

УТВЕРЖДЕНО  
ВУ.РТНК.41005-01 34 01-ЛУ

**Программный комплекс**  
**«Bel VPN КР 4.1»**  
**Руководство администратора**  
**ВУ.РТНК.41005-01 34 01**

Листов 184

## Содержание

1.	Программный комплекс «Bel VPN KP 4.1»	4
1.1.	Назначение	4
1.2.	Возможности продукта	5
1.3.	Характеристика продукта	6
2.	Сценарии управления	8
2.1.	Сценарий первого обновления	8
2.2.	Сценарий последующих обновлений	8
3.	Установка Сервера управления	9
3.1.	Инсталляция Сервера управления	9
4.	Настройка Сервера управления	25
4.1.	Настройка механизма идентификации и аутентификации в Сервер управления	25
4.2.	Настройка Сервера управления	28
4.2.1.	Ввод лицензии	29
4.2.2.	Создание СА сертификата	30
4.2.3.	Создание рабочего сертификата	31
4.2.4.	Задание адресов Сервера управления	32
5.	Настройка и управление центральным шлюзом	34
5.1.	Создание учетной записи клиента для центрального шлюза	34
5.2.	Подготовка скриптов для Клиента управления и Bel VPN Gate 4.1	44
5.3.	Доставка и запуск скриптов	46
6.	Настройка и управление устройством с Bel VPN Client 4.1	50
6.1.	Создание учетной записи клиента на Сервере управления	50
6.2.	Создание инсталляционных файлов Клиента управления и Bel VPN Client 4.1	58
6.3.	Инсталляция Клиента управления и Bel VPN Client 4.1	59
7.	Сценарий перехода на аутентификацию с использованием сертификатов	62
7.1.	Создание обновления с параметрами ключевой пары и запроса на сертификат	63
7.2.	Создание на клиенте ключевой пары и запроса на сертификат	66
7.3.	Получение сертификата по запросу	67
7.4.	Создание обновления с новым сертификатом для шлюза	67
7.5.	Создание обновления с новым сертификатом для устройства с клиентом	75
8.	Сценарий неудачного обновления клиента	83
9.	Информация о клиенте на Сервере управления	88
10.	Сценарий выполнения расширенного обновления	94
11.	Сценарий создания клонов клиента Bel VPN Gate 4.1	99
11.1.	Создание базового проекта	99
11.2.	Подготовка материалов для клонов	104
11.3.	Настройка управляемого устройства	106

12. Сценарий включения в систему управления работающего устройства с Bel VPN Gate/Client .....	108
13. Групповые операции на Сервере управления.....	113
13.1. Создание шаблона проекта .....	113
13.2. Использование шаблона проекта .....	117
14. Управление с использованием командной строки – утилита upmgr .....	119
15. Изменение готового проекта с настройками VPN агента – утилита vpnmaker .....	124
16. Настройки Сервера управления.....	127
17. Настройки Клиента управления .....	132
18. Описание интерфейса Сервера управления.....	140
18.1. Вкладка Clients .....	140
18.2. Меню File .....	142
18.3. Меню Groups.....	142
18.4. Меню Clients.....	143
18.5. Меню Tools.....	147
18.5.1. Задание политики и настроек с использованием вкладок.....	147
Сохранение и загрузка настроек продукта .....	157
18.5.2. Задание политики и настроек с использованием мастера .....	158
18.5.3. Конвертирование политики .....	166
18.5.4. Создание носителя с образом диска .....	167
18.5.5. Редактирование настроек базы данных .....	168
18.6. Меню Help .....	168
19. Протоколирование событий.....	170
19.1. Сервер управления .....	170
19.2. Клиент управления.....	170
19.3. Продукт Bel VPN Gate/Client.....	170
20. UPWEB - система учета, анализа и отображения статистических показателей VPN-агентов .....	171
20.1. Создание пользователя для работы со статистикой .....	171
20.2. Запуск системы UPWeb .....	171
20.3. Переменные статистики .....	172
20.4. Основные возможности .....	173
20.5. Фильтрация клиентов по имени и времени .....	173
20.6. Фильтрация по значениям переменных статистики (критерии).....	177
20.7. Построение графиков .....	180
20.8. Снимки.....	183

# 1. Программный комплекс «Bel VPN КР 4.1»

## 1.1. Назначение

Программный комплекс «Bel VPN КР 4.1» (далее ПК Bel VPN КР) является самостоятельным Продуктом, но поставляется и работает только совместно с программными и программно-аппаратными продуктами линейки Bel VPN Gate и Bel VPN Client, а именно:

- программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1»;
- программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»;
- программный продукт «Клиент безопасности Bel VPN Client 4.1»;
- программно-аппаратное устройство «Клиент безопасности Bel VPN Client 4.1».

ПК Bel VPN КР предназначен для централизованного удаленного управления программными и программно-аппаратными продуктами линейки Bel VPN Gate и Bel VPN Client, а именно:

- программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1»;
- программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»;
- программный продукт «Клиент безопасности Bel VPN Client 4.1»;
- программно-аппаратное устройство «Клиент безопасности Bel VPN Client 4.1».

ПК Bel VPN КР состоит из трех компонент (рисунок 1):

- **Программный продукт «Сервер управления Bel VPN Update Server 4.1» (далее – Сервер управления)** – серверная часть продукта, устанавливается на выделенный компьютер и предназначена для управления процессом обновления продуктов Bel VPN Gate/Client и их настроек, установленных на управляемых устройствах;
- **Программный продукт «Клиент управления Bel VPN Update Client 4.1 для ОС семейства Microsoft Windows» (далее – Клиент управления Windows)** – клиентская часть продукта, устанавливается на управляемое устройство с установленным продуктом линейки Bel Client и предназначена для его управления;
- **Программный продукт «Клиент управления Bel VPN Update Client 4.1 для ОС семейства Linux» (далее – Клиент управления Linux)** – клиентская часть продукта, устанавливается на управляемое устройство с установленным продуктом Bel VPN Gate и предназначена для его управления.

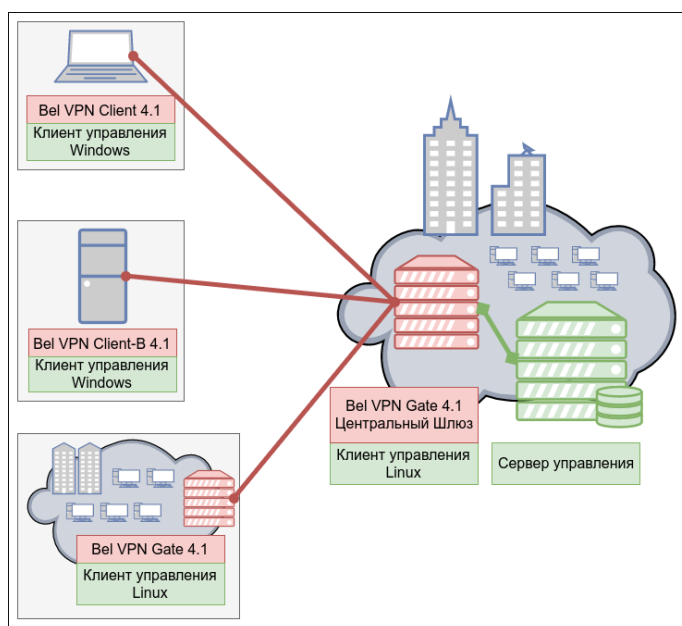


Рисунок 1

Сервер управления устанавливается на физическую или виртуальную аппаратную платформу в архитектуре Intel (x86/x86-64 совместимых) и функционирует под управлением одной из перечисленных операционных систем:

- Windows Server 2003 SP2 Edition (32-bit)
- Windows Server 2008 SP1 Edition (32-bit, 64-bit)
- Windows Server 2008R2 SP1 Edition (64-bit)
- Windows Server 2012 Edition (64-bit).

Сервер управления размещается в защищенной локальной подсети.

Для каждого управляемого устройства создается Клиент управления, который устанавливается на управляемое устройство.

Все обмены между Сервером управления и Клиентом управления осуществляются по протоколу FTP и UDP (передаются нотификации), трафик передается по защищенному IPsec-соединению, организуемому управляемыми Продуктами.

Инициатором сетевого взаимодействия между Клиентом управления и Сервером управления всегда выступает Клиент управления. В случае временной потери соединения на Клиенте управления предусмотрена возможность “докачки” данных с Сервера управления.

## 1.2. Возможности продукта

На управляемом устройстве с установленным продуктом Bel VPN Gate/Client 4.1 и **Клиентом управления** могут быть изменены следующие настройки:

- локальная политика безопасности, предписанная данному устройству (в текстовом виде или в виде cisco-like конфигурации)
- политика драйвера по умолчанию продукта Bel VPN Gate/Client 4.1
- настройки драйвера продукта Bel VPN Gate/Client 4.1
- предопределенные ключи продукта Bel VPN Gate/Client 4.1
- локальные сертификаты продукта Bel VPN Gate/Client 4.1, CA-сертификат, сертификаты партнеров, список отозванных сертификатов
- контейнеры с ключами сертификатов
- метод аутентификации партнеров
- настройки сетевых интерфейсов
- настройки сетевых маршрутов
- настройки регистрации событий продукта Bel VPN Gate/Client 4.1
- лицензия на продукт Bel VPN Gate/Client 4.1
- настройки Клиента управления.

На **Сервере управления** имеются возможности:

- создания обновлений для изменения настроек управляемых устройств
- выполнения групповых операций, например, одновременное создание обновлений для нескольких устройств
- использования шаблонов проекта при создании обновлений для устройств

На **Сервере управления** ведется мониторинг состояния и настроек всех управляемых устройств, предоставляемых **Клиентами управления**, а именно:

- дата и время последнего успешного соединения каждого устройства с Сервером управления
- IP-адреса устройств, с которых было осуществлено последнее успешное соединение
- версия Клиента управления

- версия Bel VPN Gate/Client 4.1
- локальная политика безопасности продукта Bel VPN Gate/Client 4.1 (в текстовом виде или в виде cisco-like конфигурации)
- настройки драйвера продукта Bel VPN Gate/Client 4.1
- локальные сертификаты продукта Bel VPN Gate/Client 4.1, списки отозванных сертификатов, СА сертификаты, сертификаты партнеров
- имена контейнеров с ключами сертификатов (если нет возможности сбора информации обо всех контейнерах, допускается сбор информации только о контейнерах, созданных с использованием Клиента управления)
- ближайшее время и дата истечения срока действия одного из сертификатов, размещенных в базе продукта Bel VPN Gate/Client 4.1 на каждом устройстве
- запросы на локальные сертификаты
- имена предопределенных ключей продукта Bel VPN Gate/Client 4.1
- настройки сетевых интерфейсов
- настройки сетевых маршрутов
- настройки регистрации событий продукта Bel VPN Gate/Client 4.1
- журнал регистрации событий продукта Bel VPN Gate/Client 4.1 и Клиента управления
- информация о лицензиях продуктов Bel VPN Gate/Client 4.1
- статистические данные о работе системы управляемого устройства.

На **Сервере управления** в данной версии реализованы новые возможности:

- использование окон мастера для создания несложной политики безопасности продукта Bel VPN Gate/Client 4.1 управляемого устройства
- включение в систему управления уже работающего устройства с Bel VPN Gate/Client 4.1
- создание клонов клиента для устройства с Bel VPN Gate 4.1, отличающихся локальными сертификатами, лицензиями и т. д.
- изменение настроек готового проекта для Bel VPN Gate/Client 4.1 – утилита vpnmaker.

### 1.3. Характеристика продукта

На Сервере управления каждый Клиент управления имеет уникальный идентификатор, а создаваемые обновления имеют порядковые номера. Уникальный идентификатор и порядковый номер входят в состав данных, загружаемых с Сервера управления. Полученные данные используются Клиентом управления только в том случае, если содержат верный идентификатор Клиента управления и если номер обновления больше последнего установленного обновления.

**Продукт обеспечивает защиту от злоумышленника, пытающегося с помощью механизма обновления запустить на компьютере с Клиентом управления “чужеродное” ПО. Защита осуществляется на основе ЭЦП, позволяющей осуществить аутентификацию и проверить целостность пересылаемых данных от Сервера управления к Клиенту управления. Предполагается, что злоумышленник не имеет доступа к управлению компьютером с Сервером управления и доступа к управлению устройствами с Клиентами управления.**

Действительно, перед тем как предоставить данные для скачивания Клиентам управления, Сервер управления формирует электронно-цифровую подпись для этих данных с использованием секретного ключа рабочего сертификата Сервера управления. А Клиент управления перед использованием полученных данных с Сервера управления проверяет электронно-цифровую подпись, используя открытый ключ рабочего сертификата Сервера управления.

Рабочий сертификат Сервера управления распространяется среди Клиентов управления в составе скачиваемых данных. Подлинность рабочего сертификата Сервера управления проверяется на основе построения цепочки сертификатов до СА сертификата Сервера управления. СА сертификат

Сервера управления устанавливается на каждый Клиент управления во время инсталляции Клиента управления на устройство.

Перевыпуск рабочего сертификата Сервера управления производится по мере необходимости на Сервере управления. Время жизни рабочего сертификата, среди прочего, зависит и от объема подписываемых данных, то есть от количества обслуживаемых Клиентов управления и частоты обновлений. Рекомендуемое время жизни рабочего сертификата - от 1 месяца до 1 года.

В комплект поставки продукта Bel VPN KP 4.1 входят каталоги и файлы:

```

setup.exe
setup.ini
updater_server.cab
updater_server.msi
upweb.war
version.txt
LINUXDEBIAN6
LINUXRHEL5
OTHERS
SOLARIS
WINDOWS

```



Note

Если на управляемом устройстве уже инсталлирован продукт Bel VPN Client 4.1 то рекомендуется его деинсталлировать, а затем создать заново его инсталляционный файл и файл Клиента управления, как описано в данном документе. При невозможности выполнить деинсталляцию (большое количество клиентов или др.причины) обращайтесь в службу поддержки по адресу [support@s-terra.by](mailto:support@s-terra.by).



Note

Шлюз безопасности Bel VPN Gate 4.1 поставляется с инсталлированным Клиентом управления, который следует инициализировать.

В дальнейшем описании документа приведены примеры для стенда (Рисунок 2), в который включен шлюз безопасности с установленным продуктом Bel VPN Gate 4.1, защищающий подсеть с конечным устройством, на котором установлен Сервер управления. Для удаленного управления устройством с Сервера управления в стенде присутствует компьютер с IP-адресом 40.0.0.101/16. Взаимодействие между управляемым устройством и Сервером управления осуществляется по IPsec-туннелю.

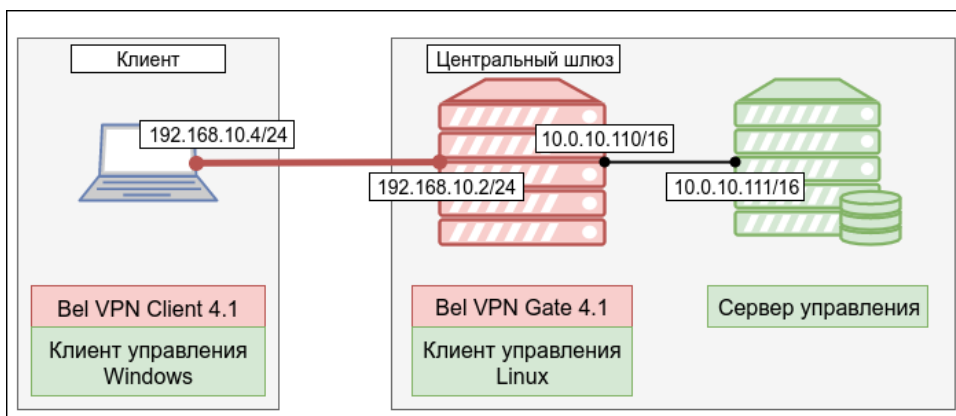


Рисунок 2

Далее по тексту управляемые устройства будем называть клиентами, на которые устанавливается (установлен) продукт Bel VPN Gate/Client 4.1 и Клиент управления.

Шлюз безопасности Bel VPN Gate 4.1, защищающий подсеть с Сервером управления, будем называть центральным шлюзом.

## 2. Сценарии управления

---

Можно выделить два последовательных сценария обновления продукта Bel VPN Gate/Client 4.1 на управляемом устройстве.

**Сценарий первого обновления** (при первом обращении к управляемому устройству):

- для Bel VPN Client 4.1 – подготовка инсталляционных файлов Клиента управления и Bel VPN Client 4.1, доставка и локальная установка на управляемом устройстве;
- для Bel VPN Gate 4.1 – подготовка скриптов для инсталляции (инициализации) Клиента управления и настройки установленного продукта Bel VPN Gate 4.1, доставка и локальный запуск на управляемом устройстве

**Сценарий последующих обновлений** (все последующие взаимодействия с управляемым устройством) – создание обновлений на Сервере управления и передача их по защищенному VPN соединению.

Опишем подробно приведенные выше два сценария.

### 2.1. Сценарий первого обновления

- Шаг 1:** Установите Сервер управления на выделенный компьютер с установленной ОС Windows Server 2003/2008 и настройте его, как описано в разделе [«Установка и настройка Сервера управления»](#).
- Шаг 2:** Настройте центральный шлюз - на Сервере управления подготовьте скрипты, доставьте их и запустите локально (см. раздел [«Настройка и управление центральным шлюзом»](#)).
- Шаг 3:** На Сервере управления подготовьте инсталляционные файлы продукта Bel VPN Client 4.1 и Клиента управления, доставьте и установите локально на управляемое устройство (см.раздел [«Настройка и управление устройством с Bel VPN Client 4.1»](#)) (а для Bel VPN Gate 4.1 – подготовьте скрипты).
- Шаг 4:** Установленный Клиент управления автоматически выполнит проверку возможности устанавливая соединение с Сервером управления и получать обновления.

### 2.2. Сценарий последующих обновлений

- Шаг 1:** На Сервере управления сформируйте обновление для управляемого устройства., В заданное время пакет обновления будет создан автоматически и сразу будет доступен для скачивания.
- Шаг 2:** Клиент управления, периодически проверяя наличие доступных для него обновлений, скачает его с Сервера управления. Можно задать подряд несколько обновлений с указанием времени создания каждого, и они будут применены в том порядке, в котором и были созданы.



## 3. Установка Сервера управления

### 3.1. Инсталляция Сервера управления

Инсталляция Сервера управления осуществляется на выделенном компьютере с установленной ОС:

- Windows Server 2003 SP2 Edition (32-bit)
  - Windows Server 2008 SP1 Edition (32-bit,64-bit)
  - Windows Server 2008R2 SP1 Edition (64-bit)
  - Windows Server 2012 Edition (64-bit).
1. Для инсталляции Сервера управления запустите файл `setup.exe` из состава дистрибутива. Появится окно с запросом на установку необходимых компонент, нажмите кнопку **Установить** (Рисунок 3).

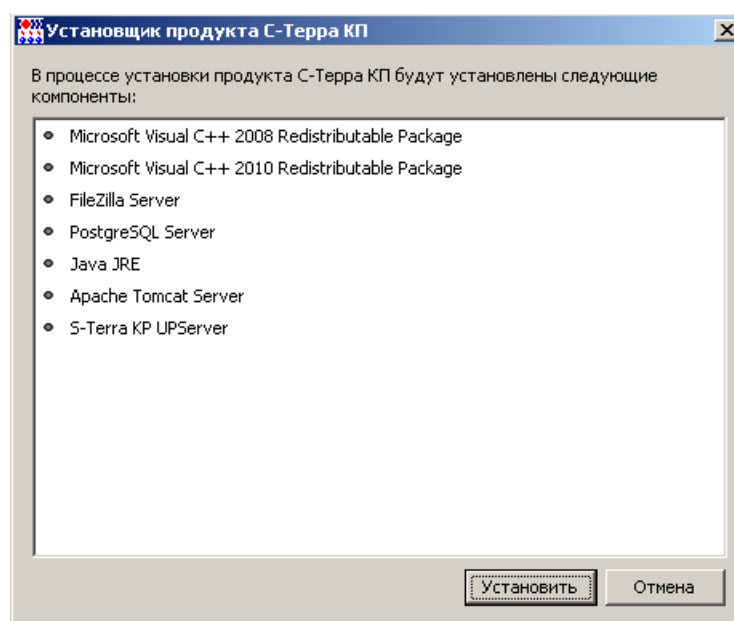


Рисунок 3

2. Выполняется сбор информации для Microsoft Visual C++ Redistributable Package и подготовка к инсталляции.

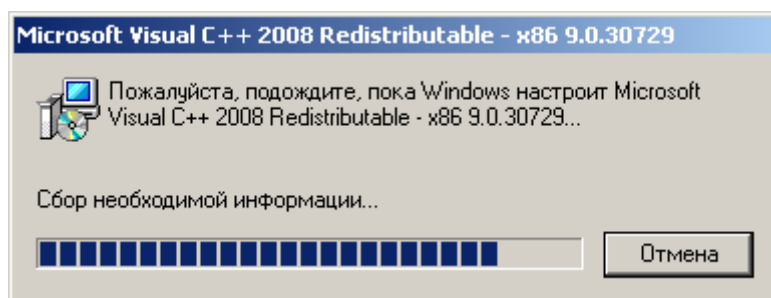


Рисунок 4

3. Установка Microsoft Visual C++ Redistributable Package выполняется без вмешательства администратора (Рисунок 5).

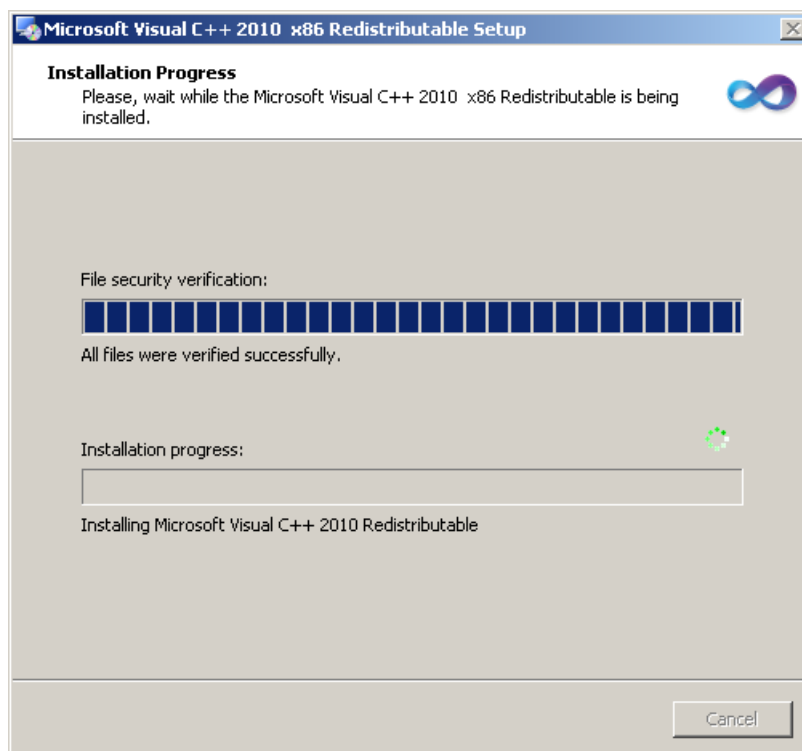


Рисунок 5

4. Далее устанавливается продукт FileZilla Server (Рисунок 6). Примите условия лицензионного соглашения – нажмите кнопку [I Agree](#).

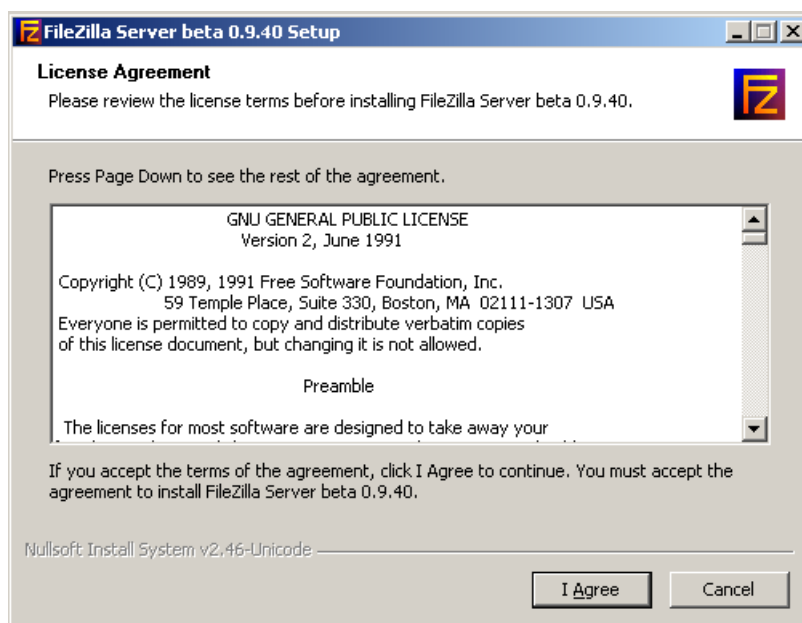


Рисунок 6

5. В следующем окне (Рисунок 7) предлагается выбрать компоненты для инсталляции. Оставьте настройки по умолчанию и нажмите кнопку [Next](#).

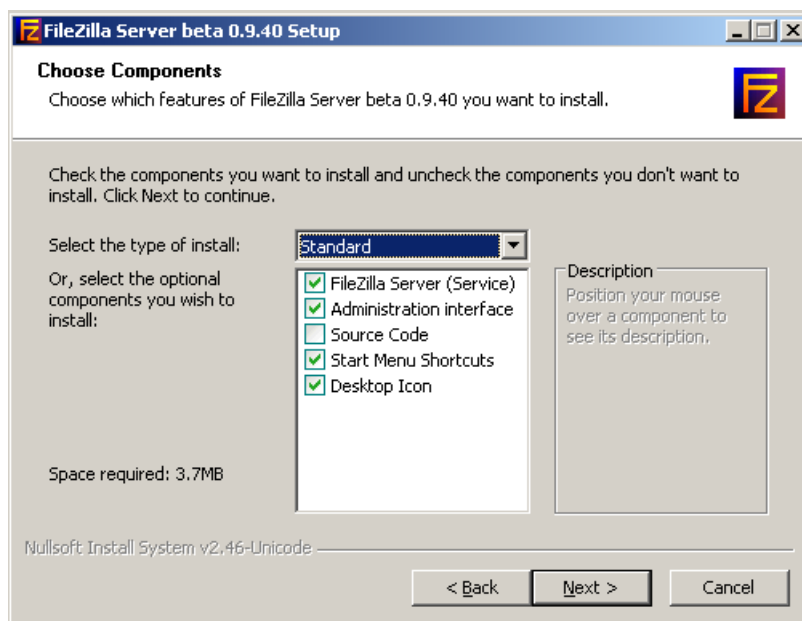


Рисунок 7

6. Укажите папку, в которую будет установлен продукт FileZilla Server (Рисунок 8).

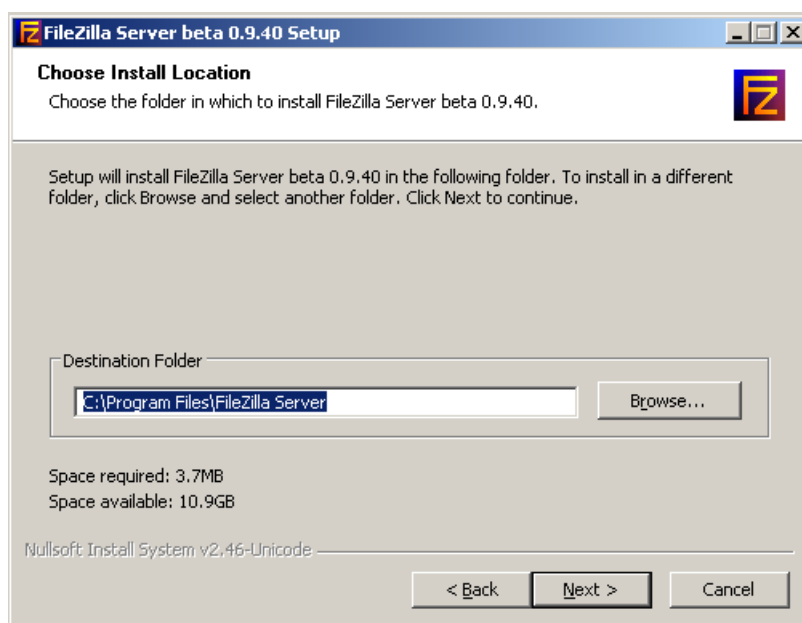


Рисунок 8

7. В окне выбора настроек для запуска сервиса продукта FileZilla Server оставьте значения по умолчанию и нажмите кнопку **Next** (Рисунок 9).

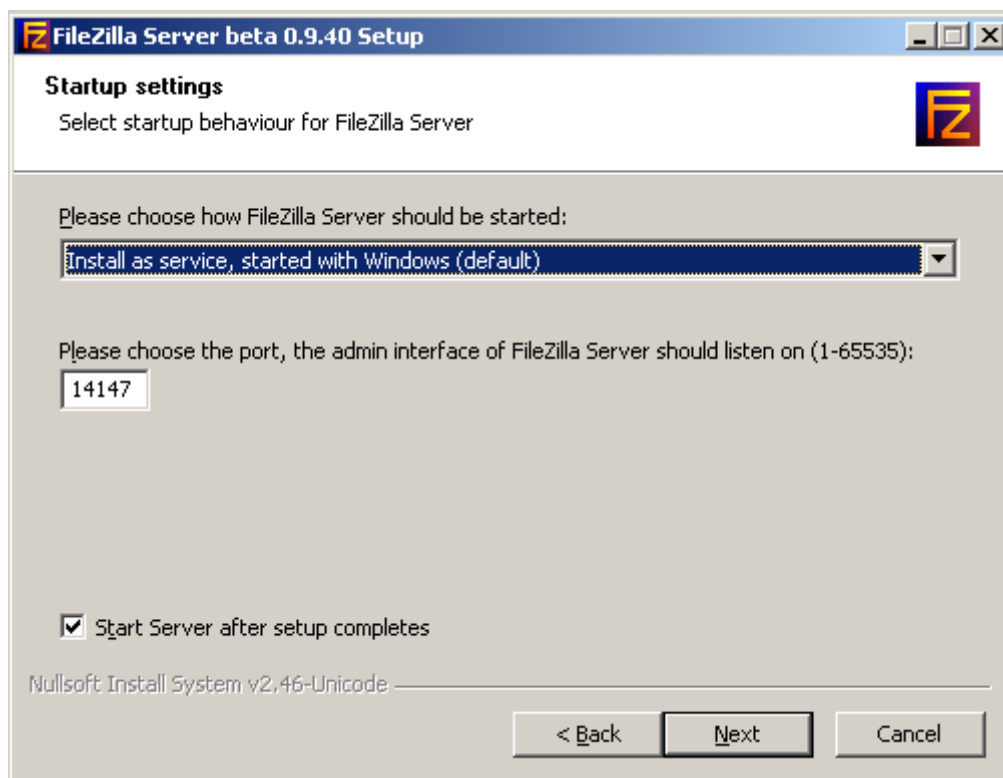


Рисунок 9

8. В окне с настройками старта консоли управления продуктом FileZilla Server оставьте значения по умолчанию и нажмите кнопку **Install** (Рисунок 10), после чего запустится процесс установки.

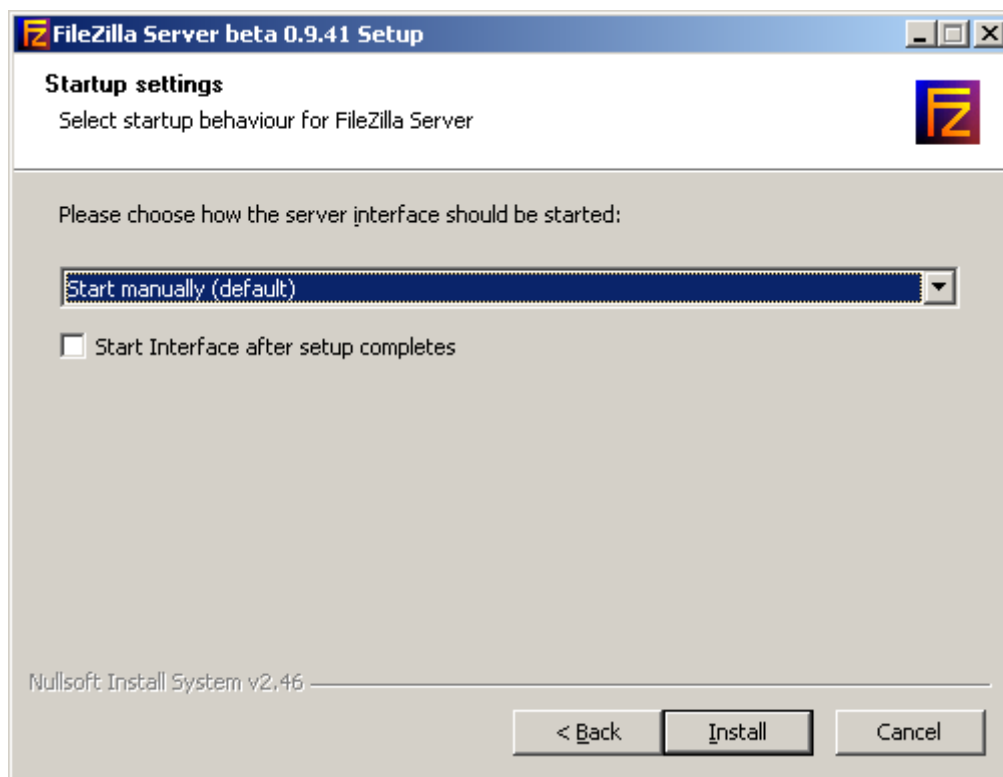


Рисунок 10

9. По завершению процесса установки FileZilla Server нажмите кнопку **Close** (Рисунок 11).

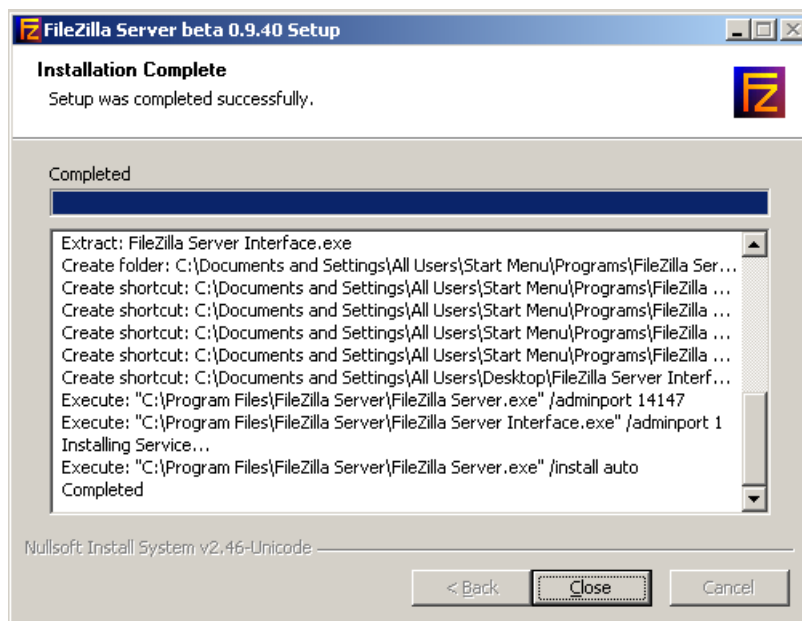


Рисунок 11

10. Далее устанавливается компонент PostgreSQL Server, нажмите кнопку **Next>** (Рисунок 12).

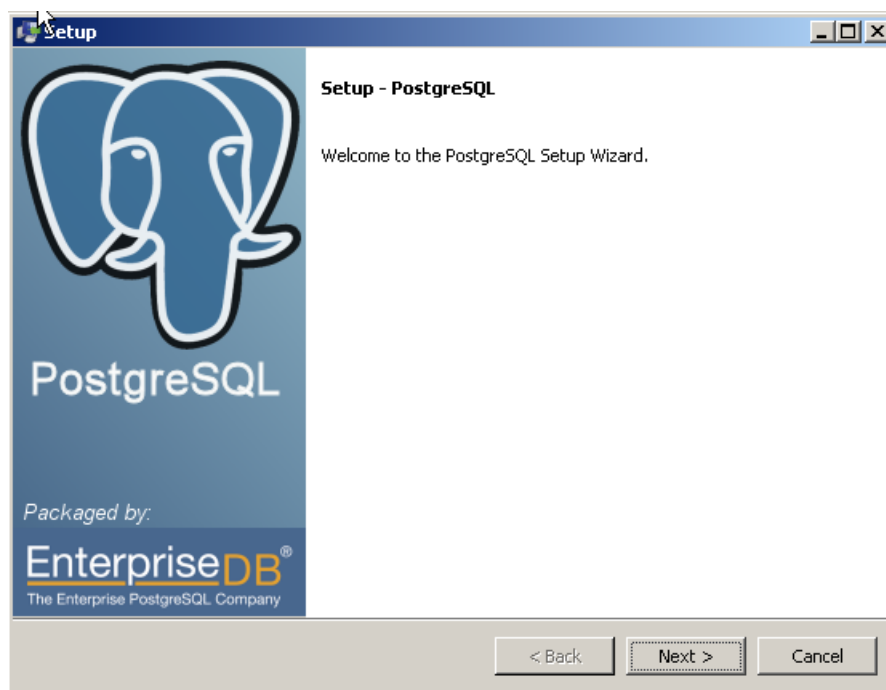


Рисунок 12

11. Задайте каталог установки продукта PostgreSQL Server, можно оставить по умолчанию или указать другой (Рисунок 13).

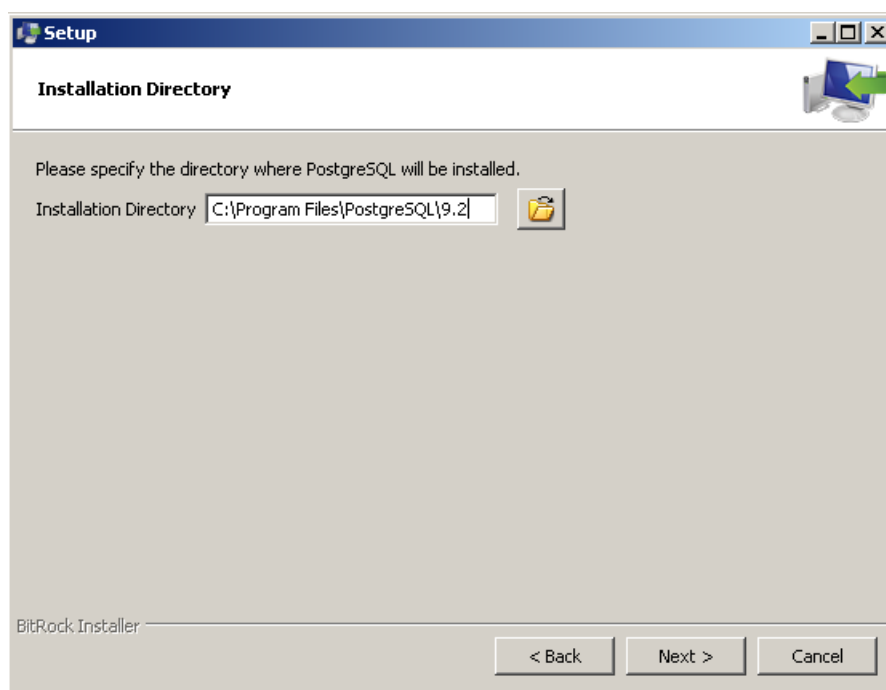


Рисунок 13

12. Задайте каталог инсталляции файлов базы данных (Рисунок 14).

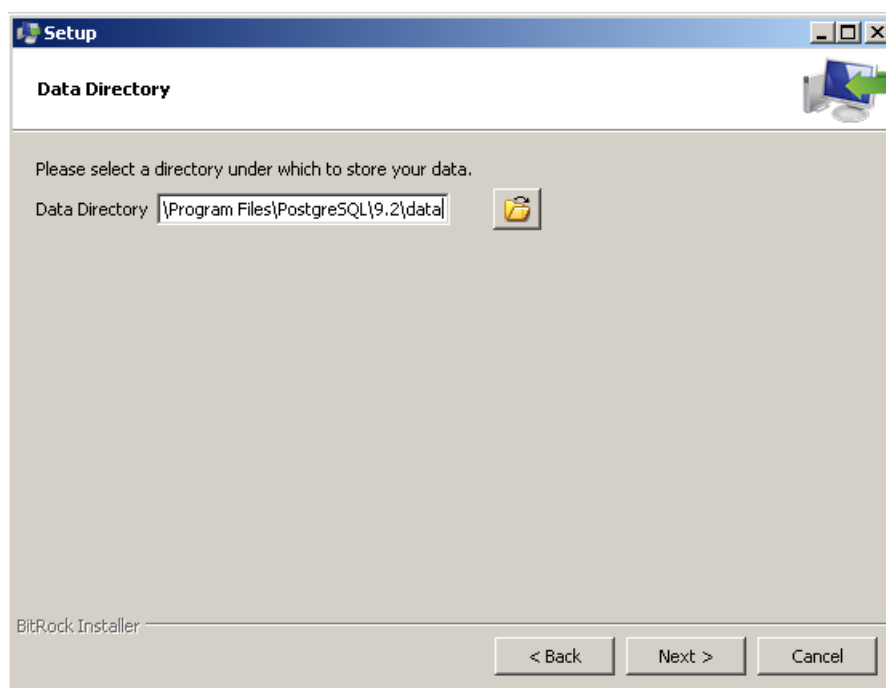


Рисунок 14

13. Далее появится окно с запросом пароля суперпользователя для работы с базой данных (Рисунок 15). По умолчанию задан пароль 1234567890. Этот пароль не должен изменяться администратором в процессе инсталляции, так как это не позволит модернизировать базу данных нужным образом в процессе инсталляции. Если есть потребность изменить этот пароль, администратор может это сделать после завершения инсталляции, изменив пароль в самой базе данных и в конфигурационном файле Сервера управления (чтобы Сервер управления мог взаимодействовать с базой данной).

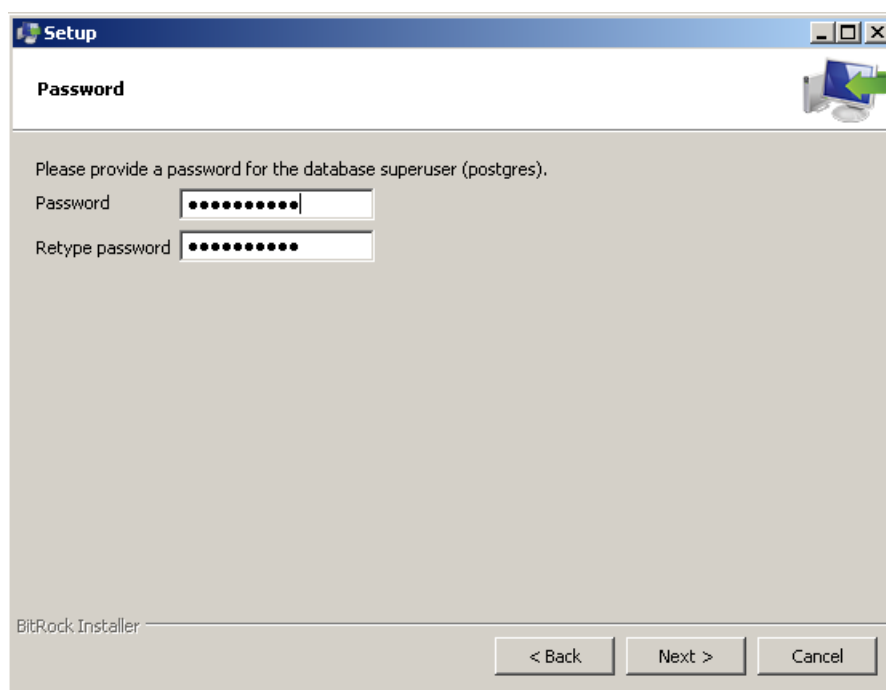


Рисунок 15

14. Далее появится окно с указанием порта - 5432, по которому будет происходить обращение к базе данных (Рисунок 16). Рекомендуется оставить это значение, в противном случае придется вносить новое значение в конфигурационный файл Сервера управления. Нажмите кнопку [Next](#).

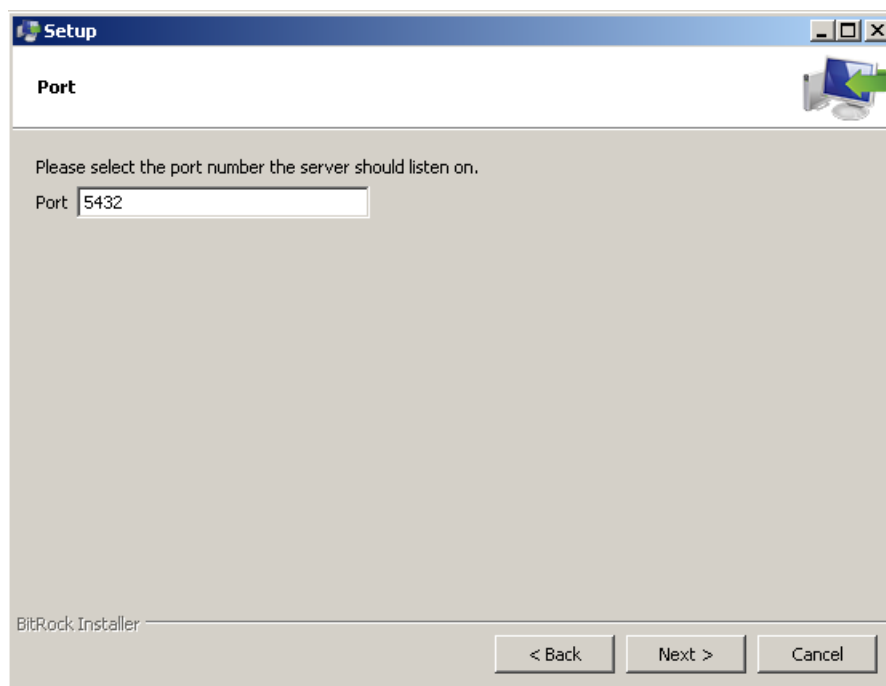


Рисунок 16

15. В окне задания языка хранения данных (Рисунок 17) оставьте значение по умолчанию.

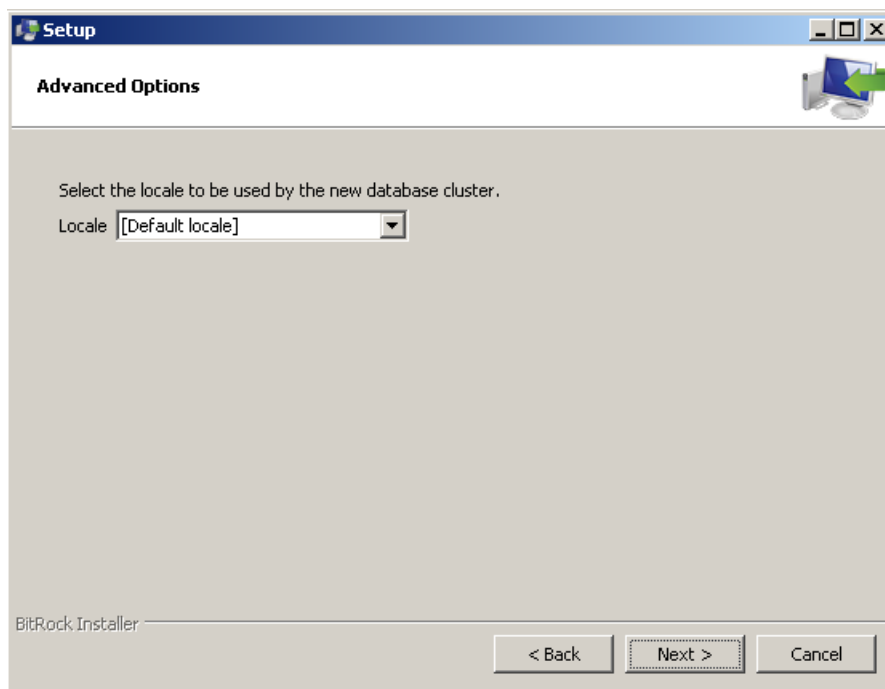


Рисунок 17

16. Далее начнется инсталляция PostgreSQL (Рисунок 18).

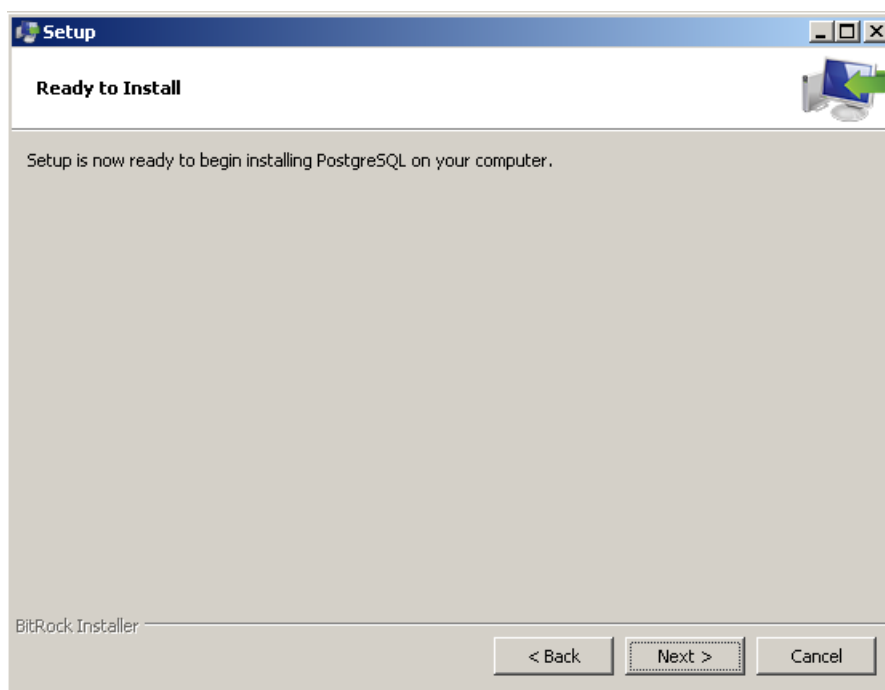


Рисунок 18



17. По окончании инсталляции PostgreSQL нажмите кнопку Finish (Рисунок 19).



Рисунок 19

18. Далее устанавливается Java JRE (Рисунок 20). Нажмите кнопку **Install**.



Рисунок 20

19. Инсталляция занимает некоторое время (Рисунок 21).



Рисунок 21

20. По окончании инсталляции Java JRE нажмите кнопку [Close](#) (Рисунок 22).



Рисунок 22

21. Устанавливается компонента Apache Tomcat Server, нажмите кнопку [Next](#) (Рисунок 23).



Рисунок 23

22. Согласитесь с лицензионным соглашением, нажав кнопку **I Agree** (Рисунок 24).

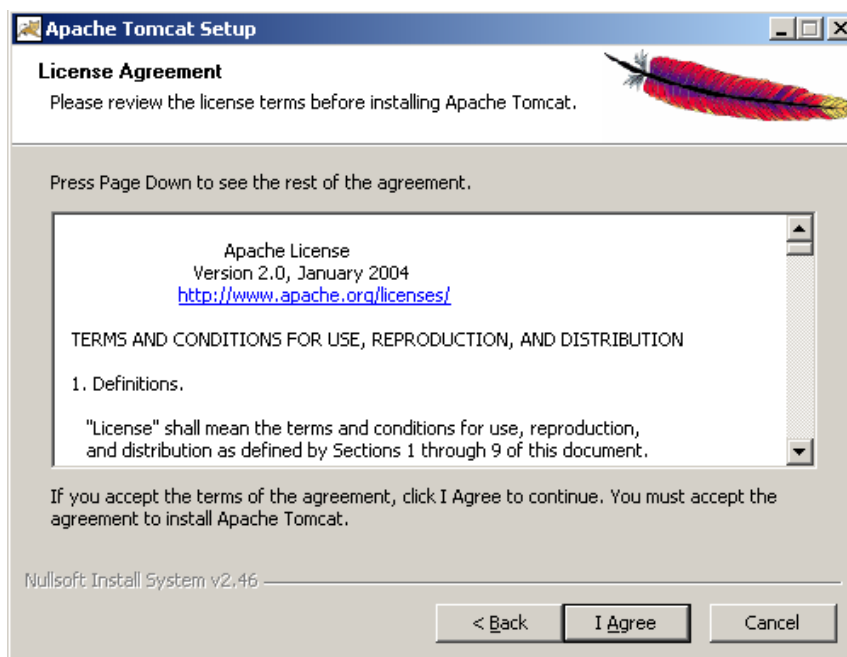


Рисунок 24

23. Выбранные компоненты для инсталляции по умолчанию можно оставить и нажать [Next](#) (Рисунок 25).

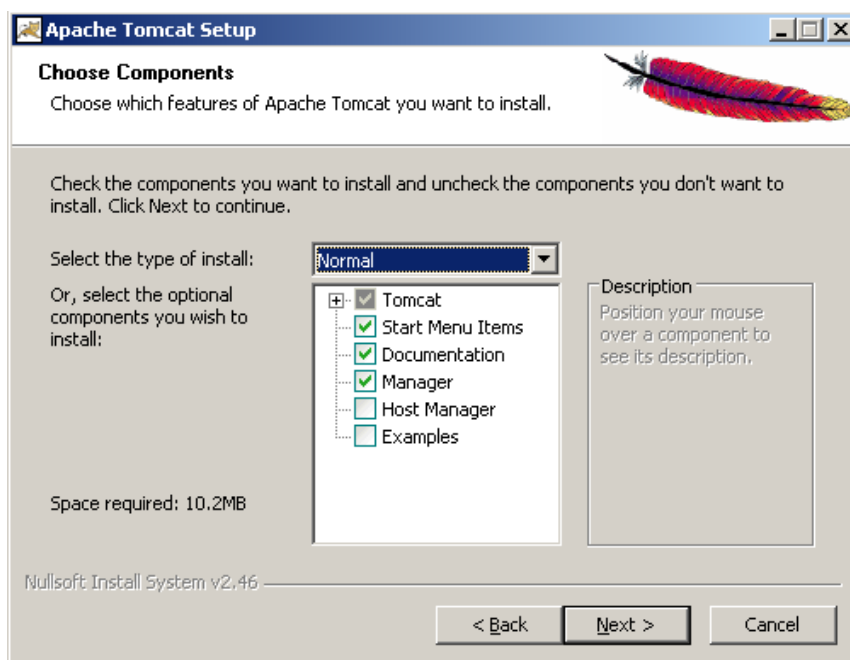


Рисунок 25

24. Основные параметры работы продукта оставьте по умолчанию (Рисунок 26).

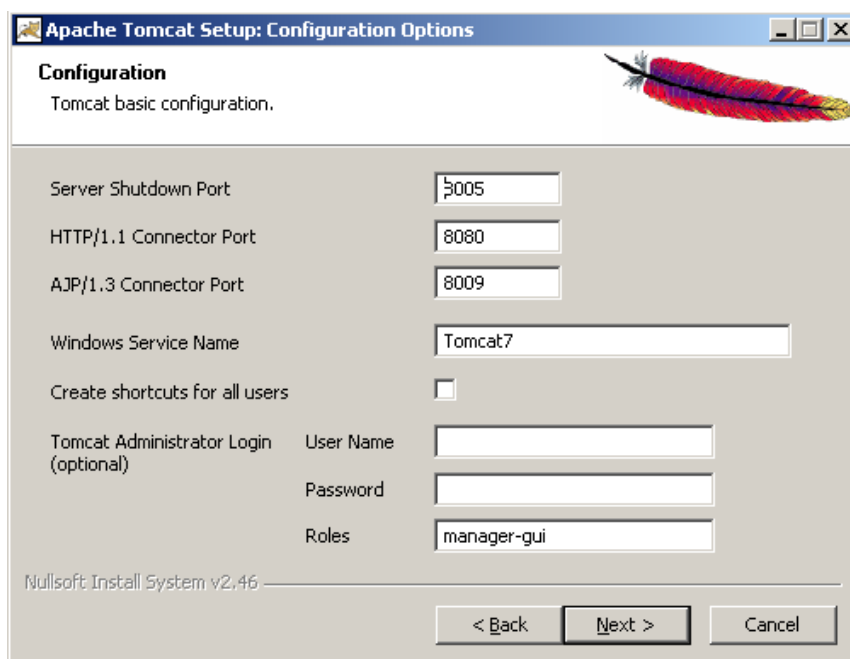


Рисунок 26

25. Укажите папку, в которую был инсталлирован Java SE, можно оставить путь по умолчанию и нажать кнопку Next (Рисунок 27).

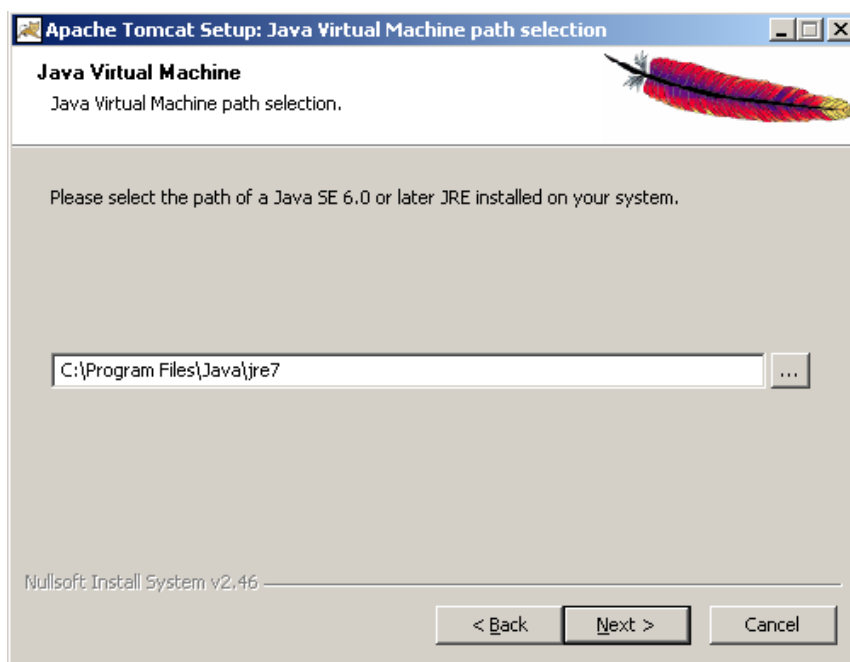


Рисунок 27

26. Для инсталляции бинарных кодов Apache Tomcat Server папку можно оставить по умолчанию и нажать **Install** (Рисунок 28).

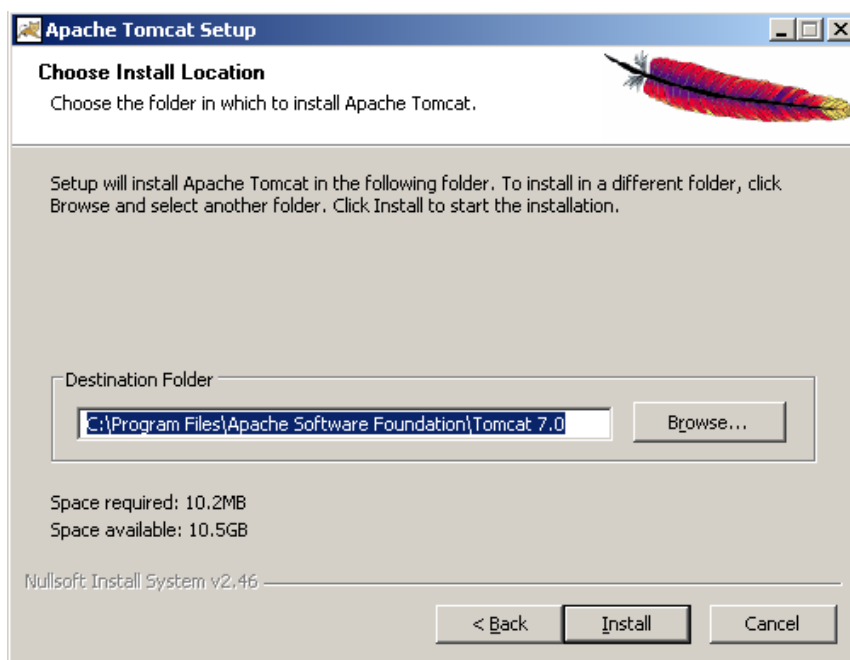


Рисунок 28

27. Начнется процесс инсталляции (Рисунок 29).

