Построение VPN туннеля между удаленным клиентом и подсетью, защищаемой шлюзом безопасности Bel VPN Gate. Аутентификация на Preshared Key

Описание стенда

Сценарий представляет собой две подсети, которые защищаются шлюзами безопасности Bel VPN Gate. Для удаленного доступа к защищаемой подсети LAN2 в схеме присутствует компьютер с фиксированным IP-адресом. В качестве защиты подсетей используется VPN туннель между шлюзами безопасности. Подсети могут общаться между собой только по защищенному каналу (VPN). Также из подсети LAN2 возможно общение с Host 3 по защищенному каналу (VPN).

Настройка политики безопасности на шлюзах производится с учетом положений инструкции администратора категорированной сети (см. «Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1.» Инструкция администратора категорированной сети»).

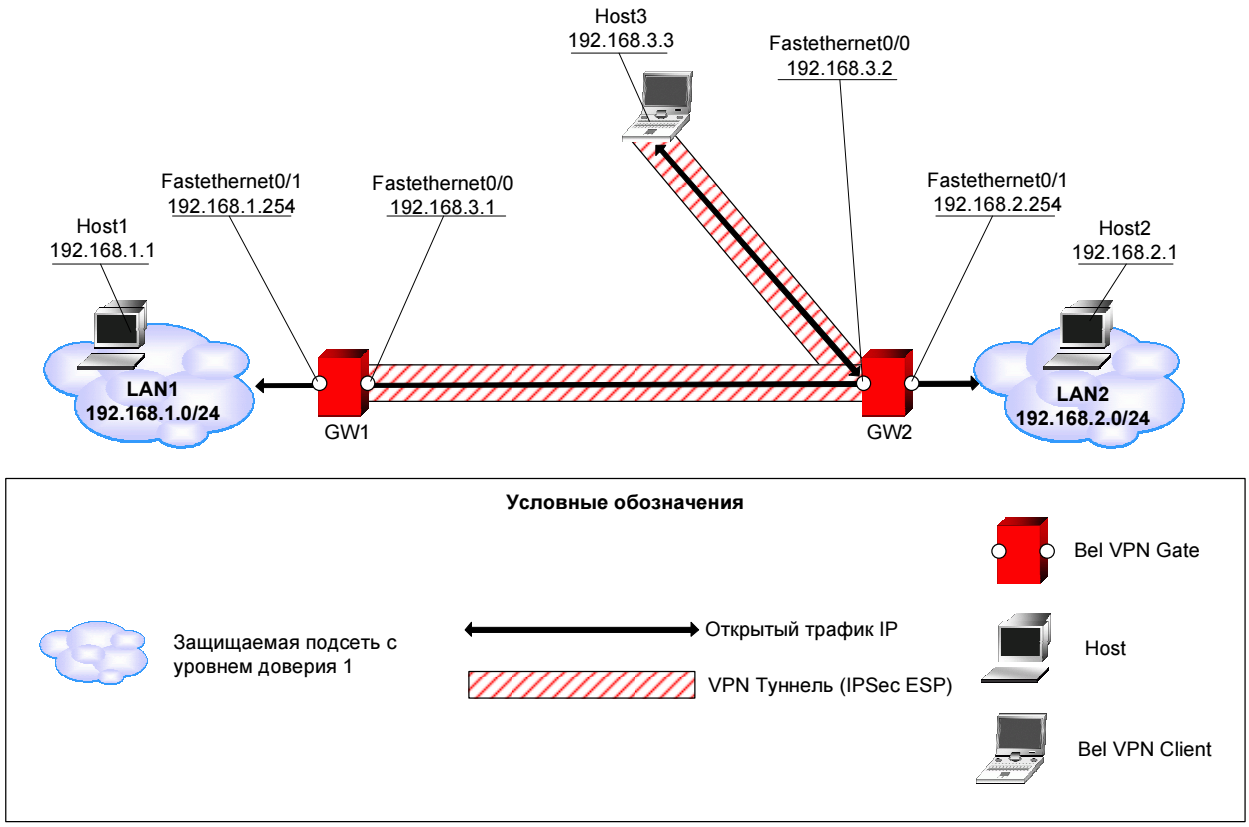

Рис. 1. Схема стенда

Параметры защищенных соединений между подсетями, между Host 3 и GW2:

- Аутентификация на Preshared Key.
- IKE parameters:
  - Encryption algorithm – ГОСТ 28147-89
  - Hash algorithm – СТБ 1176.1-99
  - DH-group – group5 (1536)

- IPSec parameters:
  - ESP encryption algorithm – ГОСТ 28147-89
  - ESP integrity algorithm – ГОСТ 28147-89
  - PFS – group5 (1536)

Сконфигурируем сначала два шлюза безопасности GW1 и GW2. Затем создадим инсталляционный пакет Bel VPN Client и установим его на Host 3.

Предварительные настройки

Перед созданием защищенного соединения необходимо настроить маршрутизацию и убедиться в том, что на устройствах стенда сделаны корректные настройки. Для этого нужно:

1. На устройстве Host1 задать команду: ping 192.168.2.1 и убедиться, что на echo request приходят echo reply с этого адреса:

   ping 192.168.2.1

   Pinging 192.168.2.1 with 32 bytes of data:

   Reply from 192.168.2.1: bytes=32 time<1ms TTL=128

   Reply from 192.168.2.1: bytes=32 time<1ms TTL=128

   Reply from 192.168.2.1: bytes=32 time<1ms TTL=128

   Reply from 192.168.2.1: bytes=32 time<1ms TTL=128

   Ping statistics for 192.168.2.1:

   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

   Approximate round trip times in milli-seconds:

   Minimum = 0ms, Maximum = 0ms, Average = 0ms

2. На устройстве Host1 задать команду tracert 192.168.2.1 (или ей аналогичную) и убедиться, что вывод совпадает с приведенным ниже в примере:

   tracert 192.168.2.1

   Tracing route to 192.168.2.1 over a maximum of 30 hops

   1 <1 ms <1 ms <1 ms 192.168.1.254

   2 <1 ms <1 ms <1 ms 192.168.3.2

   3 <1 ms <1 ms <1 ms 192.168.2.1

   Trace complete.

3. На устройстве Host2 задать команду: ping 192.168.3.3 и убедиться, что на echo request приходят echo reply с этого адреса.

4. На устройстве Host2 задать команду tracert 192.168.3.3 (или ей аналогичную) и убедиться, что вывод совпадает с приведенным ниже в примере:

   tracert 192.168.3.3

   Tracing route to 192.168.3.3 over a maximum of 30 hops

   1 <1 ms <1 ms <1 ms 192.168.2.254

   2 <1 ms <1 ms <1 ms 192.168.3.3

   Trace complete.

Конфигурирование GW1

Настройку шлюза безопасности GW1 будем производить в интерфейсе командной строки. Для входа в консоль перейдем в директорию `/opt/VPNagent/bin/` и запустим `cs_console`. В глобальном конфигурационном режиме выполним следующее:

Зададим сначала тип идентификатора ключа- identity. В качестве типа identity будем использовать address:

```
gw1(config)#crypto isakmp identity address
```

зададим параметры для IKE:

```
gw1(config)#crypto isakmp policy 1
gw1(config-isakmp)#hash md5
gw1(config-isakmp)#encryption des
gw1(config-isakmp)#authentication pre-share
gw1(config-isakmp)#group 5
gw1(config-isakmp)#exit
```

создадим предопределенные ключи для шлюза GW2:

```
gw1(config)#crypto isakmp key 1234567890 address 192.168.3.2
```

создадим набор преобразований для IPsec:

```
gw1(config)#crypto ipsec transform-set TS1 esp-des esp-md5-hmac
gw1(cfg-crypto-trans)#mode tunnel
gw1(cfg-crypto-trans)#exit
```

опишем трафик, который планируется защищать:

```
gw1(config)#ip access-list extended LAN1toLAN2
gw1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
gw1(config-ext-nacl)#exit
```

создадим криптокарту:

```
gw1(config)#crypto map CMAP 1 ipsec-isakmp
gw1(config-crypto-map)#match address LAN1toLAN2
gw1(config-crypto-map)#set transform-set TS1
gw1(config-crypto-map)#set pfs group5
gw1(config-crypto-map)#set peer 192.168.3.2
```

привяжем криптокарту к интерфейсу, на котором будут терминироваться туннели:

```
gw1(config)#interface FastEthernet0/0
gw1(config-if)# crypto map CMAP
gw1(config-if)#exit
```

Настройка устройства GW1 завершена. При выходе из конфигурационного режима произойдет загрузка конфигурации. Устройство готово к работе.

