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

## Настройка шлюза

РЛКЕ.00009-01 90 03

15.06.2015

# Содержание



# Настройка шлюза

Перед настройкой шлюза и созданием политики безопасности выполните инициализацию «Программного комплекса С-Терра Шлюз. Версия 4.1», которая описана в документе «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64» или, в случае использования модуля МСМ-950, выполните действия, описанные в документе «Руководство по установке и настройке модуля МСМ-950».

## Этапы настройки шлюза

Настройка «Программного комплекса С-Терра Шлюз» осуществляется в два этапа:

- Общая настройка шлюза.
- Создание политики безопасности шлюза.

## Общие настройки шлюза

Перечислим общие настройки шлюза, описанные подробно далее:

- Регистрация Лицензий на продукт S-Terra Gate и КриптоПро CSP, если их необходимо перерегистрировать после инициализации продуктов.
- Особенности генерации ключевой пары для исполнения класса защиты КС2/КС3, если для АМПДЗ не поддерживается функциональность ДСЧ.
- Работа с токенами.
- Изменение паролей (рекомендуется выполнить).
- Настройка интерфейсов:
  - Назначение IP-адресов интерфейсам.
  - Назначение нескольких IP-адресов одному интерфейсу.
  - Добавление сетевых интерфейсов.
  - Настройка сетевых интерфейсов, поддерживающих 802.1Q.
  - Настройка MTU интерфейса.
  - Перезагрузка LSP при изменении состояния интерфейсов.
- Настройка переменных окружения для балансировки нагрузки на шлюз.
- Настройка параметров параллельной обработки сетевого трафика.
- Синхронизация часов на шлюзе безопасности с NTP-сервером точного времени.
- Настройка NAT.
- Настройка RRI.
- Удаленная настройка шлюза.

# Регистрация Лицензий после инициализации

## Регистрация Лицензии на S-Terra Gate

Регистрация Лицензии на Продукт выполняется во время инициализации «Программного комплекса С-Терра Шлюз», но если появится необходимость перерегистрировать Лицензию после инициализации, то используется утилита `lic_mgr`.

Утилита `lic_mgr`, описанная в документе «Специализированные команды», запускается из интерфейса командной строки из каталога Продукта `/opt/VPNagent/bin`:

```
lic_mgr set -p PRODUCT_CODE -c CUSTOMER_CODE -n LICENSE_NUMBER
-l LICENSE_CODE
```

## Регистрация Лицензии на КриптоПро CSP

В случае необходимости перерегистрировать лицензию на СКЗИ «КриптоПро CSP» следует запустить утилиту `cpconfig` (утилита находится в каталоге `/opt/cprocsp/sbin/ia32` или `/opt/cprocsp/sbin/amd64`):

```
cpconfig -license -set xxxxxxx
```

`xxxxxxx` – серийный номер продукта «КриптоПро CSP».

Для регистрации драйверной части лицензии выполните команду:

```
set_driver_license.sh
```

После регистрации перезапустите `vpn-демона`, выполнив команду:

```
/etc/init.d/vpngate restart
```

# Особенности генерации ключевой пары для исполнения класса защиты КС2/КС3, если для АМПДЗ не поддерживается функциональность ДСЧ

Существуют некоторые особенности генерации ключевой пары и создания запроса на сертификат в случае использования «Программного комплекса С-Терра Шлюз» исполнения класса защиты КС2/КС3, т.к. для некоторых АПМДЗ не поддерживается функциональность ДСЧ.

Возможны различные варианты, в зависимости того, какая криптографическая библиотека применяется в «С-Терра Шлюз»:

- Если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи», то при генерации ключевой пары возможно использование биологического ДСЧ.
- Если используется СКЗИ «КриптоПро CSP»:
  - Администратор, на отдельной машине, с установленными СКЗИ «КриптоПро CSP» (класс защиты КС2/КС3) и электронным замком «Соболь», изготавливает внешнюю гамму, доставляет ее безопасным способом на «С-Терра Шлюз» и затем, при помощи утилиты `cert_mgr`, создает ключевую пару и запрос на сертификат. Подробнее изготовление внешней гаммы описано ниже.
  - Администратор, на отдельной машине, используя СКЗИ «КриптоПро CSP» создает ключевую пару и запрос на сертификат, получает сертификат и доставляет его и контейнер на «С-Терра Шлюз». Подробное описание приведено в документе «Программный комплекс С-Терра Шлюз. Версия 4.1. Руководство администратора. Приложение», в разделе «Создание локального сертификата с использованием СКЗИ «КриптоПро CSP».
  - Администратор, на отдельной машине, с установленными СКЗИ «КриптоПро CSP» и «Программным комплексом С-Терра Клиент», создает ключевую пару и запрос на сертификат, получает сертификат и доставляет его на «С-Терра Шлюз». Подробнее см. документ «Программный комплекс С-Терра Клиент. Версия 4.1. Руководство администратора. Приложение А», раздел «Создание сертификата пользователя с использованием СКЗИ «КриптоПро CSP».

## Изготовление внешней гаммы

Внешнюю гамму можно применять на «С-Терра Шлюз», независимо от используемой криптобиблиотеки.

На отдельной машине должно быть установлено СКЗИ «КриптоПро CSP» (класс защиты КС2/КС3) и электронный замок «Соболь».

Для изготовления внешней гаммы в командной строке запустите утилиту `genkpim`, например:

```
genkpim.exe 500 12121111 f:\gamma
```

`500` – необходимое количество случайных отрезков гаммы для записи на носитель,

`12121111` – номер комплекта внешней гаммы (8 символов в 16-ричном коде),

`f:\gamma` – путь на носителе, по которому будет записан файл с внешней гаммой.

В результате выполнения команды создается файл `kis_1`, который записывается на носитель по пути `f:\gamma` дублированием в два каталога: `DB1` и `DB2`.

Далее действия будут различаться в зависимости от используемого СКЗИ:

- В случае использования СКЗИ «КриптоПро CSP», выполните копирование файлов с внешней гаммой с носителя на «С-Терра Шлюз» в следующие каталоги: `/var/opt/cprocsp/dsrf/db1/` и `/var/opt/cprocsp/dsrf/db2/` соответственно.

- В случае использования криптобиблиотеки от компании «С-Терра СиЭсПи», выполните копирование одного файла с внешней гаммой с носителя на «С-Терра Шлюз», в каталог `/var/s-terra/ext-gamma`. Переименуйте файл с внешней гаммой в `eg_data`.
  В конфигурационном файле `/etc/S-Terra/skzi.conf` пропишите путь до каталога с внешней гаммой:

  ```
  ExtGammaPath=/var/s-terra/ext-gamma
  ```

Надёжно удалите файлы с внешней гаммой с носителя. Перезагрузите «С-Терра Шлюз».

# Работа с токенами

Существуют некоторые особенности работы с eToken 32 Кб и 64 Кб в случае использования «Программного комплекса С-Терра Шлюз» исполнения класса защиты КС2 и СКЗИ «КриптоПро CSP 3.6R4». Для успешной работы с токенами, с указанным объемом памяти, необходимо выполнить команды:

```
sed -e '/\[KeyDevices\\PCSC\]/{:a;n;/^$/!ba;i\[KeyDevices\\PCSC\\"AKS
ifdh [Main Interface] 00 00"\\Default]' -e '}'
/etc/opt/cprocsp/config.ini > /tmp/config.ini

mv /tmp/config.ini /etc/opt/cprocsp/config.ini
```

Побочным эффектом от выполнения этих команд может быть то, что токены 72 Кб перестанут обнаруживаться.

# Изменение или восстановление PIN для СЗН «СПДС-USB-01»

Существуют возможность изменить PIN администратора или восстановить PIN пользователя в случае использования «Программного комплекса С-Терра Шлюз», предустановленного на СЗН «СПДС-USB-01».

Для этого перезагрузите ОС и во время загрузки войдите в режим администратора, нажав клавишу “A” в ответ на сообщение:

```
Press 'a' to enter SPDS-USB Administrator mode or Esc to continue OS
loading
```

Далее будет запрошен PIN администратора (изначально 12345678):

```
Enter Administrator's PIN:
```

В случае успешной аутентификации будет предложено выбрать одно из действий:

```
Press next keys to select sub-mode:
1. To change SPDS-USB Administrator's PIN
2. To unblock SPDS-USB User's PIN
3. To SPDS-USB image recovery
4. To continue OS loading
```

Действие `To SPDS-USB image recovery` – восстановление образа СПДС-USB-01 с внешнего носителя подробно описано в документе «Инструкции по восстановлению и обновлению ПАК», в разделе «Инструкция по восстановлению ПАК с S-Terra Gate, предустановленным на СЗН «СПДС-USB-01» и здесь рассматриваться не будет.

При выборе `To change SPDS-USB Administrator's PIN` – изменение PIN администратора СПДС-USB-01 будет предложено ввести новый PIN администратора и подтвердить его повторным вводом:

```
Enter new Administrator's PIN:
Retype new Administrator's PIN:
```

Длина пароля должна быть не менее 8 символов, пароль может содержать цифры, буквы верхнего и нижнего регистров, специальные символы: (@, #, $, &, *, % и т.п.).

При несовпадении введенных PIN-кодов будет выведено сообщение: `New PINs not match` и будет предложено заново ввести PIN администратора. При совпадении введенных PIN-кодов выводится сообщение `Administrator's PIN changed` и предлагается нажать любую клавишу для перехода в административный режим.

При выборе `To unblock SPDS-USB User's PIN` – восстановление PIN пользователя СПДС-USB-01 будет предложено ввести новый PIN пользователя и подтвердить его повторным вводом:

```
Enter new User's PIN:
Retype new user's PIN:
```

Длина пароля должна быть не менее 4 символов, пароль может содержать цифры, буквы верхнего и нижнего регистров, специальные символы: (@, #, $, &, *, % и т.п.). При совпадении введенных PIN-кодов выводится сообщение `User's PIN unblocked` и предлагается нажать любую клавишу для перехода в административный режим. При несовпадении введенных PIN-кодов будет выведено сообщение: `New PINs not match` и будет предложено заново ввести PIN пользователя.

# Изменение паролей

После инициализации Продукта пользователь "root" с правами системного администратора имеет пустой пароль, который рекомендуется изменить системными средствами:

- зайдите в систему пользователем "root";
- выполните команду "passwd";
- введите новый пароль.

Специальный пользователь, созданный в процессе инсталляции с именем "cscons", имеет пароль "csp" и уровень привилегий 15. Ему предоставляется возможность управлять настройками S-Terra Gate и создавать политику безопасности. Рекомендуется после инсталляции изменить пароль этого пользователя. Изменение пароля пользователя, создание новых пользователей с разными уровнями привилегий осуществляется в специализированной консоли – в интерфейсе командной строки либо локально, либо удаленно с использованием команды username password или username secret.

Задание пароля для доступа к привилегированному (а также к конфигурационному) режиму для пользователей с уровнями привилегий от 0 до 14 осуществляется командами enable password или enable secret.

# Настройка интерфейсов (ОС Debian)

В зависимости от способа создания политики безопасности шлюза настройка интерфейсов выполняется:по-разному:

- если политика безопасности создается с использованием cisco-like консоли, то и настройка интерфейсов должна выполняться там же (при помощи команд cisco-like консоли);
- если политика безопасности создается путем написания конфигурационного текстового файла, то настройку интерфейсов рекомендуется выполнять при помощи средств ОС (команда `ifconfig`).

Cisco-like консоль автоматически запускается при входе в систему пользователем “cscons”. Пользователи, обладающие административными привилегиями, могут запустить консоль командой `cs_console` из каталога `/opt/VPNagent/bin/`.

Посмотреть IP-адреса интерфейсов можно с использованием команды cisco-like консоли `show running-config`. Для настройки адресов требуется сначала войти в глобальный конфигурационный режим консоли, используя команду `configure terminal`, а затем – в режим `interface configuration`, задав команду `interface type port/number`. Данная команда позволяет управлять настройками только зарегистрированных сетевых интерфейсов. Изменения, сделанные в этом режиме, вступают в действие немедленно и сохраняются в загрузочных скриптах ОС. Команды консоли описаны в документе «Cisco-like команды» (Console_command_reference.pdf).

Для просмотра IP-адресов интерфейсов в ОС используется команда `ifconfig –a`.

## Назначение IP-адресов интерфейсам

Измененить IP-адреса и маски подсети сетевых интерфейсов можно:

- при помощи команд cisco-like консоли;
- при помощи команды `ifconfig`.

### Назначение IP-адресов в cisco-like консоли

1. Войдите в режим interface configuration:

   ```
   interface fastethernetport/number
   ```

2. Назначьте интерфейсу IP-адрес и маску:

   ```
   ip address IP-адрес маска
   ```

Повторное задание IP-адреса замещает предыдущее значение.

Для того, чтобы увидеть сделанные изменения в конфигурации, используйте команду `show running-config`.

### Назначение IP-адресов командой ifconfig

1. При помощи команды `ifconfig` назначьте адрес и маску интерфейсу, например:

   ```
   ifconfig имя_интерфейса IP-адрес netmask маска up
   ```

2. Вызовите скрипт, сохраняющий данные об интерфейсе в конфигурационных файлах:

   ```
   /bin/ni_saveif.sh имя_интерфейса
   ```

# Назначение нескольких IP-адресов одному интерфейсу

## Назначение IP-адресов в cisco-like консоли

Различаются primary и secondary IP-адреса. В качестве primary адреса выбирается первый по списку адрес, остальные – в качестве secondary. Primary адрес может быть только один. Адресов secondary может быть несколько.

В режиме interface configuration введите команду:

```
ip address IP-адрес маска secondary
```

## Назначение IP-адресов командой ifconfig

Назначить несколько IP-адресов одному интерфейсу, т.е. создать несколько виртуальных (логических) интерфейсов, можно при помощи команды `ifconfig`.

1. Создайте сначала виртуальный интерфейс:

   ```
   ifconfig имя_интерфейса:1 IP-адрес netmask маска up
   ```

2. Вызовите скрипт, сохраняющий данные об интерфейсе в конфигурационных файлах:

   ```
   /bin/ni_saveif.sh имя_интерфейса
   ```

# Добавление сетевых интерфейсов

1. В зависимости от типа интерфейса добавьте в файл `/etc/ifaliases.cf` строку:

   для Ethernet 1000 Mbit

   ```
   interface (name="GigabitEthernet0/X" pattern="Y")
   ```

   для Ethernet 100Mbit и др.:

   ```
   interface (name="FastEthernet0/X" pattern="Y")
   ```

   X – номер физического порта ethernet

   Y – имя интерфейса в операционной системе.

2. Необходимо пересчитать контрольную сумму измененного файла. Запустите утилиту `integr_mgr calc`:

   ```
   integr_mgr calc –f /etc/ifaliases.cf
   ```

3. Перезапустите vpn-демона, выполнив команду:

   ```
   /etc/init.d/vpngate restart
   ```

# Настройка сетевых интерфейсов, поддерживающих 802.1Q

Интерфейс 802.1Q является расширением обычного Ethernet интерфейса (см. Стандарт IEEE 802.1Q). Для примера настроим VLAN-интерфейс 10 на интерфейсе `eth0`:

1. В файл `/etc/network/interfaces`, в раздел ###netifcfg-begin###, добавьте строки:

   ```
   auto eth0.10
   iface eth0.10 inet static
   address 192.168.0.2
   netmask 255.255.255.0
   ```

2. Добавьте в файл `/etc/ifaliaces.cf` следующую строку:

   ```
   interface (name="FastEthernet0/0.10" pattern="eth0.10")
   ```

3. Пересчитайте контрольную сумму измененного файла `ifaliaces.cf`, запустив утилиту `integr_mgr calc`:

   ```
   integr_mgr calc –f /etc/ifaliases.cf
   ```

4. Поднимите интерфейс:

   ```
   ifup eth0.10
   ```

5. Перезапустите vpn-демона, выполнив команду:

   ```
   /etc/init.d/vpngate restart
   ```

## Настройка MTU интерфейса

Настроить значение MTU сетевого интерфейса, которое задает максимальный размер пакета, передаваемого без фрагментации через данный интерфейс, можно, используя либо средства ОС, либо команду mtu интерфейса командной строки консоли.

