УТВЕРЖДЕНО

BY.РТНК.00001-03.01 34 01 17-ЛУ

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1»

ИНСТРУКЦИЯ АДМИНИСТРАТОРА КАТЕГОРИРОВАННОЙ СЕТИ

BY.РТНК.00001-03.01 34 01 17

Листов 20

Подп.	
Инв.	
Взам.	
Подп.	
Инд.	

2012

Содержание

1. Сокращения

ПАК Bel VPN Gate – Программно-аппаратный комплекс Шлюз безопасности Bel VPN Gate 3.0.1

ПАУ Bel VPN Client – Программно-аппаратное устройство Клиент безопасности Bel VPN Client 3.0.1

Package Maker – Утилита генерации дистрибутива Bel VPN Client из пакета Bel VPN Client 3.0.1 Admin Tool

2. Аннотация

Настоящий документ содержит описание действий администратора по установке, настройке и эксплуатации Программно-аппаратного комплекса «Шлюз безопасности Bel VPN Gate 3.0.1» и Программно-аппаратного устройства «Клиент безопасности Bel VPN Client 3.0.1» при использовании Продуктов в сетях с информацией ограниченного распространения.

3. Назначение

ПАК Bel VPN Gate и ПАУ Bel VPN Client предназначены для обеспечения:

- криптографической защиты передаваемой в режиме on-line по TCP/IP протоколу информации, не содержащих сведений, составляющих государственную тайну, между ПЭВМ абонентов;
- двусторонней криптографической аутентификации абонентов при установлении соединения в соответствии с протоколом ISAKMP.

4. Требования к системному ПО

ПАК Bel VPN Gate 3.0.1 функционирует на ПЭВМ с архитектурой Intel x86 под управлением операционной системы Red Hat Linux 9.

ПАУ Bel VPN Client 3.0.1 функционирует на ПЭВМ с архитектурой x86(32bit) под управлением операционных систем MS Windows XP/Vista/7.

5. Начало работы

5.1. Администратор ПАК должен изменить пароль на внешнем устройстве хранения информации (USB-носителе (в соответствии с **«Правилами выбора пароля»**, раздел 8 настоящей инструкции):

5.1.1. Подключить внешнее устройство хранения информации (ключевой usb-носитель) к АРМ Администратора (ПК с ОС Windows);

5.1.2. Вызвать утилиту AvPassInit.exe:

AvPassInit.exe –p=%new_password%,

где %new_password% - новый пароль, в соответсвии с разделом 8 «Правила выбора пароля»

5.1.3. Отключить ключевой usb-носитель от АРМ Администратора.

5.2. Подключить к ПАК Bel VPN Gate:

- питание 220В либо комплектный блок питания (в зависимости от поставки аппаратной платформы);
- VGA-монитор;
- USB(PS/2)-клавиатуру;
- внешнее устройство хранения информации (USB-носитель), совместимое с «AvCrypt 5.1»– по усмотрению пользователя.

5.3. Включить ПАК.

5.4. При старте ПАК после загрузки операционной системы автоматически запускается скрипт ***ipsetup*** для настройки сетевых параметров.

Шаг 1: У администратора запрашивается подтверждение на конфигурирование сетевых параметров: "`Would you like to configure network parameters?`" Если подтверждение на вопрос "`Configure network now?`" не будет получено, то будут использоваться установки по умолчанию, а инсталляция будет продолжена. После инсталляции администратор должен сконфигурировать сетевые интерфейсы.

Шаг 2: При получении подтверждения запрашивается информация о сетевых интерфейсах: "`Please, enter IP address/mask for eth0 or word "none" to disable the interface [10.10.10.1/24]:`" предлагается ввести IP-адрес и маску подсети для указанного сетевого интерфейса или слово "none" для отключения интерфейса. В квадратных скобках указано текущее значение IP-адреса/маски и формат, в котором они должны быть введены. При вводе в другом формате будет предложено ввести данные еще раз. Текущее значение сохраняется при вводе пустой строки. При нажатии комбинации Ctrl-C работа скрипта ipsetup прерывается.

Шаг 3: Предлагается ввести имя хоста: "`Please, specify hostname for this system [cspgate]:`" Предлагается ввести имя хоста. В квадратных скобках указано текущее имя хоста, которое сохранится при вводе пустой строки.

5.5. Затем запускается скрипт ***/opt/cspvpn/cspvpn_install.sh*** для инсталляции программного комплекса.

Инсталляцию Продукта Bel VPN Gate условно можно разделить на несколько фаз.

Подготовительная фаза установки. *При возникновении ошибки на этом этапе процесс установки прерывается. Сначала предлагается ознакомиться с файлом Лицензионного соглашения и сообщается о его местонахождении.*

Шаг 4: У администратора на консоли запрашивается подтверждение инсталляции: "`Do you want to install Bel VPN Gate 3.0.xxxx av now?`"
Если подтверждение не получено, продолжается нормальная загрузка системы, и при следующем старте снова будет запрашиваться подтверждение на инсталляцию. Если подтверждение получено, запускается процесс установки всего программного комплекса Bel VPN Gate.

Шаг 5: Далее инсталлятор запрашивает об использовании датчика случайных числовых последовательностей на базе AvPass RNG: "`Would you like to use AvPass RNG? [Yes]`". Следует ответить ***Yes***, после чего будет запрошен пароль для доступа к AvPass: *"Enter password: "*.

Основная фаза установки. *При возникновении ошибки на этой стадии процесс установки прерывается с последующей деинсталляцией успешно установившихся компонент.*

Устанавливается пакет VPNagent. Действия администратора не требуются.