Текст cisco-like конфигурации для GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons privilege 15 password 0 csp
hostname GW1
enable password csp
!
!
!
!
!
crypto isakmp policy 1
 hash md5
 encr des
 authentication pre-share
 group 5
!
crypto isakmp key 1234567890 address 192.168.3.2
!
crypto ipsec transform-set TS1 esp-des esp-md5-hmac
!
ip access-list extended LAN1toLAN2
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LAN1toLAN2
 set transform-set TS1
 set pfs group5
 set peer 192.168.3.2
!
!
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 crypto map CMAP
!
interface FastEthernet0/1
 ip address 192.168.1.254 255.255.255.0
!
!
end
```

Текст LSP для GW1

Используйте утилиту lsp_mgr show из /opt/VPNagent/bin для просмотра текста LSP, которая была сконфигурирована на GW1:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Sat Apr 12 23:21:43 2014


GlobalParameters(
    Title                       = "This LSP was automatically generated by
CSP Converter at Sat Apr 12 23:21:43 2014"
    Version                     = "2.1"
    LDAPLogMessageLevel         = INFO
    SystemLogMessageLevel       = INFO
    PolicyLogMessageLevel       = INFO
    CertificatesLogMessageLevel = INFO
)


SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)


IKETransform IKETransform_1
(
    CipherAlg   *= "G2814789CPRO1-K256-CBC-65530"
    HashAlg     *= "STB1176199-65530"
    GroupID     *= MODP_1536
    LifetimeSeconds = 86400
)


ESPProposal ESP_TS1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)


AuthMethodPreshared IKE_auth_cs_key_192_168_3_2
(
    RemoteID = IdentityEntry(
```

```
        IPv4Address *= 192.168.3.2
    )
    SharedIKESecret = "cs_key_192_168_3_2"
)

IKERule IKE_CMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_3_2
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_3_2
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_1
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.3.2

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_1
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth0"
    Action *= ( PASS )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
```

```
        PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
        NetworkInterfaces *= "eth1"
        Action *= ( PASS )
    )
```

Конфигурирование GW2

Настройку шлюза безопасности GW2 будем производить в интерфейсе командной строки так же как и для GW1. Для входа в консоль перейдем в директорию `/opt/VPNagent/bin/` и запустим `cs_console`. В глобальном конфигурационном режиме выполним следующее:

Зададим сначала тип идентификатора ключа- identity. В качестве типа identity будем использовать address:

```
gw1(config)#crypto isakmp identity address
```

зададим параметры для IKE:

```
gw2(config)#crypto isakmp policy 1
gw2(config-isakmp)#hash md5
gw2(config-isakmp)#encryption des
gw2(config-isakmp)#authentication pre-share
gw2(config-isakmp)#group 5
gw2(config-isakmp)#exit
```

создадим предопределенные ключи для шлюза GW1:

```
gw2(config)#crypto isakmp key 1234567890 address 192.168.3.1
```

создадим предопределенные ключи для клиента:

```
gw2(config)#crypto isakmp key 12345 address 192.168.3.3
```

создадим набор преобразований для IPsec:

```
gw2(config)#crypto ipsec transform-set TS1 esp-des esp-md5-hmac
gw2(cfg-crypto-trans)#mode tunnel
gw2(cfg-crypto-trans)#exit
```

опишем трафик, который планируется защищать:

```
gw2(config)#ip access-list extended LAN2toLAN1
gw2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255
gw2(config-ext-nacl)#exit

gw2(config)#ip access-list extended LAN2toRemoteClient
gw2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.3.3
0.0.0.0
gw2(config-ext-nacl)#exit
```

создадим криптокарту с 2 записями:

```
gw2(config)#crypto map CMAP 1 ipsec-isakmp
gw2(config-crypto-map)#match address LAN2toLAN1
gw2(config-crypto-map)#set transform-set TS1
gw2(config-crypto-map)#set pfs group5
gw2(config-crypto-map)#set peer 192.168.3.2

gw2(config)#crypto map CMAP 2 ipsec-isakmp
```

```
gw2(config-crypto-map)#match address LAN2toRemoteClient
gw2(config-crypto-map)#set transform-set TS1
gw2(config-crypto-map)#set pfs group5
gw2(config-crypto-map)#set peer 192.168.3.3
```

привяжем криптокарту к интерфейсу, на котором будут терминироваться туннели:

```
gw2(config)#interface FastEthernet0/0
gw2(config-if)# crypto map CMAP
gw2(config-if)#exit
```

Настройка устройства GW2 завершена. При выходе из конфигурационного режима произойдет загрузка конфигурации. Устройство готово к работе.

Текст cisco-like конфигурации для GW2

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons privilege 15 password 0 csp
hostname GW2
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 hash md5
 encr des
 authentication pre-share
 group 5
!
crypto isakmp key 12345 address 192.168.3.3
!
crypto isakmp key 1234567890 address 192.168.3.1
!
crypto ipsec transform-set TS1 esp-des esp-md5-hmac
!
ip access-list extended LAN2toLAN1
 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
ip access-list extended LAN2toRemoteClient
```

```
 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.3
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LAN2toLAN1
 set transform-set TS1
 set pfs group5
 set peer 192.168.3.1
!
crypto map CMAP 2 ipsec-isakmp
 match address LAN2toRemoteClient
 set transform-set TS1
 set pfs group5
 set peer 192.168.3.3
!
!
!
interface FastEthernet0/0
 ip address 192.168.3.2 255.255.255.0
 crypto map CMAP
!
interface FastEthernet0/1
 ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0/2
 ip address 10.10.10.50 255.255.255.0
!
!
!
end
```

Текст LSP для GW2

Используйте утилиту lsp_mgr show из /opt/VPNagent/bin для просмотра текста LSP, которая была lзагружена на шлюз безопасности GW2:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Sun Apr 13 01:40:27 2014


GlobalParameters(
    Title                       = "This LSP was automatically generated by
CSP Converter at Sun Apr 13 01:40:27 2014"
    Version                     = "2.1"
    LDAPLogMessageLevel         = DEBUG
    SystemLogMessageLevel       = DEBUG
    PolicyLogMessageLevel       = DEBUG
    CertificatesLogMessageLevel = DEBUG
```

```
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

IKETransform IKETransform_1
(
    CipherAlg   *= "G2814789CPRO1-K256-CBC-65530"
    HashAlg     *= "STB1176199-65530"
    GroupID     *= MODP_1536
    LifetimeSeconds = 86400
)

ESPProposal ESP_TS1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

ESPProposal ESP_TS1_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

AuthMethodPreshared IKE_auth_cs_key_192_168_3_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.3.1
    )
    SharedIKESecret = "cs_key_192_168_3_1"
)
```

```
IKERule IKE_CMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_3_1
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_3_1
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_1
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.3.1

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_1
)

AuthMethodPreshared IKE_auth_cs_key_192_168_3_3
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.3.3
    )
    SharedIKESecret = "cs_key_192_168_3_3"
)

IKERule IKE_CMAP_2
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_3_3
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_3_3
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.3.3

        DFHandling=COPY
    )
```

```
    ContainedProposals *= ( ESP_TS1_1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_2
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl_CMAP_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.3.3 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_2 )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth0"
    Action *= ( PASS )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth1"
    Action *= ( PASS )
)
```

Создание инсталляционного пакета Bel VPN Client

Ниже опишем создание инсталляционного пакета Bel VPN Client для установки на Host3.

В этот пакет мы включим политику безопасности, которая будет состоять из правила доступа в защищенную подсеть (192.168.2.2/24) по протоколу IKE/IPSec. Аутентификация будет проводиться на предопределенных ключах. В качестве идентификатора будем использовать IP Address. Предполагается, что Bel VPN Client будет установлен на стационарный компьютер, имеющий постоянный IP Address.

Настройка безопасности на клиенте производится с учетом положений инструкции администратора категорированной сети (см. «Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1.» Инструкция администратора категорированной сети»)

1. Запускаем Bel Client Administrator Package Maker:

   ```
   Start – Programs – Bel VPN Client AdminTool av– Package Maker.
   ```

   Откроется главное окно приложения, показанное на Рис. 1 на первой вкладке – Auth. В этой вкладке производятся настройки аутентификации.