Настройка MTU сетевого интерфейса в ОС Debian осуществляется следующим образом:

1. в файл `/etc/network/interfaces`, в раздел ###netifcfg-begin###, в описание выбранного сетевого интерфейса добавьте строчку:

   ```
   MTU YYYY
   ```

   `YYYY` – размер MTU сетевого интерфейса.

2. Перезапустите сетевого демона, выполнив команду:

   ```
   /etc/init.d/networking restart
   ```

Таким образом устанавливается постоянное значение MTU.

Установка значения MTU интерфейса на время одной сессии (до перезагрузки ОС) осуществляется командой:

```
ifconfig eth0 mtu YYYY (для интерфейса fa 0/0)
ifconfig eth1 mtu YYYY (для интерфейса fa 0/1)
```

`YYYY` – размер MTU сетевого интерфейса.

## Перезагрузка LSP при изменении состояния интерфейсов

Периодически демон (vpnsvc) Продукта опрашивает операционную систему об изменениях в состоянии интерфейсов. Если в последний опрос произошли какие-либо изменения по сравнению с предыдущим, то автоматически происходит перезагрузка политики безопасности (LSP), загруженной в базе Продукта.

Изменения в состоянии интерфейсов могут быть следующими:

- состав интерфейсов;
- IP-адрес интерфейса;
- маска IP-адреса интерфейса;
- индекс интерфейса;
- Broadcast адрес.

# Настройка переменных окружения

Имеется возможность настроить некоторые переменные окружения, которые могут повлиять на работу S-Terra Gate или дать возможность получить дополнительную информацию в лог-файле.

Можно изменить значения следующих переменных окружения:

CSP_SYS_RESPONSE_TIMEOUT

CSP_LOG_TASK_TIME

CSP_LOG_TASK_QUEUE_PERIOD

VPNGATE_CONFIGURED

Начальные значения, установленные инсталлятором, для всех переменных окружения равны 0 и совпадают со значениями, установленными по умолчанию.

Изменить значение переменных окружения можно следующим образом:

1. отредактировать файл `/etc/default/vpngate`
2. перезапустить vpn-демона, выполнив команду

   `/etc/default/vpngate restart`

## Описание переменных окружения

CSP_SYS_RESPONSE_TIMEOUT — задает максимальное время (в секундах), на которое vpn-демон может "подвиснуть" перед тем как аварийно закончить свою работу. "Подвисание" – состояние, когда ни одна из рабочих нитей не может взяться за выполнение задания. По достижении указанного времени vpn-демон сам аварийно завершает свою работу и создает core-файл.

Механизм слежения за зависанием vpn-демона позволяет завершить работу неработоспособного демона и запустить новую сессию, тем самым повысив отказоустойчивость системы.

Если CSP_SYS_RESPONSE_TIMEOUT = 0, то механизм слежения за зависанием vpn-демона не включается.

Переменные окружения CSP_LOG_TASK_TIME и CSP_LOG_TASK_QUEUE_PERIOD используются службой поддержки для диагностики различных ситуаций. Обе переменные задают время, по истечении которого в файл лога выдаются сообщения. CSP_LOG_TASK_QUEUE_PERIOD выдает сообщения уровня `info`, CSP_LOG_TASK_TIME выдает сообщения уровня `warning`.

CSP_LOG_TASK_TIME — задает время (в секундах), которое должно быть затрачено на выполнение одной задачи. При превышении заданного времени в файл лога будет выдаваться сообщение о большем затраченном времени на выполнение одной задачи:

```
Event Manager profiler: task time is <n> sec
(src=<hex> dst=<hex> idx=<n> proc=<hex>)
```

Если CSP_LOG_TASK_TIME = 0, то сообщение в файл лога не выводится.

| | |
|---|---|
| CSP_LOG_TASK_QUEUE_PERIOD | задает период (в секундах), с которым в файл лога будут выдаваться сообщения о времени ожидания задачи в очереди и длине очереди задач. Сообщения выводятся следующего вида:<br>`Event Manager profiler: waiting time of task queue is <n> sec, queue length is <n> tasks`<br>Если CSP_LOG_TASK_QUEUE_PERIOD = 0, то сообщения в файл лога не выводятся. |
| VPNGATE_CONFIGURED | показывает выполнил ли пользователь процесс инициализации S-Terra Gate. Может принимать значения: yes или no. |

# Настройка параметров параллельной обработки сетевого трафика

Необходимость настройки параметров с целью оптимизации IPsec обработки сетевого трафика на многопроцессорных системах, может быть вызвана особенностями аппаратного устройства системы, оптимизацией под определенный характер сетевого трафика, оптимизацией под характеристики сетевых интерфейсов и канала связи.

На рисунке ниже представлена схема параллельной обработки трафика в Linux.

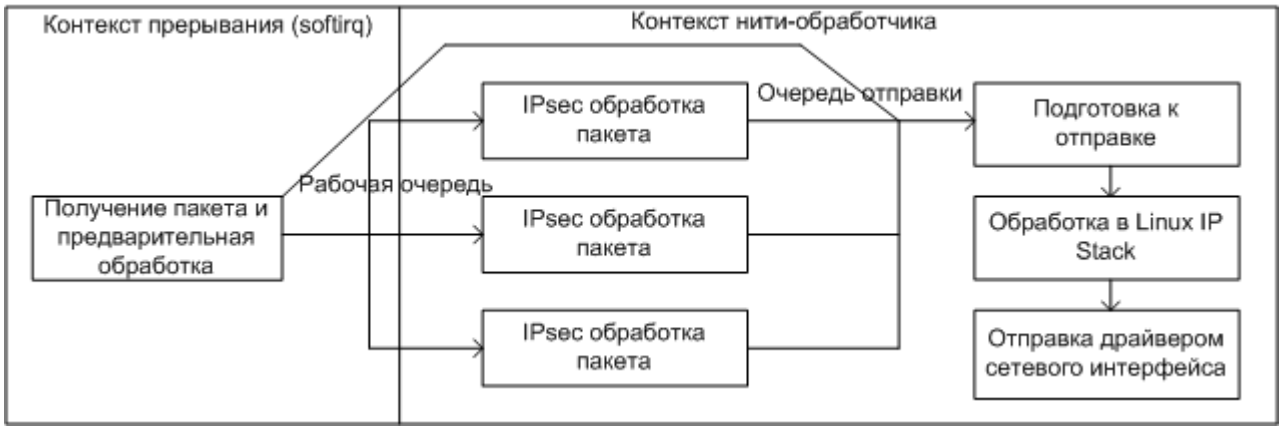



Рисунок 1

После получения, пакет преобразуется к внутреннему формату. Проверяется, нет ли превышения размера рабочей очереди или очереди отправки. Далее пакет помещается в рабочую очередь и очередь отправки.

Пакеты забираются из рабочей очереди несколькими нитями обработчика одновременно. Происходит фильтрация и криптографическая обработка.

Пакет отмечается в очереди отправки как готовый (при работе с очередью отправки производится 3 операции – включение в очередь, разрешение отправки, извлечение из очереди; для рабочей очереди операции две – включение в очередь, извлечение из очереди).

В контексте одной из нитей-обработчиков происходит извлечение пакетов из очереди отправки и выполняются действия, связанные с маршрутизацией и дальнейшей отправкой пакета.

## Настройка параметров рабочей очереди

Параметры рабочей очереди настраиваются в файле /etc/modprobe.d/vpndrvr.conf (параметр cpu_distribution) и с помощью утилиты drv_mgr (параметр pq_thread_q_size).

### cpu_distribution

Назначением параметра cpu_distribution является оптимизация доступа к памяти и кешам процессоров при обработке трафика, минимизация переключения контекстов нитей ядра Linux, а также более эффективное распределение вычислительной мощности многопроцессорной системы между задачами обработки трафика. Многопроцессорные системы, использующие NUMA архитектуру, разделяют оперативную память между несколькими NUMA-узлами. К NUMA-узлу приписано некоторое число процессорных ядер. Доступ к памяти внутри своего NUMA-узла происходит гораздо быстрее, чем к памяти чужого узла. Поэтому целью настройки является обработка выделенного потока сетевого трафика в

рамках одного NUMA узла: получение IP-пакета, выделение памяти под него и IPsec-обработка должна происходить на ядрах процессора, приписанных к одному узлу.

Ядра, выделенные для обработки прерываний, по возможности размещаются в разных NUMA-узлах. Каждому выделенному для обработки ядру соответствует своя рабочая очередь. В случае переполнения своей очереди, трафик будет помещаться в самую свободную "чужую" очередь (если такая найдется), при этом возможна потеря производительности.

Привязка прерываний позволяет добиться большей эффективности обработки т.к. для обработки пакета будет использована очередь, находящаяся в контексте NUMA и кеша процессора, на котором произошло прерывание. Кроме того, привязка прерываний обеспечивает возможность параллельной обработки прерываний при значении числа процессорных ядер два и более.

Параметр cpu_distribution имеет следующий формат:

<NIC0>,<NIC1>,...:<irq cores>/<working cores>

<NIC0>,<NIC1>,... – список интерфейсов, для которых выполняется привязка прерываний.

Допускается пустой список интерфейсов, тогда привязка прерываний к процессорам не выполняется, и прерывания сетевых интерфейсов распределятся в соответствии с алгоритмом назначения прерываний LINUX. В этом случае возможна менее эффективная обработка пакетов.

Все интерфейсы, явно указанные в списке должны быть подняты на момент старта драйвера.

Перечислять интерфейсы смысла не имеет. Можно указать '*', тогда "привязываются" все прерывания интерфейсов, или пустой список (ничего перед символом ':'), тогда привязки прерываний не будет.

При значении <irq_cores> = 0 привязка прерываний делается ко всем процессорам одновременно.

<irq cores> – число процессорных ядер, полностью выделенных под обработку прерываний сетевых интерфейсов.

<irq_cores> = 0 используется для распределения прерываний по умолчанию.

<irq cores> = 1 одно выделенное ядро для прерываний.

<working cores> – количество рабочих ниток, число процессорных ядер, используемых для IPsec обработки.

<working cores> может иметь значение "*", которое означает "использовать все доступные ядра, за исключением ядер прерываний". Рекомендуется указывать значение, кратное <irq cores>, в этом случае обеспечится равномерное распределение процессорных ядер по обслуживаемым очередям.

**Значения по умолчанию:**

- Если явно не задавать cpu_distribution и число процессорных ядер 3 и более, принимается значение *:1/*
- Если явно не задавать cpu_distribution и число процессорных ядер 2 или одно, принимается значение *:0/*

**Ограничения на значения в cpu_distribution**

- <irq cores> < число процессорных ядер
- <irq cores> + <working cores> ≤ число процессорных ядер
- <irq cores> ≤ <working cores>

### pq_thread_q_size

Параметр pq_thread_q_size ограничивает размер очереди и задается утилитой drv_mgr, описанной в документе «Специализированные команды».

Если <irq_cores> больше одного, то вычисляется для каждой очереди в отдельности. Максимальное суммарное количество ожидающих пакетов умножается на количество очередей.

Настройка длины очереди делается в зависимости от характера трафика. Большая длина позволяет избежать потерь пакетов при пиковых и неравномерных нагрузках, а также обеспечит максимальную пропускную способность. Маленький размер очереди позволяет ограничить максимальное время обработки одного пакета, снижает используемый объем памяти ядра Linux (особенно это актуально для 32-битных систем).

### Рекомендации по использованию

Для систем с одним-двумя процессорными ядрами достаточно значения по умолчанию *:0/*.

Если в системе есть один многоядерный процессор (3 и более ядер), рекомендуется конфигурация по умолчанию *:1/*. Для оптимальных результатов при большом количестве ядер, может быть полезно сократить число <working cores>: то есть выставить *:1/N, где N число процессорных ядер-2 и менее.

Для систем с двумя и более многоядерными процессорами возможны следующие варианты:

- если аппаратная конфигурация и характер трафика позволяет параллельную обработку прерываний, то число <irq cores> можно увеличить (выставить 2);
- если добиться параллельной обработки прерываний невозможно, то надо выставить <irq cores> = 1 далее, в зависимости от сложности криптографических вычислений, оптимальной конфигурацией может быть локализация всех IPsec вычислений на одном процессоре путем ограничения числа <working cores> до числа ядер на одном процессоре-1.

## Настройки параметров очереди отправки

Очередь отправки предназначена для восстановления порядка пакетов после параллельной обработки. Очередь управляется параметрами pq_thread_q_size и pq_force_ordering, которые задаются утилитой drv_mgr, описанной в документе «Специализированные команды».

### pq_send_q_size

Параметр pq_thread_q_size задает максимальное число пакетов в очереди отправки.

Значение 0 отключает очередь отправки. Это можно сделать, если шлюзом обрабатывается одновременно много сетевых соединений и сессий, регулирование порядка отправки пакетов в этом случае не требуется. При отключенной очереди отправки, завершающие стадии обработки пакета, начиная с блока "подготовка к отправке" (Рисунок 1), выполняются сразу после блока "IPsec обработка пакета". То есть отправка пакета происходит параллельно, минуя очередь. Отключение очереди может давать выигрыш в производительности за счет сокращения общего времени обработки пакета и параллельной отправки, а может и наоборот, приводить к деградации производительности из-за потери переупорядоченных пакетов в пользовательских протоколах. Параллельная отправка пакетов в некоторых случаях тоже ухудшает производительность.

Размер, как и для рабочей очереди, подстраивается под характер трафика. Ограничения очереди отправки и рабочей очереди проверяются одновременно, и трафик может уничтожаться при заполнении одной из них.

### pq_force_ordering

Параметр pq_force_ordering определяет, что происходит при заполнении очереди отправки:

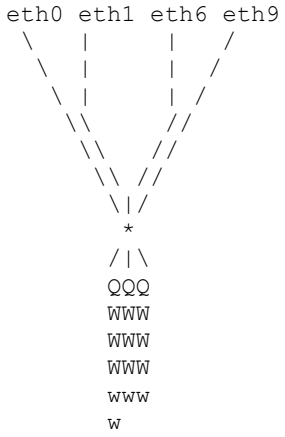
- Если выставлено значение 1, пакеты при переполнении очереди уничтожаются.
- Если выставлено значени 0, пакеты все равно обрабатываются – то есть порядок отправки пакетов регулируется только в случае низкой загрузки. При установке pq_force_ordering = 0 рекомендуется выставлять маленькое значение pq_send_q_size.

Если pq_send_q_size = 0, значение pq_force_ordering не имеет смысла.

**Пример:**

Имеется 4 NUMA-узла, по 4 ядра на узел. Установим cpu_distribution=eth0,eth1,eth6,eth9:3/*.

Получим следующее распределение:




Q – очереди/выделенные ядра прерываний,
W – рабочие нитки, запущенные на том же процессоре, что и очереди,
w – рабочие нитки, запущенные в "чужом" NUMA-узле,
линии – привязка прерываний.

То, что в примере не изображено, что нет соответствия между интерфейсом и очередью – не случайно. Если интерфейс имеет множество прерываний MSI-X, они распределяются между всеми выделенными для обработки прерываний ядрами.

## Замечания

Привязка прерываний интерфейсов не всегда срабатывает. Возможно, есть ограничение на количество прерываний, привязанных к одному процессору. Специальной диагностики в этом случае не выдается, результат привязки можно проверить, изучив /proc/irq/*/smp_affinity и /proc/interrupts.

Распределение между очередями (<irq_cores> > 1) зависит от автоматического распределения трафика между несколькими прерываниями сетевого интерфейса. Это работает не всегда.

