ЗАО «С-Терра СиЭсПи»
124460, г. Москва, Зеленоград, проезд 4806, д.6, этаж 4-й
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com

Сайт: http://www.s-terra.com

Программный Продукт CSP L2VPN Gate Версия 1.2

Руководство администратора

11.02.2011

Содержание

Лицензионное Соглашение

о праве пользования Продуктом CSP L2VPN Gate производства ЗАО «С-Терра СиЭсПи»

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного Продукта CSP L2VPN Gate (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 ЗАО «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 (ЗАО «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 (ЗАО «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.

Sun Solaris и Java являются торговыми марками компании Sun Microsystems, Inc в США и в других странах.

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. ЗАО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих продуктов.

Напечатано в Российской Федерации

Закрытое Акционерное Общество «С-Терра СиЭсПи»

124460, г. Москва, Зеленоград, проезд 4806, д.6, этаж 4-й

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 CSP L2VPN Gate поставляется только в составе программно-аппаратного комплекса (ПАК) CSP L2VPN Gate, работающего под управлением ОС Sun Solaris 10, в следующей комплектации:

- жесткий диск ПАК или компакт-флеш карта содержат:
  - установленную ОС Sun Solaris 10
  - подготовленный к инсталляции дистрибутив CSP VPN Gate (типовая поставка CSP VPN Gate)
  - установленный дистрибутив Продукта CSP L2VPN Gate версии 1.2
- компакт-диск, который содержит:
  - дистрибутив Продукта CSP L2VPN Gate – `l2vpn.pkg`
- компакт-диск с документацией
- в печатном виде поставляется:
  - Приложение с описанием отличительных особенностей использования сетевых адаптеров ПАК (если такие особенности имеются).

Требования на базовые платформы и совместимость

Продукт CSP L2VPN Gate работает на ПАК под управлением операционной системы Sun Solaris 10.

Все поставляемые ПАК CSP L2VPN Gate комплектуются сетевыми адаптерами и драйверами, удовлетворяющими требованиям по совместимости с программным обеспечением CSP L2VPN Gate. Если существуют отличия в функционировании и использовании сетевых адаптеров, присущие конкретным ПАК, то в комплект поставки входит Приложении в печатном виде, где указываются внутренние интерфейсы, которые могут контролироваться Продуктом CSP L2VPN Gate, и внешние, контролируемые CSP VPN Gate.

На аппаратной платформе каждый разъем интерфейса, который является внутренним, может быть помечен шильдиком со следующей надписью: “Порты A и/или B использовать только для внутренних (inner) L2VPN подключений”.

Если Приложение поставляется , то строго следуйте указаниям, изложенным в нем для вашей аппаратной платформы.

CSP L2VPN Gate является самостоятельным Продуктом, но для защиты передаваемого трафика может использоваться продукт CSP VPN Gate.

Назначение и функции Продукта

Продукт CSP L2VPN Gate 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 CSP L2VPN Gate 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 L2VPN-туннель). А для защиты UDP-трафика используется продукт CSP VPN Gate – выполняется IPsec-инкапсуляция (VPN-туннель).

Настройка Продукта и туннелей производится в конфигурационном файле `/etc/l2vpn.conf`.

Программно Продукт реализован как модуль-драйвер ядра (`l2gate`), работающий под управлением демона (`l2vpn`).

На Рисунке 1 представлен пример использования Продукта. В каждой ЛВС выделены два сегмента, которые попарно связываются между собой. На шлюзах безопасности GW1 и GW2 указаны интерфейсы, трафик на которых обрабатывает Продукт CSP L2VPN Gate (здесь и далее они понимаются как внутренние). Этими интерфейсами ПАК подключается к соответствующим сегментам объединяемых ЛВС. На шлюзе GW1 Продукт принимает любые Ethernet-кадры на внутреннем интерфейсе, инкапсулирует их в UDP-пакеты, а продукт CSP VPN Gate, установленный на этом же шлюзе, при необходимости создает IPsec-туннель и передает данные в удаленную сеть на шлюз назначения GW2. На GW2 производится сначала IPsec-декапсуляция, а затем – UDP-декапсуляция и полученные Ethernet-кадры испускаются в сеть назначения через внутренний интерфейс GW2. Встречный трафик между сетями идёт аналогичным образом от GW2 к GW1.

Для обработки Продуктом захватываются все Ethernet-фреймы, доступные на внутреннем интерфейсе в режиме прослушивания (promiscuous mode).