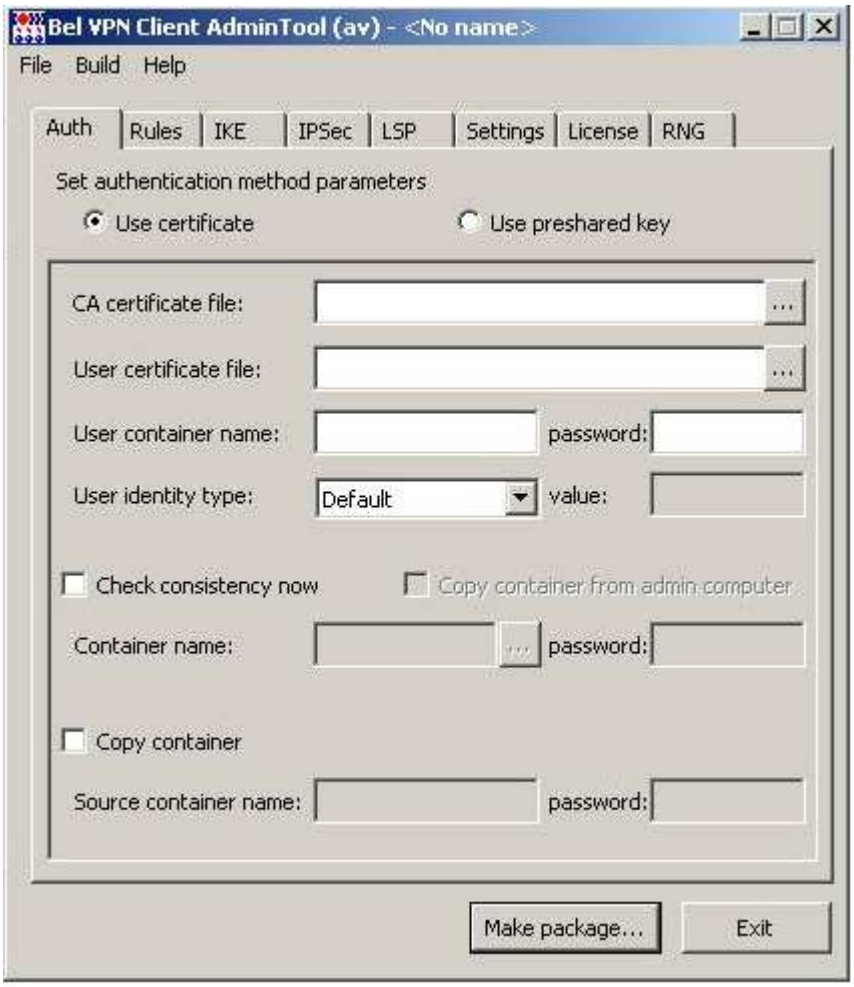

Рис. 1

2. Так как мы будем проводить аутентификацию на Preshared Keys, установим переключатель в положение Use Preshared Key. При этом изменится состав элементов конфигурирования (Рис. 2). В этом окне произведем следующие настройки:

   - Присвоим ключу имя – key
   - Установим значение ключа, равное 12345, которое было установлено у шлюза безопасности GW2 для связи с Host3.
   - Установим User Identity Type = IPV4Addr
   - Введем в поле Value адрес компьютера, на котором будет установлен Bel VPN Client – 192.168.3.3

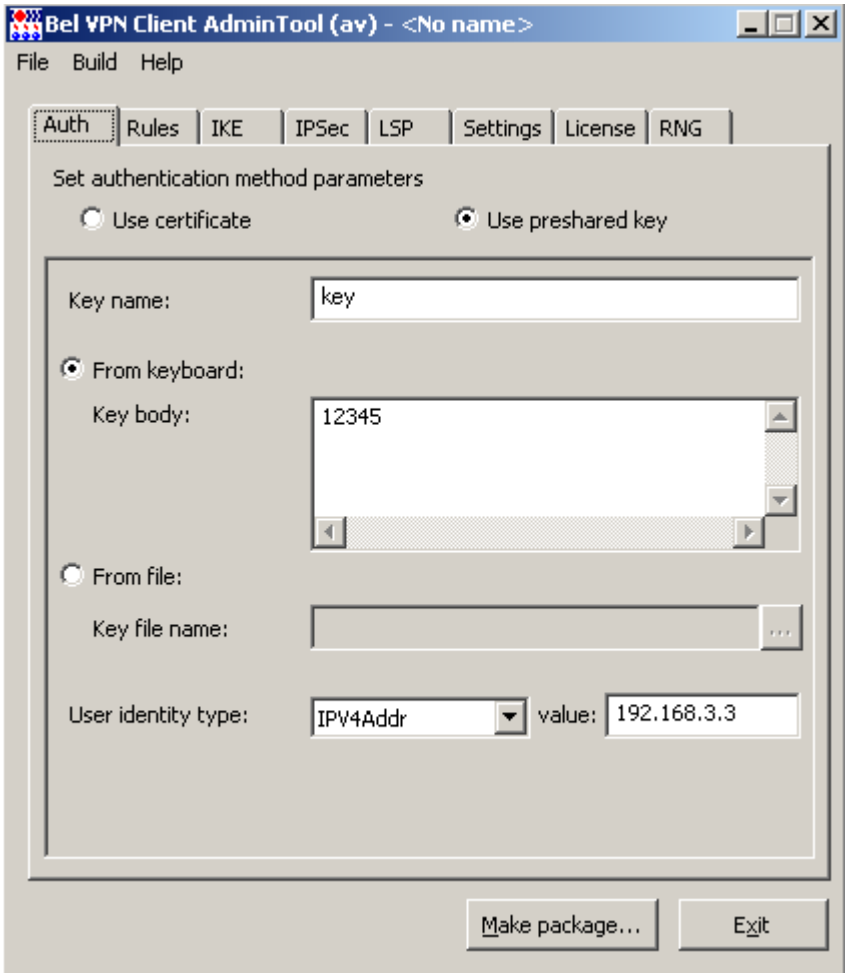

Рис. 2

3. Переходим во вкладку Rules.

   Вкладка содержит предустановленное правило Any to Any Pass. Это правило разрешает открытый трафик ко всем ресурсам Интернета. Однако, так как подсеть 192.168.2.0 защищена Bel VPN Gate, то доступ к ней разрешен только по защищенному каналу. Мало того, по защищенному каналу разрешен доступ только владельцам определенных сертификатов и ключей. Нам нужно создать правило доступа в подсеть 192.168.2.0 по защищенному каналу (IPSec).

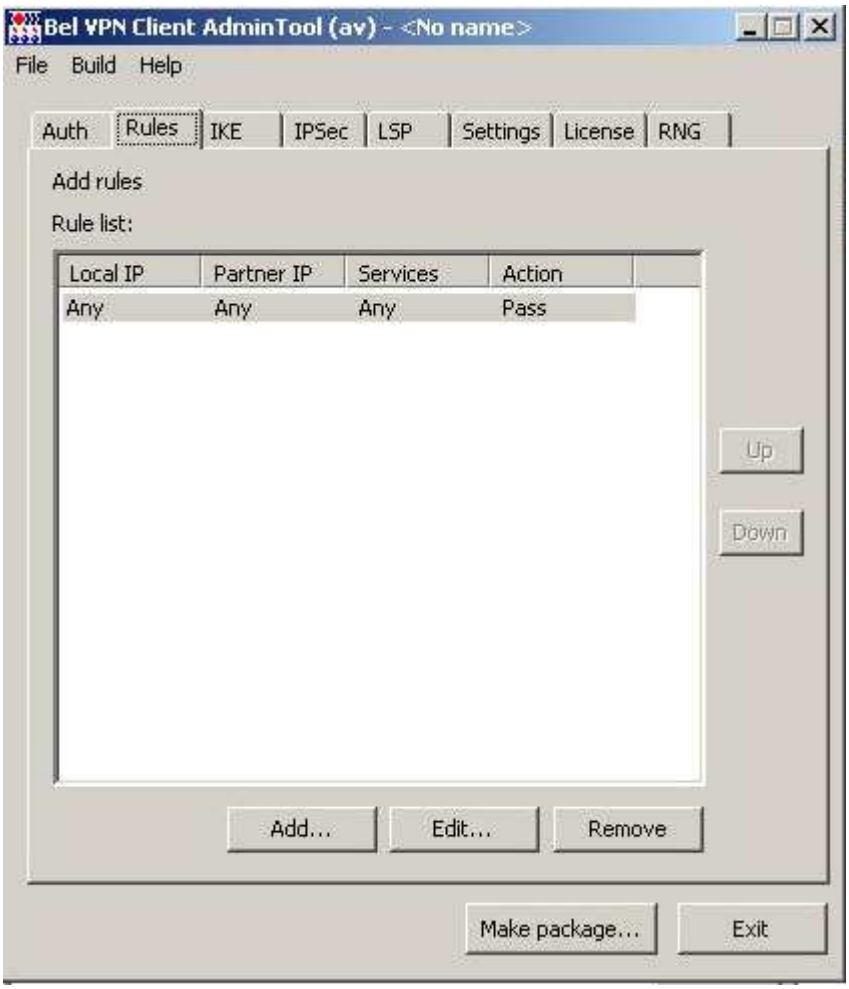

Рис. 3

4. Создаем новое правило. Для этого нажимаем кнопку Add. Откроется окно создания нового правила. Мы создадим правило, которое будет отвечать за шифрование трафика от локального компьютера в защищенную подсеть 192.168.2.0/24. Для этого выполним:

- В группах Local IP Address и Services and Protocols оставляем все без изменений (Any, Any)
- В группе Partner IP Address выбираем режим Custom и регистрируем адрес подсети, с которой мы планируем общаться по защищенному каналу. Для этого нажимаем кнопку Add и в открывшемся окне вводим адрес и маску подсети 192.168.2.0 и нажимаем OK (Рис. 24)..
- В группе Action устанавливаем переключатель в положение Protect using IPsec, нажимаем кнопку Add и в открывшемся окне вводим IP Address интерфейса шлюза безопасности, защищающего подсеть 192.168.2.0. Согласно нашей схеме это будет адрес 192.168.3.2 (Рис. 5).