При интенсивной, но не полной загрузке шлюза, на время обработки пакета влияет скорость пробуждения нити ядра Linux. На время пробуждения нити в свою очередь могут влиять разнообразные процессы внутри Linux (например, влияют вызовы команды ps или аналогичные действия, интенсивный доступ к файловой системе). Особенно негативный эффект проявляется при включенной очереди отправки, т.к. при этом задержка одного пакета влияет на другие, которые поступили на обработку позже по времени.

Привязка прерываний важна не только для сетевых интерфейсов, к которым привязаны действия IPsec-обработки. Если пакет исходящий, то его обработка происходит в контексте интерфейса, на который пакет поступил как входящий.

# Настройка NTP (Network Time Protocol)

Предварительно настроим на шлюзе безопасности системную дату и часовой пояс:

Установим текущую системную дату командой:

```
date MMDDhhmm[[CC]YY][.ss]
```

MM — месяц, DD — день, hh — часы, mm — минуты, CCYY —год, ss — секунды (год и секунды указывать не обязательно).

Выберем нужный часовой пояс. Список всех доступных часовых поясов можно найти в каталоге `/usr/share/zoneinfo`. Делаем ссылку на нужный часовой пояс, например:

```
ln -sf /usr/share/zoneinfo/Europe/Moscow /etc/localtime
```

Выбранную зону добавим в файл `/etc/sysconfig/clock`.

Для синхронизации часов с NTP-сервером точного времени в ОС используется демон `ntpd`, который может выступать как в роли сервера, так и клиента, в зависимости от настроек, заданных в конфигурационном файле `/etc/ntp.conf`. По умолчанию демон настроен как NTP-клиент.

## Настройка NTP-сервера

Опишем некоторые параметры, задающиеся в файле `/etc/ntp.conf` и позволяющие настроить Linux NTP-сервер:

Параметр `server` задает внешний эталонный NTP-сервер, который будет использоваться для синхронизации с локальным Linux NTP-сервером:

```
server <server_addr>
```

`<server_addr>` – P-адрес или доменное имя внешнего эталонного NTP-сервера.

Таких эталонных серверов может быть указано несколько, каждый в отдельной строке. Например:

```
server ntp1.vniiftri.ru
server ntp2.vniiftri.ru
```

Параметр `restrict` позволяет задать ограничения на доступ и управление Linux NTP-сервером:

Разрешите внешним эталонным NTP-серверам обращаться к Linux NTP-серверу, например:

```
restrict ntp1.vniiftri.ru
restrict ntp2.vniiftri.ru
```

Если к Linux NTP-серверу будут поступать запросы на NTP синхронизацию (без модификации и отсылки трапов) от других компьютеров локальной сети, то добавьте в файл строку:

```
restrict <addr_local_network> mask <addr_local_mask> nomodify notrap
```

`<addr_local_network>` – адрес локальной подсети, которую обслуживает Linux NTP-сервер;

`<addr_local_mask>` – маска подсети.

Чтобы Linux NTP-сервер имел полный доступ к самому себе без ограничений, впишите строку:

```
restrict 127.0.0.1
```

Параметр `driftfile` указывает файл, в котором хранится погрешность системных часов:

```
driftfile /var/lib/ntp/ntp.drift
```

Параметр `logfile` задает лог-файл:

```
logfile /var/log/ntpstats
```

## Настройка NTP-клиента

Для настройки Linux NTP-клиента, в файле `/etc/ntp.conf` должны присутствовать строки, задающие следующие параметры:

Параметр `server` задает локальный NTP-сервер, который будет использоваться для синхронизации времени NTP-клиентом:

```
server <server_addr>
```

`<server_addr>` – IP-адрес или доменное имя NTP-сервера локальной сети.

Параметр `restrict` позволяет задать ограничения на доступ и управление Linux NTP-сервером:

Ограничьте доступ к серверу по умолчанию:

```
restrict default ignore
```

Разрешите доступ к Linux NTP-серверу, ограничив взаимодействие:

```
restrict <server_addr> noquery notrap
```

`<server_addr>` – IP-адрес или доменное имя NTP-сервера локальной сети.

Разрешите доступ только локальному NTP-серверу:

```
restrict 127.0.0.1 nomodify notrap
```

Параметр `driftfile` указывает файл, в котором хранится погрешность системных часов:

```
driftfile /var/lib/ntp/ntp.drift
```

Параметр `logfile` задает лог-файл:

```
logfile /var/log/ntpstats
```

## Управление демоном

Для управления демоном `ntpd` используются стандартные команды:

```
/etc/init.d/ntp start
/etc/init.d/ntp restart
/etc/init.d/ntp stop
```

Проверьте параметры запуска демона – в конфигурационном файле `/etc/default/ntp` – рекомендуем установить параметр `NTPD_OPTS='-g'`, позволяющий выполнять синхронизацию даже при большой разнице во времени.

## Проверка работы NTP-сервера

Команда `ntpq -p` выводит список источников точного времени и их характеристики.

Обратите внимания на поля `delay` и `offset`:

Поле `delay` показывает количество времени (в секундах) необходимого для получения ответа на запрос времени.

Поле `offset` показывает разницу между временем локального и удаленного серверов.

Знак `*` перед именем удаленного сервера (поле `Remote`) указывает, что сервер выбран для синхронизации.

## Время при работе с сертификатами

В сертификате время указано относительно Гринвича.

Шлюз работает с сертификатами в локальном времени.

Время жизни сертификата не зависит от временного пояса.

Время жизни сертификата будет зависеть от сезонного перевода часов, т.к. время корректируется в фиксированный момент по локальному времени, поэтому может возникнуть сбой именно в момент перевода часов в разных поясах. Как только перевод будет окончен во всех поясах, время жизни сертификата в них будет одинаковым.

# Настройка NAT на шлюзе безопасности

На шлюзе безопасности NAT (Network Address Translation) осуществляется средствами ОС, а именно при помощи утилиты iptables. Описание iptables можно посмотреть на сайте проекта Netfilter.

Обработка трафика шлюзом безопасности осуществляется в последовательности аналогичной Cisco IOS. Исходящие пакеты сначала обрабатываются iptables, а затем VPN-продуктом в соответствии с политикой безопасности. Входящие пакеты сначала обрабатываются VPN-продуктом, а затем iptables. В алгоритме возможны изменения при включении в iptables механизмов обработки трафика помимо PREROUTING, FORWARDING и POSTROUTING.

Использование NAT на шлюзе безопасности позволяет производить трансляцию следующих видов:

- Статический NAT – выполняется взаимно-однозначное отображение внутренних IP-адресов во внешние. Этот вид трансляции может использоваться при настройке IPsec-туннеля между подсетями с одинаковым адресным пространством.
- Динамический NAT – в этом случае происходит динамическая трансляция внутренних локальных IP-адресов в пул глобальных IP-адресов или в адрес внешнего интерфейса шлюза. Этот вид трансляции также может использоваться для IPsec-трафика между подсетями, а также для открытого доступа к интернет-серверам.
- Port Address Translation (PAT) или Network Address Port Translation (NAPT) – адреса назначения в пакетах, приходящих на адрес внешнего интерфейса шлюза, подменяются на локальные в зависимости от порта TCP, что позволяет организовать доступ к нескольким серверам в локальной сети. Этот сценарий можно использовать как совместно с IPsec, так и для открытого трафика.

Во всех приведенных трансляциях поддерживается работа по протоколу FTP.

# Использование RRI

RRI (Reverse Route Injection) – это новый механизм связи управления топологией VPN и системой маршрутизации, позволяющий маршрутам к удаленным защищенным подсетям и клиентам автоматически принимать участие в процессе маршрутизации.

Смысл механизма RRI состоит в том, что после создания защищенного соединения IPsec SA, в таблицу маршрутизации шлюза безопасности с включенным RRI автоматически вносится запись о маршруте к удаленной сети партнера или клиенту. При нарушении защищенного соединения добавленный маршрут из таблицы маршрутизации шлюза удаляется.

Механизм RRI может использоваться в сетях большого размера для обеспечения надежности – в схемах резервирования с балансировкой сетевой нагрузки.

Для оповещения соседних сетевых устройств, стоящих за шлюзом безопасности, о доступных ему хостах, сетях, новых маршрутах, соответствующих изменениям в топологии VPN, используются протоколы динамической маршрутизации, например, RIP. Такие протоколы маршрутизации реализованы в пакете программ Quagga.

Рассмотрим пример использования механизма RRI в сети (см. Рисунок 2). Подсеть Lan2 защищена шлюзом безопасности GW3, а подсеть Lan1 – двумя шлюзами безопасности GW1 и GW2, включенными в схему резервирования с распределением нагрузки, т.е. доступ в подсеть Lan1 можно получить либо через шлюз GW1, либо через шлюз GW2. Оба канала работают. На шлюзах безопасности установлен продукт S-Terra Gate 4.1, на GW1 и GW2 включен RRI. В сеть включены маршрутизаторы Cisco. После создания IPsec SA между шлюзами GW3 и GW1, в таблицу маршрутизации GW1 добавляется запись о маршруте до сети Lan2 (обратный маршрут).

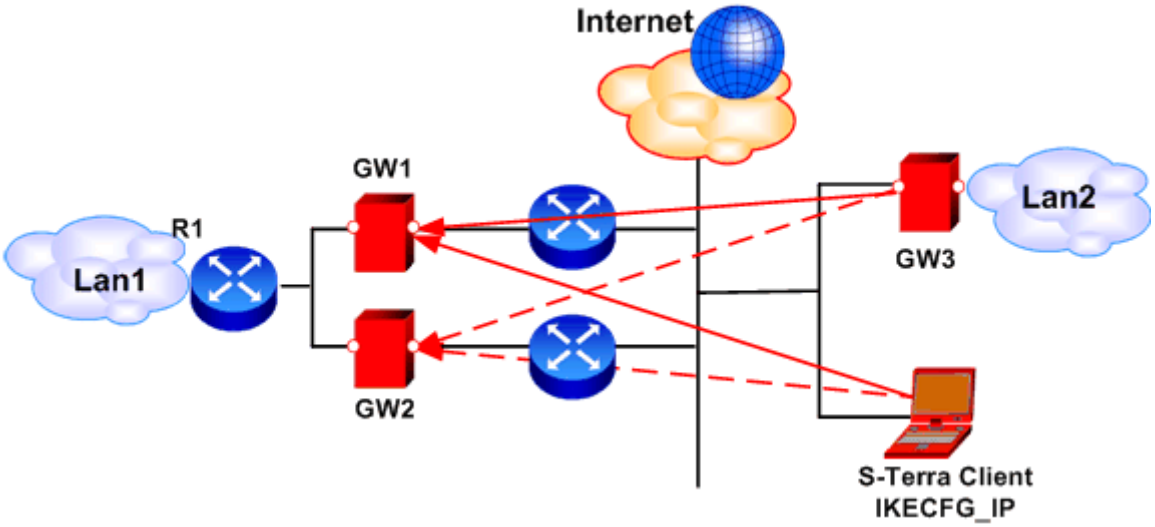



Рисунок 2

При нарушении установленного защищенного соединения (GW3 – GW1), запись об обратном маршруте в таблице маршрутизации шлюза GW1 удаляется. В случае, если соединение от шлюза GW3 будет перестроено на шлюз безопасности GW2, то в таблицу маршрутизации шлюза GW2 будет добавлен маршрут к сети Lan2.

Для обмена маршрутной информацией с маршрутизатором R1, на сетевых интерфейсах шлюзов GW1 и GW2, через которые происходит соединение с R1, нужно включить протокол RIP. Демоны RIP на шлюзах нужно настроить таким образом, чтобы они только передавали информацию о маршрутах соседним устройствам, но не добавляли маршруты, полученные от соседних устройств, в свою таблицу маршрутизации. Маршрут до подсети Lan2, посланный по протоколу RIP шлюзом GW1, должен добавиться в таблицу маршрутизации R1, но не добавиться в таблицу маршрутизации GW2, и наоборот. Эти сведения используются сетевым устройством R1 для динамического перенаправления сетевого трафика.

В случае с мобильным пользователем – на основании предъявленного им сертификата и запроса, шлюз GW1 выдает ему адрес из IKECFG пула. После создания защищенного соединения, на шлюзе GW1 в таблицу маршрутизации вносится запись о маршруте до мобильного клиента, о чем по протоколу динамической маршрутизации уведомляется маршрутизатор R1. Если мобильный клиент построит сначала соединение с GW1, а затем – с GW2, то это приведет к появлению двух маршрутов до мобильного клиента на маршрутизаторе R1. Такая ситуация может быть разрешена стандартными средствами DPD. При разрыве соединения, шлюз GW1 оповещает R1, что адрес, выданный из пула, ему более недоступен.

**Примечание:**

При физическом обрыве связи между шлюзом GW1 и маршрутизатором R2 (next hop), шлюз безопасности GW1 не может, используя DPD (Dead Peer Detection), обнаружить разрыв соединения с шлюзом GW3 (или с клиентом), так как сессия DPD запускается только при отправке исходящего пакета. А исходящий пакет не отправляется, так как ОС не может найти куда его отправить, потому что маршрутизатор R2 на arp запрос не отвечает и GW1 не может получить MAC-адрес устройства R2.

Поэтому могут возникать проблемы с переключением с GW1 на GW2 при физическом обрыве связи между шлюзом GW1 и маршрутизатором R2 (next hop). SA умрет только по истечению времени жизни и после этого из таблицы маршрутзации GW1 будет удален маршрут в подсеть Lan2 (или до мобильного клиента) и об этом будет уведомлен маршрутизатор R1. Для решения этой проблемы можно необходимую запись в arp-таблице сделать статической, добавьте на GW1 запись в arp-таблицу:

```
arp –s <IP_address_R2> <mac_address_R2>
```

Аналогично, добавьте на шлюз GW2 запись в arp-таблицу:

```
arp –s <IP_address_R3> <mac_address_R3>
```

# Настройка RRI

Настройка механизма RRI заключается в следующем:

- Включить механизм RRI на шлюзе безопасности, внеся соответствующие изменения в политику безопасности.
- Настроить динамическую маршрутизацию по протоколу RIP на маршрутизаторе Cisco.
- Создать конфигурационный файл для продукта Quagga.

*Примеры сценариев, в которых используется RRI, приведены на сайте http://www.s-terra.com/ в разделе «Решения – Типовые сценарии применения продуктов S-Terra».*

## Включение механизма RRI на шлюзе безопасности

При создании политики безопасности посредством командной строки включение механизма RRI производится в режиме конфигурирования криптокарты командой `reverse-route`.

Если политика безопасности задается в конфигурационном файле, то для включения RRI в структуре `IPsecAction` необходимо атрибуту `ReverseRoute` присвоить значение `TRUE`.

## Настройка cisco-маршрутизатора

Для того, чтобы маршутизатор воспринимал посылаемые продуктом Quagga маршруты по протоколу RIPv2, достаточно добавить в его конфигурацию строки:

```
router rip
```

```
version 2
network <подсеть сетевого интерфейса для CISCO RIP>
```

## Настройка Quagga

В разделе приведена краткая информация о продукте Quagga, описан конфигурационный файл и даны некоторые сведения об особенностях реализации RRI на шлюзе безопасности.

### Краткое описание продукта Quagga

Продукт Quagga входит в комплект поставки ПК S-Terra Gate и инсталлирован на нем.

Quagga состоит из пакета программ, реализующих протоколы динамической маршрутизации, основанных на TCP/IP – RIPv1, RIPv2, OSPFv2, OSPFv3, BGPv4. Для работы со шлюзом безопасности будем использовать протокол RIPv2. Дальнейшее описание работы с Quagga касается только протокола RIPv2.

