ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный продукт «С-Терра L2». Версия 3.11

Руководство администратора

РЛКЕ.00005-02 90 03

15.06.2015

Содержание

Лицензионное Соглашение

о праве пользования Продуктом «С-Терра L2» производства ООО «С-Терра СиЭсПи»

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного Продукта «С-Терра L2» (далее – Изделия) Конечным Пользователем (физическим или юридическим лицом). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Изделием.

Под Изделием понимается комплекс материальных объектов (программных и, при наличии, аппаратных средств, носителей информации, кода программных продуктов, документации в печатной и электронной формах), состав которых определяется артикулом из прайс-листа ООО «С-Терра СиЭсПи».

Изделие 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.

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

Изделие и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Российской Федерации об авторском и имущественном праве на объекты интеллектуальной собственности.

Установка Изделия 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. 433 ГК РФ имеет силу договора между Конечным Пользователем и Производителем Изделия (ООО «С-Терра СиЭсПи»).

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 Изделия. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Изделия только в составе работ, связанных с эксплуатацией Изделия. 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 Изделия, и не имеет права хранить, устанавливать, использовать большее количество экземпляров Изделия.

Конечный Пользователь не имеет права распространять Изделие в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Изделия 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 Изделия, вносить какие-либо изменения в бинарный код программ и совершать относительно Изделия другие действия, нарушающие Российские и международные нормы по авторскому праву и использованию программных средств.

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

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" 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 Изделия Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ООО «С-Терра СиЭсПи») обеспечивает:

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

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

Примечание 1. Гарантийное обязательство 2 базируется на следующем определении: Критичная Проблема заключается в том, что Изделие, 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 Изделия дефекты в составе информационных носителей или некомплектность Изделия, то информационные носители будут заменены, а комплектность Изделия 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 Изделия любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Изделия и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Ввиду того, что Изделие 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 Изделия, 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 Изделия)
- 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 Изделия и трактуется Производителем Изделия как основание для отказа Конечному Пользователю в сервисе технического сопровождения и поддержки Изделия.

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

Настоящее Лицензионное Соглашение (в рамках законодательства Российской Федерации 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 Изделия и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Изделия.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Изделия 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 Изделия, включая информацию на внутренних носителях Изделия. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Ядро операционной системы Linux является свободно распространяемым Продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (http://www.kernel.org/pub/linux/kernel/COPYING).

Другие названия компаний и продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Изделия 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. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих продуктов.

Напечатано в Российской Федерации

Общество с ограниченной ответственностью «С-Терра СиЭсПи»

124498, г. Москва, Зеленоград, Георгиевский проспект, дом 5, помещение I, комната 33

Телефон: +7 (499) 940 9061

Факс: +7 (499) 940 9061

Эл.почта: information@s-terra.com

http://www.s-terra.com

Комплект поставки Продукта

Продукт «С-Терра L2» поставляется только в составе программно-аппаратного комплекса (ПАК) CSP VPN Gate, работающего под управлением операционных систем: Crossbeam Systems Linux 9, Red Hat Enterprise Linux 5 или CentOS 5 в следующей комплектации:

- жесткий диск ПАК или компакт-флеш карта содержат:
  - установленную ОС Crossbeam Systems Linux 9/Red Hat Enterprise Linux 5/CentOS 5.
  - подготовленный к инициализации Продукт CSP VPN Gate (типовая поставка CSP VPN Gate)
  - установленный дистрибутив Продукта «С-Терра L2»
- компакт-диск, который содержит:
  - дистрибутив Продукта «С-Терра L2» – sterra_l2-3.11-xxxxx.i686.rpm
- компакт-диск с документацией.

Требования на базовые платформы и совместимость

Продукт «С-Терра L2» работает на ПАК под управлением операционных систем:

- Crossbeam Systems Linux 9
- Red Hat Enterprise Linux 5
- CentOS 5.

«С-Терра L2» является самостоятельным Продуктом, но работает только в комплексе с CSP VPN Gate, который используется для защиты передаваемого трафика.

Назначение и функции Продукта

Продукт «С-Терра L2» предназначен:

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

Продукт «С-Терра 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 продукт CSP VPN Gate – выполняется IPsec-инкапсуляция (VPN-туннель).

Программно Продукт «С-Терра L2» реализован как usermode-демон – l2svc. Используя драйвер TUN/TAP, для каждого L2-туннеля на шлюзе безопасности 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. Продукт CSP VPN Gate, установленный на этом же шлюзе, 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.com/ в разделе «Решения – Типовые сценарии применения продуктов S-Terra».

Инсталляция Продукта

Программный Продукт «С-Терра L2» поставляется предварительно инсталлированным.

Перед запуском Продукта необходимо создать файл с лицензией и конфигурационный файл с настройками.

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

Описание конфигурационного файла приведено в разделе «Настройка Продукта».

Создание лицензионного файла описано ниже, в соответствующем подразделе.