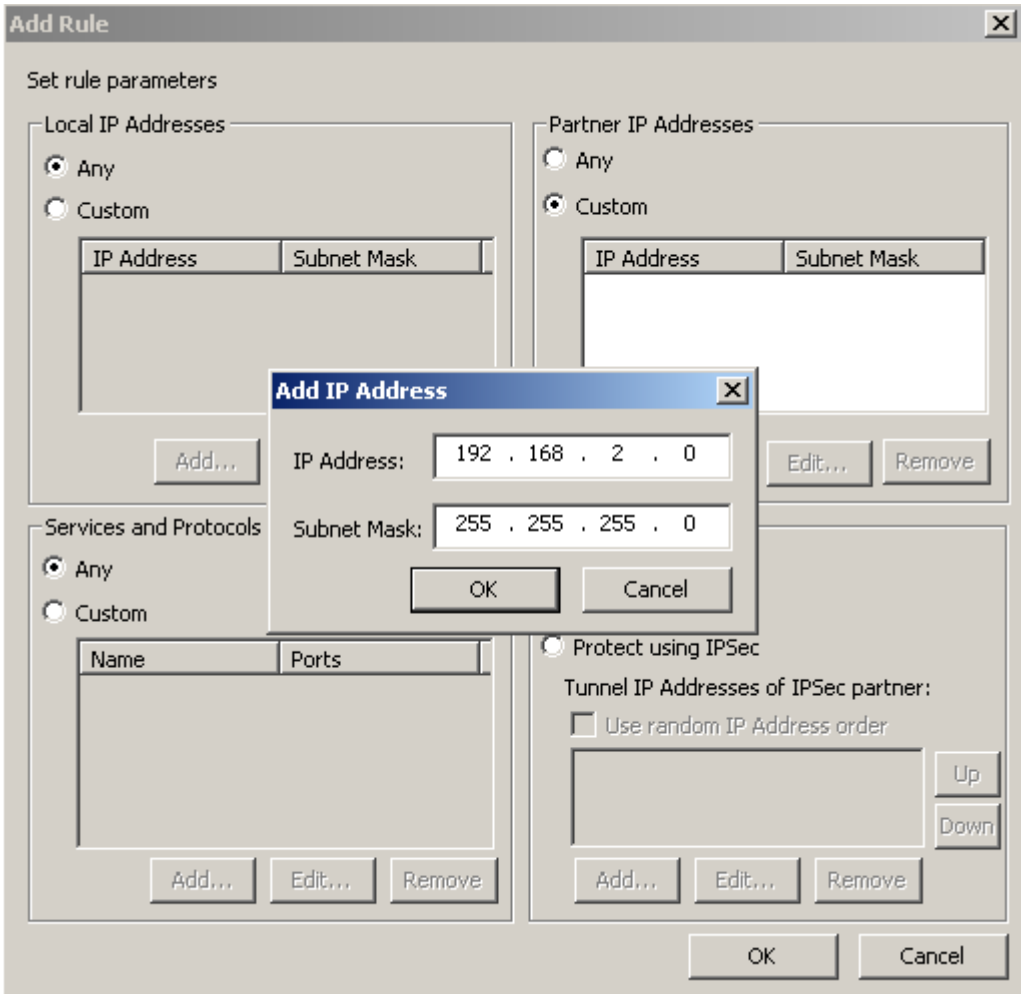

Рис. 2

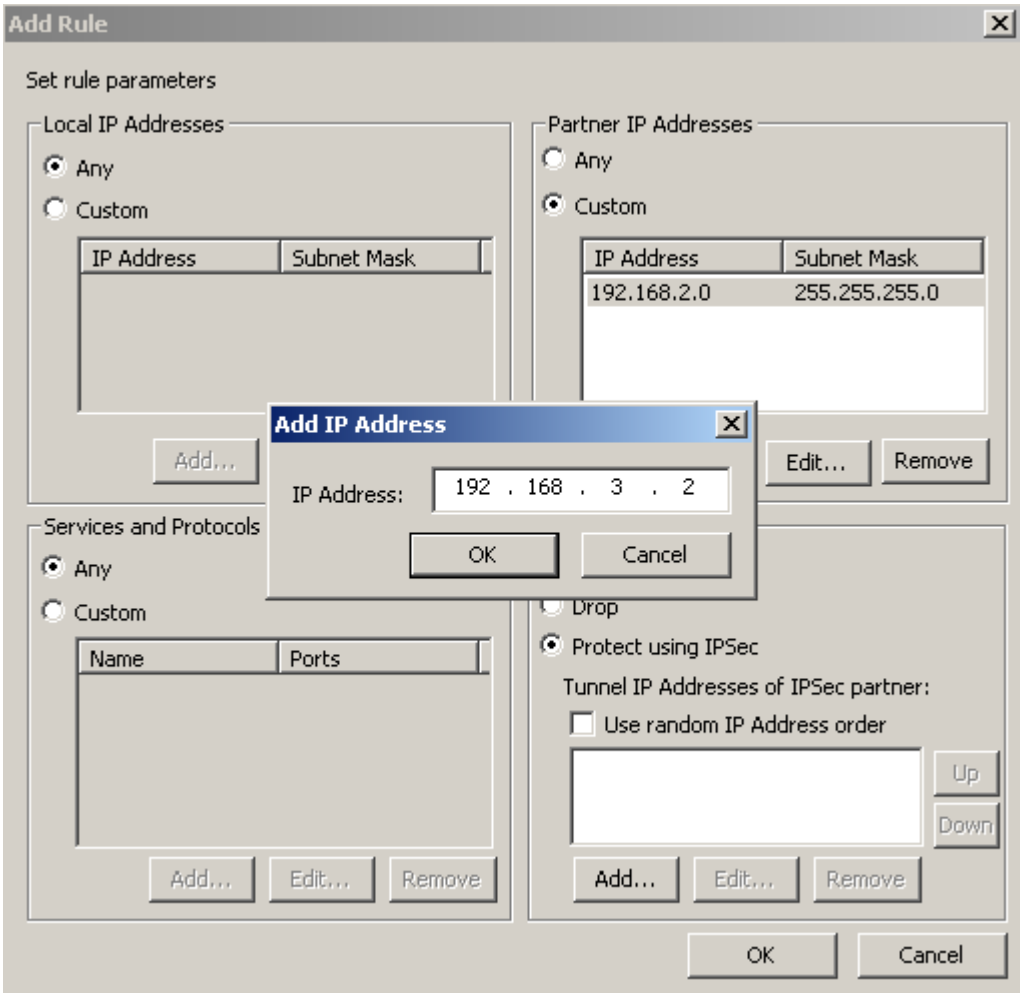
Add Rule
Set rule parameters
Local IP Addresses
Any
Custom
IP Address
Subnet Mask
Add...
Partner IP Addresses
Any
Custom
IP Address
Subnet Mask
192.168.2.0
255.255.255.0
Edit...
Remove
Add IP Address
IP Address:
192 . 168 . 3 . 2
OK
Cancel
Services and Protocols
Any
Custom
Name
Ports
Add...
Edit...
Remove
Drop
Protect using IPSec
Tunnel IP Addresses of IPSec partner:
Use random IP Address order
Up
Down
Add...
Edit...
Remove
OK
Cancel

Рис. 5

5. Нажимаем ОК и возвращаемся в главное окно. В этом окне появилась строка только что созданного правила (Рис. 6).
6. Однако, это правило не будет работать, так как перед ним стоит правило Any to Any Pass. Чтобы наше правило стало актуальным, его следует переместить на первую позицию. Эту операцию мы выполняем с помощью кнопки Up. Выделяем строку только что созданного правила и нажимаем кнопку Up. Выделенное правило переместится в начало списка (Рис. 7).