Quagga состоит из нескольких демонов, каждый из которых поддерживает свой протокол маршрутизации. Одновременно работать могут несколько разных демонов в сообществе с управляющим демоном zebra.

zebra – демон управления процессом маршрутизации. Он обеспечивает взаимодействие между демонами маршрутизации и операционной системой. Демоны маршрутизации получают/устанавливают записи из таблицы маршрутизации через zebra.

ripd – демон маршрутизации, поддерживающий работу протоколов RIPv1 (RFC1058), RIPv2 (RFC2453).

Каждый демон имеет свою консоль конфигурирования, доступную посредством протокола ***telnet***:

```
zebra:      telnet 127.0.0.1 2601
ripd:       telnet 127.0.0.1 2602
```

Работа через консоль защищена паролем, который нужно задать в конфигурационном файле каждого из демонов (если пароль в конфигурационном файле не задан или конфигурационный файл отсутствует, то работа через консоль невозможна). Адрес и порт, по которым будут доступны демоны, задаются при запуске демонов (в нашем случае они соответствуют вышеуказанным, то есть извне недоступны).

Более подробную информацию о продукте и его настройке можно смотреть в Интернете (например, http://www.quagga.net/docs/quagga.html или http://www.opennet.ru/base/net/zebra_doc.txt.html).

### Настройка Quagga для передачи маршрута посредством протокола RIPv2

Продукт Quagga поставляется без конфигурационных файлов.

Сначала необходимо создать конфигурационные файлы демонов zebra и ripd (`zebra.conf` и `ripd.conf`), разместив их в каталоге `/etc/quagga/`.

Примеры конфигурационных файлов демонов `zebra.conf.sample` и `ripd.conf.sample` размещены в каталоге `/etc/quagga/`.

**Рекомендуемый шаблон конфигурационного файла для демона ripd**

```
! -*- rip -*-
!
! RIPd template configuration file
!
hostname ripd
password <пароль для входа в консоль управления>
enable password <пароль для входа в привилегированный режим консоли управления>
!
!
router rip
 version 2
 redistribute kernel
 network <имя сетевого интерфейса, на котором включается RIP>
!
! фильтрация исходящих и входящих пакетов RIP (маршрутов RIP) на
! интерфейсе при помощи списков доступа
!
 distribute-list acl-in in
 distribute-list acl-out out
!
!
access-list acl-in deny any
access-list acl-out permit <адреса, до которых интересны изменения маршрутов>
access-list acl-out deny any
!
```

Обратите внимание на команду ***access-list acl-in deny any*** – она запрещает получать информацию о маршрутах от других устройств, шлюз должен только передавать информацию о маршрутах другим сетевым устройствам.

В некоторых случаях ***access-list acl-out*** удобнее задавать так:

```
access-list acl-out deny <адреса, до которых не интересны изменения маршрутов>
access-list acl-out permit any
```

Рекомендуется настроить аутентификацию устройств, работающих по протоколу RIPv2 (см. документацию на Quagga).

Для работы демона `ripd` требуется запущенный демон zebra.

Запуск или остановка демона осуществляются скриптом:

```
/etc/init.d/zebra {start|stop}
/etc/init.d/ripd {start|stop}
```

Для активизации RIPv2 при загрузке ОС выполните команды:

```
chkconfig zebra on
chkconfig ripd on
```

# Особенности реализации RRI

После построения IPsec SA, на шлюзе безопасности (при включенном RRI) вычисляется обратный маршрут (RR), который вносится в таблицу маршрутизации. Основанием для такого маршрута являются следующие данные:

селектор SA (ID второй фазы IKE)

адрес назначения туннельного заголовка SA (tdst)

системная таблица маршрутизации (без учета маршрутов, добавленных подсистемой RRI).

Вычисление маршрута:

ID партнера[1] второй фазы IKE преобразуется в адрес и маску подсети. Полученные адрес и маска будут адресом назначения создаваемого RR. Если ID имеет протоколы и/или порты, содержит произвольный диапазон адресов, которые невозможно преобразовать в адрес и маску подсети, то обратный маршрут не создается.

В системной таблице производится поиск туннельного адреса SA.

Если правил не найдено (“Destination Unreachable”), RR не добавляется.

Если найдено правило прямой маршрутизации через интерфейс, вычисленный маршрут будет через gateway tdst.

Если найдено правило прямой маршрутизации через gateway GW, вычисленный маршрут будет через gateway GW.

Если маршрут успешно вычислен, проверяется следующее:

Такой же маршрут был ранее добавлен подсистемой RRI для SA с тем же tdst. В этом случае увеличивается счетчик ссылок, маршрут не добавляется.

Маршрут для SA с такими же ID второй фазы и tdst уже добавлен, но отличается. В этом случае существующий маршрут обновляется, увеличивается счетчик ссылок.

Маршрут с такими же параметрами уже добавлен, но для SA с другим tdst. Маршрут не создается, счетчик ссылок не увеличивается.

Маршрут, соответствующий ID партнера есть в системной таблице, но подсистемой RRI он не добавлялся. В этом случае маршрут не создается.

При удалении SA из ядра, счетчик ссылок соответствущего маршрута уменьшается, при обнулении счетчика маршрут удаляется.

В случае аварийного завершения работы сервиса vpnsvc маршруты, добавленные RRI в таблицу маршрутизации, будут удалены.

**Предупреждение:** недопустимо вручную изменять или удалять правила маршрутизации, которые автоматически формируются при использовании RRI.

В Таблица 1 приведены некоторые возможные конфликтные ситуации.

[1] Поскольку протокол в ID второй фазы один для обоих партнеров, а порты без указания протокола смысла не имеют, присутствие портов и протоколов с обоих сторон не допускается.

Таблица 1

| N | Ситуация | Поведение продукта | Отличие в поведении в Cisco IOS |
|---|---|---|---|
| 1 | Строится IPsec SA, при этом ID партнера второй фазы IKE не является подсетью (содержит диапазон IP-адресов, порты и/или протоколы). | Маршрут RR не добавляется и выдается предупреждение в файл лога 1.2 | Диапазоны адресов в Cisco IOS также не поддерживаются.<br>При наличии портов, протоколов в ID партнера в Cisco IOS маршрут создается. |
| 2 | Имеется построенный IPsec SA и в таблицу внесен вычисленный RR по нему. Строится другой IPsec SA и по нему также вычисляется RR. Оба IPsec SA имеют разные локальные ID, но одинаковые ID партнеров. Если при этом отличаются туннельные адреса, то для двух таких SA могут потребоваться разные маршруты, а добавить второй маршрут невозможно. | Маршрут RR создается только для первого из конфликтующих SA, а при создании второго SA в файл лога выдается предупреждение 1.1 | Создаются два маршрута. |
| 3 | При создании IPsec SA вычисляется маршрут RR, который вступает в конфликт с существующими маршрутами. | Если в таблице есть такой же маршрут (адрес назначения совпадает), маршрут RR не добавляется. В файл лога выдается сообщение 1.4<br>Если есть более приоритетный маршрут, пересекающийся, но не совпадающий с маршрутом RR, то маршрут RR добавляется в таблицу маршрутизации. | Добавляется новый RR маршрут (выбор маршрута при этом строго не определен). |
| 4 | Конфликт с более узкими фильтрами без RRI. | Маршрут создается без учета таких конфликтов, то есть через pass или ipsec фильтр без RRI пакет может уйти не туда. | |
| 5 | При построении IPsec SA в транспортном или туннельном режиме, ID партнера совпадает с туннельным адресом. Маршрут будет как бы рекурсивным – адрес назначения совпадает с адресом шлюза. | Добавляется RR маршрут. | Маршрут не создается. |
| 6 | При попытке создания IPsec SA, | Маршрут RR не добавляется, в | |

| N | Ситуация | Поведение продукта | Отличие в поведении в Cisco IOS |
|---|---|---|---|
| | отсутствует маршрут до туннельного адреса2, например, произошел разрыв соединения. | файл лога выдается диагностика 1.3 | |
| 7 | Рассинхронизация с системной таблицей роутинга, т.е. маршруты для созданных SA не актуальны. | Каждый раз при создании IPsec SA с RRI происходит перезачитывание системной таблицы маршрутизации. Если для вновь создаваемого SA старый маршрут оказывается неправильным, он обновляется (см. 5). Другие, ранее созданные RR маршруты, не проверяются. | |

## Сообщения протоколирования

1. Ошибки, из-за которых не создался RR для SA:

   - Для двух SA с разными селекторами требуются конфликтующие маршруты.

     ```
     [RRI] SA conflicts with the route created for different SA, route not
     created: destination 10.0.16.96, SA selector 10.0.16.61-
     >192.168.1.0..192.168.1.255
     ```

     см. п.2 Таблица 1

   - ID второй фазы не является подсетью.

     ```
     [RRI] SA selector shouldn't have protocols, route not created: destination
     10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255 proto 6
     [RRI] destination part of SA selector shouldn't have ports, route not
     created: destination 10.0.16.96, SA selector 10.0.16.61:32798-
     >192.168.1.6:23 proto 6
     [RRI] destination part of SA selector shouldn't have arbitrary IP range,
     route not created: destination 10.0.16.96, SA selector 10.0.16.61-
     >192.168.1.1..192.168.1.255
     ```

     см. п.1 Таблица 1

   - Нет маршрута до туннельного адреса.

     ```
     [RRI] no route to destination, route not created: destination 10.0.16.96,
     SA selector 10.0.16.61->192.168.1.0..192.168.1.255
     ```

     см. п.6 Таблица 1

     Объяснение: в данном случае в таблице маршрутизации нет маршрута до 10.0.16.96

   - В системной таблице уже есть маршрут, соответствующий SA, но подсистема RRI его не создавала.

     ```
     [RRI] route already exists, route not created: destination 10.0.16.96, SA
     selector 10.0.16.61->192.168.1.0..192.168.1.255
     ```

     см. п.3 Таблица 1

[2] Ситуация экзотическая – маршрут нужен для построения SA. Ошибка возможна, если маршрут удалится в процессе создания SA или из-за ошибки чтения/разбора таблицы роутинга.

- Другие ошибки.

```
[RRI] can't read system routing table, route not created: destination
10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255
```

Объяснение: системная или внутренняя ошибка - не получилось получить таблицу маршрутизации

```
[RRI] can't add route 10.0.0.0/8 via 192.168.1.4: <rtctl err>
```

Объяснение: не удалось добавить маршрут в системную таблицу (системная или внутренняя ошибка). Возможные варианты <rtctl err> см. ниже.

2. Ошибка удаления правила из системной таблицы маршрутизации.

```
[RRI] can't delete route 10.0.0.0/8 via 192.168.1.4: <rtctl err>
```

Объяснение: Ошибки такого типа не приводят к каким-либо дополнительным действиям кроме выдачи данного сообщения. Возможные варианты <rtctl err> см. ниже.

3. Добавление нового RR.

```
[RRI] created route 192.168.1.0/24 via 10.0.135.1 for destination
10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255
```

4. Удаление RR.

```
[RRI] removed route 192.168.1.0/24 via 10.0.135.1 for destination
10.0.16.96
```

Объяснение: выводится при удалении записи из системной таблицы. То есть когда удалены все SA, использующие данный маршрут.

5. Обновление RR.

```
[RRI] updated route to 192.168.1.0/24: new gw 10.0.16.96, old gw 10.0.135.1
```

Объяснение: сообщение выдается, если при создании нового SA обнаружено, что изменилась таблица роутинга и надо обновить ранее созданный RR.

6. Ошибки <rtctl err>.

```
out of memory
syscall error
route not found
route already exists
gateway unreachable
```

# Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза

Если планируется проводить настройки и управлять локальной политикой безопасности шлюза удаленно по протоколу SSH1 или SSH2 при помощи команд консоли, после инициализации S-Terra Gate рекомендуется загрузить начальную конфигурацию, которая позволит в дальнейшем создать защищенный канал для настройки политики безопасности по протоколу SSH.

Загрузка начальной конфигурации на шлюз безопасности должна осуществляться с локального терминала с использованием команд консоли.

Для создания защищенного канала также необходимо на компьютер, с которого будет осуществляться удаленная настройка шлюза, установить продукт S-Terra Client версии 4.1 с согласованной начальной конфигурацией для создания IPsec SA между этим компьютером и шлюзом.

Ниже приведен сценарий настройки начальной конфигурации на шлюзе и удаленном компьютере. Сценарий иллюстрирует построение защищенного соединения между шлюзом безопасности S-Terra Gate (GW1) и компьютером администратора (AdminHost). Адрес компьютера администратора считается заранее неизвестным и может находиться за динамическим NAT-ом. В ходе построения защищенного соединения устройство AdminHost получает адрес из заранее определенного на шлюзе пула. В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6R4.

Схема стенда показана на рисунке ниже.

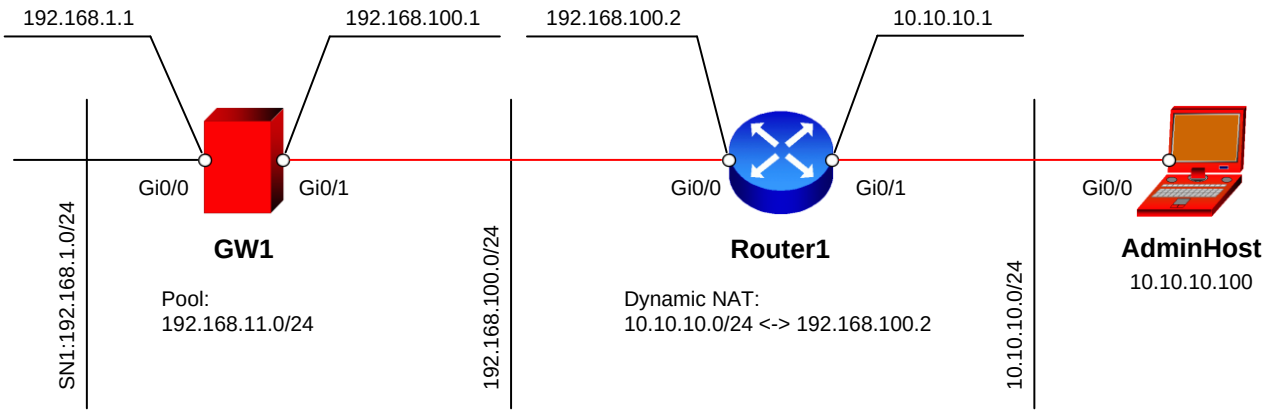



Рисунок 3

Параметры защищенного соединения:

- Аутентификация на сертификатах – GOST R 34.10-2001 Signature;
- IKE параметры:
  - Алгоритм шифрования – GOST 28147-89 Encryption;
  - Алгоритм вычисления хеш-функции – GOST R 34.11-94 Hash;
  - Группа Диффи-Хеллмана – VKO GOST R 34.10-2001;
- IPsec параметры:
  - ESP алгоритм шифрования – ESP_GOST-4M-IMIT cipher.

# Настройка шлюза безопасности GW1

Настройку начните со шлюза безопасности GW1. Все настройки производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Шлюз должен быть предварительно инициализирован.

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен.

## Регистрация CA сертификата (сертификата УЦ)

Для регистрации CA сертификата необходимо выполнить следующие действия:

1. Установите правильное системное время. Например:

   ```
   root@sterragate:~# date 041013152013
   Wed Apr 10 13:15:00 UTC 2013
   ```

   Данная запись соответствует 10 апреля 2013 года 13:15.

2. Создайте папку `/certs`:

   ```
   root@sterragate:~# mkdir /certs >
   ```

3. Доставьте файл CA сертификата на шлюз безопасности в предварительно созданный на нем каталог `/certs`. Для доставки можно воспользоваться утилитой `pscp.exe` из пакета Putty, применив команду:

   ```
   pscp D:\ca.cer root@192.168.1.1:/certs
   …
   Store key in cache? (y/n)
   root@192.168.1.1's password:
   ```

Предупреждение

**Среда передачи в этом случае должна быть доверенной**

4. С помощью утилиты `cert_mgr`, входящей в состав S-Terra Gate, зарегистрируйте сертификат в базе продукта:

   ```
   root@sterragate:~# cert_mgr import -f /certs/ca.cer -t
   1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-CA
   ```

   Параметр `-t` в данной команде указывает на то, что импортируемый сертификат – корневой (сертификат УЦ).