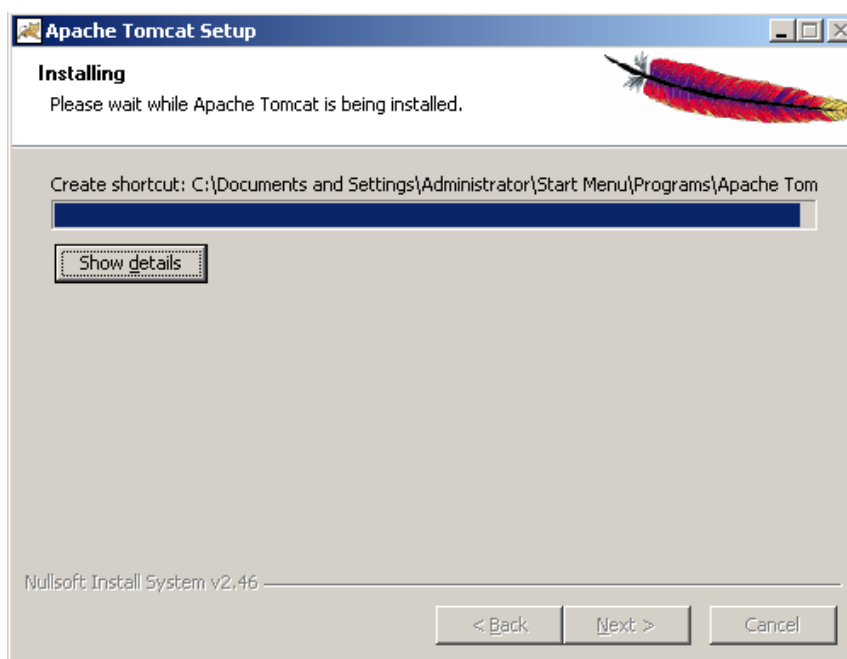


Рисунок 29

28. По окончании инсталляции нажмите кнопку **Finish**, предварительно отменив запуск сервиса Apache и показа информации о продукте, если нужно (Рисунок 30).

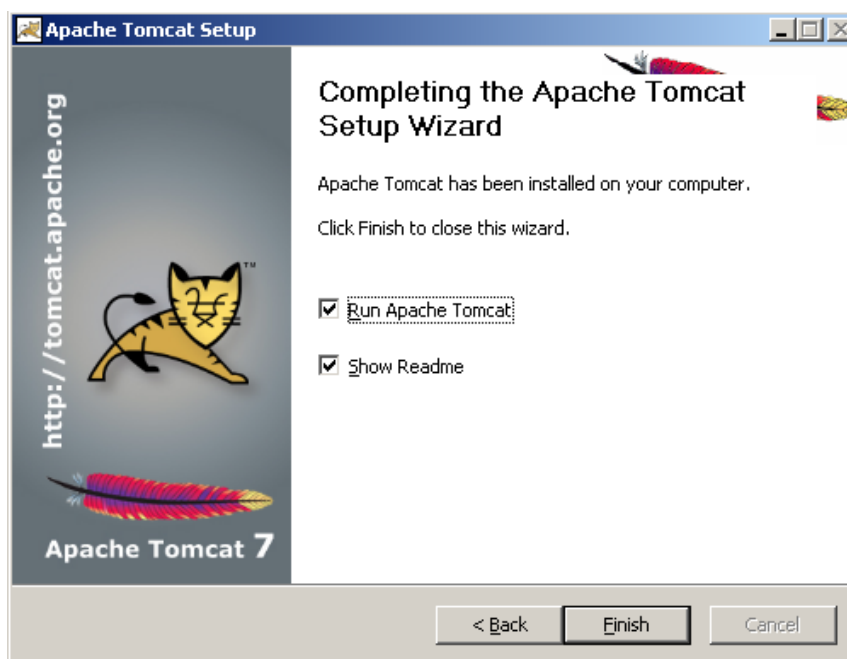


Рисунок 30

29. Если запуск сервиса Apache не был отменен, то происходит его запуск (Рисунок 31).

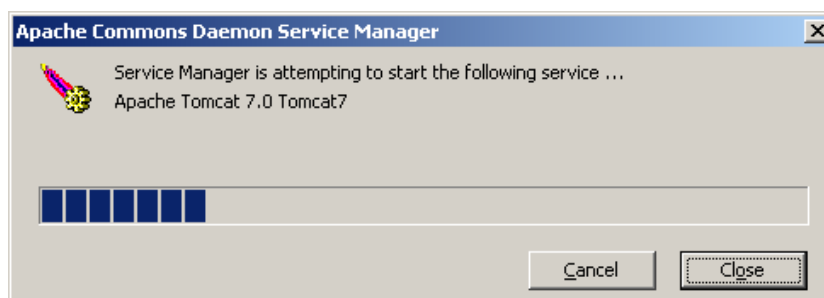


Рисунок 31

30. Появляется окно с адресом лицензионного соглашения и ограничениями к применению.

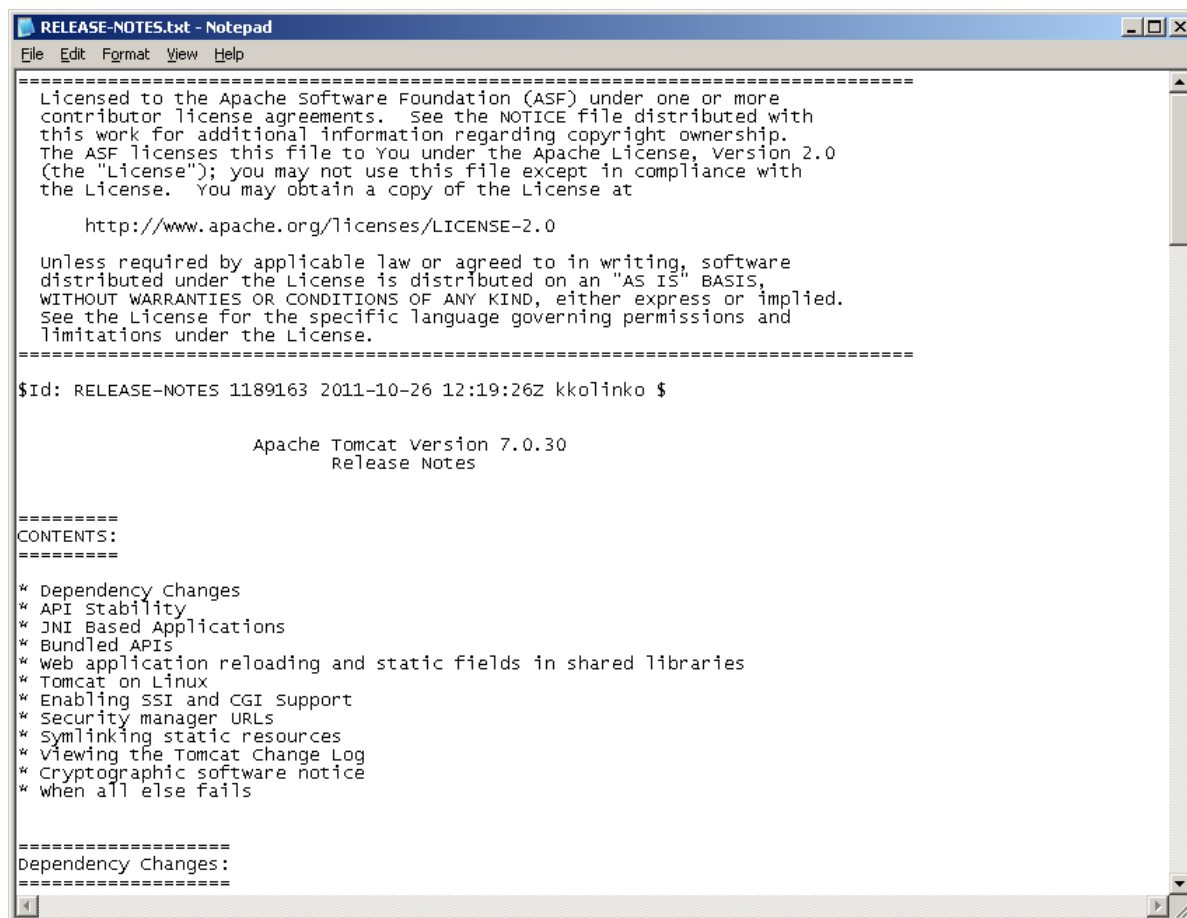


Рисунок 32

31. Начинается инсталляция Сервера управления (Рисунок 33). Нажмите кнопку **Next**.

Рисунок 33

32. Каталог, в который устанавливается Сервер управления, можно оставить по умолчанию и нажать **Next** (Рисунок 34).

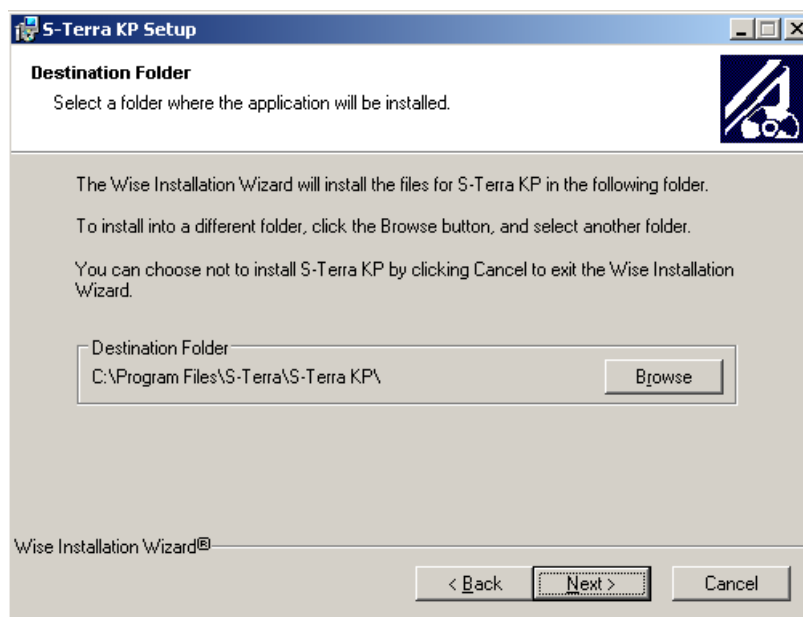


Рисунок 34

33. После установки Сервера управления и запуска сервиса, который может быть продолжительным порядка двух минут, так как проверяется целостность файлов программной части, выдается окно об окончании установки, нажмите в нем кнопку **Finish**.



Рисунок 35



## 4. Настройка Сервера управления

### 4.1. Настройка механизма идентификации и аутентификации в Сервер управления

Для настройки механизма идентификации и аутентификации для доступа к Серверу управления выполните следующее:

1. Запустите консоль Сервера управления – **Bel VPN UPServer Console** (Пуск→Программы→S-Terra Bel→Bel VPN KP→UPServer Console).
2. В консоли выберите меню **Tools** и предложение **User editor...** (Рисунок 36).

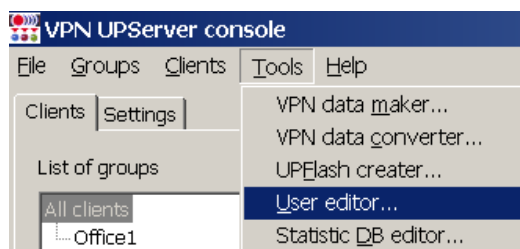


Рисунок 36

3. Появится окно **UPServer login** для ввода пароля пользователя с именем «superuser». Для этого пользователя предустановлен пустой пароль. Нажмите кнопку **OK** (Рисунок 37).

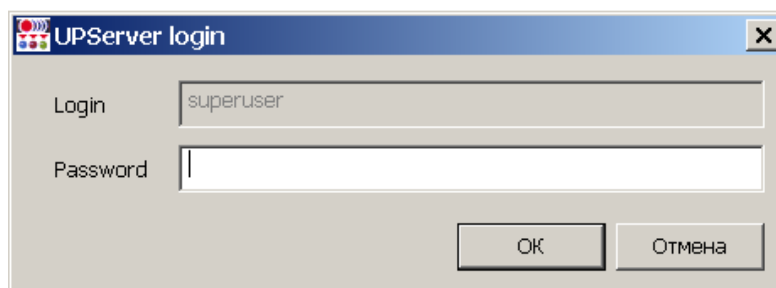


Рисунок 37

4. В окне **UPServer user list** назначьте непустой пароль пользователю «superuser», нажав кнопку **Edit...** (Рисунок 38).

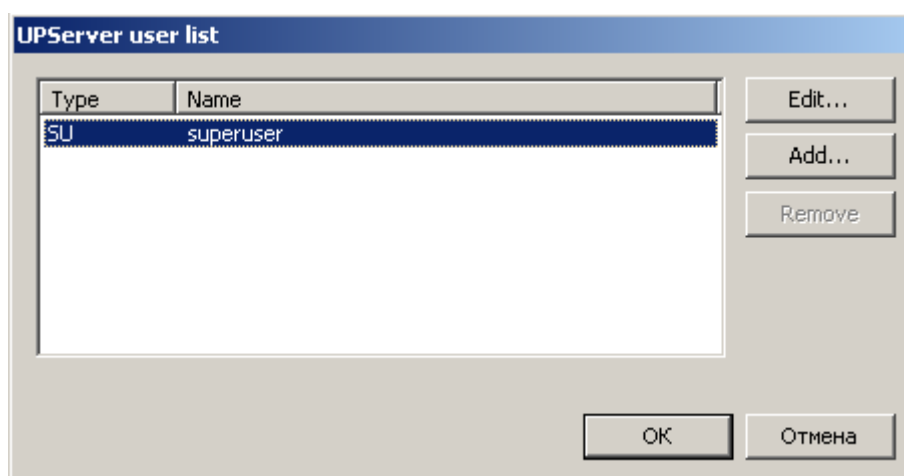


Рисунок 38

5. В окне **UPServer user** введите пароль дважды и нажмите ОК (Рисунок 39).

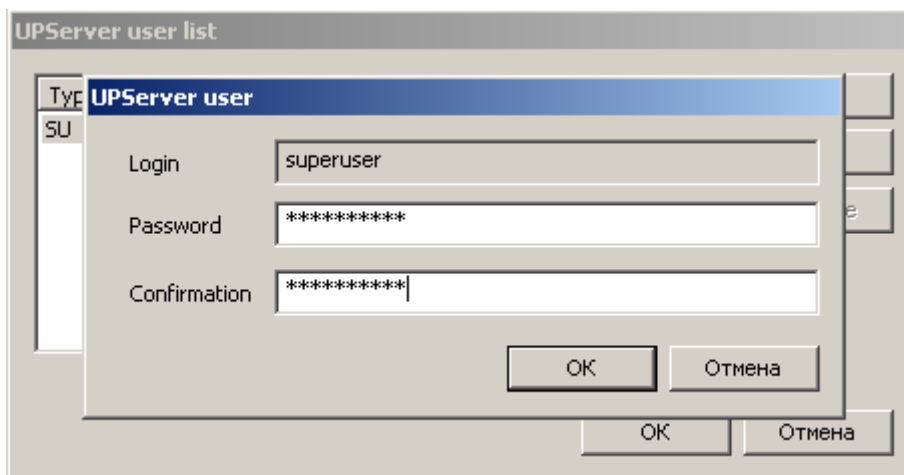


Рисунок 39

6. Только пользователь с идентификатором «superuser» и знающий его пароль может в дальнейшем назначать администратора, имеющего право доступа к Серверу управления.
7. Для назначения администратора нажмите кнопку **Add...** (Рисунок 40).

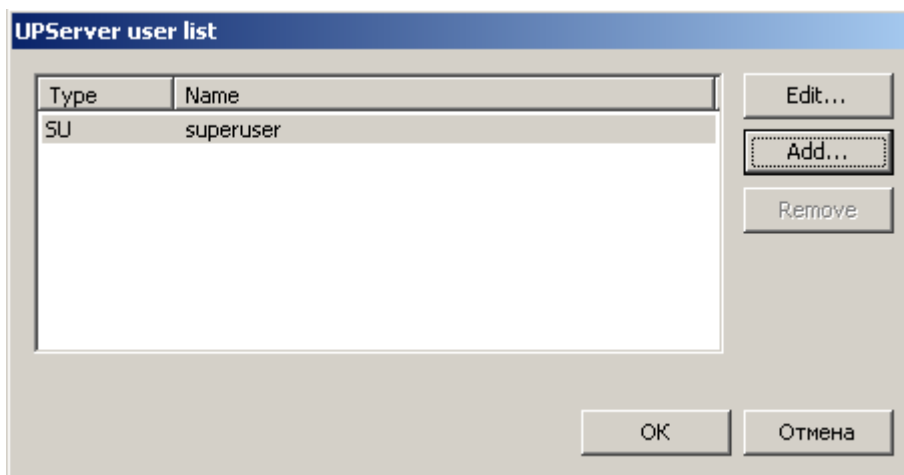


Рисунок 40

8. Назначьте имя и пароль администратору и нажмите кнопку **OK** дважды (Рисунок 41).

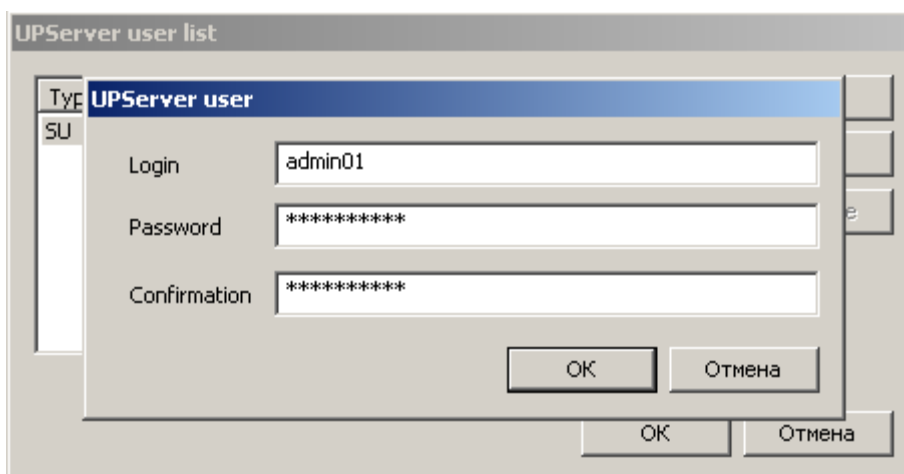


Рисунок 41

9. Закройте консоль Сервера управления - **VPN UPServer Console**.

10. В дальнейшем при запуске консоли Сервера управления (Пуск-Программы-S-Terra\_Bel-Bel VPN КР- UPServer Console) будет появляться окно **UPServer login** для ввода имени и пароля администратора для доступа к Серверу управления (Рисунок 42).

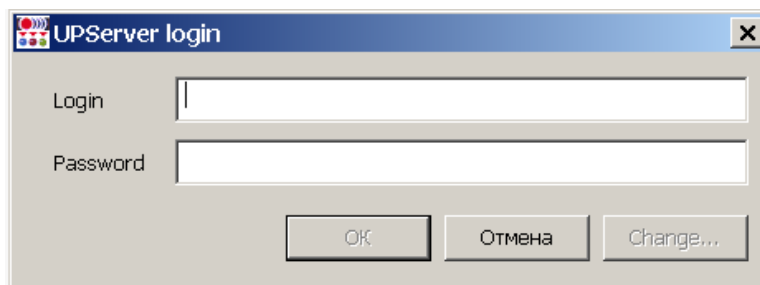


Рисунок 42

11. В этом же окне назначенный администратор может изменить свой пароль, нажав кнопку **Change...** (Рисунок 43).

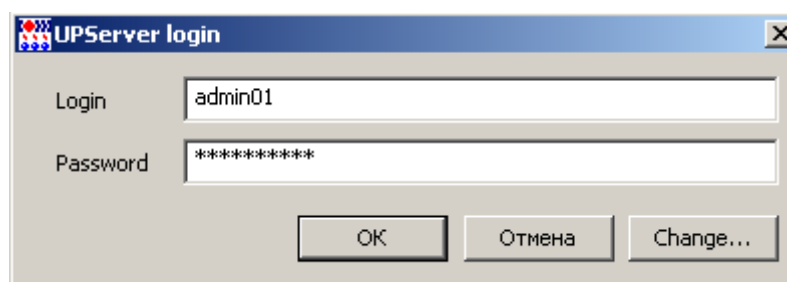


Рисунок 43

12. После нажатия кнопки **ОК** при успешном вводе данных запустится консоль Сервера управления - **VPN UPServer Console** (Рисунок 44).
13. После трех общих неуспешных попыток ввода идентификатора и пароля администратора, окно консоли Сервера управления не откроется, а появится сообщение о трех неуспешных попытках ввода данных и закрытии системы.
14. Если администратор с именем «superuser» не назначит еще одного администратора, кроме себя, для доступа к Серверу управления, то при запуске консоли Сервера управления окно **UPServer login** появляться не будет.

## 4.2. Настройка Сервера управления

Начальная настройка Сервера управления производится во вкладке **Settings**, а настройка и управление клиентами – во вкладке **Clients** (Рисунок 44).

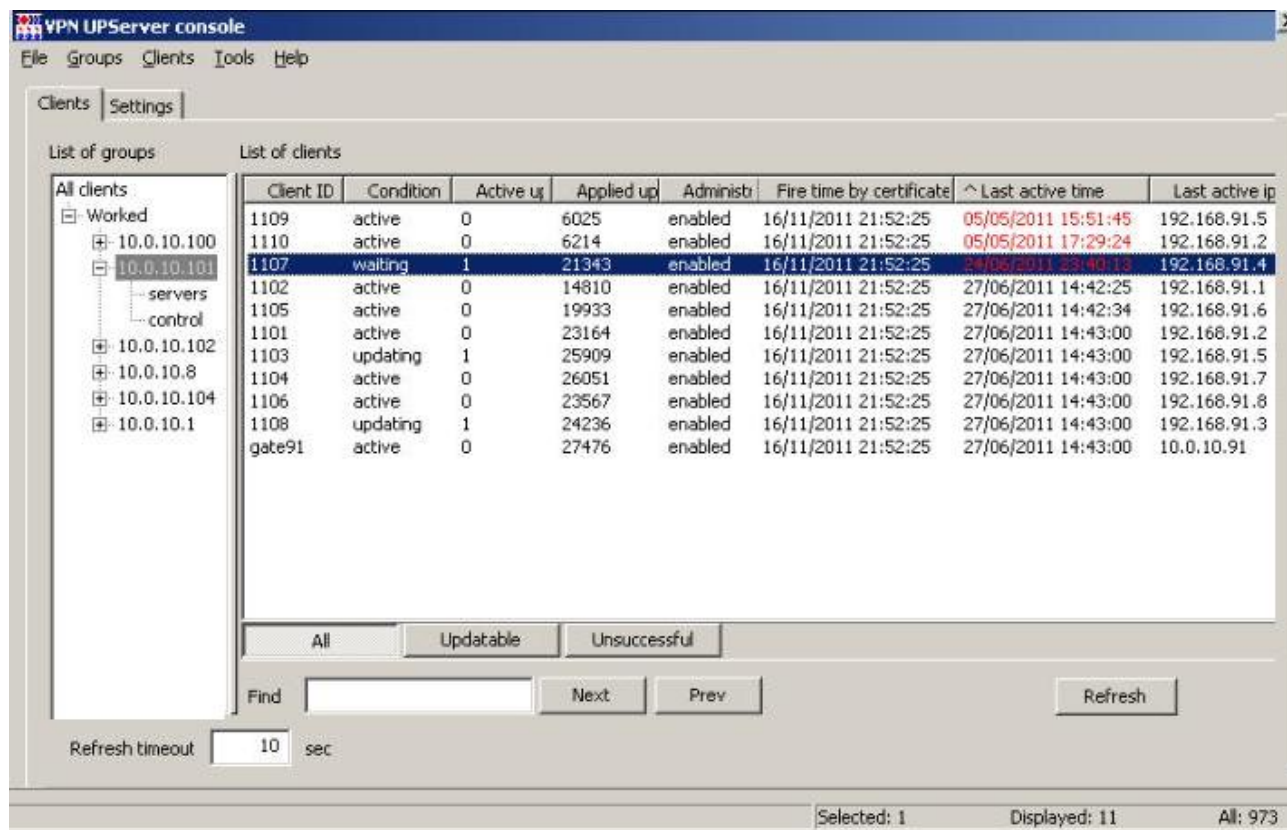


Рисунок 44

Меню графического интерфейса описано в главе «[Описание интерфейса Сервера управления](#)».

Начальная настройка Сервера управления производится во вкладке **Settings**, а настройка и управление клиентами – во вкладке **Clients**.

При первом запуске приложения **VPN UPServer Console** выводится предупреждение о необходимости задать настройки продукта **Сервер управления** (Рисунок 45).

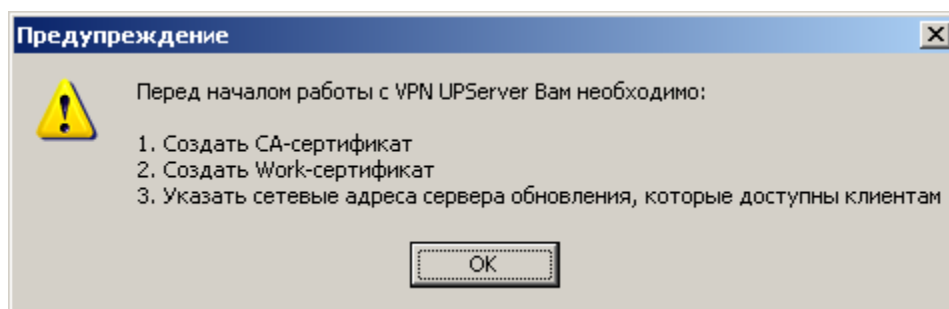


Рисунок 45

Нажмите кнопку **OK**, откроется окно настроек продукта Сервер управления (Рисунок 46). Во вкладке **Settings** введите данные лицензии, создайте CA-сертификат и рабочий сертификат (work certificate) Сервера управления, а также задайте сетевые адреса Сервера управления, что далее описано подробно по пунктам.

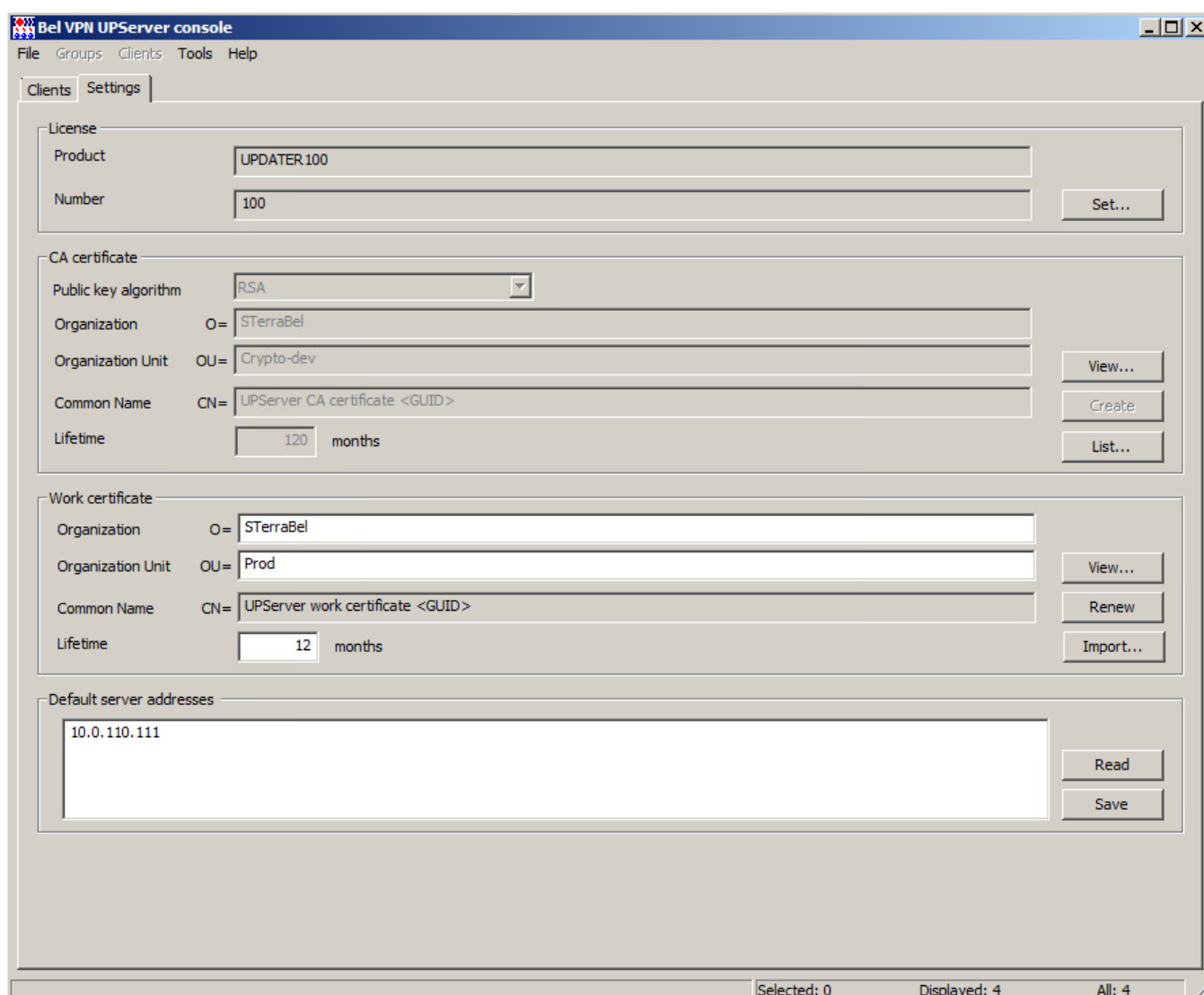


Рисунок 46

### 4.2.1. Ввод лицензии

Для ввода лицензии на продукт Сервер управления нажмите кнопку [Set...](#) (Рисунок 46).

В появившемся окне **Set license** (Рисунок 47):

в поле **Product** выберите тип продукта из выпадающего списка:

UPDATER100 – продукт будет работать с количеством Клиентов управления не более 10;

UPDATER1000 – продукт будет работать с количеством Клиентов управления не более 50;

UPDATER3000 – продукт будет работать с количеством Клиентов управления не более 1000;

UPDATER7000 – продукт будет работать с неограниченным количеством Клиентов управления

в поле **Customer code** укажите название организации, которой выдана лицензия

в поле **License number** введите номер лицензии

в поле **License code** введите код лицензии.

Все эти данные можно взять с бланка лицензии, поставляемой вместе с продуктом.

Если лицензия была получена в виде файла, то нажмите кнопку [Load from file...](#) и данные для заполнения полей будут взяты из этого файла.

Если лицензия на продукт не введена, то продукт будет работать максимум с двумя Клиентами управления.

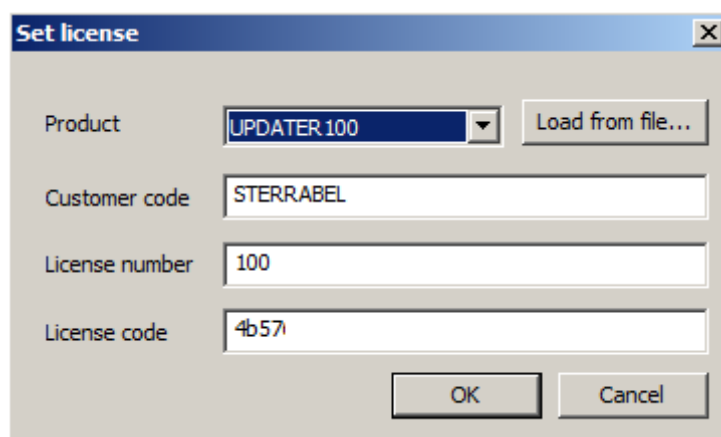


Рисунок 47

## 4.2.2. Создание CA сертификата



Note

Создать CA сертификат и рабочий сертификат Сервера управления можно с помощью доверенного УЦ, а потом импортировать их на Сервер управления. Существует одно ограничение: поле CN такого сертификата должно начинаться с зарезервированной строки **CN=UPServer CA certificate**.

Можно выполнить создание CA сертификата прямо на Сервере управления.

1. В группе **CA certificate** (Рисунок 46) нажмите кнопку **Create** и заполните поля в окне **Create new CA certificate**, например, следующими значениями (Рисунок 48):

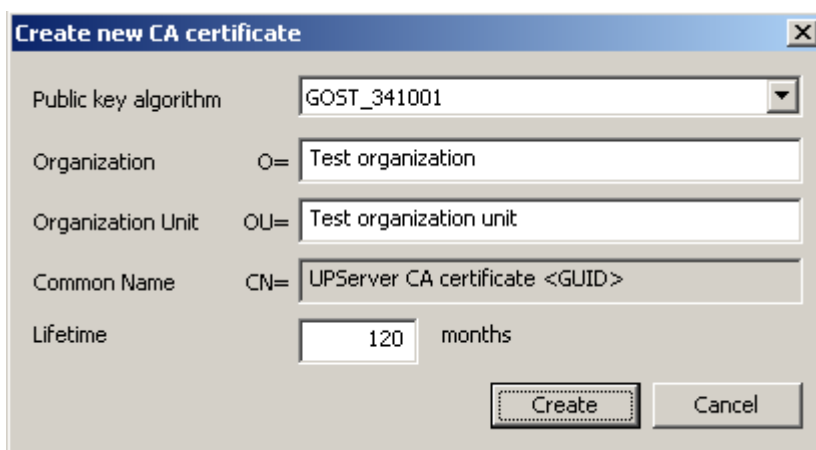


Рисунок 48

где

**Public key algorithm** – алгоритм генерации открытого ключа CA сертификата и ЭЦП, доступны два алгоритма:

RSA - длина открытого ключа – 2048 бит

**Organization** – название организации

**Organization Unit** – название отдела в организации

**Common Name** – имя владельца сертификата, заполняется автоматически

**Lifetime** – срок действия сертификата в месяцах.

- После этого нажмите кнопку **Create**, будет выдано **Предупреждение** (Рисунок 49), нажмите **OK**.

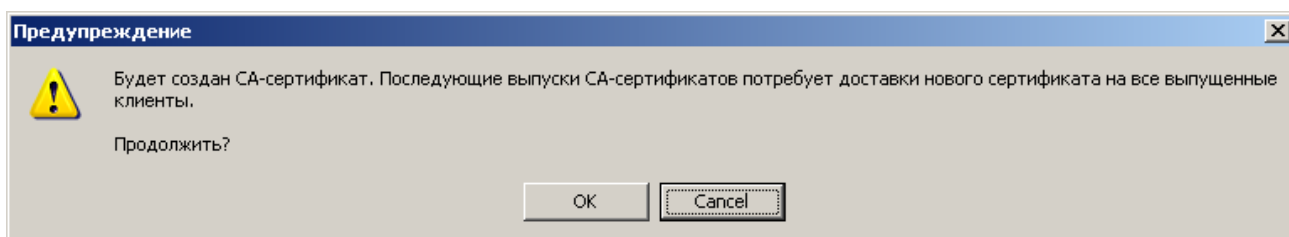


Рисунок 49

- СА сертификат создан и хранится в сертификатном хранилище операционной системы, нажмите **OK**.

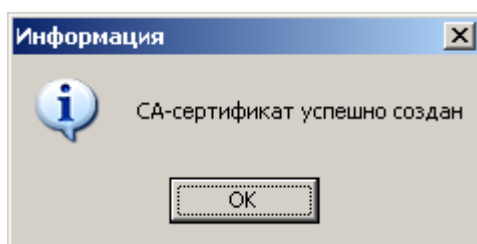


Рисунок 50



Note

Рекомендуется СА сертификат и секретный ключ к нему сохранить на другом компьютере для предотвращения потери СА-сертификата при поломке компьютера, на котором установлен Сервер управления.

### 4.2.3. Создание рабочего сертификата

- В группе **Work certificate** (Рисунок 46) заполните поля рабочего (локального) сертификата Сервера управления и нажмите кнопку **Create**. Перед созданием будет выдано **Предупреждение** (Рисунок 51):

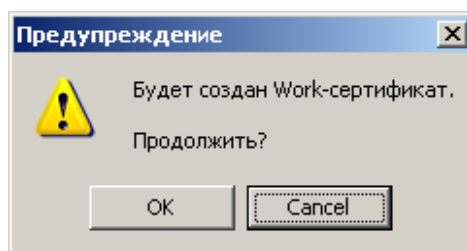


Рисунок 51

- Если поля заполнены верно – нажмите кнопку **OK**. Возможен запрос ключевого носителя для размещения контейнера с секретным ключом рабочего сертификата.
- Серверу управления необходимо сообщить пароль на контейнер рабочего сертификата, если он не пустой, введя в поле **Key container password**. Имя и пароль на контейнер будут использованы при подписании обновлений для клиентов (Рисунок 52).

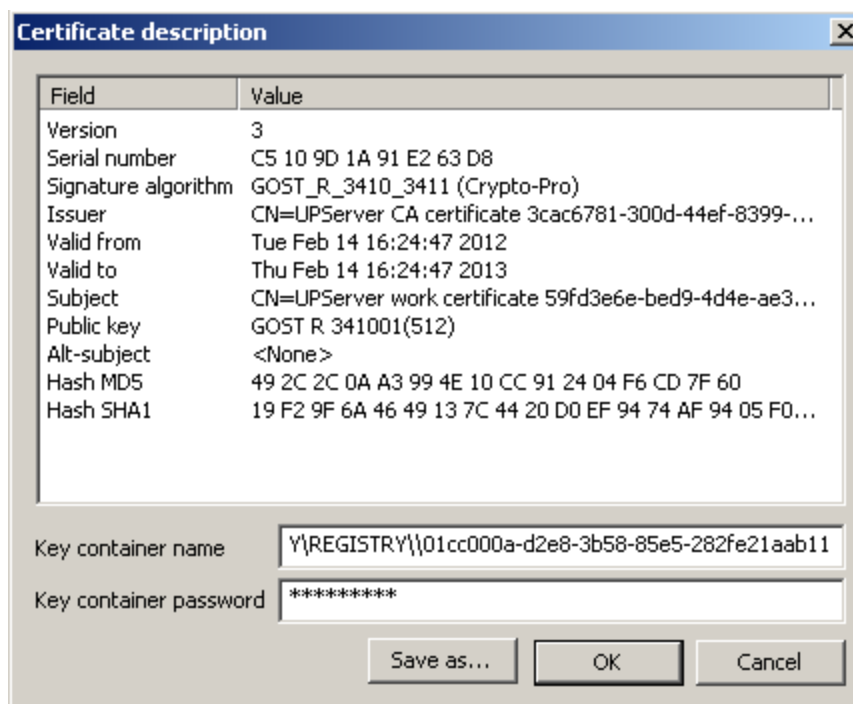


Рисунок 52

- После успешного создания сертификата будет выдано подтверждение, нажмите кнопку **OK** (Рисунок 53).

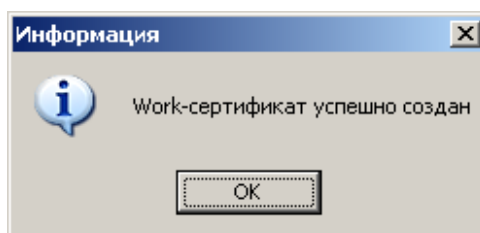


Рисунок 53

После этого кнопка **Create** в группе **Work certificate** изменится на **Renew** (Рисунок 46).

По истечению срока действия рабочего сертификата пересоздайте его, нажав кнопку **Renew**.

#### 4.2.4. Задание адресов Сервера управления

- В группе **Default server addresses** (Рисунок 46) задайте список сетевых адресов Сервера управления, которые доступны с управляемых устройств, следуя при этом следующим правилам:
  - каждый адрес должен располагаться на отдельной строке, перевод строки осуществляется нажатием клавиши **Enter** или **Ctrl-Enter**
  - сетевой адрес представляет собой IP-адрес или DNS-имя, которое будет транслироваться в IP-адрес на устройстве в момент создания соединения с Сервером управления
  - Сервер управления должен размещаться в подсети, защищенной шлюзом безопасности (центральным). Согласно Рисунку 2 адрес Сервера управления – 10.0.10.111.
- После задания адресов обязательно нажмите кнопку **Save**, появится предупреждение (Рисунок 54).



3. Если адреса введены верно, то нажмите кнопку **OK**, при этом происходит проверка введенных данных и только после этого во все создаваемые дистрибутивы Клиентов управления по умолчанию будет вноситься список адресов Сервера управления.

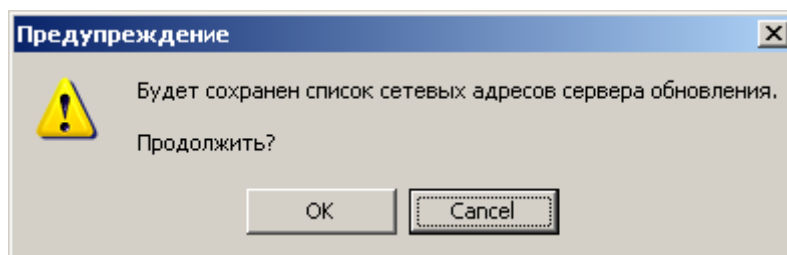


Рисунок 54



На данном этапе категорически не рекомендуется задавать адреса, не принадлежащие Серверу управления. Адреса, не принадлежащие Серверу управления, могут быть указаны только при процедуре перевода клиентов на другой Сервер управления. Инструкция по переводу клиентов на другой Сервер управления будет выдаваться по запросу пользователя при появлении такой потребности.

Далее перейдите во вкладку **Clients** и выполните настройки для центрального шлюза.

## 5. Настройка и управление центральным шлюзом

Создание и удаление учетных записей клиентов управляемых устройств, создание для них Клиентов управления, обновлений будем выполнять во вкладке **Clients** (Рисунок 55) Сервера управления, интерфейс которой описан в разделе «Описание интерфейса Сервера управления».

Во вкладке **Clients** отражается информация обо всех управляемых устройствах. Далее, будет выполняться настройка центрального шлюза для стенда, приведенного на рисунке 2.

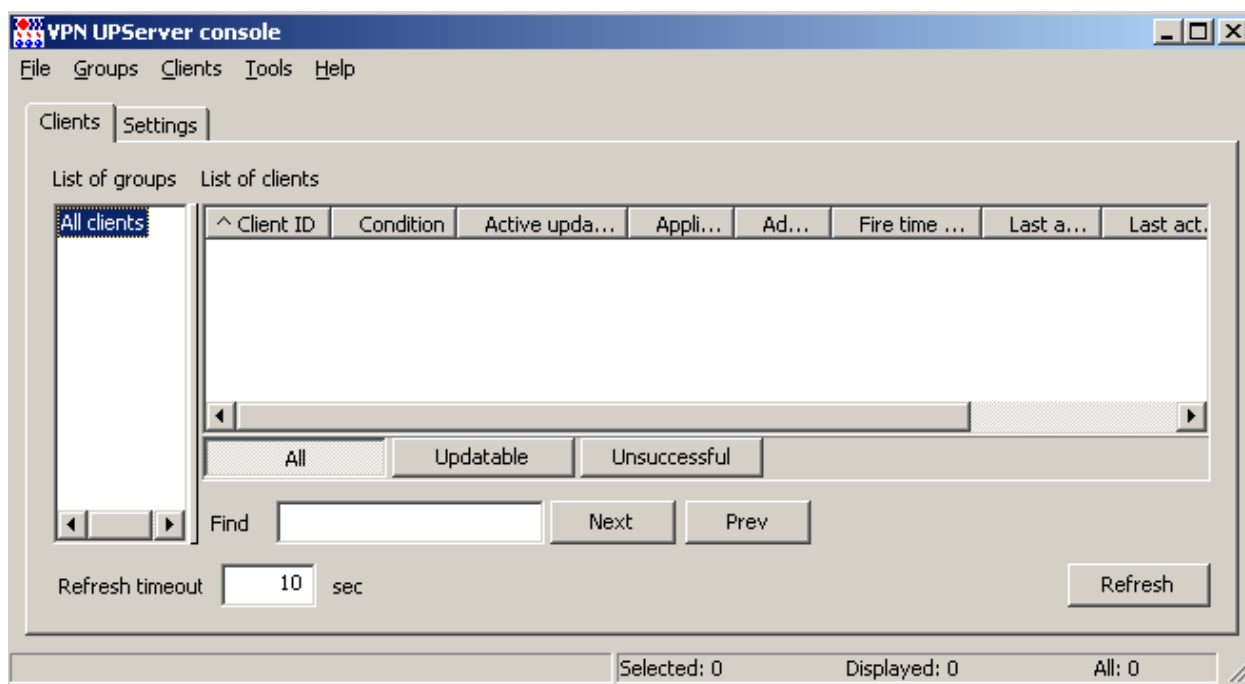


Рисунок 55

### 5.1. Создание учетной записи клиента для центрального шлюза

1. В меню **Clients** выберите предложение **Create** (Рисунок 56).

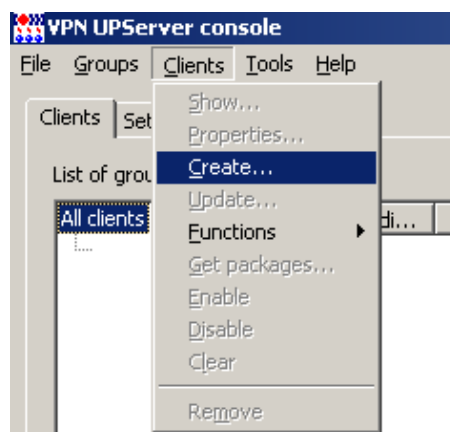


Рисунок 56

Появившееся окно **Create new client** (Рисунок 57) создания нового клиента имеет следующие поля:

**Client ID** – уникальный идентификатор клиента, может состоять из любых символов, за исключением следующих: <ПРЯМОЙ СЛЕШ>, <ОБРАТНЫЙ СЛЕШ>, <ДВОЕТОЧИЕ>, <ЗВЕЗДОЧКА>, <СИМВОЛ ВОПРОСА>, gate0<ДВОЙНЫЕ КАВЫЧКИ>, <ЗНАК МЕНЬШЕ>, <ЗНАК БОЛЬШЕ>, <ВЕРТИКАЛЬНАЯ ЧЕРТА>, <ТАБУЛЯЦИЯ>. Идентификатор не должен начинаться или заканчиваться символами <ПРОБЕЛ> или <ТОЧКА>, и не должен быть равен “NUL” или “CON”, или “PRN”, или “AUX”, или “COMx”, где  $x \in [1..9]$ , или “LPTx”, где  $x \in [1..9]$

**Product package** – имя инсталляционного файла Bel VPN Gate 4.1, созданного с помощью окна **VPN data maker**, вызываемого кнопкой **E**

Кнопка **E** – вызывает окно **VPN data maker** (Рисунок 58) для задания политики безопасности и настроек продукта Bel VPN Gate 4.1

**Device password** – пароль устройства для выполнения дополнительных действий на нем, в данной версии поле не используется

**UPAgent settings** – имя файла с настройками Клиента управления, по умолчанию имя файла уже задано (см. главу «Настройки Клиента управления»).

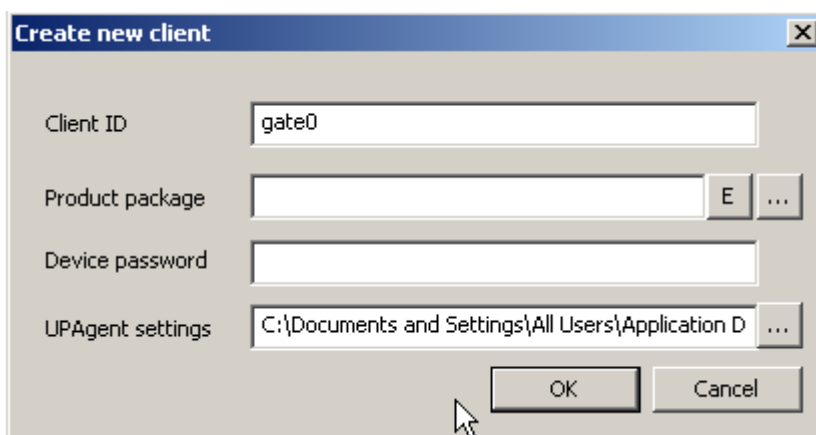


Рисунок 57

2. В поле **Client ID** введите идентификатор клиента, например, gate0.
3. Поле **UPAgent settings** оставьте без изменений, в нем указано имя файла с настройками Клиента управления.
4. В поле **Product package** нажмите кнопку **E**, появится окно **VPN data maker** (Рисунок 58).

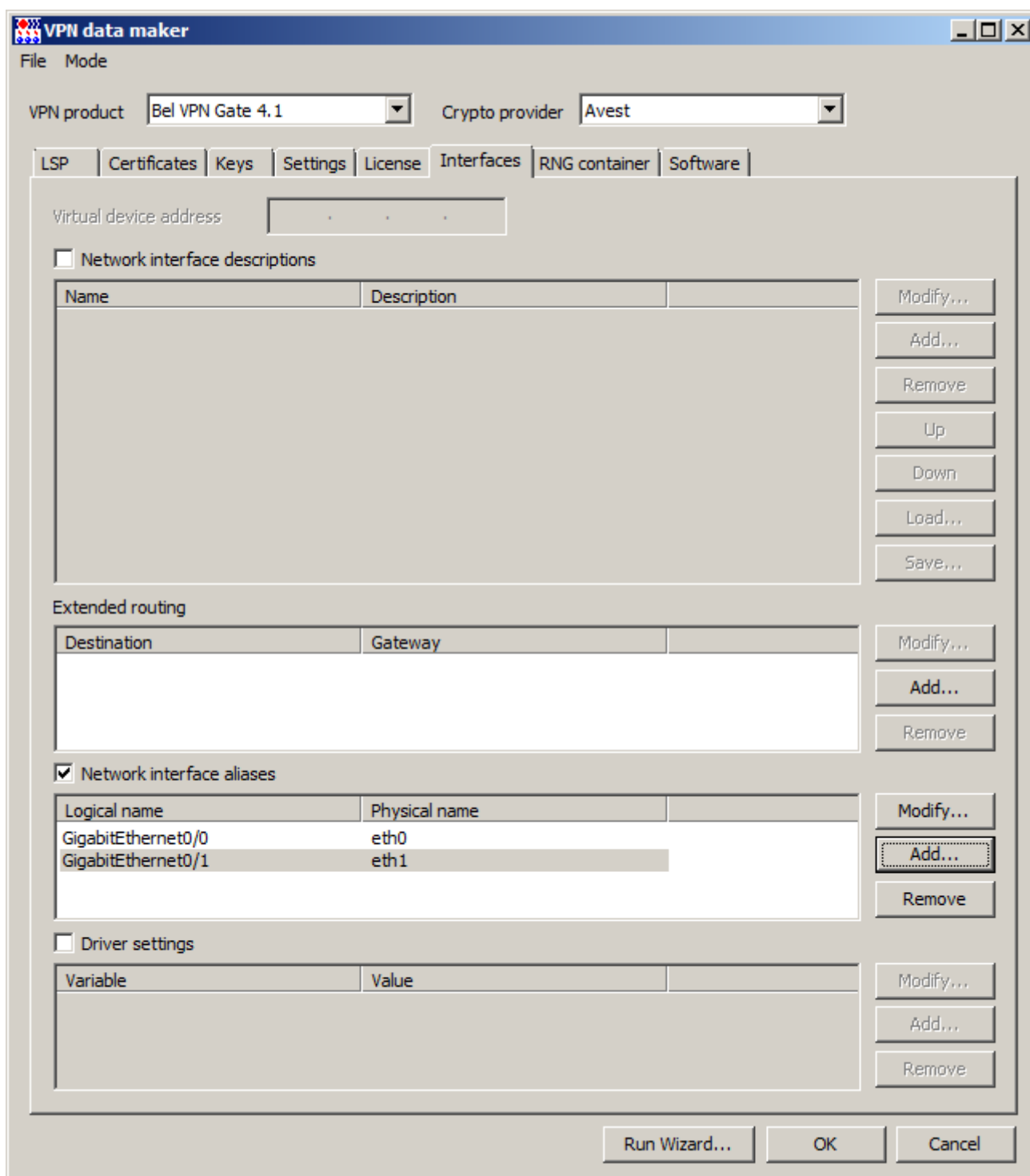


Рисунок 58

5. В окне **VPN data maker** выберите продукт Bel VPN Gate 4.1 и криптопровайдера, например, CryptoPro (Рисунок 58).
6. Далее нужно задать политику безопасности для шлюза и другие настройки. Сложную политику можно задать во вкладке **LSP** (Рисунок 58) в текстовом виде или в виде cisco-like конфигурации, или загрузить из файла, предварительно создав его. А остальные настройки ввести в других вкладках.

Для создания несложной политики можно использовать окна мастера, нажав кнопку [Run Wizard](#) в окне **VPN data maker**, появится окно для выбора метода аутентификации шлюза при взаимодействии со своими партнерами (Рисунок 59). Интерфейс этого окна описан в разделе «[Задание политики и настроек с использованием мастера](#)».

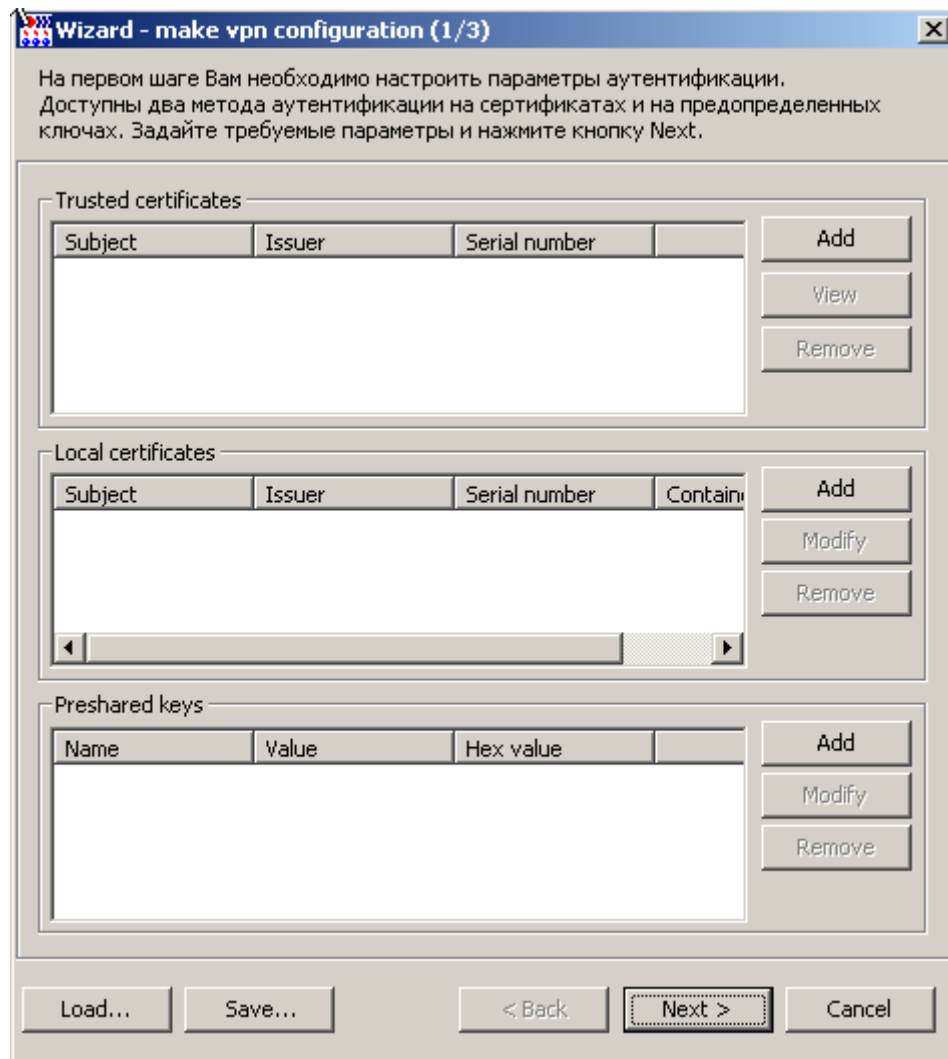


Рисунок 59

- Для примера выберем аутентификацию с использованием предопределенного ключа. В разделе Preshared keys нажмите кнопку **Add** (Рисунок 59).

8. В открывшемся окне Preshared key (Рисунок 60) введите имя ключа, например, `key0`, и значение ключа, нажмите кнопку **OK**.

**Preshared key**

Key name:

Key value:

Key hex value:

Load from file...

OK Cancel

Рисунок 60

9. Предопределенный ключ добавился в проект, нажмите кнопку **Next** (Рисунок 61).

**Wizard - make vpn configuration (1/3)**

На первом шаге Вам необходимо настроить параметры аутентификации. Доступны два метода аутентификации на сертификатах и на предопределенных ключах. Задайте требуемые параметры и нажмите кнопку Next.

**Trusted certificates**

Subject	Issuer	Serial number

Add View Remove

**Local certificates**

Subject	Issuer	Serial number	Contains

Add Modify Remove

**Preshared keys**

Name	Value	Hex value
key0	1234567890key0	31 32 33 34 35...

Add Modify Remove

Load... Save... < Back Next > Cancel

Рисунок 61

10. В следующем окне задайте правила обработки трафика, согласно которым центральный шлюз будет пропускать трафик от управляемых устройств к Серверу управления и обратно. При этом трафик между управляемыми устройствами и центральным шлюзом должен быть защищен (Рисунок 62). Для создания правила нажмите кнопку **Add**.

