**УТВЕРЖДЕНО**

**BY.PTHK.45001-01 34 01-1-ЛУ**

# Программный комплекс

# «Шлюз безопасности Bel VPN Gate 4.5»

# Руководство пользователя

# Настройка

**BY.PTHK.45001-01 34 01-1**

**Листов 65**

| | |
|---|---|
| Подп. и дата | |
| Инв. № дубл. | |
| Взам. инд. № | |
| Подп. и дата | |
| Инд. № подл. | |

2020

# Содержание



# Лицензионное Соглашение

## о праве пользования программным комплексом «Bel VPN Gate 4.5» производства ООО «С-Терра Бел»



Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного программного комплекса «Шлюз безопасности Bel VPN Gate 4.5» (далее – Продукт) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Продукта, являющейся неотъемлемой частью Продукта). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных прав использования Продукта на территории Республики Беларусь.

Под Продуктом понимается комплекс объектов (программного кода Продукта и документации на него в печатной и электронной формах), включенных в Комплект поставки Продукта.

*Продукт может использоваться только в качестве средства защиты информации и не предназначено для использования в других целях. Использование Продукта в прочих продуктах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.*

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

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

Продукт и его компоненты являются интеллектуальной собственностью Производителя (ООО «С-Терра Бел») и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Республики Беларусь об авторском праве на объекты интеллектуальной собственности.

Установка Продукта после предъявления Конечному Пользователю Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступлением его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 403 Гражданского кодекса Республики Беларусь имеет силу договора между Конечным Пользователем и Производителем Продукта.

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

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

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

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

Конечный Пользователь не имеет права дизассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и компоненты Продукта, вносить какие-либо изменения в

бинарный код программ и совершать относительно Продукта другие действия, нарушающие белорусское и международное законодательство по авторскому праву и использованию программных средств.

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

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Республики Беларусь «Об авторском праве и смежных правах» и преследуется по закону.

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

1. В случае, если при использовании Продукта Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Продукта обеспечивает[1]:

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

б) бесплатное предоставление обновлений программного обеспечения Производителя Продукта, в которых устранены Критичные Проблемы[2].

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

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

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

Срок действия настоящего Лицензионного Соглашения распространяется на весь период использования Продукта Конечным Пользователем. В случае использования лицензии с ограниченным сроком действия - на срок, указанный в лицензии. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие программный код и прочие компоненты Продукта. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

«Debian» является зарегистрированной в США торговой маркой Software in the Public Interest, Inc. (Программное обеспечение в интересах общества) и управляется проектом Debian,
Торговая марка «Linux» принадлежит создателю и основному разработчику ядра Линусу Торвальдсу.

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

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

2 Обновления программного обеспечения в соответствии с гарантийным обязательством п.1б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

Напечатано в Республике Беларусь
ООО «С-Терра Бел»
220012, г. Минск ул. Чернышевского, д. 10А, пом. 611
Телефон: (+375 17) 280 6000
Эл.почта: info@s-terra.by
https://s-terra.by

# Комплект поставки

В комплект поставки программного комплекса «Шлюз безопасности Bel VPN Bel VPN Gate 4.5» (далее – Bel VPN Gate) входит:

| № пп | Элемент комплекта | Пояснения |
|---|---|---|
| 1 | Файл «belvpngate_4.5.xxxxav+c3_amd64.deb» | файл установки комплекса для ОС Linux/Debian |
| 2 | Файлы «Bel_VPN_Gate_4.5_UserGuide-XX.pdf» | документы в электронном виде «Программный комплекс «Шлюз безопасности Bel VPN Gate 4.5». Руководство пользователя» |
| 3 | Сертификат соответствия техническому регламенту Республики Беларусь | заверенная копия документа на бумажном носителе |
| 4 | Лицензия на использование экземпляра Bel VPN Gate | набор данных пользователя комплекса, передаваемый на любом носителе или в электронном виде |
| | утилита командой строки ОС Windows avpassinit.exe | используется для инициализации носителей типа AvPass |
| | утилита командой строки ОС Windows avtoksvc.exe | используется для инициализации носителей типа AvBign |

Другая документация по особенностям использования программного комплекса «Шлюз безопасности Bel VPN Bel VPN Gate 4.5» доступна для загрузки на сайте компании: https://www.s-terra.by

# Назначение и функции ПК Bel VPN Gate

ПК Bel VPN Gate является средством шифрования/дешифрования сетевого трафика с контролем целостности по СТБ 34.101.31.

Количество туннелей шифрования – определяется лицензией (от 10 до без ограничений).

ПК Bel VPN Gate обеспечивает:

1. создание виртуальных частных сетей (VPN) по технологии IPsec VPN;
2. защиту транзитного трафика между различными узлами сети и защиту трафика самого шлюза безопасности на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP в рамках международных стандартов:
   a. Security Architecture for the Internet Protocol – RFC2401
   b. IP Authentication Header (AH) – RFC2402
   c. IP Encapsulating Security Payload (ESP) – RFC2406
   d. Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
   e. The Internet Key Exchange (IKE) – RFC2409
   f. The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407;
3. пакетную stateless фильтрацию трафика;
4. контекстную (stateful) фильтрацию для протоколов TCP и FTP;
5. работу по расписанию для правил пакетной фильтрации;
6. классификацию и маркирование трафика;
7. возможность применения различных наборов правил обработки трафика на различных виртуальных сетевых интерфейсах ПК;
8. возможность получения сертификатов открытых ключей по протоколу LDAP;
9. поддержку сертификатов открытых ключей ГосСУОК;
10. событийное протоколирование (по протоколу syslog), с возможностью объединять события в группы и задавать для каждой группы свой независимый уровень протоколирования;
11. сбор статистики для мониторинга (по протоколу SNMP v1 и v2c);
12. маскировку топологии защищаемого сегмента сети (туннелирование трафика);
13. возможность задания дополнительной аутентификации партнера на основе запросов на RADIUS сервер;
14. возможность загрузки локальной политики безопасности из внешнего файла;
15. защиту сети, подсети и самого шлюза от несанкционированного доступа;
16. контроль целостности программной и информационной части программного обеспечения ПАК;
17. построение отказоустойчивых схем, в том числе кластерных решений, горячее резервирование и балансировку.

Управление ПК Шлюз осуществляется:

1. централизованно-удаленно, посредством программного продукта «Bel VPN KP»;
2. локально и удаленно по протоколу SSH с помощью интерфейса командной строки;
3. локально, при помощи конфигурационного текстового файла, описывающего политику безопасности.

ПК Bel VPN Gate использует криптографическую библиотеку программного средства электронной цифровой подписи и шифрования «AvC ver.1.0» (РБ.ЮСКИ.13000-01), а также может использовать внешнее устройство хранения информации: AvPass (ИЯТА.467532.002) или AvBign (ИЯТА.467532.003) производства ЗАО «Авест».