Завершающая стадия установки. *При возникновении ошибки выводится предупреждение, но процесс установки продолжается.*

Шаг 6: В процессе инсталляции запрашивается лицензионная информация для Bel VPN Gate: "Would you like to enter license [Yes]?" Если администратор откажется от ввода Лицензии, то её потребуется ввести позже. Если администратор решил ввести Лицензию, то предлагаются следующие пункты для ввода:

- Available product codes:

  GATE100
  GATE100B
  GATE100V
  GATE1000
  GATE1000V
  GATE3000
  GATE7000
  GATE10000
  RVPN
  RVPNV
  UVPN
  UVPNV
  KZVPN
  KZVPNV
  BELVPN
  BELVPNV
- Enter product code: ввести **код продукта** с листа Лицензии
- Enter customer code: ввести **код конечного пользователя** с листа Лицензии
- Enter license number: ввести **номер лицензии** с листа Лицензии
- Enter license code: ввести **код лицензии** с листа Лицензии

Шаг 7: Следует вопрос о корректности введенных данных*:*`"Is the above data correct ?"` Следует ответить Yes.

После получения подтверждения инсталляция продолжается без дополнительных вопросов. Если подтверждение не получено, то предлагается ввести Лицензию еще раз.

5.6. Далее инсталляция продолжается без дополнительных вопросов. Запускается vpn-демон, создается пользователь "cscons" с назначенным ему начальным паролем "csp".

Если установка завершилась успешно, то выдается сообщение: "`Bel VPN Gate was successfully installed`". При последующих стартах системы скрипт, запрашивающий у администратора подтверждение на инсталляцию, не вызывается.

Если установка завершилась неуспешно, то об этом выдаётся соответствующее сообщение. При следующем старте комплекса у администратора снова будет запрашиваться подтверждение на инсталляцию.

При инсталляции Bel VPN Gate устанавливается `политика Default Driver Policy = Pass All`, при которой интерфейсы шлюза безопасности пропускают все пакеты в незащищенном виде

После инсталляции программного комплекса Bel VPN Gate в обязательном порядке:

1. Установить политику по-умолчанию *passdhcp*:
   1) Выполнить вход под учетной записью администратора root
   2) Выполнить в консоли команду *dp_mgr set –ddp passdhcp.*

      Данная политика запрещает прохождение пакетов любых IP-протоколов кроме DHCP.

2. Назначить учетной записи администратора root пароль (в соответствии с **«Правилами выбора пароля»**, раздел 8 настоящей инструкции):
   1) Выполнить вход под учетной записью администратора root
   2) Выполнить в консоли команду *passwd root*
   3) На запрос “New password: “ ввести новый пароль администратора
   4) На запрос “Retype new password: ” повторить пароль.
   5) Убедиться, что пароль успешно обновлен – будет выведено сообщение: *passwd: all authentication tokens updated successfully*
3. Назначить учетной записи администратора cscons пароль (в соответствии с **«Правилами выбора пароля»**, раздел 8 настоящей инструкции):
   1) Выполнить в консоли команду passwd cscons
   2) На запрос “New password: “ ввести новый пароль администратора cscons
   3) На запрос “Retype new password: ” повторить пароль.
   4) Убедиться, что пароль успешно обновлен – будет выведено сообщение: *passwd: all authentication tokens updated successfully*
4. Настроить политику безопасности для управления ПАК по протоколу *ssh*, мониторинга его работы по протоколу *smtp*, а также получения журнала аудита по протоколу *syslog* в соответствии с **«Политикой безопасности для удаленного управления ПАК»**, раздел 9 настоящей инструкции.

6. Настройка

При настройке политик Шлюза и Клиента безопасности администратор должен руководствоваться следующими правилами.

6.1. Должен быть установлен уровень детализации логирования не ниже **info** (установлен по-умолчанию):

- ПАК Bel VPN Gate:
  - Cisco-like config[1]: ***logging trap info***
    либо
  - LSP-config[2]: ****LogMessageLevel=INFO***
- ПАУ Bel VPN Client[3]: Package Maker, вкладка «Settings» → SysLog → Severity

6.2. При настройке политики безопасности ПАК ПАУ должны использоваться следующие параметры:

6.2.1. Протокол IKE:

6.2.1.1. Алгоритм хэширования: СТБ 1176.1-99 (установлен по умолчанию):

- ПАК Bel VPN Gate:
  - Cisco-like config: ***crypto policy → hash md5***
  - Lsp-config: ***IKETransform → HashAlg="STB1176199-65530"***
- ПАУ Bel VPN Client: Package Maker, вкладка «IKE» → IKE Proposals list → столбец Integrity, значение **СТБ 1176.1-99**

6.2.1.2. Алгоритм шифрования: ГОСТ 28147-89 (установлен по умолчанию):

- ПАК Bel VPN Gate:
  - Cisco-like config: ***crypto policy → encryption des***
  - Lsp-config: ***IKETransform → CipherAlg="G2814789CPRO1-K256-CBC-65530"***
- ПАУ Bel VPN Client: Package Maker, вкладка «IKE» → IKE Proposals list → столбец Encryption, значение **ГОСТ 28147-89**

6.2.1.3. Группа Диффи-Хеллмана:

- ПАК Bel VPN Gate:
  - Cisco-like config: ***crypto policy → group 5***
  - Lsp-config: ***IKETransform → GroupID="MODP_1536"***
- ПАУ Bel VPN Client: Package Maker, вкладка «IKE» → IKE Proposals list → столбец Group, значение **MODP_1536**

6.2.2. Протокол IPsec:

Должен использоваться протокол ESP со следующими параметрами:

6.2.2.1. Шифрование по алгоритму ГОСТ 28147-89 в режиме ГОС:

- ПАК Bel VPN Gate:
  - Cisco-like config: ***crypto ipsec transform-set esp-des*** *esp-md5-hmac*
  - LSP-config: ***ESPProposal → CipherAlg="G2814789CPRO1-K256-CBC-250"***
    - ПАУ Bel VPN Client: Package Maker, вкладка «IPsec» → IPsec Proposal list → столбец ESP Encryption, значение **ГОСТ 28147-89**

6.2.2.2. Контроль целостности ГОСТ 28147-89 в режиме вычисления имитовставки:

- ПАК Bel VPN Gate:
  - Cisco-like config: ***crypto ipsec transform-set*** *esp-des* ***esp-md5-hmac***
  - LSP-config: ***ESPProposal → CipherAlg="G2814789AV1-K256-MAC-65531"***

[1] См. «ПАК Шлюз безопасности Bel VPN Gate 3.0.1. Руководство администратора. Cisco-like команды»
[2] См. «ПАК Шлюз безопасности Bel VPN Gate 3.0.1. Руководство администратора. Создание конфигурационного файла»
[3] См. «ПАУ Клиент безопасности Bel VPN Client 3.0.1. Руководство оператора. Руководство администратора»

- ПАУ Bel VPN Client: Package Maker, вкладка «IPsec» → IPsec Proposal list → столбец ESP Integrity, значение **ГОСТ 28147-89**

6.2.2.3. Должна использоваться опция Perfect Forward Security (**pfs**) со значением группы Диффи-Хеллмана 1536:

- ПАК Bel VPN Gate:
  - Cisco-like config: ***crypto map → set pfsgroup5***
  - LSP-config: ***IPsecAction → GropuID=MODP_1536***
- ПАУ Bel VPN Client: Package Maker, вкладка «IPsec» → переключатель Group, значение **MODP_1536**

7. Эксплуатация

7.1. При запуске ПАК Шлюз безопасности администратор должен убедиться в успешном завершении операции проверки целостности и самотестирования ПО ПАК Bel VPN Gate:

Журнал syslog (удаленный либо локальный: ***/tmp/cspvpngate.log***) должен содержать строку вида:

Sep 18 21:11:20 gw1 cspvpn_vefiry: Verification SUCCESS: 79 files verified, где

Sep 18 21:11:20 –дата и время запуска ПАК

gw1 – hostname данного шлюза.

7.2. При эксплуатации ПАУ Клиент безопасности на операционной системе Microsoft Windows 7 необходимо отключить службу **«Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности»**, иначе корректная работа Клиента безопасности будет невозможна.

7.3. Автоматическая проверка целостности ПО ПАК производится раз в сутки.

7.4. Должен проводиться периодический (не реже 1 раза в месяц) контроль целостности ПО ПАК с помощью специализированной утилиты cspvpn_verify полученной из доверенного источника (диска из поставки ПАК), а также осмотр аппаратной платформы ПАК на отсутствие повреждений пломб. В случае обнаружения нарушения целостности ПО необходимо принять следующие меры:

1) зарегистрировать событие в журнале;

2) выполнить действия в соответствии с ведомственной инструкцией;

3) восстановить ПО в соответствии с инструкцией по восстановлению ПАК;

4) сменить используемые пароли.

7.5. Администратор должен выполнять периодическое резервное копирование журнала аудита устройства.

8. Правила выбора пароля

Пароли, используемые в ПАК и ПАУ должны соответствовать следующим правилам:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.п.) а также общепринятые сокращения (user, admin и.т.п.);
- при смене пароля новое значение должно отличаться от старого не менее чем на 5 символов.

9. Политика безопасности для удаленного управления ПАК

Предположим, что на ПАК Bel VPN Gate один сетевой интерфейс (FastEthernet0/1 с IP-адресом 192.168.13.1. см.Рисунок 1) подключен к локальной сети. К этой же локальной сети подключен ПК (АРМ администратора) с IP-адресом 192.168.13.2 для удаленной настройки шлюза и на нем установлен административный пакет Bel VPN Client AdminTool для создания инсталляционного пакета Bel VPN Client.

Изначально, аутентификация сторон осуществляется на предварительно согласованных ключах, затем – на сертификатах открытого ключа.

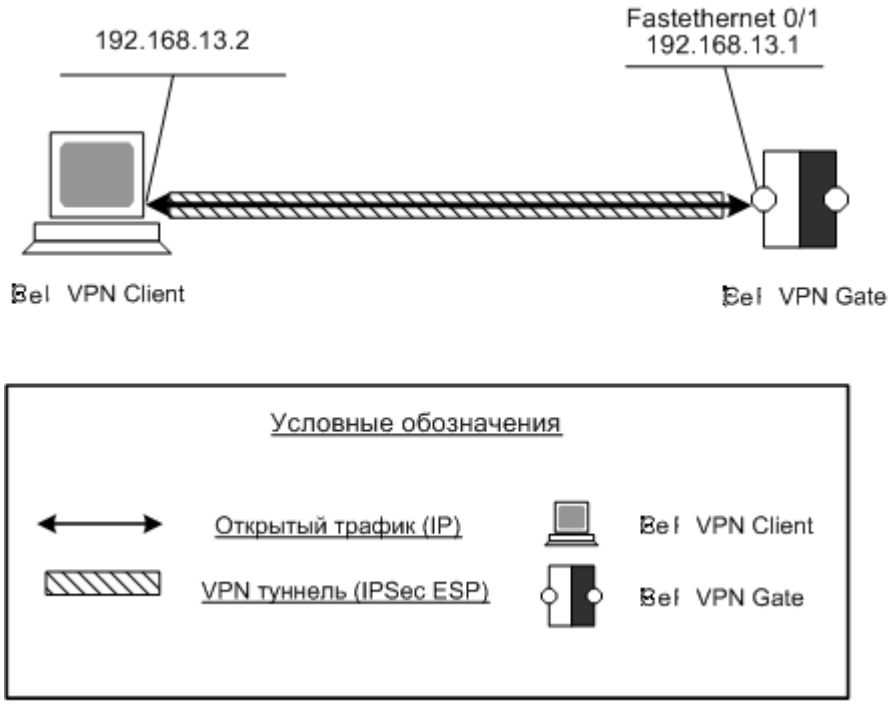

Рисунок 1

9.1. Настройка ПАК

9.1.1. Локально выполнить вход в систему под учетной записью cscons.