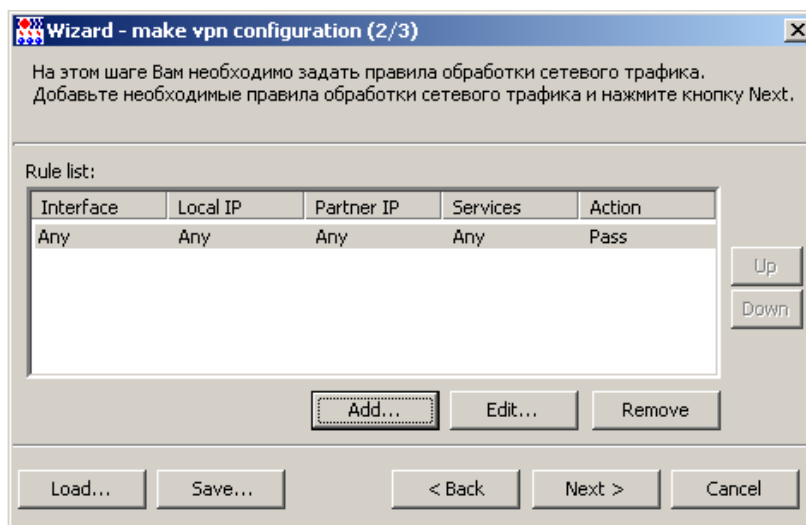


Рисунок 62

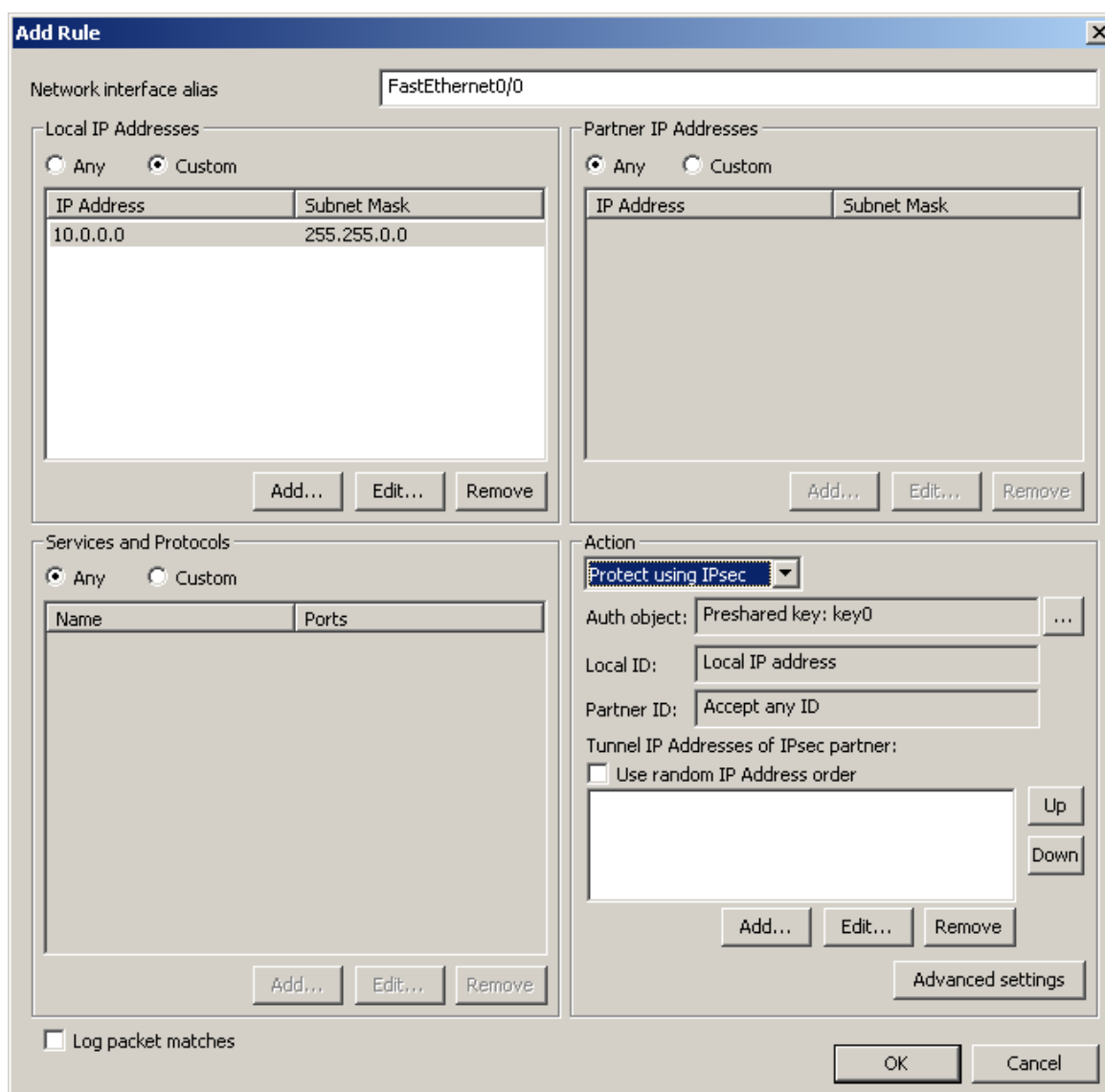


Рисунок 63

11. Создаваемое правило привяжите к интерфейсу шлюза с логическим именем `FastEthernet0/0`, который смотрит во внешнюю сеть (Рисунок 2). В области **Local IP Addresses** (Рисунок 63) укажите адрес защищаемой подсети - `10.0.0.0/16`, в эту подсеть смотрит интерфейс шлюза с именем `eth1`. Шлюз должен взаимодействовать с любыми партнерами, поэтому в области **Partner IP Addresses** поставьте переключатель в положение `Any`. В области **Action** - переключатель в положение **Protect using IPsec**, не указывая адрес IPsec партнера (адрес может быть любым).
12. После нажатия кнопки **OK** появится предупреждение (Рисунок 64). Нажмите кнопку **Yes**.

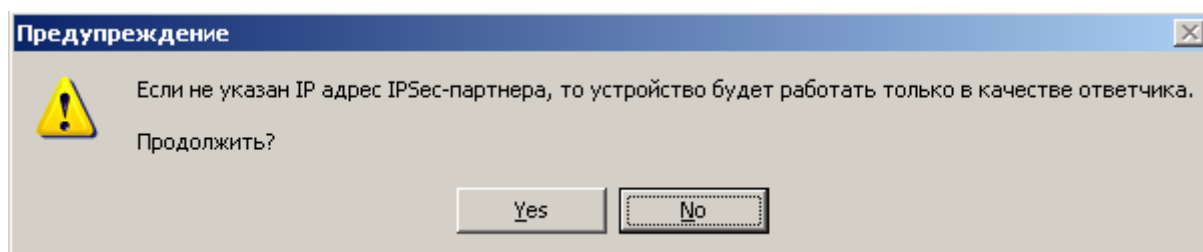


Рисунок 64

13. Увеличьте приоритет созданного правила (Рисунок 65), нажав кнопку **Up**.

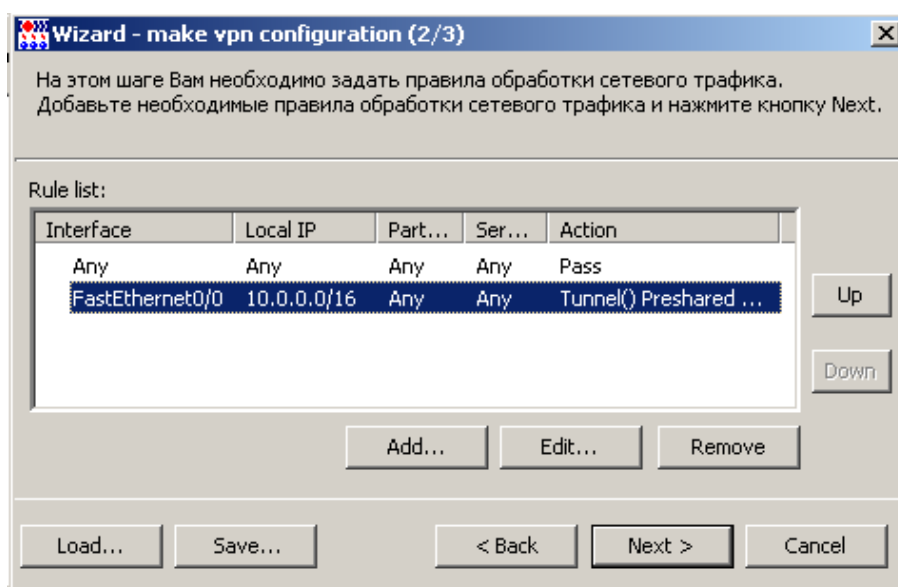


Рисунок 65

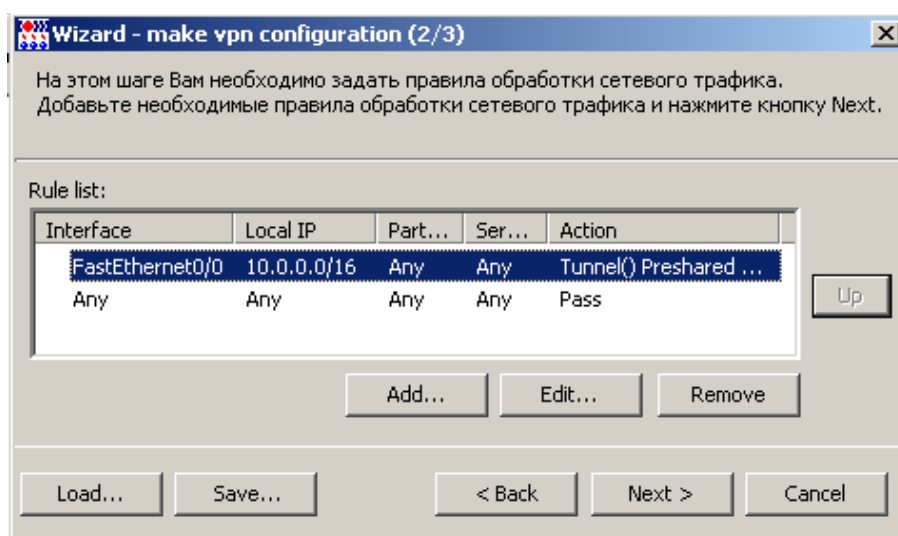


Рисунок 66



14. Нажмите кнопку **Next** (Рисунок 66).
15. Введите данные лицензии на продукт Bel VPN Gate 4.1 (Рисунок 67).

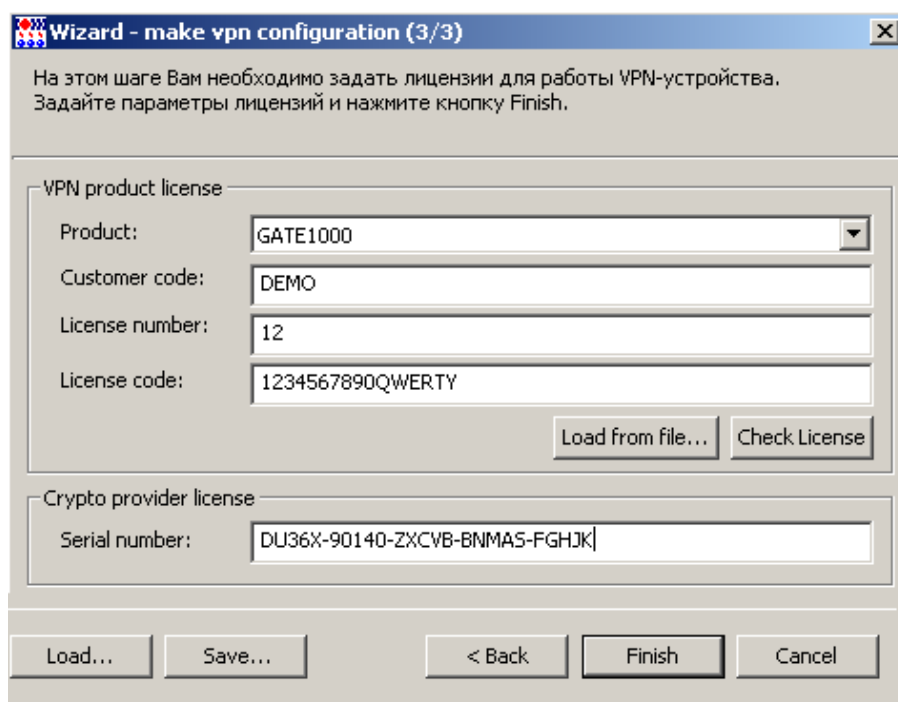


Рисунок 67

16. Сохраните введенные данные в окна мастера, нажав кнопку **Save...** (Рисунок 67), и укажите имя файла-проекта в любом созданном вами каталоге (Рисунок 68).

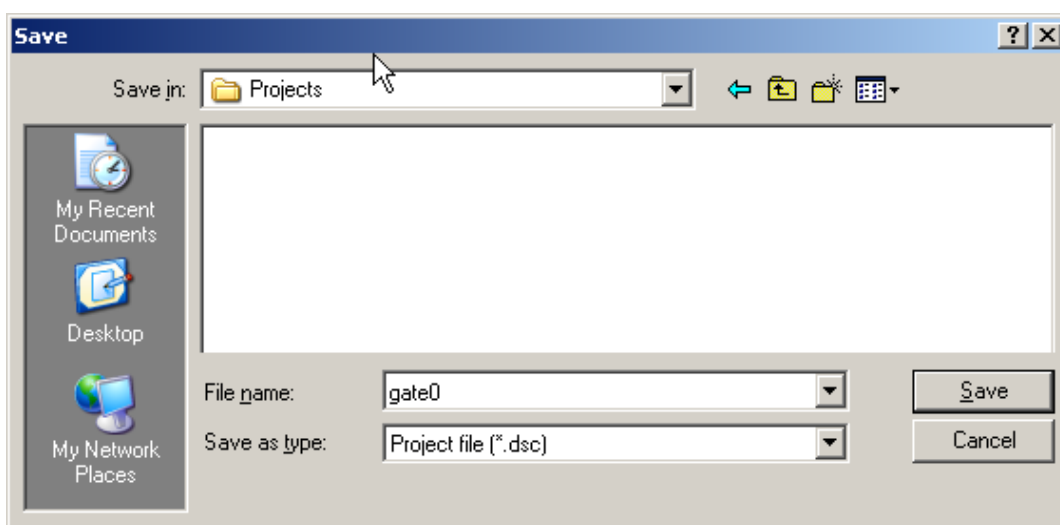


Рисунок 68

17. В окне мастера нажмите кнопку **Finish** (Рисунок 67). Все введенные данные будут отражены во вкладках проекта (Рисунок 69), за исключением вкладки **Interfaces**.

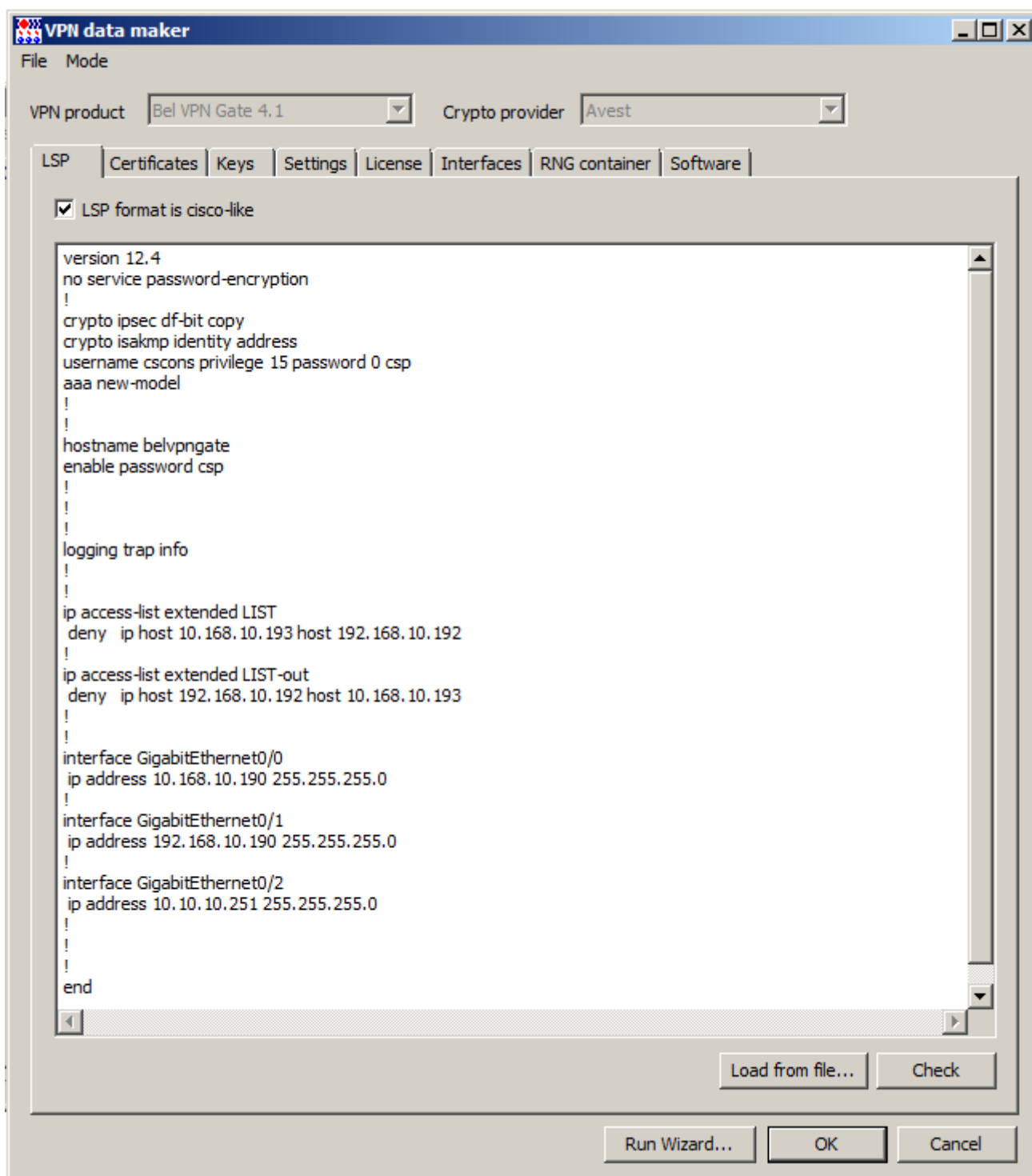


Рисунок 69

18. Перейдите во вкладку **Interfaces** и задайте соответствие между логическими и физическими именами интерфейсов шлюза безопасности. Для получения имен интерфейсов используйте:

утилиту `/opt/VPNagent/bin/if_show` - для Gate 4.1.

Во вкладке **Interfaces** установите флажок **Network interface aliases**, нажмите кнопку **Add** и в окне **Network interface alias** введите логическое и физическое имя интерфейсов (Рисунок 70).

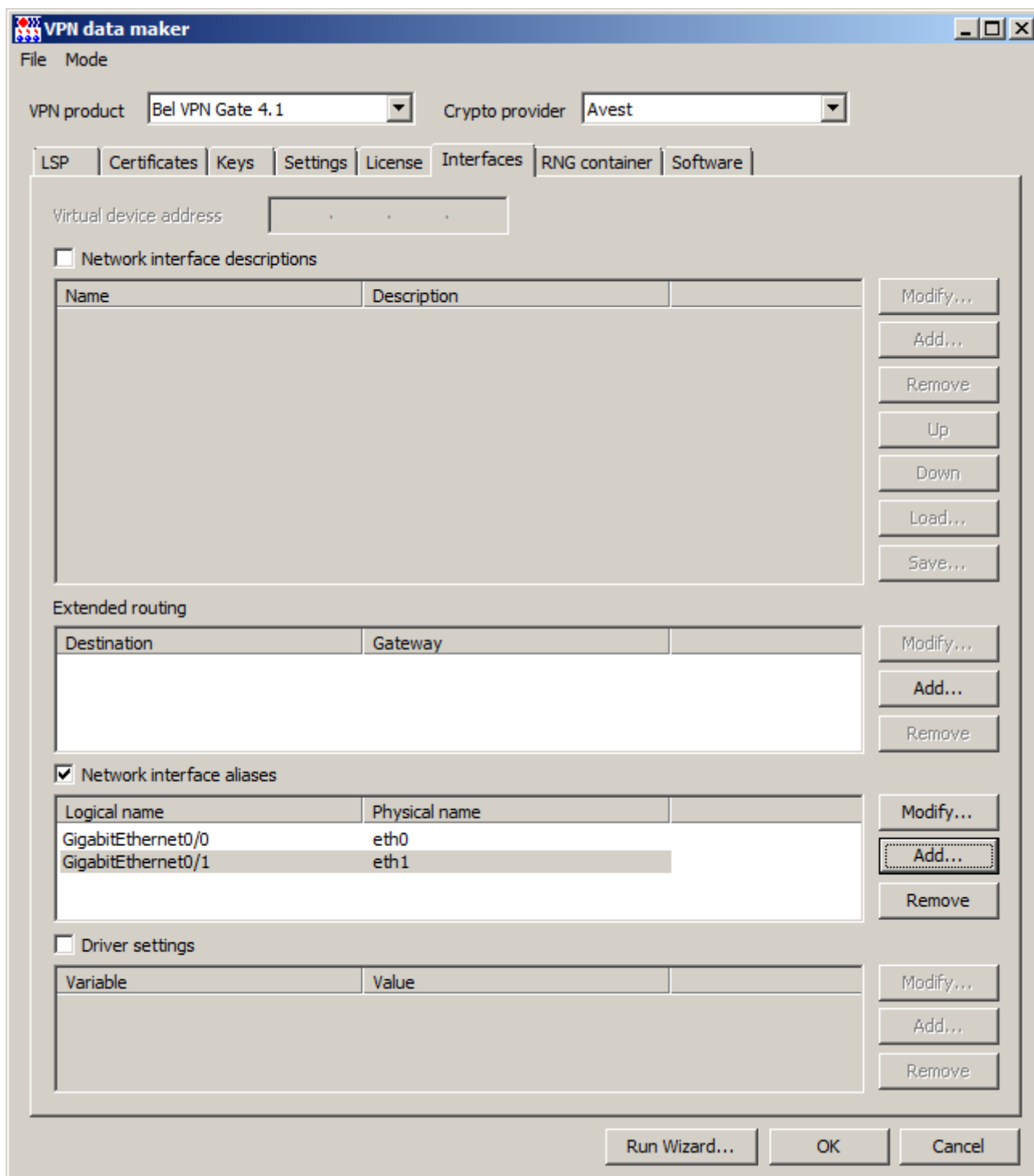


Рисунок 70

19. Во вкладке **Interfaces** нажмите кнопку **OK**, появится окно с настройками нового клиента (Рисунок 71), опять нажмите кнопку **OK**.

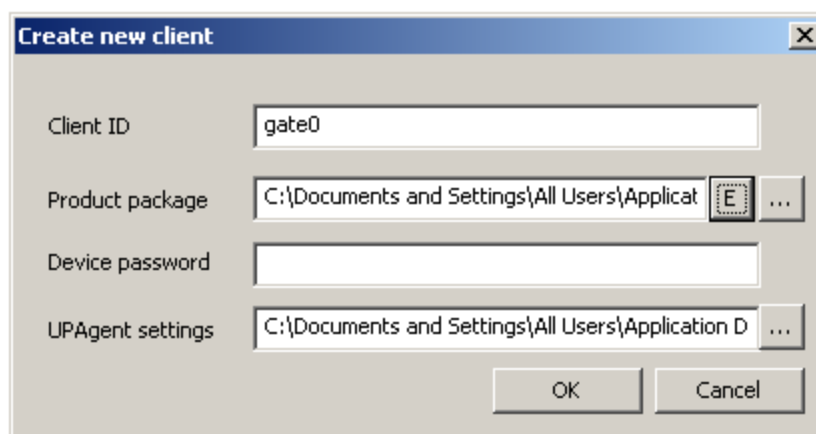


Рисунок 71

20. На Сервере управления в таблице клиентов появился новый клиент `gate0`. Переведите его в активное состояние, выбрав в контекстном меню предложение **Enable** (Рисунок 72).

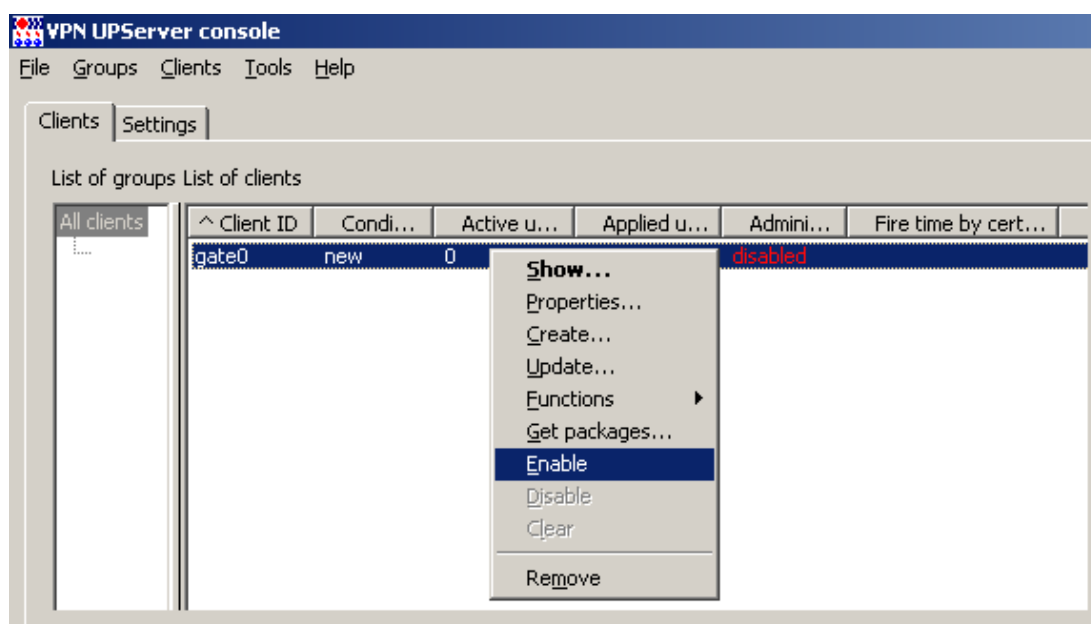


Рисунок 72

## 5.2. Подготовка скриптов для Клиента управления и Bel VPN Gate 4.1

1. Для установки Клиента управления, дистрибутив которого размещен на шлюзе в каталоге `/packages`, и обновления настроек Bel VPN Gate 4.1 следует подготовить два скрипта. Для клиента `gate0` выберите предложение **Get packages** в контекстном меню (Рисунок 73).

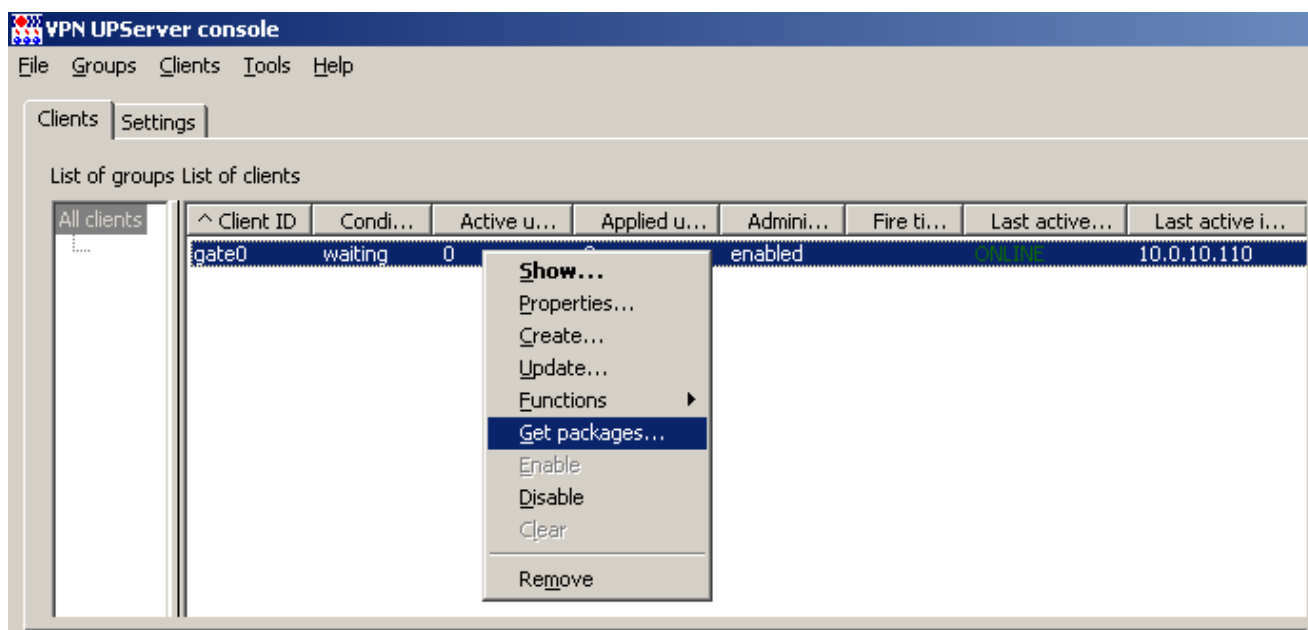


Рисунок 73

2. В открывшемся окне укажите каталог для сохранения скриптов (Рисунок 74).

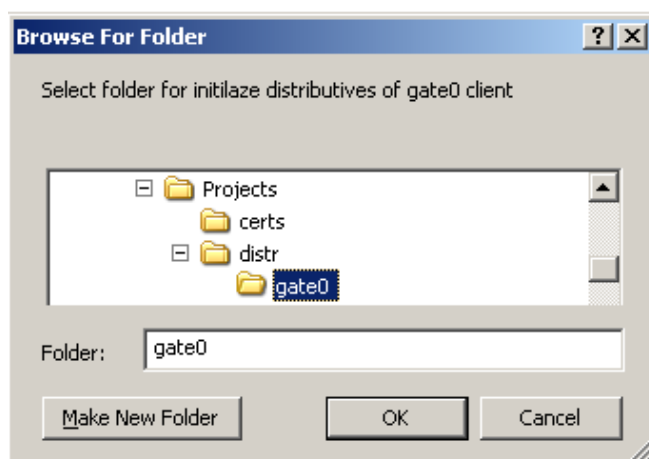


Рисунок 74

В указанный каталог будут сохранены два файла (Рисунок 75), (Рисунок 76):

- setup\_upagent.sh – скрипт для инициализации Клиента управления
- setup\_product.sh – скрипт для настройки продукта Bel VPN Gate 4.1.

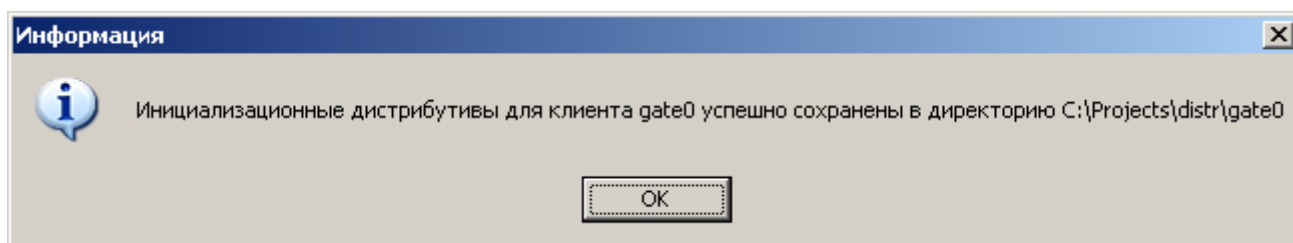


Рисунок 75

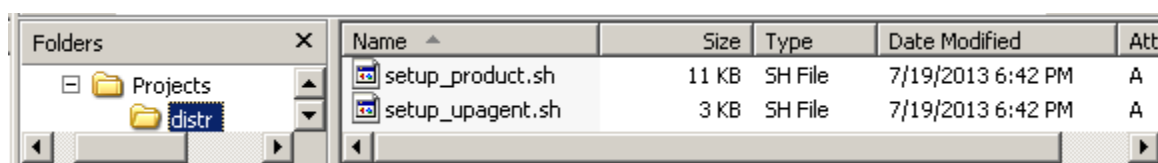


Рисунок 76

### 5.3. Доставка и запуск скриптов

Установка созданных скриптов на центральном шлюзе осуществляется в следующем порядке - сначала скрипт `setup_upagent.sh`, а затем - `setup_product.sh`. Такой порядок обусловлен тем, что для успешного выполнения скрипта `setup_product.sh`, необходим установленный и инициализированный Клиент управления.

Примечание: продукт Bel VPN Gate 4.1 версии 4.1, поставляется на устройстве в установленном состоянии вместе с Клиентом управления, требуется инициализировать только Клиента управления.

Если на устройстве уже работает продукт Bel VPN Gate 4.1 и не предполагается изменение его политики безопасности, то инициализируйте (инсталлируйте) только Клиента управления.

Установка созданных скриптов осуществляется локально, так как Клиент управления на этом устройстве еще не инициализирован (инсталлирован). Поэтому доставьте скрипты на шлюз безопасности по заслуживающему доверия каналу связи и запустите локально.

1. Для доставки можно использовать:

- распространяемую бесплатно утилиту `pscp.exe` из пакета Putty;
  - либо терминальную программу, например, Putty;
  - либо USB-флеш
  - либо FTP-сервер (FileZilla Server) на Сервере управления.
- а) При использовании утилиты `pscp.exe` на Сервере управления выполните команды, предварительно создав каталог `/tmp` на шлюзе:

```
pscp setup_upagent.sh root@10.0.10.110:/tmp
pscp setup_product.sh root@10.0.10.110:/tmp
```

Далее перейдите к [пункту 2](#).

- б) При использовании терминальной программы, например, Putty Configuration, укажите адрес интерфейса шлюза `eth1` - `10.0.10.110` (Рисунок 77).

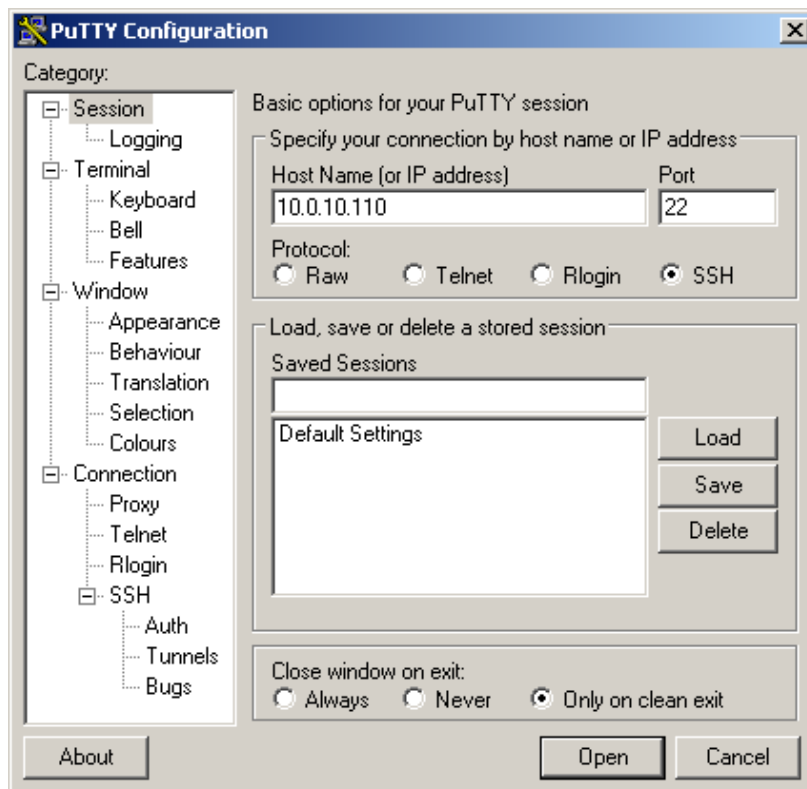


Рисунок 77

На шлюзе создайте каталог, например, /tmp. Скопируйте каждый скрипт в буфер, предварительно открыв его, например, в Wordpad, так как они являются текстовыми файлами. После открытия терминальной сессии со шлюзом задайте команду:

```
cat > /tmp/setup_upagent.sh
```

После нажатия **Enter** вставьте скопированный скрипт и нажмите **Ctrl-D** (Рисунок 78).

```

root@cspgate:~
login as: root
Sent username "root"
root@10.0.10.110's password:
Last login: Wed Nov 30 16:33:06 2011 from 192.168.2.111
[root@cspgate ~]# cat > /tmp/setup_upagent.sh
if [ -e /packages/VPNUPagent/install.sh ] ; then
    cd /packages/VPNUPagent; /packages/VPNUPagent/install.sh
    if [ $? != 0 ] ; then
        echo Error: Cannot install VPNUPagent
        exit 1
    fi
fi
FILE_NAME=/tmp/vpnupagent.txt
echo "PDw8PCBTRlggMS4wWkxJQiAgICBUaXRzZT1FeHRyYWNOIGRpc3RyaWJldG12
ZQpRdWVzdGlvbj1WUE4gVVBzZ2VudCBmb3IgZ2FOZTAgd2lscCBiZSBpbmNO
YWxsZWQuIERvIGVbnRpbmVlPwptZXRlcD1zZXRlcC5zaCBDTElFTlRfSUQ9
ImdhGdUwIiBDTElFTlRfUFDkPSJiYzAyNDE5NDE0Yjc4NzIxMzY1ZjQ5NGQw
YmM3YjA1OSIgVVBfTU9ERT0id2luZG93bGVzcyIgVVFU9BU0tfTU9ERT0i
YXV0byIAeNpZS05MT10qOQMSDAMzHcNmphvGjQxHV3AzMTIxQWw3B+vuOx
LwtcFTZfmyiV/dGak41Vm4+ZSZAuVWSDUMFAjo05lIVZWDwOIdi1qCy1SMHZ
UQFkXmZaZnJiSaghvIESSAW3sFhIaGJQn5RemJeZlViSWZ+nkJpXmaJoZSB
BEgB17AghgIDOXFeQwMDSyMTQyMjCjOTKHFeIwTXOIr2DmhiVDLgZePUavNo
+87LyMjIysDcxMjPABTnYmpizGTyBFFntZ7/bj2XT7b9spzGXbM+dEe6XHnO
mmO4ZtPtsFt/nizsXovUVXhr4YdDR52kKj1WteMX/SO5S2/ehDwIZwpdmrfX3
K/JYndx+4CbDjkfa58V4fj7dL7NNlvvQPY+Dmk6VqHK65I4ujXu6THf5dFP
iV9zv+1jsKCJ2duo1Sui+qW+FLBrX9EXTdUXmrKMo0q0TePD/iZ3ZeaGmQyv
Ldi36nKGRPTSm7jgH3/H9NtpsgqHr9Xfm/66ozR01fTk+BtzXO797ud78/yc
Fic740IbT/kHV9bxbBtv7dv29vriRiCvz78Xviu98vSWTY1fnUtZ3HrDI/G3
Xt803P/rOsdME5eLvX5Gr2ne99nYmZkYFzcOMOgcapB4yRgMMoysjR2GTS2
NwJ02Joo6fhhXhrLurDhqsj3+IWJNi+uJnyplRkUX/59nh+jTs+YvCfwOH+2
ma2GB7prfx965rNa2HfaYpHfK3ok/qbdfDfxQq9gYbWa2e6262vbn19p4Pz+0
Xb12tvTs9zcMA+qrvIqDwzSt41Wk1+3o8NU22MRoXfTBavOL+NA2ExsHO5/6
7QvXflk7ob42azbzZGFZ+wfhlly6JmZ2dXLQ68OsNO2a5PGbhGZsbVd7OyuIx
iDfRW2Ba+25/ZsOPY65ME0uKlHdbtXk7ZC6WrY8yYRHNg+rdfeHH8sD3Q7++
X1z77pCDUmVCWaKdRJYD/zzRrQdXGSR9VPiU9jU8Z80Js8qzP1b91fY+euD+
PKvPK3W3bHw1/Xv97H8H1zpv8axMOyV70EEk+nLca7ei1HS9kooSYE5n2B8d
708WEu4Y5BoTGuCYnppXEsV5elimw6MBgNertDi1CK/xNxUZH5AYnFxeX5R
im1SsgEwF1qaGJoknVuYGxsmW5immViapBgkZsnGZha8nIFJJZk2OrnF5To
Qw3n5fLNTOm1Lc/MS8kvz0ktLoYy6VicDRZPLC3J5+Xi5UI4KizATwHmLIRp
QNFEiHFuxaklJZ156cUwD+2J9s1PByp2y8xJ9U2sCM6sSrU1NTQyABsbWpAC
9AdQ1jkjNTkbgCOgtSgzP8XWDCLtFgJNjOAVwQWpqSk+mbmZJbZASaBJIUWV
zvmleSW2xrxcQDZUJ9hksGxiGjDxhmTnpuaXltgaWgCFHVNSioBeNLA1NNAz
OAMShoaGYHs889LyY8HagB4BoHfsSEMzXi4ANKcHKwAABVgAAAAAIFNGWCA+
Pj4+
" > $FILE_NAME
/opt/UPAgent/bin/init.sh $FILE_NAME
RET=$?
rm -f $FILE_NAME
exit $RET

[root@cspgate ~]#

```

Рисунок 78

Аналогичным образом доставьте на шлюз второй скрипт `setup_product.sh`.

2. Измените права доступа к скриптам, выполнив локально на шлюзе команды:

```
[root@cspgate ~]# chmod +x /tmp/setup_upagent.sh
[root@cspgate ~]# chmod +x /tmp/setup_product.sh
```

3. Запустите локально скрипты на выполнение (для класса защиты КС1 и КС2):

```
[root@cspgate ~]# /tmp/setup_upagent.sh
warning: /packages/VPNUPAgent/libidn-0.6.5-1.1.i386.rpm: Header V3
DSA signature: NOKEY, key ID e8562897
Info: libidn is installed successfully
Info: Link /var/log/upagent to /tmp is created successfully
Info: VPNUPAgent is installed successfully
Adding new rndm:
Nick name: cpsd
Name device: CPSD RNG
Level: 1
Succeeded, code:0x0
File decompression...

cacert.cer
reg.txt
settings.txt

...Done
Starting VPN UPAgent watchdog daemon.done.
Initialization is successful
```

При запуске скрипта `setup_upagent.sh` выполняется проверка - установлен ли продукт VPNUPAgent (Клиент управления). Если он еще не установлен, то устанавливаются необходимые дистрибутивы и настраивается среда функционирования. В процессе установки дистрибутивов возможны интерактивные запросы на подтверждение действий.

Если Клиент управления не установлен, то на поставленном шлюзе будет непустой каталог `/packages/VPNUPAgent` с дистрибутивом продукта VPNUPAgent. Если Клиент управления установлен, то каталог `/packages` отсутствует. Если Клиент управления не установлен и каталог пустой, то на установленном Сервере управления имеется архив `vpnupagent.tar`, который размещен:

```
для ОС Debian/Linux6 (64-bit)
C:\Program Files\S-Terra\S-Terra КР\upagent\LINUXDEBIAN6\amd64\
vpnupagent.tar

для ОС Debian/Linux6 (32-bit)
C:\Program Files\S-Terra\S-Terra КР\upagent\LINUXDEBIAN6\i686\
vpnupagent.tar

для ОС Red Hat Enterprise Linux 5
C:\Program Files\S-Terra\S-Terra
КР\upagent\LINUXRHEL5\i486\vpnupagent.tar

для ОС Solaris 10
C:\Program Files\S-Terra\S-Terra КР\
UPServer\upagent\SOLARIS\i386\vpnupagent.tar
```

Перед запуском скриптов самостоятельно доставьте архив `vpnupagent.tar` на шлюз, предварительно создав на шлюзе каталог:



```
mkdir /packages
```

Для доставки архива используйте, например, утилиту `pscp.exe` из пакета Putty:

```
pscp vpnupagent.tar root@10.0.10.110:/packages
```

И на шлюзе выполните команды:

```
cd /packages
```

```
tar xvf vpnupagent.tar
```

Запустите второй скрипт:

```
[root@cspgate ~]# /tmp/setup_product.sh
```

- При успешном выполнении скриптов установится соединение с Сервером управления для проверки возможности скачивания обновлений. Состояние клиента сначала изменится с **waiting** на **updating**.

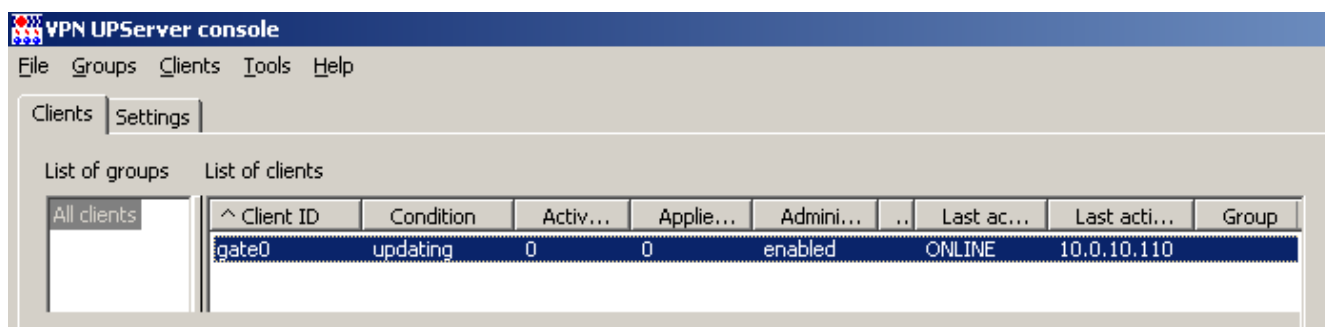


Рисунок 79

- А затем с **updating** на **active**. В состоянии **active** клиент готов для получения новых обновлений.

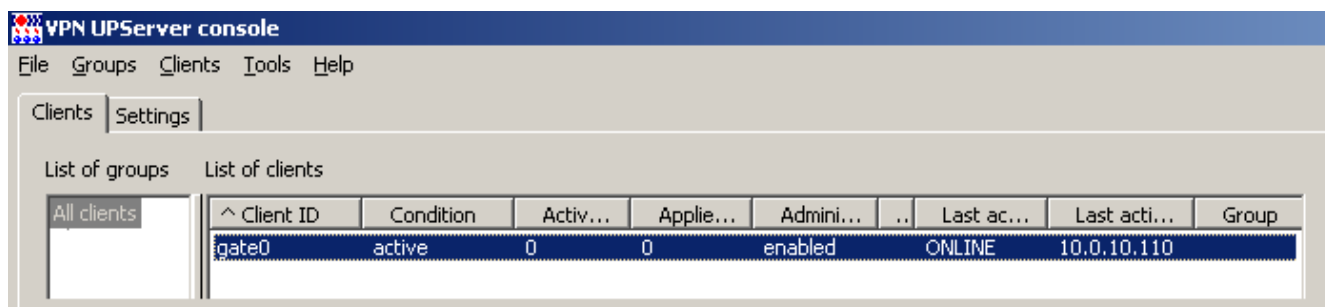


Рисунок 80

## 6. Настройка и управление устройством с Bel VPN Client 4.1

### 6.1. Создание учетной записи клиента на Сервере управления

Во вкладке **Clients** создадим группу, в ней учетную запись клиента для управляемого устройства, на котором установлен или будет установлен продукт Bel VPN Client 4.1.

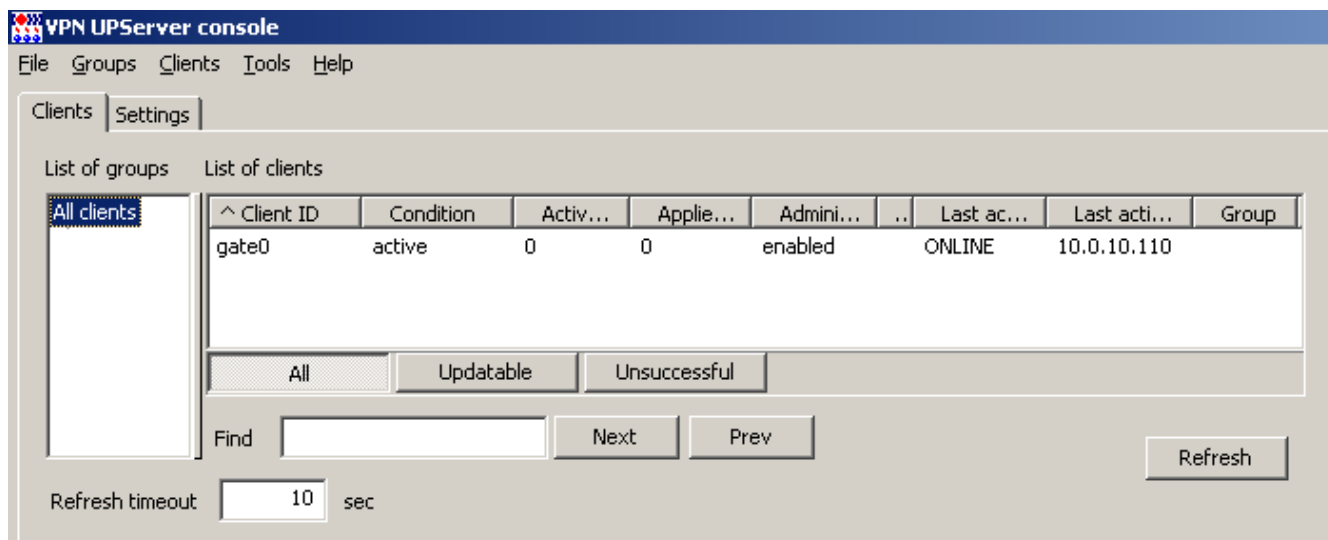


Рисунок 81

1. Для создания группы выделите группу All clients, а в меню **Groups** выберите предложение **Create** (Рисунок 82).

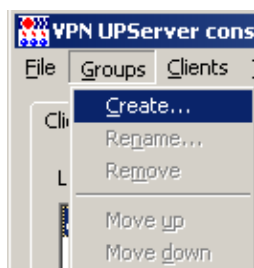


Рисунок 82

В поле **Group name** введите имя группы, например, Office1, в которой будут созданы в дальнейшем клиенты (Рисунок 83), и нажмите **OK**.

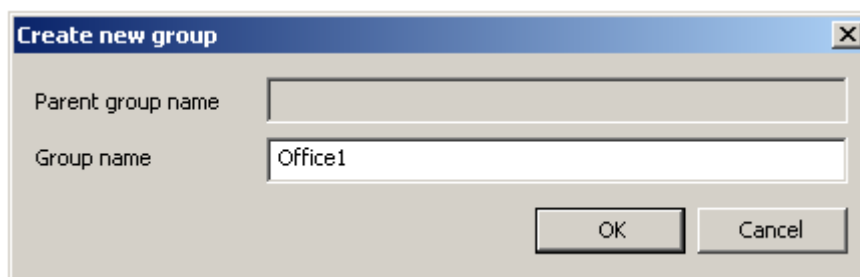


Рисунок 83

- В меню **Clients** выберите предложение **Create** (Рисунок 84).

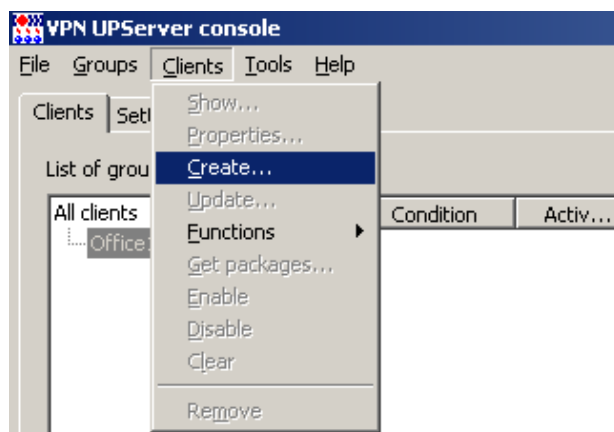


Рисунок 84

- В окне создания нового клиента **Create new client** введите идентификатор клиента, например, `client01`, а в поле **Product package** нажмите кнопку **E** (Рисунок 85).

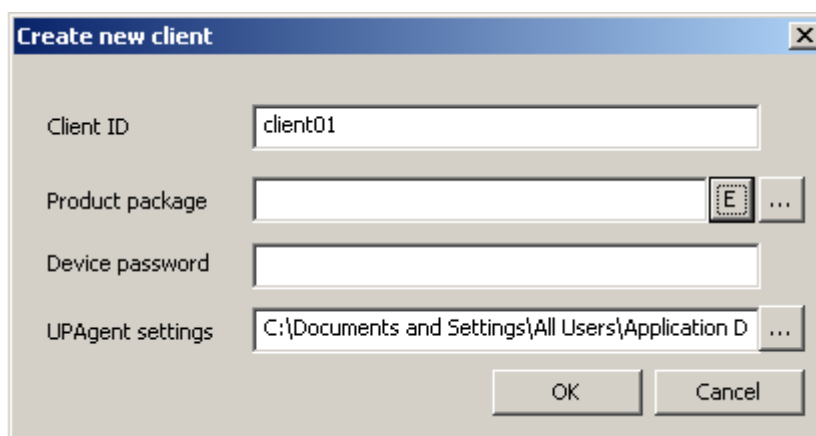


Рисунок 85

- В окне **VPN data maker** (Рисунок 86) задайте политику безопасности и все настройки продукта, например, Bel VPn Client 4.1, выбрав его в поле **VPN product**, а в поле **Crypto provider** – Avest. Политику и настройки можно ввести во вкладки или загрузить из файла, а можно воспользоваться окнами мастера, нажав кнопку [Run Wizard...](#)

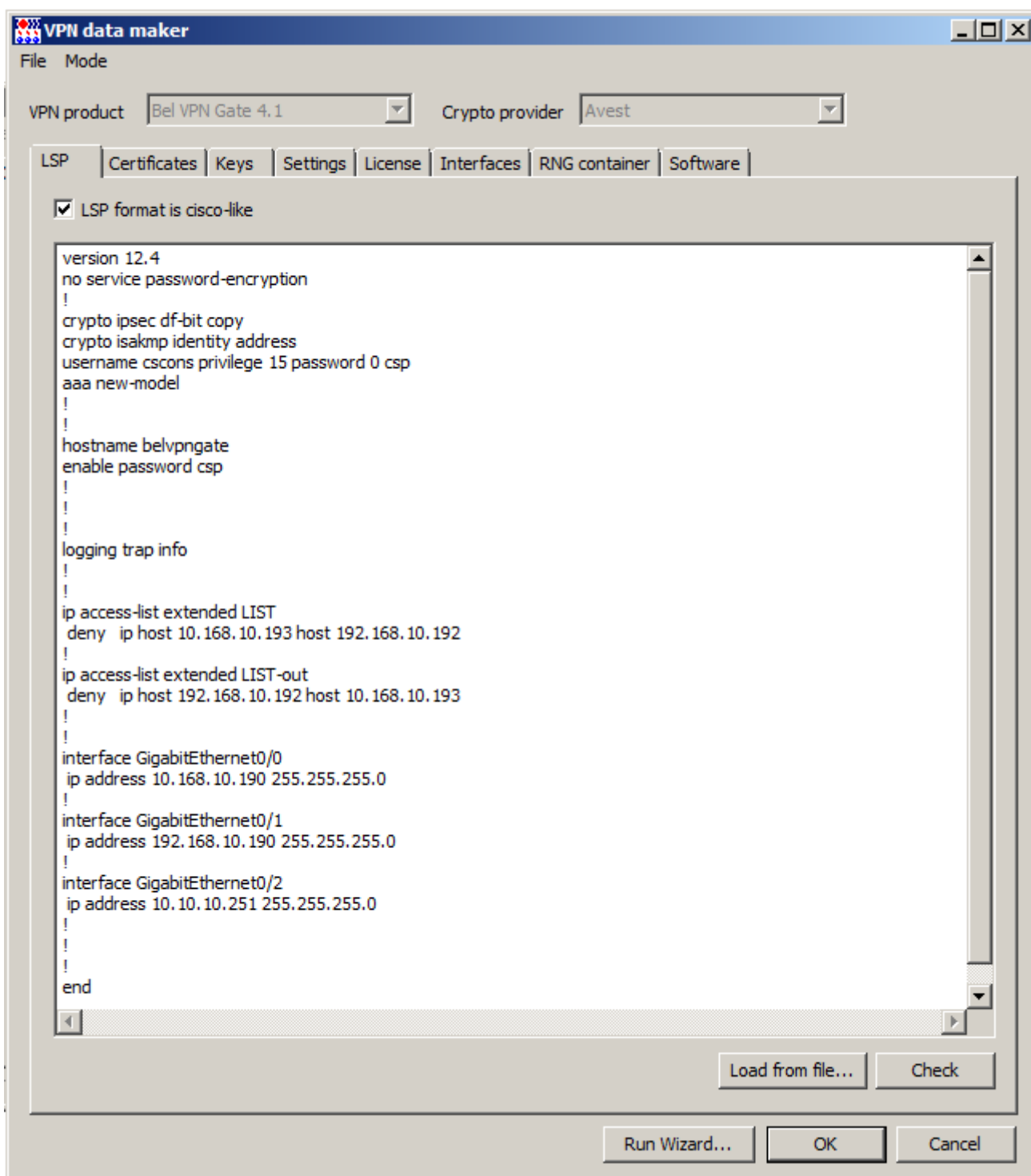


Рисунок 86

5. Выберите метод аутентификации такой же как и у партнера - шлюза Bel VPN Gate, введите такое же значение ключа (Рисунок 87), нажмите кнопку [Next](#).

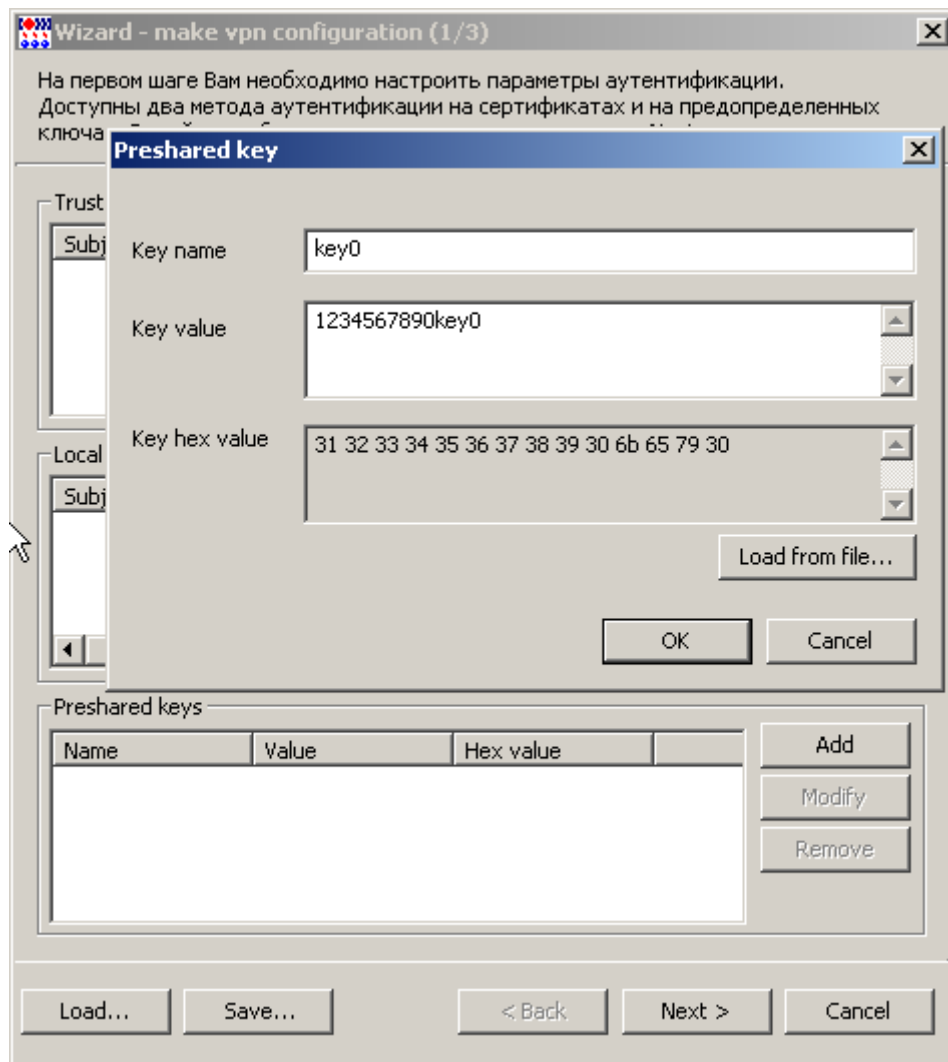


Рисунок 87

- В следующем окне задайте правило для создания соединения между устройством с установленным продуктом Bel VPN Client и Сервером управления, при этом соединение с центральным шлюзом должно быть защищенным, для этого нажмите кнопку [Add](#) (Рисунок 88).

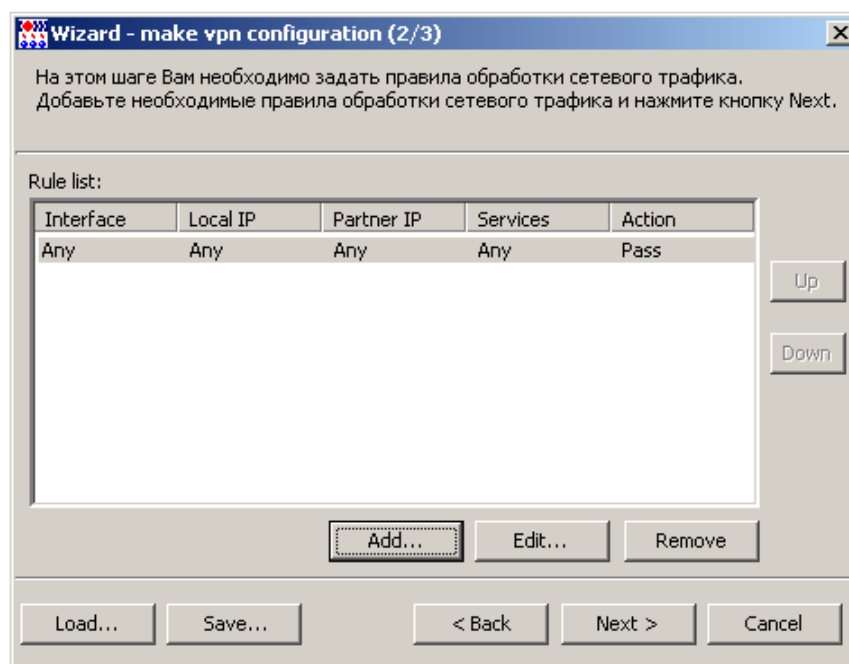


Рисунок 88.