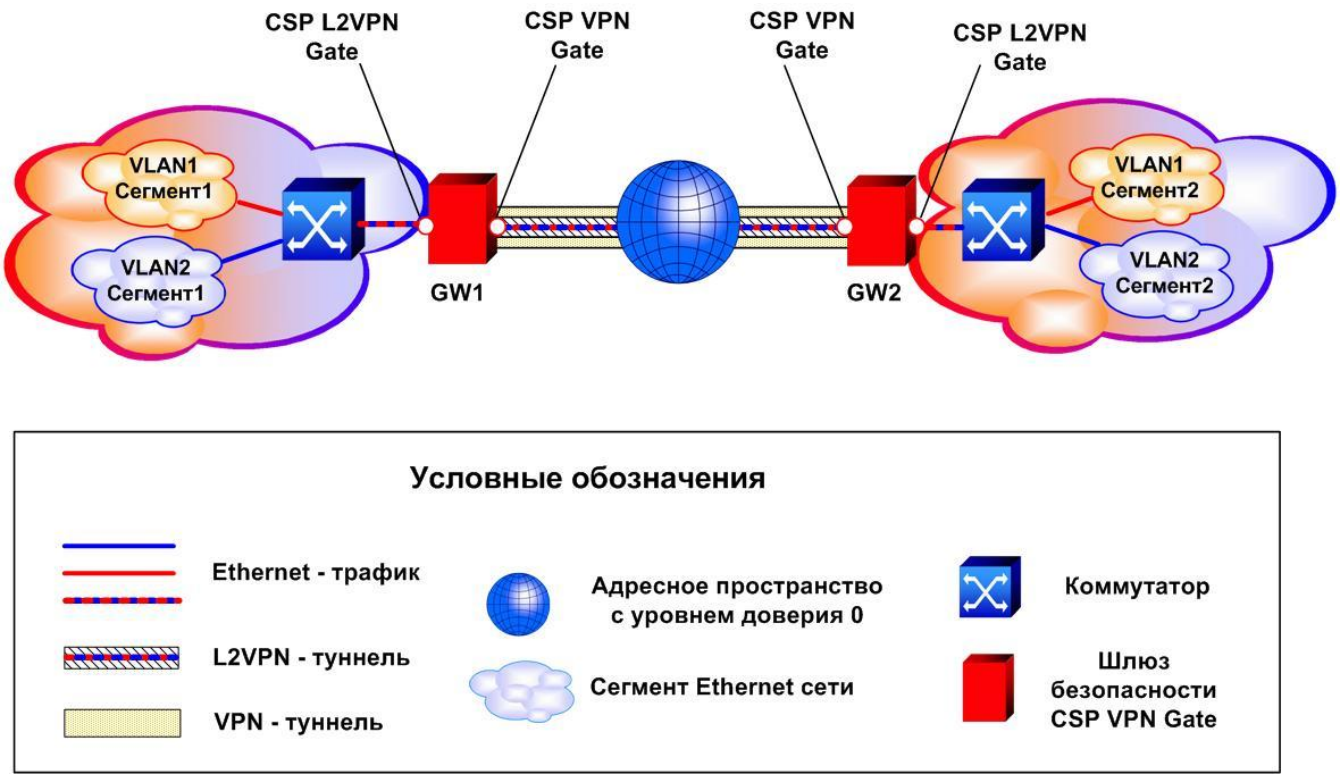

Рисунок 1

Инсталляция Продукта

Программный Продукт CSP L2VPN Gate поставляется предварительно инсталлированным.

В процессе инсталляции Продукта созданы каталоги, в которых размещаются необходимые для работы Продукта файлы:

- исполняемый файл (демон) – `/opt/l2vpn/l2vpn`
- исполняемый файл (драйвер) – `/kernel/drv/l2gate` и ссылка на него в `/kernel/strmod`
- файл конфигурации – `/etc/l2vpn.conf`
- файл конфигурации драйвера с установленными настройками – `/kernel/drv/l2gate.conf`
- скрипт запуска Продукта – `/etc/init.d/l2vpnd`.

Продукт CSP L2VPN Gate поставляется с пустым конфигурационным файлом и запустить его невозможно. Поэтому перейдите к настройке конфигурационного файла, описанного в разделе “Настройка Продукта”.