9.1.2. Включить отсылку журнала аудита на АРМ Администратора:

9.1.2.1. Добавить в файл /etc/hosts запись с адресом АРМ Администратора:

vi /etc/hosts

добавить строку: *192.168.13.2[TAB[4]]loghost*

9.1.2.2. Добавить в конфигурационный файл syslog (/etc/syslog.conf) запись следующего вида:

local7.[TAB]@loghost*

9.1.2.3. Перезапустить syslogd: killall –HUP syslogd

9.1.3. Ввести политику, выполнив следующие команды (строки, начинающиеся с # являются комментариями, в консоль не вводить; строки, заключенные в %% являются параметрами, значения вводить без %):

```
configure terminal

# идентификация партнера по адресу
crypto identity address

# включение логгирования
logging on
logging trap info
logging %любой_внутренний_сетевой_ip-адрес_ПАК%

#включение snmp
snmp-server community VPNGate ro
snmp-server host %адрес_АРМ_администратора% version 2c VPNGate
snmp-server enable traps
snmp-server trap-source

# основная политика для управления Шлюзом
crypto isakmp policy 1
      hash md5
      encryption des
      authentication rsa-sig
      group 5
      exit

#вспомогательная политика, используется для первоначальной настройки Шлюза
(передачи сертификатов открытого ключа)
crypto isakmp policy 2
      hash md5
      encryption des
      authentication pre-share
      group 5
      exit
```

[4] [TAB] означает вставку символа табуляции

```
crypto isakmp key %случайный_ключ(см.правила выбора пароля, раздел 8)% address
%адрес_АРМ_администратора%

crypto ipsec transform-set RemoteAdminTS esp-des esp-md5-hmac
      mode tunnel
      exit

ip access-list extended RemoteADminACL
      # SSH/SCP-доступ
      permit tcp host 192.168.13.1 eq 22 host %адрес_АРМ_администратора%
      # syslog-трафик, порт по умолчанию
      permit udp host 192.168.13.1 eq 514 host %адрес_АРМ_администратора%
      # snmp-трафик, порт по умолчанию
      permit udp host 192.168.13.1 eq 161 host %адрес_АРМ_администратора%
      exit

crypto map RemoteAdminCMAP 1 ipsec-isakmp
      match address RemoteAdminACL
      set transform-set RemoteAdminTS
      set pfs group5
      set peer %адрес_АРМ_администратора%
      exit

      # внутренний интерфейс
interface FastEthernet0/1
      crypto map RemoteAdminCMAP
      exit
end
```

9.1.4. Далее следует создать согласованную политику для Bel VPN Client (см п.9.2).

9.1.5. После создания согласованного клиента безопасности и установки его на АРМ администратора, необходимо:

9.1.5.1. Создать на ключевом носителе, подключенном к ПАК контейнер с личным ключом[5]:

(/opt/Avest/bin/)cryptocont n –n=avpass:%имя_контейнера% ***–p=***%пароль_от_контейнера%

9.1.5.2. Создать запрос на сертификат для вновь созданного личного ключа[4]:

cryptocont r –f=%путь_к_файлу_запроса% ***–n=avpass: %имя-контейнера%*** ***–p=***%пароль_от_контейнера%

9.1.5.3. Передать запрос на сертификат на АРМ Администратора (например, с помощью утилиты scp/WinSCP), используя ранее созданный защищенный канал связи.

9.1.5.4. Отправить запрос на сертификат в УЦ, обслуживающий организацию.

[5] Подробнее: см. документ «Шлюз безопасности Bel VPN 3.0.1. Руководство администратора. Приложение», раздел 7 «Создание локального сертификата при использовании AvCrypt ver.5.1»

9.1.5.5. После получения сертификата открытого ключа, передать его на ПАК, используя защищенный канал связи.

9.1.5.6. Зарегистрировать полученный сертификат, а также сертификат УЦ и СОС в базе продукта.

9.1.6. Далее следует переключить политику ПАК на аутентификацию по сертификатам:

```
configure terminal

# переключаем идентификацию партнера на идентификацию по сертификату
crypto identity dn

# основная политика для управления Шлюзом
crypto isakmp policy 1
      hash md5
      encryption des
      authentication rsa-sig
      group 5
      exit

# удаляем вспомогательную политику
no crypto isakmp policy 2

# удаляем pre-shared ключ
no crypto isakmp key %случайный_пароль(см.правила выбора пароля, раздел 8)% address
%адрес_АРМ_администратора%

end
```

Создать согласованную политику безопасности для Bel VPN Client (см п.9.3)

Внимание! При изменении политики безопасности шлюза необходимо сохранять правило, созданное для его настройки.