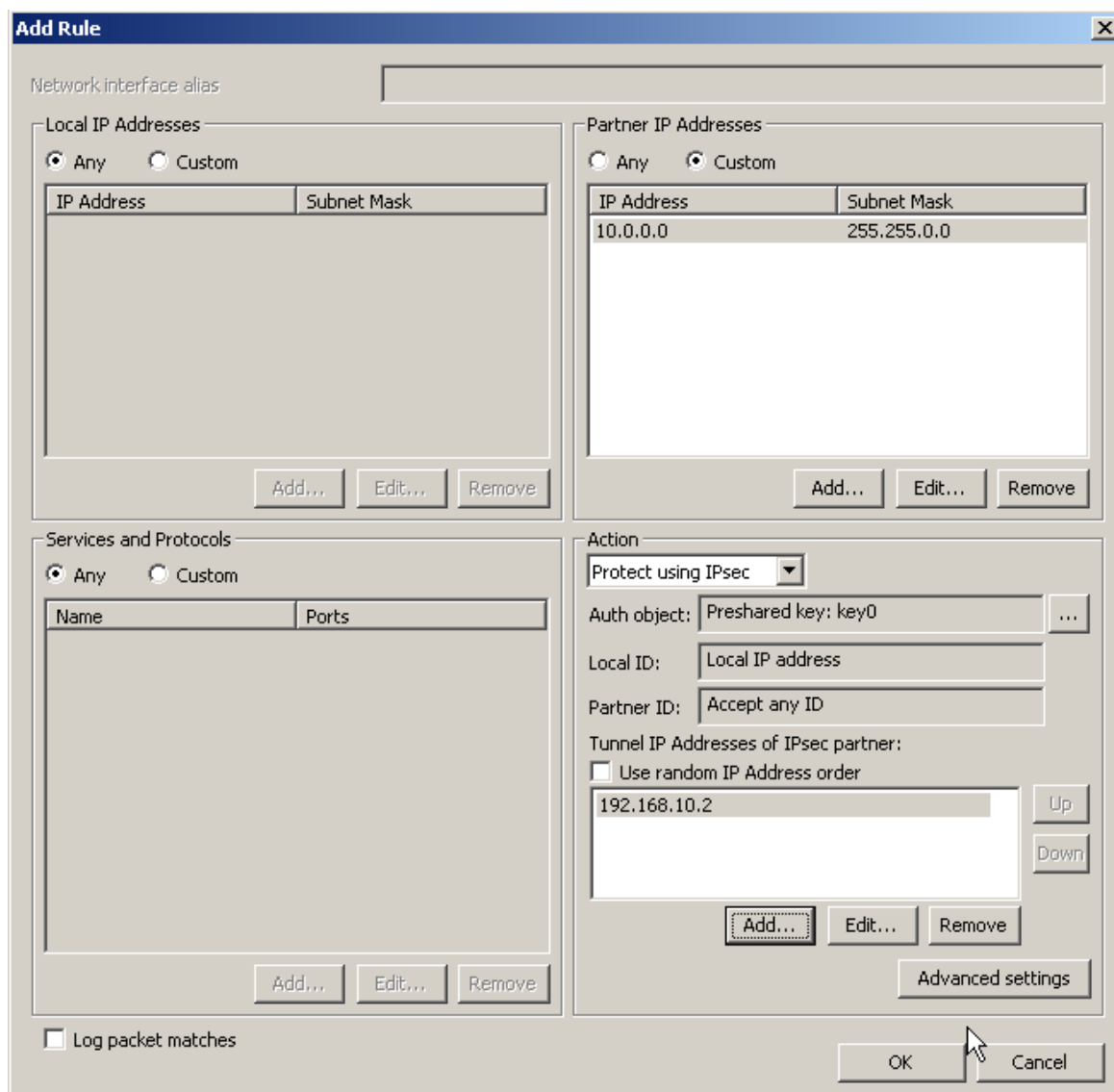


Рисунок 89

7. В поле **Network interface alias** (Рисунок 89) имя интерфейса не задается – правило будет привязано ко всем интерфейсам. В области партнера укажите всю подсеть 10.0.0.0/16 Сервера управления, в качестве адреса, до которого будет построен IPsec-туннель, задайте адрес интерфейса шлюза 192.168.10.2, защищающего подсеть с Сервером управления. Нажмите кнопку **OK**
8. Увеличьте приоритет созданного правила, используя кнопку **Up** (Рисунок 90), затем нажмите **Next**.

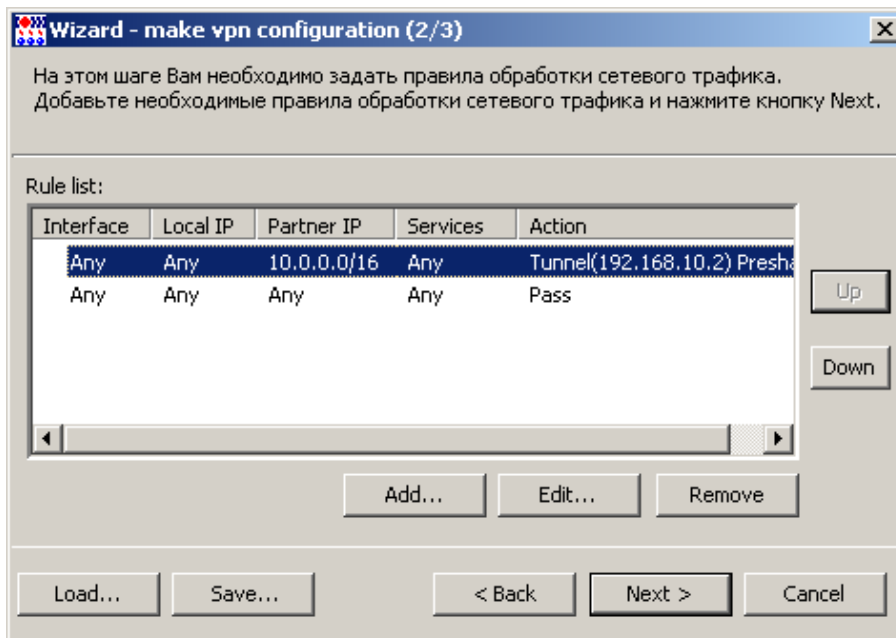


Рисунок 90

9. Введите данные лицензии на продукт Bel VPN Client 4.1 (Рисунок 91).

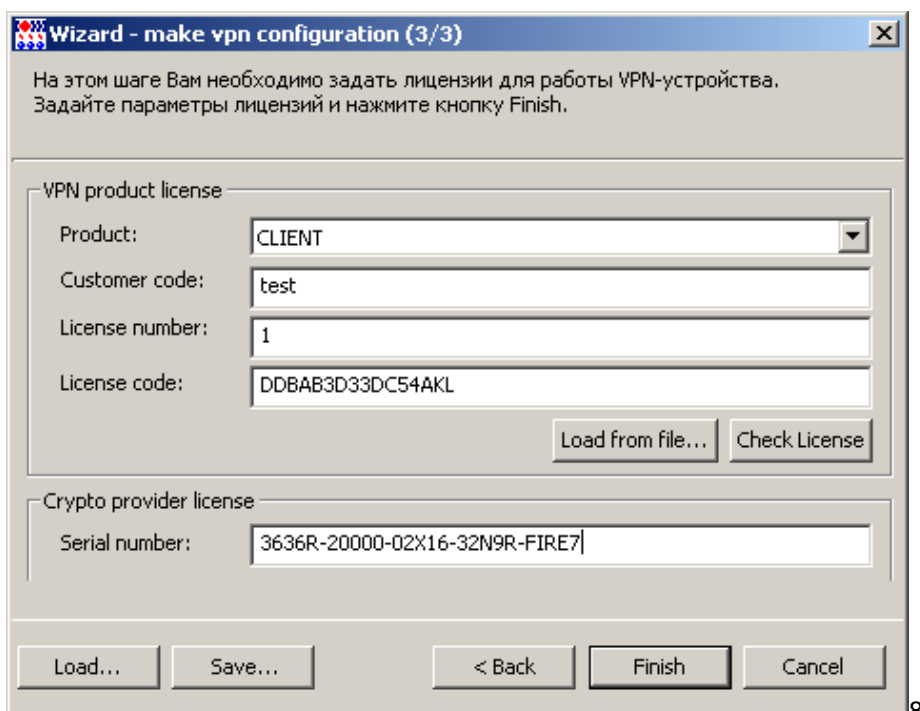


Рисунок 91

10. Сохраните все введенные данные, нажав кнопку **Save...**, и укажите имя файла-проекта в любом созданном вами каталоге (Рисунок 92).

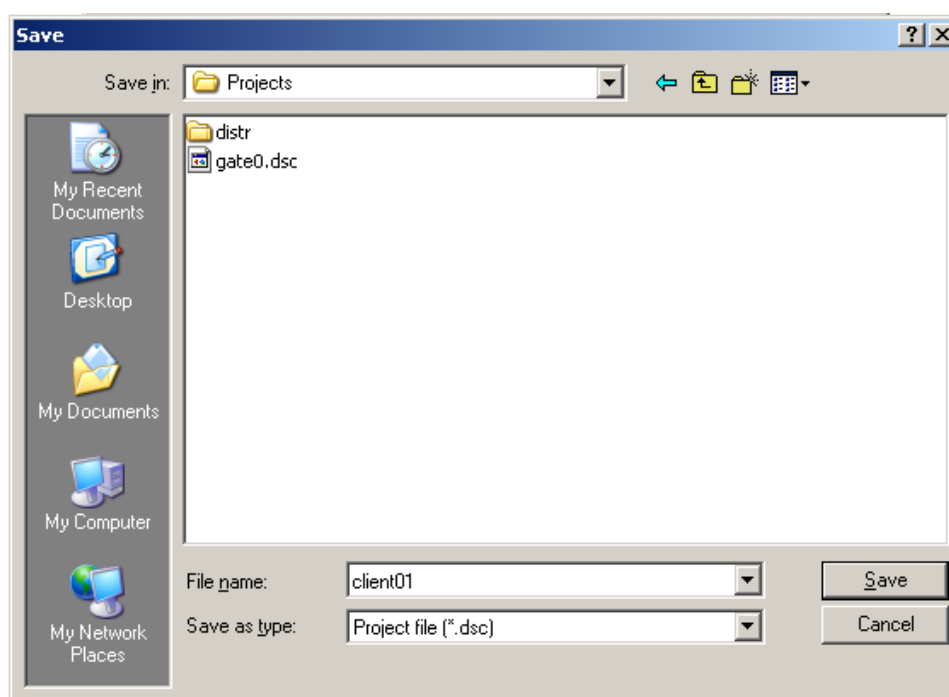


Рисунок 92

11. В окне мастера нажмите кнопку **Finish** (Рисунок 91). Все введенные данные будут отражены во вкладках проекта (Рисунок 93). Нажмите кнопку **OK**.

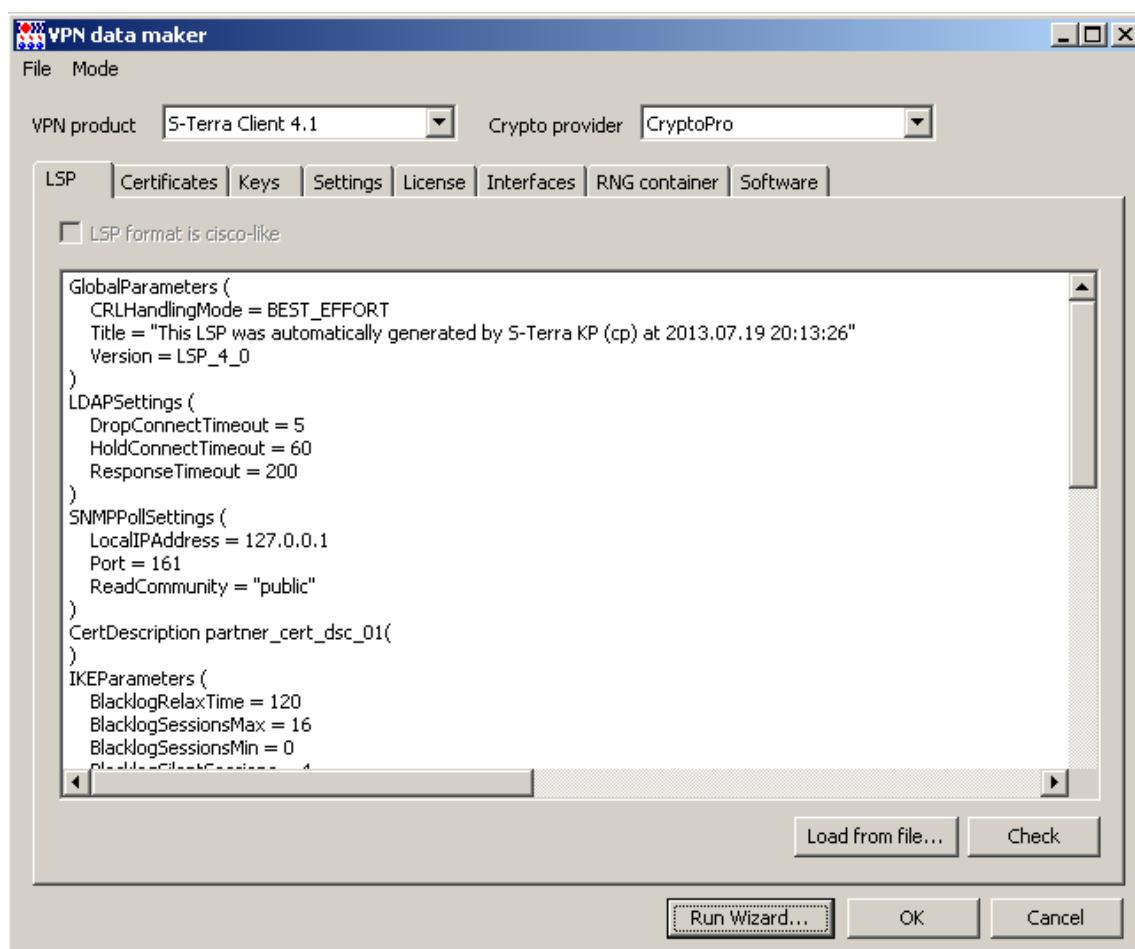


Рисунок 93



12. В окне создания нового клиента server01 также нажмите **OK** (Рисунок 94).

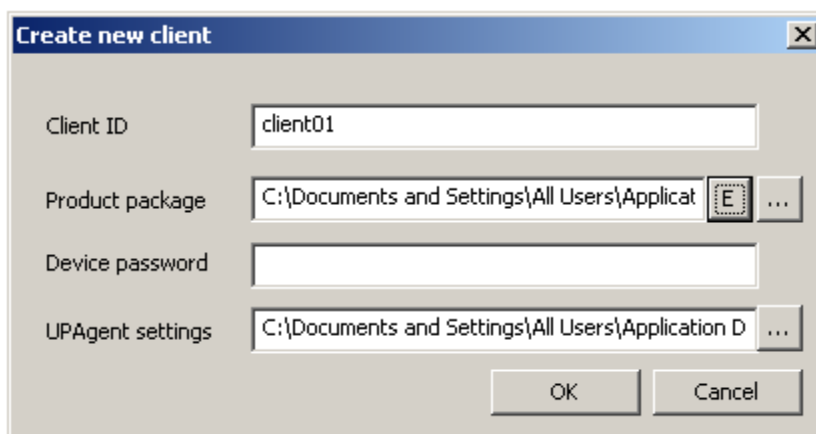


Рисунок 94

13. Созданного клиента переведите в активное состояние, выбрав в контекстном меню предложение **Enable** (Рисунок 95). Процедура **Enable** необходима для того, чтобы в момент инсталляции Клиента управления он смог связаться с Сервером управления и провести проверку возможности получения обновлений. После изменения статуса клиента на **enable**, для него будет сформировано проверочное (тестовое) обновление, и состояние клиента изменится на **waiting**.

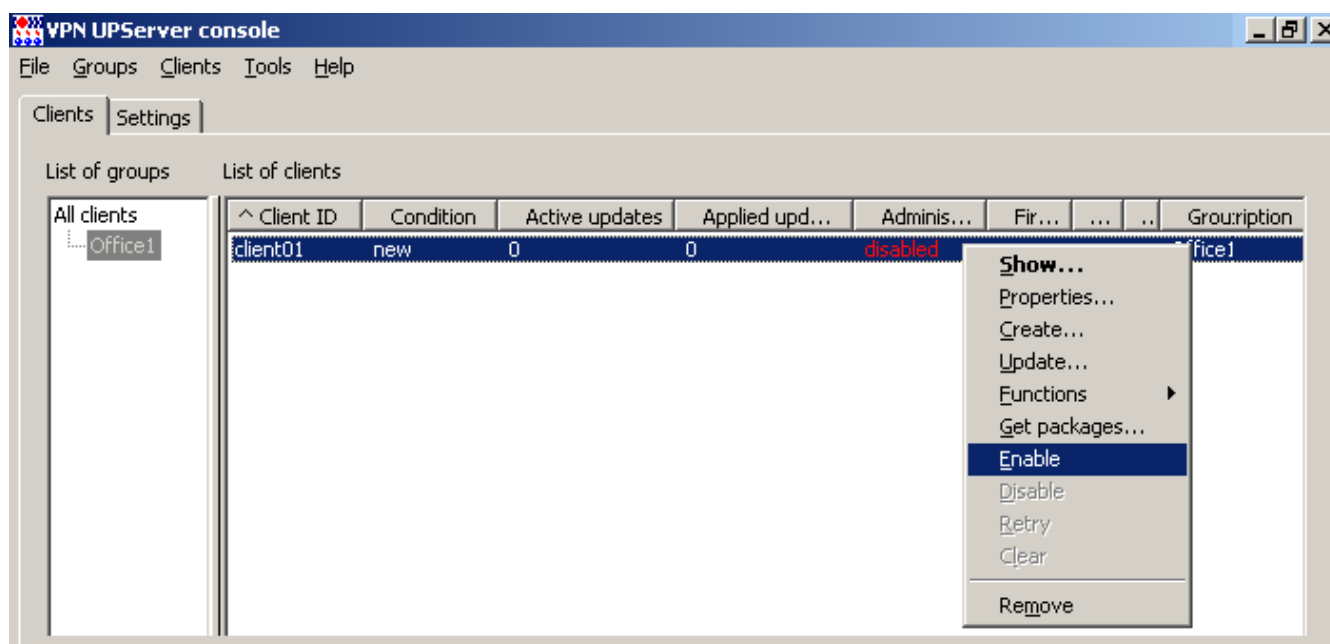


Рисунок 95

## 6.2. Создание инсталляционных файлов Клиента управления и Bel VPN Client 4.1

1. Для создания инсталляционных файлов Клиента управления и Bel VPN Client для учетной записи клиента client01 выберите предложение **Get packages** (Рисунок 96).

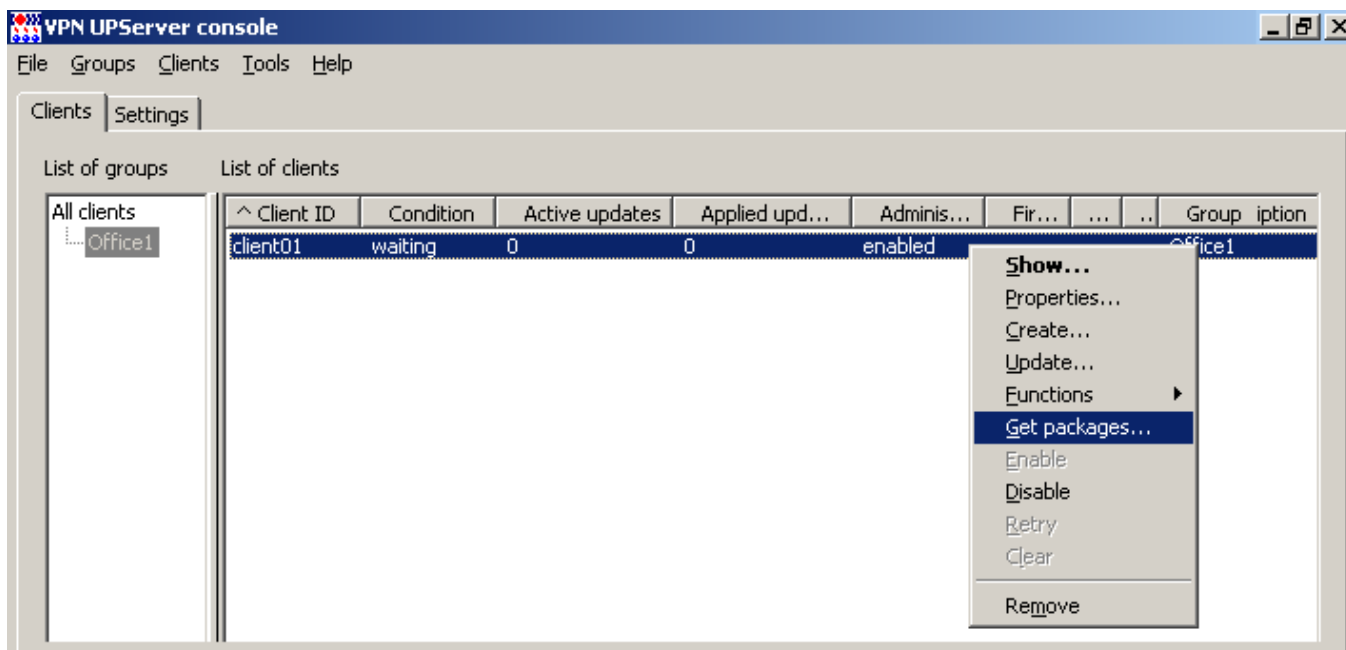


Рисунок 96

2. Укажите каталог для сохранения инсталляционных файлов (Рисунок 97) и нажмите **OK**.

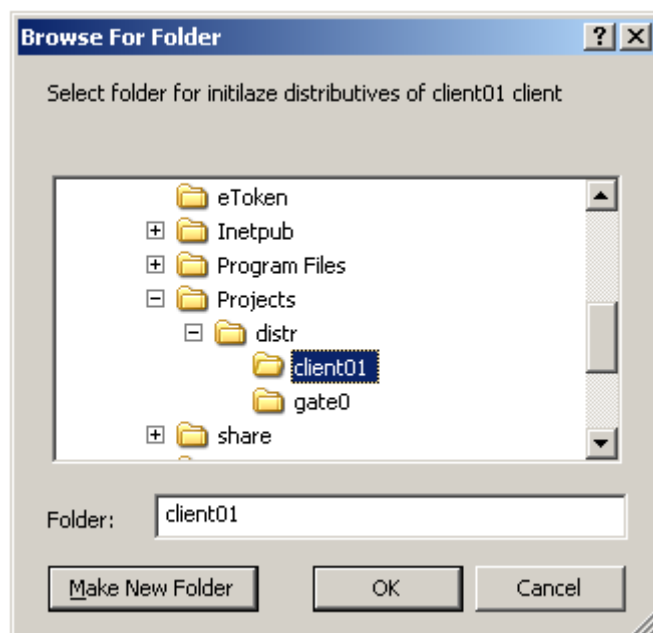


Рисунок 97

3. В указанный каталог будут сохранены два файла (Рисунок 98):  
 setup\_product.exe – инсталляционный файл Bel VPN Client 4.1  
 setup\_upagent.exe – инсталляционный файл Bel VPN KP 4.1 (Клиента управления).

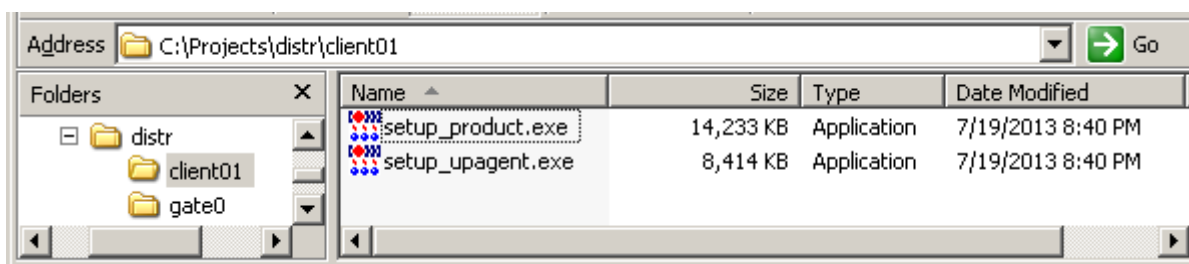


Рисунок 98

### 6.3. Установка Клиента управления и Bel VPN Client 4.1

Установка подготовленных файлов на управляемое устройство осуществляется локально. Доставьте на устройство два файла и запустите установку в следующем порядке:

- 1) `setup_product.exe`
- 2) `setup_upagent.exe`.

Если порядок изменить, то Клиент управления сразу после установки попытается выйти на связь с Сервером управления по незащищенному соединению.

1. Процесс установки продукта Bel VPN Client 4.1 описан в документе «Программный продукт «Клиент безопасности Bel VPN Client 4.1» Руководство администратора. Общее руководство». Перезагрузите операционную систему и введите пароль для доступа к продукту Bel VPN Client 4.1 (изначально установлен пустой пароль, измените его значение) (Рисунок 99).

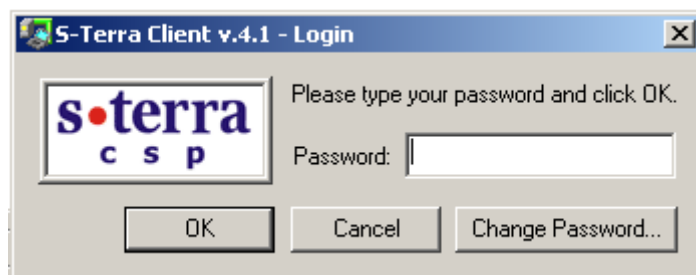


Рисунок 99

2. Установка Клиента управления (продукт Bel VPN КР 4.1) запускается программой `setup_upagent.exe`. В появившемся окне (Рисунок 100) нажмите кнопку **Да**.

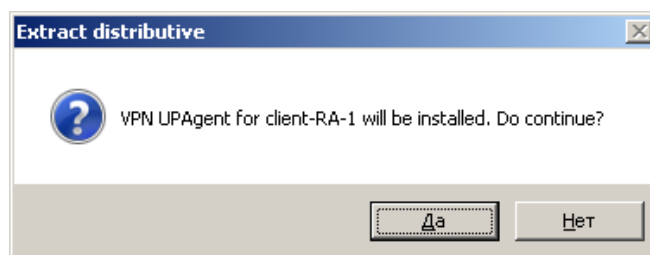


Рисунок 100

Для продолжения установки нажмите кнопку **Next**.



Рисунок 101

Выберите каталог для инсталляции Клиента управления (Рисунок 102).

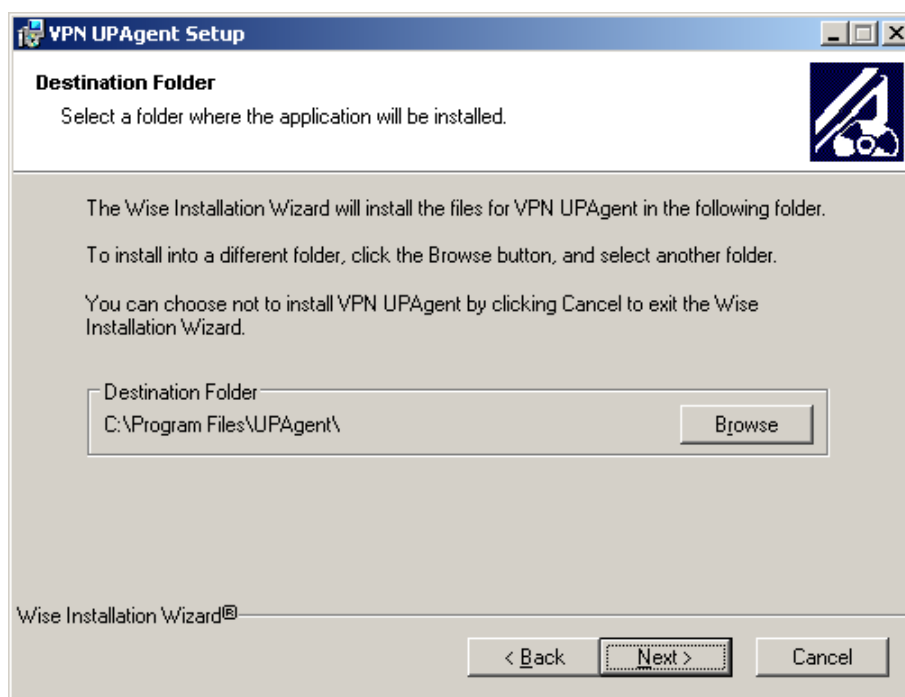


Рисунок 102

В следующем окне подтвердите готовность к установке и нажмите кнопку [Next](#).

По завершению инсталляции нажмите кнопку [Finish](#) (Рисунок 103).

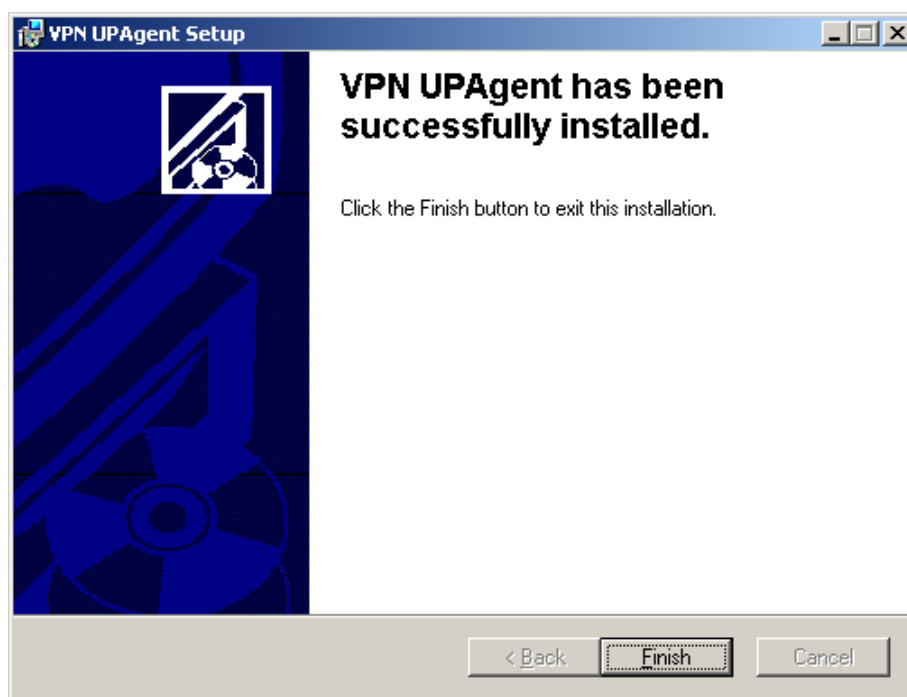


Рисунок 103

3. По завершению установки Клиент управления попытается установить связь с Сервером управления. После успешного соединения и проверки возможности получения обновлений, состояние клиента на Сервере управления изменится с **waiting** на **updating**, а затем на **active**. Это означает, что Клиент управления готов к скачиванию обновлений (Рисунок 104).

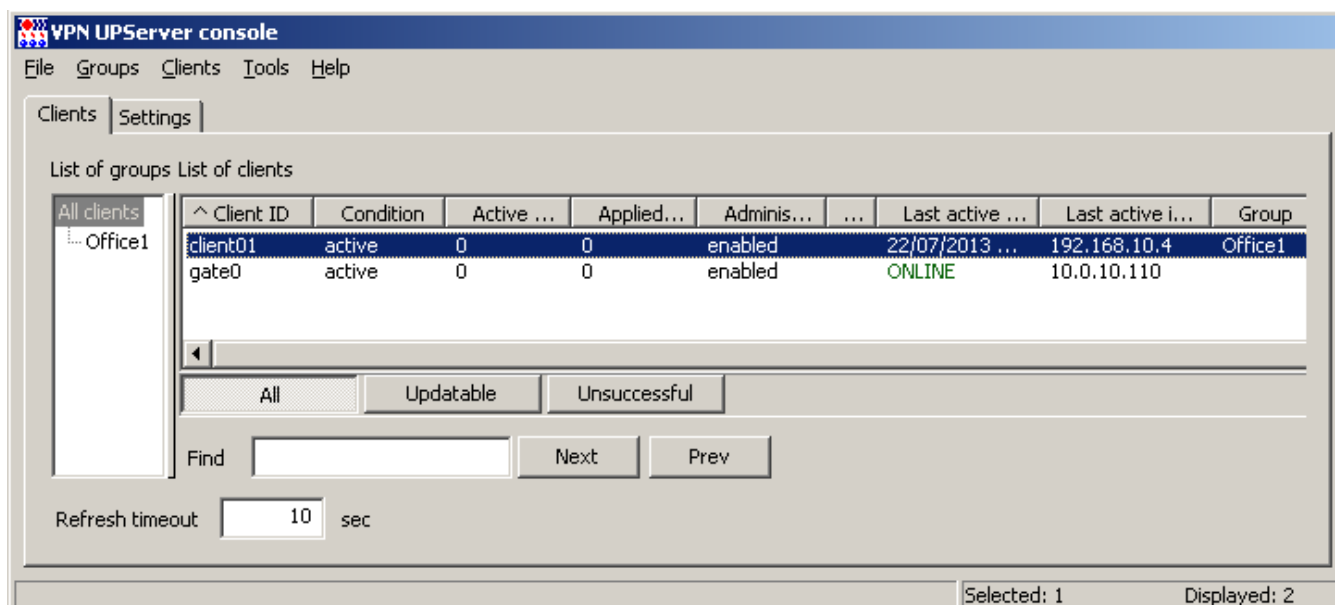


Рисунок 104

## **7. Сценарий перехода на аутентификацию с использованием сертификатов**

---

Предположим, что на управляемом устройстве установлен Клиент управления, продукты Bel VPN Client 4.1 . На центральном шлюзе также установлен Клиент управления и продукт Bel VPN Gate 4.1. Для аутентификации оба продукта используют предопределенный ключ. Требуется изменить метод аутентификации – использовать на обоих устройствах локальные сертификаты.

Сценарий перехода на аутентификацию с использованием сертификатов осуществляется в несколько этапов:

1. на Сервере управления для клиента подготовьте обновление, которое включает в себя случайную последовательность чисел, имя контейнера для ключевой пары и пароль на контейнер
2. получив обновление, на управляемом устройстве создается ключевая пара и запрос на сертификат
3. на Сервере управления появится новая информация о клиенте - создан контейнер с ключевой парой и запрос на сертификат. С Сервера управления отошлите запрос в Удостоверяющий Центр, а затем получите СА и локальный сертификат для клиента
4. на Сервере управления подготовьте обновление, включающее новый локальный сертификат, СА сертификат и отредактированную политику для данного клиента

Далее эти этапы расписаны подробно.

Для создания ключевой пары на управляемом устройстве на нем должна быть настроена возможность использовать «Исходный Материал».

## 7.1. Создание обновления с параметрами ключевой пары и запроса на сертификат

1. На Сервере управления сразу для двух устройств создайте обновления для генерации ключевой пары и запроса на сертификат на этих устройствах. Поэтому выделите в таблице строки с клиентами и выберите предложение **Functions – Key pairs – Generate** (Рисунок 105).

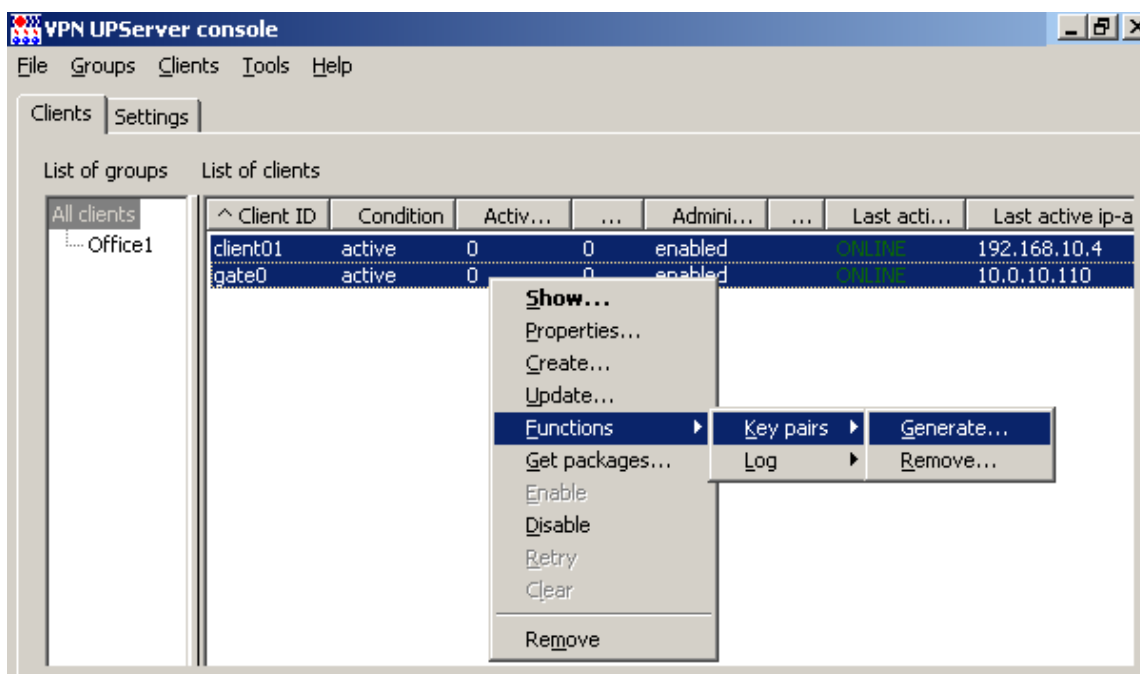


Рисунок 105

2. В открывшемся окне (Рисунок 106) заполните только два поля – задайте пароль на контейнер и его подтверждение, в который будет размещена ключевая пара для локального сертификата.

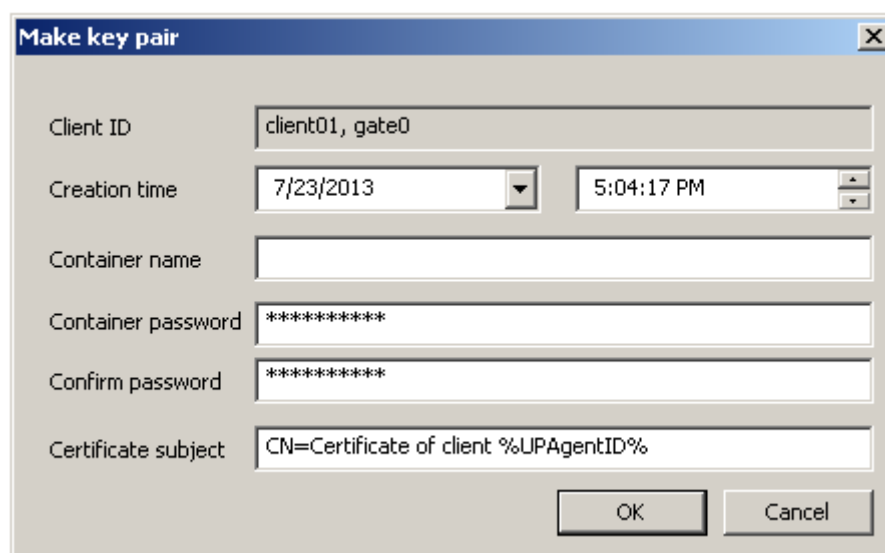


Рисунок 106

Окно **Make key pair** имеет следующие поля:

- ♦ **Creation time** – время, когда Сервер управления сделает доступным для Клиента управления обновление, содержащее необходимые данные для создания ключевой пары и запроса на сертификат

- ♦ **Container name** – имя контейнера на управляемом устройстве, в который будет записана ключевая пара. Если это поле не задано, то имя контейнера будет подобрано автоматически. При указании имени оно должно быть уникальным и включать имя считывателя, если на управляемом устройстве установлено несколько считывателей. Например,

av:AVP2050050123:Client50123.cont<sup>1</sup>

av:Gate50123.cont<sup>2</sup>

GateV4250.cont<sup>3</sup>

Client4754.cont<sup>4</sup>

- ♦ **Container password** – пароль для защиты контейнера. Если это поле не задано, то пароль для контейнера будет считаться пустым
  - ♦ **Confirm password** – поле для повторного ввода пароля. Должно совпадать со значением Container password
  - ♦ **Certificate subject** – строка, используемая в качестве поля Subject при создании запроса на сертификат. В этой строке можно использовать макросы, такие как %UPAgentID%, %UPAgentGroup% и т.п., которые будут заменены на их значения (список макросов, которые можно использовать, совпадает с переменными, передаваемыми в файл cook.bat при его запуске).
3. При нажатии кнопки **OK** предлагается выполнить «биологическую» инициализацию ДСЧ – нажимайте клавиши или перемещайте указатель мыши (Рисунок 107). Если на Сервере управления установлен аппаратный ДСЧ, то данное окно не выводится.

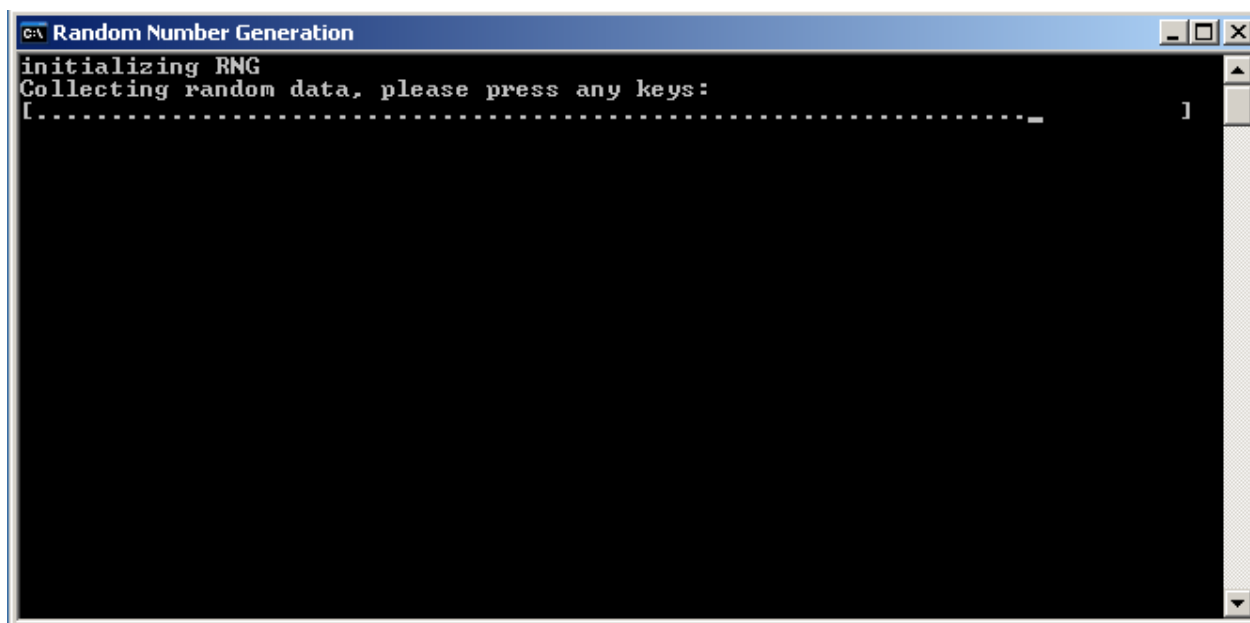


Рисунок 107

<sup>1</sup> Формат записи названия контейнера для ПАУ Bel VPN Client 4.1 с ключевым носителем

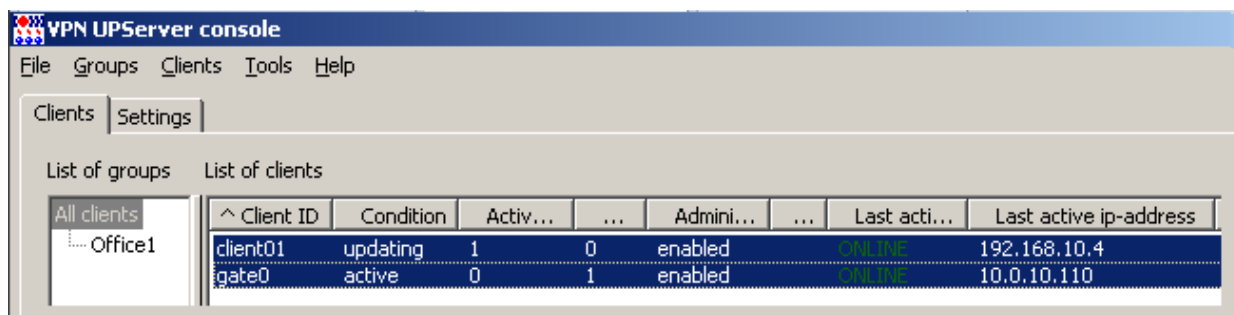
<sup>2</sup> Формат записи названия контейнера для ПАК Bel VPN Gate 4.1 с ключевым носителем

<sup>3</sup> Формат записи названия контейнера для ПК Bel VPN Gate-V 4.1 без ключевого носителя

<sup>4</sup> Формат записи названия контейнера для ПП Bel VPN Client 4.1 без ключевого носителя



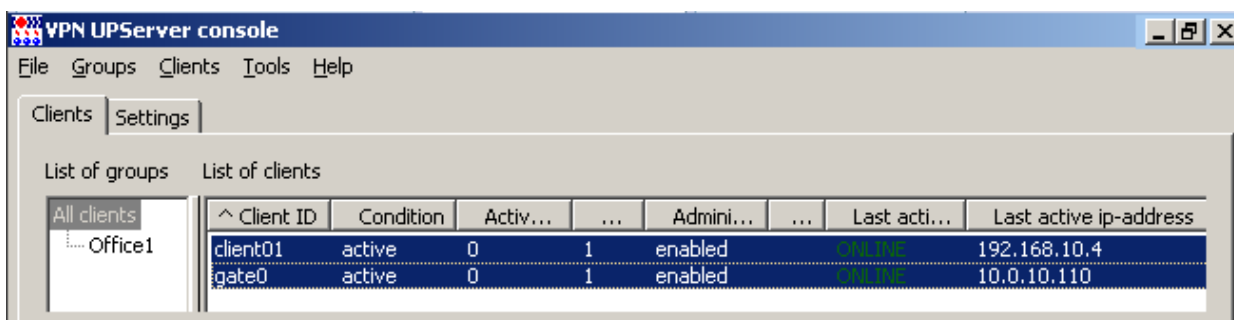
4. После этого в таблице появятся новые обновления с параметрами ключевых пар и контейнеров для данных клиентов (Рисунок 108). Количество активных обновлений (столбец Active updates) увеличится на единицу.



Client ID	Condition	Activ...	...	Admini...	...	Last acti...	Last active ip-address
client01	updating	1	0	enabled		...	192.168.10.4
gate0	active	0	1	enabled		...	10.0.10.110

Рисунок 108

5. На устройстве с установленным Bel VPN Gate 4.1 обновление применяется автоматически. На устройстве с установленным Bel VPN Client 4.1 запрашивается разрешение на применение обновления, для этого посмотрите раздел [«Действия администратора при обновлении»](#) и на устройстве с Bel VPN Client 4.1 дважды кликните мышкой на иконке в трее задач с запросом разрешения, в открывшемся окне нажмите кнопку [Применить](#). Через некоторое время обновления будут применены на устройствах, что отразится в таблице на Сервере управления (Рисунок 109). Количество успешных примененных обновлений увеличится на единицу, а количество готовых к скачиванию - уменьшится на единицу.



Client ID	Condition	Activ...	...	Admini...	...	Last acti...	Last active ip-address
client01	active	0	1	enabled		...	192.168.10.4
gate0	active	0	1	enabled		...	10.0.10.110

Рисунок 109

## 7.2. Создание на клиенте ключевой пары и запроса на сертификат

В результате на каждом устройстве будет создан контейнер с ключевой парой и запрос на сертификат, которые можно увидеть на Сервере управления. Для выделенного клиента в контекстном меню выберите предложение **Show** (Рисунок 110).

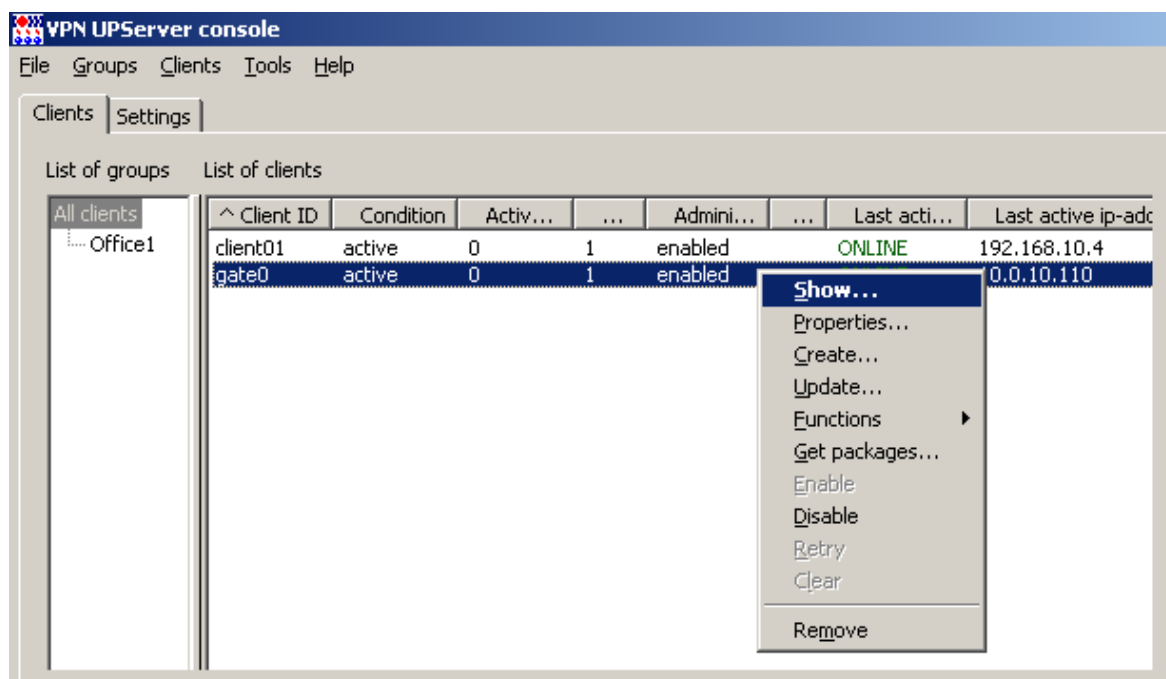


Рисунок 110

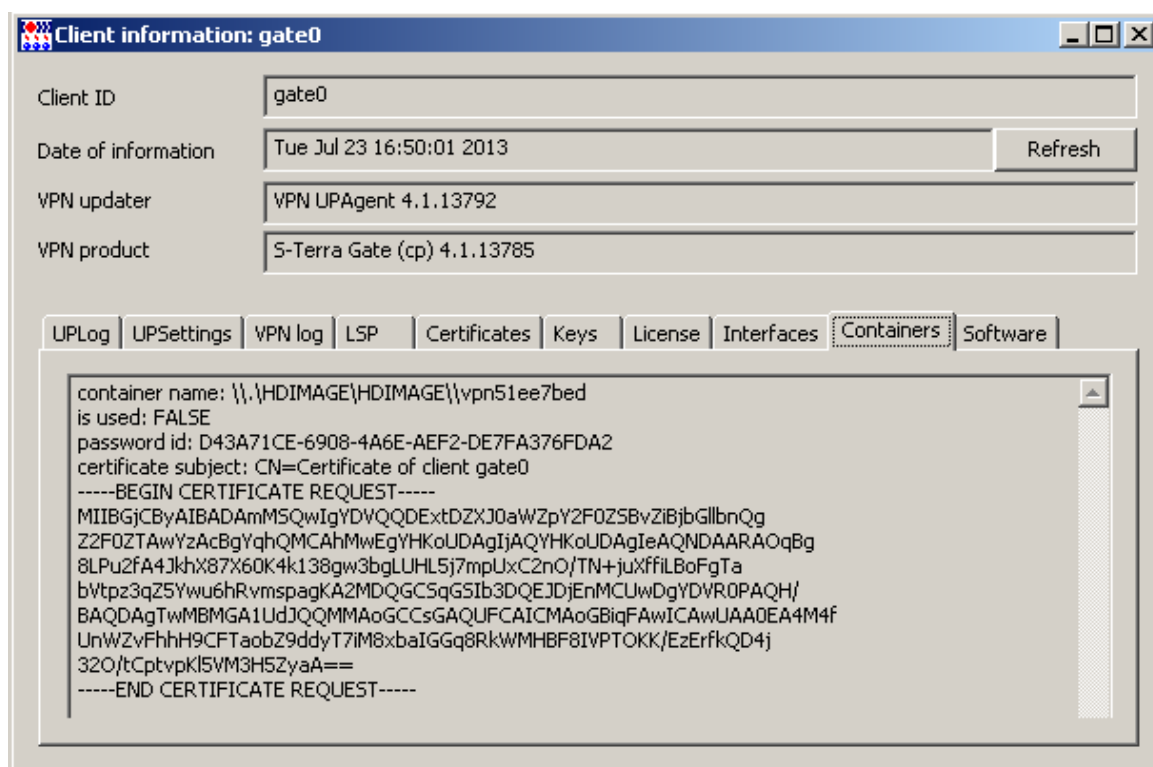


Рисунок 111

Во вкладке **Containers** для gate0 появилась запись о созданном контейнере и запросе на сертификат (Рисунок 111):

- **container name** – имя созданного контейнера на жестком диске
- **is used: FALSE** – признак того, что контейнер еще не используется продуктом Bel VPN Gate 4.1, так как сертификат не создан
- **password id** – уникальный идентификатор пароля к контейнеру
- **certificate subject** – строка, которая использовалась в качестве поля Subject при создании запроса на сертификат
- тело запроса на сертификат.

### 7.3. Получение сертификата по запросу

Для получения сертификата открытого ключа по сформированному запросу необходимо:

1. Скопировать текстовое представление запроса (формат base64) из вкладки **Containers**, сохранить в текстовый файл.
2. Сформировать карточку открытого ключа, убедиться, что данные об организации и устройстве в запросе указаны верно.
3. Отправить в Удостоверяющий центр текстовый файл с запросом и карточку открытого ключа (если требуется по регламенту Удостоверяющего центра).

### 7.4. Создание обновления с новым сертификатом для шлюза

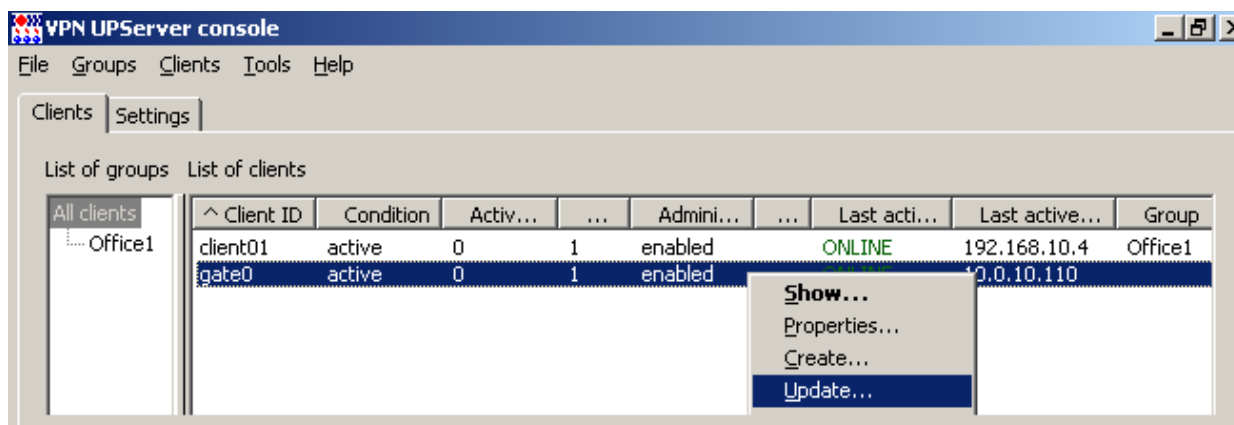


Рисунок 112

1. На Сервере управления в контекстном меню выберите предложение **Update** (Рисунок 112).
2. В открывшемся окне **Update client** нажмите кнопку **E** (Рисунок 113).

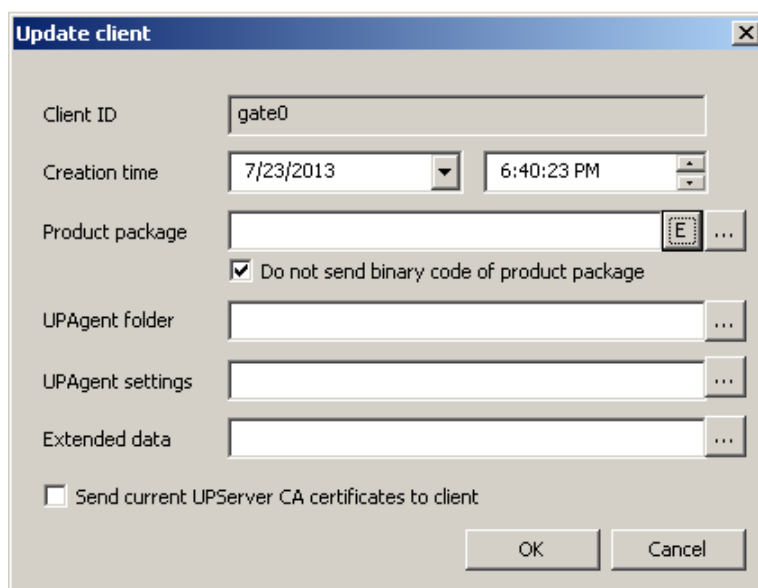


Рисунок 113

3. В окне **VPN data maker** (Рисунок 114) перейдите в окна мастера для редактирования настроек Bel VPN Gate 4.1, нажав кнопку [Run Wizard](#).