Если появится необходимость инсталлировать Продукт с дистрибутива CSP L2VPN Gate, то выполняется это следующим образом:

1. разместите файл дистрибутива `l2vpn.pkg` в каталог `/opt`
2. запустите инсталляцию Продукта командой:

```
pkgadd –d /opt/l2vpn.pkg
```

В процессе выполнения команды администратору будут заданы два вопроса для подтверждения инсталляции:

> “`Select package(s) you wish to process (or ‘all’ to process all packages). (default: all) [?,??,q]:`” – выберите ответ по умолчанию, т.е. нажмите Enter.
>
> “`This package contains scripts which will be executed with super-user permission during the process of installing this package. Do you want to continue with the installation of <L2VPN> [y,n,?]`” – При отрицательном ответе инсталляция будет прервана, а при положительном [`y`, Enter] - инсталляция будет продолжена.

Если инсталляция Продукта завершилась успешно, то выдается сообщение: `"Installation of <L2VPN> was successfull"`.

Деинсталляция Продукта

Деинсталляция Продукта осуществляется запуском команды:

```
pkgrm L2VPN
```

В процессе выполнения команды будут заданы два вопроса для подтверждения удаления Продукта, на которые надо ответить утвердительно и нажать Enter:

```
Do you want to remove this package? [y,n,?,q]
```

```
This package contains scripts which will be executed with super-user
permission during the process of removing this package.
Do you want to continue with the removal of this  package [y,n,?,q].
```

Настройка Продукта

Настройка Продукта производится в конфигурационном файле `/etc/l2vpn.conf`.

Рекомендуется не использовать Продукт на всех интерфейсах ПАК, поскольку хотя бы один интерфейс необходим для передачи трафика на удаленный шлюз безопасности (WAN-интерфейс).

Настройки Продукта и L2VPN-туннелей считываются из конфигурационного файла при запуске Продукта, поэтому после внесения изменений следует перезапустить демон или операционную систему (при этом демон запустится автоматически).

Файл конфигурации драйвера l2gate.conf

Файл `/kernel/drv/l2gate.conf` предназначен для настройки драйвера Продукта и содержит следующие параметры:

```
name="l2gate" parent="pseudo" instance=0;
ddi-forceattach=1;
bandwidth=<значение>;
```

Параметры в первых двух строчках являются обязательными для корректного запуска Продукта, изменять их запрещено.

Параметр `bandwidth` является опциональным и задает максимально допустимое количество активных хостов в локальной сети. Его значение по умолчанию равно 2048.

При появлении в файле лога ошибки "Error: packet dropped - filter overflow", рекомендуется изменить значение параметра `bandwidth`. Изменения вступят в силу после перезагрузки системы.

Файл конфигурации l2vpn.conf

В файле конфигурации `/etc/l2vpn.conf` описываются L2VPN-туннели, которые должны быть созданы, и общие параметры Продукта.

Текст в файле конфигурации, начинающийся с "#" и до конца строки считается комментарием и игнорируется Продуктом.

Как настроить туннели описано в разделе "Настройка L2VPN-туннелей".

Настройка общих параметров Продукта описана в разделе "Изменение порта".

Настройка L2VPN-туннелей

Описание каждого туннеля начинается со слова"`tunnel`" и состоит из набора параметров, заключенных в круглые скобки:

```
tunnel (
        <параметры>
)
```

Параметры туннеля:

- имя Ethernet интерфейса, на котором происходит перехват пакетов
- параметры UDP-соединения, по которому данные передаются по туннелю.

Обозначения параметров:

`interface` – имя физического интерфейса (указывается в кавычках)

`local_ip` – локальный IP-адрес UDP-соединения

`local_port` – локальный порт соединения

`remote_ip` – удаленный IP-адрес UDP-соединения

`remote_port` – удаленный порт соединения.

Все параметры, кроме номеров портов, должны присутствовать в описании каждого туннеля. Если порт не указан, то используется значение по умолчанию.

Параметры, описывающие туннель, должны быть уникальны, т.е. их значения не должны использоваться при описании других туннелей (IP-адрес и соответствующий порт рассматриваются как один составной параметр). В частности, одному интерфейсу может быть приписан только один туннель.

Примечание: на ответном шлюзе тоже должен быть описан соответствующий туннель.