9.2. Создание пакета дистрибутива и конфигурации Клиента безопасности на pre-shared ключах

На компьютере с установленным административным пакетом Bel VPN Client AdminTool запускаем графический интерфейс (`Start → Programs → Bel VPN Client AdminTool → Package Maker`) и создаем согласованную со шлюзом политику для создания защищенного соединения между ними:

Шаг 1. Во вкладке Auth заполняем поля для настройки аутентификации на сертификатах открытого ключа (Рисунок 2):

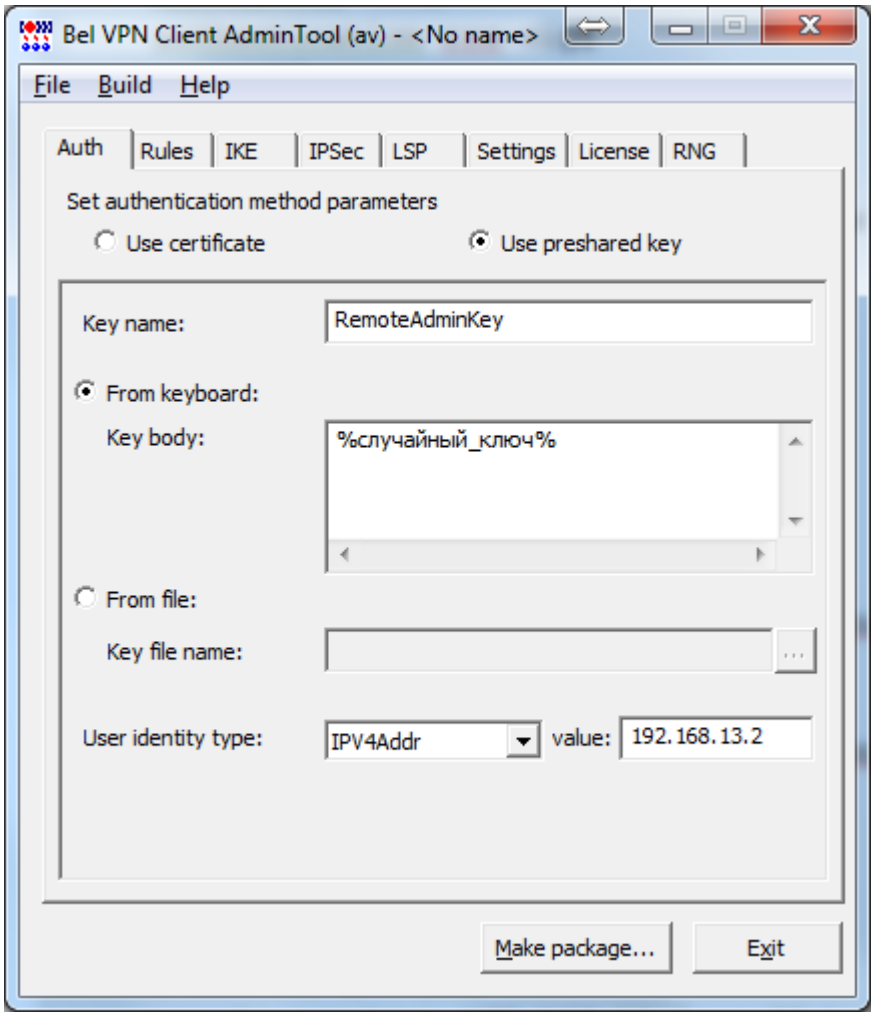

Рисунок 2

Шаг 2. Во вкладке Rules создаем правило для создания защищенного соединения. Для этого нажимаем кнопку *Add* и устанавливаем параметры для правила

- Блок Local IP Addresses: локальный IP-адрес АРМ администратора (192.168.13.2)
- Блок Partner IP Addresses: адрес Шлюза безопасности (192.168.13.1)
- Блок Services and Protocols: выбираем Custom и добавляем следующие протоколы:
  - SSH Client;
  - SNMP;
  - SNMP Trap;
  - UDP протокол с портом 514(соответствует протоколу syslog)
- Блок Action:
  1. Выбрать Protect using IPsec;
  2. Нажать Add и ввести адрес Шлюза безопасности.

Шаг 3. Во вкладке Rules для нового правила нажимаем кнопку Up для повышения приоритета. Вкладка Rules будет иметь следующий вид (Рисунок 3):