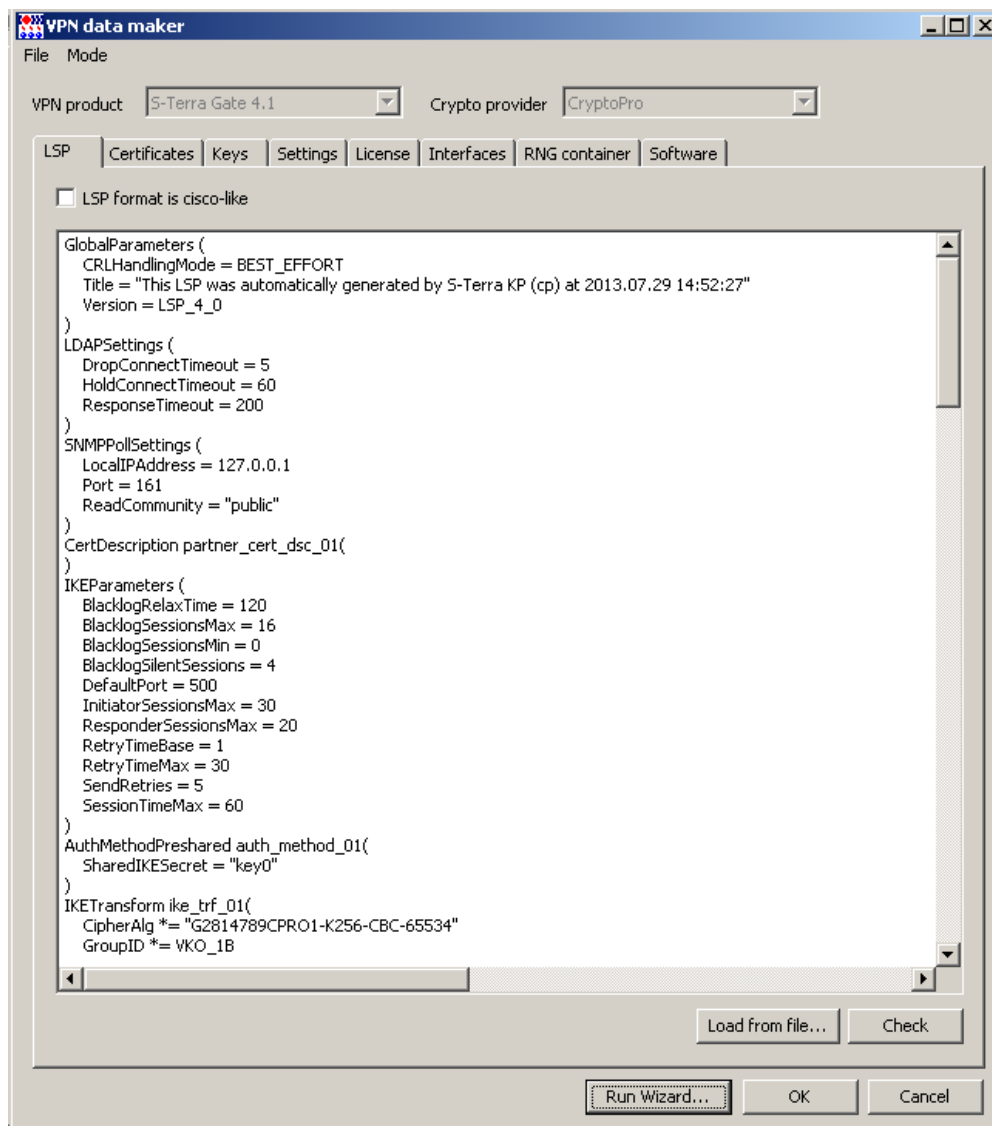


Рисунок 114

4. В открывшемся окне добавьте CA сертификат, которым были подписаны сертификаты для client01 и gate01, и локальный сертификат для gate0 (Рисунок 115). Нажмите кнопку [Next](#).

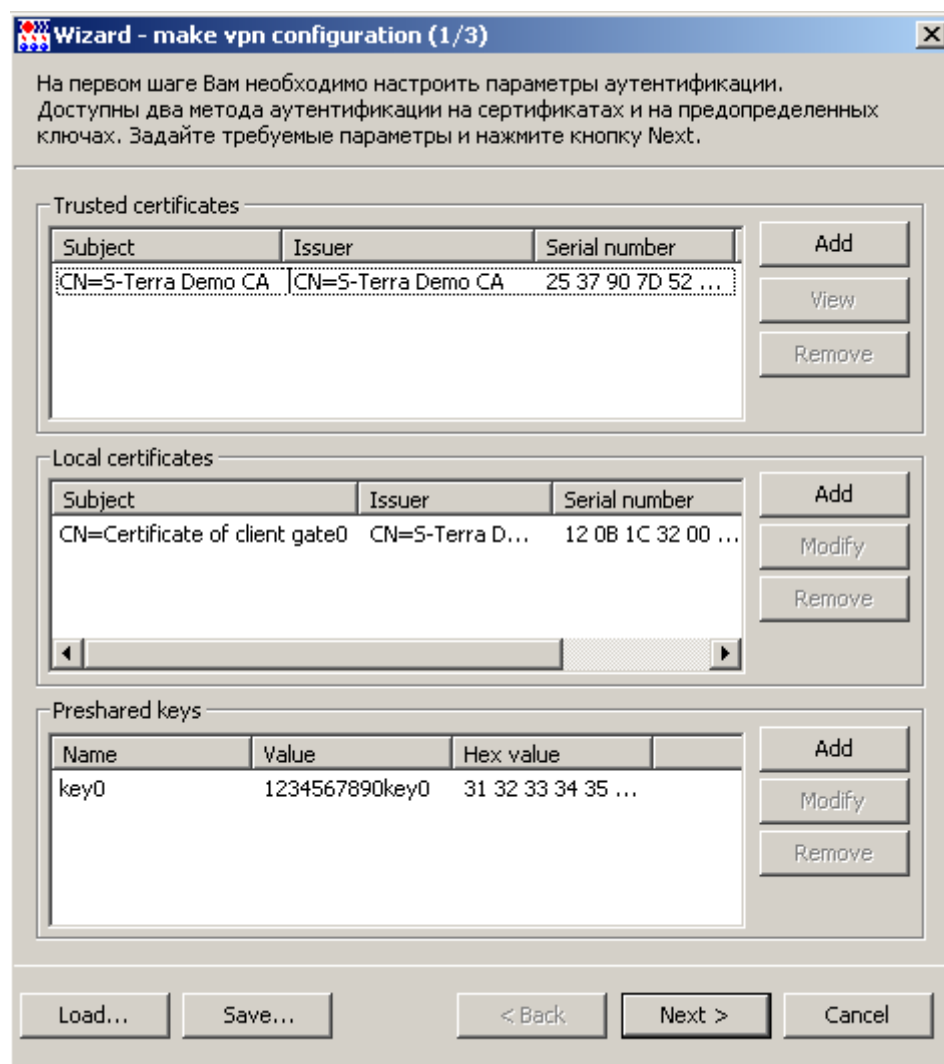


Рисунок 115

5. Для добавления нового правила нажмите кнопку [Add](#) (Рисунок 116).

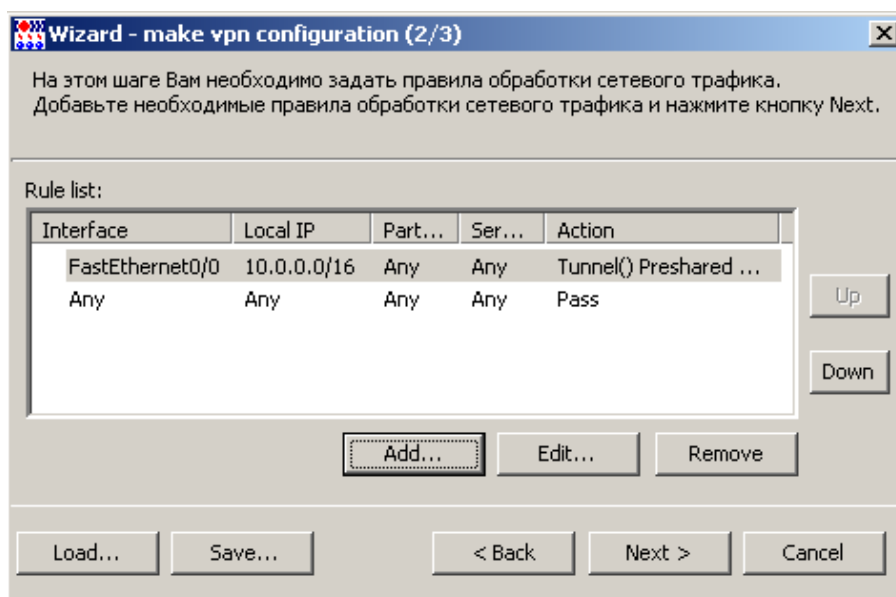


Рисунок 116

6. Новое правило нужно привязать к интерфейсу с псевдонимом FastEthernet0/0, который обращен во внешнюю подсеть (в нашей схеме это интерфейс с адресом 192.168.10.2). В разделе **Local IP Addresses** укажите всю внутреннюю подсеть 10.0.0.0/16, в разделе **Partner IP Addresses** – значение Any, партнер может быть с любым адресом. В разделе **Action** – соединение с партнером должно быть защищено, строится IPsec туннель, для аутентификации устройства используется локальный сертификат, в качестве идентификатора gate0 используется поле DistinguishedName локального сертификата, у партнера идентификатор может быть любым. Нажмите кнопку **OK** (Рисунок 117).

**Add Rule**

Network interface alias: FastEthernet0/0

**Local IP Addresses**

☐ Any ☒ Custom

IP Address	Subnet Mask
10.0.0.0	255.255.0.0

Add... Edit... Remove

**Partner IP Addresses**

☒ Any ☐ Custom

IP Address	Subnet Mask
------------	-------------

Add... Edit... Remove

**Services and Protocols**

☒ Any ☐ Custom

Name	Ports
------	-------

Add... Edit... Remove

**Action**

Protect using IPsec

Auth object: Certificate: CN=Certificate of client gate

Local ID: DistinguishedName: CN=Certificate of cl

Partner ID: Accept any ID

Tunnel IP Addresses of IPsec partner:

☐ Use random IP Address order

Up Down

Add... Edit... Remove

Advanced settings

☐ Log packet matches

OK Cancel

Рисунок 117

7. На открывшемся предупреждении нажмите кнопку **Yes** (Рисунок 118).

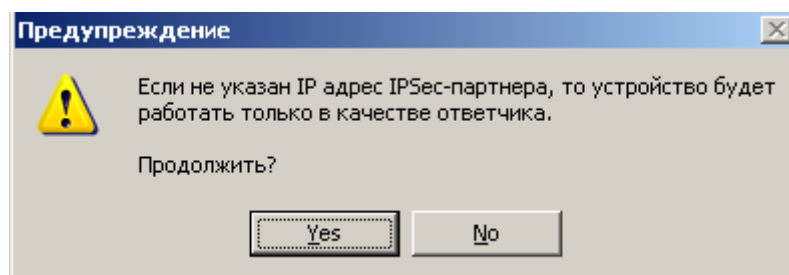


Рисунок 118

8. Созданному правилу увеличьте приоритет, используя кнопку **Up** (Рисунок 119). После этого нажмите кнопку **Next**.

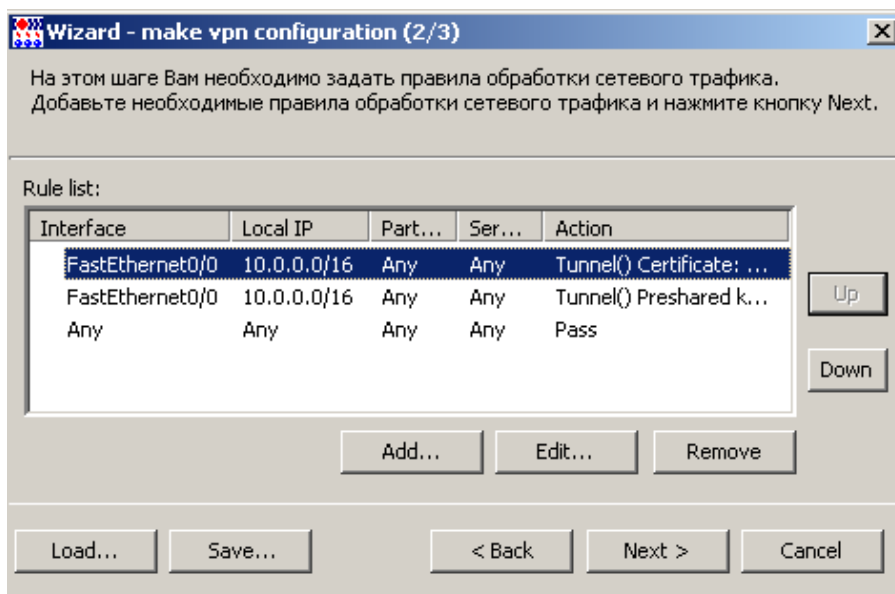


Рисунок 119

9. Лицензионные данные оставьте без изменений, нажмите кнопку **Finish** (Рисунок 120).

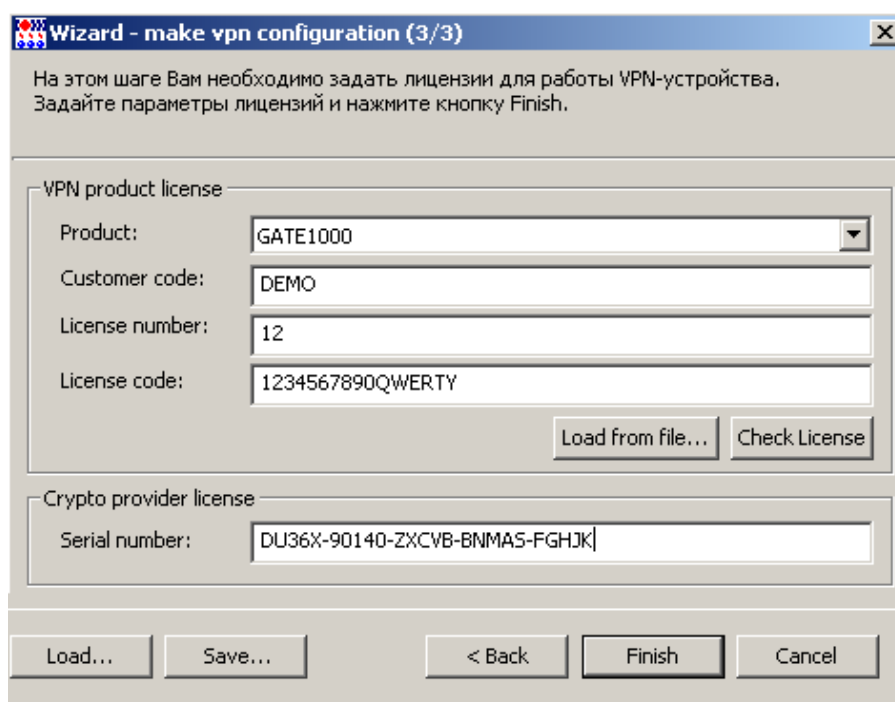


Рисунок 120

10. Все введенные данные размещены мастером во вкладках проекта, нажмите кнопку **OK** (Рисунок 121).

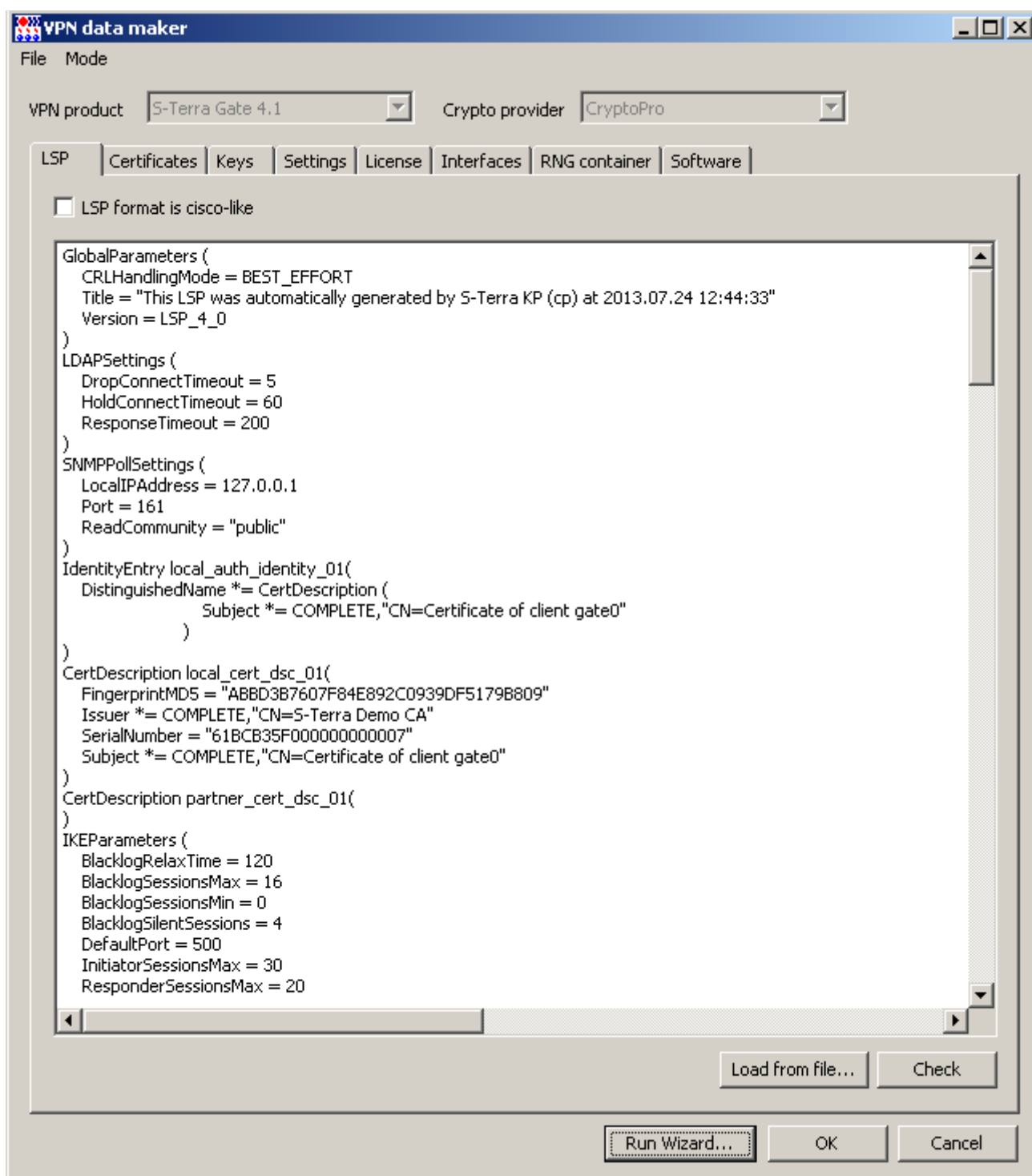


Рисунок 121



11. В окне создания обновления нажмите кнопку **OK** (Рисунок 122).

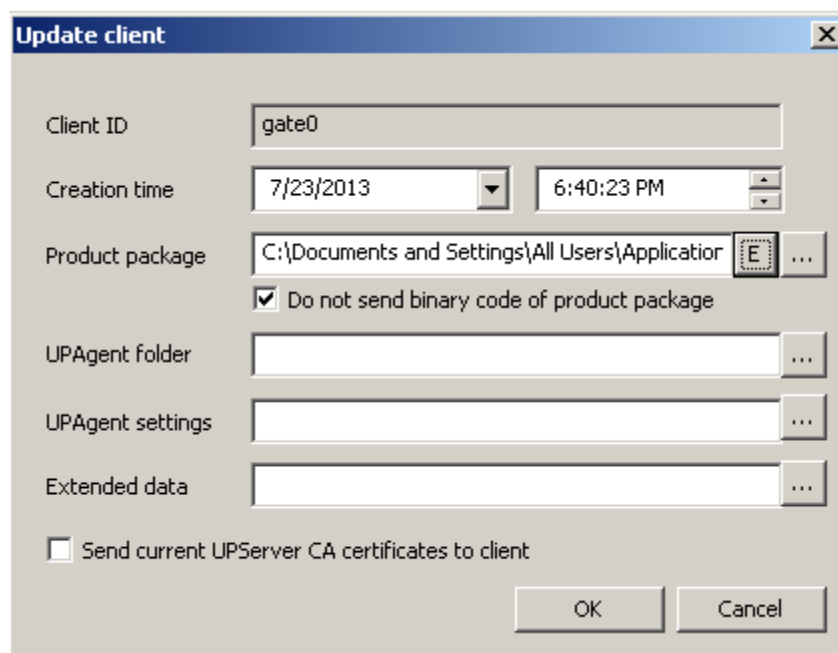


Рисунок 122

12. Обновление для gate0 с использованием локального сертификата для аутентификации создано (Рисунок 123).

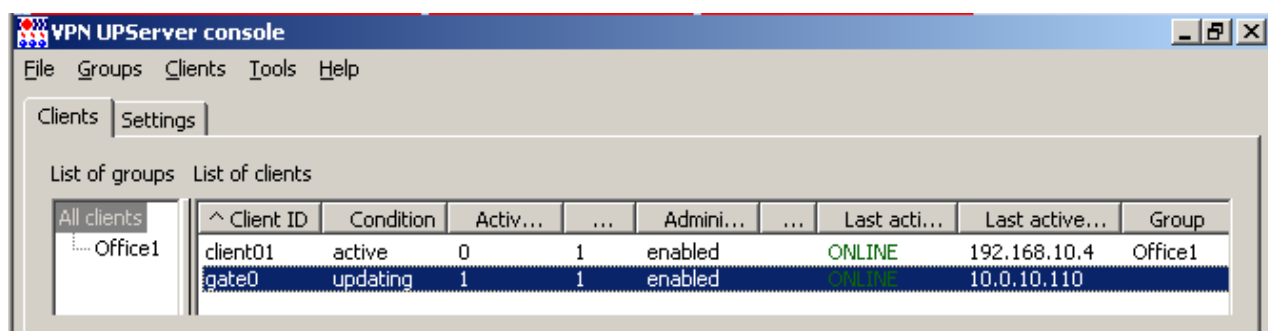


Рисунок 123

13. После того как центральный шлюз скачает подготовленное обновление и применит его, на Сервере управления можно посмотреть вкладку **Certificates**, выбрав в контекстном меню предложение **Show**, – CA и локальный сертификаты зарегистрированы в продукте и используются (Рисунок 124).

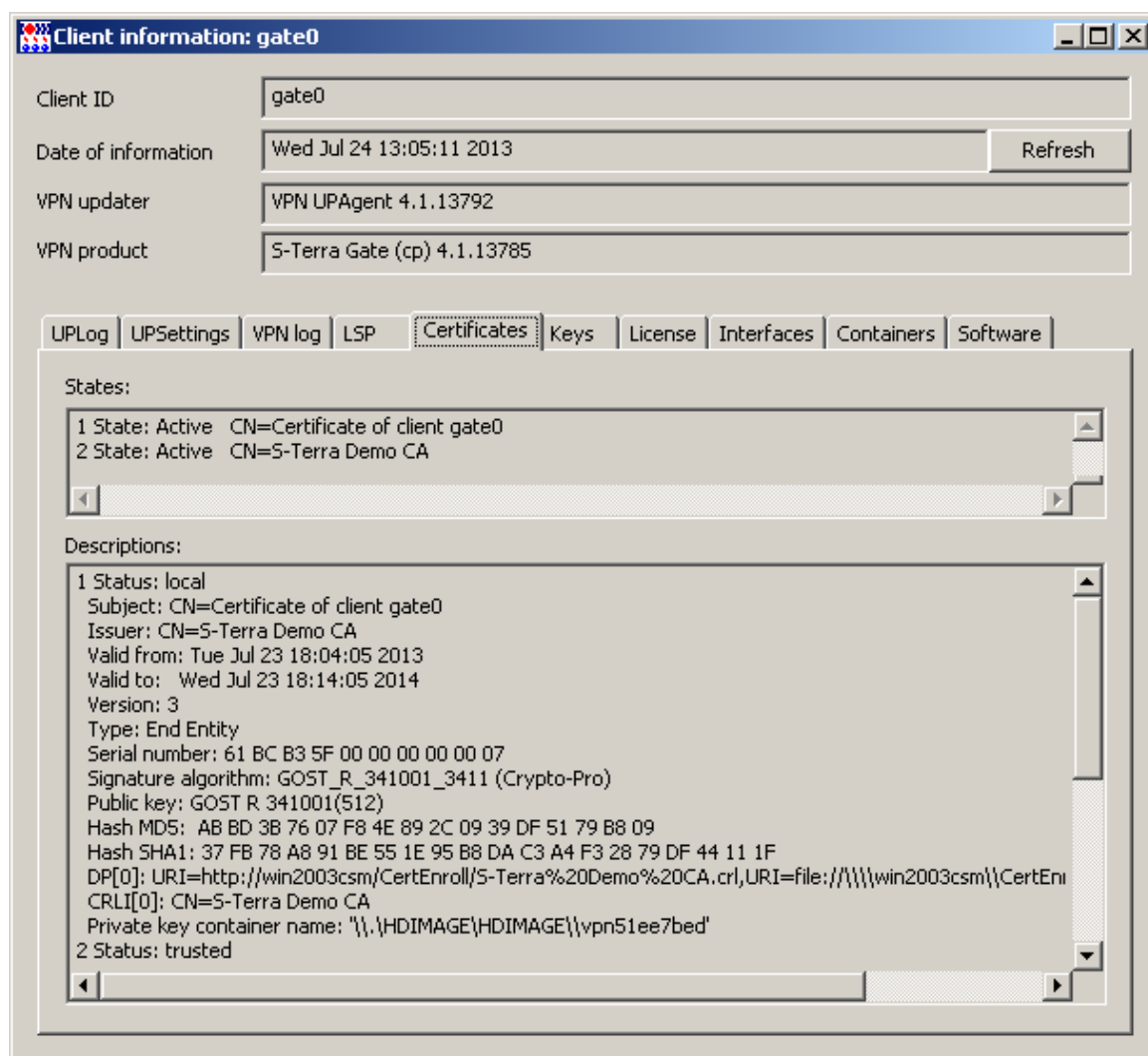


Рисунок 124

14. Во вкладке **Containers** видно, что на центральном шлюзе используется контейнер с ключевой парой локального сертификата – `is used: TRUE`.

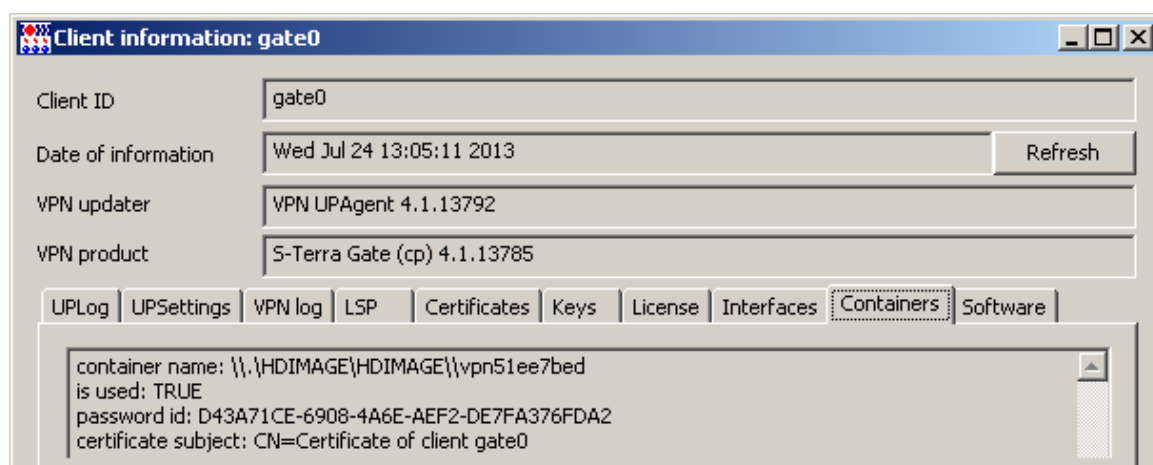


Рисунок 125

## 7.5. Создание обновления с новым сертификатом для устройства с клиентом



Note

Обратите внимание, что на момент замены сертификата на клиенте с Bel VPN Gate/Client 4.1, его партнеры уже должны быть настроены на работу с новым сертификатом на Bel VPN Gate/Client 4.1.

1. Создание обновления для устройства с клиентом выполняется также как и для центрального шлюза – в контекстном меню выберите предложение **Update** (Рисунок 126).

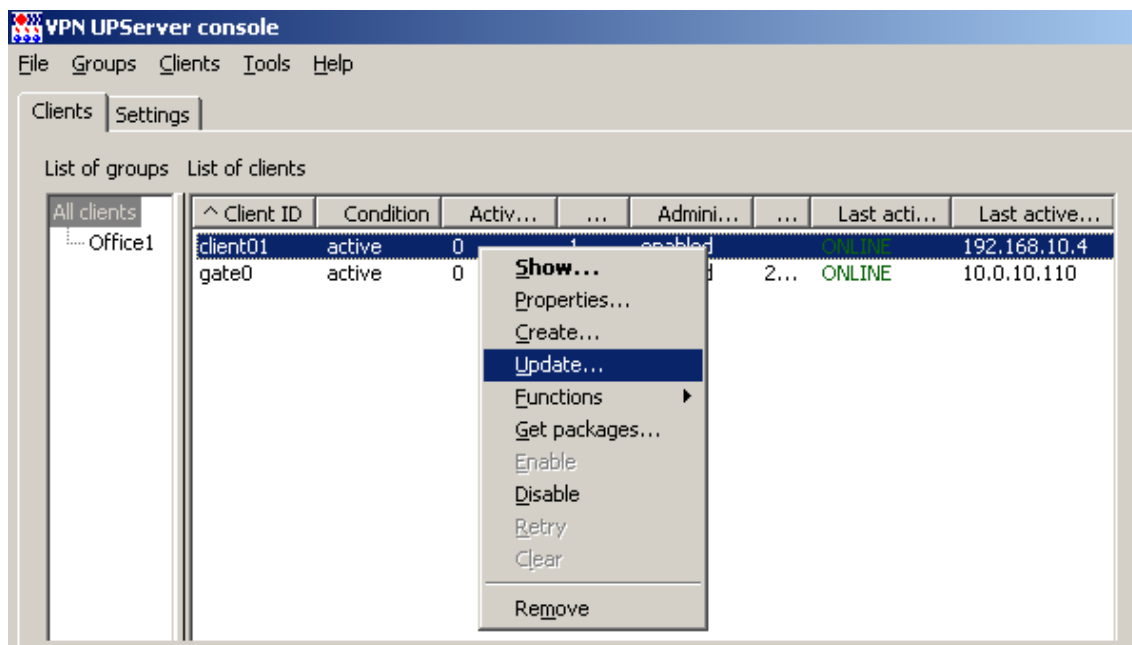


Рисунок 126

2. В следующем окне нажмите кнопку **E** для вызова окна для ввода данных (Рисунок 127).

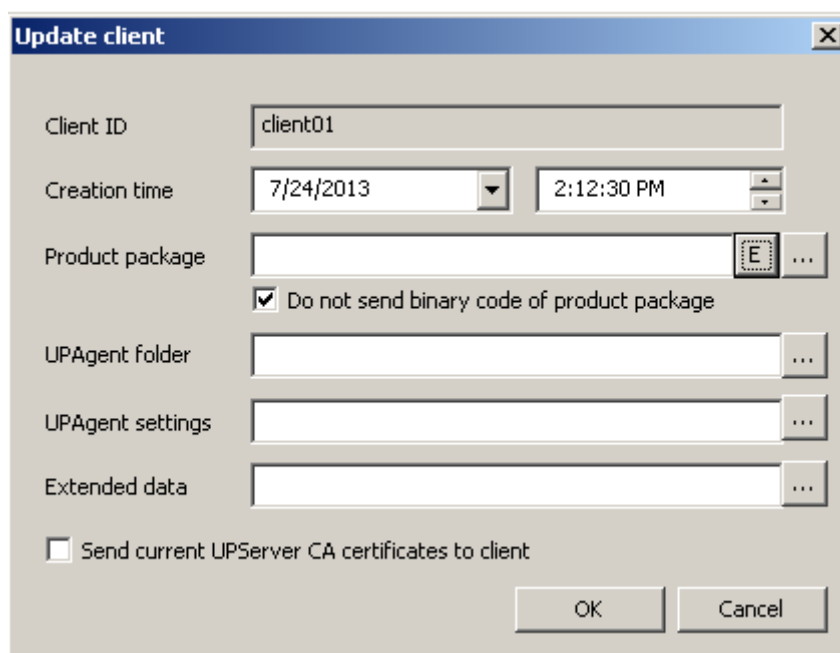


Рисунок 127

3. Появится окно **VPN data maker** с текущими настройками продукта Bel VPN Client 4.1. Для перехода на аутентификацию с использованием сертификатов в этом случае воспользуемся окнами мастера – нажмите кнопку [Run Wizard](#).

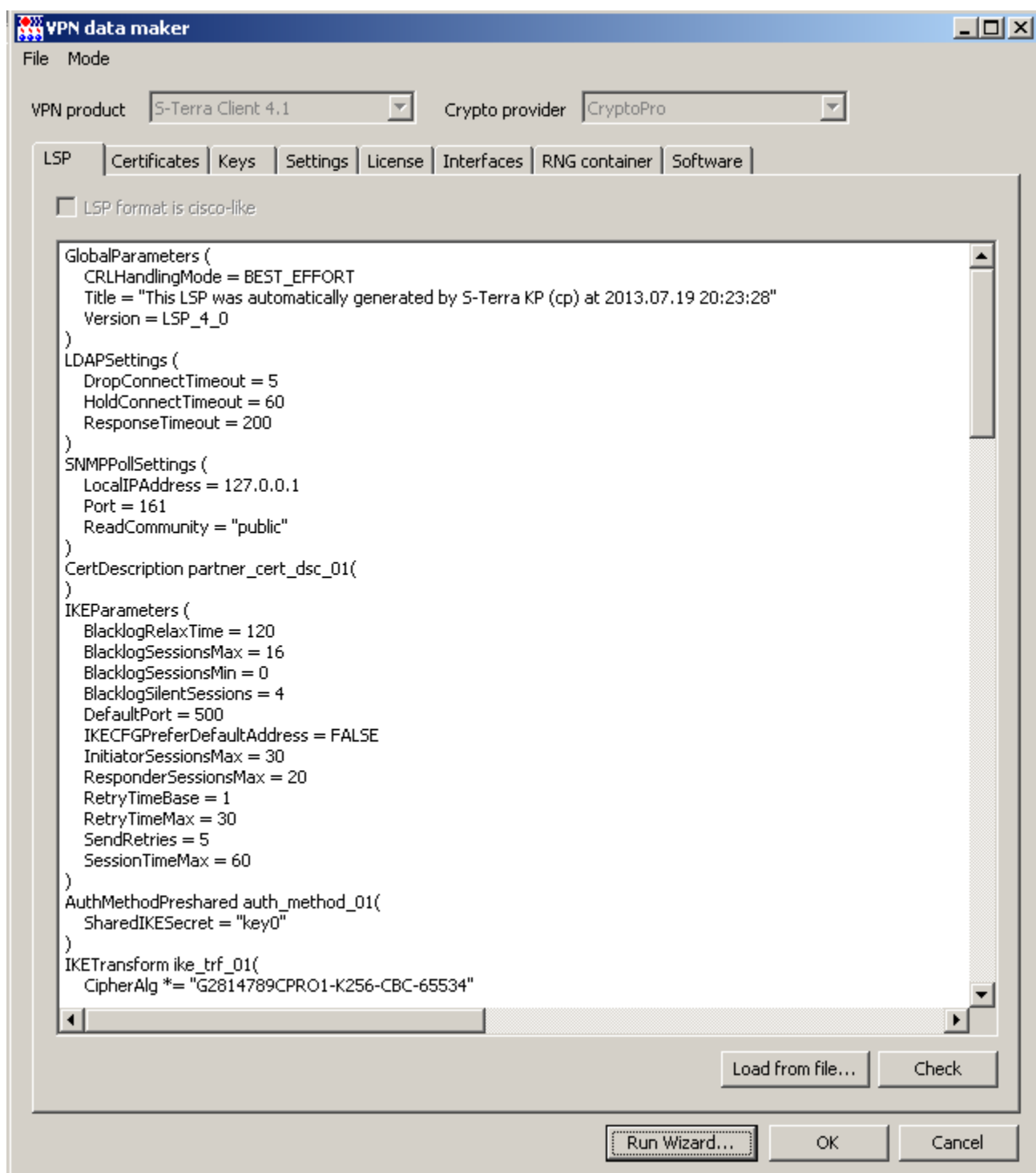


Рисунок 128

- В первом окне мастера добавьте CA сертификат и локальный сертификат клиента client01, а предопределенный ключ с именем key0 удалите (Рисунок 129).

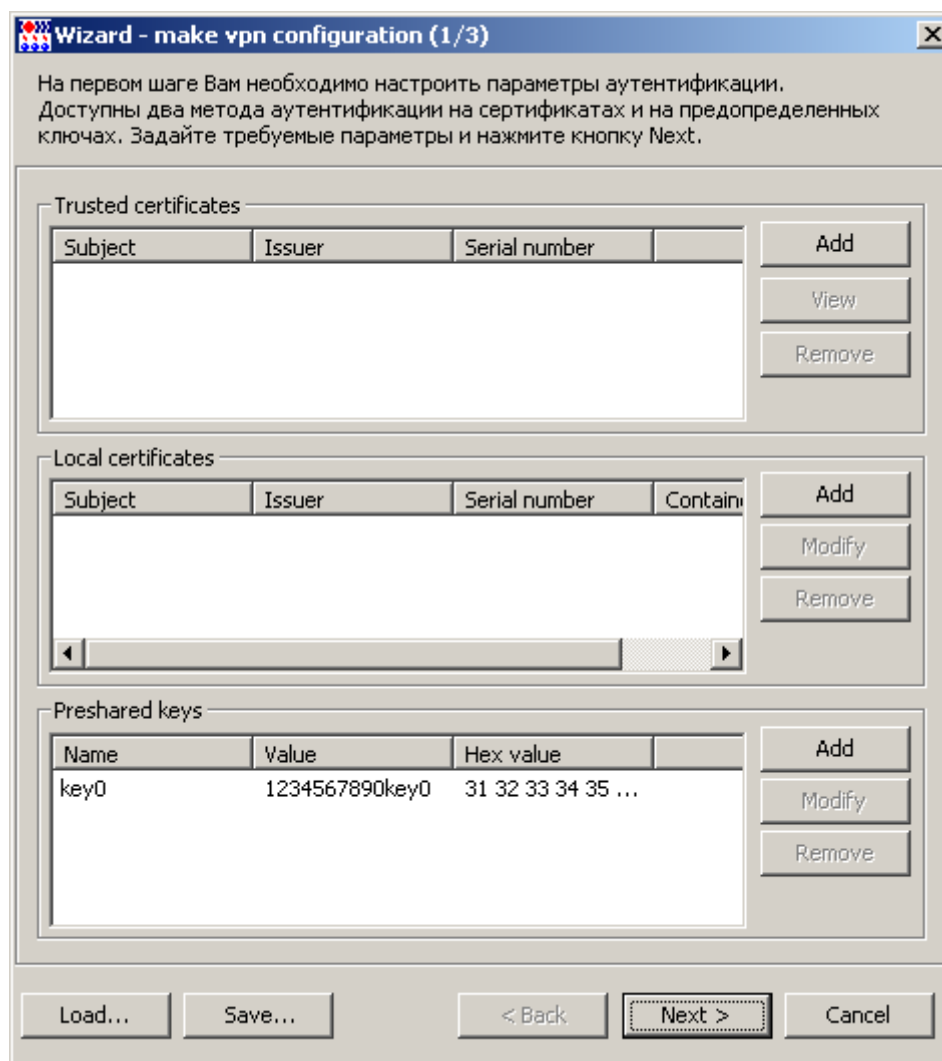


Рисунок 129

- При добавлении сертификатов выберите файл, в котором лежат два сертификата - CA сертификат и локальный сертификат для client01.

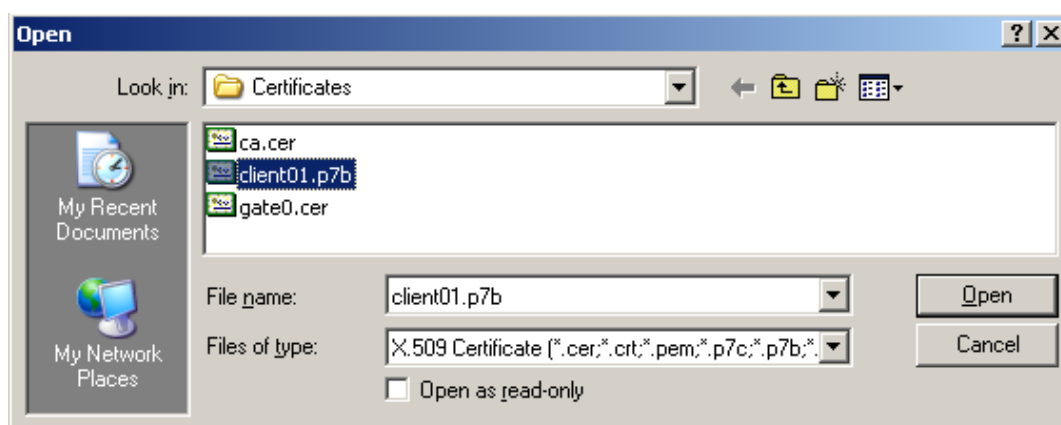


Рисунок 130

6. В открывшемся окне выберите CA сертификат или локальный и нажмите **OK**.

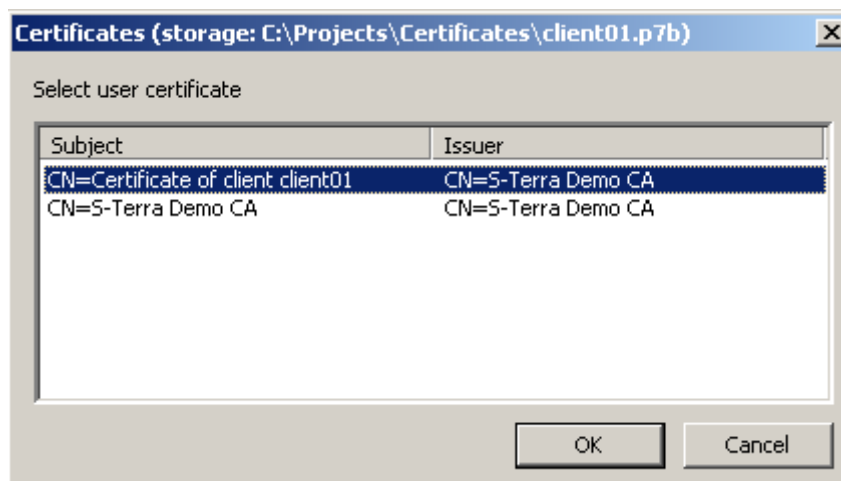


Рисунок 131

7. В окне добавления сертификатов нажмите кнопку **Next** (Рисунок 132).

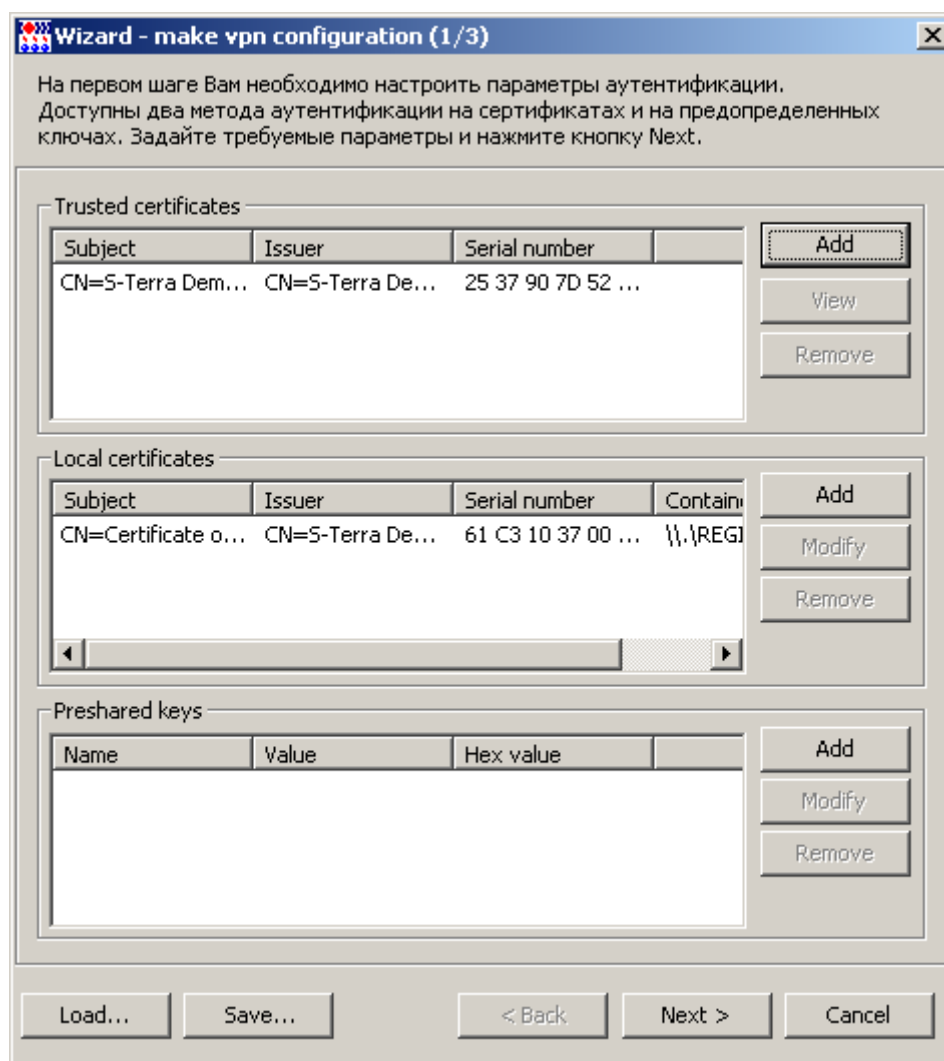


Рисунок 132

8. В следующем окне отредактируйте первое правило, так как для аутентификации клиента будет использоваться только локальный сертификат (Рисунок 133).

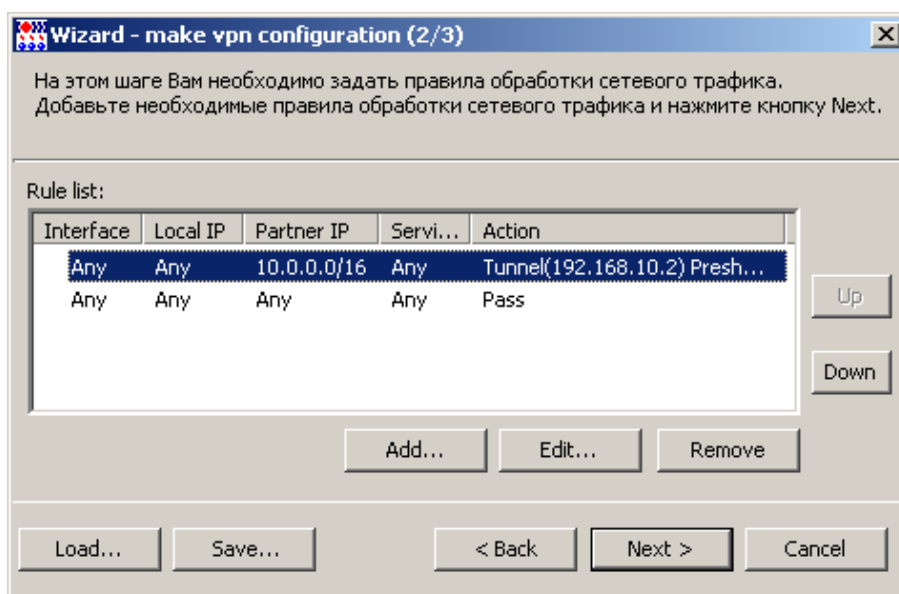


Рисунок 133

9. В правиле измените только метод аутентификации клиента – укажите локальный сертификат, в качестве идентификатора – поле DN сертификата (Рисунок 134).Нажмите **OK**.

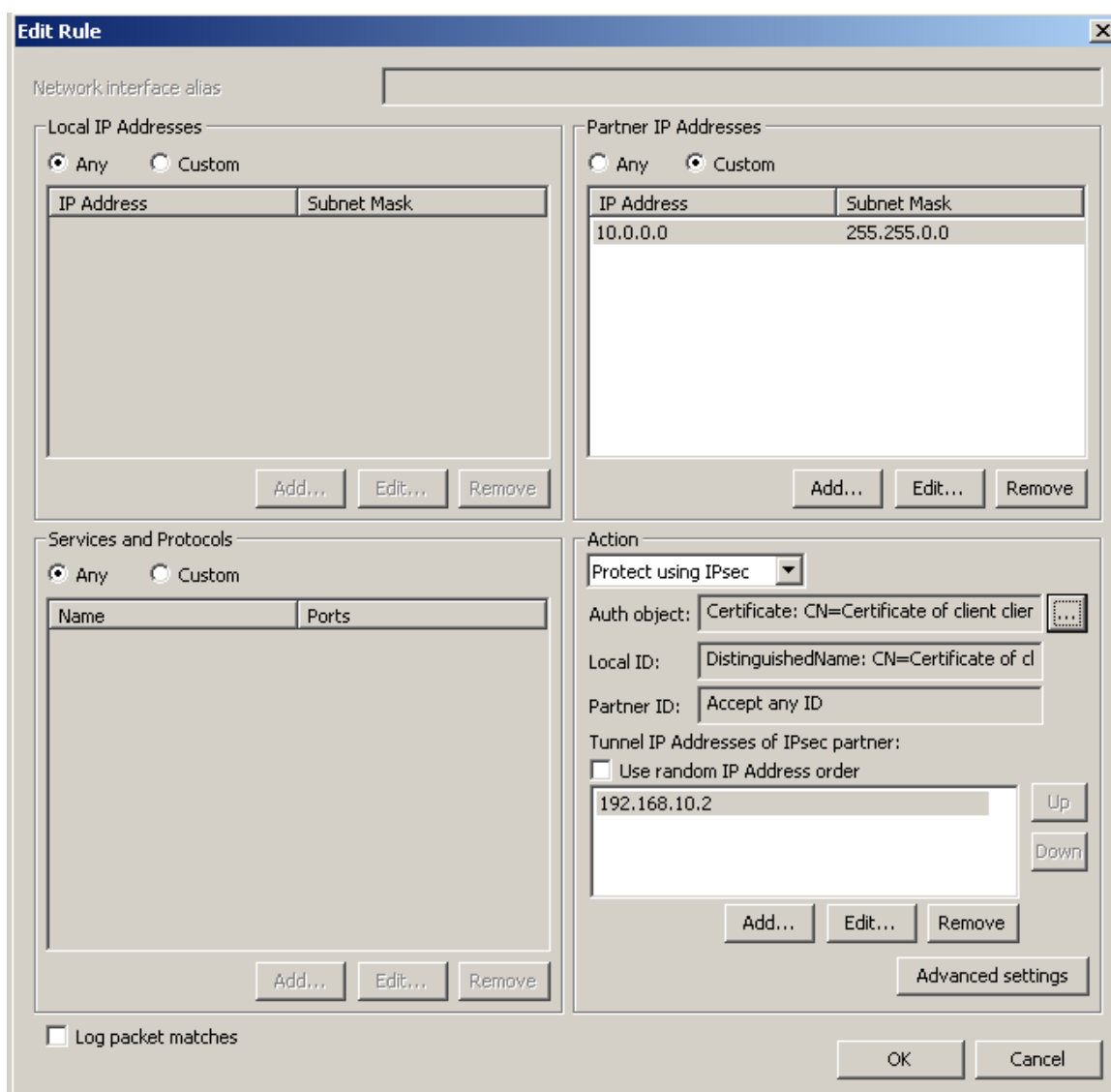


Рисунок 134

10. В окне с правилами для client01 нажмите кнопку **Next** (Рисунок 135).

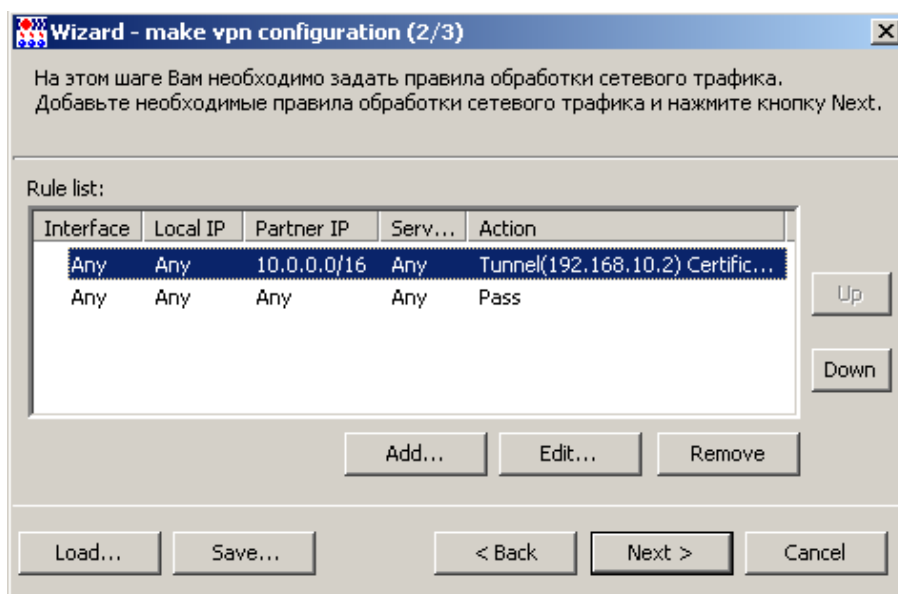


Рисунок 135

11. Лицензионные данные оставьте без изменений и нажмите кнопку **Finish** (Рисунок 136).

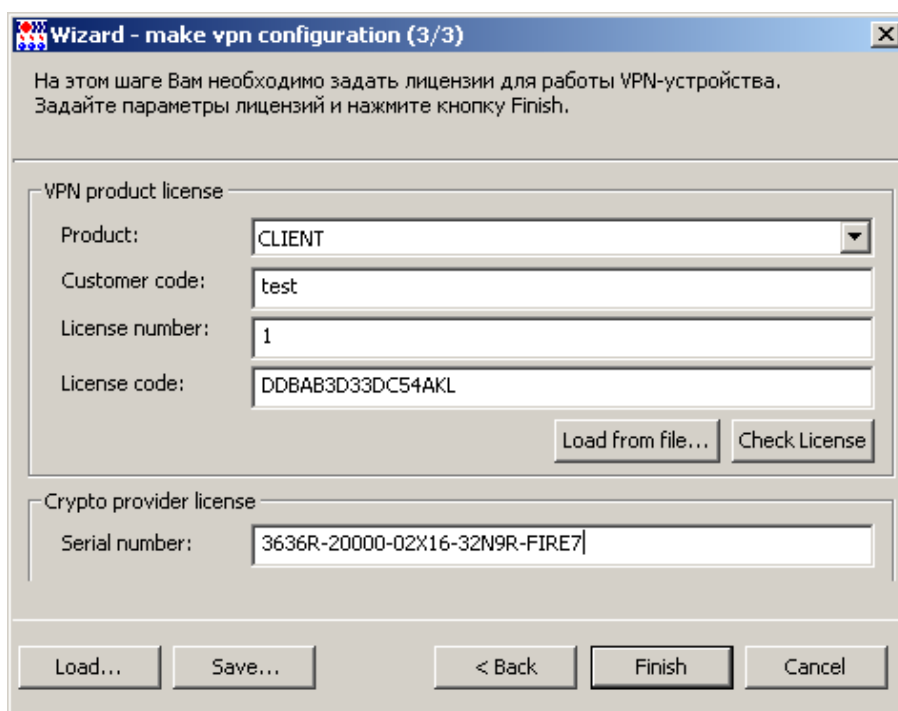


Рисунок 136

12. В окне **VPN data maker** со вкладками нажмите кнопку **OK**.
13. В окне создания обновления **Update client** также нажмите кнопку **OK** (Рисунок 137).



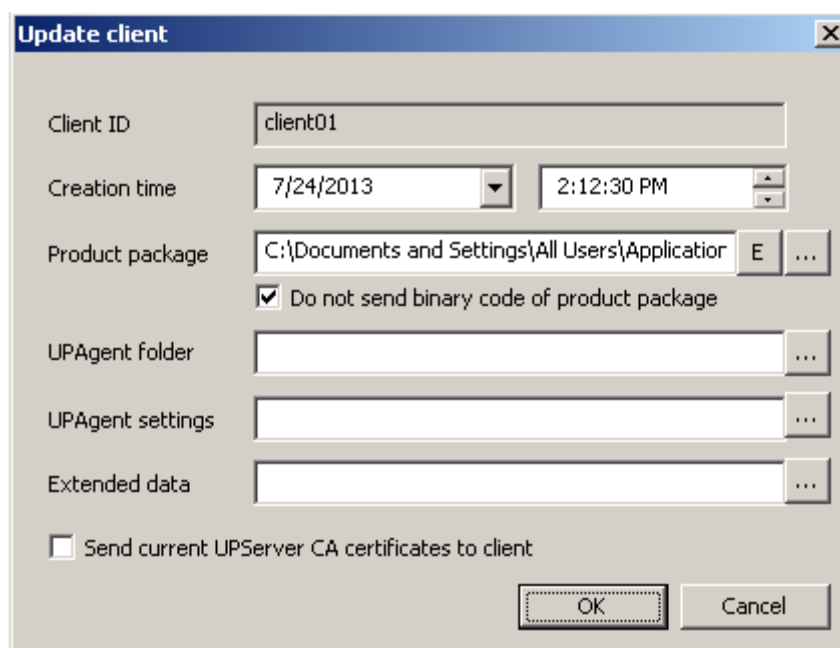


Рисунок 137

14. Обновление для client01 создано (Рисунок 138). Помните, что на клиенте требуется дать разрешение на применение обновления.

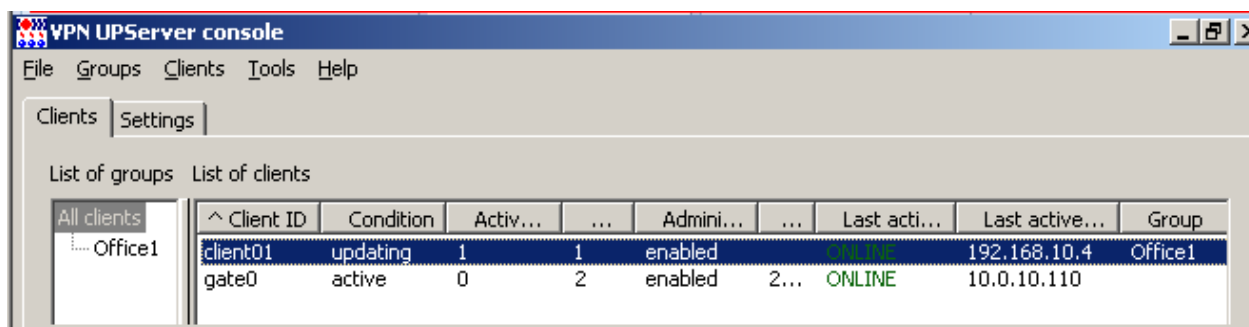


Рисунок 138

15. После применения обновления на клиенте (Рисунок 139), Клиент управления пришлет на Сервер управления информацию о настройках клиента.

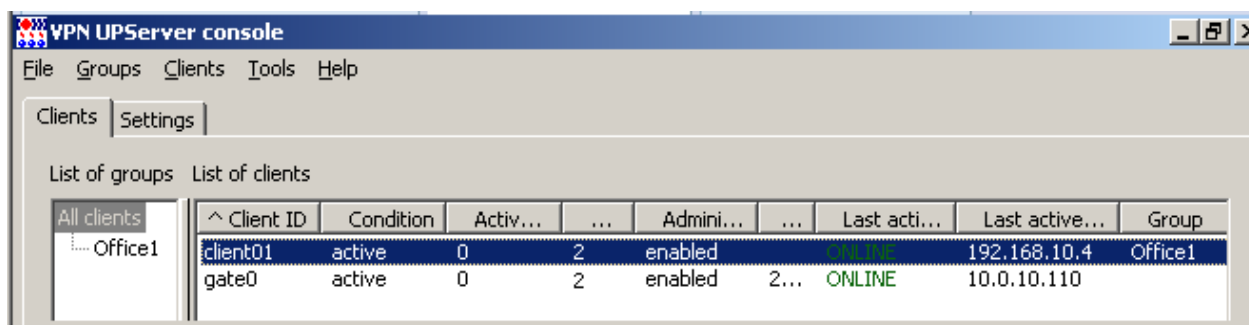


Рисунок 139

16. В контекстном меню по команде **Show** откройте вкладку **Certificates** (Рисунок 140). Видно, что на устройстве с клиентом зарегистрировано 3 сертификата, при создании соединения с центральным шлюзом он прислал по IKE свой сертификат.