ПК Bel VPN Gate работает под управлением операционной системы Debian GNU/Linux 9,

ПК Bel VPN Gate реализует требования Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» – ТР 2013/027/BY (взаимосвязанные ТНПА):

| | |
|---|---|
| СТБ 34.101.31-2011 (пп. 6.4, 6 6) | Шифрование в режиме гаммирования с обратной связью и выработка имитовставки |
| СТБ 34.101.66-2014 (приложение А) | Формирование общего ключа по протоколу Диффи — Хеллмана |
| СТБ 34.101.47-2017 (п. 6.2) | Генерация псевдослучайных чисел в режиме счетчика |
| СТБ 34.101.17-2012 | Синтаксис запроса на получение сертификата |
| СТБ 34.101.19-2012 (разделы 6-8) | Форматы сертификата открытого ключа и списка отозванных сертификатов, а также их расширений |
| | Верификация маршрута сертификации |
| СТБ 34.101.78-2019 (пп. 8.2, 8.3, 8.5) | Структура и атрибуты запроса на получение сертификата; форматы сертификата открытого ключа и списка отозванных сертификатов |
| СТБ 34.101.45-2013 (п. 6.2) | Генерация личного и открытого ключей и проверка ключей (алгоритмы управления параметрами и ключами) |
| СТБ 34.101.27-2011 (класс 1) | Требования безопасности |
| СТБ 34.101.73-2017 (пп. 7.3, 7.4) | Межсетевой экран сетевого и транспортного уровней |

Также реализованы функции, определенные в ТНПА Республики Беларусь, обеспечивающие функционирование ПК Bel VPN Gate (подтверждение соответствия не требуется):

| | |
|---|---|
| СТБ 34.101.45-2013 (п. 7.1) | Электронная цифровая подпись на основе эллиптических кривых |
| СТБ 34.101.45-2013 (приложение Е) | Парольная защита личного ключа |
| СТБ 34.101.31-2011 (п. 6.9) | Функция хеширования |
| Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Методика создания и распределения ключевых данных. BY.PTHK.00001-04.1 91 01 | Управление криптографическими ключами, рекомендованное ОАЦ |

# Запуск ПК Bel VPN Gate

В этом разделе описана установка и запуск ПК Bel VPN Gate установленного в среду функционирования ОС GNU/Linux Debian 9 (32-bit или 64-bit) на вычислительных системах архитектуры Intel x86/x86-64.

Установка ПК Bel VPN Gate проводится в следующей последовательности:

- доставить установочный deb-файл на целевое устройство;
- перейти в каталог с файлом посредством команды “cd путь_к_каталогу”;
- запустить установку при помощи команды: “dpkg -i имя_установочного_файла.deb”.

В качестве терминала для доступа к аппаратной платформе (АП), на которой установлен ПК Bel VPN Gate, можно использовать монитор и клавиатуру или последовательный интерфейс, подключенные к соответствующим разъемам АП.

**Шаг 1:** Подключить к АП монитор и клавиатуру или последовательный порт компьютера в качестве терминала, используя нуль-модемный кабель (5 проводов).

На компьютере используйте терминальную программу, например, Windows HyperTerminal или Putty.

В программе HyperTerminal выполните настройки:

```
File-> Properties-> Settings-> Emulation-> VT100
```

Во вкладке `Connect To` нажать кнопку `Configure` и выполнить следующие настройки COM-порта:

```
Bits per second: 115200
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None
```

**Шаг 2:** В процессе загрузки указать, что будет использоваться в качестве терминала для аппаратной платформы:

1) монитор и клавиатура
   **`Bel VPN Gate`**
2) последовательный порт
   **`Bel VPN Gate (serial)`**

**Шаг 3:** После загрузки ОС войти в систему, используя следующие реквизиты:

имя пользователя – **`root`**

пароль – пустой.

**Шаг 4:** Выполнить процедуру инициализации ПК Bel VPN Gate, описанную в разделе «Инициализация ПК Bel VPN Gate при первом старте».

# Инициализация ключевого носителя информации

Для хранения личного ключа электронной цифровой подписи в ПК Bel VPN Gate используются ключевые носители AvPass 11-E-02/04, AvBign 128-C-01, которые необходимо инициализировать перед использованием.

Для инициализации носителей типа AvPass используется утилита командой строки AvPassInit.exe.

## Инициализация носителя типа AvPass

**Шаг 1:** Подключить ключевой носитель к USB-порту персонального компьютера.

**Шаг 2:** Вставить компакт-диск поставки в устройство считывания компакт-дисков.

**Шаг 3:** Запустить командную строку (`cmd.exe`) и перейти в каталог Utils, развешенный на компакт-диске.

**Шаг 4:** Вызывать утилиту `avpassinit.exe` с параметром «–pin=», указав после «=» новый пароль.

Пример:

```
avpassinit.exe –pin=s3CR3tPassWorD
```

**Шаг 5:** Отключить ключевой носитель от ПК и подключить его к АП с установленным ПК Bel VPN Gate.

## Инициализация носителя типа AvBign

**Шаг 1:** Подключить ключевой носитель к usb-порту персонального компьютера.

**Шаг 2:** Вставить компакт-диск поставки в устройство считывания компакт-дисков.

**Шаг 3:** Запустить командную строку (`cmd.exe`) перейти в каталог Utils, развешенный на компакт-диске.

**Шаг 4:** Вызвать утилиту `avtoksvc.exe` с параметром `info`, найти номер слота, к которому подключен ключевой носитель. Номер будет указан в строке `CK_SLOT_ID.`

**Шаг 5:** Вызывать утилиту avtoksvc.exe с параметрами `newpasswd –slot=номер-слота –password=пароль-пользователя –new_password=новый-пароль-пользователя`».

В случае успеха будет выведено сообщение

```
User PIN changed.
Done in 0:00:00.577.
Testing new user password...
New user password passed OK.
```

В случае неуспешного выполнения операции смены пароля, сообщение будет следующее:

```
C_Login(U) returned 0xa0 PIN INCORRECT
```

Пример:

```
avtoksvc.exe newpasswd -slot=0 -password=P2Ss!0Rd
-new_password= P2Ss!0Rd
User PIN changed.
Done in 0:00:00.577.
Testing new user password...
New user password passed OK.
```

**Шаг 6:** Отключить ключевой носитель от ПК и подключить его к АП с установленным ПК Bel VPN Gate.

# Инициализация ПК Bel VPN Gate при первом старте

При первом запуске ПК Bel VPN Gate после загрузки ОС появляется предупреждение `"System is not initialized. Please run /opt/VPNagent/bin/init.sh to start initialization procedure"` и приглашение для входа в ОС.

Ниже пошагово описаны действия, которые необходимо выполнить для инициализации ПК Bel VPN Gate .

**Шаг 1:** Запустить скрипт `/opt/VPNagent/bin/init.sh` для старта процедуры начальной инициализации шлюза безопасности Bel VPN Gate.

Во время выполнения, инициализационный скрипт может быть прерван нажатием комбинации клавиш `Ctrl+C`.

При возникновении ошибки процесс инициализации прерывается и на экран выдается сообщение об ошибке.