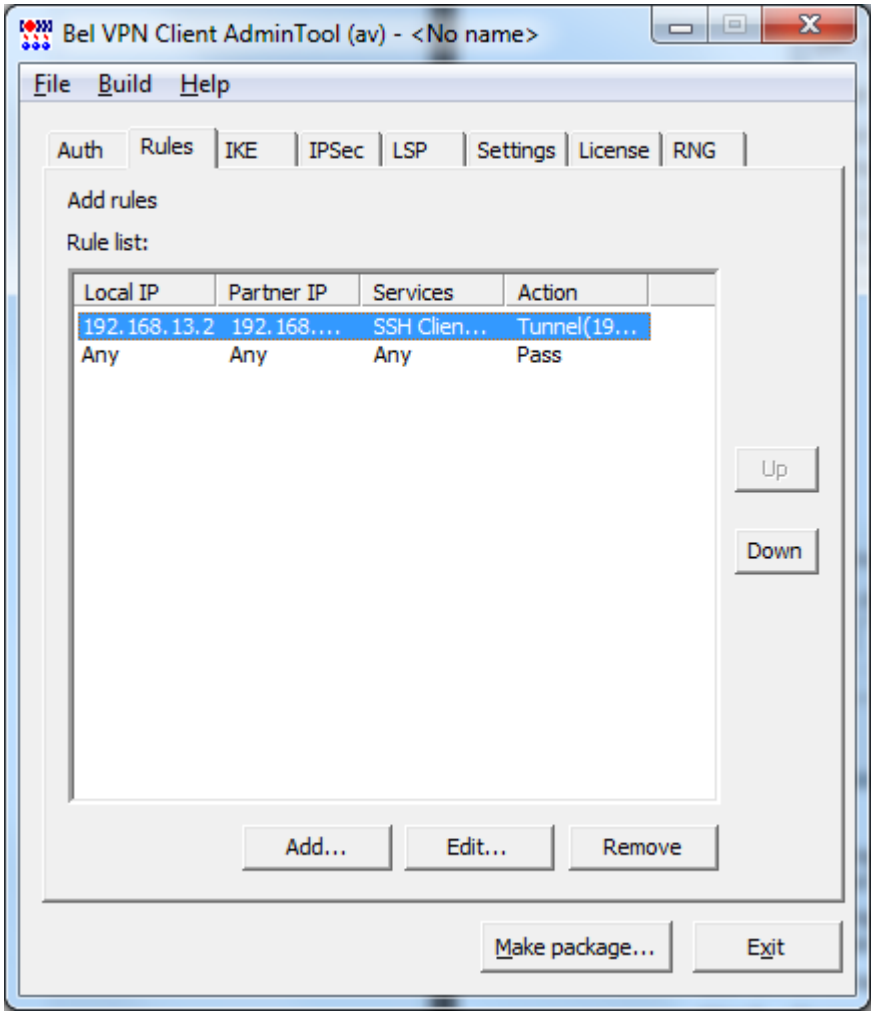

Рисунок 3

Шаг 4. Во вкладке *IKE* оставляем настройки без изменения.

Шаг 5. Во вкладке *IPsec* указываем значение группы **MODP_1536** для параметра Group, а также с помощью кнопки Up поднимаем на первую позицию запись с значения ESP Encryption=«ГОСТ 28147-89» и ESP Integrity=«ГОСТ 28147-89»(Рисунок 4):

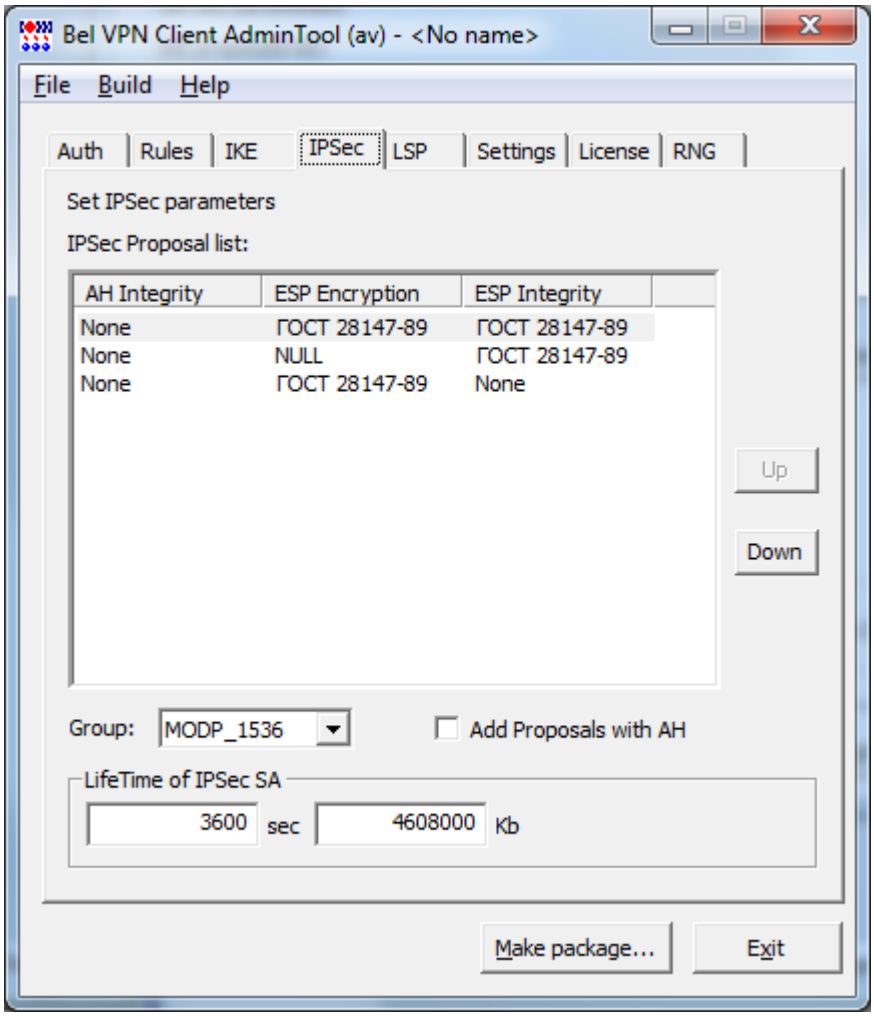

Рисунок 4

Шаг 6. Во вкладке Settings укажите настройки протоколирования событий: в выпадающем списке Severity оставить **info**.

Шаг 7. Во вкладке License введите регистрационные данные на продукт Bel VPN Client с бланка Лицензии.

Шаг 8. Во вкладке RNG выбрать **User hardware RNG on AvPass token**.

Шаг 9. После заполнения всех вкладок нажмите копку `Make package,` выберите тип инсталляции **Normal** и сохраните инсталляционный файл на диске.

Шаг 10. Установите на этом же компьютере Bel VPN Client, запустив созданный инсталляционный файл.

Таким образом, создана согласованная политика на шлюзе безопасности и клиенте, которая позволяет создавать *защищенный канал* для удаленной настройки шлюза при помощи консоли по протоколу SSH, а также получать записи системы логирования по протоколу syslog и статистику по протоколу snmp.

9.3. Создание пакета дистрибутива и конфигурации Клиента безопасности на сертификатах

Перед созданием пакета дистрибутива Клиента безопасности работающего с сертификатами открытых ключей необходимо инициализировать ключевой носитель (см. пункт 5.1 настоящей инструкции), создать секретный ключ и сертификат открытого ключа Администратора ПАК (см. документ «Шлюз безопасности Bel VPN 3.0.1. Руководство администратора. Приложение», раздел 7 «Создание локального сертификата при использовании AvCrypt ver.5.1»).

Предположим, что секретный ключ Администратора создан и сертификат открытого ключа Администратора получен.