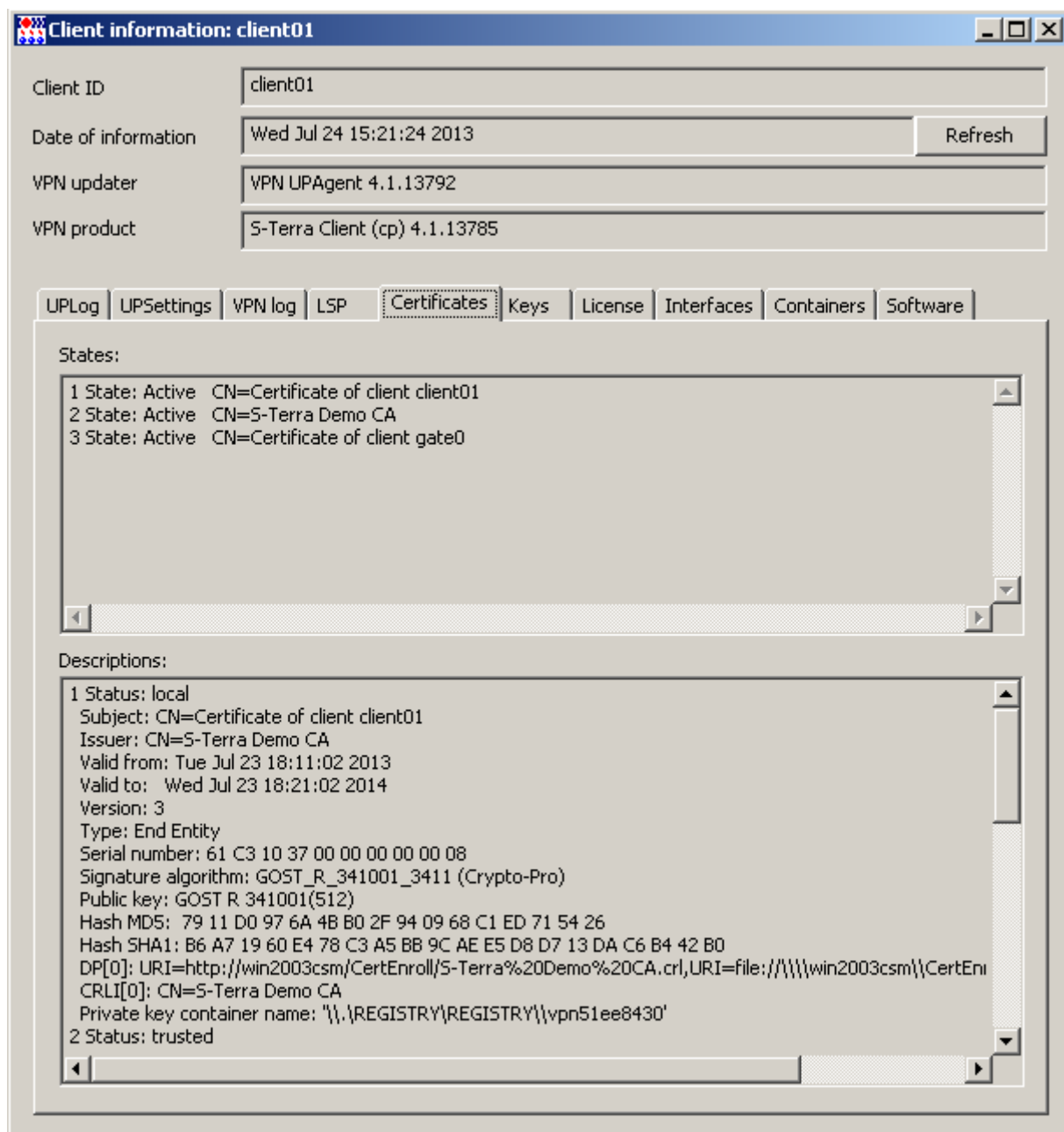


Рисунок 140

## 8. Сценарий неудачного обновления клиента

1. Для получения неудачного обновления клиента укажите неверный адрес Сервера управления в настройках Клиента управления. Для этого во вкладке **Settings** измените, например, адрес 10.0.10.111 на адрес 10.0.10.112 и нажмите кнопку **Save**.

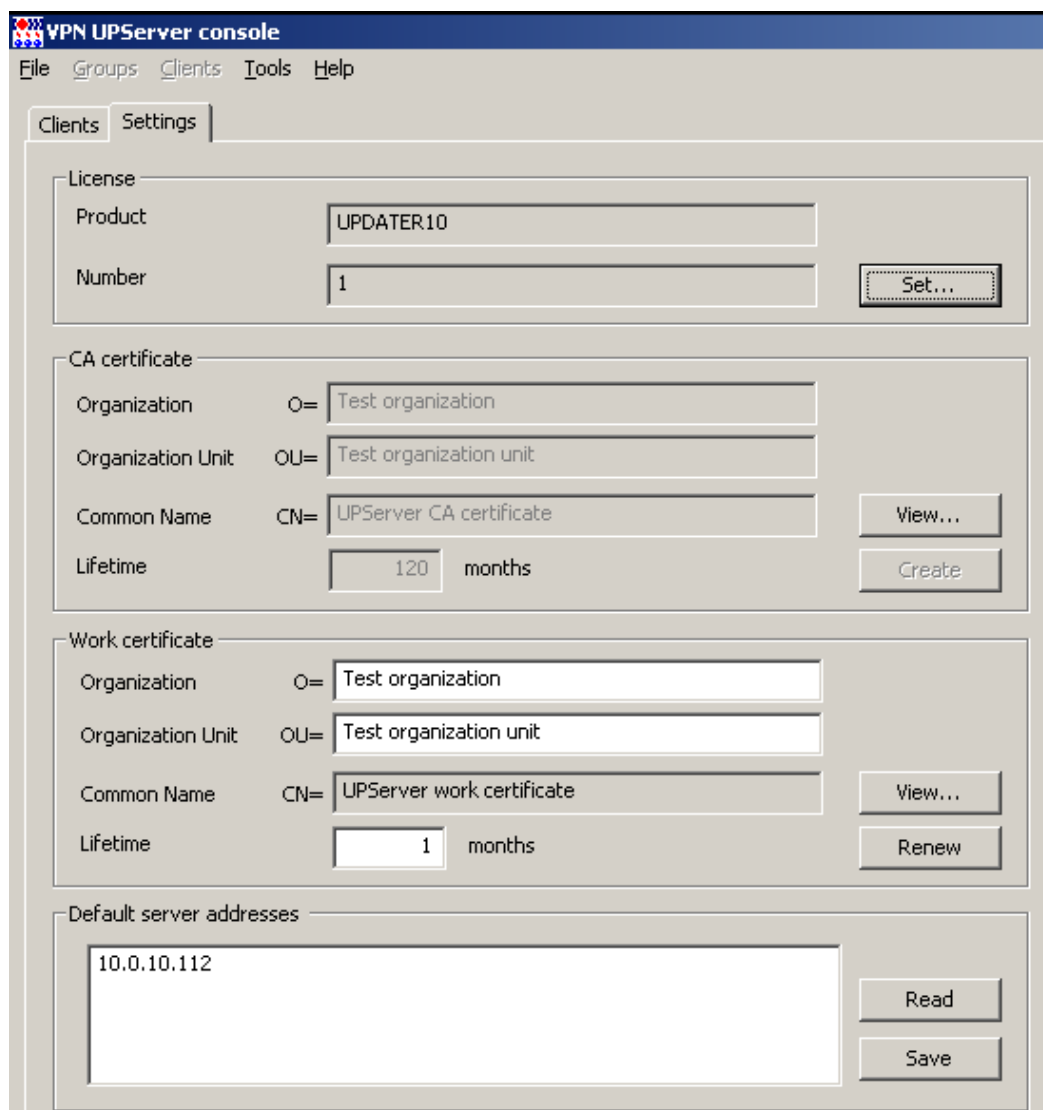


Рисунок 141

2. В окне **Предупреждение** нажмите кнопку **OK**.

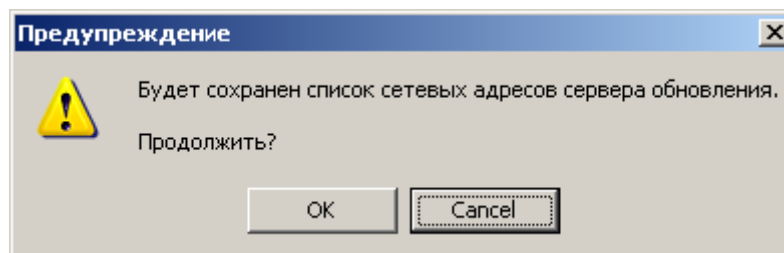


Рисунок 142

3. Создайте новое обновление для существующего клиента. Перейдите на вкладку **Clients** и выберите операцию **Update...**

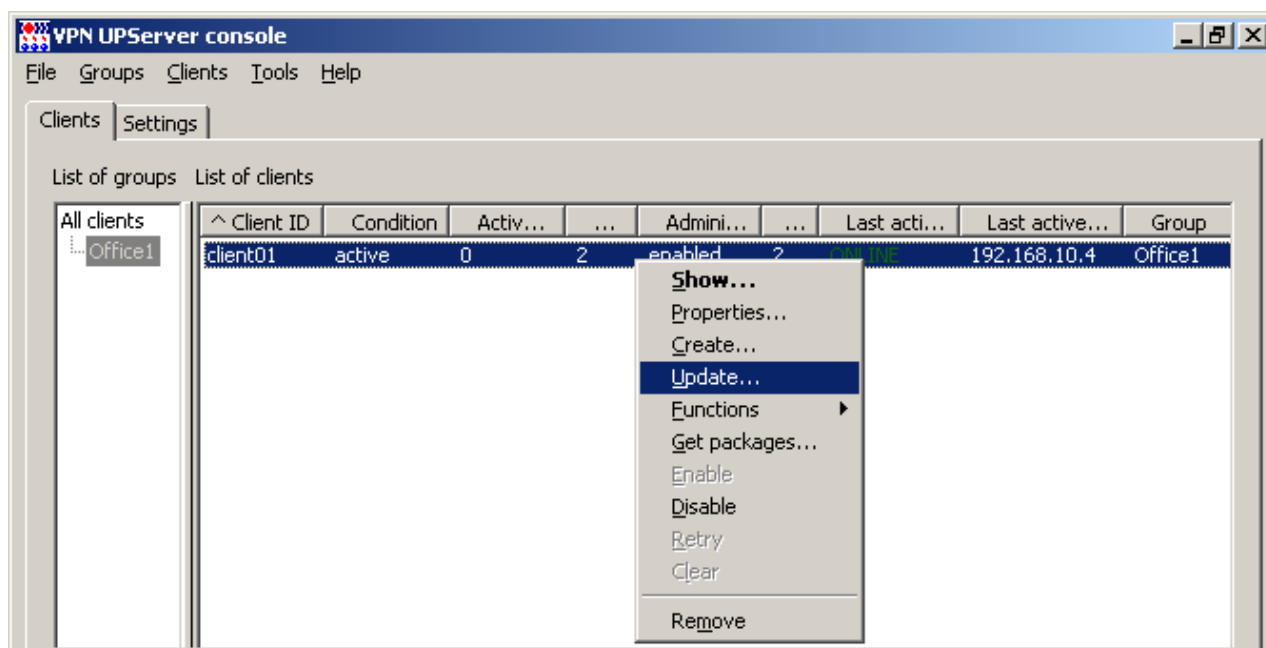


Рисунок 143

4. В открывшемся окне **Update client** задайте файл настроек Клиента управления в поле **UPAgent settings**, в котором уже записан неверный адрес Сервера управления. Расположение файла зависит от операционной системы:

"C:\ProgramData\UPServer\csettings.txt" (начиная с ОС Vista) или

"C:\Documents and Settings\All Users\Application Data\UPServer\csettings.txt".

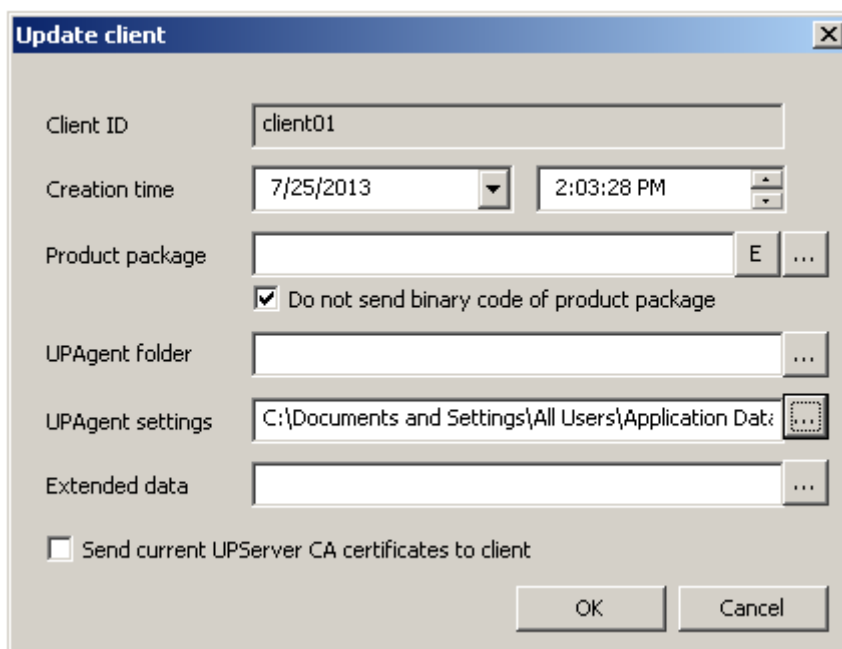


Рисунок 144

5. После нажатия кнопки **OK** количество активных обновлений увеличится на единицу, и через некоторое время состояние изменится с **active** на **waiting**.

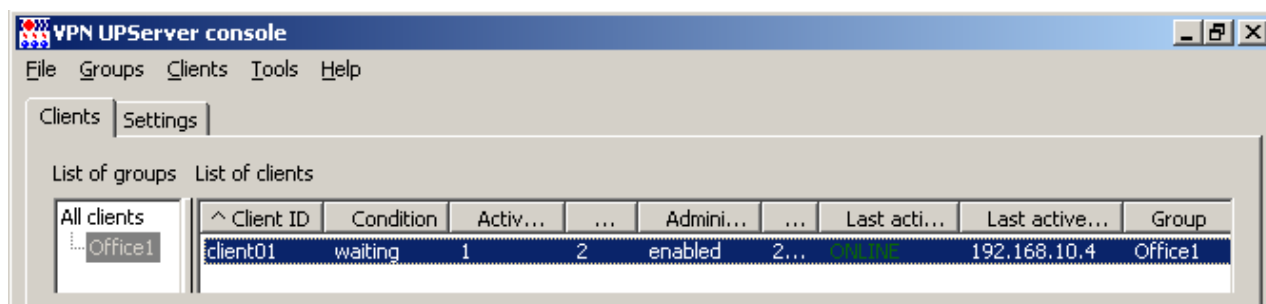


Рисунок 145

6. После того, как Клиент управления обнаружит обновление, состояние изменится с **waiting** на **updating**.

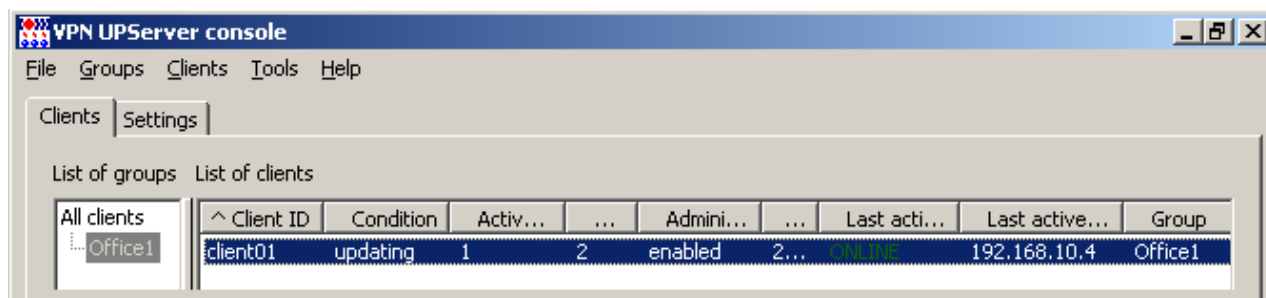


Рисунок 146

7. На устройстве с установленным Bel VPN Client 4.1 будет запрошено разрешение на применение обновления, разрешите обновление. По истечении некоторого времени (если настройки по умолчанию не менялись, то примерно через 6 минут) состояние изменится с **updating** на **failed**.

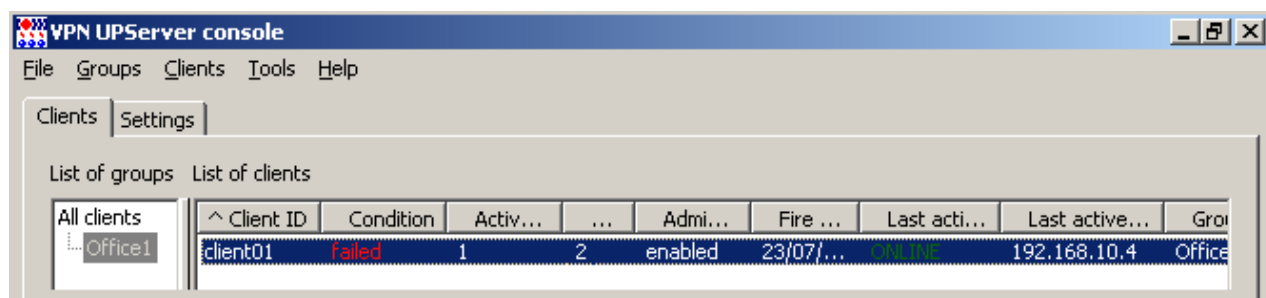


Рисунок 147

8. Состояние **failed** означает, что Клиент управления отверг обновление и вернулся к старой конфигурации. Причины неприятия обновления можно посмотреть, открыв окно информации о клиенте (**Show** в контекстном меню), и во вкладке **UPLog** - лог операции обновления (Рисунок 148, Рисунок 149).

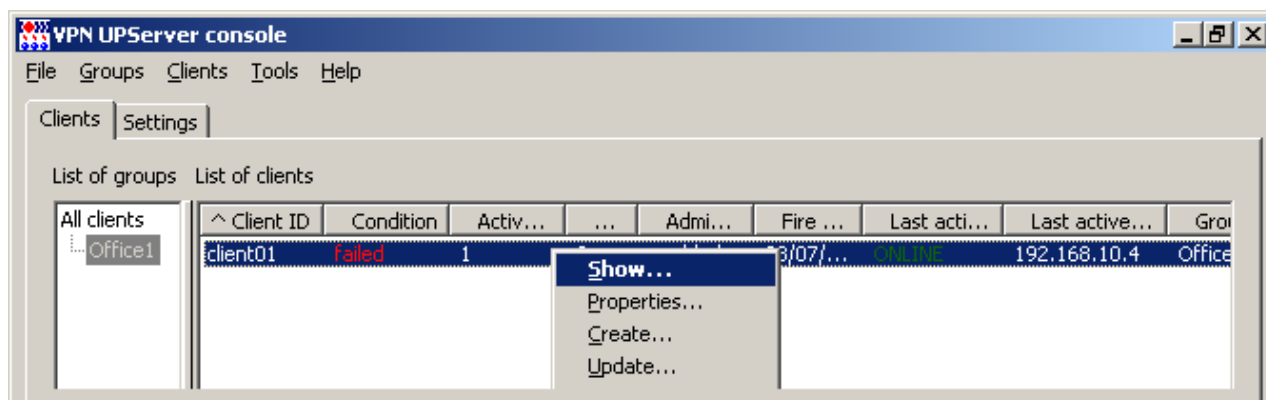


Рисунок 148

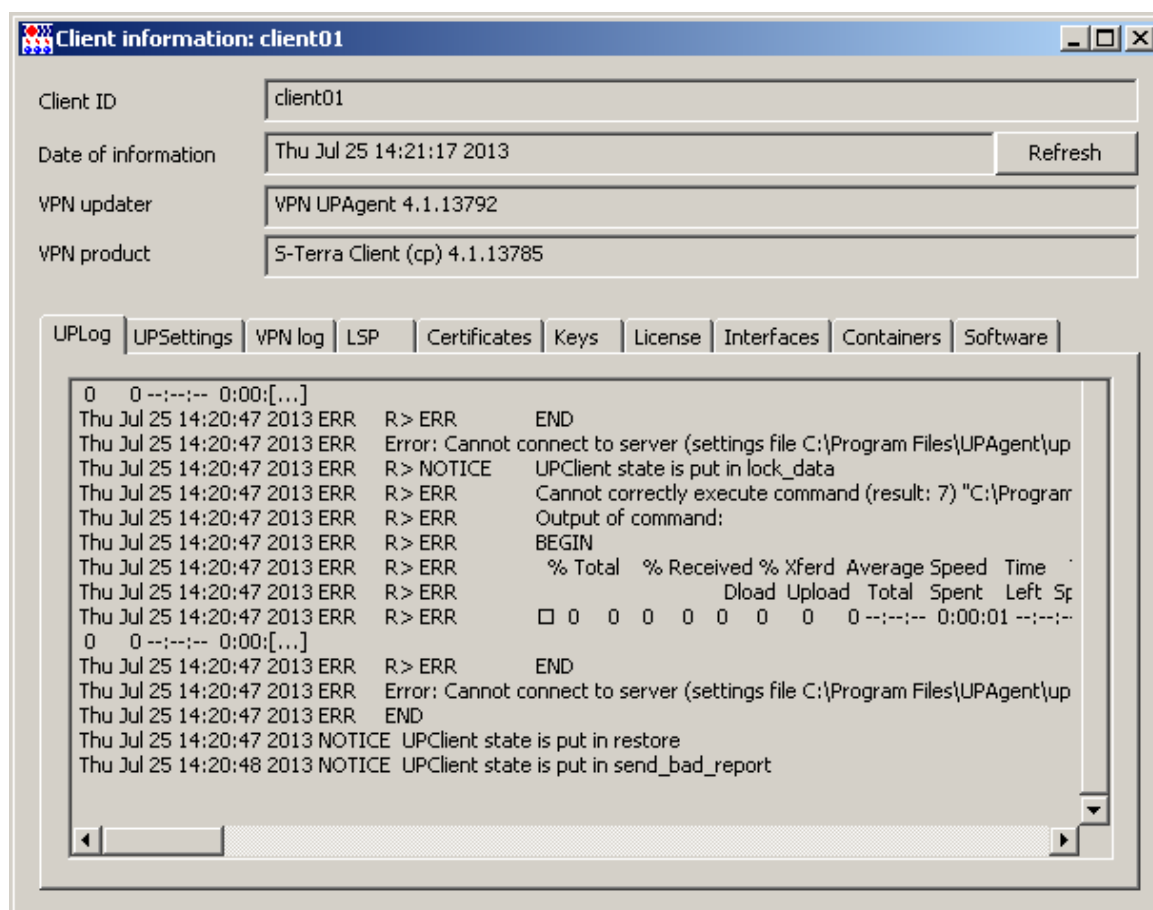


Рисунок 149

9. Для отмены неудачного обновления для данного клиента в меню **Clients** выберите предложение **Clear**.

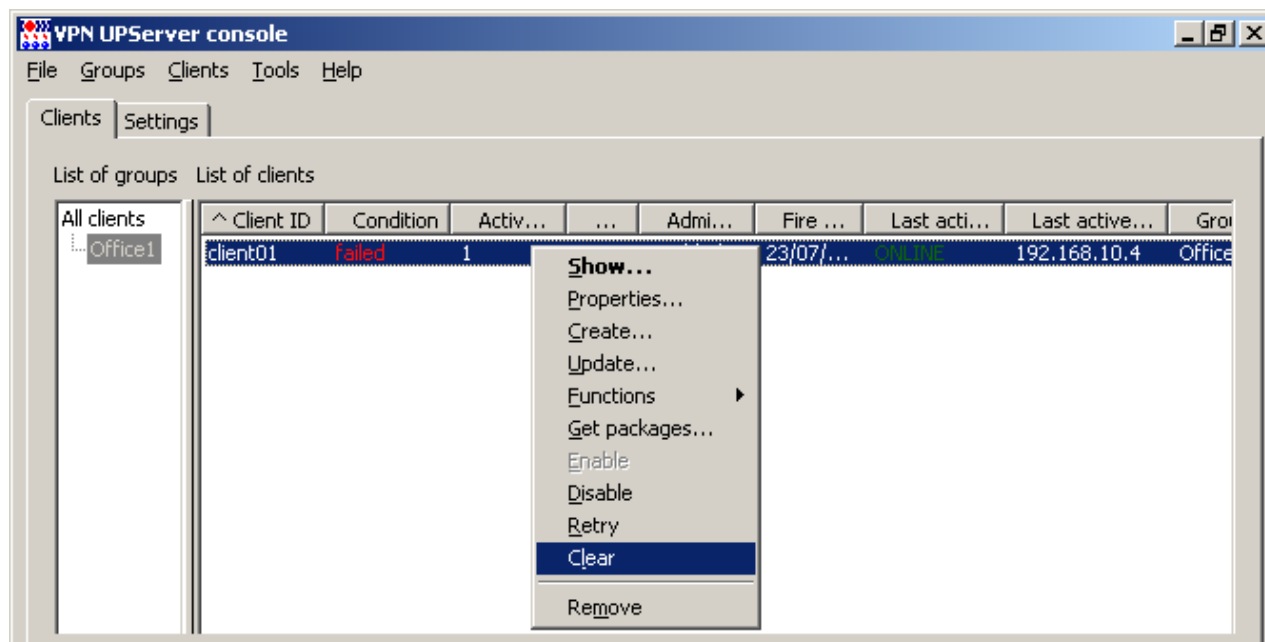


Рисунок 150

10. Выдается предупреждение с просьбой подтвердить удаление всех не примененных обновлений. Нажмите кнопку **OK**.

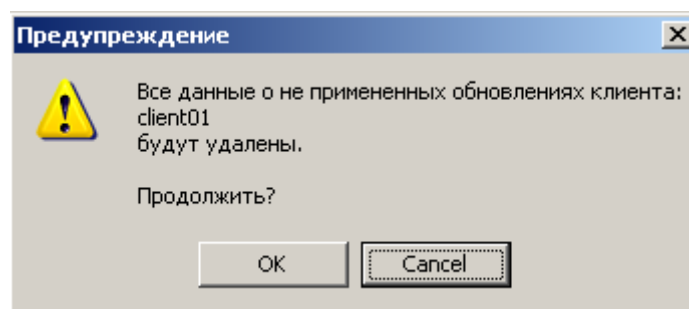


Рисунок 151

11. После этого количество активных обновлений станет равным нулю и через некоторое время состояние изменится с **failed** на **active**. В этом состоянии клиент готов для последующих обновлений.

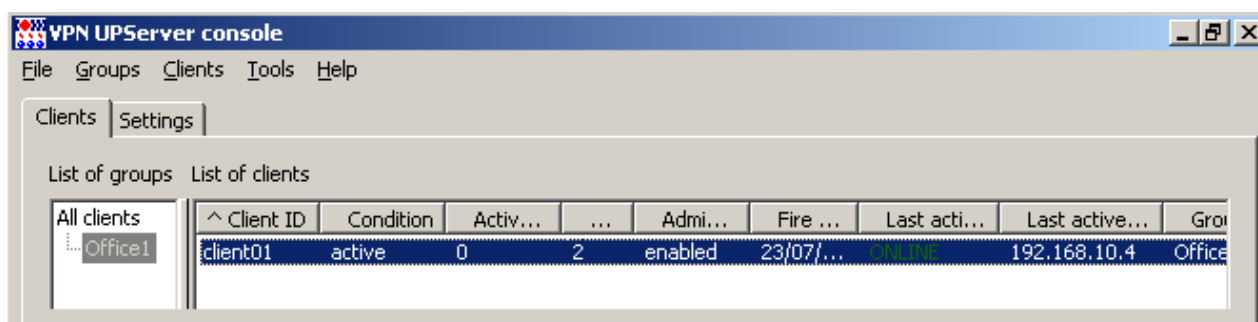


Рисунок 152

12. Не забудьте изменить адрес Сервера управления во вкладке **Settings** на правильное значение.

## 9. Информация о клиенте на Сервере управления

1. Клиент управления на управляемом устройстве собирает информацию о его настройках и передает ее на Сервер управления, где ведется мониторинг состояния и настроек всех управляемых устройств. Для выделенного клиента выберите предложения **Show** меню **Clients** или в контекстном меню.

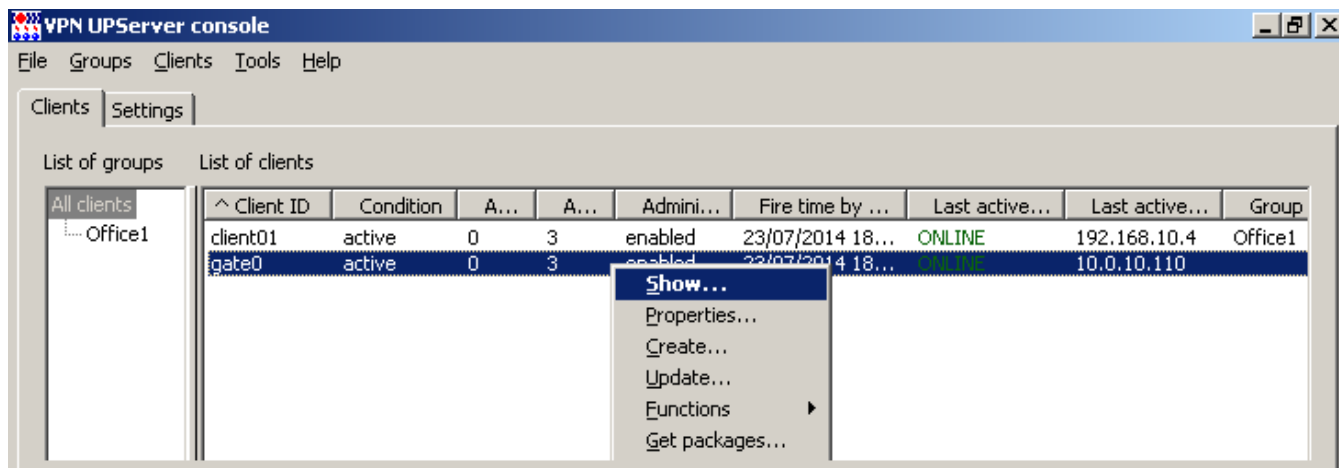


Рисунок 153

2. В результате будет выдано окно с разными вкладками (Рисунок 154), в которых отражена информация о проведенных обновлениях, настройках Клиента управления, действующей в данный момент политике безопасности на устройстве, используемых предопределенных ключах или сертификатах, об интерфейсах устройства, таблице маршрутизации и т.п.
3. Во вкладке **UPLog** ведется регистрация событий при обновлении клиента.

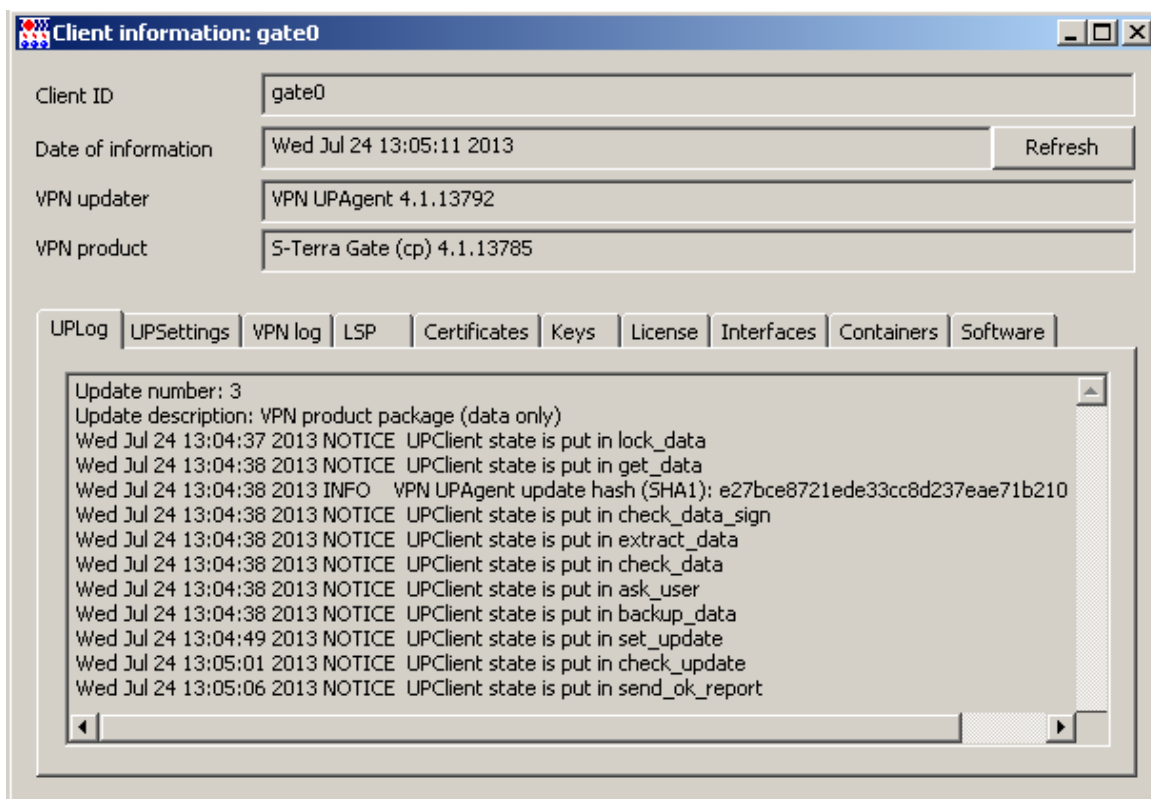


Рисунок 154



4. Во вкладке **UPSettings** (Рисунок 155) отражены настройки Клиента управления. Описание этих настроек дано в главе «[Настройки Клиента управления](#)».

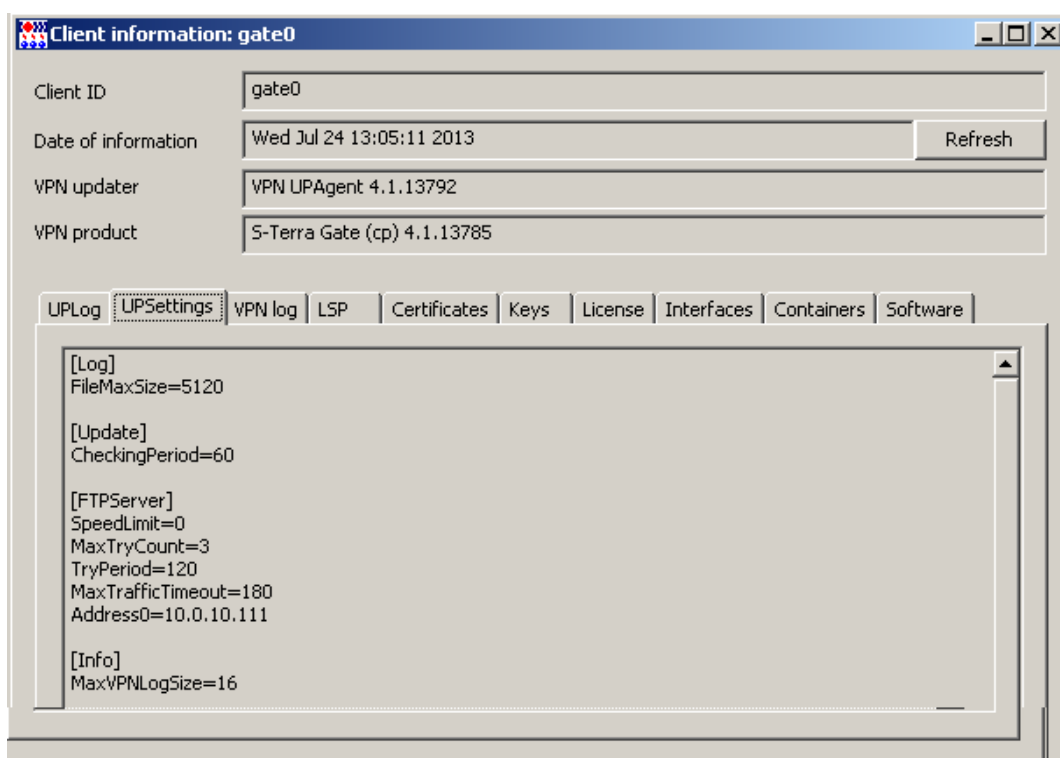


Рисунок 155

5. Во вкладке **VPN log** отражается регистрация событий, связанных с работой VPN-продукта, в частности, Bel VPN Gate, и настройки syslog-клиента.

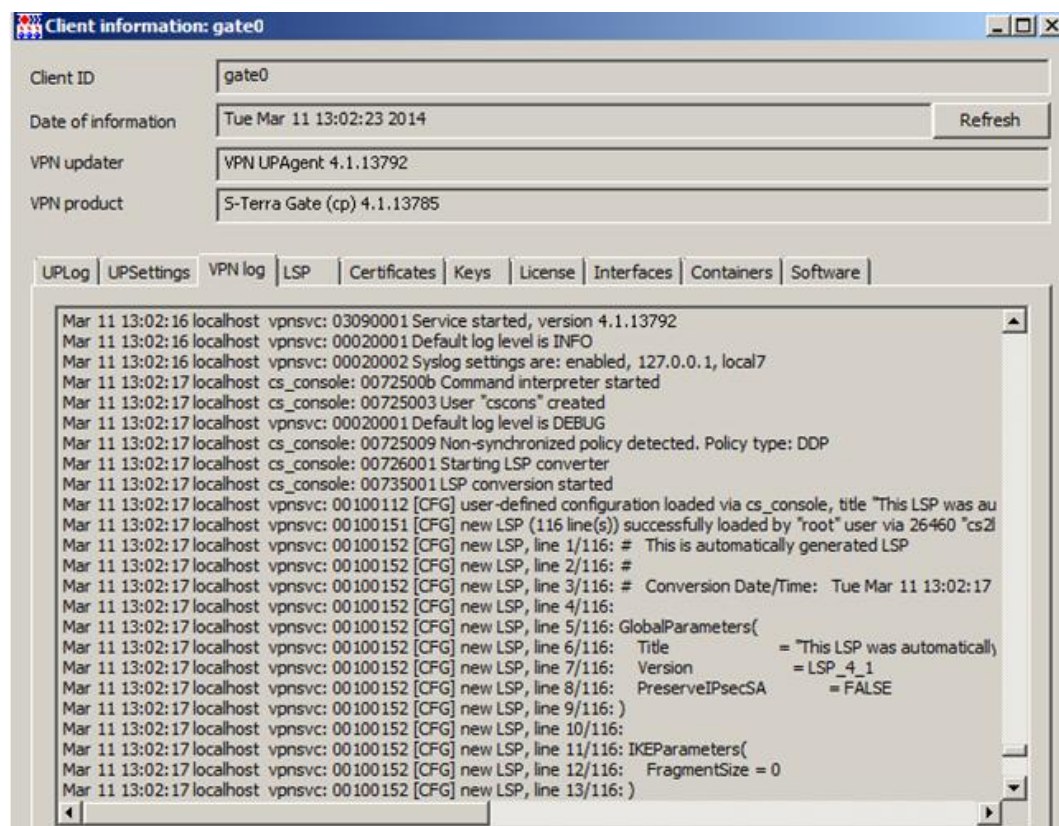


Рисунок 156

6. Вкладка **LSP** показывает загруженную политику безопасности на управляемом устройстве в виде текстового файла и в виде cisco-like конфигурации, а также политику по умолчанию (Рисунок 157).

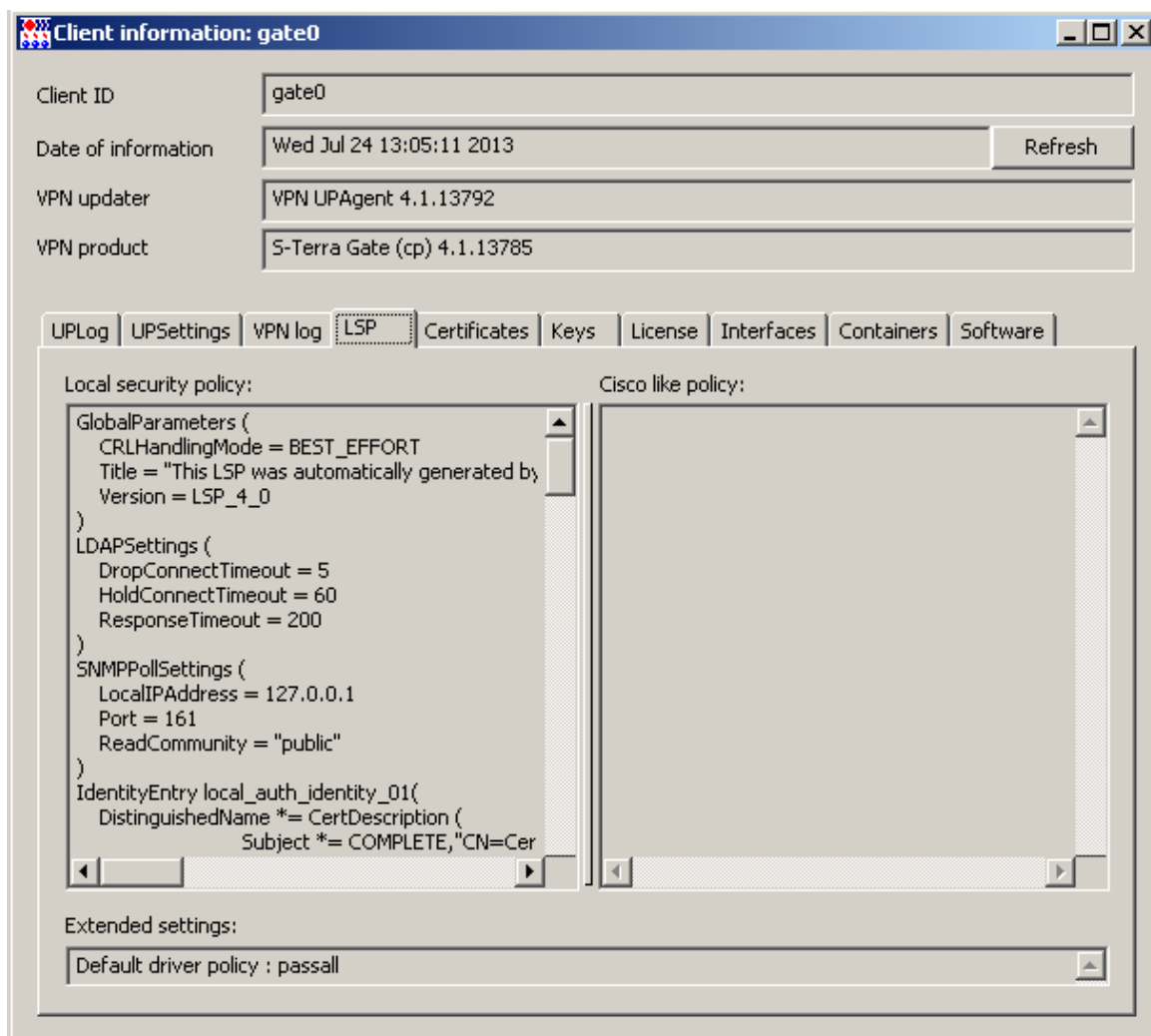


Рисунок 157

7. Вкладка **Keys** показывает только имена предопределенных ключей, используемых при работе с партнерами, не выдавая их значений.

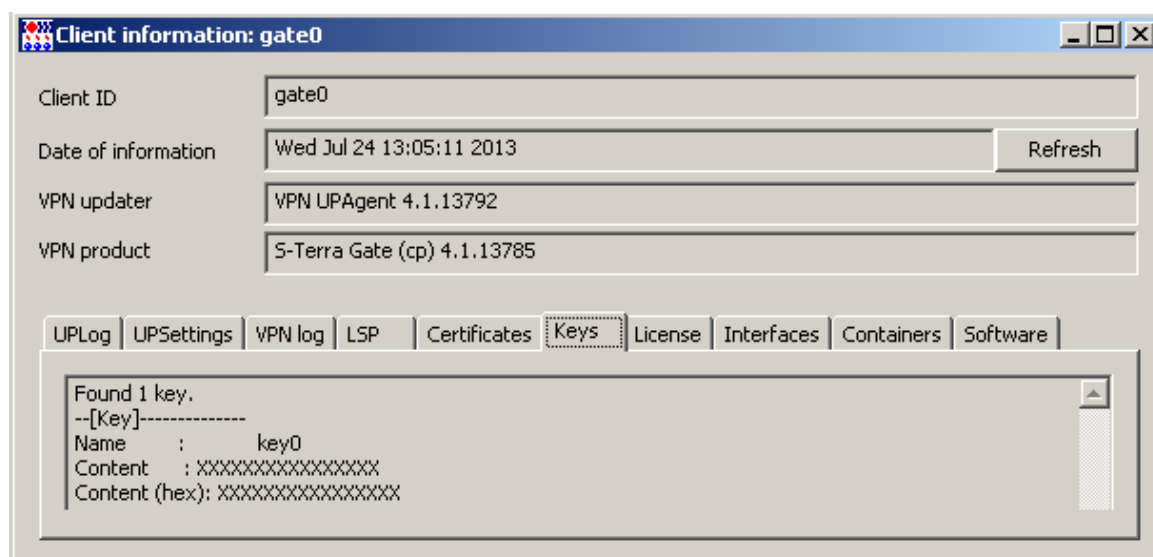


Рисунок 158

8. Вкладка **Certificates** показывает все зарегистрированные в продукте Bel VPN Gate сертификаты и их статус.

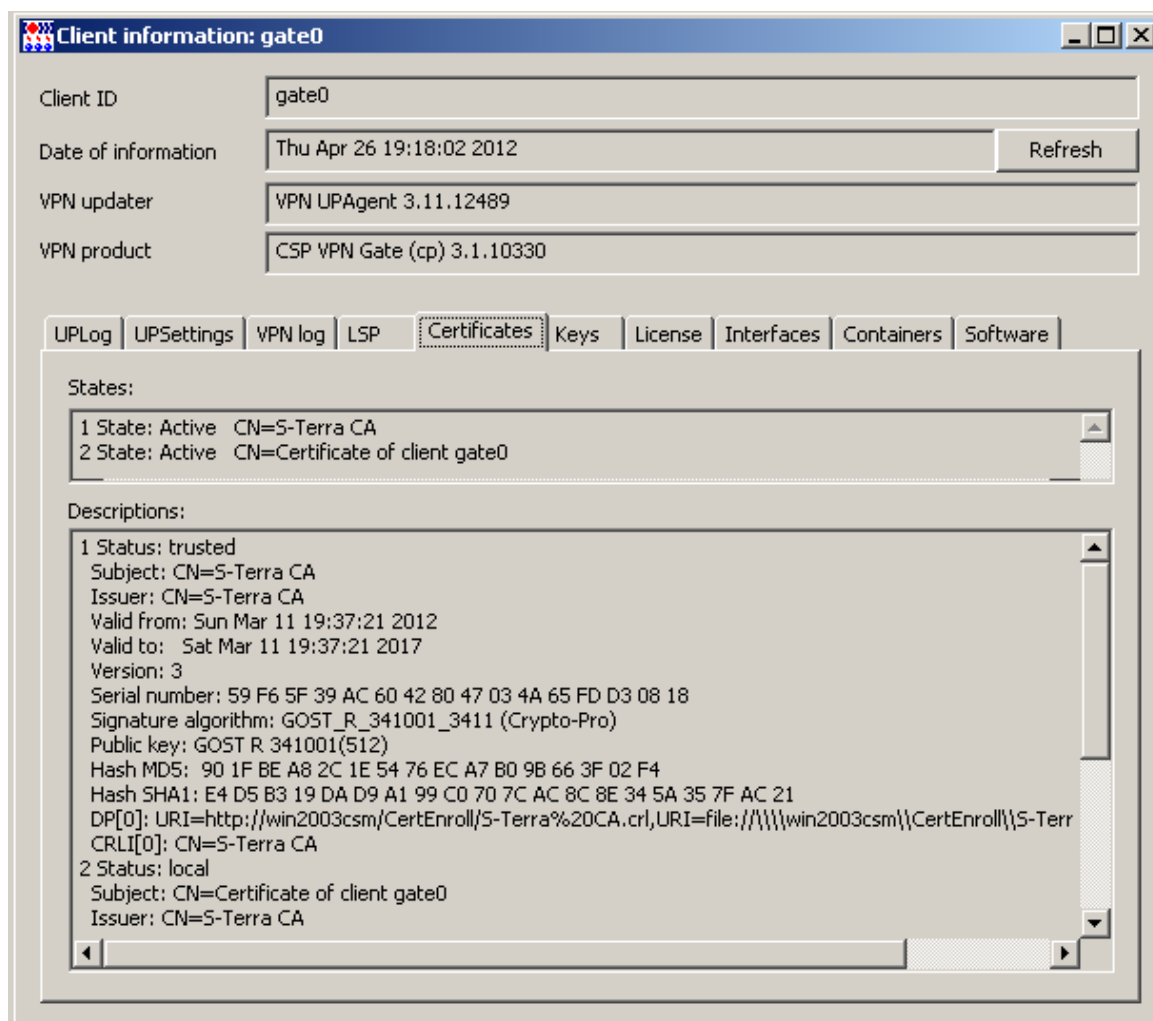


Рисунок 159

9. Во вкладке **License** отражена информация о Лицензиях на продукты.

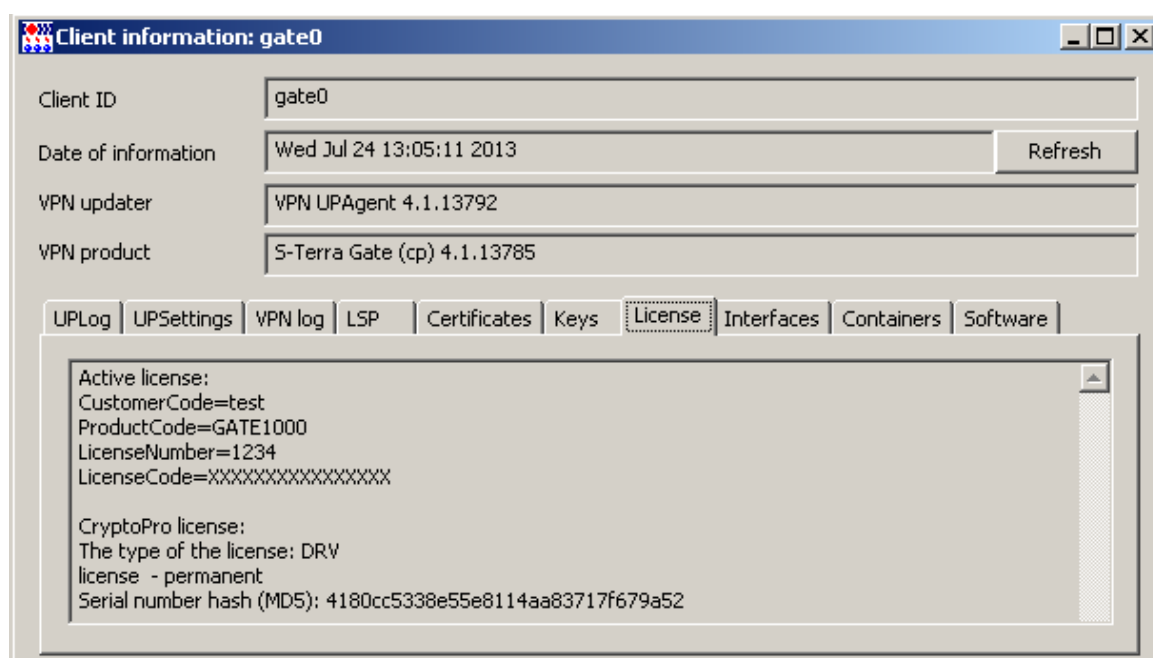


Рисунок 160

10. Вкладка **Interfaces** содержит информацию обо всех сетевых интерфейсах управляемого устройства, маршрутах, а раздел Driver settings показывает настройки IPsec драйвера (для продуктов Bel VPN Gate 4.1, Bel VPN Client 4.1).

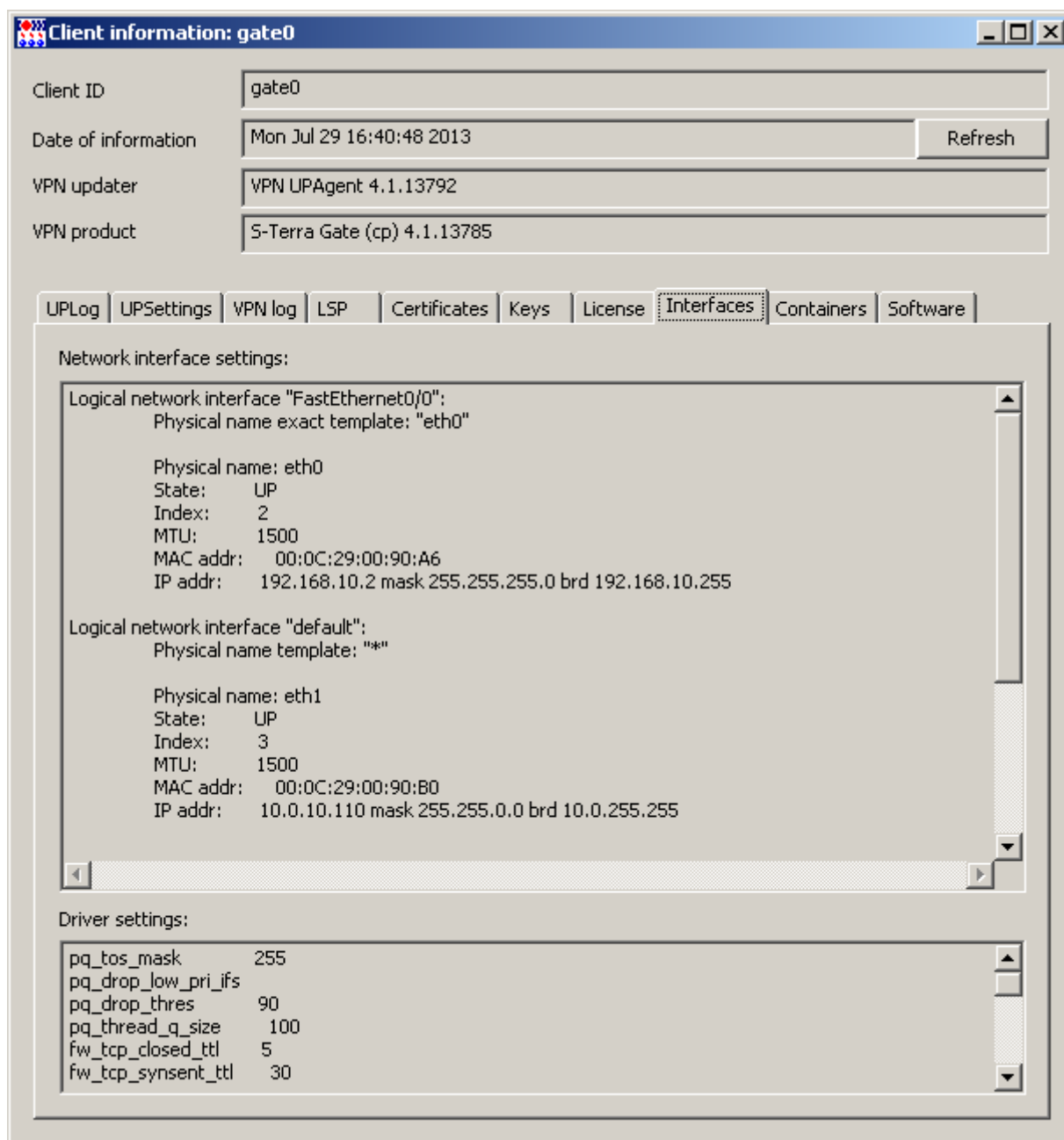


Рисунок 161

11. Вкладка **Containers** показывает созданные на управляемом устройстве запросы на сертификаты, используемые и неиспользуемые контейнеры с ключевыми парами.

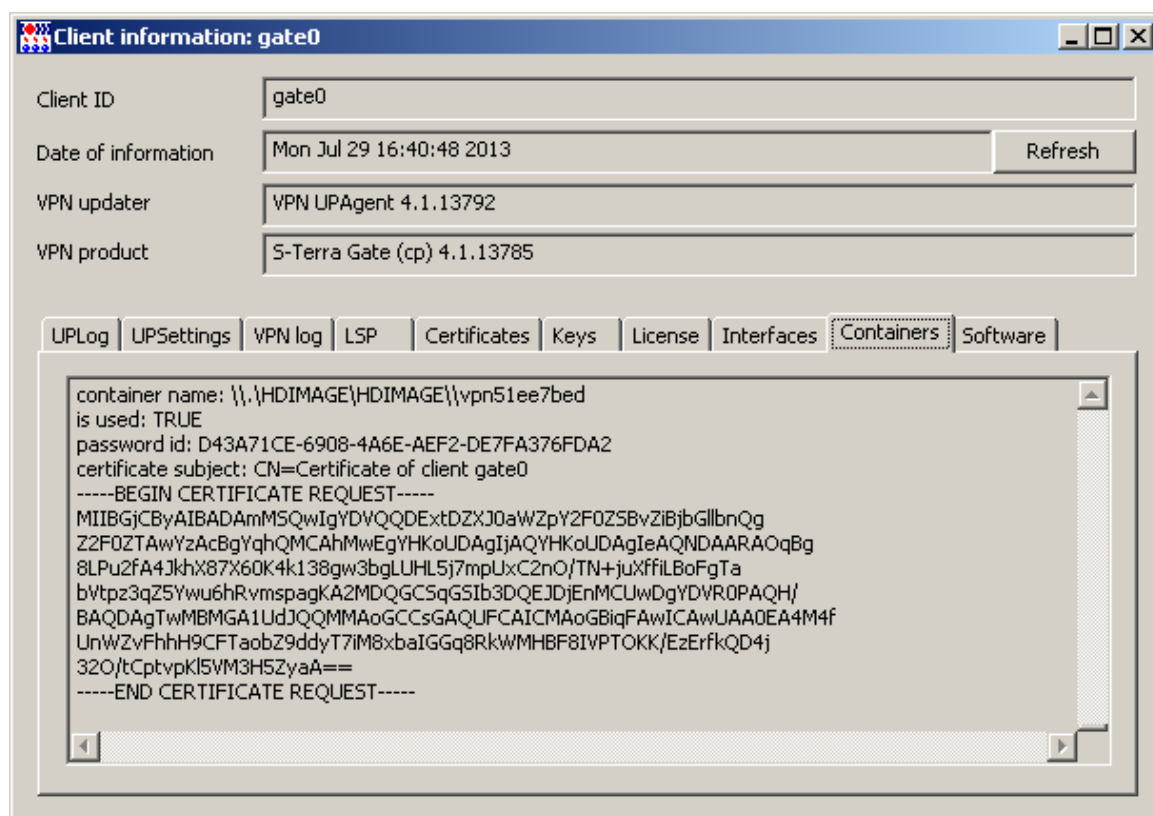


Рисунок 162

12. Вкладка **Software** используется только для продукта Bel VPN Gate 4.1 on token и описана в разделе «[Настройка и управление СПДС «ПОСТ»](#)».

## 10. Сценарий выполнения расширенного обновления

Для примера на управляемом устройстве требуется вывести информацию об имени хоста, выполнив команду

```
hostname
```

Для этого надо создать обновление с командой `hostname`, например, для клиента `client01`, скачав которое Клиент управления и запустит эту команду. Порядок действий следующий:

1. На устройстве с Сервером управления создайте каталог `C:\test` и в нем сохраните файл `update.bat` со следующим содержанием:
 

```
hostname
```
2. На Сервере управления выделите клиента `client01`, в контекстном меню выберите предложение **Update**.