## Регистрация локального сертификата

Перед регистрацией локального сертификата в базе продукта выполните следующие действия:

1. Сформируйте запрос на сертификат с использованием утилиты cert_mgr:

```
root@sterragate:~# cert_mgr create -subj "C=RU,OU=Research,CN=GW1" -
GOST_R3410EL

Press keys...
[.....................................]
-----BEGIN CERTIFICATE REQUEST-----
MIIBCjCBuAIBADAuMQswCQYDVQQGEwJSVTERMA8GA1UECxMIUmVzZWFyY2gx
DDAKBgNVBAMTA0dXMTBjMBwGBiqFAwICEzASBgcqhQMCAiMBBgcqhQMCAh4B
A0MABECTQeB5UoPsTbSs8obnrQ6KMJwpc/BFrUgfI6AjQl95ccE4D5jEAq8m
HB3ZvXfxMsQ/1NAy73OPgaz32W/scOkgoB4wHAYJKoZIhvcNAQkOMQ8wDTAL
BgNVHQ8EBAMCB4AwCgYGKoUDAgIDBQADQQBAuCzk8bASJqbP5pYHAG5A3LKx
OPFjiF1m+2/WkxGkWJWEm5gjNNyWquslmxLq9nX2rff4X3E5xF40iudzHoZz
```

2. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документе «Приложение».
3. Перенесите полученный файл на шлюз безопасности (параметры pscp описаны выше)
4. Зарегистрируйте локальный сертификат в базе продукта, используя утилиту `cert_mgr`:

```
root@sterragate:~# cert_mgr import -f /certs/gw1.cer

1 OK C=RU,OU=Research,CN=GW1
```

5. Убедитесь, что сертификаты импортированы успешно:

```
root@sterragate:~# cert_mgr show

Found 2 certificates. No CRLs found.

1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-
W2008SP1-X64-CA

2 Status: local   C=RU,OU=Research,CN=GW1
```

## Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для шлюза. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль перейдите в директорию `/opt/VPNagent/bin/` и запустите `cs_console`.

```
root@sterragate:~# cs_console
sterragate>en
Password:
```

Пароль по умолчанию: csp.

1. Перейдите в режим настройки:

```
sterragate#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Смените пароль по умолчанию:

```
sterragate(config)#username cscons password <пароль>
```

3. Смените название шлюза:

```
sterragate(config)#hostname GW1
```

4. В настройках интерфейсов задайте ip-адреса:

```
GW1(config)#interface GigabitEthernet 0/0
GW1(config-if)#ip address 192.168.1.1 255.255.255.0
GW1(config-if)#no shutdown
GW1(config-if)#exit
GW1(config)#interface GigabitEthernet 0/1
GW1(config-if)#ip address 192.168.100.1 255.255.255.0
GW1(config-if)#no shutdown
GW1(config-if)#exit
```

5. Задайте адрес шлюза по умолчанию:

```
GW1(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

6. Задайте тип идентификации:

```
GW1(config)#crypto isakmp identity dn
```

7. Задайте параметры для IKE:

```
GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)#hash gost
GW1(config-isakmp)#encryption gost
GW1(config-isakmp)#authentication gost-sig
GW1(config-isakmp)#group vko
GW1(config-isakmp)#exit
```

8. Создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-gost28147-4m-imit
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

9. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа. В списке доступа разрешите ssh трафик:

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit tcp host 192.168.100.1 eq 22 any
GW1(config-ext-nacl)#exit
```

10. Создайте список доступа, в котором будет запрещено прохождение любого трафика, кроме ssh:

```
GW1(config)#ip access-list extended LIST2
GW1(config-ext-nacl)#permit tcp host 192.168.100.1 eq 22 any
GW1(config-ext-nacl)#permit udp host 192.168.100.1 eq 4500 any
GW1(config-ext-nacl)#permit udp host 192.168.100.1 eq 500 any
GW1(config-ext-nacl)#deny   ip any any
GW1(config-ext-nacl)#exit
```

11. Опишите требования, которым должен удовлетворять сертификат партнера (администратора):

```
GW1(config)#crypto identity my_admin
GW1(config-crypto-identity)#dn C=RU,L=Moscow,O=S-Terra
CSP,OU=Research,CN=adminhost
GW1(config-crypto-identity)#exit
```

Команда crypto identity my_admin в данном случае описывает сертификат электронной подписи пользователя, только с которым будет возможно установление соединения для обработки трафика, описанного в листе доступа LIST.

12. Создайте динамическую крипто-карту:

```
GW1(config)#crypto dynamic-map DMAP 1
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs vko
GW1(config-crypto-map)#set identity my_admin
GW1(config-crypto-map)#reverse-route
GW1(config-crypto-map)#exit
```

13. Привяжите динамическую карту к статической:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp dynamic DMAP
```

14. Привяжите крипто-карту к интерфейсу, на котором будет туннель. Так же привяжите к интерфейсу список доступа, который запрещает остальной трафик:

```
GW1(config)#interface GigabitEthernet 0/1
GW1(config-if)#crypto map CMAP
GW1(config-if)#ip access-group LIST2 out
GW1(config-if)#exit
```

15. Отключите обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-terra_technological_trustpoint
GW1(ca-trustpoint)#revocation-check none
GW1(ca-trustpoint)#exit
```

16. Настройка устройства GW1 завершена. При выходе из конфигурационного режима происходит загрузка конфигурации.

```
GW1(config)#end
GW1#exit
```

В Приложении представлен текст cisco-like конфигурации и текст LSP для шлюза GW1.

## Настройка рабочего места администратора AdminHost

Настройка рабочего места администратора состоит из нескольких этапов:

- получение сертификатов и секретных ключей;
- формирование инсталляционного пакета S-Terra Client для AdminHost;
- установка «КриптоПро CSP» на AdminHost;
- установка инсталляционного пакета S-Terra Client на AdminHost.

На компьютере, где будет создаваться инсталляционный пакет для AdminHost, должен быть установлен пакет «КриптоПро CSP» и административный пакет S-Terra Client AdminTool (см. документацию «Программный комплекс С-Терра Клиент. Руководство администратора»).

В случае если ключи были сгенерированы вне целевого компьютера, их требуется туда доставить защищенным образом (например, на токене).

Процесс получения сертификата и доставки секретных ключей описан в документе «Программный комплекс С-Терра Клиент. Руководство администратора. Приложение А».

Запустите графический интерфейс S-Terra Client AdminTool (`Start – Programs – S-Terra Client AdminTool – Package Maker`) и создайте, согласованную со шлюзом политику безопасности.

1. Во вкладке `Auth` (Рисунок 4) выполните следующие действия:
   - в данном сценарии используется метод аутентификации на сертификатах – пункт `Use certificate` выбран по умолчанию;
   - укажите путь к сертификату УЦ и пользовательскому сертификату;
   - отметьте пункт `Check consistency now` и нажмите кнопку …, где выберите нужный контейнер; если при генерации сертификатов указывался пароль на контейнер, введите его в графе `password`;
   - отметьте пункт `Copy container` и скопируйте имя контейнера из `Container name` в `Source container name`; если при генерации сертификатов указывался пароль на контейнер, введите его в `password`;
   - задайте имя контейнера в графе `User container name`; в данном случае указано – `\\.\REGISTRY\Adminhost`. Данная запись означает, что контейнер с переносного устройства (токен или USB Flash) будет скопирован в реестр с именем `Adminhost`.
   - в графе `User identity type` выберите `DistinguishedName` (выбрано по умолчанию).

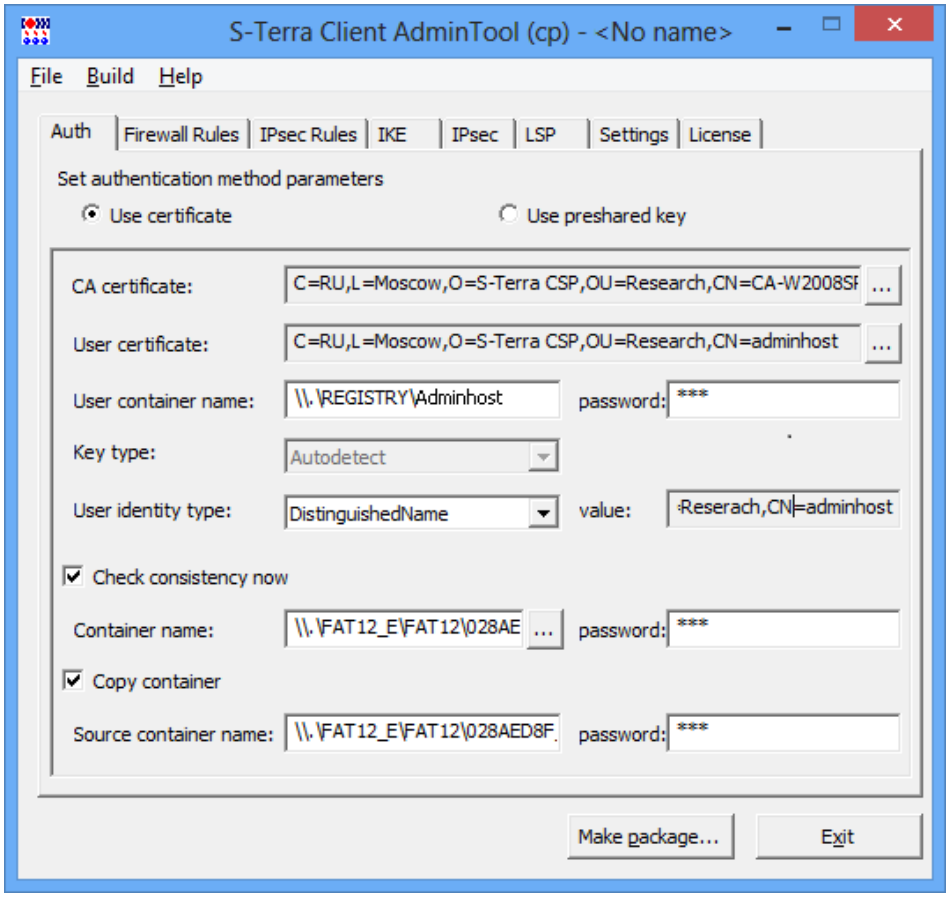



Рисунок 4

2. Во вкладке `Firewall Rules` (Рисунок 5) можно настроить правила фильтрации трафика. В данном сценарии оставим настройки по умолчанию – разрешать весь трафик.

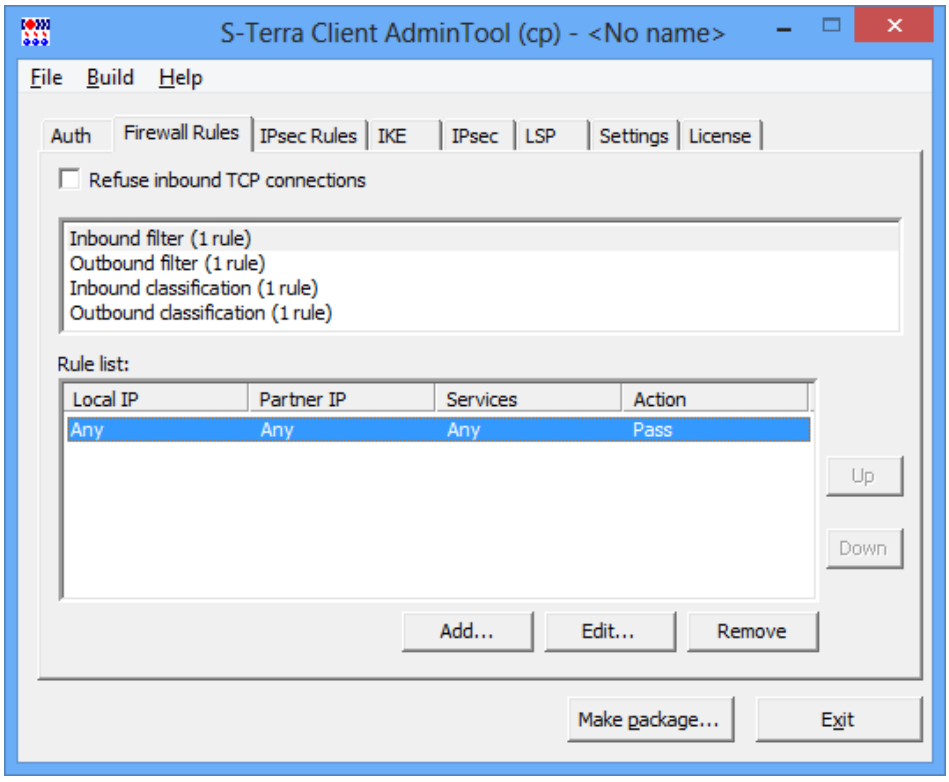



Рисунок 5

3. Во вкладке `IPsec Rules` (Рисунок 6) добавьте правило для трафика, подлежащего шифрованию, IP-адрес шлюза, с которым будет построено защищенное соединение (Рисунок 7). Так же разрешите только SSH-трафик.

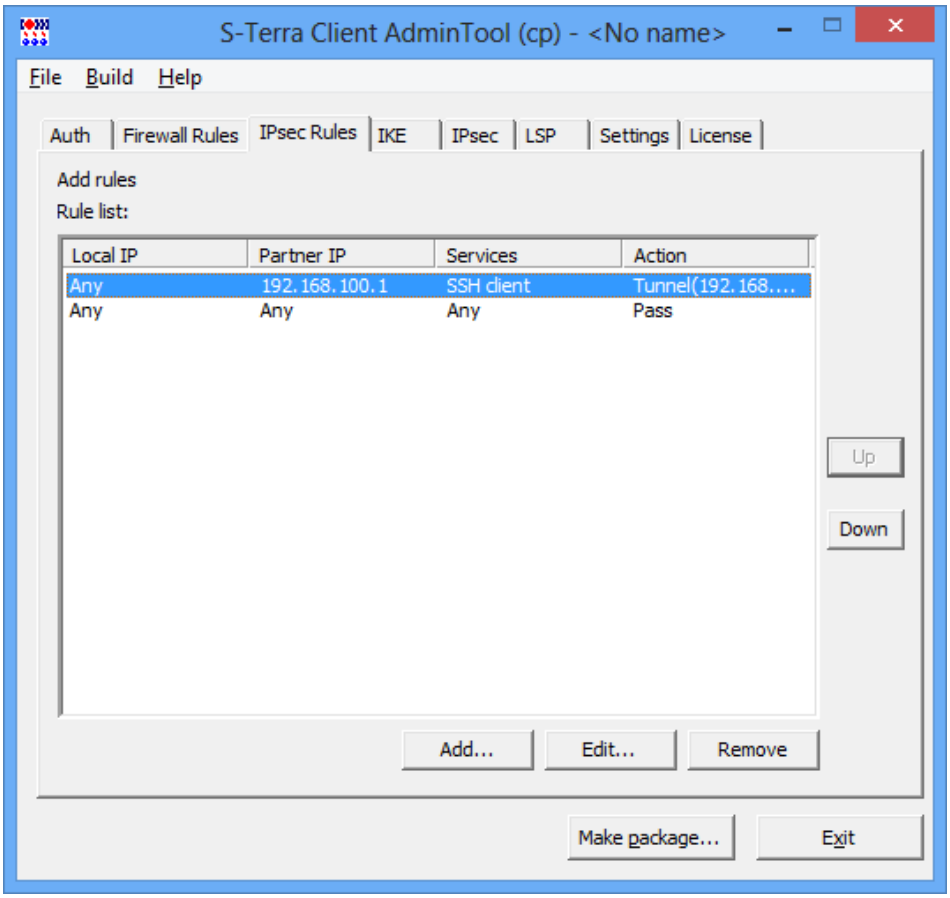



Рисунок 6

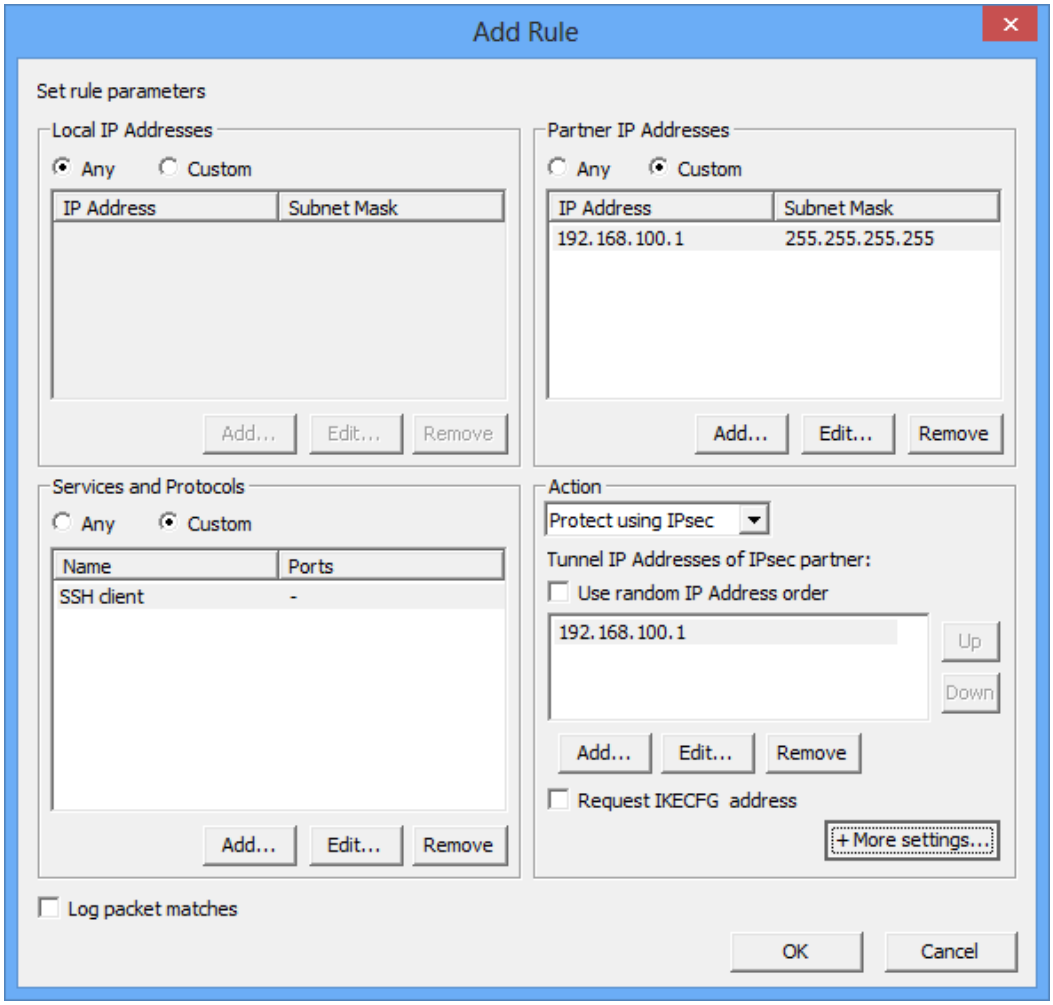



Рисунок 7

Закройте окно `Add Rule`.

На вкладке `IPsec Rules` повысим приоритет созданного правила, нажимая кнопку `Up` (Рисунок 6).

4. Во вкладке `IPsec` поднимите вверх правило, соответственно настроенному на шлюзе IPsec Transform Set и выберете `Group` – `VKO_1B` (Рисунок 8).

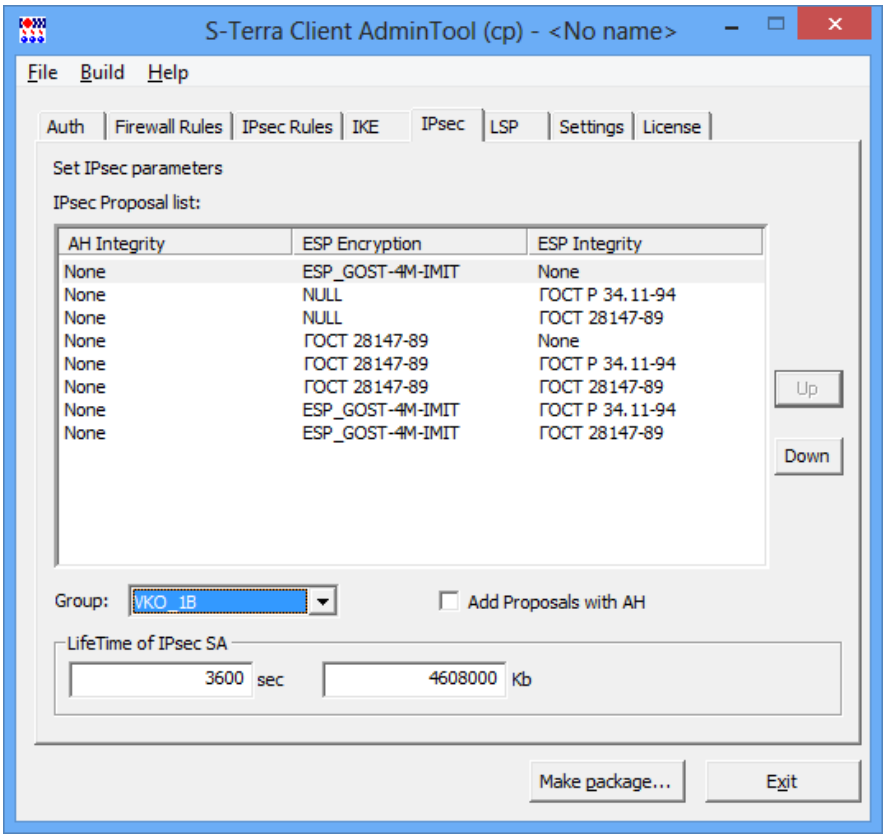



Рисунок 8

5. Во вкладке `License` введите регистрационные данные на продукт S-Terra Client с бланка Лицензии.
6. Сохраните файл созданного проекта, на тот случай, если захотите в будущем сделать похожий инсталляционный пакет. Для этого нажмите `File->Save Project`
7. Далее сгенерируйте инсталляционный exe-файл, нажав кнопку `Make package…`
8. Вставьте в целевой компьютер AdminHost носитель с секретными ключами и установите на нем полученный инсталляционный exe-файл. Перегрузите компьютер (на операционных системах Windows 7 и Windows 8 перезагрузка не требуется).

В Приложении представлен текст LSP.

## Настройка устройства Router1

На устройстве необходимо настроить динамический NAT, который будет преобразовывать адреса из подсети 10.10.10.0/24 во внешний адрес 192.168.100.2 и наоборот.

## Проверка работоспособности стенда

После того, как настройка GW1 и AdminHost завершена, инициируйте создание защищенного соединения.

На рабочем компьютере администратора зайдите на шлюз при помощи SSH:

В результате выполнения этой команды между устройствами GW1 и AdminHost будет установлен VPN туннель.

Убедиться в этом можно на мобильном клиенте, выбрав предложение `Show SA Information` (Рисунок 9), (Рисунок 10):

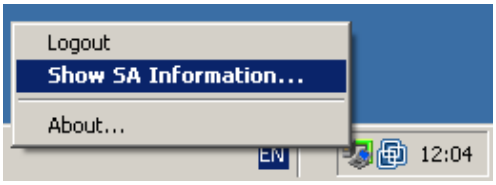



Рисунок 9

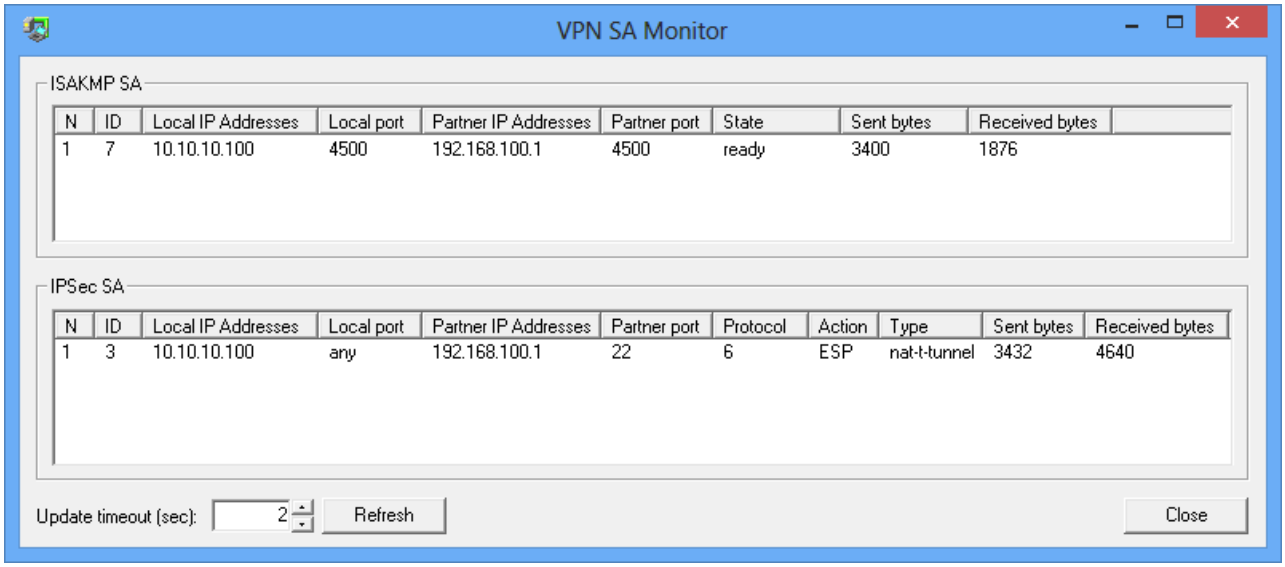



Рисунок 10

Так же в этом можно убедиться на устройстве GW1, выполнив команду:

```
root@GW1:~# sa_mgr show
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 13 (192.168.100.1,4500)-(192.168.100.2,4500) active 1876 3400

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 3 (192.168.100.1,22)-(10.10.10.100,*) 6 ESP nat-t-tunn 4640 3432
```

В то же время ping проходить не будет:

```
ping 192.168.100.1
Обмен пакетами с 192.168.100.1 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.100.1:
    Пакетов: отправлено = 3, получено = 0, потеряно = 3
    (100% потерь)
```

На шлюзе GW1 данные пакеты будут отбрасываться, данное действие можно увидеть, выполнив команду:

```
root@GW1:~# klogview -f drop
dropped out packet 192.168.100.1->192.168.100.2, proto 1, len 60, if eth1:
firewall
dropped out packet 192.168.100.1->192.168.100.2, proto 1, len 60, if eth1:
firewall
dropped out packet 192.168.100.1->192.168.100.2, proto 1, len 60, if eth1:
firewall
```

Таким образом был создан доверенный сеанс, по которому администратор может удаленно настраивать шлюз безопасности.

# Создание политики безопасности шлюза

В данном разделе рассмотрены основные принципы создания политики безопасности S-Terra Gate и даны лишь общие понятия. Более подробное описание дано в соответствующих документах, в зависимости от выбранного способа настройки шлюза.

# Способы создания политики безопасности

Настроить шлюз безопасности S-Terra Gate или создать политику безопасности для шлюза возможно:

- Локально или удаленно по протоколу SSH с использованием команд интерфейса командной строки, описанных в документе «Cisco-like команды» (такую конфигурацию будем называть «cisco-like конфигурацией»). Написанные команды являются родственными Cisco IOS 12.4 (13a).
- Создав текстовый конфигурационный файл и загрузив его на ПАК с помощью специализированных команд. Создание такого файла описано в документе «Создание конфигурационного файла» (такую конфигурацию будем называть «native-конфигурацией» или «LSP-конфигурацией»). Команды, при помощи которых можно загрузить конфигурационный файл, описаны в документе «Специализированные команды».
- Централизованно–удаленно с помощью графического интерфейса Cisco Security Manager (CSM), описанного в документе «Настройка S-Terra Gate с помощью Cisco Security Manager».
- Централизованно–удаленно с использованием продукта «С-Терра КП», предназначенного для управления всей линией продуктов, производимых компанией «С-Терра СиЭсПи», и описанного в документе «Программный продукт С-Терра КП. Руководство администратора».

# Сценарии создания политики безопасности шлюза

Рассмотрим некоторые **команды интерфейса командной строки** и аналогичные им по функциональности **структуры текстового конфигурационного файла**, которые используются при создании локальной политики безопасности шлюза.

Подробный список команд и их описание дано в документе «Cisco-like команды». Описание синтаксиса и структур данных конфигурационного файла приведено в документе «Создание конфигурационного файла».

## Фильтрация, классификация и маркирование пакетов

Порядок обработки пакетов зависит от направления трафика. Для исходящего трафика порядок обработки следующий: маркирование, инкапсуляция, пакетная и контекстная фильтрация. Для входящего трафика – пакетная и контекстная фильтрация, декапсуляция, маркирование трафика.

### Создание правил пакетной фильтрации

Создание правил пакетной фильтрации состоит из формирования списков доступа и привязывания их к конкретным интерфейсам аппаратной платформы S-Terra или сетевого модуля MCM/MCM-950.

В интерфейсе командной строки с помощью команды ***ip access-list*** создаются листы доступа.

Команда ***ip access-list*** осуществляет вход в режим редактирования списков доступа. В этом режиме с помощью команд ***permit*** и ***deny*** формируются списки доступа.

В конфигурационном файле правила пакетной фильтрации создаются в структуре ***Filter***.

### Создание правил контекстной фильтрации

В интерфейсе командной строки для создания правил контекстной фильтрации используются следующие команды:

- Команда ***ip port-map***, служит для ассоциации протоколов (сервисов) прикладного уровня с номерами TCP-портов и позволяет перенаправлять трафик стандартных (системных) протоколов и пользовательских, заданных пользователем, на любой TCP-порт.
- Команда ***ip inspect name*** применяется для создания правила проверки трафика для протоколов прикладного уровня.
- Команды ***ip inspect tcp synwait-time, ip tcp finwait-time, ip inspect tcp idle-time, ip inspect max-incomplete hight, ip inspect max-incompletelow, ip inspect one-minute hight. Ip inspect one-minute low*** являются командами управления состоянием сеансов в системе CBAC (управление доступом на основе контекста).

В конфигурационном файле правила контекстной фильтрации задаются в структурах ***Filter*** и ***FirewallParameters***.

### Классификация и маркирование пакетов

Классификация и маркирование будет производиться до IPsec-инкапсуляции исходящих пакетов и после декапсуляции входящих.

Описанные ниже команды позволяют задать определенный сервис обслуживания сетевого трафика. Они классифицируют пакеты (относят пакеты к определенному классу трафика) и маркируют их (назначают соответствующий приоритет). Формирование трафика выполняется в три шага:

- пакеты распределяются по классам (команды ***class-map***)
- задаются правила для каждого класса (команды ***policy-map***)
- заданная политика привязывается к интерфейсу (команды ***service-policy***).

В конфигурационном файле классификация и маркирование пакетов задается в структурах ***Filter***, которые привязываются к описаниям сетевых интерфейсов (***NetworkInterface***) через поля ***InputClassification*** и ***OutputClassification***.

## Создание защищенных VPN туннелей

### Создание политики IKE

Для создания защищенного канала, который будет обеспечивать защиту части обменов информацией первой фазы и все обмены второй фазы IKE, создаются ISAKMP политики (или одна политика) с разными приоритетами, которые будут предложены партнеру для согласования. В политиках описываются желаемые алгоритмы и параметры защищенного канала.

Перед созданием ISAKMP SA должны быть выбраны параметры, которые будут использоваться сторонами для защиты части обменов первой фазы и второй фазы IKE. В интерфейсе командной строки с помощью команды ***crypto isakmp policy*** задаются IKE политики (или одна политика) с различными приоритетами, которые будут предложены партнеру для согласования. Выполнение этой команды осуществляет вход в режим ISAKMP

policy configuration, в котором предлагаются параметры для согласования с помощью следующих команд:

- ***authentication*** – указывается метод аутентификации (с использованием электронной подписи или предопределенных ключей);
- ***encryption*** – указывается алгоритм шифрования, используемый в рамках протокола IKE;
- ***hash*** – указывается хэш-алгоритм, используемый в рамках протокола IKE;
- ***lifetime*** – устанавливается время жизни ISAKMP SA;
- ***group*** – указывается алгоритм, который будет использоваться в рамках протокола IKE для получения ключевого материала.

В конфигурационном файле в структуре ***IKERule*** задается метод аутентификации сторон, режим для первой фазы IKE, а также предлагается для согласования с партнером политика защиты первой и второй фазы IKE, которая описывается в структуре ***IKETransform***. Структура ***IKEParameters*** описывает глобальные настройки протокола IKE.

## Создание IPsec наборов преобразований

Далее нужно предложить партнеру для согласования наборы преобразований, которые будут использоваться для создания защищенного виртуального соединения (IPsec SA). IPsec SA – это однонаправленное логическое соединение, поэтому при двустороннем обмене данными нужно установить два IPsec SA.

В интерфейсе командной строки с помощью команды ***crypto ipsec transform-set*** описать параметры IPsec наборов преобразований (или одного набора преобразований). Можно указать до трех наборов преобразований.

С помощью команды ***mode*** указать режим использования (туннельный или транспортный) для заданного набора преобразований.

В конфигурационном файле структура ***IPsecAction*** определяет режим использования IPsec, список предлагаемых наборов преобразований IPsec. Каждое преобразование описывается в структурах ***AHTransform*** и ***ESPTransform***.

## Создание списков доступа

В интерфейсе командной строки с помощью команды ***ip access-list*** указываются списки доступа, в которых задается трафик, который будет потом просто пропускаться, защищаться или запрещаться. Для создания защищенных туннелей используются только расширенные списки доступа.

Команда ***ip access-list*** с параметром extended осуществляет вход в режим config-ext-nacl (режим редактирования расширенных списков доступа). В этом режиме с помощью команд ***permit*** и ***deny*** формируются списки доступа.

В конфигурационном файле списками доступа являются правила фильтрования, описываемые структурой ***Filter***.

## Создание криптографических карт

В интерфейсе командной строки создание политики IPsec выполняется с помощью команды ***crypto map***, которая осуществляет переход в режим настройки криптографических карт. В этом режиме могут использоваться следующие команды:

- ***match address*** осуществляет привязку списка доступа к записи криптографической карты;
- ***set peer*** определяет партнера, с которым будем устанавливаться туннель;
- ***set pfs*** задает режим pfs, позволяющий повысить уровень защищенности трафика;
- ***set pool*** указывает имя пула адресов для криптографической карты;
- ***set identity*** задает идентификатор для криптографической карты;
- ***set security-association lifetime*** устанавливает время жизни IPsec SA;
- ***set transform-set*** дает ссылку на ранее созданный трансформ или трансформы (определяет параметры туннеля);
- ***set ip access-group*** устанавливает правила фильтрации, применяемые к входящим IPsec пакетам после декапсуляции, или к исходящим IPsec пакетам до инкапсуляции.

Создание набора динамических криптографических карт в интерфейсе командной строки осуществляется командой ***crypto dynamic map***.

В конфигурационном файле политика IPsec задается в структуре ***IPsecAction***.

### Привязка криптографической карты к интерфейсу

В интерфейсе командной строки на последнем этапе производится привязка листов доступа и криптографических карт к конкретным интерфейсам аппаратной платформы. Эти операции производятся в режиме настройки интерфейсов.

Команда ***interface*** с указанием логического имени интерфейса осуществляет переход в режим настройки данного интерфейса.

В этом режиме командой ***ip access-group*** указываем список доступа для правил пакетной фильтрации, которые будут использоваться на этом интерфейсе.

Командой ***crypto map*** указываем криптографическую карту, с помощью которой будут создаваться VPN туннели.

В конфигурационном файле для привязки правила фильтрования к интерфейсу аппаратной платформы используется атрибут ***IPsecPolicy*** в структуре ***NetworkInterface***.

## Настройка маршрутизации

Добавление строки в таблицу маршрутизации в интерфейсе командной строки задается командой ***ip route*** с указанием адреса и маски подсети назначения пакета, IP-адреса следующего маршрутизатора либо выходного интерфейса локального устройства, на который нужно передать пакет для передачи его далее по сети к получателю пакета.

В конфигурационном файле создание таблицы маршрутизации осуществляется структурой ***RoutingTable***. Строка, которая добавляется в таблицу маршрутизации, задается в структуре ***Route***. Эта строка задает маршрут, указывая адрес назначения, выходной интерфейс либо IP-адрес следующего маршрутизатора и метрику маршрута.

## Настройка Syslog-клиента

Настройка Syslog-клиента в cisco-like конфигурации и LSP-конфигурации подробно описана в документе «Протоколирование событий».

## Настройка SNMP

Для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP в интерфейсе командной строки используются три команды. Команда ***snmp-server community*** задает строку, которая играет роль пароля при аутентификации сообщений SNMP и разрешает SNMP-менеджеру чтение статистики из базы управления SNMP-агента. Команда ***snmp-server location*** содержит информацию о физическом расположении SNMP-агента. В команде ***snmp-server contact*** указывается лицо, ответственное за работу SNMP-агента.

В конфигурационном файле задание настроек SNMP-агента осуществляется в структуре ***SNMPPollSettings***. В этой структуре указывается IP-адрес и порт, на который можно получать запросы от SNMP-менеджера, а также строку, играющую роль пароля при аутентификации сообщений, размещение SNMP-агента и контактное лицо. В документе «Мониторинг» описаны переменные, которые могут быть запрошены у SNMP-агента.

Настройка отсылки трапов SNMP-агента производятся в структурах ***SNMPTrapSettings*** и ***TrapReceiver***. В этих структурах указывается IP-адрес и порт, на который отсылаются трап-сообщения, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой создаются трап-сообщения.

# Загрузка политики безопасности

Созданную политику безопасности необходимо загрузить на шлюз.

**Cisco-like конфигурация** сама загружается на шлюз после выхода из конфигурационного режима, при этом она будет интерпретирована конвертером в LSP-конфигурацию. Конвертор работает в рамках программы cs_console.

Если конвертирование конфигурации завершается с ошибкой; то на консоль выдается сообщение об ошибке: "LSP conversion failed. You can use the "show load-message" command to obtain the additional information." ("Конвертирование LSP завершилось с ошибкой. Вы можете использовать команду show load-message для получения дополнительной информации.")