Пример описания туннеля:

```
tunnel (
        interface = ”eth0”
        local_ip = 192.168.0.11
        local_port = 1770
        remote_ip = 192.168.0.22
        )
```

Изменение порта

По умолчанию для всех L2VPN-туннелей используется порт 1701 (порт протокола L2TP), который можно не указывать в описаниях туннелей. Но если требуется его изменить для всех туннелей одновременно, то внесите соответствующий блок в файл конфигурации, например,

```
defaults (
        def_port = 1333
)
```

Отладочный режим

После внесения изменений в файл конфигурации рекомендуется сначала запустить демона в отладочном режиме, чтобы убедиться в отсутствии ошибок:

```
cd /opt/l2vpn
./l2vpn -d
```

В отладочном режиме все сообщения об ошибках в ходе работы выдаются на консоль. При некоторых ошибках Продукт останавливает свою работу, а при других – продолжает.

Для прекращения работы Продукта в этом режиме нажмите комбинацию клавиш ”Ctrl-C”.

Настройка сетевой карты

Интерфейс, на котором происходит перехват пакетов, должен пропускать все Ethernet-фреймы размером на 4 байта больше, чем максимальный размер фреймов в локальной сети (1500 байт). Это необходимо для передачи тега VLAN в заголовке фрейма. Для этого интерфейса рекомендуется выполнить настройки сетевой карты в следующей последовательности:

- включить Jumbo-фреймы в драйвере сетевой карты
- увеличить значение MTU, выполнив команду ОС:

  `ifconfig <interface> mtu <value>`.

Запуск CSP L2VPN Gate

Для запуска программного продукта CSP L2VPN Gate с настройками из штатного файла конфигурации следует выполнить команду:

```
/etc/init.d/l2vpnd start
```

Эта же команда выполняется автоматически при запуске операционной системы.

Если, настройки записаны в альтернативный файл конфигурации, например `/etc/l2vpn_alt.conf`, выполните команды:

```
cd /opt/l2vpn
./l2vpn /etc/l2vpn_alt.conf
```

При запуске демона `l2vpn` на консоль выдается сообщение:

```
L2VPN Gate v.1.2 (build 10490)
Copyright S-Terra CSP 2003-2010
```

Запуск одновременно двух и более копий Продукта невозможен. При попытке запуска – второй процесс немедленно завершится.

В случае запуска CSP L2VPN Gate без предварительной настройки, в файл протоколирования будет выдано сообщение – “empty configuration file” или “empty input file”, после чего процесс завершится.

Для просмотра версии Продукта и номера сборки следует запустить демон с опцией `-v`:

```
/opt/l2vpn/l2vpn -v
```

При этом будет выдано на консоль сообщение:

```
L2VPN Gate v.1.2 (build 10490)
Copyright S-Terra CSP 2003-2010
```

и данная копия Продукта завершит свою работу.

Остановить работу Продукта можно командой:

```
/etc/init.d/l2vpnd stop
```

Для перезапуска демона остановите его и запустите снова:

```
/etc/init.d/l2vpnd stop
/etc/init.d/l2vpnd start
```

Перезапуск демона используется в следующих случаях:

- после изменения конфигурационного файла
- для устранения установленных соединений с партнерами, после запуска они восстанавливаются вновь
- во внештатных ситуациях – зависание демона и др.

Протоколирование событий

Настройка Syslog-клиента

Протоколирование событий происходит только по протоколу Syslog.

В Продукте Syslog-клиент настроен следующим образом:

- источником сообщений для протоколируемых событий является ядро (`kern`) и демон (`daemon`)
- уровни важности протоколируемых событий – `error, notice и warning.`

Изменить настройки Syslog-клиента нельзя.

Настройка локального Syslog-сервера

Настройте самостоятельно Syslog-сервер, например, локальный, используя стандартный системный файл `/etc/syslog.conf`:

например, для сохранения информации в файл `/var/l2vpn/message_kern`, пришедшей от источника `kern` и имеющей уровни важности `error` и выше, добавьте строку (поля разделяются символами табуляции):

```
kern.error    /var/l2vpn/message_kern
```

После изменения файла `/etc/syslog.conf` произведите рестарт syslog:

```
svcadm disable system-log
svcadm enable system-log
```

Сообщения уровня notice

Сообщение	Описание события
L2VPN Gate started	Запуск Продукта
L2VPN Gate stopped	Остановка Продукта
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>

Сообщения об ошибках

Все сообщения об ошибках передаются в настроенный файл лога.

В отладочном режиме сообщения выдаются только на консоль.

При появлении внутренних ошибок (Internal error) обращайтесь в службу поддержки по адресу support@s-terra.com.