**Шаг 2:** Далее проводится инициализация начального значения ДСЧ.

**Шаг 3:** Далее запрашивается лицензионная информация на Шлюз безопасности Bel VPN Gate (сведения, необходимые для ввода находятся на бланке «Лицензии на использование ПК Bel VPN Gate», входящем в комплект поставки):

`You have to enter license for Bel VPN Gate`

Предлагаются следующие пункты для ввода:

`Available product codes:`

```
GATE100
GATE100B
GATE100V
GATE1000
GATE1000V
GATE3000
GATE7000
GATE10000
RVPN
RVPNV
BELVPN
BELVPNV
UVPN
UVPNV
KZVPN
KZVPNV
```

`Enter product code:` – ввести код продукта

`Enter customer code:` – ввести код конечного пользователя

`Enter license number:` – ввести номер лицензии

`Enter license code:` – ввести код лицензии

**Шаг 4:** Следует вопрос о корректности введенных данных:`"Is the above data correct?"`. После получения подтверждения инициализация продолжается без дополнительных вопросов. Если получен отрицательный ответ – предлагается ввести лицензионную информацию повторно.

**Шаг 5:** Далее запускается vpn-демон, создается пользователь "cscons" с назначенным ему начальным паролем "csp".

Если инициализация завершилась успешно, то выдается сообщение: "Initialization complete". При последующих стартах системы предупреждение о необходимости инициализации системы не выдается.

Если инициализация завершилась неуспешно, то об этом выдаётся соответствующее сообщение. При следующем старте комплекса администратору снова будет выдаваться предупреждение об инициализации.

При инициализации шлюза безопасности Bel VPN Gate устанавливается политика безопасности, при которой интерфейсы шлюза безопасности не пропускают пакеты – Default Driver Policy = Dropall. Выдается информационное сообщение:

```
Default driver policy is configured to block network traffic.
Network is inaccessible in this mode.
You can change it using "${AgentRoot}bin/dp_mgr" utility or load security
policy.
```

Для входа в Cisco-like интерфейс командной строки нужно использовать имя пользователя "cscons" (начальный пароль "csp"),

Для входа в ОС предназначено имя "root" (изначально без пароля).

Сразу после инициализации программного комплекса автоматически запускается утилита cspvpn_verify для проверки целостности установленного комплекса шлюз безопасности Bel VPN Gate, которая описана в документе «Программные продукты Bel VPN. Руководство пользователя. Специализированные команды» (BY.PTHK.45000 34 01-3).

Утилита управления ключевыми контейнерами cryptocont размещается в каталоге /opt/Avest/bin. Подробное описание данной утилиты приведено в документе «Программные продукты Bel VPN. Руководство пользователя. Специализированные команды» (BY.PTHK.45000 34 01-3).

# Регистрация Лицензии на ПК Bel VPN Gate

Регистрация Лицензии на комплекс выполняется во время инициализации ПК Bel VPN Gate, но если появится необходимость перерегистрировать Лицензию после инициализации, то используется утилита `lic_mgr`.

Утилита `lic_mgr`, описанная в документе Bel VPN Gate 4.5. Специализированные команды», запускается из интерфейса командной строки из каталога комплекса `/opt/VPNagent/bin`:

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

# Изменение паролей

После инициализации комплекса пользователь "root" с правами системного администратора ОС 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 Bel VPN 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 _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 шлюза настройка интерфейсов выполняется:

- 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 «Программный комплекс «Шлюз безопасности Bel VPN Gate 4.5» Руководство пользователя. Cisco-like команды».

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

## Назначение IP-адресов интерфейсам

Изменить 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
   ```

1. 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
   ```

3. 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.

4. Необходимо пересчитать хэш-сумму измененного файла. Запустите утилиту `integr_mgr calc`:

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

5. 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` двумя способами.

**Настройка в cisco-like консоли:**

В файле /etc/ifaliases.cf должна присутствовать строка:

```
interface (name="GigabitEthernet0/0" pattern="eth0")
```

Команды для настройки:

```
(config)#interface GigabitEthernet0/0.10
(config-subif)#encapsulation dot1Q 10
(config-subif)#ip address 192.168.0.2 255.255.255.0
```