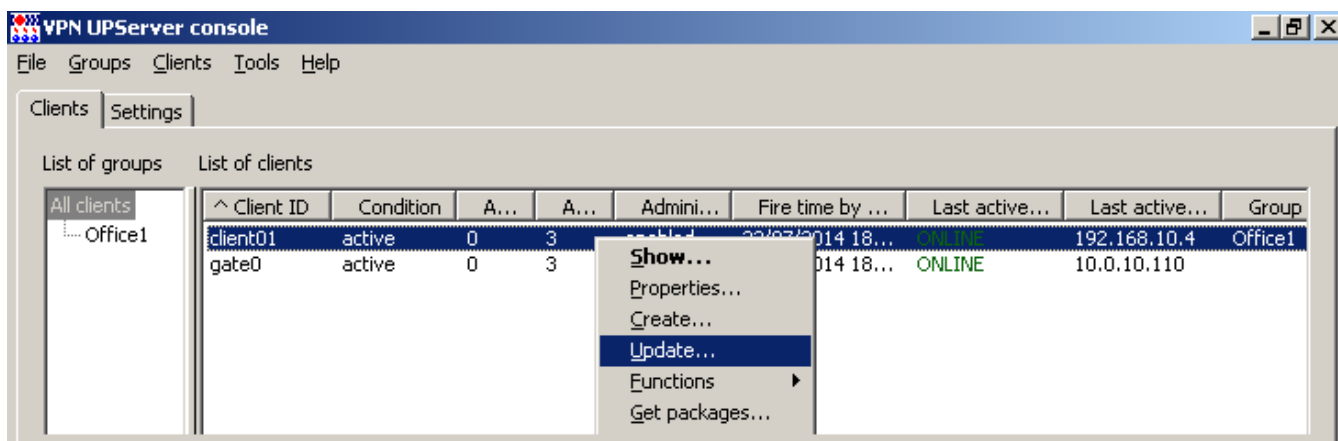


Рисунок 163

3. После этого будет выдано окно формирования обновления для клиента.

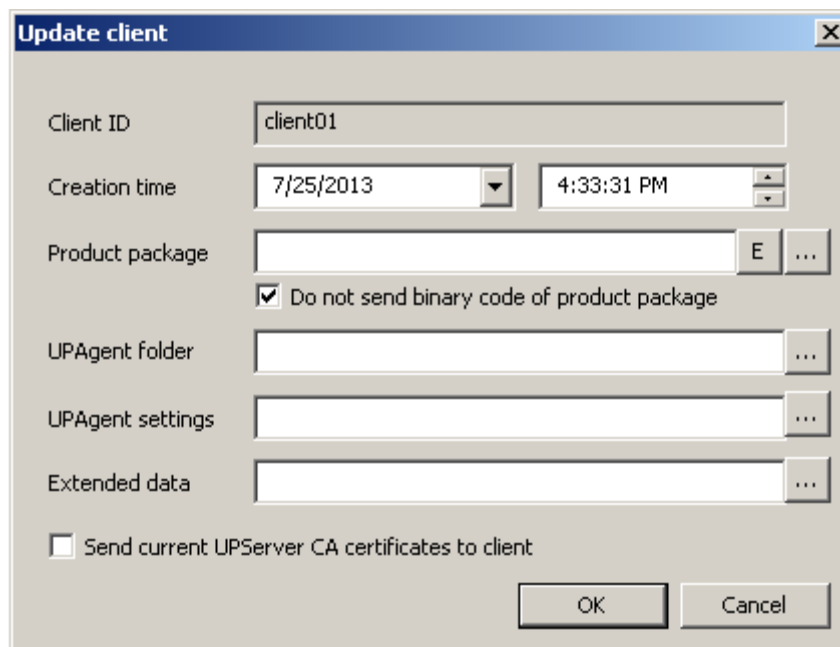


Рисунок 164

В этом окне надо заполнить поле **Extended data**, которое может иметь следующие значения:

**Extended data** – каталог, в котором размещены расширенные данные и скрипты обновления. Данный каталог может содержать любые данные с любой вложенностью каталогов. В данном каталоге имеются зарезервированные названия файлов:

**Файл *cook.bat*** – пакетный файл, который вызывается перед упаковкой каталога для отсылки Клиенту управления.

Файл может отсутствовать.

Если возвращаемое значение файла отлично от нуля - вся операция подготовки обновления завершается с ошибкой.

Каталогом запуска для файла является каталог, в котором он находится.

Перед вызовом файла *cook.bat* автоматически выставляются следующие переменные окружения:

*UPServerBinDir* – каталог Сервера управления, в котором располагаются исполняемые файлы

*UPServerDir* – каталог Сервера управления, в котором располагаются данные продукта

*UPAgentID* – идентификатор Клиента управления, для которого готовится обновление

*VPNProductType* – тип VPN-продукта, установленного на удаленном компьютере (SERVER,CLIENT,GATE)

*VPNProductVersionMajor* – старшая версия VPN-продукта, установленного на управляемом устройстве (например, 3.1)

*VPNProductVersionMinor* – младшая версия VPN-продукта, установленного на управляемом устройстве (например, 10330)

*VPNProductCryptoProvider* – криптопровайдер, используемый VPN-продуктом, который установлен на управляемом устройстве (AV)

*UPAgentGroup* – идентификатор группы, к которой принадлежит *UPAgent*

*UPAgentOS* – тип операционной системы, для которой был собран *UPAgent* (WIN2K, LINUXDEBIAN6)

*UPAgentCPU* – тип процессора системы, для которой был собран *UPAgent* (i386,i486,i686)

*UPAgentLastActiveTime* – время, в которое *UPAgent* установил соединение с FTP-сервером (dd/mm/yyyy hh:mm:ss)

*UPAgentLastIPAddr* – сетевой адрес, с которого *UPAgent* установил соединение с FTP-сервером

*VPNProductFireTimeByCert* – ближайшая дата истечения срока действия сертификатов Устройства, на котором установлен *UPAgent*

*UPAgentVersionMajor* – старшая версия Клиента управления, установленного на управляемый компьютер (1.2 и так далее)

*UPAgentVersionMinor* – младшая версия Клиента управления, установленного на управляемый компьютер (10330 и так далее)

*EX\_???* – расширенные переменные, заданные администратором для клиента, посредством окна Properties... в VPN UPServer console.

**Файл *backup.bat (backup.sh)*** – пакетный файл, который вызывается на Клиенте управления перед запуском процедуры обновления.

Файл может отсутствовать.

Если возвращаемое значение файла отлично от нуля - вся операция обновления завершается с ошибкой.

Каталогом запуска для файла является каталог, в котором он находится.

**Файл *update.bat (update.sh)*** – пакетный файл, который вызывается на Клиенте управления процедуры обновления.

Файл может отсутствовать.

Если возвращаемое значение файла отлично от нуля - вся операция обновления завершается с ошибкой.

Каталогом запуска для файла является каталог, в котором он находится.

**Файл *restore.bat (restore.sh)*** – пакетный файл, который вызывается на Клиенте управления в случае неудачи во время процедуры обновления или при завершении с ошибкой выполнения пакетного файла ***update.bat***.

Файл может отсутствовать.

Строго не рекомендуется возвращать значение, отличное от нуля, так как Клиент управления будет периодически вызывать этот скрипт, пока он не завершится успехом.

Каталогом запуска для файла является каталог, в котором он находится.

Перед вызовом файлов ***backup.bat (backup.sh)***, ***update.bat (update.sh)***, ***restore.bat (restore.sh)*** автоматически выставляются следующие переменные окружения:

**UPAgentBinDir** – каталог Клиента управления, в котором располагаются исполняемые файлы

**UPAgentDir** – каталог Клиента управления, в котором можно сохранять данные

**VPNProductBinDir** – каталог продукта Bel VPN Gate/Client, в котором располагаются исполняемые файлы

**UPAgentID** – идентификатор Клиента управления

**UPServerAddr** – рабочий адрес Сервера управления

**VPNProductType** – тип VPN-продукта, установленного на управляемом устройстве (SERVER,CLIENT,GATE,TGATE)

**VPNProductVersionMajor** – старшая версия VPN-продукта, установленного на управляемом устройстве (например, 3.1)

**VPNProductVersionMinor** – младшая версия VPN-продукта, установленного на управляемом устройстве (например, 10330)

**VPNProductCryptoProvider** – криптопровайдер, используемый VPN-продуктом, который установлен на управляемом устройстве (CP,SC,ST)

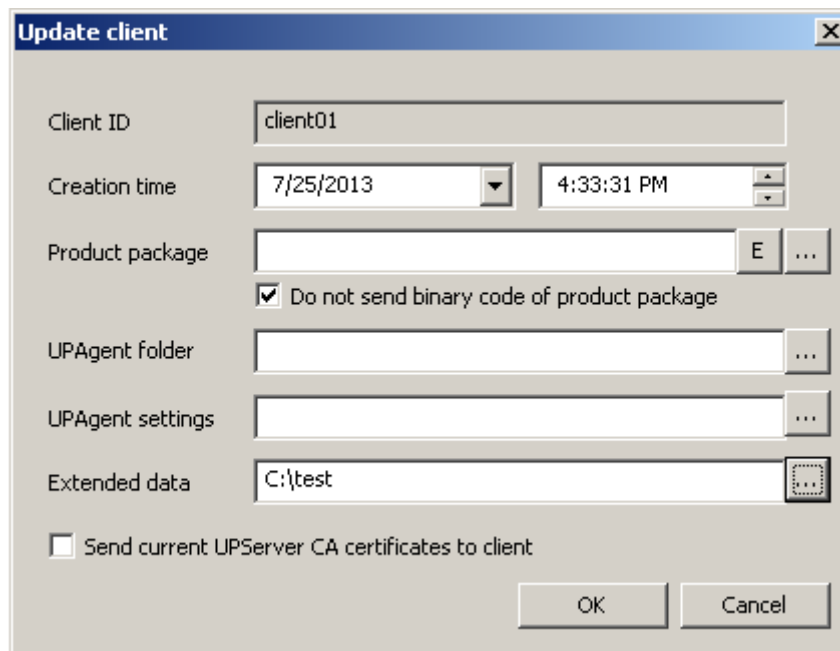
**UPAgentVersionMajor** – старшая версия UPAgent, установленного на управляемом устройстве (например, 1.2)

**UPAgentVersionMinor** – младшая версия UPAgent, установленного на управляемом устройстве (например, 11687)

**VPNProductUtilitySuffix** – суффикс, используемый для различия имен утилит разных версий VPN-продукта (“\_3\_1”, “\_4\_0”, “\_4\_1”).

4. В поле **Extended data** внесите каталог C:\test с файлом *update.bat* и нажмите ОК.



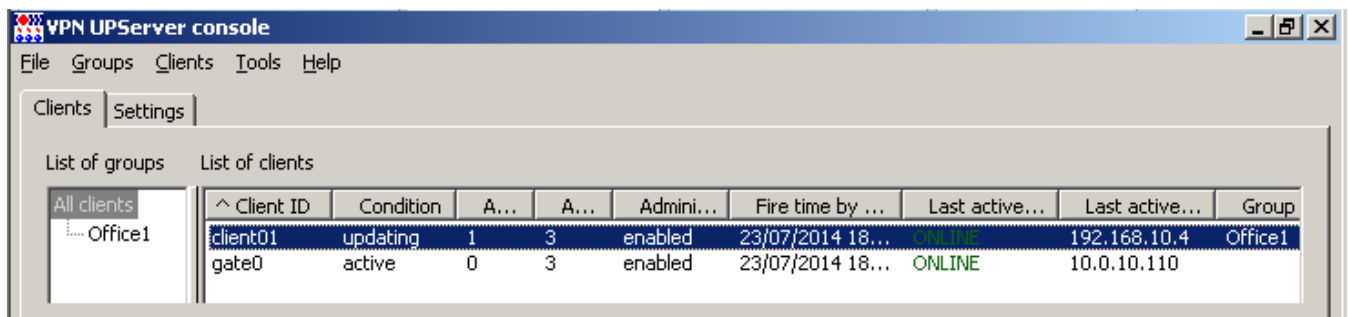


The 'Update client' dialog box contains the following fields and options:

- Client ID:** client01
- Creation time:** 7/25/2013 (calendar icon) 4:33:31 PM (time picker)
- Product package:** [empty] E ...
- ☒ Do not send binary code of product package
- UPAgent folder:** [empty] ...
- UPAgent settings:** [empty] ...
- Extended data:** C:\test [empty]
- ☐ Send current UPServer CA certificates to client
- Buttons:** OK, Cancel

Рисунок 165

5. После нажатия **OK** будет создано обновление для клиента `client01`, которое будет скачено Клиентом управления и применено после получения разрешения.



The screenshot shows the 'VPN UPServer console' window with the 'Clients' tab selected. It displays a list of clients under the 'List of clients' header.

Client ID	Condition	A...	A...	Admini...	Fire time by ...	Last active...	Last active...	Group
client01	updating	1	3	enabled	23/07/2014 18...	ONLINE	192.168.10.4	Office1
gate0	active	0	3	enabled	23/07/2014 18...	ONLINE	10.0.10.110	

Рисунок 166

6. Результат применения команды **hostname** можно увидеть во вкладке **UpLog** для данного клиента на Сервере управления. В данном примере – это «vpnclient01» (Рисунок 167).

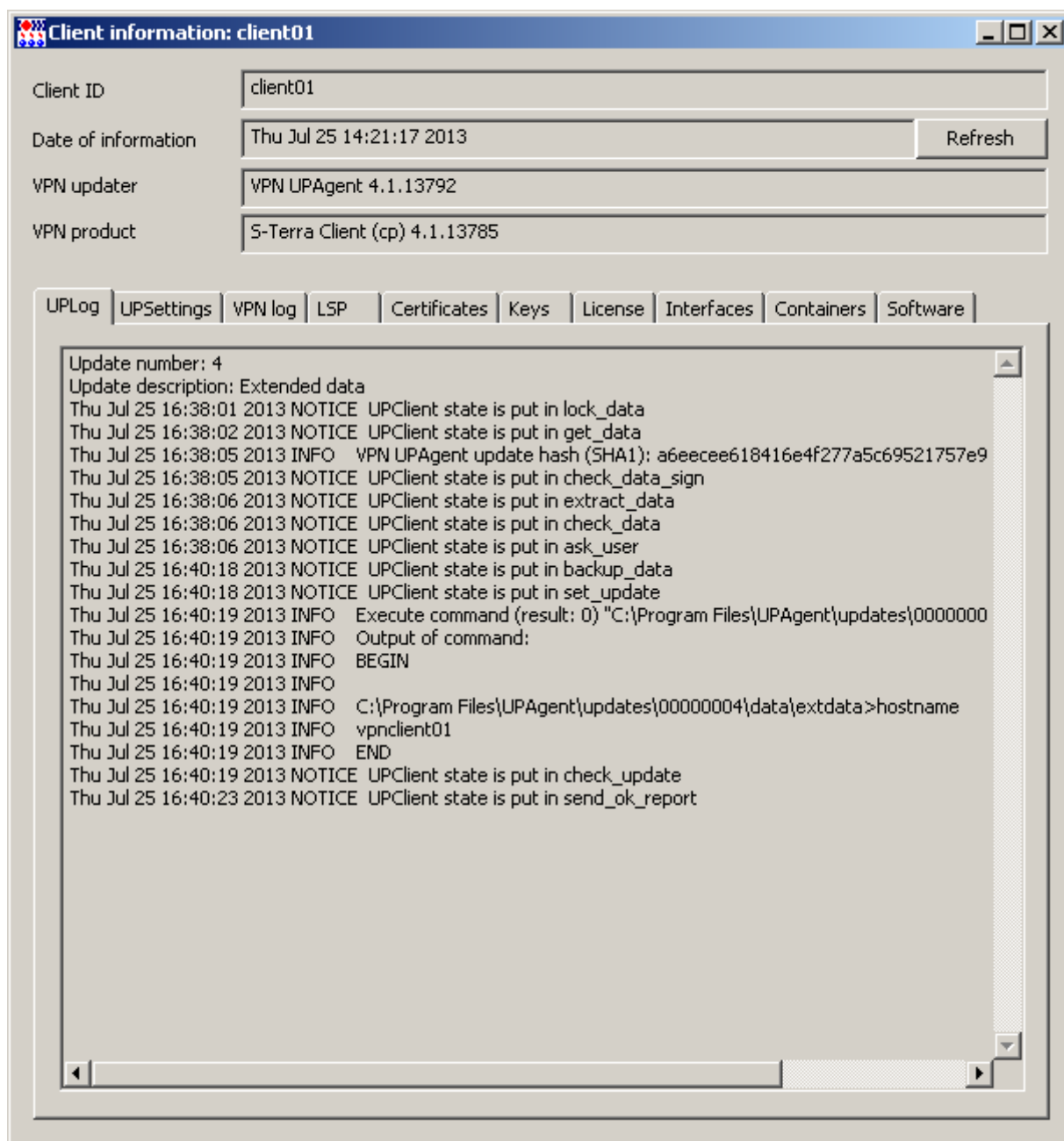


Рисунок 167

## 11. Сценарий создания клонов клиента Bel VPN Gate 4.1

Предположим, что имеется устройство с установленной ОС и продуктом Bel VPN Gate 4.1. Данный сценарий описывает создание базового проекта, включающего настройки продукта Bel VPN Gate 4.1, лицензии, сертификаты, контейнер с ключевой парой, а на его основе создание клона базового проекта, отличающегося локальным сертификатом, лицензиями, контейнером и IP-адресами.

### 11.1. Создание базового проекта

1. Задайте настройки продукта S-Terra Gate для базового проекта `base_gate.pvd`, который будет использоваться для клонирования. Для этого в меню **Tools** выберите предложение **VPN data maker** (Рисунок 168).

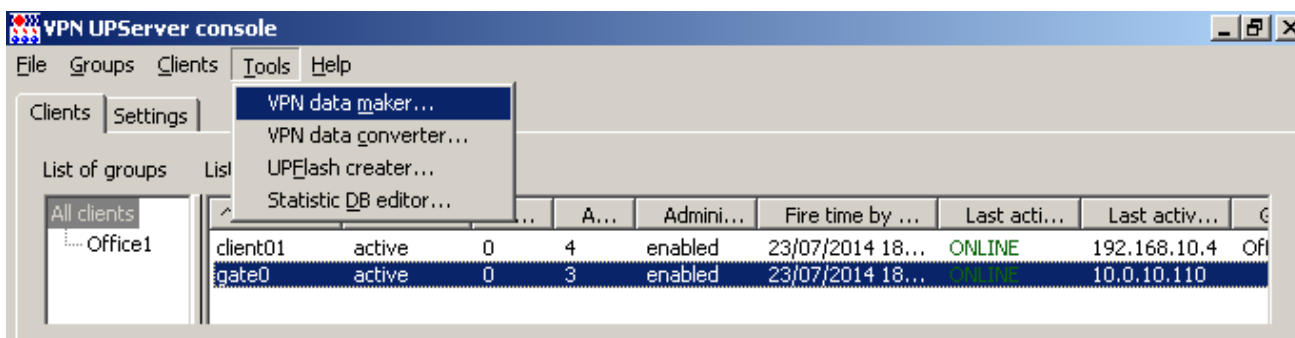


Рисунок 168

2. Выберите продукт Bel VPN Gate 4.1 и CryptoPro, нажмите кнопку **Run Wizard**.

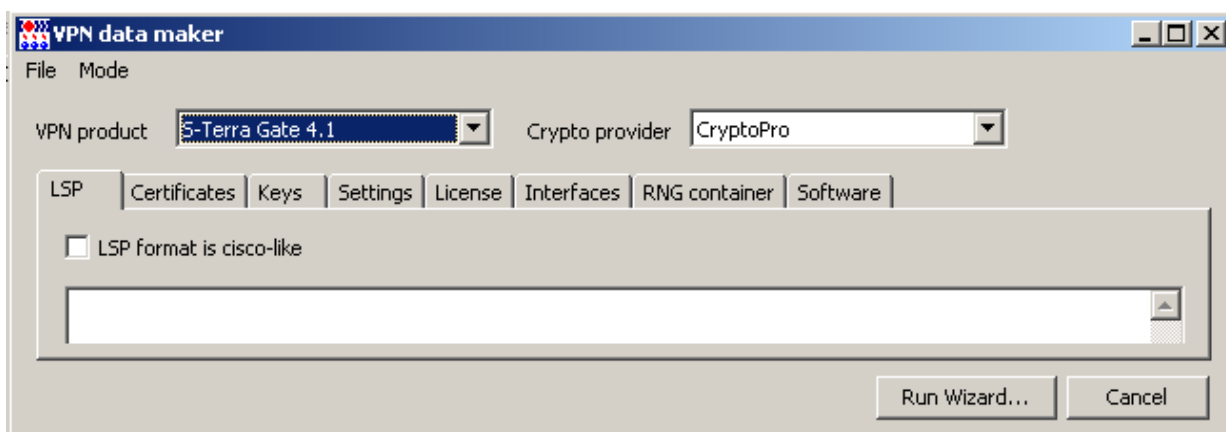


Рисунок 169

3. В следующем окне укажите CA и локальный сертификат, который у вас есть или создайте новый с полем **Subject**, например, `base_clone0`, а также укажите имя контейнера на жестком диске нового устройства (клона), в который будет скопирован контейнер с USB-флеш. Пароль на контейнер должен быть пустым (Рисунок 170).

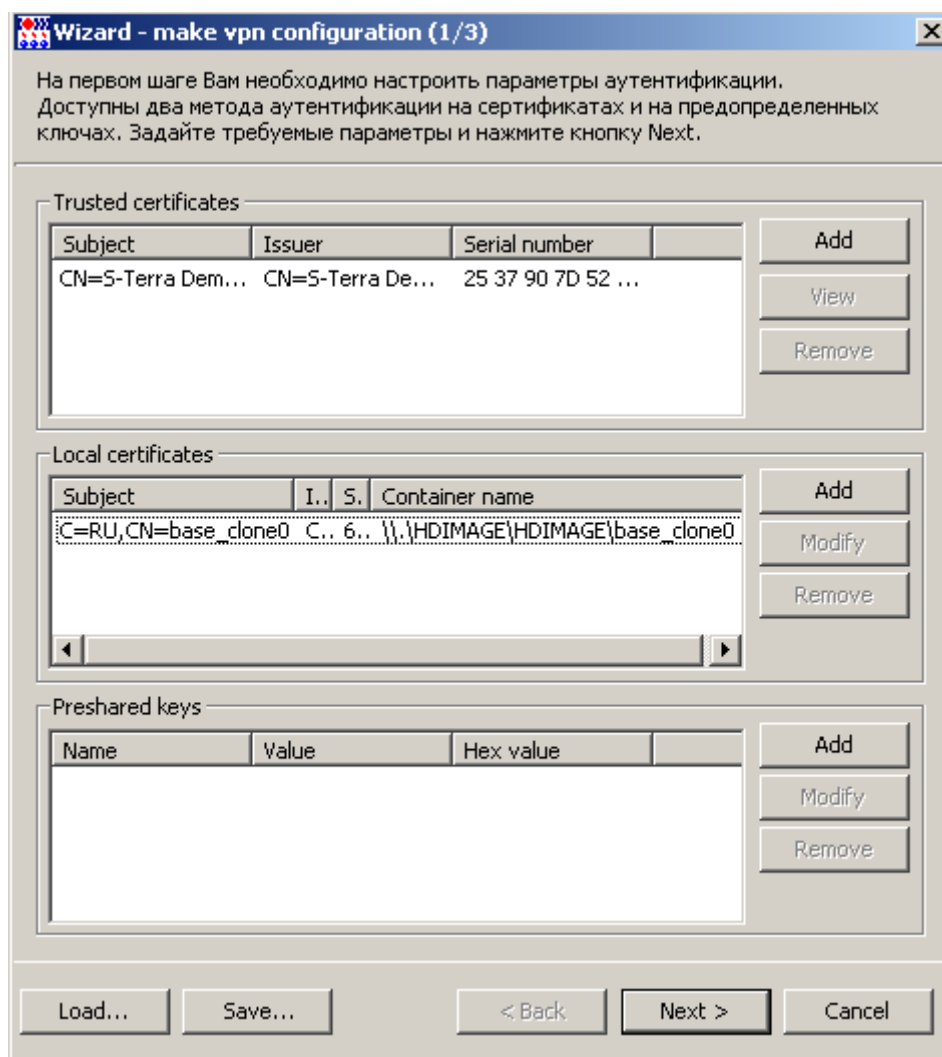


Рисунок 170

4. Создайте правило для пропускания трафика от любого управляемого устройства к Серверу управления, трафик между управляемым устройством и центральным шлюзом должен быть защищен, для аутентификации шлюза используется локальный сертификат. Правило привязывается к внешнему интерфейсу с именем FastEthernet0/0 (Рисунок 171).

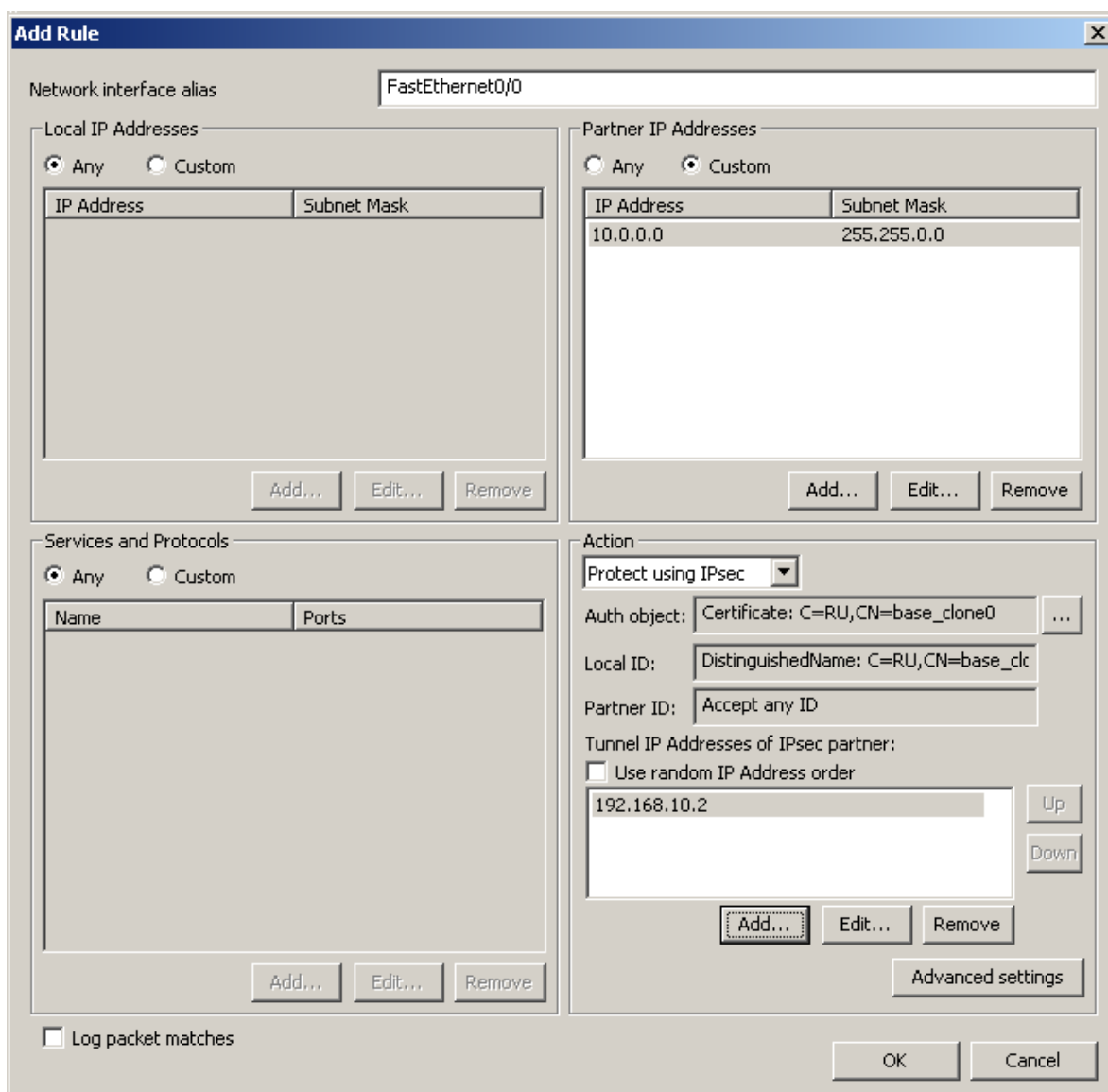


Рисунок 171

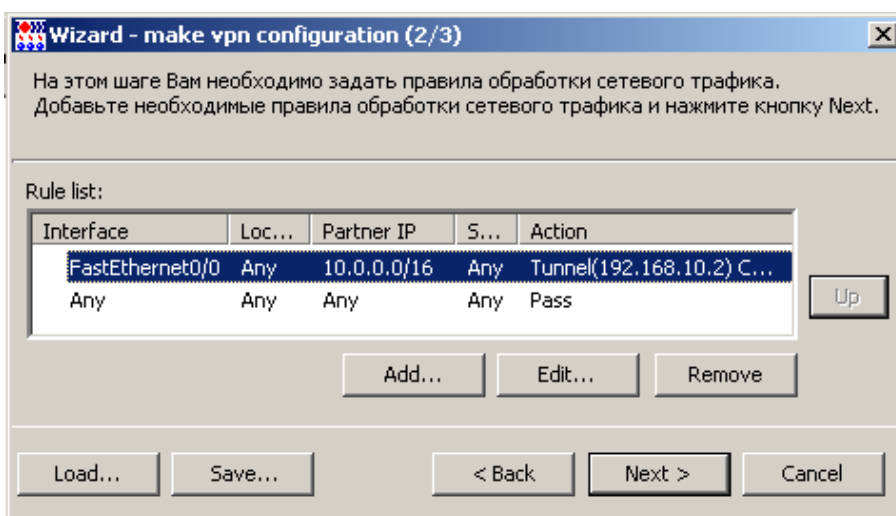


Рисунок 172

5. Увеличьте приоритет созданного правила (Рисунок 172).
6. Введите данные лицензий на Bel VPN Gate и нажмите кнопку **Finish**.

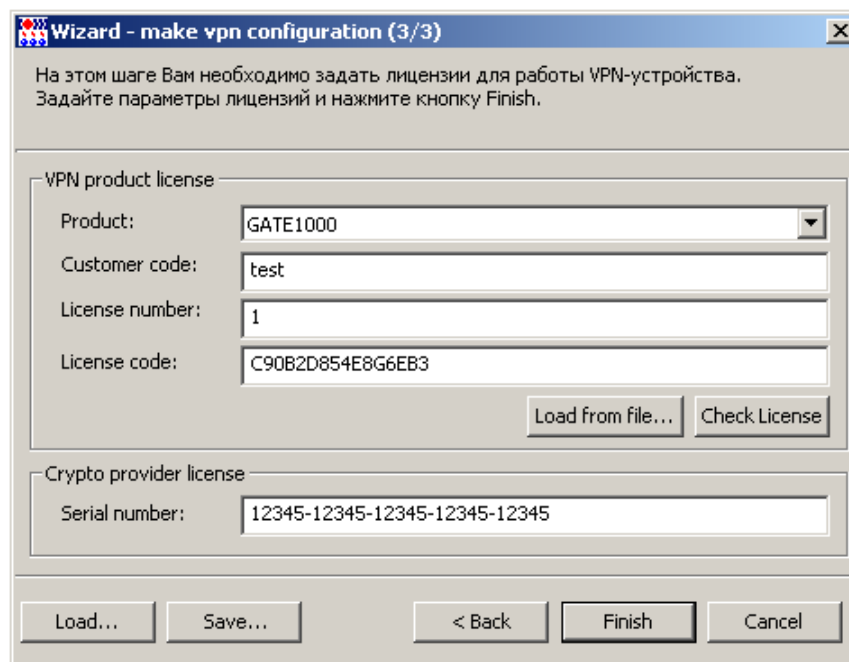


Рисунок 173

7. Таким образом, все выставленные настройки отражены во вкладках. Для того, чтобы в базовом проекте конфигурация не зависела от полей локального сертификата, во вкладке **LSP** следует следующие структуры (Рисунок 174):

```
IdentityEntry local_auth_identity_01(
    DistinguishedName *= CertDescription(
        Subject *= COMPLETE, "C=RU, CN=base_clone0"
    )
)
CertDescription local_cert_dsc_01(
    FingerprintMD5 = "6B681CA341C8D7E8AE8DD4438DEAC243"
    Issuer *= COMPLETE, "CN=S-Terra Demo CA"
    SerialNumber = "612D03BE000000000000D"
    Subject *= COMPLETE, "C=RU, CN=base_clone0"
)
```

заменить на строки:

```
IdentityEntry local_auth_identity_01(
    DistinguishedName *= USER_SPECIFIC_DATA
)
CertDescription local_cert_dsc_01(
)
```

В этом случае любой локальный сертификат, лежащий в базе продукта, будет использован для аутентификации. Необходимо, чтобы в базе управляемого устройства лежал только один локальный сертификат.

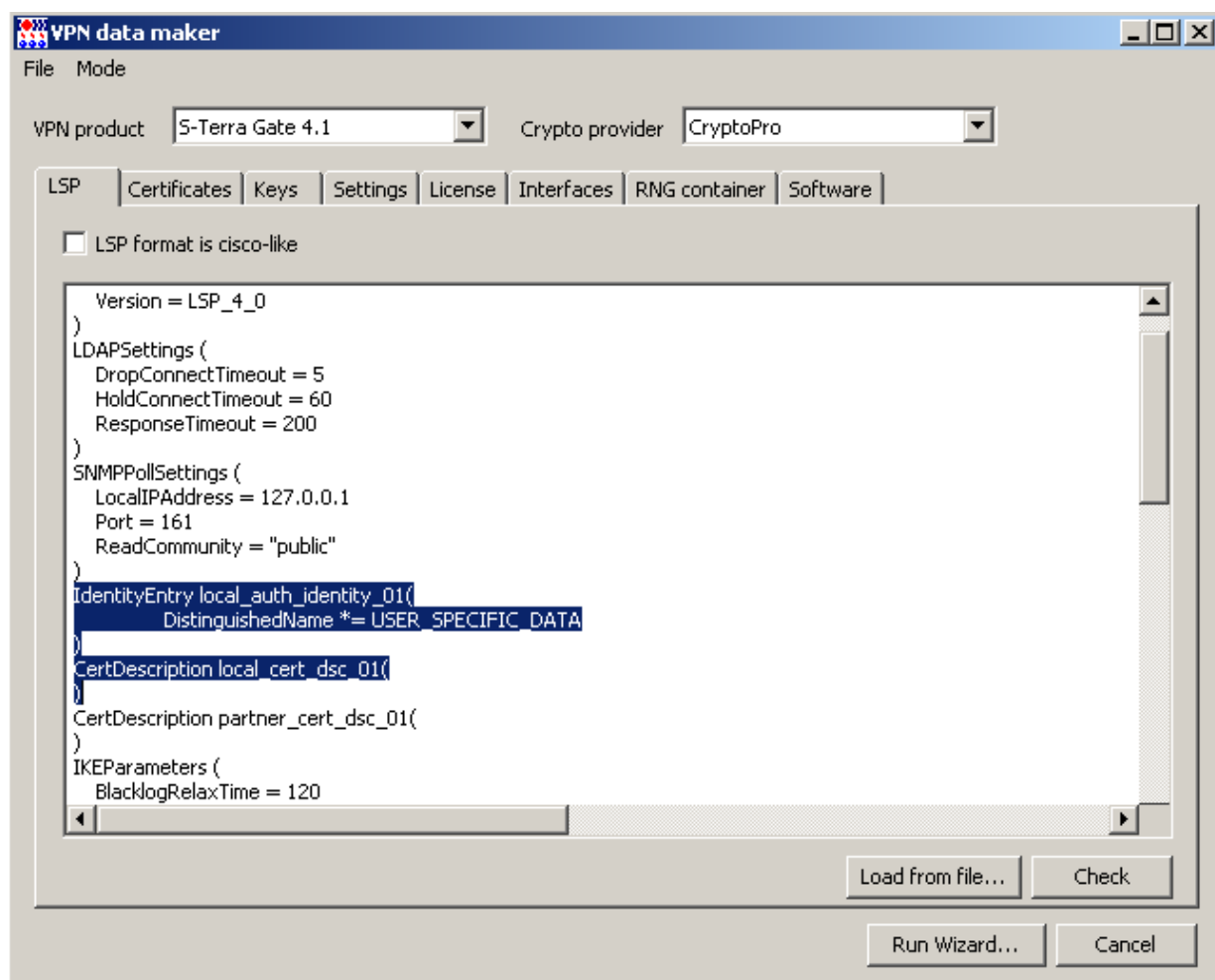


Рисунок 174

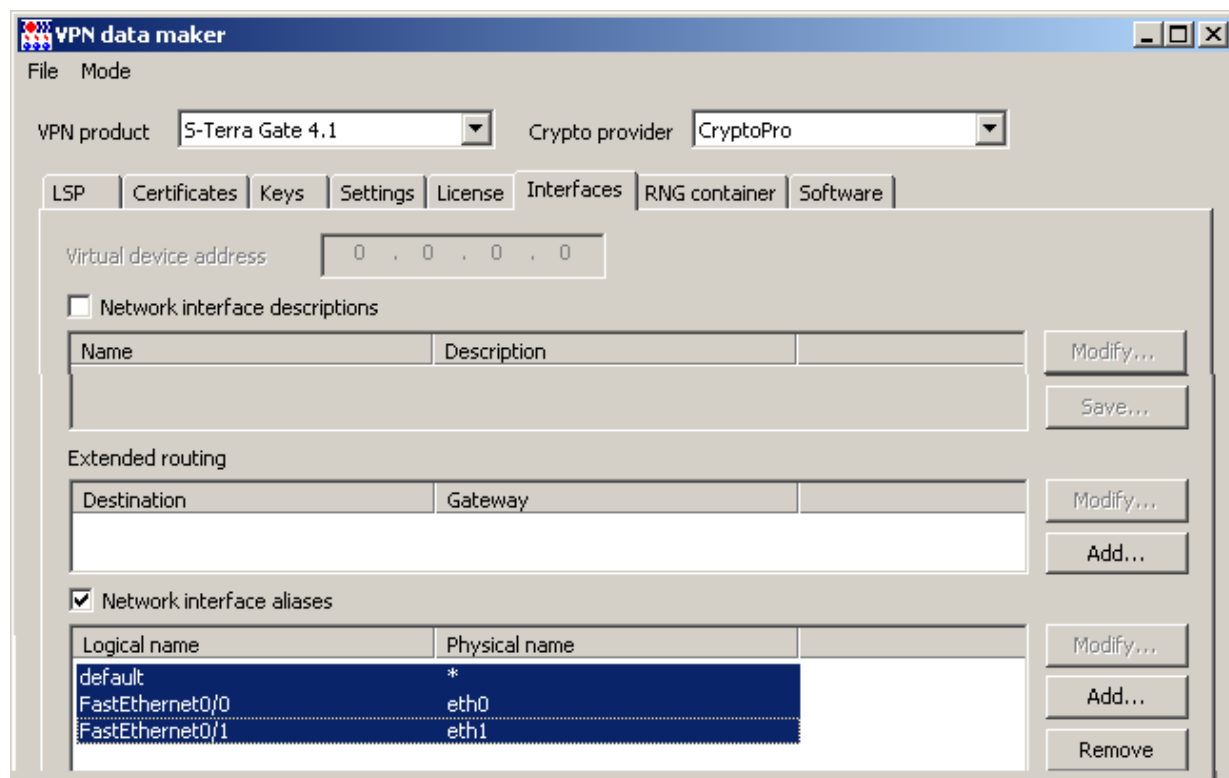


Рисунок 175

8. Далее во вкладке **Interfaces** задайте алиасы сетевых интерфейсов. Допустим, на устройствах, на которые будут устанавливаться клоны, имеется по 3 сетевых интерфейса с именами – eth0, eth1, eth2 (Рисунок 175).
9. Получен базовый проект, сохраните его в файл на Сервере управления, выбрав в меню **File** предложение **Save as....**

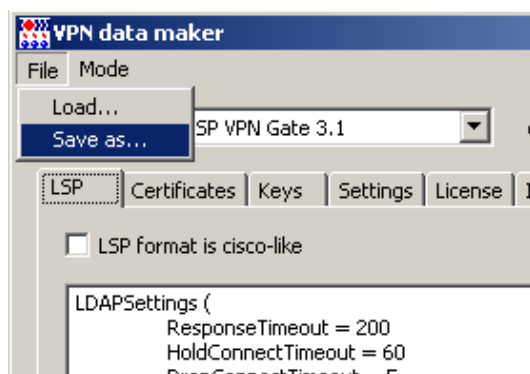


Рисунок 176

10. Сохраните базовый проект в каталоге Clone под именем, например, base\_gate.vpd.

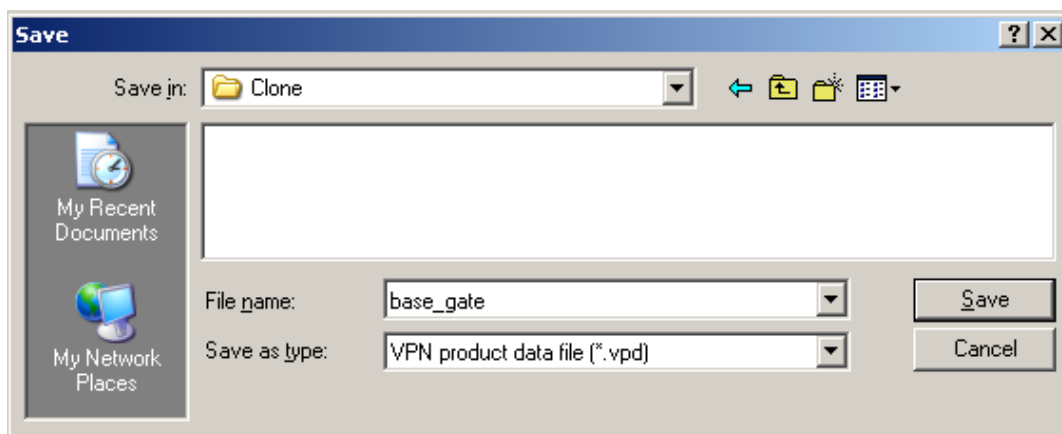


Рисунок 177

## 11.2. Подготовка материалов для клонов

Далее следует подготовить материал для создания клонов на основе базового проекта – для каждого управляемого устройства создайте локальный сертификат, политику безопасности (LSP), файлы с лицензией на Bel VPN Gate, сохранив все это на Сервере управления. Все эти действия описываются далее.

11. Подключите USB-флеш к Серверу управления. Узнайте имя доступной USB-флеш, на которую будут записываться подготовленные скрипты и контейнер, выполнив команду:
12. Создайте ключевую пару, запрос на локальный сертификат и отправьте его в УЦ. Если УЦ настроен на автоматическое издание сертификатов при получении запросов, то созданный сертификат будет установлен в контейнер с ключевой парой на USB-флеш, например, FAT12\_E, которую укажите в команде, например, для клиента gate01:

```
"C:\Program Files\Crypto Pro\CSP\cryptcp.exe" -creatcert -dn "CN=gate01" -both -km -cont "\\.\FAT12_E\gate01" -expirt -CA http://10.0.10.111/certsrv -dm
```

13. Создайте на Сервере управления каталог, например, C:\Clone. Скопируйте созданный локальный сертификат в кодировке DER из контейнера в файл C:\Clone\gate01.cer:

```
"C:\Program Files\Crypto Pro\CSP\cryptcp.exe" -CSPcert -cont "\\.\FAT12_E\gate01" -df C:\Clone\gate01.cer -der
```



14. Создайте файл C:\Clone\st\_gate01.lic с лицензией на продукт Bel VPN Gate, например:

```
[license]
CustomerCode=test
ProductCode=GATE1000
LicenseNumber=1
LicenseCode=01234567890ABCDEF
```

15. Создайте файл алиасов сетевых интерфейсов C:\Clone\ia\_gate01.txt, например:

```
FastEthernet0/0=eth0
FastEthernet0/1=eth1
FastEthernet0/0=eth2
```

16. Создайте файл с настройками сетевых интерфейсов C:\Clone\ifdesc\_gate01.txt, например,

```
[ExtendedDeviceRoutes]
!Route to net of UPServer (10.0.0.0/16) via gate (192.168.10.2)
Route_0=10.0.0.0/16 192.168.10.2

!Description eth0
[IF_eth0]
STATE=UP
Address_0=192.168.10.8/24

!Description eth1
[IF_eth1]
STATE=UP
Address_0=172.16.1.5/12

!Description eth2
[IF_eth2]
STATE=UP
Address_0=172.16.2.5/12
```

17. Создайте файл нового проекта C:\Clone\gate01.pvd на основе базового проекта, выполнив команду:

```
"C:\Program Files\S-Terra\S-Terra KP\vpnmaker.exe" replace -fi
C:\Clone\base_gate.vpd -fo C:\Clone\gate01.vpd -lic C:\Clone\st_gate01.lic -
cryptolic C:\Clone\cp_gate01.lic -cert C:\Clone\gate01.cer -certkey
\\.\HDIMAGE\HDIMAGE\vpngate01 -certkeypwd 12345678 -ifaliases
C:\Clone\ia_gate01.txt -ifdesc C:\Clone\ifdesc_gate01.txt
```

где

\\.\HDIMAGE\HDIMAGE\vpngate01 – имя контейнера на жестком диске нового устройства, в который будет скопирован контейнер gate01 с USB-флеш. Контейнер на USB-флеш будет найден по локальному сертификату.

certkeypwd – пароль на скопированный контейнер на жестком диске.

18. Создайте на Сервере управления учетную запись клиента gate01 для нового проекта, а потом переведите его в состояние **Enable**:

```
"C:\Program Files\S-Terra\S-Terra KP\upmgr.exe" create -i gate01 -p
C:\Clone\gate01.vpd
"C:\Program Files\S-Terra\S-Terra KP\upmgr.exe" enable -i gate01
```

19. Создайте два скрипта для настройки Bel VPN Gate и инсталляции (инициализации) Клиента управления на управляемом устройстве, сохранив их на USB-флеш в каталоге `gate01`:

```
mkdir E:\gate01
"C:\Program Files\S-Terra\S-Terra KP\upmgr.exe" get -i gate01 -d E:\gate01
```

В каталоге `gate01` будут сохранены два скрипта:

`setup_product.sh` – скрипт для настройки продукта Bel VPN Gate

`setup_upagent.sh` – скрипт для инсталляции (инициализации) продукта Bel VPN KP (Клиент управления).

20. Скопируйте дистрибутив Клиента управления с Сервера управления на USB-флеш:

```
C:\Program Files\S-Terra\S-Terra KP\upagent\<OS>\vpnapagent.tar
```

Таким образом, на USB-флеш записаны два скрипта и контейнер с ключевой парой.

### 11.3. Настройка управляемого устройства

1. На управляемом устройстве настройте на интерфейсах IP-адреса и сохраните их значения в системе, например:

```
ifconfig eth0 192.168.10.8/24
ifconfig eth1 172.16.1.5/12
ifconfig eth1 172.16.2.5/12
/bin/nf_saveif_all.sh
```

2. Если на управляемом устройстве отсутствует дистрибутив продукта VPN UPAgent, скопируйте его с USB-флеш в каталог `/packages`:

```
mkdir /packages
cd /packages
tar -xvf /mnt/vpnupagent.tar
```

3. Запустите скрипт для инсталляции Клиента управления Bel VPN KP:

```
/mnt/gate01/setup_upagent.sh
```

4. Запустите скрипт для настройки Bel VPN Gate 4.1:

```
/mnt/gate01/setup_product.sh
```

5. Выполните окончательную инициализацию продукта Bel VPN Gate 4.1:

```
/opt/VPNagent/bin/init.sh
```

6. По завершению инициализации управляемое устройство `gate01` перейдет в состояние `active`.

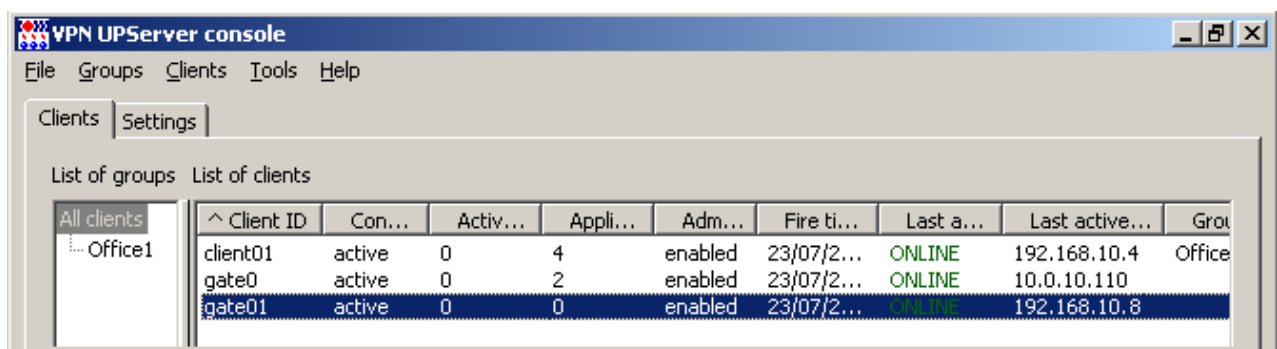


Рисунок 178

7. Не забудьте настроить маршрут в подсеть с адресом `10.0.0.0/16`, в которой размещен Сервер управления:

```
route add -net 10.0.0.0/16 gw 192.168.10.2
```

## 12. Сценарий включения в систему управления работающего устройства с Bel VPN Gate/Client

Имеется устройство с установленной ОС и продуктом Bel VPN Gate/Client, которое настроено сторонними методами и включено, например, в подсеть 192.168.10.0/24 с адресом 192.168.10.6. Устройство настроено так, что может создавать защищенные соединения с партнерами в сети 10.0.0.0/16, в которой также размещен Сервер управления. Данный сценарий описывает включение работающего устройства в систему управления с использованием Сервера управления.

1. На Сервере управления создайте учетную запись клиента для работающего устройства, например, с установленным продуктом Bel VPN Gate Gate - work\_gate02.

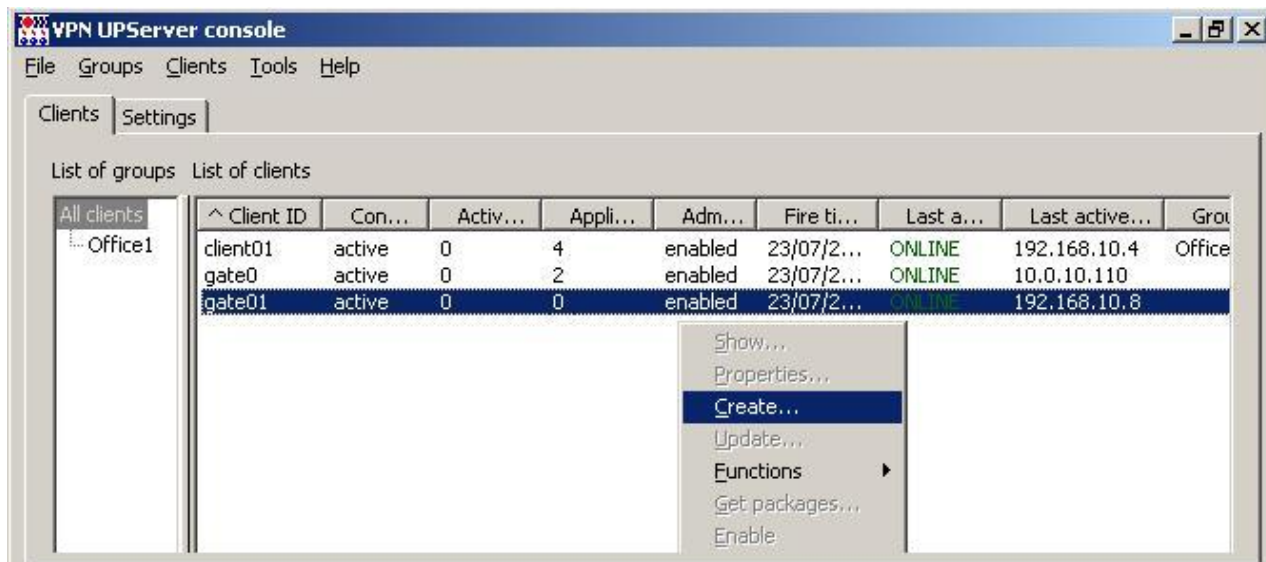


Рисунок 179

2. Введите уникальное имя клиента и нажмите кнопку **E**.

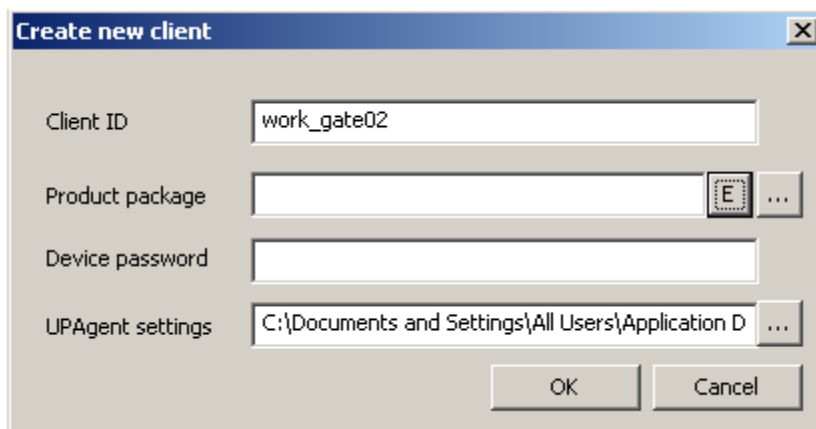


Рисунок 180

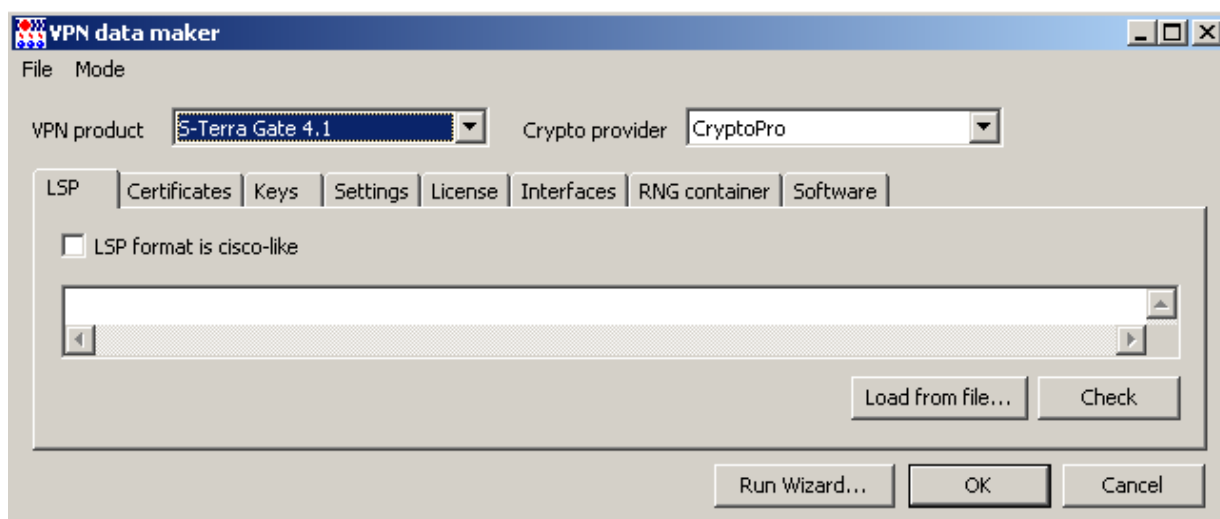


Рисунок 181

3. Выберите продукт, установленный на работающем устройстве, Avest и нажмите кнопку **OK**.
4. Создается фиктивный проект, настройки на устройстве уже заданы, поэтому в предупреждении нажмите кнопку **OK**.

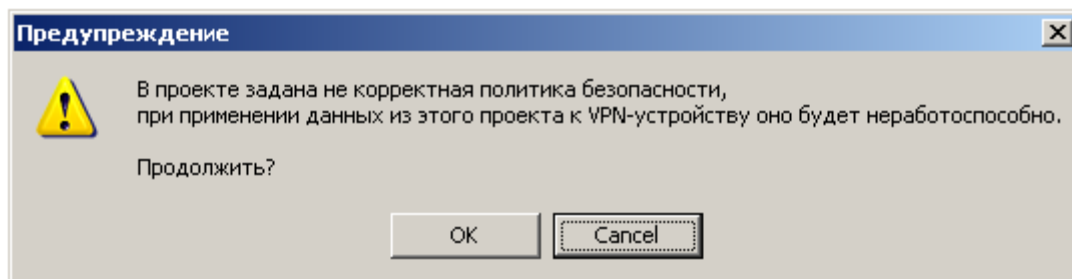


Рисунок 182

5. В следующем предупреждении также нажмите **OK**.

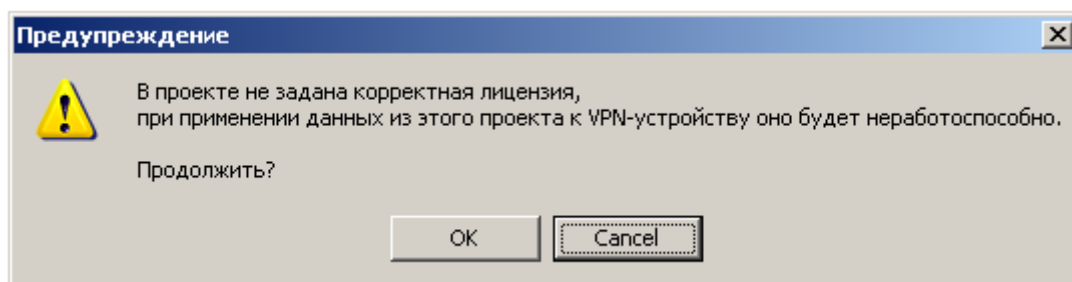


Рисунок 183

6. В окне создания клиента нажмите **OK**.

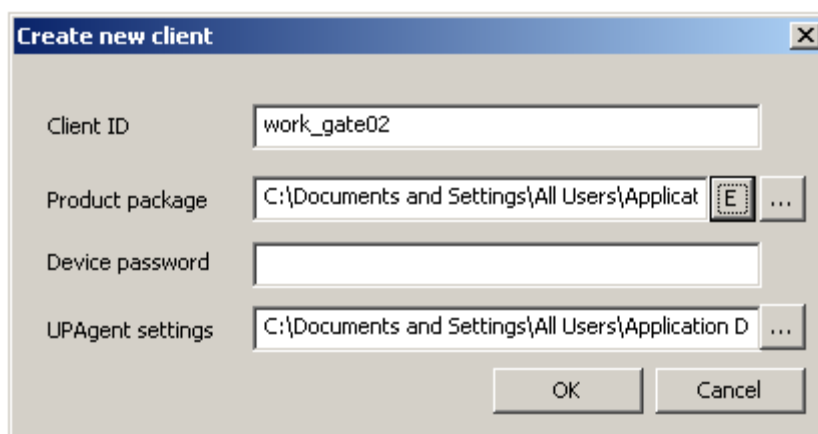


Рисунок 184

7. Для нового клиента в контекстном меню выберите операцию **Enable**, а затем **Get packages** для создания скриптов.

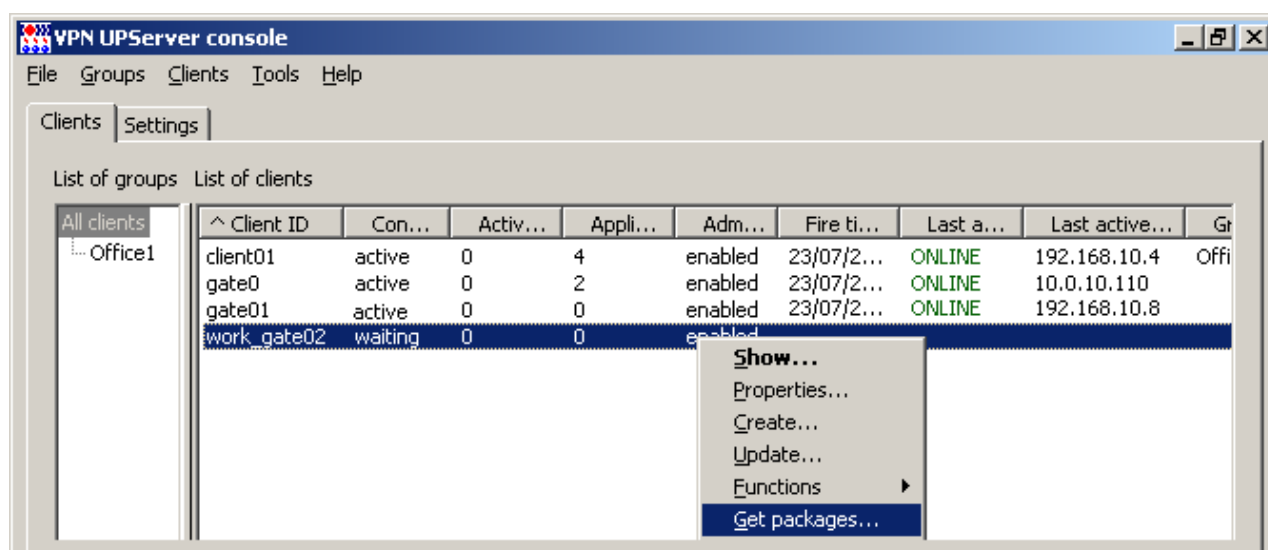


Рисунок 185

8. Выберите каталог для сохранения настроечных скриптов и нажмите **OK**.