Если появится необходимость инсталлировать Продукт с дистрибутива «С-Терра L2», то выполняется это следующим образом:

1. Разместите на шлюзе.необходимые пакеты: `lzo-2.06-1.el5.rf.i386.rpm`, `bridge-utils-1.1-3.el5.i386.rpm` и файл дистрибутива sterra_`l2-3.11-xxxxx.i686.rpm`
2. Установите пакеты командой:

```
rpm –i lzo-2.06-1.el5.rf.i386.rpm
rpm –i bridge-utils-1.1-3.el5.i386.rpm
rpm –i sterra_l2-3.11-xxxxx.i686.rpm.
```

Создание лицензионного файла

Для нормальной работы Продукта необходимо создать файл с лицензией `l2.lic` в директории `/opt/l2svc/etc`. При запуске Продукта 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 `/opt/l2svc/bin/license.sh` ввести значения запрашиваемых полей.

При запуске скрипта, проверяется наличие уже существующего файла с лицензией. В случае обнаружения файла, пользователь может его использовать 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.

Деинсталляция Продукта

Деинсталляция Продукта осуществляется запуском команды:

```
rpm –e sterra_l2-3.11-xxxxx.i686.rpm
```

Настройка Продукта

Перед запуском Продукт надо настроить. Настройка Продукта 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`. Там же можно посмотреть пример конфигурационного файла – `sample_conf.txt`.

Для каждого создаваемого туннеля нужно 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 Продукт на всех интерфейсах ПАК, поскольку хотя бы один интерфейс необходим для передачи трафика на удаленный шлюз безопасности (WAN-интерфейс).

Настройки «C-Терра L2» считываются из конфигурационного файла при запуске Продукта, 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;
- *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, а именно – mtu следующих интерфейсов: capture-интерфейса, виртуального tap-интерфейса (vif) и виртуального интерфейса моста (bridge). Значение по-умолчанию – 1500.
- *mssfix [n]* – при включении данной опции поле MSS всех проходящих через туннель tcp-пакетов будет выставлено в *n*. 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 – 1400;
- *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 CSP VPN Gate

При совместной работе с CSP VPN Gate в политике безопасности должны быть указаны правила шифрования UDP-трафика, проходящего по туннелю, а также правила, запрещающие поступление UDP-пакетов на внешний интерфейс шлюза с остальных хостов WAN.

Запуск и останов «C-Терра L2»

Запуск Продукта

Для запуска программного продукта «C-Терра L2» следует выполнить команду:

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

или

```
service l2svc start.
```

При запуске демона `l2svc` на консоль выдается сообщение о версии Продукта.

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 Продукта, 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 Продукта

Остановить работу Продукта можно командой:

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

либо

```
service l2svc stop.
```


Перезапуск Продукта

Для перезапуска демона остановите его и запустите снова:

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

или

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

Можно воспользоваться командой:

```
service l2svc restart.
```

Перезапуск отдельных 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 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 «С-Терра L2» и CSP VPN Gate.

По умолчанию для С-Терра 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	Ракрытие виртуального интерфейса

Сообщение	Описание события
Data Channel MTU parms	Параметры MTU туннеля
Fragmentation MTU parms	Параметры фрагментации
Local Options String:	Строка опций локального конца туннеля
Expected Remote Options String:	Ожидаемая строка опций удалённого конца туннеля
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
Keepalive parameters must be > 0	Цифровые значения параметра keepalive должны быть больше 0
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
Bad compression option: -- must be 'always' or 'adaptive'	Параметр сжатия задан неверно. Возможные варианты – always или adaptive

Сообщение об ошибке	Описание ошибки
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

Сообщение об ошибке	Описание ошибки
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.

Пример построения L2-туннеля между двумя сегментами сети, защищенными шлюзами безопасности CSP VPN Gate

Описание стенда

Пример представляет собой простую конфигурацию (Рисунок 1). Два сегмента одной сети (SN1 – 192.168.1.0/24). объединяются в общую сеть туннелем L2. В качестве защиты туннеля используется VPN соединение между шлюзами безопасности CSP VPN Gate. L2-туннель полностью прозрачен для всех протоколов сетевого уровня и выше, а также для VLAN и Spanning Tree протоколов.