**Настройка без использования cisco-like консоли:**

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
   vlan_raw_device eth0
   ```

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

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

7. Пересчитайте хэш-сумму измененного файла `ifaliaces.cf`, запустив утилиту `integr_mgr calc`:

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

8. Поднимите интерфейс:

   ```
   ifup eth0.10
   ```

9. 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.

10. 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 VPN демон (vpnsvc) комплекса 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 комплекса.

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 Bel VPN 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`
11. 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 Bel VPN 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 обеспечения, оптимизацией под определенный характер сетевого трафика, оптимизацией под характеристики сетевых интерфейсов и канала связи.

На рисунке ниже представлена схема параллельной обработки трафика в Linux.

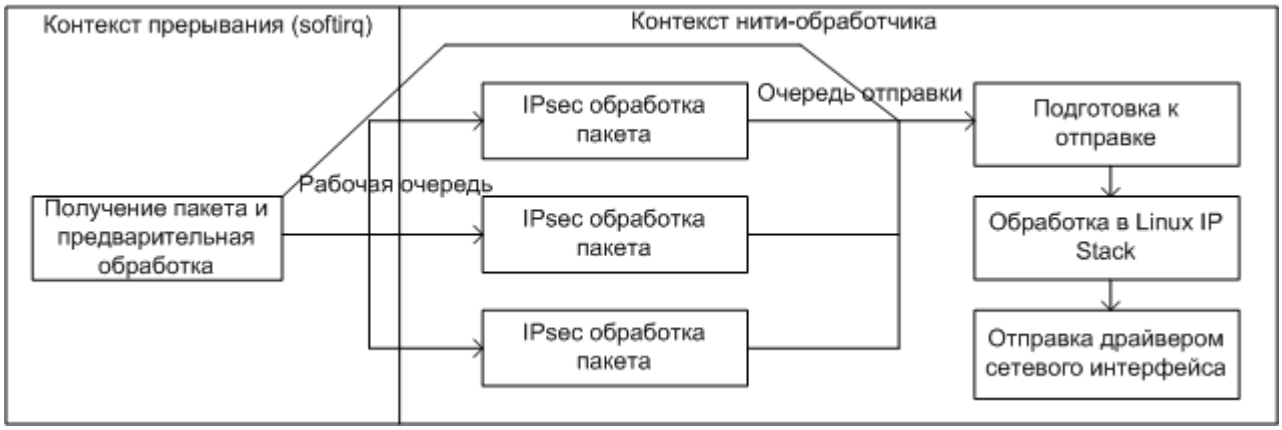



Рисунок 1

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).

### a) 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>

### b) pq_thread_q_size

Параметр pq_thread_q_size ограничивает размер очереди и задается утилитой drv_mgr, описанной в документе «Программные продукты Bel VPN. Руководство пользователя. Специализированные команды» (BY.PTHK.45000 34 01-3)».

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).

### c) 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 «Программные продукты Bel VPN. Руководство пользователя. Специализированные команды» (BY.PTHK.45000 34 01-3).

### d) 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 ), 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.

### e) pq_force_ordering

Параметр pq_force_ordering определяет, что происходит при заполнении очереди отправки:

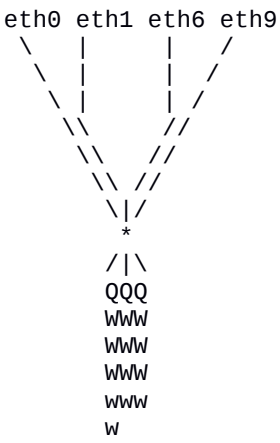
- Если выставлено значение 1, пакеты при переполнении очереди уничтожаются.
- Если выставлено значени 0, пакеты все равно обрабатываются – то есть порядок отправки пакетов регулируется только в случае низкой загрузки. При установке pq_force_ordering = 0 рекомендуется выставлять маленькое значение pq_send_q_size.

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

Обработка трафика шлюзом безопасности осуществляется в той же последовательности, что и в Cisco IOS – исходящие пакеты проходят через NAT (Network Address Translation), потом происходит их шифрование (если необходимо), а входящие пакеты – сначала расшифровываются (если необходимо), а затем над ними осуществляется трансляция адресов.

Управление настройками NAT на шлюзе безопасности осуществляется средствами ОС.

В ОС Linux NAT настраивается при помощи утилиты iptables. Описание iptables можно посмотреть на сайте .

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 ). 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 комплекс Bel VPN Gate 4.5, 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).

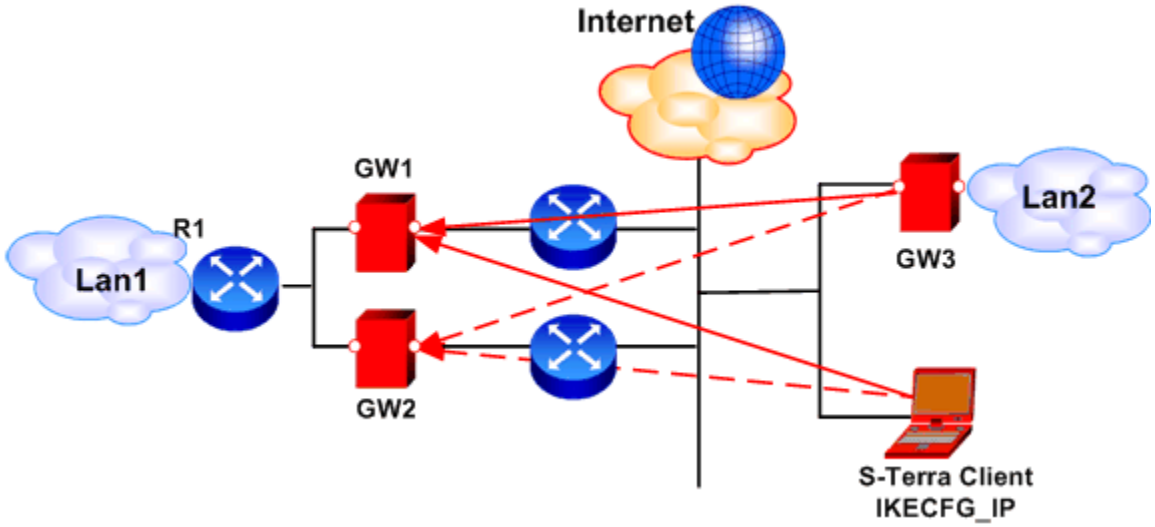



Рисунок 2

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.

### f) Краткое описание продукта Quagga

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).

### g) 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[3] 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 соответствующего 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  приведены некоторые возможные конфликтные ситуации.

Таблица 1

| N | Ситуация | Поведение комплекса | Отличие в поведении в Cisco IOS |
|---|---|---|---|
| 1 | Строится IPsec SA, при этом ID партнера второй фазы IKE не является подсетью (содержит | Маршрут RR не добавляется и выдается предупреждение в файл лога | Диапазоны адресов в Cisco IOS также не поддерживаются. |

3

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.

| N | Ситуация | Поведение комплекса | Отличие в поведении в Cisco IOS |
|---|---|---|---|
| | диапазон IP-адресов, порты и/или протоколы). | | 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 | 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<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, отсутствует маршрут до туннельного адреса[4], например, произошел разрыв соединения. | Маршрут RR не добавляется, в файл лога выдается диагностика | |
| 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 | |

4

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

| N | Ситуация | Поведение комплекса | Отличие в поведении в Cisco IOS |
|---|---|---|---|
| | | таблицы маршрутизации. Если для вновь создаваемого SA старый маршрут оказывается неправильным, он обновляется (см. ). 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. Таблица
   - 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. Таблица
   - 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. Таблица

     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. Таблица
   - 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 см. ниже.

12. 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 см. ниже.

13.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
```

14.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.

15.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.

16.Ошибки <rtctl err>.

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

# Построение VPN туннеля между шлюзом безопасности Bel VPN Gate 4.5 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 Bel VPN 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 клиент безопасности Bel VPN Client 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 Bel VPN 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. Также будет использовано программное средство электронной цифровой подписи и шифрования AvC ver 1.1.

Параметры защищенного соединения:

- Аутентификация на сертификатах;
- IKE параметры:
  - Алгоритм шифрования – СТБ 34.101.31;
  - Алгоритм вычисления хеш-функции – СТБ 34.101.31-2011 (пункт 6.9);
  - Группа Диффи-Хеллмана – 5 (1536 бит);
- IPsec параметры:
  - ESP алгоритм шифрования – СТБ 34.101.31.

## 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.

## Создание ключевой пары и формирование запроса на сертификат

Для создания ключевой пары и формирования запроса для шлюза безопасности GW1 необходимо выполнить следующие действия:

18. Убедиться, что ключевой носитель подключен к шлюзу
19. Создать контейнер, содержащий личный ключ, используя утилиту cryptocont (размещается в каталоге opt/Avest/bin):

```
root@sterragate:/opt/Avest/bin#./cryptocont n -n=av:gw1container
-p=12345678
```

где:

`–n=av:gw1container` – имя контейнера, «av:» означает, что контейнер размещается на ключевом носителе;

`-p=12345678` – пароль доступа к ключевому носителю (и контейнеру).

20. Создайте запрос на сертификат, содержащий открытый ключ ЭЦП

```
root@sterragate:/opt/Avest/bin#./cryptocont r –n=av:gw1container
–p=12345678 –cn=GW1 –o=OrgName –c=BY –f=/opt/requestgate.req
```

где:

`–n=av:gw1container` – имя контейнера, созданного на предыдущем шаге;

`-p=12345678` – пароль доступа к ключевому носителю (и контейнеру);

`-cn=GW1` – значение поля CommonName в запросе;

`-o=OrgName` – наименование организации;

`-f=/opt/request.req` – путь к создаваемому файлу запроса.

21. Отправьте созданный запрос достпным вам способом в УЦ, где по данному запросу будет создан локальный сертификат.

Предупреждение

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

22. Создайте папку `/opt/certs`:

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

23. Получите из УЦ локальный сертификат, цепочку сертификатов издателя в виде файлов (с расширением `.cer` или `.p7b`) и доставьте их на шлюз безопасности.

