename>
No configuration files found. Exiting	В директории /opt/l2svc/etc не найдено файлов с расширением `.conf`, завершение работы
Status written to file specified in "status" parameter of configuration or to /tmp/l2svc_<N>_status if "status" parameter undefined (<N> – local port number)	Информация о статусе туннеля записана в файл, определённый параметром статус конфигурационного файла, либо в /tmp/l2svc_<N>_status, если параметр status не задан
Initialization Sequence Completed	Закончена инициализация и построение туннеля

Информационные сообщения

Сообщение	Описание события
TAP device tap0 opened	Создан виртуальный адаптер tap0
TAP device MAC address set to N	MAC-адрес tap интерфейса выставлен в <N>
Closing TAP interface	Закрытие виртуального интерфейса
Data Channel MTU parms	Параметры MTU туннеля

Сообщение	Описание события
Fragmentation MTU parms	Параметры фрагментации
Local Options String:	Строка опций локального конца туннеля
Expected Remote Options String:	Ожидаемая строка опций удалённого конца туннеля
NOTE: Beginning empirical MTU test -- results should be available in 3 to 4 minutes.	Начинается тестирование MTU, результаты будут доступны через 3-4 минуты
NOTE: Empirical MTU test completed [Tried,Actual] local->remote=[m,n] remote->local=[j,r]	Завершено тестирование MTU. Результаты (попытка/актуальный)
NOTE: This connection is unable to accomodate a UDP packet size of N. Consider using --fragment or --mssfix options as a workaround.	По текущему соединению невозможно передать UDP пакет размера N. Используйте fragment или mssfix, чтобы обойти это ограничение
TAP TX queue length set to N	Очередь отправки пакетов виртуального интерфейса выставлена в N
Peer Connection Initiated with M	Инициировано соединение с удалённым хостом M
Inactivity timeout, restarting	Нет входящих пакетов, перезапуск. Это сообщение возникает, если в конфигурации задан параметр keepalive m n, и в течение n секунд от партнёра не пришло ни одного пакета
WARNING: S is used inconsistently	Опция S имеет различные значения на локальном и удалённом концах туннеля
NOTE: --mute triggered...	Превышен порог протоколирования однотипных сообщений, дальнейшие сообщения не будут записаны в лог

Ошибки в файле конфигурации

Сообщение об ошибке	Описание ошибки
Remote and local addresses are the same	Адреса локального и удалённого компьютеров должны отличаться
WARNING: using --fragment and --mtu_test together may produce an inaccurate MTU test result	Совместное использование параметров fragment и mtu_test может привести к неправильному вычислению значения MTU
Keepalive parameters must be > 0	Цифровые значения параметра keepalive должны быть больше 0

Сообщение об ошибке	Описание ошибки
The second parameter to --keepalive (restart timeout=<N>) must be at least twice the value of the first parameter (ping interval=<M>). Recommended setting is --keepalive 10 60.	Второе число параметра keepalive (таймаут перезапуска) должно быть, как минимум, в два раза больше первого (интервал отсылки пакетов). Рекомендуемое значение – keepalive 10 60
invalid --pmtud type: '%s' -- valid types are 'do', 'dont', or 'want'	Неправильный тип path mtu discovery. Возможные значения: do, don't, want
Only one of pmtud or mtu_test may be defined	Одновременно может быть задан только один из параметров pmtud и mtu_test
Local and nobind don't make sense when used together	Параметры local и nobind не могут применяться вместе
Local_port and nobind don't make sense when used together	Параметры local_port и nobind не могут применяться вместе
Nobind doesn't make sense unless used with remote	При задании параметра nobind также необходимо указать параметр remote
Bad compression option: -- must be 'always' or 'adaptive'	Параметр сжатия задан неверно. Возможные варианты – always или adaptive
Unrecognized option or missing parameter(s):	Задана несуществующая опция либо у опции отсутствует необходимый параметр.
Wrong capture interface name	Интерфейс, указанный как capture, отсутствует в системе
TUN MTU value (N) must be at least 100	Значение tun_mtu (N) должно быть не менее 100 байт

Ошибки, связанные с лицензией на продукт

Сообщение об ошибке	Описание ошибки
l2svc: Error – License file not found	Не удалось найти файл с лицензией
Error – license file has wrong format.	Файл с лицензией имеет неправильный формат
Error – unsupported product code	Неправильное поле “Product Code”
Error – invalid license number	Неправильный формат поля “License Number”
Error – license check failed	Ошибка при проверке лицензии
Error – wrong license	Неправильная лицензия

Ошибки во время выполнения

Сообщение об ошибке	Описание ошибки
FRAG_IN error flags=	Ошибка фрагментации (появляется, как правило, если на одном конце туннеля включена фрагментация, а на другом нет)
Open error on pid file <filename>	Не удалось открыть файл <filename> для записи PID процесса
External program exited with error status:	При выполнении скрипта up/down произошла ошибка. (как правило, это свидетельствует о проблемах с мостом (bridge))
UDP: Cannot create UDP socket	Не удалось создать UDP-сокет
Socket bind failed on local address	Не удалось задать сокету адрес и порт. Возможно, они уже используются
UDP: Incoming packet rejected from M[N], expected peer address: F	Входящий UDP-пакет с адреса M порта N удалён. Ожидался пакет с адреса F. Данная ошибка означает, что в локальной конфигурации задан параметр remote, и пришедший пакет отправлен с иного адреса