На компьютере с установленным административным пакетом Bel VPN Client AdminTool запускаем графический интерфейс (`Start → Programs → Bel VPN Client AdminTool → Package Maker`) и создаем согласованную со шлюзом политику для создания защищенного соединения между ними:

Шаг 1. Во вкладке Auth заполняем поля для настройки аутентификации на сертификатах открытого ключа (Рисунок 2):

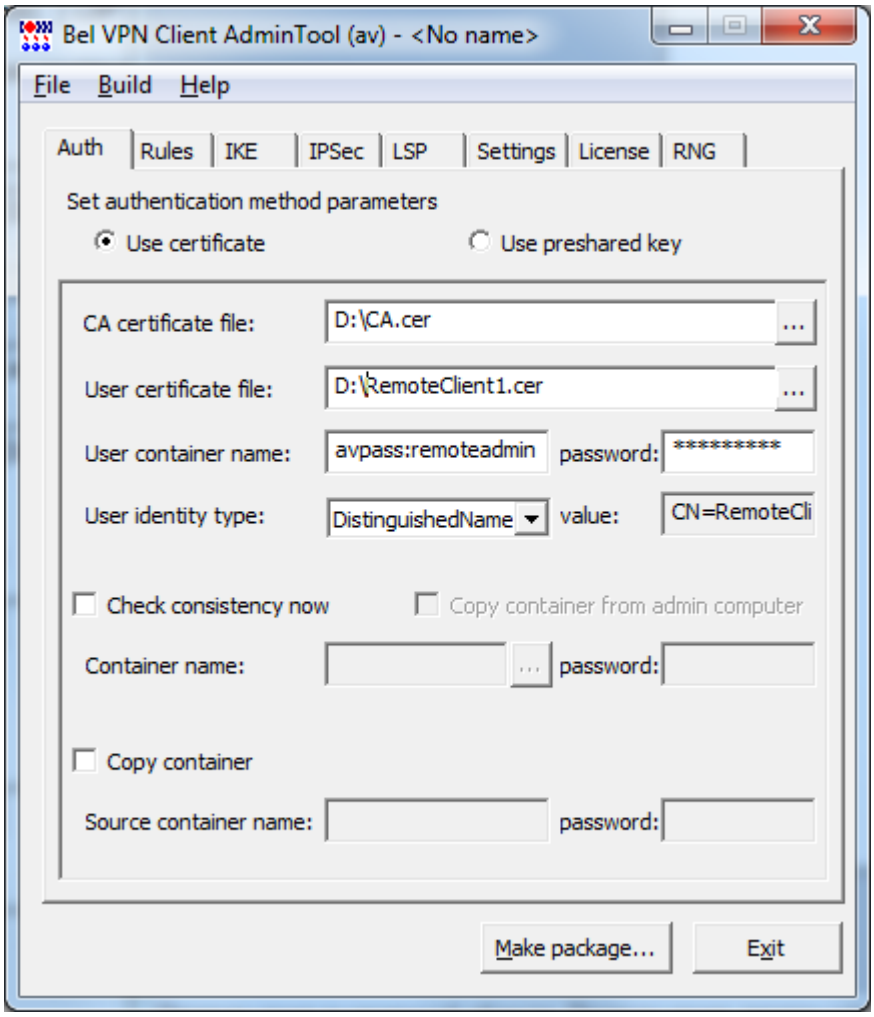

Рисунок 5

Шаг 2. Во вкладке Rules создаем правило для создания защищенного соединения. Для этого нажимаем кнопку *Add* и устанавливаем параметры для правила

- Блок Local IP Addresses: локальный IP-адрес АРМ администратора (192.168.13.2)
- Блок Partner IP Addresses: адрес Шлюза безопасности (192.168.13.1)
- Блок Services and Protocols: выбираем Custom и добавляем следующие протоколы:
  - SSH Client;
  - SNMP;
  - SNMP Trap;
  - UDP протокол с портом 514(соответствует протоколу syslog)
- Блок Action:
  3. Выбрать Protect using IPsec;
  4. Нажать Add и ввести адрес Шлюза безопасности.

Шаг 3. Во вкладке Rules для нового правила нажимаем кнопку Up для повышения приоритета. Вкладка Rules будет иметь следующий вид (Рисунок 3):