    Для доставки можно воспользоваться утилитой `pscp.exe` из пакета Putty, применив следующую команду:

```
pscp D:\ca.cer root@192.168.1.1:/opt/certs
```

Предупреждение

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

## Регистрация сертификатов

Для регистрации СА сертификата необходимо выполнить следующие действия:

1. Установите правильное системное время. Например:

```
root@sterragate:~# date 041013152015
Wed Apr 10 13:15:00 UTC 2015


Описание строки:
    04    10    13    15          2015
    Месяц день  часы  минуты      год
```

Данная запись соответствует 10 апреля 2015 года 13:15.

17. С помощью утилиты `cert_mgr`, входящей в состав шлюза безопасности Bel VPN Gate, зарегистрируйте сертификат УЦ в базе комплекса.

    Пример:

    ```
    root@sterragate:~# cert_mgr import -f /opt/certs/ca.cer -t
    1 OK C=BY,L=Minsk,O=CAOrgName,OU=CAOrgUnitName,CN=CA-W2008SP1-X64-CA
    ```

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

18. Зарегистрируйте локальный сертификат в базе комплекса, используя утилиту `cert_mgr`:

    ```
    root@sterragate:~# cert_mgr import -f /opt/certs/gw1.cer
    1 OK C=BY,OU=OrgunitName,CN=GW1
    ```

19. Убедитесь, что сертификаты импортированы успешно:

    ```
    root@sterragate:~# cert_mgr show
    Found 2 certificates. No CRLs found.
    1 Status: trusted C=BY,L=Minsk,O=CAOrgName,OU=CAOrgUnitName,CN=CA-W2008SP1-X64-CA
    2 Status: local   C=BY,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 запустите `cs_console` (возможно, потребуется переход в директорию `/opt/VPNagent/bin/`):

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

Пароль по умолчанию: `csp`

1. Перейдите в режим настройки:

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

20. Смените пароль по умолчанию:

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

21. Смените название шлюза:

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

22. 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
    ```

23. Задайте адрес шлюза по умолчанию:

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

24. Задайте тип идентификации:

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

25. Задайте параметры для IKE:

    ```
    GW1(config)#crypto isakmp policy 1
    ```

```
GW1(config-isakmp)#hash belt
GW1(config-isakmp)#encryption belt
GW1(config-isakmp)#authentication belt-sig
GW1(config-isakmp)#group beltdh
GW1(config-isakmp)#exit
```

26. Создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-belt esp-belt-mac
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

27. 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
```

28. 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
```

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

```
GW1(config)#crypto identity adminID
GW1(config-crypto-identity)#dn C=BY,L=Minsk,O=S-Terra Bel,
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.

30. 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 beldh
GW1(config-crypto-map)#set identity adminID
GW1(config-crypto-map)#reverse-route
GW1(config-crypto-map)#exit
```

31. Привяжите динамическую карту к статической:

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

32. 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
```

33. 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
```

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

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

В Приложении представлен  и  для шлюза GW1.

# Настройка рабочего места администратора AdminHost

Настройка рабочего места администратора состоит из нескольких этапов:

- получение сертификатов и секретных ключей;
- формирование инсталляционного пакета клиент безопасности Bel VPN Client для AdminHost;
- установка инсталляционного пакета клиент безопасности Bel VPN Client на AdminHost.

На компьютере, где будет создаваться инсталляционный пакет для AdminHost, должен быть установлен административный пакет Bel VPN Client 4.1 AdminTool (см. документацию «Программный продукт Клиент безопасности Bel VPN Client 4.1 . Руководство пользователя»).

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 продукт Клиент безопасности Bel VPN Client 4.1 . Руководство пользователя».

Запустите графический интерфейс Bel VPN Client 4.1 AdminTool (`Start –> Programs –> Bel VPN Client 4.1 AdminTool –> Package Maker)` и создайте, согласованную со шлюзом политику безопасности.

4. Во вкладке `Auth` (Рисунок ) 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, а также введите пароль для доступа нему в графе `password`;
   - отметьте пункт `Copy container from admin computer`;
   - задайте имя контейнера в графе `User container name`; в данном случае указано – `av:Admin25067`. 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).