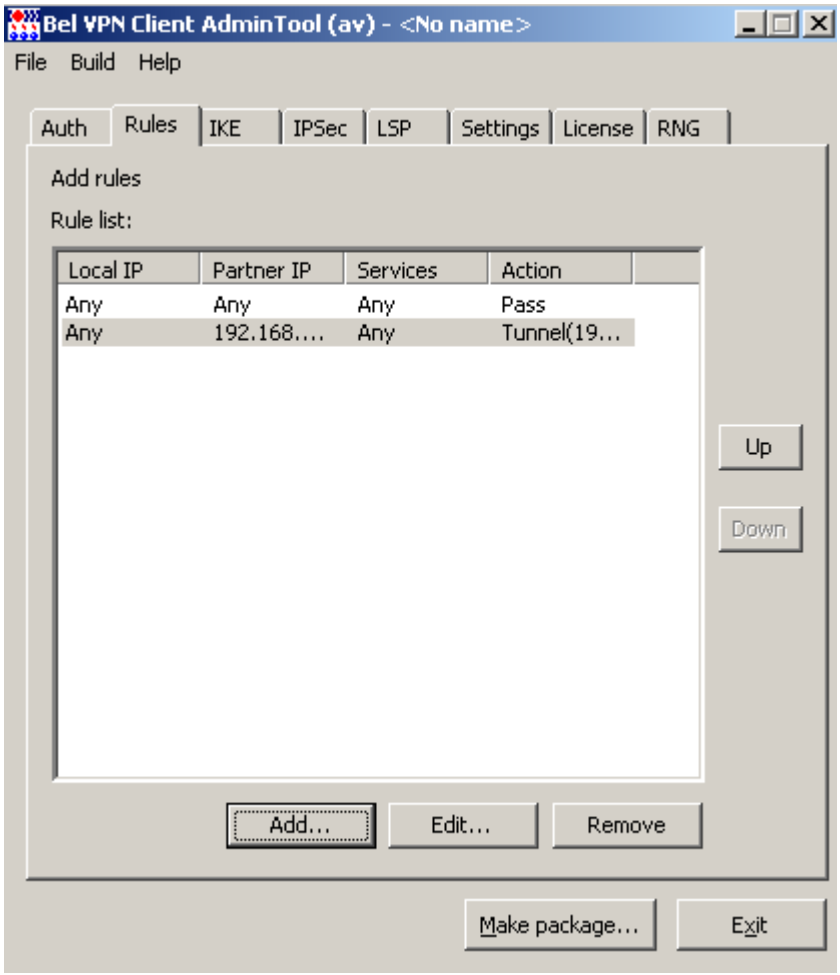

Рис. 6

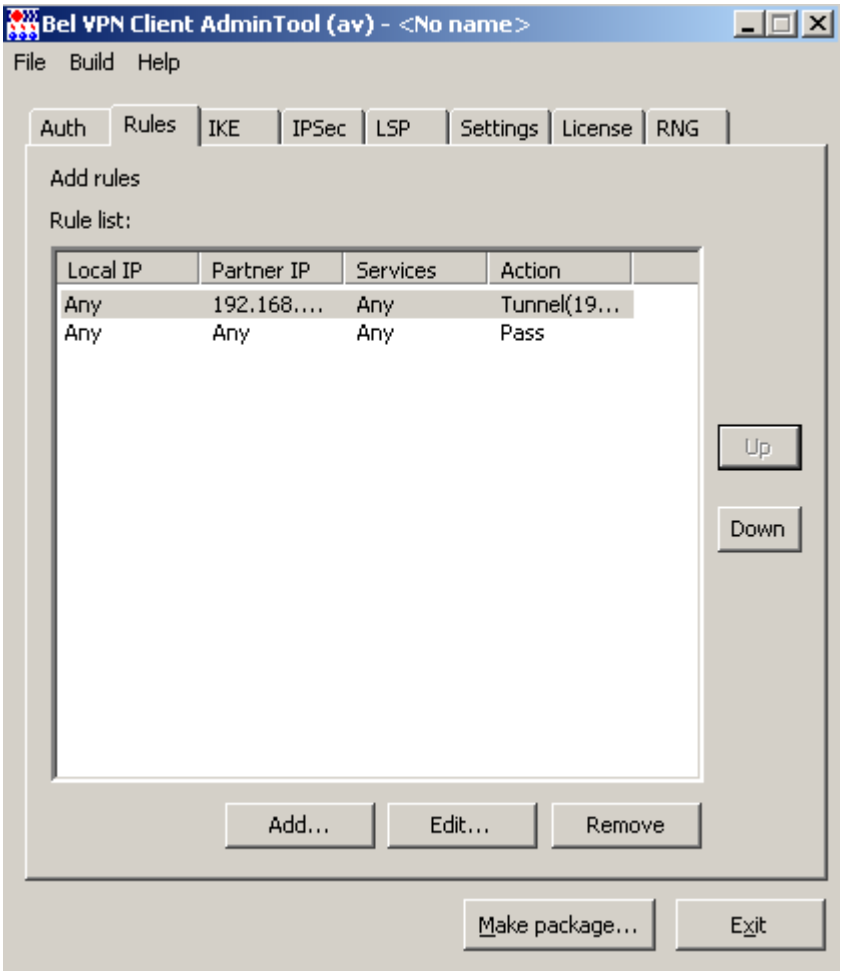
Bel VPN Client AdminTool (av) - <No name>
File Build Help
Auth Rules IKE IPSec LSP Settings License RNG
Add rules
Rule list:
Local IP Partner IP Services Action
Any 192.168.... Any Tunnel(19...
Any Any Any Pass
Up
Down
Add...
Edit...
Remove
Make package...
Exit

Рис. 7

7. Переходим во вкладку IKE. Здесь мы ничего трогать не будем. В этой вкладке представлен список предустановленных IKE Proposals, базирующихся на алгоритмах семейства ГОСТ. Мы можем перемещать строки относительно друг друга с помощью кнопок Up и Down, понижая или повышая приоритеты IKE Proposal. Значения 0 означают, что объем передаваемых данных не ограничен и количество IPsec SA – не ограничено.

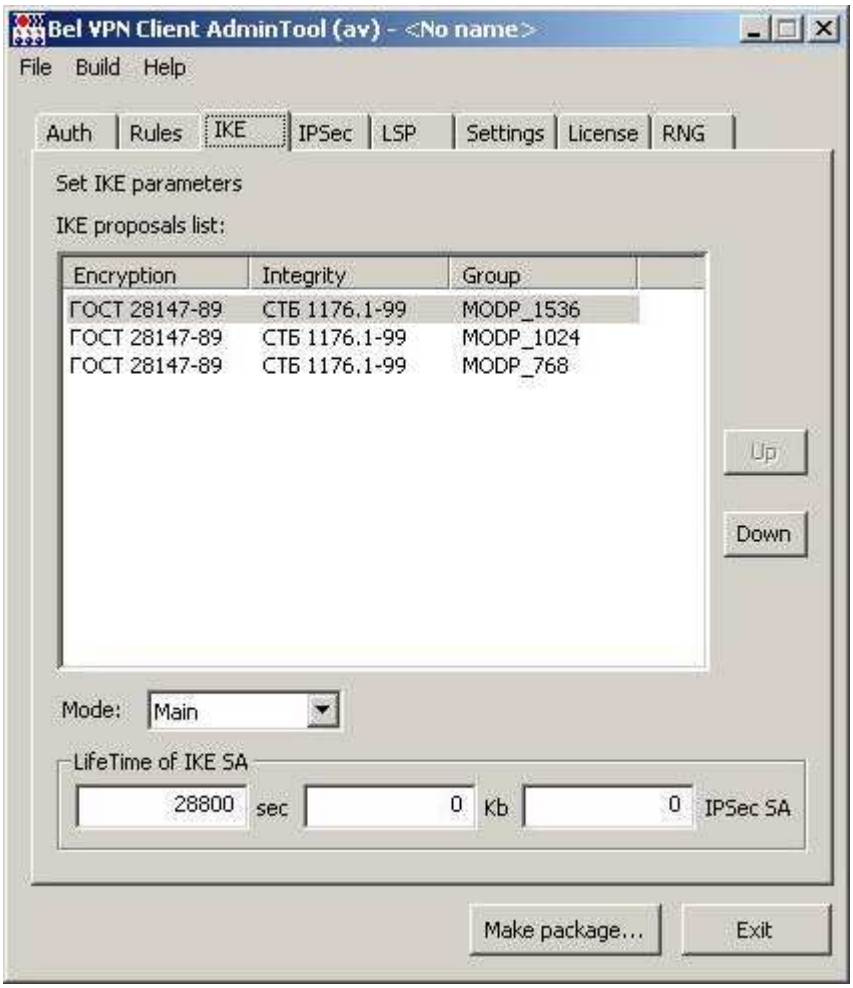

Рис. 8

8. Следующая вкладка – IPSec. Эта вкладка содержит список предустановленных IPSec Proposals. По умолчанию список содержит только варианты IPSec ESP Proposals. Нам требуется создать защищенное соединение с использованием IPSec ESP Encryption и IPSec ESP Integrity.(Рис. 9).
9. Список мы можем редактировать только путем перемещения строк относительно друг друга, изменяя этим приоритеты, аналогично IKE Proposals. Переместим нужный нам Proposal в начало списка, используя кнопку Up. Больше ничего в этом разделе не делаем.