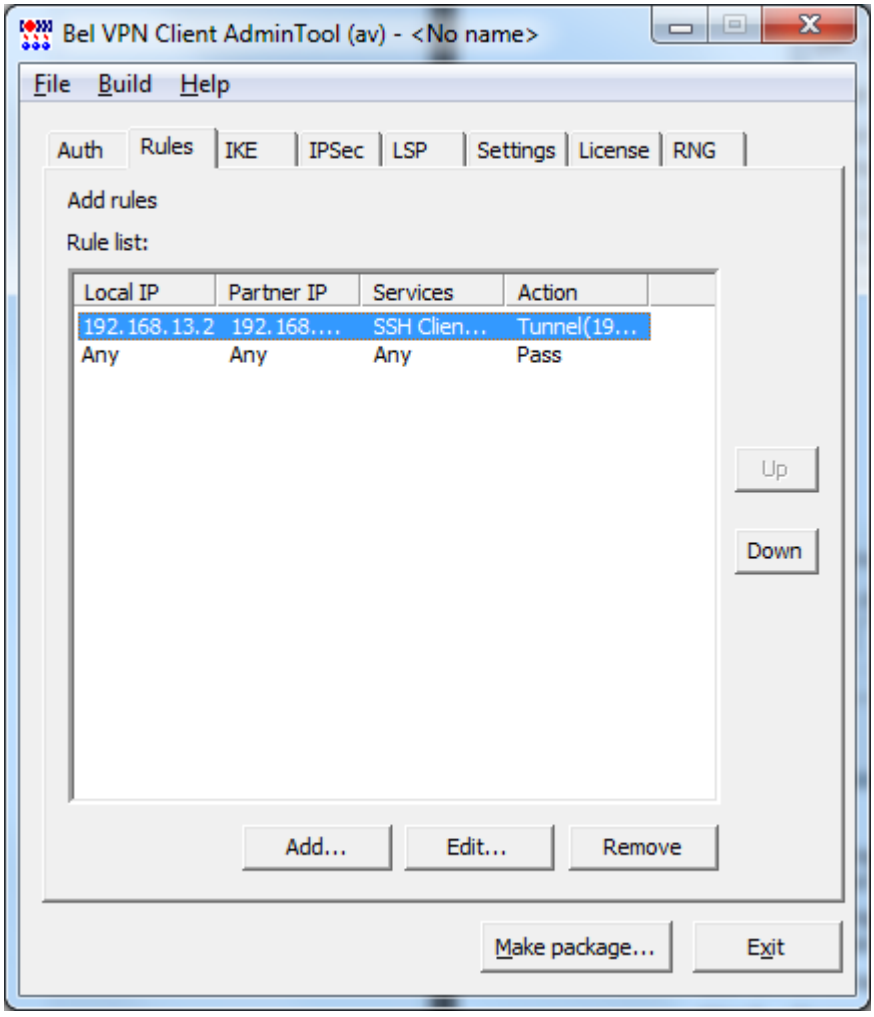

Рисунок 6

Шаг 4. Во вкладке *IKE* оставляем настройки без изменения.

Шаг 5. Во вкладке *IPsec* указываем значение группы **MODP_1536** для параметра Group, а также с помощью кнопки Up поднимаем на первую позицию запись с значениями ESP Encryption= «ГОСТ 28147-89» и ESP Integrity= «ГОСТ 28147-89» (Рисунок 4):

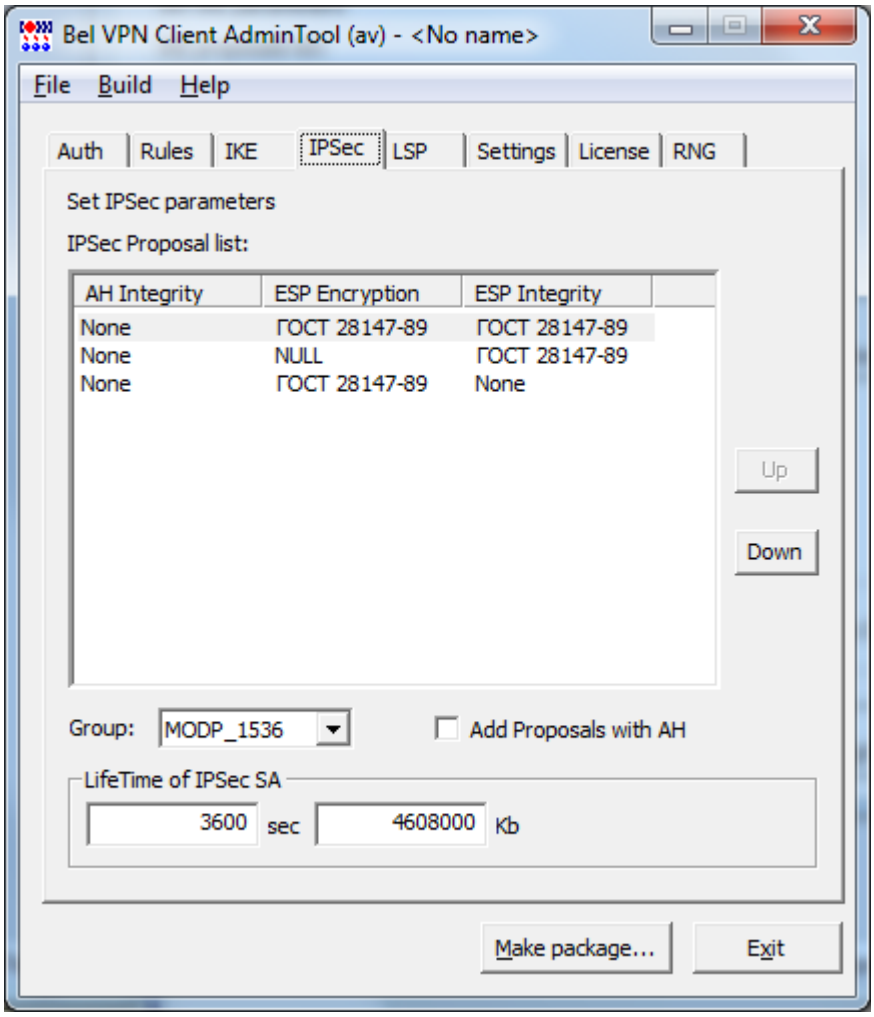

Рисунок 7

Шаг 6. Во вкладке Settings укажите настройки протоколирования событий: в выпадающем списке Severity оставить **info**.

Шаг 7. Во вкладке License введите регистрационные данные на продукт Bel VPN Client с бланка Лицензии.

Шаг 8. Во вкладке RNG выбрать **User hardware RNG on AvPass token**.

Шаг 9. После заполнения всех вкладок нажмите копку `Make package,` выберите тип инсталляции **Normal** и сохраните инсталляционный файл на диске.

Шаг 10. Установите на этом же компьютере Bel VPN Client, запустив созданный инсталляционный файл.

Таким образом, создана согласованная политика на шлюзе безопасности и клиенте, которая позволяет создавать *защищенный канал* для удаленной настройки шлюза при помощи консоли по протоколу SSH, а также получать записи системы логирования по протоколу syslog и статистику по протоколу snmp.