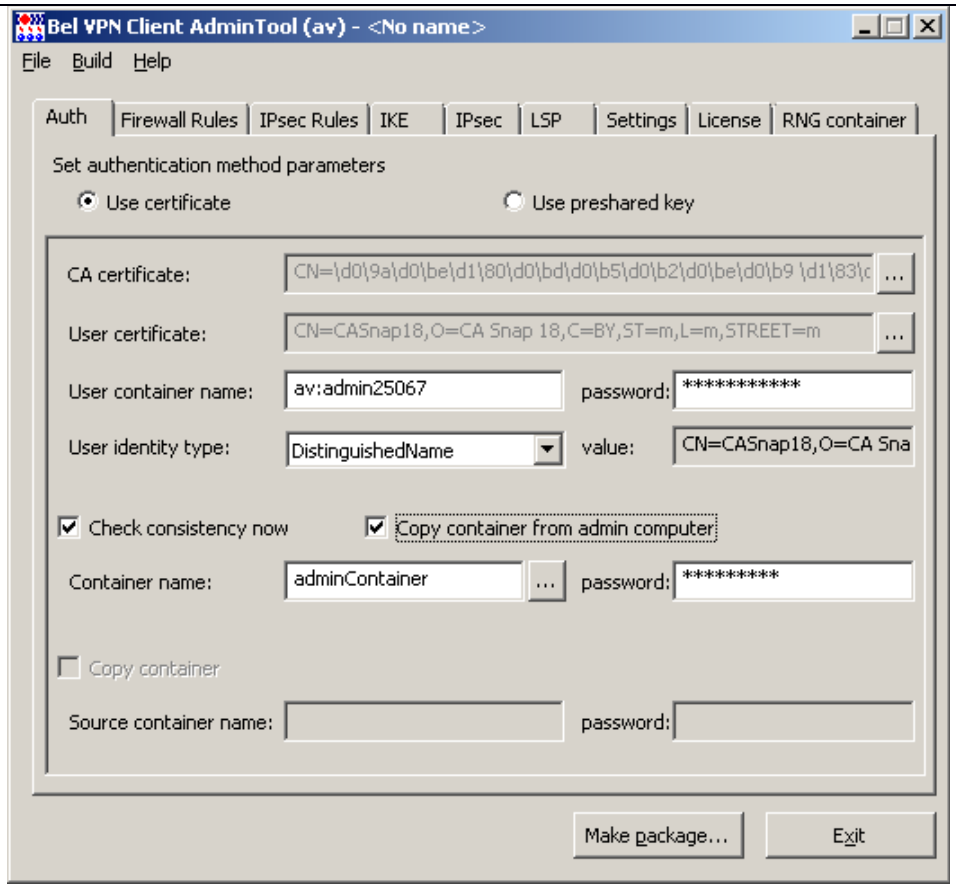



Рисунок 3

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

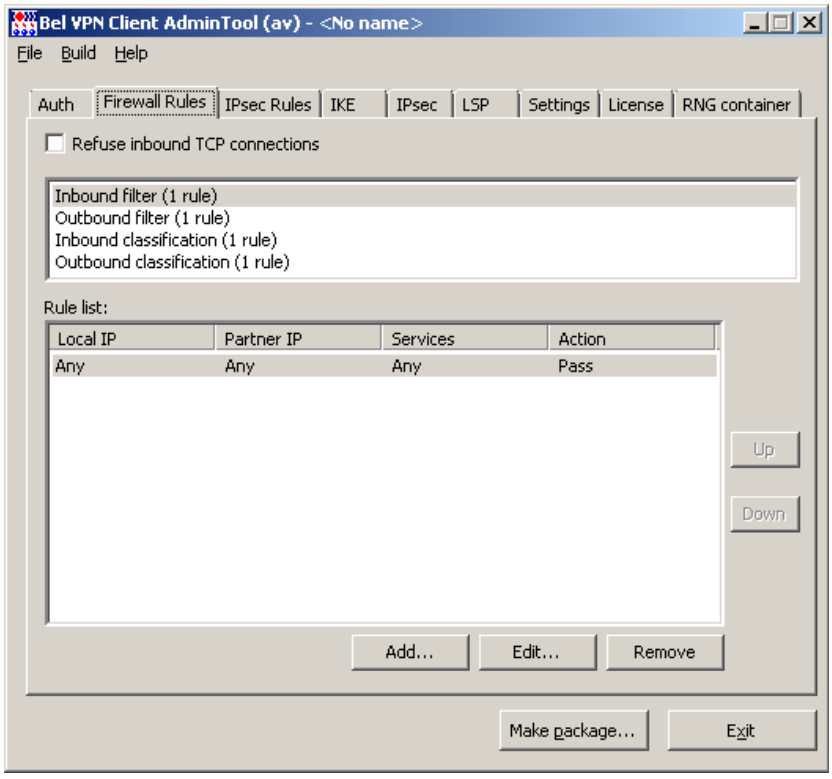



Рисунок 4

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

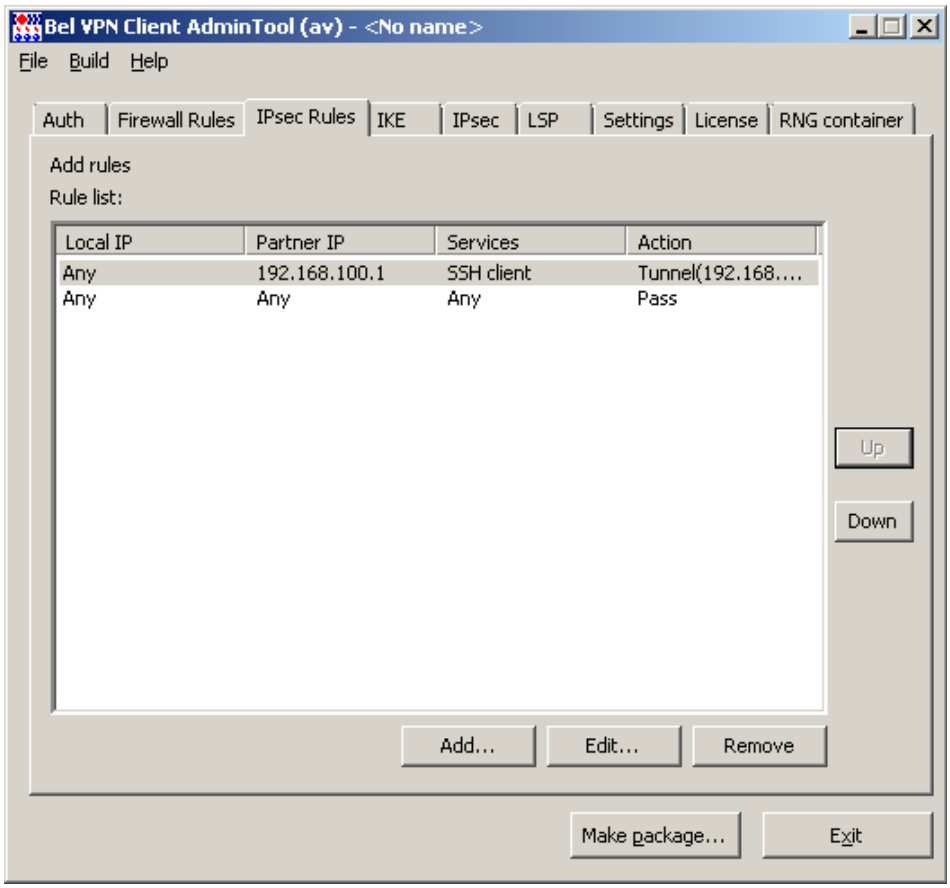



Рисунок 5

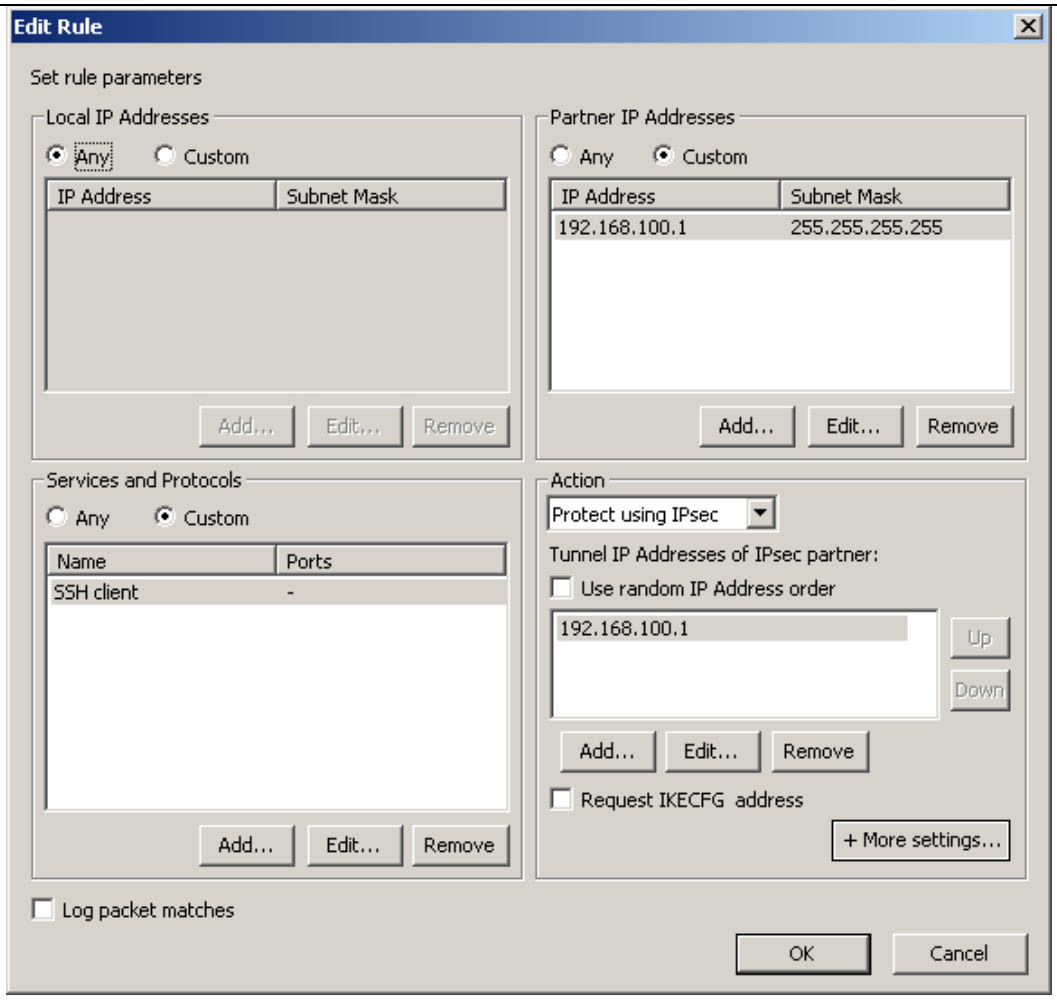



Рисунок 6

Закройте окно `Add Rule`.

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

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

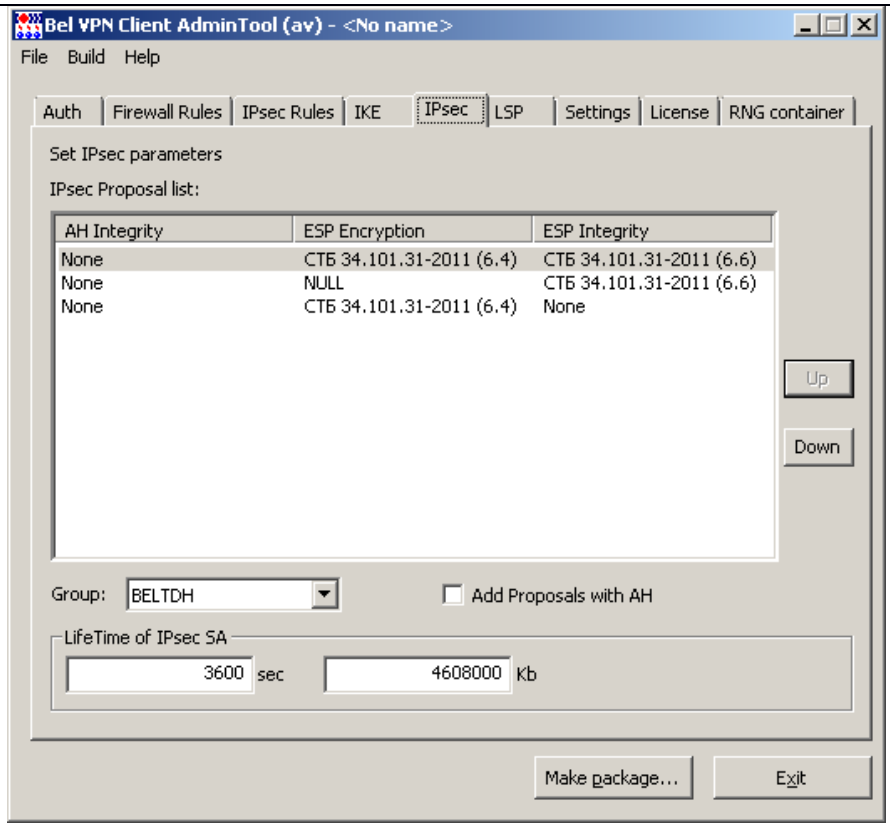



Рисунок 7

38. Во вкладке `License` введите регистрационные данные на продукт Клиент безопасности Bel VPN Client с бланка Лицензии.
39. Сохраните файл созданного проекта, на тот случай, если захотите в будущем сделать похожий инсталляционный пакет. Для этого нажмите `File->Save Project`
40. Далее сгенерируйте инсталляционный exe-файл, нажав кнопку `Make package…`
41. 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 .

## 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 рабочем месте администратора, выбрав предложение `Show SA Information` (Рисунок ), (Рисунок ):

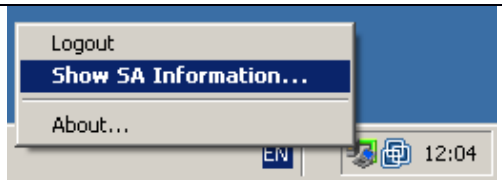



Рисунок 8

