

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



Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Программный продукт «С-Терра L2»

РЛКЕ.00009-01 90 03

22.06.2015

Содержание

Требования на базовые платформы и совместимость	3
Назначение и функции Продукта	4
Инсталляция Продукта	5
Создание лицензионного файла	5
Деинсталляция Продукта	6
Настройка Продукта	7
Настройка L2-туннелей	7
Настройка S-Terra Gate	10
Запуск и останов «С-Терра L2»	11
Запуск Продукта	11
Запуск Продукта, с указанием параметров	11
Останов Продукта	11
Перезапуск Продукта	12
Перезапуск отдельных туннелей	12
Информация о текущем состоянии туннеля	13
Протоколирование	14
Протоколируемые события	14
Информационные сообщения	14
Ошибки в файле конфигурации	15
Ошибки, связанные с лицензией на продукт	16
Ошибки во время выполнения	16

Требования на базовые платформы и совместимость

Продукт «С-Терра L2» работает под управлением операционной системы Debian GNU/Linux 6.

«С-Терра L2» является самостоятельным Продуктом, но работает только совместно с продуктом «Программный комплекс С-Терра Шлюз. Версия 4.1», который используется для защиты передаваемого трафика.

Продукт «С-Терра L2» поставляется только в составе «Программного комплекса С-Терра Шлюз. Версия 4.1».

Далее продукт «Программный комплекс С-Терра Шлюз. Версия 4.1» будем называть S-Terra Gate или С-Терра Шлюз.

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 С-Терра Шлюз – 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 создается 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 S-Terra 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 идет 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.

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 потребуются заново ввести лицензионную информацию.

Деинсталляция Продукта

Деинсталляция Продукта осуществляется запуском команды:

ОС Debian GNU/Linux 6 (i686)

```
dpkg -r sterra_12_4.1.xxxxx.i386.deb
```

ОС Debian GNU/Linux 6 (amd64)

```
dpkg -r sterra_12_4.1.xxxxx.amd64.deb
```

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 «С-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.

Оptionальные параметры

- `local <host>` – ip-адрес или символьное имя локального хоста.
- `remote <host> [port]` – ip-адрес или символьное имя и порт удаленного хоста.
- `port <port>` – номер используемого UDP-порта, используемый и для локального и для удаленного 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 I2-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 хеширования *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
```
- *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 udr-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] [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 *istr*. 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 исказить 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 перезачитываются не будут). Так как происходит 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 S-Terra Gate

При совместной работе с S-Terra 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 «С-Терра L2»

Запуск Продукта

Для запуска программного продукта «С-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, используя описанные выше команды `stop` и `start`. Можно воспользоваться командой:

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

или

```
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 -ltn | 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 направляются в файл cspvpngate.log, что является настройками по умолчанию для «C-Terra L2» и S-Terra Gate.

По умолчанию для C-Terra 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 cspvpngate
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	Заккрытие 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 keepralive 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 keepralive 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 keepralive (таймаут перезапуска) должно быть, как минимум, в два раза больше первого (интервал отсылки пакетов). Рекомендуемое значение – keepralive 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-сокеты
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