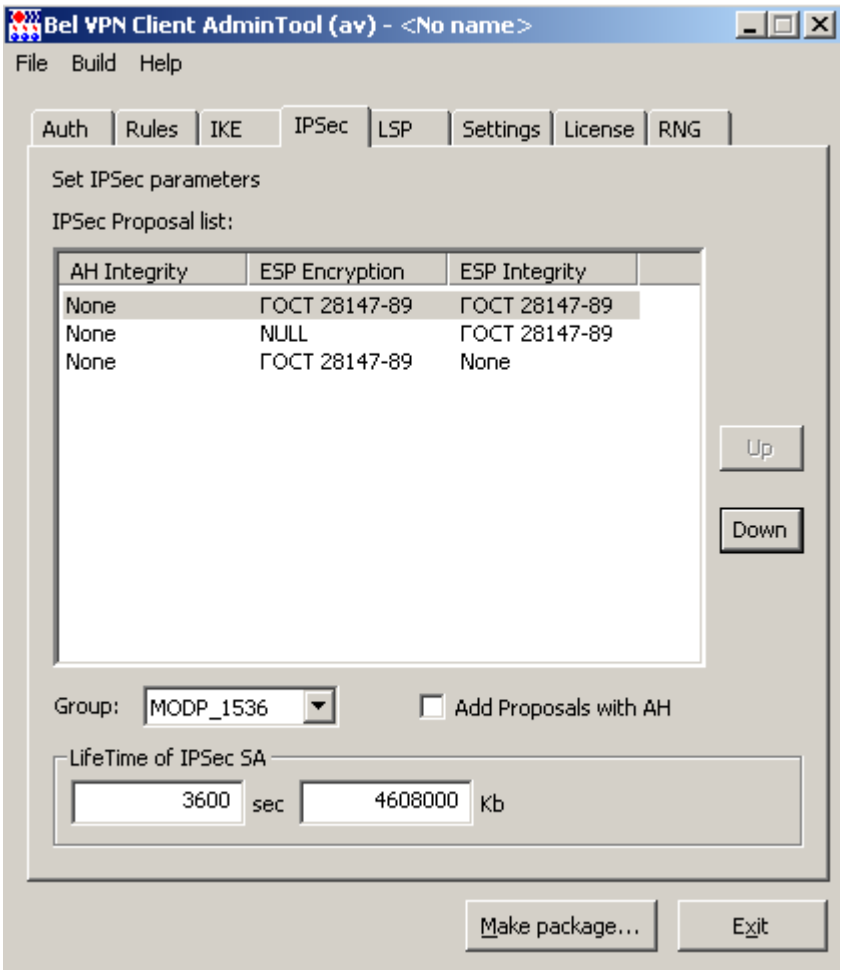

Рис. 9

10. Следующий раздел – LSP. В этом разделе мы можем просмотреть LSP, которая получилась после наших настроек в предыдущих вкладках, а также внести в нее коррективы, при необходимости. Но сначала нажимаем кнопку Advanced, в разделе IKE settings находим параметр Initiate IKE CFG Request (Рис. 10) – устанавливаем его значение в False (агент не будет посылать запрос на получение адреса у партнера), нажимаем OK и Accept:

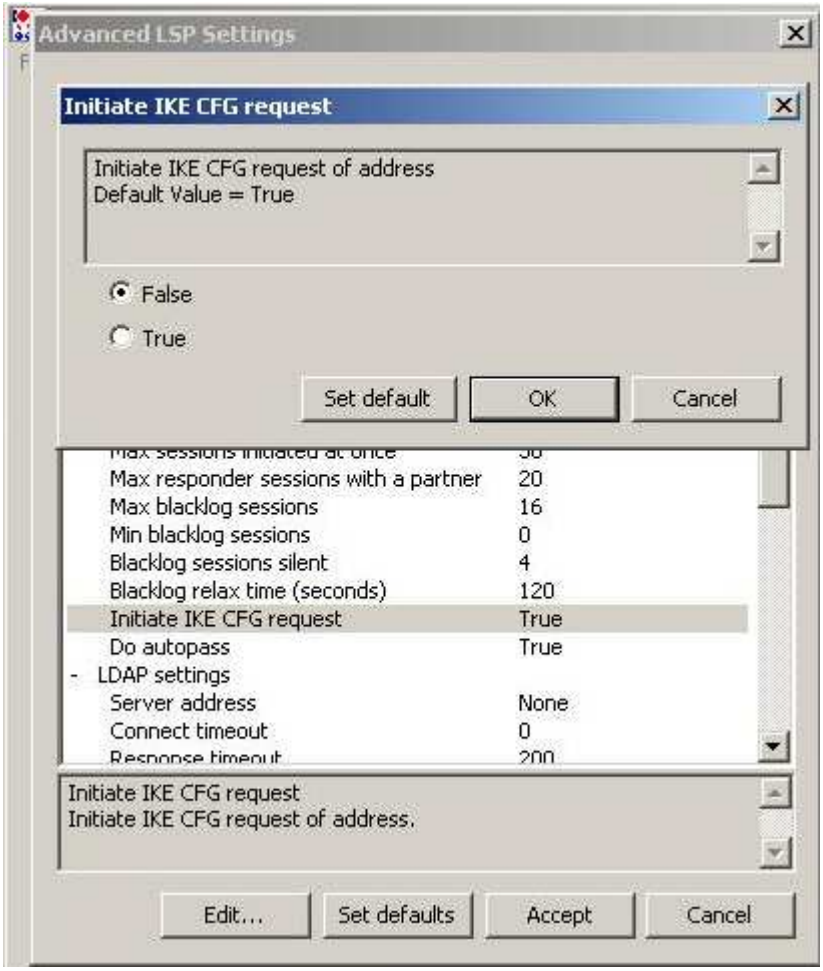

Рис. 10

11. Во вкладке LSP нажимаем кнопку Refresh LSP и видим созданную конфигурацию:

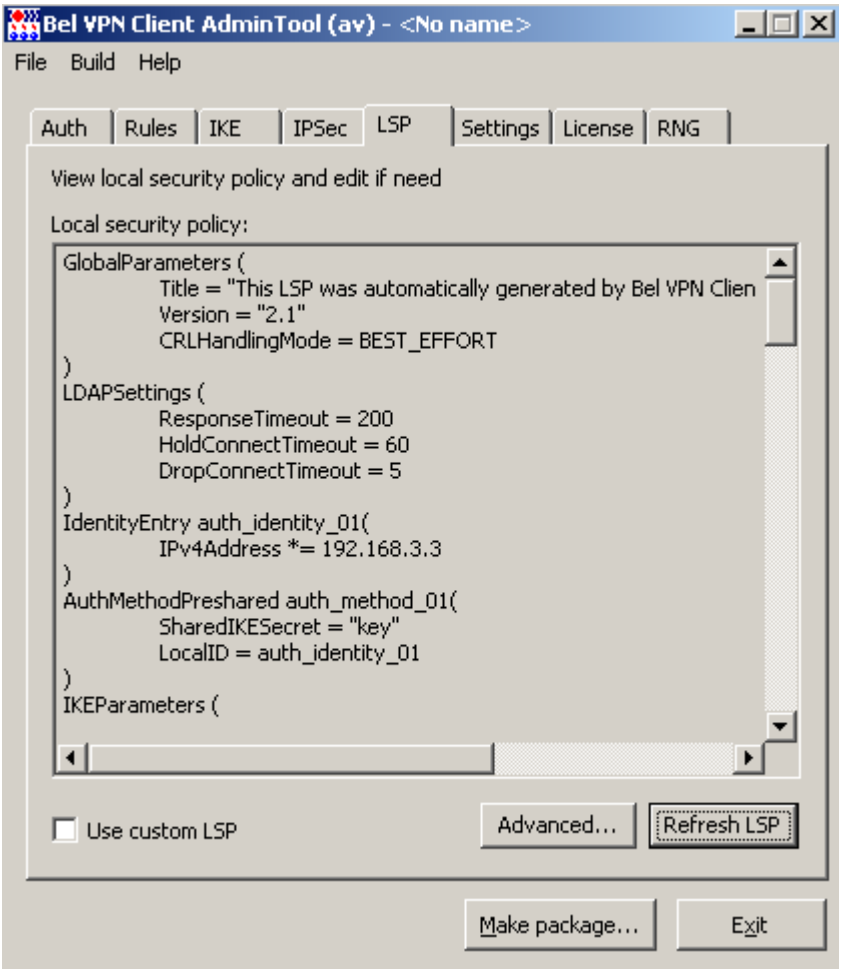

Рис. 11

Ниже приведен текст LSP, которая получилась после наших настроек и которая будет включена в состав установочного пакета Bel VPN Client.

```
GlobalParameters (
   Title = "This LSP was automatically generated by Bel VPN Client AdminTool
(av) at 2014.04.22 11:52:55"
   Version = "2.1"
   CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
   ResponseTimeout = 200
   HoldConnectTimeout = 60
   DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
   IPv4Address *= 192.168.3.3
)
AuthMethodPreshared auth_method_01(
   SharedIKESecret = "key"
   LocalID = auth_identity_01
```

```
)
IKEParameters (
   DefaultPort = 500
   SendRetries = 5
   RetryTimeBase = 1
   RetryTimeMax = 30
   SACreationTimeMax = 60
   InitiatorSessionsMax = 30
   ResponderSessionsMax = 20
   BlacklogSessionsMax = 16
   BlacklogSessionsMin = 0
   BlacklogSilentSessions = 4
   BlacklogRelaxTime = 120
)
IKETransform ike_trf_01(
   LifetimeSeconds = 28800
   CipherAlg  *= "G2814789CPRO1-K256-CBC-65530"
   HashAlg *= "STB1176199-65530"
   GroupID *= MODP_1536
)
IKETransform ike_trf_02(
   LifetimeSeconds = 28800
   CipherAlg  *= "G2814789CPRO1-K256-CBC-65530"
   HashAlg *= "STB1176199-65530"
   GroupID *= MODP_1024
)
IKETransform ike_trf_03(
   LifetimeSeconds = 28800
   CipherAlg  *= "G2814789CPRO1-K256-CBC-65530"
   HashAlg *= "STB1176199-65530"
   GroupID *= MODP_768
)
ESPTransform esp_trf_01(
   IntegrityAlg *= "G2814789AV1-K256-MAC-65531"
   CipherAlg *= "G2814789CPRO1-K256-CBC-250"
   LifetimeSeconds = 3600
   LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_01(
   Transform *=esp_trf_01
)
ESPTransform esp_trf_02(
   IntegrityAlg *= "G2814789AV1-K256-MAC-65531"
   CipherAlg *= "NULL"
   LifetimeSeconds = 3600
```

```
   LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_02(
   Transform *=esp_trf_02
)
ESPTransform esp_trf_03(
   CipherAlg *= "G2814789CPRO1-K256-CBC-250"
   LifetimeSeconds = 3600
   LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_03(
   Transform *=esp_trf_03
)
IKERule ike_rule(
   DoNotUseDPD = FALSE
   DPDIdleDuration = 60
   DPDResponseDuration = 5
   DPDRetries = 3
   MainModeAuthMethod *= auth_method_01
   Transform *= ike_trf_01,ike_trf_02,ike_trf_03
   IKECFGRequestAddress = FALSE
   DoAutopass = TRUE
)
IPsecAction ipsec_action_01(
   TunnelingParameters *=
          TunnelEntry(
                PeerIPAddress = 192.168.3.2
          )
   ContainedProposals *=
(esp_proposal_01),(esp_proposal_02),(esp_proposal_03)
   GroupID *= MODP_1536,MODP_1024,MODP_768
   IKERule = ike_rule
)
FilterEntry local_entry_00_00(
)
FilterEntry remote_entry_00_00(
   IPAddress *= 192.168.2.0/24
)
FilteringRule filter_rule_00_00(
   LocalIPFilter *= local_entry_00_00
   PeerIPFilter *= remote_entry_00_00
   Action *= (ipsec_action_01)
   RefuseTCPPeerInit = FALSE
)
FilterEntry local_entry_01_00(
```

```
)
FilterEntry remote_entry_01_00(
)
FilteringRule filter_rule_01_00(
   LocalIPFilter *= local_entry_01_00
   PeerIPFilter *= remote_entry_01_00
   Action *= (PASS)
)
```

12. Следующий раздел – Settings. В этой вкладке мы ничего не изменяем.

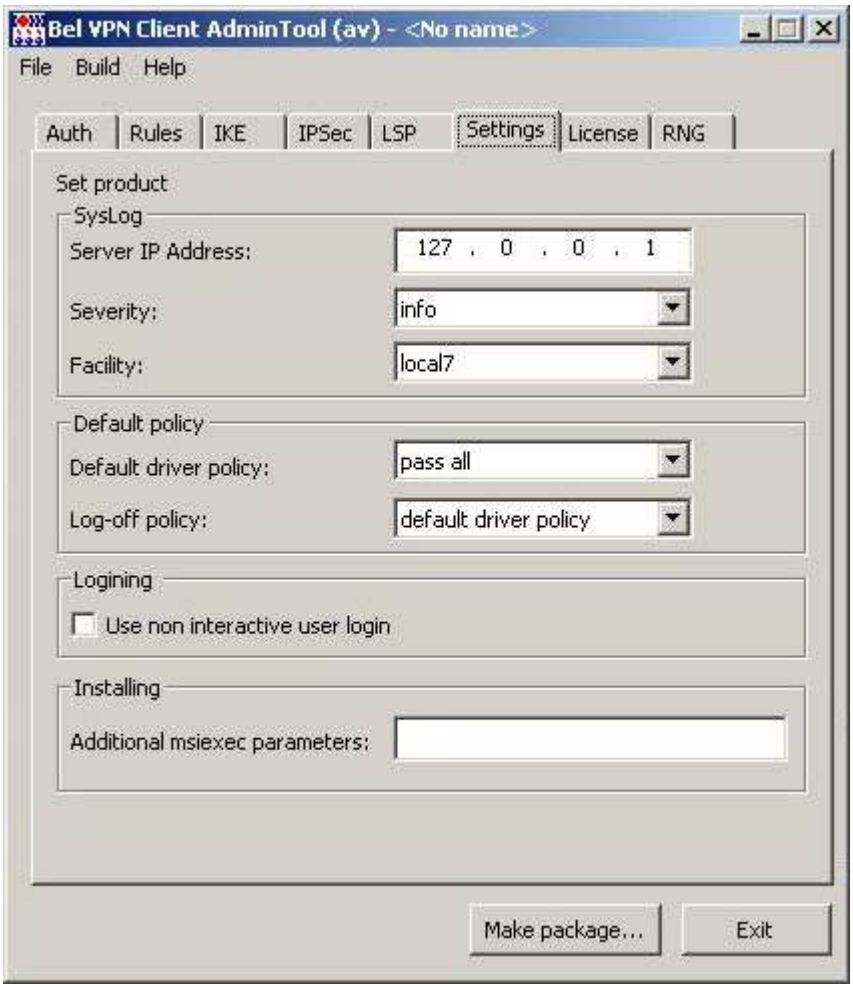

Рис. 12

`В поле Additional msiexec parameters` можно ввести дополнительные параметры запуска WinInstaller. Например, альтернативная инсталляционная директория, настройки лога Windows Installer и т.п. Эти параметры можно посмотреть по ссылке http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp

Если введем значение - /l*v! C:\log_client.txt, то при инсталляции Bel VPN Client будут выдаваться в файл C:\log_client.txt сообщения при логировании.

13. Следующий раздел – License. В этом разделе мы должны ввести информацию о лицензии на использование Bel VPN Client, для которого готовится инсталляционный пакет. Эти данные следует взять из сопровождающего продукт пакета.