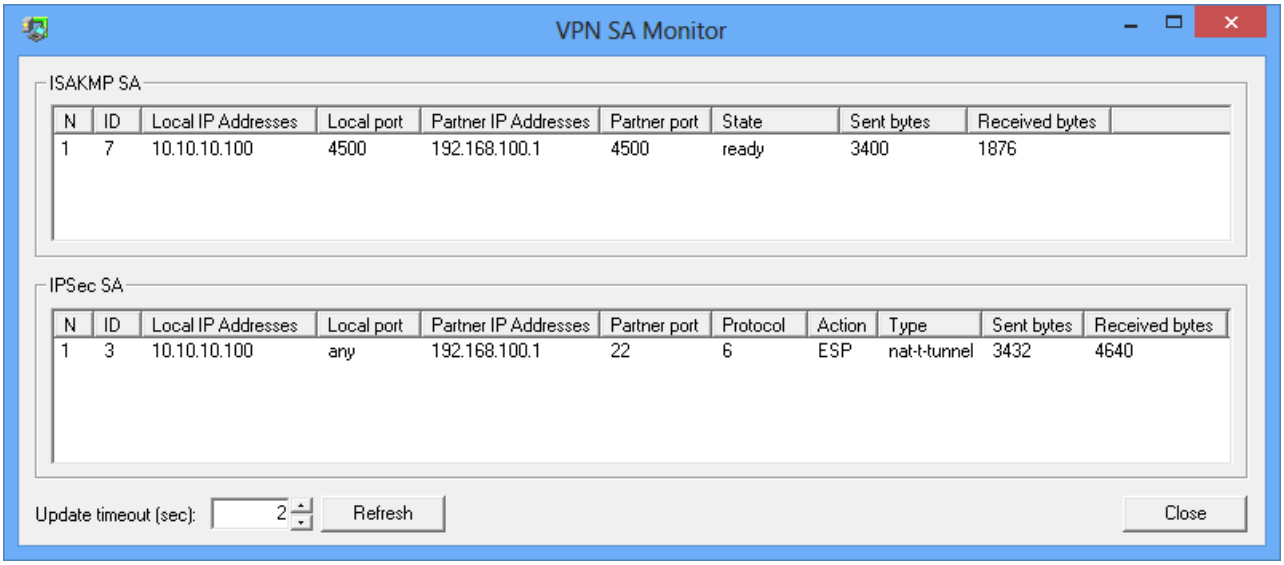



Рисунок 9

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 шлюза безопасности Bel VPN Gate 4.5 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 Bel VPN Gate 4.5 или создать политику безопасности для шлюза возможно:

- Локально или удаленно по протоколу SSH с использованием команд интерфейса командной строки, описанных в документе Bel VPN Gate 4.5. 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  (такую конфигурацию будем называть «native-конфигурацией» или «LSP-конфигурацией»). Команды, при помощи которых можно загрузить конфигурационный файл, описаны в документе .
- Централизованно–удаленно с помощью графического интерфейса Cisco Security Manager (CSM), описанного в документе S-Terra Gate с помощью Cisco Security Manager».
- Централизованно–удаленно с использованием программного продукта Bel VPN Updater, предназначенного для управления всей линией продуктов, производимых компанией «С-Терра Бел», и описанного в документе «Программный продукт Bel VPN Updater. 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 . Описание синтаксиса и структур данных конфигурационного файла приведено в документе .