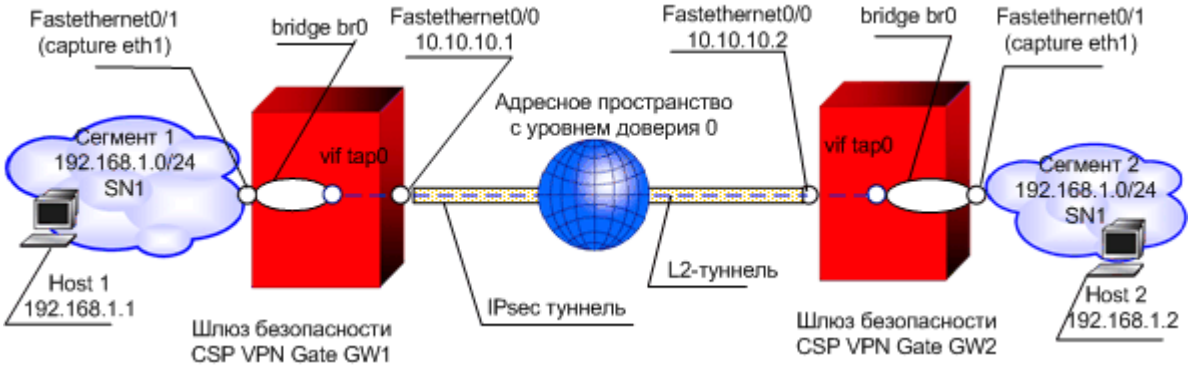

Рисунок 1

Рассмотрим работу S-Terra L2 на примере трафика, идущего от Host 1 к Host 2. На шлюзе GW1 запущен процесс l2svc, который захватывает фреймы канального уровня, приходящие на интерфейс Fa0/1, и инкапсулирует их в пакеты сетевого уровня. Далее они попадают под правила шифрования и передаются по IPsec туннелю между шлюзами GW1 и GW2. На GW2 происходит обратный процесс.

Так как шифруемые пакеты имеют в качестве source и destination адресов внешние адреса шлюзов, то в настройках рекомендуется использовать транспортный режим для уменьшения накладных расходов.

Нужно отметить, что между шлюзами безопасности GW1 и GW2 могут находиться устройства 3 уровня (маршрутизаторы, межсетевые экраны и др.), то есть они не обязаны быть связаны на канальном уровне.

Параметры защищенного соединения:

- Аутентификация на сертификатах.
- IKE parameters:
  - Encryption algorithm – GOST 28147-89;
  - Hash algorithm – GOST R 34.11-94 Hash;
  - DH-group – VKO GOST R 34.10-2001.
- IPsec parameters:
  - ESP encryption algorithm – GOST 28147-89;
  - ESP integrity algorithm – GOST R 34.11-94 HMAC.

Настройка GW1

В политику безопасности шлюза GW1 должно быть записано правило шифрования трафика для L2-туннеля со шлюзом GW2. Полученная cisco-like конфигурация будет иметь вид:

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
hostname gw1
enable password csp
!
!
crypto isakmp policy 1
 hash md5
 encr des
 group vko
!
crypto ipsec transform-set TSET esp-des esp-md5-hmac
 mode transport
!
ip access-list extended LIST
 permit udp host 10.10.10.1 host 10.10.10.2
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set TSET
 set pfs vko
 set peer 10.10.10.2
!
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 crypto map CMAP
!
!
crypto pki trustpoint s-terra_technological_trustpoint
```

```
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 14AF87E16ECB8E924BE0D08040A72273
308202BB30820268A003020102021014AF87E16ECB8E924BE0D08040A7227330
…
521B572D2503E017E236A13D3AA0BD9A49494E3132840B52182260B2E0C072

quit
!
End
```

Настройка GW2

Аналогично настраивается шлюз безопасности GW2. Cisco-like конфигурация будет иметь вид:

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
hostname gw2
enable password csp
!
!
crypto isakmp policy 1
 hash md5
 encr des
 group vko
!
crypto ipsec transform-set TSET esp-des esp-md5-hmac
 mode transport
!
ip access-list extended LIST
 permit udp host 10.10.10.2 host 10.10.10.1
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set TSET
```

```
 set pfs vko
 set peer 10.10.10.1
!
!
interface FastEthernet0/0
 ip address 10.10.10.2 255.255.255.0
 crypto map CMAP
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 14AF87E16ECB8E924BE0D08040A72273
308202BB30820268A003020102021014AF87E16ECB8E924BE0D08040A7227330
…
521B572D2503E017E236A13D3AA0BD9A49494E3132840B52182260B2E0C072

quit
!
End
```

Настройка L2-туннелей

Для настройки L2-туннеля необходимо описать его параметры в конфигурационных файлах на шлюзах GW1 и GW2. Создайте в каталоге `/opt/l2svc/etc/` обоих шлюзов текстовый конфигурационный файл `config.conf`.

Пример конфигурационного файла `config.conf` для шлюза GW1:

```
vif tap0
bridge br0
capture eth1
remote 10.10.10.2
fragment 1430
mssfix
passtos
```

Пример конфигурационного файла `config.conf` для шлюза GW2:

```
vif tap0
bridge br0
capture eth1
remote 10.10.10.1
```



```
fragment 1430
mssfix
passtos
```

После создания конфигурационных файлов на шлюзах следует запустить «С-Терра L2»:

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

Проверка работоспособности стенда

После того, как настройка GW1 и GW2 завершена, инициируем создание L2-туннеля и защищенного соединения.

На Host1 выполним команду:

```
ping 192.168.1.2
```

Вывод утилиты ping должна говорить о том, что пакеты между Host1 и Host2 успешно передаются.

В результате выполнения этой команды между устройствами GW1 и GW2 будет установлен L2-туннель, защищенный VPN-туннелем.

В этом можно убедиться, выполнив на устройстве GW1 команду:

```
gw1#/opt/VPNagent/bin/sa_mgr show
```