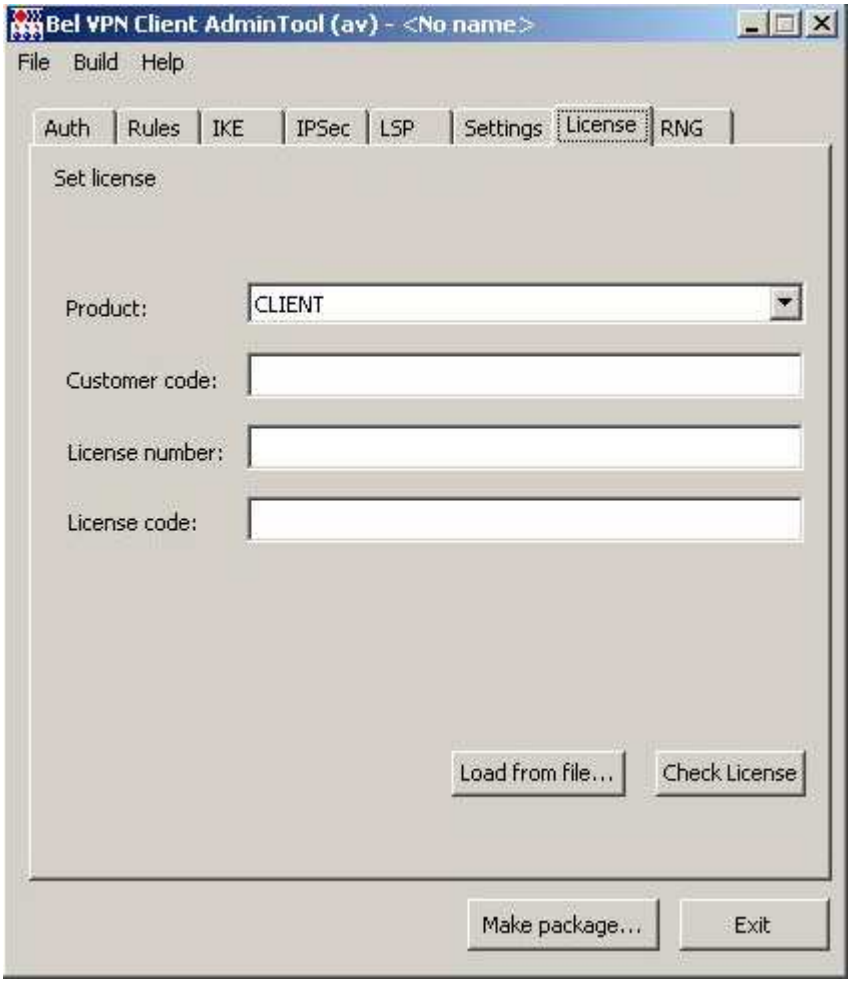

Рис. 13

14. Следующий раздел – RNG. В этом разделе мы должны настроить источник случайности для инсталляции Bel VPN Gate. Выставим флажок в значение Use biological initialization on user computer – при инсталляции пакета пользователю будет предложено нажимать на клавиши для сбора случайных данных.

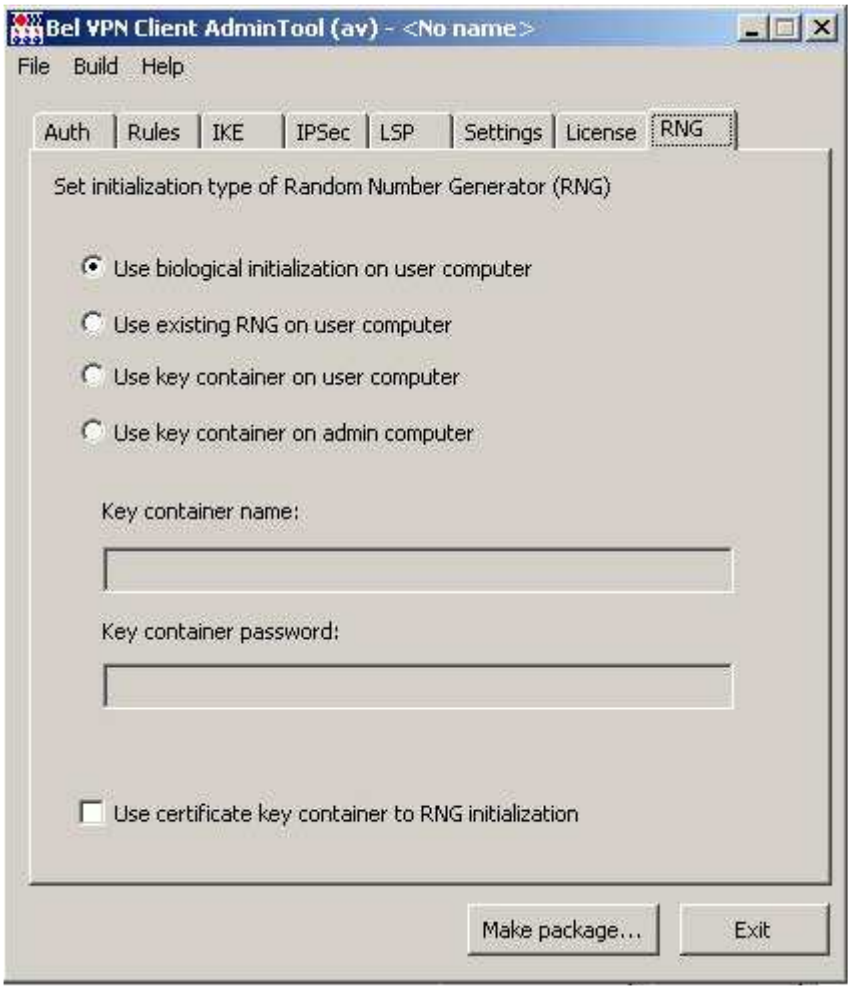

Рис. 143

15. На этом все настройки можно считать законченными. Нажимаем кнопку Make Package. Будет открыто окно, в котором нам следует выбрать тип инсталляционного пакета и путь к генерируемому файлу. Возможны следующие варианты:

    - Basic – инсталлятор содержит минимальное количество окон. В этом случае пользователь будет отвечать только на вопрос согласен ли он установить продукт Bel VPN Client и на вопрос готов ли он произвести перезагрузку операционной системы, который будет задан после завершения процедуры инсталляции.
    - Normal – инсталлятор содержит полный набор окон.
    - Silent – скрытый режим установки. На протяжении инсталляции никаких окон показываться не будет, а по завершении инсталляции автоматически будет инициирован рестарт операционной системы.

    Установим режим basic. В качестве пути к файлу установим путь: C:\Packages\Client1.exe.

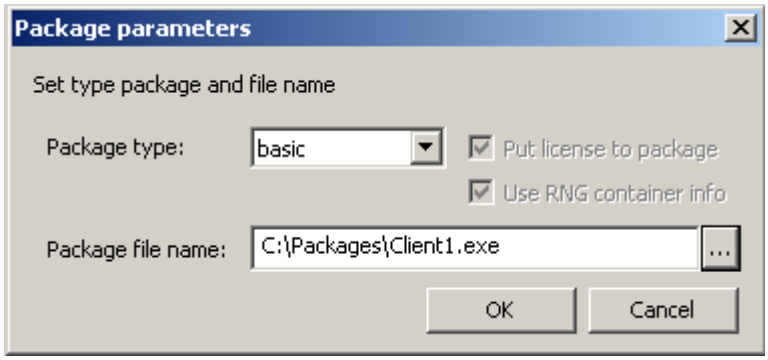

Рис. 15

16. Нажимаем кнопку OK. Начнется процесс генерации инсталляционного пакета.

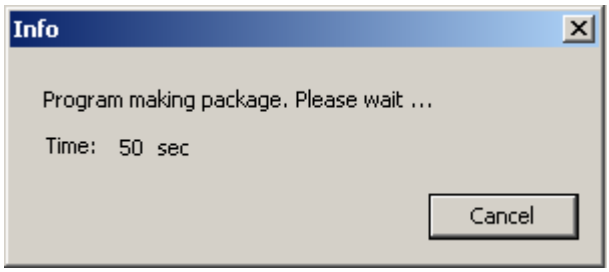

Рис. 16

После того, как процесс завершится, будет открыто окно подтверждающее успешное создание инсталляционного файла.

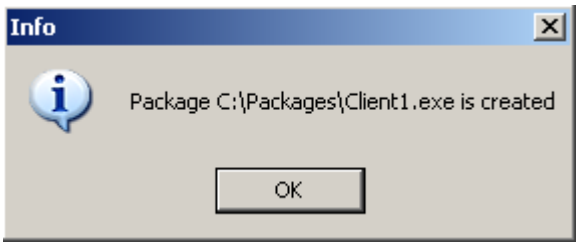

Рис. 17

Инсталляция и старт Bel VPN Client

В предыдущем разделе мы рассмотрели процедуру создания инсталляционного пакета Bel VPN Client. Теперь перейдем к инсталляции Bel VPN Client и проверке его работоспособности.

Запуск процедуры инсталляции производится активизацией файла client1.exe, который мы создали на предыдущем этапе.

Первым откроется окно:

Рис. 18

Нажимаем кнопку Yes. Далее следуют стандартные окна визарда и в завершение предлагается перезагрузить операционную систему. После перезагрузки и ввода пароля операционной системы открывается окно логина Bel VPN Client.

Рис. 19

По умолчанию пароль не установлен. Поэтому просто нажимаем OK. После этого окно закрывается и продолжается загрузка операционной системы. После загрузки операционной системы в панели задач (в правой области, где располагается иконка часов) появится иконка Bel VPN Client. При наведении курсора на иконку будет всплывать подсказка, содержащая информацию о количестве защищенных соединений и объеме обработанного трафика. При нажатии правой кнопкой мыши на иконке появляется меню, при выборе предложения Show SA Information появится окно VPN SA Monitor с полной информацией об ISAKMP и IPsec SAs.

Проверим работу Bel VPN Client. Для этого выполним команду

```
ping 192.168.2.1
```

Client имеет одно правило, по которому только при обращении к подсети 192.168.2.0/24, строится туннель. Иконка в панели задач должна изменить свой цвет, а при наведении на нее курсора должна показываться информация о создании одного защищенного соединения. В окне VPN SA Monitor появится информация о созданных соединениях ISAKMP и IPsec.