Ошибки в файле конфигурации

Сообщение об ошибке	Описание ошибки
L2VPN: failed to open config file!	Не удалось открыть файл конфигурации (/etc/l2vpn.conf)
L2VPN config error: empty configuration file	В файле конфигурации не задан ни один туннель
L2VPN config error: line: <number>: empty input file	В файле конфигурации нет данных
L2VPN config error: line: <number>:	Ошибка в строке <number>. Сопровождается кратким описанием ошибки
L2VPN config error: too many tunnels	Задано слишком большое количество туннелей
L2VPN config error: tunnel: <number> parameter duplicated	В описании туннеля с порядковым номером <number> значение одного из параметров уже используется в другом туннеле

Ошибки во время работы Продукта

Сообщение об ошибке	Описание ошибки
Invalid interface name <name>	Некорректное имя Ethernet-интерфейса
Failed to open interface <name>	Не удалось подключиться к Ethernet-интерфейсу
Error: packet dropped - filter overflow	Пакет уничтожается, переполнение внутренних списков MAC-адресов в сети.

Внутренние ошибки

Сообщение об ошибке	Описание ошибки
Internal error: open socket	Не удалось создать UDP сокет
Internal error: socket bind	Не удалось связать сокет с локальным IP-адресом. Причиной ошибки “socket bind” может быть наличие уже подключенного к этому IP-адресу и порту UDP сокета
Internal error: open command interface	Не удалось установить связь демона с драйвером
Internal error: ioctl	Ошибка при обмене данными между демоном и драйвером
Internal error: start l2gate	Драйвер не смог подключиться к сетевому интерфейсу
Internal error:start l2gsock	Драйвер не смог подключиться к сокету
Internal error: memory allocation	Ошибка выделения памяти

Пример построения L2VPN-туннеля между двумя сегментами сети, защищенными шлюзами безопасности CSP VPN Gate

Описание стенда

Пример представляет собой простую конфигурацию (Рисунок 2) – два сегмента Ethernet сети (SN1 и SN2) объединяются в общую сеть туннелем L2VPN. В качестве защиты туннеля используется VPN соединение между шлюзами безопасности CSP VPN Gate. L2VPN-туннель полностью прозрачен для всех протоколов сетевого уровня и выше, а также для VLAN и Spanning Tree протоколов. Весь обмен данными в сегменте SN1 виден в сегменте SN2 и наоборот – пакеты, проходящие в сегменте SN2 видны в сегменте SN1.

Объединяемые сегменты SN1 и SN2 принадлежат к адресному пространству одной IP-сети - 192.168.103.0/24. В случае, если сегменты принадлежат к разным сетям, между ними должна быть настроена маршрутизация, как если бы они находились в одном сегменте.

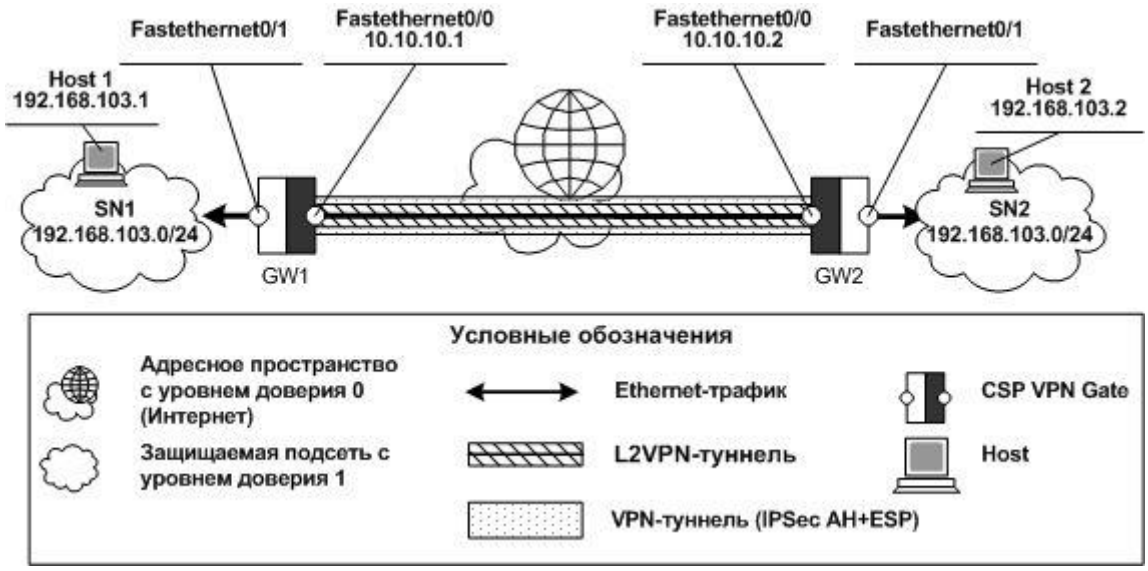

Рисунок 2

Параметры VPN - туннеля:

- Аутентификация на Preshared Key.
- IKE parameters:
  - Encryption algorithm – GOST
  - Hash algorithm – GOST
  - DH-group – group2 (1024)
- IPsec parameters:
  - ESP encryption algorithm – GOST
  - AH integrity algorithm – GOST

Настройка GW1

В политику безопасности шлюза GW1 должно быть записано правило шифрования UDP-трафика для L2VPN-туннеля со шлюзом GW2 (используется порт по умолчанию `1701`). Полученная cisco-like конфигурация будет иметь вид:

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons privilege 15 password 0 csp
hostname cspgate
enable password csp
!
!
!
!
!
crypto isakmp policy 1
 hash md5
 encr des
 authentication pre-share
 group 1
!
crypto isakmp key 12345 address 10.10.10.2
!
crypto ipsec transform-set tr ah-md5-hmac esp-des esp-md5-
hmac
!
ip access-list extended crypto_acl
 permit udp host 10.10.10.1 eq 1701 host 10.10.10.2 eq 1701
!
ip access-list extended filter_acl
 permit udp host 10.10.10.2 eq 1701 host 10.10.10.1 eq 1701
!
!
crypto map cm 1 ipsec-isakmp
 match address crypto_acl
 set transform-set tr
 set peer 10.10.10.2
!
!
!
interface FastEthernet0/0
```

```
 ip address 10.10.10.1 255.255.255.0
 ip access-group filter_acl in
 crypto map cm
!
!
!
end
```

Настройка GW2

Аналогично настраивается шлюз безопасности GW2. В политику безопасности шлюза должно быть записано правило шифрования UDP-трафика, передающего данные L2VPN-туннеля на порт 1701 (порт по умолчанию L2VPN) шлюза GW1. Полученная cisco-like конфигурация будет иметь вид:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons privilege 15 password 0 csp
hostname cspgate
enable password csp
!
!
!
!
!
crypto isakmp policy 1
 hash md5
 encr des
 authentication pre-share
 group 1
!
crypto isakmp key 12345 address 10.10.10.1
!
crypto ipsec transform-set tr ah-md5-hmac esp-des esp-md5-
hmac
!
ip access-list extended crypto_acl
 permit udp host 10.10.10.2 eq 1701 host 10.10.10.1 eq 1701
!
ip access-list extended filter_acl
 permit udp host 10.10.10.1 eq 1701 host 10.10.10.2 eq 1701
!
!
crypto map cm 1 ipsec-isakmp
 match address crypto_acl
 set transform-set tr
 set peer 10.10.10.1
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.2 255.255.255.0
 ip access-group filter_acl in
 crypto map cm
```



```
!
!
!
end
```

Настройка L2VPN туннелей

Для создания L2VPN-туннеля следует внести его параметры в файлы конфигурации `/etc/l2vpn.conf` на шлюзах GW1 и GW2. В эти файлы в текстовом редакторе записываются IP-адреса защищенного соединения и имя интерфейса, на котором выполняется перехват пакетов:

на шлюзе GW1:

```
tunnel  (
   interface = "e1000g1"
   local_ip = 10.10.10.1
   remote_ip = 10.10.10.2
)
```

на шлюзе GW2:

```
 tunnel (
   interface = "bge0"
   local_ip = 10.10.10.2
   remote_ip = 10.10.10.1
   )
```

После изменения конфигурационного файла на шлюзах следует остановить демон, если он был запущен, и запустить его снова:

```
/etc/init.d/l2vpnd stop
/etc/init.d/l2vpnd start
```

Проверка работоспособности стенда

После того, как настройка GW1 и GW2 завершена, инициируем создание L2VPN-туннеля и защищенного соединения.

На Host1 выполним команду:

```
ping 192.168.103.2
```

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 L2VPN-туннель, защищенный VPN-туннелем.

В этом можно убедиться, выполнив на устройстве GW1 команду:

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