Далее происходит попытка загрузки LSP-конфигурации на шлюз безопасности. Если по каким-либо причинам произошла ошибка при загрузке, LSP-конфигурация записывается в файл erroneous_lsp.txt, расположенный в каталоге шлюза безопасности. В конце работы конвертора выдается результат (успех/неуспех) обратно в cs_console.

При конвертировании cisco-like конфигурации прописываются фильтры для каждого интерфейса в отдельности.

Во время работы конвертора используются настройки конвертора, некоторые из которых могут редактироваться пользователем. Подробно работа конвертора описана в документе «Программный комплекс С-Терра Шлюз. Версия 4.1. Приложение» в разделе «Конвертор».

**LSP-конфигурацию,** созданную в виде текстового конфигурационного файла, нужно загрузить специализированной командой lsp_mgr load, с указанием полного пути к файлу конфигурации.

**Политики безопасности, созданные с использованием остальных платформ управления**, также конвертируются в LSP-конфигурацию во время загрузки на шлюз.

Для просмотра загруженной конфигурации используется специализированная команда lsp_mgr show.

# Работа с сертификатами

## Регистрация CA сертификата

Зарегистрировать CA сертификат в базе Продукта можно двумя способами:

- с помощью утилиты командной строки ***cert_mgr import***;
- через cs_console командами ***crypto pki trustpoint*** и ***crypto pki certificate chain***.

При регистрации сертификата первым способом при первом старте консоли после добавления сертификатов, добавленные сертификаты будут доступны для использования в cisco-like конфигурации. Для них будет создан *trustpoint* с именем *s-terra technological trustpoint*.

Для регистрации CA сертификата через cs_console используются команды:

- ***crypto pki trustpoint*** *name* – для объявления имени CA и входа в режим *ca trustpoint configuration*, можно задать несколько таких команд для объявления разных trustpoint.

  В режиме этой команды можно указать адрес LDAP-сервера и режимы использования CRL при проверке сертификатов:

  - ***crl query*** *ldap://IP-адрес(:порт)* – задает адрес LDAP-сервера. При обращении к LDAP-серверу шлюз безопасности сначала смотрит поле CDP сертификата, если в этом поле прописанный путь к LDAP-серверу является неполным, то добавляются данные (IP-адрес и порт) из команды *crl query*. Если CDP содержит полный путь, *crl query* не используется. Если в сертификате нет поля CDP, то используется эта команда для задания *url* LDAP.
  - ***revocation-check*** *method1 [method2]*
    - method1 – параметр, принимающий одно из двух значений:
      - *crl* – при проверке сертификата обязателен действующий CRL. Если действующий CRL не найден в базе продукта и его не удалось получить по протоколу LDAP, то сертификат не принимается;
      - *none* – при проверке сертификата действующий CRL используется, если он предустановлен в базе продукта или получен в процессе IKE обмена. Если это не так, то попытка получить CRL по протоколу LDAP не предпринимается и сертификат принимается.
    - method2 – параметр необязательный, имеет одно значение:
      - *none* – если действующий CRL не найден в базе продукта и его не удалось получить по протоколу LDAP, то сертификат принимается. Используется только тогда, когда *method1= crl*.
- ***crypto pki certificate chain*** *name* – для входа в режим настройки цепочки сертификатов CA:
  - *certificate* – для добавления CA сертификата (в шестнадцатеричном представлении) в базу Продукта:
  - можно задать несколько таких команд для добавления либо промежуточных CA сертификатов, либо любых CA сертификатов.

В отличие от Cisco, наш Продукт не проверяет являются ли добавляемые сертификаты из одной цепочки. Поэтому, можно добавлять в один *trustpoint* не только промежуточные CA сертификаты, но вообще любые CA сертификаты.

При добавлении CA сертификата в *trustpoint* командой *crypto pki certificate chain* он автоматически добавляется в базу Продукта.

При старте cs_console при поиске сертификата проверяются все существующие *trustpoint's* в базе Продукта. В случае отсутствия соответствующего CA сертификата в базе Продукта,

*trustpoint* автоматически удаляется из cisco-like конфигурации и, следовательно, удаляются все CA сертификаты, зарегистрированные в этом *trustpoint*. При этом выдается соответствующее сообщение в лог.

## Создание ключевой пары и запроса на локальный сертификат

Создать ключевую пару и запрос на локальный сертификат для S-Terra Gate можно двумя путями:

- Локально с помощью утилиты ***cert_mgr create***. В случае применения СКЗИ от компании S-Terra CSP можно также воспользоваться утилитами ***cont_mgr create*** и ***cont_mgr request*** (утилиты расположены в /opt/VPNagent/bin/).
- На отдельном компьютере с помощью средств MS Windows и СКЗИ, как описано в документе «Программный комплекс С-Терра Шлюз. Версия 4.1. Приложение».

Контейнеры с секретными ключами должны быть уровня компьютера.

## Регистрация локального сертификата

Для регистрации локального сертификата в базе Продукта используется утилита командной строки *cert_mgr import*.

## Удаление сертификатов

Удалять сертификаты из базы Продукта можно двумя способами:

- с помощью утилиты командной строки ***cert_mgr remov***;
- через cs_console командой ***no crypto pki trustpoint***.

При удалении *trustpoint* с указанным именем, все CA сертификаты из этого *trustpoint* удаляются из текущей конфигурации, базы Продукта и cisco-like конфигурации.

Если в cs_console добавить сертификат в *trustpoint,* а потом, выйдя из консоли, удалить добавленный сертификат с помощью *cert_mgr remove*, то при следующем старте консоли *trustpoint* с сертификатом удалится и оттуда.

Удалить CRL из базы Продукта помощью утилиты командной строки ***cert_mgr remove*** невозможно. Если в команде указать номер (индекс) CRL, то будет выведено сообщение об ошибке – о недопустимом индексе.

## Просмотр сертификатов в базе Продукта

Для просмотра сертификатов в базе Продукта используйте команду ***cert_mgr show***.

## Отсылка локального сертификата

Для отсылки локального сертификата партнеру по протоколу IKE:

**В LSP-конфигурации (конфигурационный файл)**

Для отсылки локального сертификата партнеру по протоколу IKE в LSP, в структуре ***AuthMethodGOSTSign*** задать атрибут ***SendCertMode*** со значением:

- *ALWAYS* – всегда отсылать локальный сертификат;
- *CHAIN* – всегда отсылать локальный сертификат, CA сертификат и промежуточные CA сертификаты.

**В cisco-like конфигурации (в интерфейсе командной строки)**

При создании политики IKE, параметры которой согласовываются с партнером, в режиме команды ***crypto isakmp policy*** задать метод аутентификации сторон с использованием сертификатов командой

***authentication rsa-sig***

В файле настроек конвертора cs_conv.ini параметру *send_cert* присвоено значение *ALWAYS*, и поэтому по умолчанию партнеру всегда будет отсылаться локальный сертификат по протоколу IKE.

## Получение сертификата партнера

Сертификат партнера можно получить либо по протоколу IKE, либо по протоколу LDAP.

Сначала S-Terra Gate пытается получить сертификат партнера по IKE. Если партнер не прислал сертификат, а прислал свой идентификатор, то S-Terra Gate по этому идентификатору ищет сертификат партнера сначала в своей базе Продукта, если не нашел, то продолжает поиск на LDAP-сервере.

## Получение сертификата партнера по IKE

Для получения сертификата партнера по протоколу IKE нужно:

**В LSP-конфигурации**

- В локальной конфигурации в структуре *AuthMethodGOSTSign* задать атрибут *SendRequestMode* со значением *ALWAYS* – всегда запрашивать сертификат партнера.
- В конфигурации партнера в структуре *AuthMethodGOSTSign* задать атрибут *SendCertMode* со значением:
  - *ALWAYS* – высылать сертификат;
  - *CHAIN* – высылать локальный сертификат, CA сертификат с цепочкой промежуточных CA.

**В cisco-like конфигурации**

В режиме команды ***crypto isakmp policy*** задать метод аутентификации сторон с использованием сертификатов командой:

***authentication rsa-sig***

В файле настроек конвертора ***cs_conv.ini*** параметру *send_request* присвоено значение *ALWAYS*, и поэтому по умолчанию у партнера всегда будет запрашиваться локальный сертификат по протоколу IKE.

## Получение сертификата партнера по LDAP

Получение сертификата партнера на LDAP-сервере. В этом случае партнер присылает свой идентификатор, а S-Terra Gate по значению Subject будет искать сертификат партнера на LDAP-сервере. Для прохождения LDAP-пакетов до LDAP-сервера необходимо в политике задать соответствующий фильтр.

**В LSP-конфигурации**

В локальной конфигурации задать структуру ***LDAPSettings*** с IP-адресом LDAP-сервера и также:

- Если прислан идентификатор типа DN:
  - шлюз безопасности по Subject ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере;

- Если прислан идентификатор другого типа:
  - для получения Subject в локальной конфигурации задаются атрибуты *RemoteID, RemoteCredential, DoNotMapRemoteIDToCert*;
  - если *DoNotMapRemoteIDToCert = TRUE*, то Subject будет составляться из *RemoteCredential*;
  - если *DoNotMapRemoteIDToCert = FALSE*, то Subject будет составляться из *RemoteCredential u RemoteID*;
  - по составленному значению Subject шлюз безопасности ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере.

**В cisco-like конфигурации**

Если партнер не прислал свой сертификат по протоколу IKE, и в базе Продукта его нет, то S-Terra Gate посылает запрос на заданный LDAP-сервер в команде ***crl query*** для получения сертификата партнера. По полученному идентификатору типа *dn* от партнера будет осуществляться поиск сертификата. Если получен идентификатор другого типа – запрос на LDAP-сервер не посылается. Если отредактировать сконвертированную native-конфигурацию для работы с идентификаторами другого типа, как описано в предыдущем пункте, то сертификат партнера можно получить по LDAP.

## Проверка сертификата по CRL

Для проверки сертификата партнера по списку отозванных сертификатов (CRL) нужно:

**В LSP-конфигурации**

В структуре GlobalParameters задать атрибут ***CRLHandlingMode***, при значениях этого атрибута:

- *optional* – используется действующий CRL из базы Продукта;
- *enable* и *best_effort* – действующий CRL может быть получен по LDAP.

Для получения CRL с LDAP-сервера сначала проверяется поле CDP в проверяемом сертификате, если поле CDP отсутствует, то в конфигурации должна быть задана структура ***LDAPSettings*** с адресом LDAP-сервера. В базу Продукта с LDAP-сервера загружается действующий CRL и по нему проверяется сертификат партнера.

Для прохождения LDAP-пакетов до LDAP-сервера необходимо в политике задать соответствующий фильтр.

**В cisco-like конфигурации**

В режиме команды *crypto pki trustpoint* командой ***revocation-check*** задается режим использования CRL.

## Несколько локальных и CA сертификатов

Иногда при работе с разными партнерами аутентификация осуществляется с использованием разных локальных сертификатов, подписанных разными УЦ, соответственно и CA сертификаты разные.

**В cisco-like конфигурации**

В командной строке нет команд для указания соответствия между идентификатором партнера, локальным сертификатом и CA сертификатом. Поэтому после конвертирования cisco-like конфигурации в LSP конфигурацию последнюю необходимо отредактировать.

**В LSP-конфигурации:**

В структуре *AuthMethodGOSTSign* существуют атрибуты, которые позволяют задать соответствие между локальным, партнерским и CA сертификатами, локальным и партнерским идентификаторами.

# Расширения сертификата (Certificate Extensions)

Имеются некоторые ограничения при работе с расширениями сертификата (Extensions), которые помечены как критичные. В таблице приведен список расширений сертификата, которые будут распознаваться и обрабатываться Продуктом, если у них установлен признак критичности TRUE. Если в сертификате будут присутствовать другие расширения, не указанные в таблице и заданные как критичные, то такой сертификат не может быть использован. Если же расширение отсутствует в таблице, но является некритичным, то оно игнорируется, и сертификат используется.

Таблица 2

| Name | OID value |
|---|---|
| Subject Key Identifier | 2.5.29.14 |
| Key Usage | 2.5.29.15 |
| Subject Alternative Name | 2.5.29.17 |
| Issuer Alternative Name | 2.5.29.18 |
| Basic Constraints | 2.5.29.19 |
| Name Constraints | 2.5.29.30 |
| CRL Distribution Points | 2.5.29.31 |
| Authority Key Identifier | 2.5.29.35 |

Описания значений и полный список Certificate Extensions можно посмотреть в документе RFC 5280 (http://tools.ietf.org/html/rfc5280#section-4.2).

Можно изменить реакцию Продукта на отдельные расширения сертификата, помеченные как критичные и отсутствующие в вышеприведенной таблице. Администратор может настроить список расширений сертификата, который будут игнорироваться Продуктом, как если бы эти расширения являлись некритичными. Эти расширения надо описать в файле `x509opts.ini`, который расположен в каталоге `/opt/VPNagent/etc`. Расширения описываются в секции `IgnoringUnsupportedCriticalExtentions`.

Игнорируемое `Critical Extention` задается в формате `<KEY>=<OID>`, где:

`<KEY>` – имя расширения, состоящее из букв и цифр и не содержащее разделителей, должно быть уникальным в передах секции;

`<OID>` – OID игнорируемого расширения, состоящий из десятичных чисел, разделенных точками. Распознавание расширения происходит по OID.

Пример файла `x509opts.ini`:

```
[IgnoringUnsupportedCriticalExtentions]
!!
! Key name is any Alpha-Numerical well-known name of OID
! Key names of different OIDs cannot match
!!
```

```
subjectDirectoryAttributes=2.5.29.9
CertificatePolicies=2.5.29.32
QcStatements=1.3.6.1.5.5.7.1.3
HcRole=1.0.21091.2.0.5
```

**Примечание 1**: следует подчеркнуть, что таким образом нельзя проигнорировать распознаваемые Продуктом `Critical Extention`s, например `BasicConstraints`.

**Примечание 2**: секция `IgnoringUnsupportedCriticalExtentions`, даже пустая, обязательно должна присутствовать в файле x509opts.ini.

# Приложение

## Текст cisco-like конфигурации для устройства GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW1
enable password csp
!
!
!
logging trap debugging
!
crypto identity my_admin
 dn C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=adminhost
!
crypto isakmp policy 1
 encr gost
 hash gost
 authentication gost-sig
 group vko
!
crypto ipsec transform-set TSET esp-gost4mimit
!
ip access-list extended LIST
 permit tcp host 192.168.100.1 eq 22 any
!
ip access-list extended LIST2
 permit tcp host 192.168.100.1 eq 22 any
 permit udp host 192.168.100.1 eq non500-isakmp any
 permit udp host 192.168.100.1 eq isakmp any
 deny   ip any any
!
!
crypto dynamic-map DMAP 1
 match address LIST
 set transform-set TSET
 set pfs vko
 set identity my_admin
!
crypto map CMAP 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.168.100.1 255.255.255.0
 ip access-group LIST2 out
 crypto map CMAP
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
interface GigabitEthernet0/3
 no ip address
 shutdown
```

```
!
!
ip route 0.0.0.0 0.0.0.0 192.168.100.2
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530
…
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F

quit
!
end
```

# Текст LSP для устройства GW1

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Mon May 27 11:07:09 2013

GlobalParameters(
    Title                       = "This LSP was automatically generated by
CSP Converter at Mon May 27 11:07:09 2013"
    Version                     = LSP_4_1
    CRLHandlingMode             = OPTIONAL
    PreserveIPsecSA             = FALSE
)

IKEParameters(
    FragmentSize = 0
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.100.2
        )
)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "G2814789CPRO1-K256-CBC-65534"
    HashAlg     = "GR341194CPRO1-65534"
    GroupID     = VKO_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO1-K288-CNTMAC-253"
```

```
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4608000
    )
)

FilterChain FilterChain:LIST2 (
    Filters = Filter (
        SourceIP = 192.168.100.1
        ProtocolID = 6
        SourcePort = 22
        Action = PASS
        LogEventID = "LIST2"
    ),
    Filter (
        SourceIP = 192.168.100.1
        ProtocolID = 17
        SourcePort = 4500
        Action = PASS
        LogEventID = "LIST2"
    ),
    Filter (
        SourceIP = 192.168.100.1
        ProtocolID = 17
        SourcePort = 500
        Action = PASS
        LogEventID = "LIST2"
    ),
    Filter (
        Action = DROP
        LogEventID = "LIST2"
    ),
    Filter (
        Action = DROP
    )
)

IdentityEntry my_admin(
    DistinguishedName* = CertDescription(
        Subject = TEMPLATE, "C=RU,L=Moscow,O=S-Terra
CSP,OU=Research,CN=adminhost"
    )
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID        =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA
)
    RemoteID       =  my_admin
    SendRequestMode    =  ALWAYS
    SendCertMode       =  ALWAYS
)

IKERule IKERule:CMAP:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DoNotUseDPD         = TRUE
    Priority            = 100
)

IPsecAction IPsecAction:CMAP:1:DMAP:1
(
    TunnelingParameters = TunnelEntry(
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    GroupID = VKO_1B
    IKERule = IKERule:CMAP:1:DMAP:1
```

```
)

FilterChain IPsecPolicy:CMAP (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.100.1
        ProtocolID = 6
        SourcePort = 22
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1:DMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:DMAP:1:LIST"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    OutputFilter = FilterChain:LIST2
    IPsecPolicy = IPsecPolicy:CMAP
)
```

# Текст LSP для устройства AdminHost

```
GlobalParameters (
    Title = "This LSP was automatically generated by S-Terra Client AdminTool
(cp) at 2013.05.27 11:15:04"
    Version = LSP_4_1
    CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
    ResponseTimeout = 200
    HoldConnectTimeout = 60
    DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
    DistinguishedName *= CertDescription(
           Subject *= COMPLETE,"C=RU,L=Moscow,O=S-Terra
CSP,OU=Research,CN=adminhost"
           )
)
CertDescription local_cert_dsc_01(
    Subject *= COMPLETE,"C=RU,L=Moscow,O=S-Terra
CSP,OU=Research,CN=adminhost"
    Issuer *= COMPLETE,"C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-
W2008SP1-X64-CA"
    SerialNumber = "611425D8000000000002"
    FingerprintMD5 = "3EE6136FE1D8A9E0473E6A020B93C510"
)
CertDescription partner_cert_dsc_01(
)
AuthMethodGOSTSign auth_method_01(
    LocalID = auth_identity_01
    LocalCredential = local_cert_dsc_01
    RemoteCredential = partner_cert_dsc_01
    SendRequestMode = AUTO
    SendCertMode = AUTO
)
IKEParameters (
    DefaultPort = 500
    SendRetries = 5
    RetryTimeBase = 1
    RetryTimeMax = 30
    SessionTimeMax = 60
```

```
    InitiatorSessionsMax = 30
    ResponderSessionsMax = 20
    BlacklogSessionsMax = 16
    BlacklogSessionsMin = 0
    BlacklogSilentSessions = 4
    BlacklogRelaxTime = 120
    IKECFGPreferDefaultAddress = FALSE
)
IKETransform ike_trf_02(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341194CPRO1-65534"
    GroupID *= VKO_1B
)
IKETransform ike_trf_03(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341194CPRO1-65534"
    GroupID *= MODP_1536
)
IKETransform ike_trf_04(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341194CPRO1-65534"
    GroupID *= MODP_1024
)
IKETransform ike_trf_05(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341194CPRO1-65534"
    GroupID *= MODP_768
)
ESPTransform esp_trf_01(
    CipherAlg *= "G2814789CPRO1-K288-CNTMAC-253"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_01(
    Transform *=esp_trf_01
)
ESPTransform esp_trf_02(
    IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
    CipherAlg *= "NULL"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_02(
    Transform *=esp_trf_02
)
ESPTransform esp_trf_03(
    IntegrityAlg *= "G2814789CPRO1-K256-MAC-65535"
    CipherAlg *= "NULL"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_03(
    Transform *=esp_trf_03
)
ESPTransform esp_trf_04(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_04(
    Transform *=esp_trf_04
)
ESPTransform esp_trf_05(
    IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    LifetimeSeconds = 3600
```

```
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_05(
    Transform *=esp_trf_05
)
ESPTransform esp_trf_06(
    IntegrityAlg *= "G2814789CPRO1-K256-MAC-65535"
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_06(
    Transform *=esp_trf_06
)
ESPTransform esp_trf_07(
    IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
    CipherAlg *= "G2814789CPRO1-K288-CNTMAC-253"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_07(
    Transform *=esp_trf_07
)
ESPTransform esp_trf_08(
    IntegrityAlg *= "G2814789CPRO1-K256-MAC-65535"
    CipherAlg *= "G2814789CPRO1-K288-CNTMAC-253"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_08(
    Transform *=esp_trf_08
)
IKERule ike_rule(
    DoNotUseDPD = FALSE
    DPDIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_02,ike_trf_03,ike_trf_04,ike_trf_05
)
IPsecAction ipsec_action_01(
    TunnelingParameters *=
           TunnelEntry(
                  PeerIPAddress = 192.168.100.1
                  Assemble = TRUE
                  ReRoute = FALSE
           )
    ContainedProposals *=
(esp_proposal_01),(esp_proposal_02),(esp_proposal_03),(esp_proposal_04),(esp_
proposal_05),(esp_proposal_06),(esp_proposal_07),(esp_proposal_08)
    GroupID *= VKO_1B,MODP_1536,MODP_1024,MODP_768
    IKERule = ike_rule
)
FilterChain filter_chain_input(
    Filters *= Filter(
           ProtocolID *= 17
           DestinationPort *= 500
           Action = PASS
           LogEventID = "pass_action_02_01"
    ),Filter(
           ProtocolID *= 17
           DestinationPort *= 4500
           Action = PASS
           LogEventID = "pass_action_02_02"
    ),Filter(
           SourceIP *= 192.168.100.1
           ProtocolID *= 50
           Action = PASS
           LogEventID = "pass_action_03_01"
    ),Filter(
```

```
            SourceIP *= 192.168.100.1
            ProtocolID *= 51
            Action = PASS
            LogEventID = "pass_action_03_02"
    ),Filter(
            Action = PASS
            LogEventID = "pass_action_04"
    )
)
FilterChain filter_chain_output(
    Filters *= Filter(
            ProtocolID *= 17
            SourcePort *= 500
            Action = PASS
            LogEventID = "pass_action_05_01"
    ),Filter(
            ProtocolID *= 17
            SourcePort *= 4500
            Action = PASS
            LogEventID = "pass_action_05_02"
    ),Filter(
            DestinationIP *= 192.168.100.1
            ProtocolID *= 50
            Action = PASS
            LogEventID = "pass_action_06_01"
    ),Filter(
            DestinationIP *= 192.168.100.1
            ProtocolID *= 51
            Action = PASS
            LogEventID = "pass_action_06_02"
    ),Filter(
            Action = PASS
            LogEventID = "pass_action_07"
    )
)
FilterChain filter_chain_classification_input(
    Filters *= Filter(
            Action = PASS
            LogEventID = "pass_action_08"
    )
)
FilterChain filter_chain_classification_output(
    Filters *= Filter(
            Action = PASS
            LogEventID = "pass_action_09"
    )
)
FilterChain filter_chain_ipsec(
    Filters *= Filter(
            ProtocolID *= 17
            SourcePort *= 500
            Action = PASS
            LogEventID = "pass_action_10_01"
    ),Filter(
            ProtocolID *= 17
            SourcePort *= 4500
            Action = PASS
            LogEventID = "pass_action_10_02"
    ),Filter(
            DestinationIP *= 192.168.100.1
            ProtocolID *= 6
            DestinationPort *= 22
            Action = PASS
            ExtendedAction *= ipsec<sa=ipsec_action_01>
            LogEventID = "ipsec_action_01_01"
    ),Filter(
            DestinationIP *= 192.168.100.1
            ProtocolID *= 17
            DestinationPort *= 22
            Action = PASS
```

```
            ExtendedAction *= ipsec<sa=ipsec_action_01>
            LogEventID = "ipsec_action_01_02"
    ),Filter(
            DestinationIP *= 192.168.100.1
            ProtocolID *= 132
            DestinationPort *= 22
            Action = PASS
            ExtendedAction *= ipsec<sa=ipsec_action_01>
            LogEventID = "ipsec_action_01_03"
    ),Filter(
            Action = PASS
            LogEventID = "pass_action_11"
    )
)
NetworkInterface(
    InputFilter = filter_chain_input
    OutputFilter = filter_chain_output
    InputClassification = filter_chain_classification_input
    OutputClassification = filter_chain_classification_output
    IPsecPolicy = filter_chain_ipsec
)
```