### 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 шлюза безопасности Bel VPN Gate.

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 ***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 policy*** устанавливает политику isakmp, которая будет использоваться криптографической картой;
- ***set priority*** устанавливает приоритет криптографической карты;
- ***set local-address*** задает локальный IP-адрес для взаимодействия с партнерами;
- ***set self-identity*** задает локальный сертификат VPN-устройства для взаимодействия с партнерами по криптографической карте;
- ***set ca identity*** задает сертификат удостоверяющего центра, который будет использоваться при проверке сертификатов партнеров;
- ***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 ***dynamic map***.

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

### Привязка криптографической карты к интерфейсу

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

Команда  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 сетевому интерфейсу используется атрибут ***IPsecPolicy*** в структуре ***NetworkInterface***.

## Настройка маршрутизации

Добавление строки в таблицу маршрутизации в интерфейсе командной строки задается командой ***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 . 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 .

## Настройка SNMP

Для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP в интерфейсе командной строки используются три команды. Команда ***-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 ***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  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  в разделе «Конвертор».

**LSP-конфигурацию,** созданную в виде текстового конфигурационного файла, нужно загрузить специализированной командой , 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 .

# Работа с сертификатами

## Регистрация CA сертификата

Зарегистрировать CA сертификат в базе комплекса 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 комплекса и его не удалось получить по протоколу LDAP, то сертификат не принимается;
      - *none* – при проверке сертификата действующий CRL используется, если он предустановлен в базе комплекса 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 комплекса 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 комплекса:
  - можно задать несколько таких команд для добавления либо промежуточных CA сертификатов, либо любых CA сертификатов.

В отличие от Cisco, наш комплекс 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 комплекса.

При старте cs_console при поиске сертификата проверяются все существующие *trustpoint's* в базе комплекса. В случае отсутствия соответствующего CA сертификата в базе комплекса, *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 Bel VPN Gate можно при помощи утилиты cryptocont, которая размещается в каталоге opt/Avest/bin.

Контейнеры с секретными ключами должны быть уровня компьютера.

## Регистрация локального сертификата

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

## Удаление сертификатов

Удалять сертификаты из базы комплекса 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 комплекса 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 комплекса с 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 комплекса

Для просмотра сертификатов в базе комплекса 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 шлюз безопасности Bel VPN Gate 4.5 пытается получить сертификат партнера по IKE. Если партнер не прислал сертификат, а прислал свой идентификатор, то шлюз безопасности Bel VPN Gate 4.5 по этому идентификатору ищет сертификат партнера сначала в своей базе комплекса, 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 шлюз безопасности Bel VPN Gate 4.5 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 комплекса, 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 и RemoteID*;
- по составленному значению Subject шлюз безопасности ищет сертификат партнера сначала в своей базе комплекса, а затем на LDAP-сервере.

**В cisco-like конфигурации**

Если партнер не прислал свой сертификат по протоколу IKE, и в базе комплекса его нет, то шлюз безопасности Bel VPN Gate 4.5 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 комплекса;
- *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 комплекса 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 cisco-like консоли для установления соответствия между локальным, партнерским и CA сертификатами используются команды `set self-identity, set identity, set ca identity` (идентификаторы для сертификатов создаются при помощи команды `crypto identity`).

**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 комплексом, 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 комплекса на отдельные расширения сертификата, помеченные как критичные и отсутствующие в вышеприведенной таблице. Администратор может настроить список расширений сертификата, который будут игнорироваться комплексом, 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 комплексом `Critical Extentions`, например `BasicConstraints`.

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

# Приложение

## Текст -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=BY,L=Minsk,O=S-Terra Bel,OU=Research,CN=adminhost
!
crypto isakmp policy 1
 encr belt
 hash belt
 authentication belt-sig
 group beltdh
!
crypto ipsec transform-set TSET esp-belt esp-belt-mac
!
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 beltdh
 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:   Tue Jun 14 09:20:53 2016
GlobalParameters(
    Title                       = "This LSP was automatically generated by
CSP Converter at Tue Jun 14 09:20:53 2016"
    CRLHandlingMode             = OPTIONAL
    PreserveIPsecSA             = FALSE
)

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   = "STB34101CIPH-K256-CBC-65532"
    HashAlg     = "STB34101HASH-65532"
    GroupID     = BELTDH
    RestrictAuthenticationTo = BELT_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "STB34101CIPH-K256-MAC-65532"
        CipherAlg*          = "STB34101CIPH-K256-CBC-252"
        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=BY,L=Minsk,O=S-Terra
Bel,OU=Research,CN=adminhost"
    )
)

AuthMethodBELTSign BELT: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  = BELT:Sign
    MainModeAuthMethod  = BELT:Sign
    DoNotUseDPD         = TRUE
    Priority            = 100
)

IPsecAction IPsecAction:CMAP:1:DMAP:1
(
    TunnelingParameters = TunnelEntry(
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    GroupID = BELTDH
    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 Bel Client
AdminTool (cp) at 2016.06.14 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=BY,L=Minsk,O=S-Terra Bel, OU=Research,
CN=adminhost"
          )
)
CertDescription local_cert_dsc_01(
    Subject *= COMPLETE,"C=BY,L=Minsk,O=S-Terra Bel, OU=Research,
CN=adminhost"
    Issuer *= COMPLETE,"C=BY,L=Minsk,O=S-Terra Bel,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_01(
```

```
    LifetimeSeconds = 28800
    CipherAlg  *= "STB34101CIPH-K256-CBC-65532"
    HashAlg *= "STB34101HASH-65532"
    GroupID *= BELTDH
)
ESPTransform esp_trf_01(
    IntegrityAlg *= "STB34101CIPH-K256-MAC-65532"
    CipherAlg *= "STB34101CIPH-K256-CBC-252"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_01(
    Transform *=esp_trf_01
)
IKERule ike_rule(
    DoNotUseDPD = FALSE
    DPDIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_01
)
IPsecAction ipsec_action_01(
    TunnelingParameters *=
           TunnelEntry(
                  PeerIPAddress = 192.168.100.1
                  Assemble = TRUE
                  ReRoute = FALSE
           )
    ContainedProposals *= (esp_proposal_01)
    GroupID *= BELTDH
    IKERule = ike_rule_01
)
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
)
```