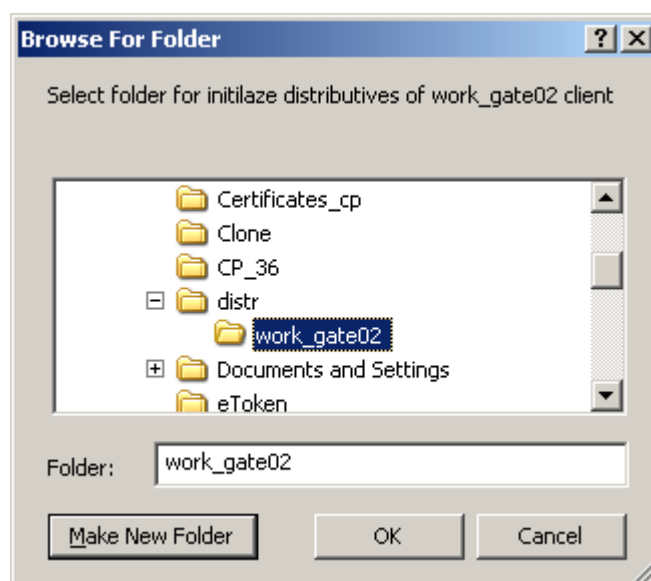


Рисунок 186

9. Два скрипта созданы. Требуется только один скрипт `setup_upagent.sh` для инсталляции (инициализации) Клиента управления, продукт Bel VPN Gate уже настроен.

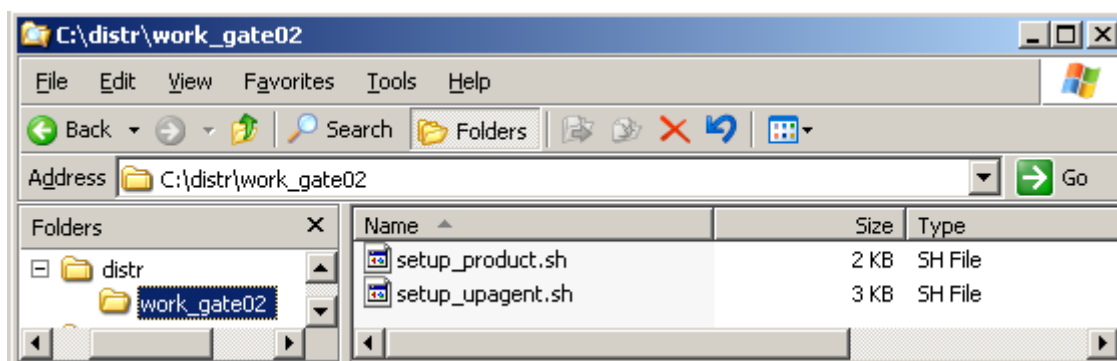


Рисунок 187

10. Доставьте скрипт `setup_upagent.sh` на работающий шлюз с адресом 192.168.10.6, например, с использованием утилиты `pscp` в предварительно созданный каталог `/tmp`:

```
pscp setup_upagent.sh root@192.168.10.6:/tmp
```

11. Измените права доступа к скрипту, выполнив локально на шлюзе команду:

```
chmod +x /tmp/setup_upagent.sh
```

12. Запустите локально скрипт на выполнение:

```
/tmp/setup_upagent.sh
```

13. По окончании инициализации Клиента управления запустите команду для сбора информации с работающего устройства и сохраните ее в файл проекта `/tmp/work_gate02.vpd`:

```
/opt/UPAgent/bin/uprun vpnupdater backup -u /tmp/work_gate02.vpd -hot_mode
```

14. Полученный файл проекта `work_gate02.vpd` доставьте на Сервер управления по заслуживающему доверия каналу связи, так как он может содержать информацию о паролях и лицензиях. Например, на Сервере управления запустите команду, предварительно создав на нем каталог `Projects`:

```
pscp root@192.168.10.6:/tmp/work_gate02.vpd C:\Projects
```

15. Создайте обновление для данного устройства, включающее полученный проект, выбрав предложение **Update**.

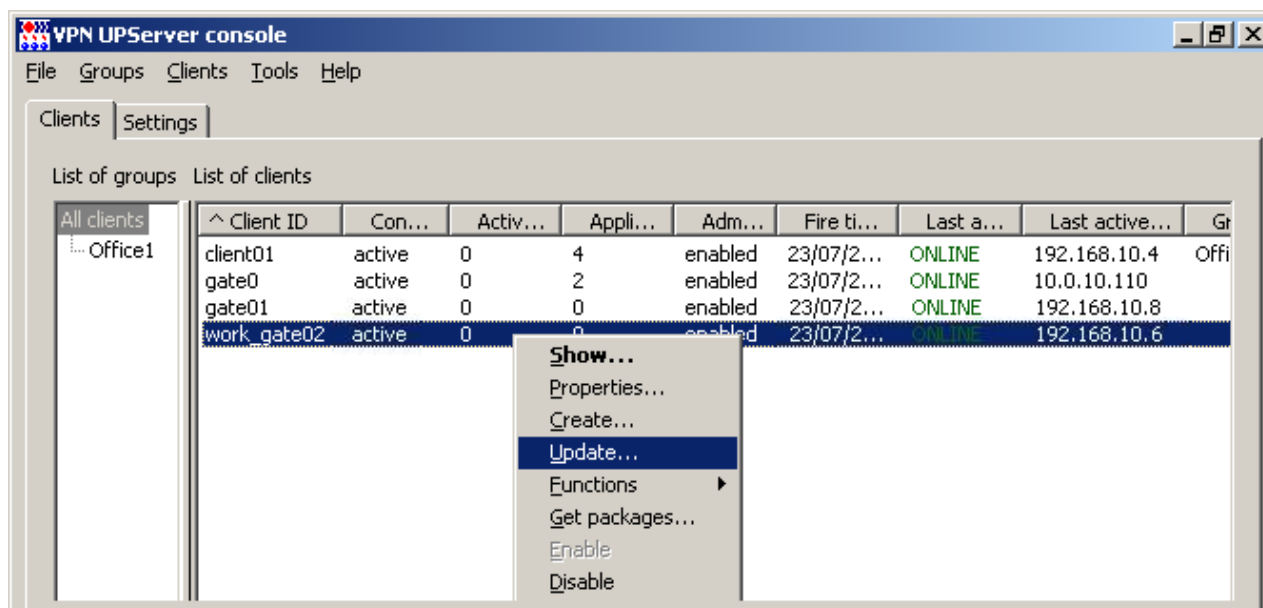


Рисунок 188

16. В окне **Update client** в поле **Product package** укажите файл с полученным проектом и нажмите кнопку **OK**.

Рисунок 189

17. Обновление будет создано для данного клиента `work_gate02` и применено.

Client ID	Con...	Activ...	Appli...	Adm...	Fire ti...	Last a...	Last active...	Gr
client01	active	0	4	enabled	23/07/2...	ONLINE	192.168.10.4	Offi
gate0	active	0	2	enabled	23/07/2...	ONLINE	10.0.10.110	
gate01	active	0	0	enabled	23/07/2...	ONLINE	192.168.10.8	
work_gate02	active	0	1	enabled	23/07/2...	ONLINE	192.168.10.6	

Рисунок 190

В результате Сервер управления располагает достоверными данными о работающем устройстве. Данный сценарий может быть применен для синхронизации данных между Сервером управления и устройством, настройка которого осуществлялась сторонними методами.



## 13. Групповые операции на Сервере управления

В таблице на Сервере управления можно выделить несколько клиентов и применить к ним операции меню **Clients**, за исключением **Create** и **Get packages**.

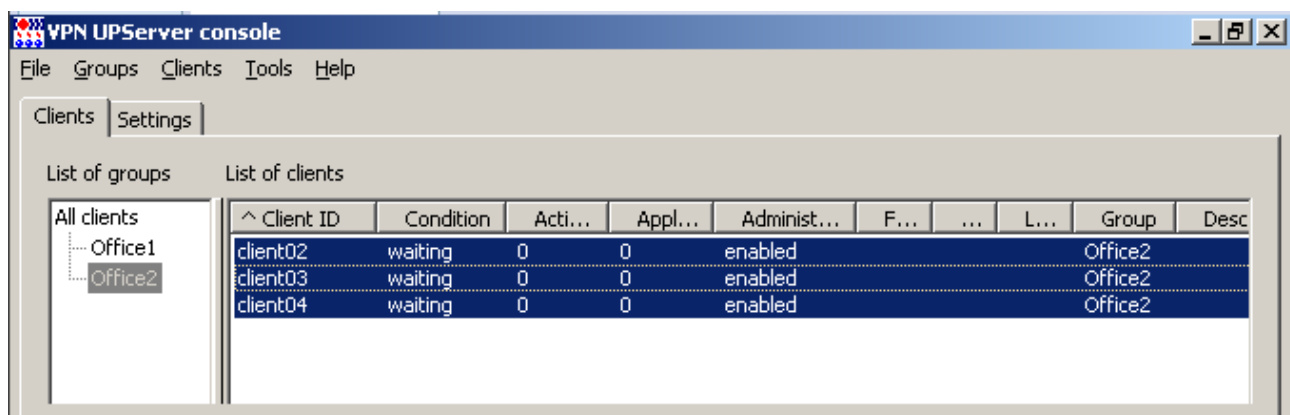


Рисунок 191

Каждый клиент на Сервере управления создается отдельно и для каждого клиента скрипты Клиента управления и Bel VPN Gate/Client также создаются отдельно.

Остальные операции могут применяться к любой выделенной группе клиентов.

Подробно операции меню **Clients** описаны в разделе «[Меню Clients](#)» главы «[Описание интерфейса Сервера управления](#)».

При выборе операции **Update** для нескольких клиентов будут созданы одинаковые обновления. После применения этих обновлений клиенты будут иметь, например, одинаковую политику безопасности, одинаковый список predetermined ключей, свой локальный сертификат. Если в базе продукта лежит список локальных сертификатов, клиент не сможет создать соединение с партнером, так как будет использоваться первый сертификат списка. Чтобы избежать таких проблем с локальными сертификатами, используйте **шаблон проекта**, при котором происходит отбор локального сертификата из списка для каждого клиента при обновлении. Такой отбор локального сертификата возможен только при наличии на управляемом устройстве запроса на локальный сертификат, который и будет использоваться для поиска нужного сертификата из списка.

### 13.1. Создание шаблона проекта

1. Не выделяя в таблице клиентов, в меню **Tools** выберите предложение **VPN data maker**.

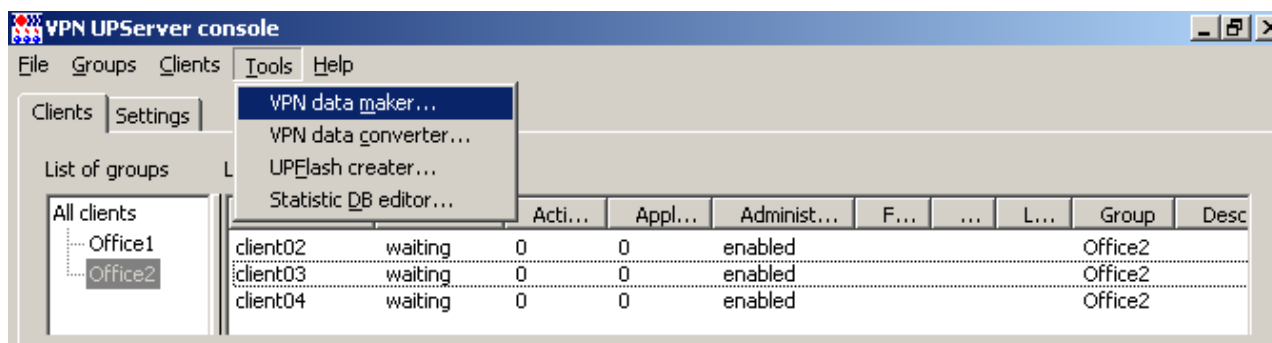


Рисунок 192

2. В открывшемся окне **VPN data maker** заполните необходимые вкладки (или используйте [Run Wizard](#)) для настройки продукта Bel VPN Gate/Client.

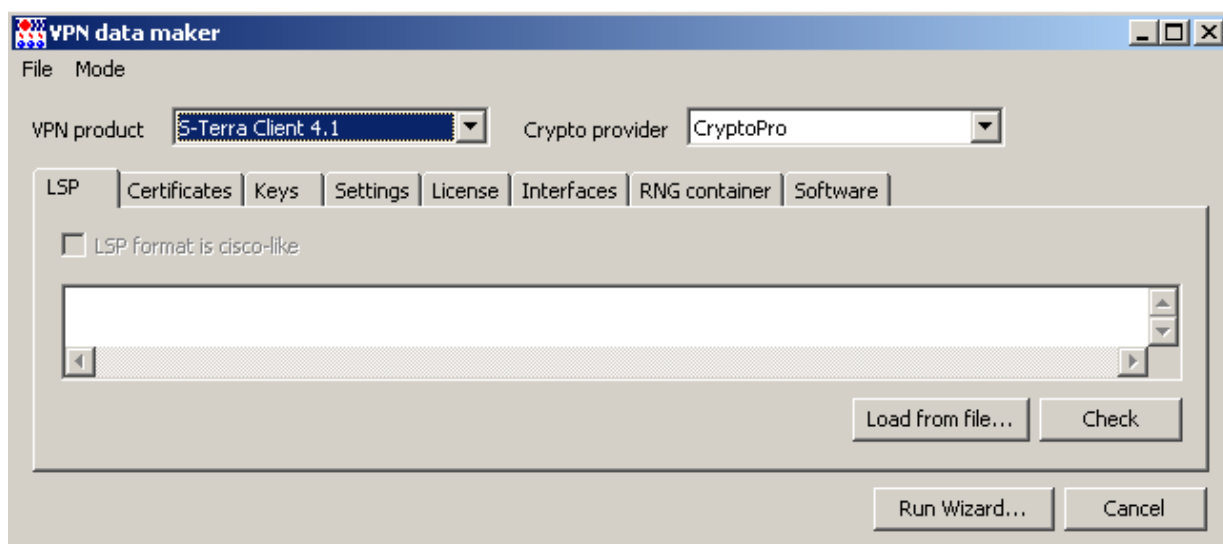


Рисунок 193

- Во вкладке **Cerificates** можно задать [список локальных сертификатов](#), для которых были созданы запросы на клиентах, список сертификатов партнеров, список удаленных сертификатов (CRL).

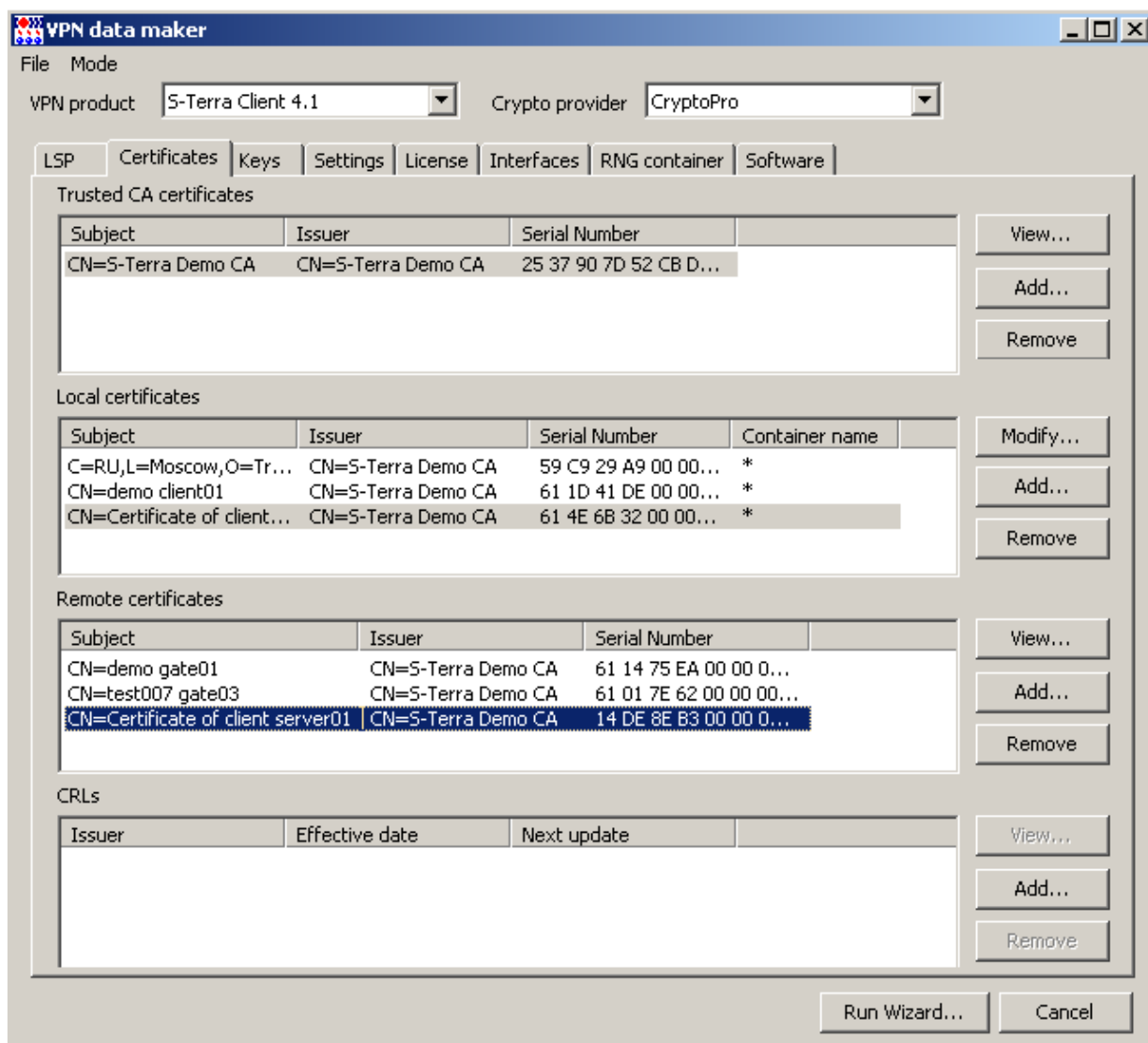


Рисунок 194

При задании локальных сертификатов появляется окно **Certificate description**, в котором надо указать имя контейнера и пароль к нему на управляемом устройстве. В этих двух полях можно указать значение «\*», которое при применении обновления будет заменено на действительные значения.

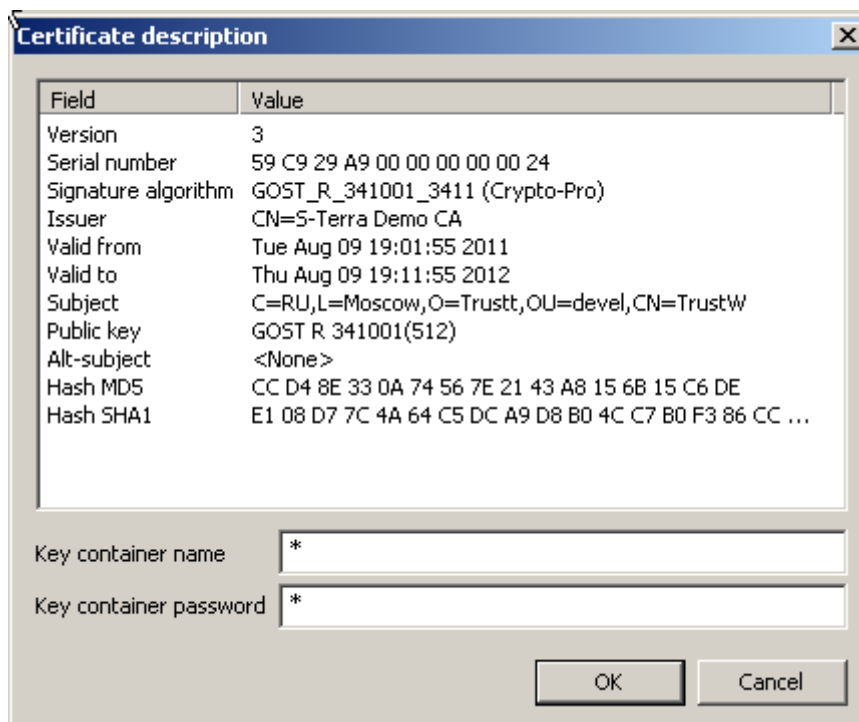


Рисунок 195

4. Заполнив вкладки, перейдите в режим шаблона проекта, выбрав в меню **Mode** предложение **Enable template mode**.

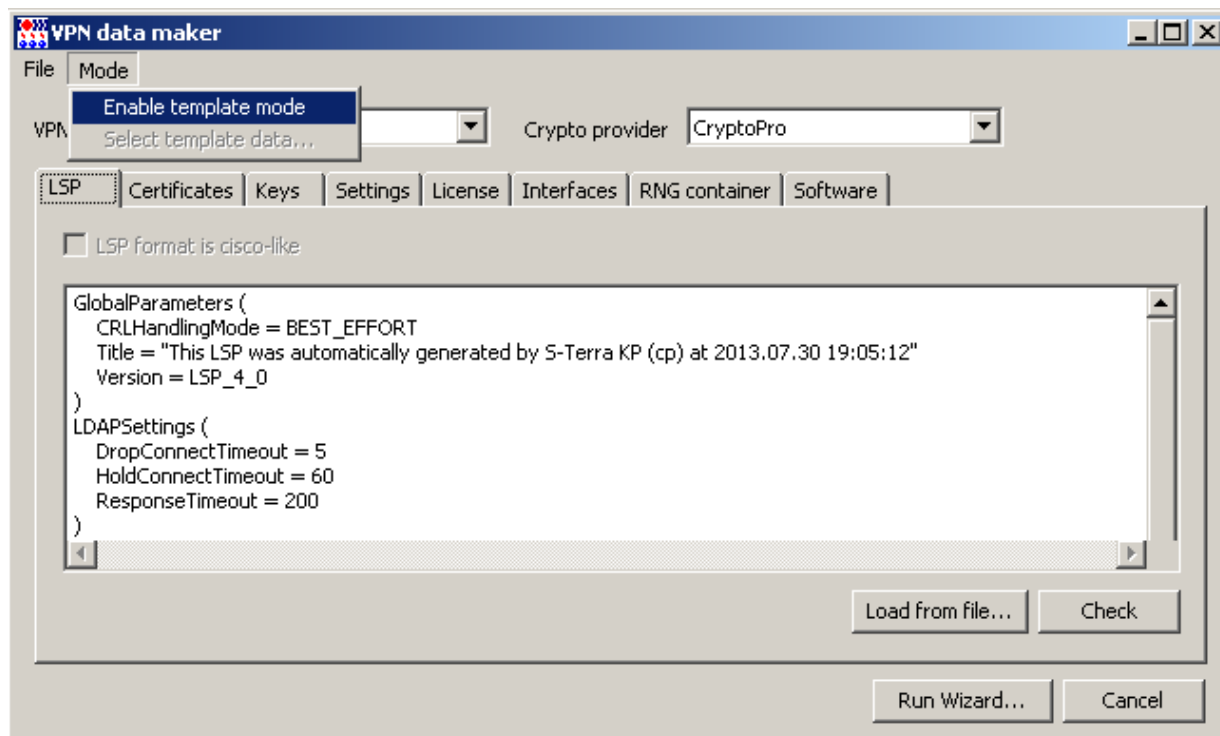


Рисунок 196

5. Затем в меню **Mode** выберите предложение **Select template data** (это предложение доступно только в режиме шаблона проекта).

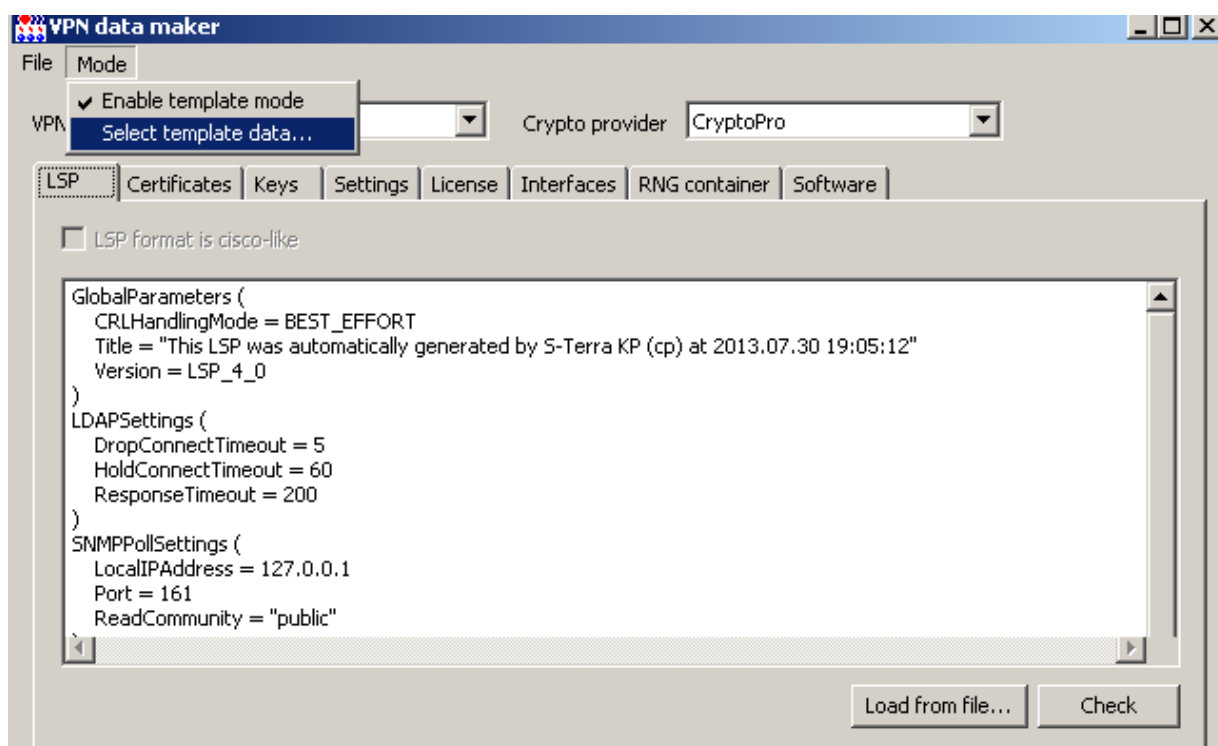


Рисунок 197

6. Появилось окно **Update data types** со списком данных, которые могут входить в шаблон проекта. Поставьте флажком данные, которые будут входить в шаблон. При применении обновления, созданного с использованием шаблона, только входящие в него данные будут изменяться на клиенте.

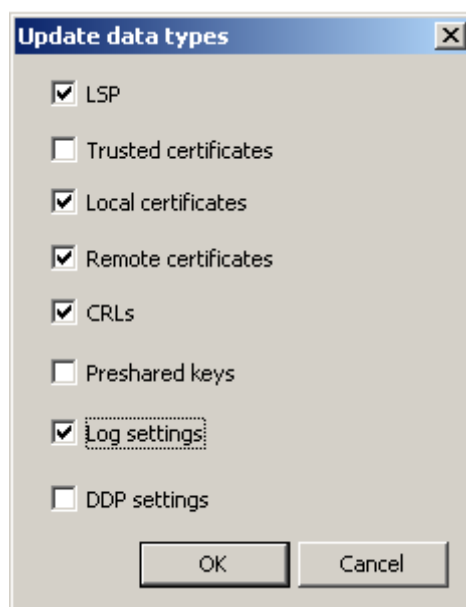


Рисунок 198

Состав окна **Update data types**:

**LSP** – при установке флажка локальная политика безопасности, указанная во вкладке **LSP**, будет входить в состав шаблона проекта

**Trusted certificates** – при установке флажка все доверенные CA-сертификаты, указанные во вкладке **Certificates**, будут входить в шаблон проекта

**Local certificates** – при установке флажка все локальные сертификаты, указанные во вкладке **Cerificates** в разделе **Local certificates**, будут входить в шаблон проекта

**Remote certificate** – при установке флажка все сертификаты партнеров, указанные во вкладке **Cerificates** в разделе **Remote certificates**, будут входить в шаблон проекта

**CRLs** – при установке флажка все списки отозванных сертификатов, указанные во вкладке **Cerificates** в разделе **CRLs**, будут входить в шаблон проекта

**Preshared keys** – при установке флажка все предопределенные ключи, указанные во вкладке **Keys**, будут входить в состав шаблона проекта

**Log settings** – при установке флажка настройки протоколирования, указанные во вкладке **Settings**, будут входить в шаблон проекта

**DDP settings** - при установке флажка политика DDP, указанная во вкладке **Settings**, будет входить в шаблон проекта.

Выбрав данные, которые будут входить в шаблон, нажмите кнопку **OK**.

7. Заполнив ранее вкладки для этих данных, сохраните созданный шаблон в файл, используя предложение **Save as** меню **File**.

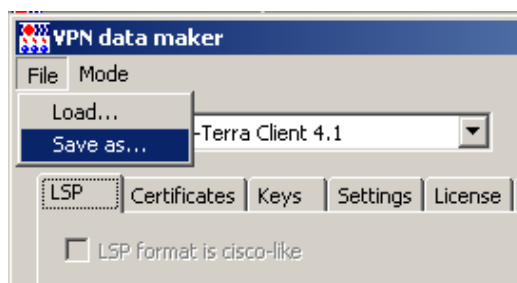


Рисунок 199

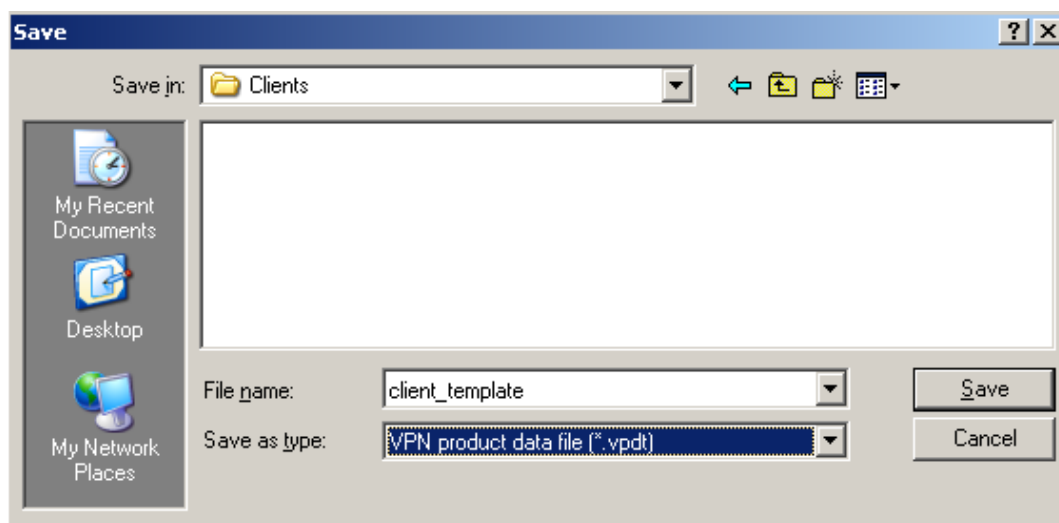


Рисунок 200

## 13.2. Использование шаблона проекта

Шаблон проекта удобно использовать при создании обновления сразу для нескольких клиентов.

1. Для этого выделите в таблице несколько клиентов, в контекстном меню выберите предложение **Update**.

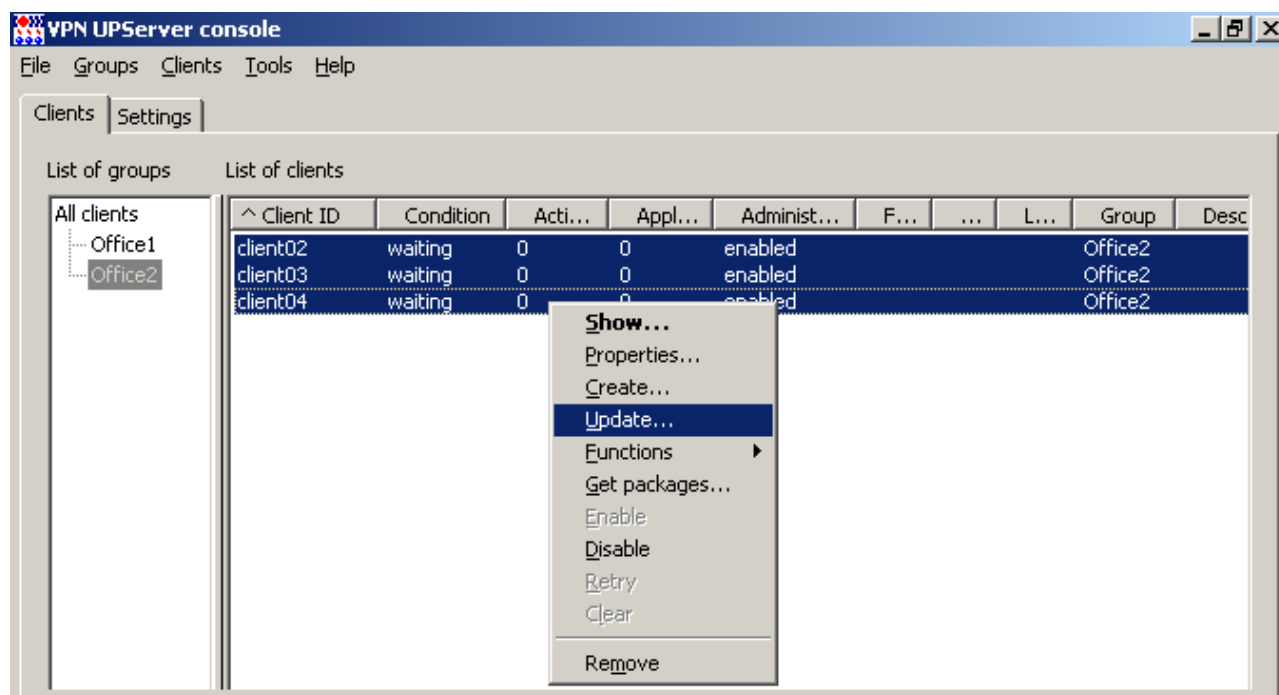


Рисунок 201

- В открывшемся окне **Update clients** в поле **Product package** нажмите кнопку [...] и в стандартном окне открытия файла укажите файл с шаблоном проекта, например, client\_template.vpdt.

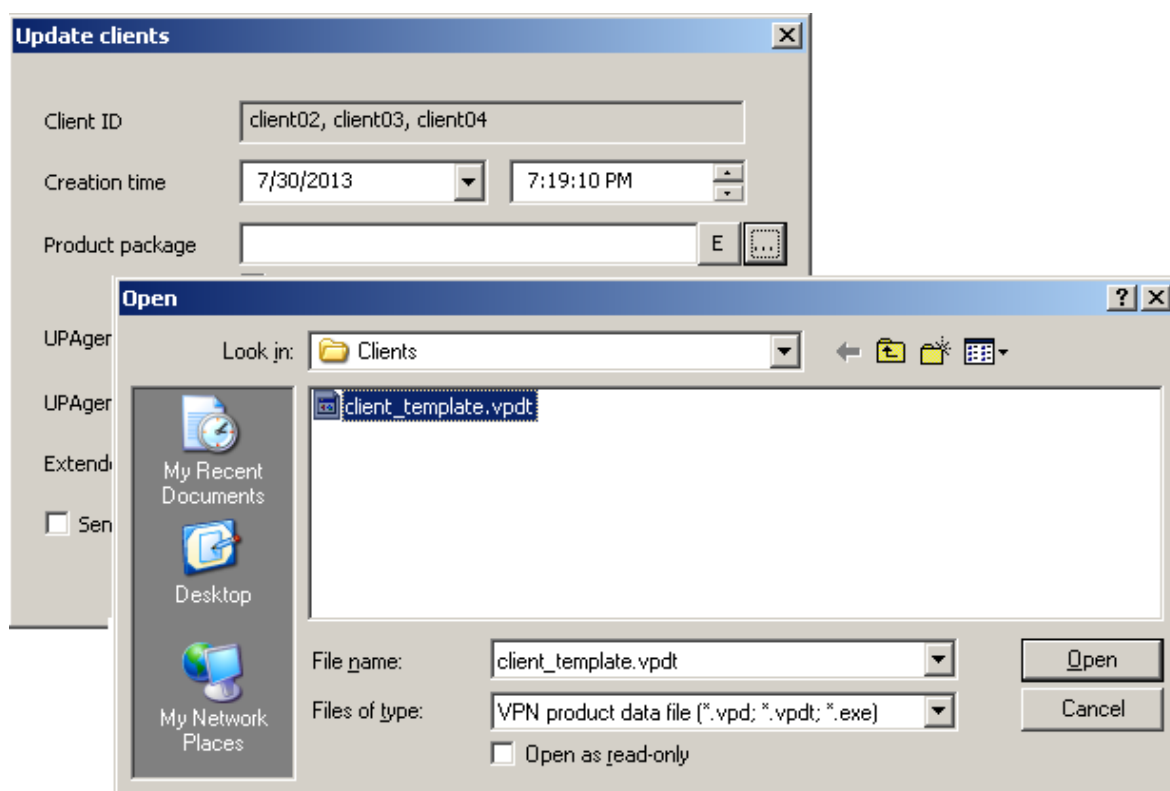


Рисунок 202

- Если в шаблон входит список локальных сертификатов, то при применении обновления для каждого клиента будет отбираться локальный сертификат из списка с выполнением проверки соответствия имеющегося у него запроса на сертификат и открытого ключа в сертификате. Такая проверка будет выполняться только при использовании шаблона. При отсутствии на клиенте запроса на его локальный сертификат такая проверка не выполняется и локальный сертификат на клиенте не обновляется.

## 14. Управление с использованием командной строки – утилита upmgr

Для автоматизации процесса управления клиентами удобно использовать интерфейс командной строки. В состав продукта **VPN UPSever** входит командно-строчная утилита `upmgr.exe`, размещенная в каталоге продукта – `C:\Program Files\S-Terra Bel\Bel VPN KP`.

### Команды утилиты upmgr.exe

#### Команда show

**Команда show выводит информацию о клиенте, аналогичную таблице клиентов** (Рисунок 81).

```
upmgr show [-i CLIENT_ID [-s SECTION_NAME]]
```

CLIENT_ID	уникальный идентификатор клиента, может состоять из любых символов, за исключением следующих: \?/:.">*< , не должен начинаться или заканчиваться символами пробел, табуляция или точка, и не должен быть равен "NUL" или "CON" или "PRN" или "AUX" или "COMx" или "LPTx", где x [1..9];  Если не указывать ключ <code>-i</code> выводится краткая информация обо всех клиентах При указании ключа <code>-i</code> выводится расширенная информация для указанного клиента.
SECTION_NAME	имя секции данных о клиенте. Например, "---VPN PRODUCT---", "---LSP---", "---LICENSE---" и т.п.

#### Пример

```
upmgr show
client01 active 0 3 enabled unknown 14/05/2012 00:21:38 40.0.0.101 none
```

#### Команда create

**Команда create позволяет создать нового клиента на Сервере управления**

```
upmgr create -i CLIENT_ID -p PRODUCT_PKG [-g CLIENT_GROUP] [-s AGENT_SETTINGS] [-dev_pwd DEVICE_PWD]
```

PRODUCT_PKG	имя файла (здесь и далее имя файла включает полный путь к нему), содержащего настройки VPN продукта, который был создан с помощью окна консоли управления VPN data maker, или имя файла дистрибутива продукта Bel VPN Gate/Client 4.1, который был создан с помощью продукта Bel VPN Gate/Client AdminTool
CLIENT_GROUP	имя группы, к которой принадлежит клиент (формат SUB1/SUB2/NAME);
AGENT_PKG	каталог, в котором размещен дистрибутив Клиента управления (указывается, если получена новая версия Клиента управления от разработчика, текущая версия размещена в каталоге upagent)
AGENT_SETTINGS	имя файла, содержащего настройки Клиента управления
DEVICE_PWD	в данной версии не используется

**Пример** создания нового клиента с идентификатором "client02", с именем дистрибутива продукта Bel VPN Client 4.1 "e:\share\test\_pkg.exe"

```
upmgr create -i client02 -p e:\share\test_pkg.exe
```

**Команда remove**

**Команда remove позволяет удалить клиента из таблицы клиентов на Сервере управления**

```
upmgr remove -i CLIENT_ID
```

**Пример** удаления клиента с идентификатором " client02":

```
upmgr remove -i client02
```

**Команда get**

**Команда get позволяет получить инициализационные файлы для управляемого устройства в указанный каталог**

```
upmgr get -i CLIENT_ID -d PRODUCT_DIR [-s UPAGENT_SETTINGS] [-ask_user_mode ASK_USER_MODE] [-check_mode CHECK_MODE] [-notify_client_port NOTIFY_CLIENT_PORT]
```

PRODUCT_DIR	каталог, в который будут сохранены дистрибутивы для Клиента управления
UPAGENT_SETTINGS	файл с настройками <i>Клиента управления</i> . Если он не указан будет использоваться конфигурационный файл по умолчанию (C:\Documents and Settings\All Users\Application Data\UPServer\csettings.txt)
ASK_USER_MODE	режим запроса подтверждения у пользователя о начале обновления, устанавливаемый в пакете Клиента управления, может принимать значения:  auto – подтверждение запрашивается, если установлен Bel VPN Client (значение по умолчанию)  never – подтверждение никогда не запрашивается  always – подтверждение запрашивается всегда.  Если значение другое, то оно трактуется как auto.
CHECK_MODE	режим проверки исполняемых модулей, подписанных ЭЦП, при получении обновления, может принимать значения:  <пустая строка> - исполняемые модули не проверяются  none – исполняемые модули не проверяются  full – проверяются присланные в обновлении расширенные обновления и бинарные коды нового Клиента управления  Если значение отсутствует, то оно приравнивается к значению none
NOTIFY_CLIENT_PORT	сетевой порт, который <i>Клиент управления</i> будет использовать для обмена сообщениями с <i>Сервером управления</i> . Если он не указан, то будет использоваться порт, указанный в конфигурационном файле <i>Клиента управления</i> (по умолчанию порт 43011);

**Пример** получения дистрибутивов для клиента с идентификатором "client02", с записью их в каталог "e:\share\#init\client02", Клиенту управления никогда не запрашивать подтверждение о начале обновления и всегда проверять на ЭЦП присланные обновления:

```
upmgr.exe get -i client02 -d e:\share\#init\client02 -ask_user_mode never -check_mode full
```



**Команда update**

**Команда update позволяет создать обновление на Сервере управления для клиента**

```
upmgr update -i CLIENT_ID [-p[d] PRODUCT_PKG] [-a AGENT_PKG] [-s
AGENT_SETTINGS] [-sca (UPCACERTS_FILE|*)] [-e EXTENDED_DATA] [-date
CREATION_DATE] [-time CREATION_TIME]
```

PRODUCT_PKG	имя файла (здесь и далее имя файла включает полный путь к нему), содержащего настройки VPN продукта, который был создан с помощью окна консоли управления VPN data maker, или имя файла дистрибутива продукта Bel VPN Gate/Client 4.1, который был создан с помощью продукта Bel VPN Gate/Client AdminTool  Если вместо ключа -p указать ключ -pd, то Клиенту управления будут пересылаться только данные, без бинарных кодов продукта Bel VPN Gate/Client.
AGENT_PKG	каталог, в котором размещен дистрибутив Клиента управления (указывается, если получена новая версия Клиента управления от разработчика, текущая версия размещена в каталоге upagent)
AGENT_SETTINGS	имя файла, содержащего настройки Клиента управления
UPCACERTS_FILE *	имя файла в формате PKCS#7 (.p7b) со списком CA сертификатов Сервера управления, которые передаются клиенту в составе обновления. Если передается один CA сертификат, то файл может быть с расширением .cer. Если нужно передать весь актуальный список CA сертификатов Сервера управления, то следует указать «*»
EXTENDED_DATA	каталог, в котором расположены расширенные данные и скрипты обновления
CREATION_DATE	формат: dd/mm/yy, hh:mm
CREATION_TIME	дата и время, когда Сервер управления сформирует пакет обновления и сделает его доступным для скачивания Клиентом управления. Если указанное время уже прошло, то пакет обновления будет сформирован и открыт для скачивания сразу после создания обновления (если параметры не указаны, то используются текущая дата и время).

**Пример** создания для клиента с идентификатором "client02" обновления данных продукта Bel VPN Gate/Client, находящихся в дистрибутиве этого продукта "e:\share\test\_pkg.exe":

```
upmgr update -i client02 -p e:\share\test_pkg.exe
```

**Команда retry**

**Команда retry позволяет снять с обновления признак неудачного обновления, тем самым указывая системе, что это обновление должно быть применено Клиентом управления еще раз**

```
upmgr retry -i CLIENT_ID
```

**Пример** снятия признака неудачного обновления для клиента с идентификатором "00000002":

```
upmgr retry -i 00000002
```

**Команда clear**

**Команда clear позволяет отменить все непримененные и незавершенные обновления для клиента**

```
upmgr clear -i CLIENT_ID [-force]
```

force                      флаг для команды clear, позволяющий произвести отчистку всех непримененных и незавершенных обновлений, не взирая на их статус.

**Пример** удаления всех непримененных обновлений для клиента с идентификатором "00000002":

```
upmgr clear -i 00000002 -force
```

**Команда disable**

**Команда disable блокирует все сетевые обмены Сервера управления с клиентом**

```
upmgr disable -i CLIENT_ID
```

**Пример** запрета всех сетевых обменов с клиентом с идентификатором "client02":

```
upmgr disable -i client02
```

**Команда enable**

**Команда enable разрешает Серверу управления сетевые обмены с клиентом**

```
upmgr enable -i CLIENT_ID
```

**Пример** разрешения сетевых обменов Серверу управления с клиентом с идентификатором "client02":

```
upmgr enable -i client02
```

**Команда set\_group**

**Команда clear изменяет группу у заданных клиентов**

```
upmgr set_group -g CLIENT_GROUP {-i CLIENT_ID|-go OLD_CLIENT_GROUP}
```

CLIENT\_GROUP            имя группы, к которой принадлежит клиент (формат SUB1/SUB2/NAME)

OLD\_CLIENT\_GROUP        имя группы, которая должна быть заменена на CLIENT\_GROUP (формат PARENT0/PARENT1[NAME][\*]);

**Пример** включения клиента "client02" в группу "Minsk/Office01":

```
upmgr.exe set_group -g Minsk/Office01 -i client02
```

**Команда set\_prop**

**Команда set\_prop добавляет описание свойств у заданного клиента**

```
upmgr set_prop -i CLIENT_ID [-dev_pwd DEVICE_PWD] [-client_desc CLIENT_DESC] [-ex_var_file FILE]
```

DEVICE\_PWD              зарезервировано для будущих версий

CLIENT\_DESC            произвольная строка для описания клиента, вносимая в поле Description

FILE                    имя файла, в котором указаны строки с переменными и их значениями, описывающие свойства клиента, которые передаются скрипту cook.bat при его запуске в процессе подготовки расширенного обновления. Формат строки:   
\_ex\_имя\_переменной=значение\_переменной

**Пример** добавления в описание client01 свойства «может работать с токеном» со значением «eToken NG-FLASH».

```
upmgr.exe set_prop -i client02 -client_desc "в одной сети с client01" -ex_var_file "C:\Program Files\S-Terra Bel\Bel VPN КР\prop_client02.txt"
```

В файле prop\_client02.txt записана строка – «может работать с токеном= eToken NG-FLASH»

**Команда show\_cert**

**Команда show\_cert запускает стандартную GUI программу операционной системы для отображения рабочего сертификата Сервера управления**

```
upmgr show_cert
```

**Пример** показа рабочего сертификата Сервера управления:

```
upmgr show_cert
```

### Команда `renew_cert`

**Команда `renew_cert` запускает перевыпуск рабочего сертификата Сервера управления (начало срока действия сертификата - за день до текущей даты, время жизни сертификата - 1 месяц)**

```
upmgr renew_cert [-expired_only]
```

`-expired_only`      рабочий сертификат Сервера управления пересоздается, если у него истек срок действия

**Пример** пересоздания рабочего сертификата Сервера управления только в том случае, если у него истек срок действия.

### Команда `check_files`

**Команда `check_files` запускает**

```
upmgr check_files
```

`check_files`      проверка целостности файлов Сервера управления

### Команда `backup`

**Команда `backup` запускает процесс сохранения данных о Клиентах управления и настройках Сервера управления в файл. В процессе сохранения архивируются данные Сервера управления, кроме контейнеров с секретными ключами сертификатов Сервера управления и статистической информации о Клиентах управления, хранимой в базе данных статистики.**

```
upmgr backup -f BACKUP_FILE_NAME
```

`BACKUP_FILE_NAME`      имя файла для сохранения данных о Клиентах управления и настройках Сервера управления.

**Пример** сохранения данных о клиентах управления и настройках Сервера управления:

```
upmgr.exe backup -f c:\backup01.bin
```

### Команда `restore`

**Команда `restore` запускает процесс восстановления данных о Клиентах управления и настройках Сервера управления из файла. В процессе будут восстановлены данные Сервера управления, кроме контейнеров с секретными ключами сертификатов Сервера управления и статистической информации о Клиентах управления, хранимой в базе данных статистики**

```
upmgr restore -f BACKUP_FILE_NAME
```

`BACKUP_FILE_NAME`      имя файла с данными о Клиентах управления и настройках Сервера управления.

**Пример** восстановления данных Сервера управления из файла `C:\backup01.bin`:

```
upmgr.exe restore -f c:\backup01.bin
```

При успешном завершении команды – код возврата равен 0, а при неуспешном - отличен от 0.

## 15. Изменение готового проекта с настройками VPN агента – утилита **vpnmaker**

Для внесения изменений в готовый проект можно использовать утилиту **vpnmaker**, расположенную в каталоге продукта – C:\Program Files\S-Terra\Bel VPN KP.

Назначение – изменение данных в готовых проектах, созданных с помощью Сервера управления, или создание новых проектов-шаблонов.

Предполагается, что утилита будет использоваться для создания большого количества похожих проектов для клиентов, незначительно отличающихся друг от друга (например, локальным сертификатом и номером лицензии агента).

Параметры утилиты:

```
vpnmaker replace -fi IN_FILE -fo OUT_FILE [-lsp LSP_TXT_FILE|-clp CISCO-
LIKE_POLICY] [-keyname KEY_NAME0N -keybody KEY_FILE0N] [-lic LIC_FILE] [-
cryptolic CRYPTO_LIC_FILE] [-cert CERT_FILE [-certpwd PWD] [-certnum NUM]
[-certkey KEY_CONT [-certkeypwd KEY_PWD]] [-trust]] [-ifdesc IF_FILE] [-
ifaliases IF_FILE] [-targetsoft TARGETSOFT_FILE]
```

```
vpnmaker make_template -fo OUT_FILE [-cert LOCAL_CERT_FILE01] [-cert
LOCAL_CERT_FILE0N] [-cp CP_VENDOR]
```

You can enter many keys and many certificates.

В режиме работы **replace** некоторые старые данные проекта заменяются новыми. Старые сертификаты удаляются из базы, но не все, а только тех типов, которые добавляются. Например, при замене только локального сертификата CA-сертификаты сохраняются. Можно добавить/заменить несколько сертификатов разных типов.

Параметры режима **replace**:

-fi IN_FILE	полный путь к файлу с проектом, который надо изменить. Расширение .exe или .vpd
-fo OUT_FILE	полный путь к файлу с измененным проектом. Расширение .exe или .vpd
-lsp LSP_TXT_FILE	полный путь к текстовому файлу с локальной политикой безопасности. Эта опция не может применяться одновременно с опцией -clp. Старые политики безопасности LSP и cisco-like из проекта удаляются. Новая LSP сохраняется в базе данных проекта.
-clp CISCO_LIKE_POLICY	полный путь к текстовому файлу с cisco-like политикой безопасности. Эта опция не может применяться одновременно с опцией -lsp. Опция допустима только для шлюзов безопасности. Старые политики безопасности LSP и cisco-like из проекта удаляются. Старые настройки лога (файлы "log_set.dsc", "syslog.ini", "syslog_3_1.ini", "syslog_4_0.ini") удаляются. Новая cisco-like политика сохраняется в базе данных проекта.
-keyname KEY_NAME	имя ключа. После имени обязательно должна следовать опция -keybody
-keybody KEY_FILE	полный путь к файлу с телом ключа.
-lic LIC_FILE	полный путь к текстовому файлу с лицензией на продукт. Пример файла: <pre>[license] CustomerCode=bank ProductCode=GATE100 LicenseNumber=1 LicenseCode=6E7AAAECBBB478B8</pre>

<code>-cryptolic CRYPTO_LIC_FILE</code>	полный путь к текстовому файлу с лицензией криптопровайдера. Пример файла: <code>LicenseSerialNumber=1282349167838947</code>
<code>-cert CERT_FILE</code>	полный путь к файлу с сертификатом (расширение .cer, .p7b, .pfx). Для этого сертификата можно указать дополнительные параметры:
<code>-certpwd PWD</code>	пароль, которым защищен файл с сертификатом.
<code>-certnum NUM</code>	порядковый номер сертификата (нужен, если файл содержит несколько сертификатов).
<code>-certkey KEY_CONT</code>	имя контейнера с секретным ключом сертификата (сам контейнер – у клиента).
<code>-certkeypwd KEY_PWD</code>	пароль, защищающий ключевой контейнер.
<code>-trust</code>	этот флаг должен выставляться у CA-сертификатов, которым мы доверяем.
<code>-ifdesc IF_FILE</code>	полный путь к текстовому файлу с описанием виртуального адреса и роутинга. Параметр может быть только для Bel VPN Gate 4.1 on token (СПДС «ПОСТ»). Пример файла: <code>VirtualDeviceAddress=23.24.24.24</code>  <code>[ExtendedDeviceRoutes] Route_0=10.0.2.0/24 192.168.5.1 Route_1=23.45.55.0/24 1.2.3.4 Route_2=24.0.0.0/16 DGA Route_3=25.0.0.0/16 VDA</code>  <code>DGA - default gateway address VDA - virtual device address</code>  <code>!Description eth0 [IF_eth0] STATE=UP Address_0=40.0.0.17/24 MTU=1400</code>  <code>!Description eth1 [IF_eth1] STATE=UP Address_0=192.168.1.1/24 MTU=1400</code>
<code>-ifaliases IF_FILE</code>	полный путь к текстовому файлу с описанием алиасов интерфейсов. Пример файла: <code>FastEthernet1/0 = eth1 FastEthernet1/1 = eth2,eth3 default = *</code>  По этой информации формируется файл <code>ifaliases.cf</code> (для продуктов версии 4.X) или информация сохраняется в базе продукта (для версий 3.X). Если не определен алиас <code>default</code> , он автоматически добавляется в виде <code>default = *</code>
<code>-targetsoft TARGETSOFT_FILE</code>	полный путь к текстовому файлу с описанием типа и параметров целевого программного обеспечения на управляемом устройстве. Параметр применяется только для Bel VPN Gate 4.1 on token. Пример файла: <code>TARGET=rdp SERVER=192.168.15.1:5444 USER=guest OPTIONS=</code>

Переменная TARGET может содержать следующие значения:

web – целевое ПО для удаленного доступа к защищаемым ресурсам в качестве Web-клиента

rdp – целевое ПО для удаленного доступа к защищаемым ресурсам в качестве RDP-клиента

other – другое целевое ПО.

Переменная OPTIONS содержит параметры ПО, установленного на управляемом устройстве

#### Параметры режима **make\_template**

В режиме работы `make_template` создается новый проект-шаблон, в котором есть только сертификаты. Они используются во внутренних тестах.

<code>-fo OUT_FILE</code>	полный путь к файлу с новым проектом. Расширение .exe или .vpd.
<code>-cert LOCAL_CERT_FILE</code>	полный путь к файлу с сертификатом
<code>-cp CPVENDOR</code>	криптопровайдер (CP или SC или ST)

## 16. Настройки Сервера управления

Администратор Сервера управления может задать некоторые настройки в файле:

C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt или

C:\ProgramData\UPServer\ssettings.txt

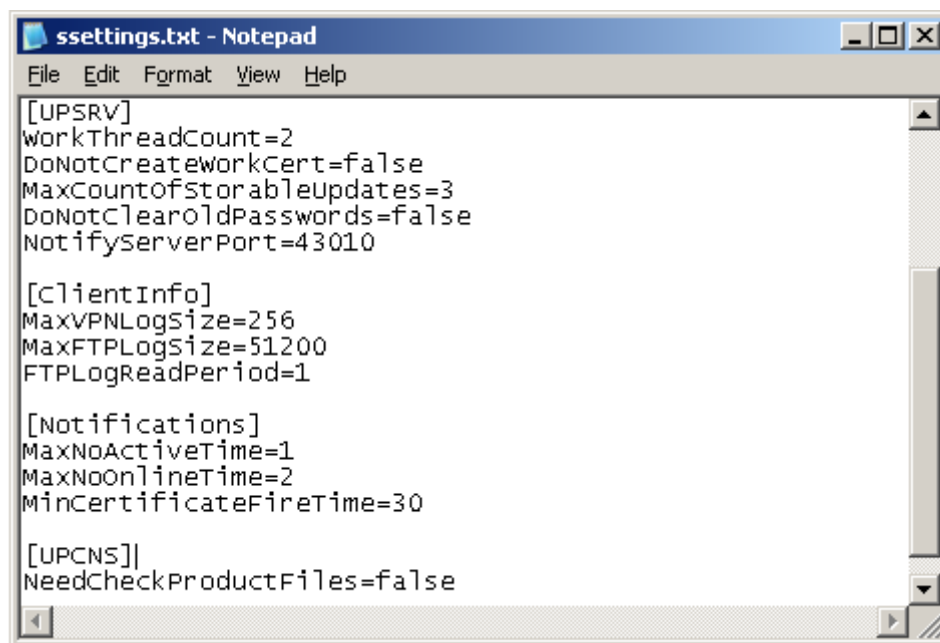


Рисунок 203

В файле ssettings.txt настройки распределены между секциями – Log, UPSRV, FTPServer, ClientInfo, Notifications, UPCNS. Описание переменных в каждой секции представлено ниже. Несколько настроек задается в реестре HKEY\_LOCAL\_MACHINE\SOFTWARE\UPServer или HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\UPServer.

Администратор может управлять следующими настройками.

Секция	Описание
Log	<p><b>Флаг включения syslog протоколирования</b></p> <p>Переменная SyslogEnable</p> <p>Значение: true – включено протоколирование</p> <p>false – выключено (значение по умолчанию – false).</p> <hr/> <p><b>Адрес Syslog-сервера</b></p> <p>Переменная SyslogSrvAddr</p> <p>Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1).</p> <hr/> <p><b>Адрес источника сообщений</b></p> <p>Переменная SyslogFacility</p> <p>Значение: строка. Возможные значения:</p> <p>log_kern, log_user, log_mail, log_daemon, log_auth, log_syslog, log_lpr, log_news, log_uucp, log_cron, log_authpriv, log_ftp, log_ntp, log_audit, log_alert, log_cron2, log_local0, log_local1, log_local2, log_local3, log_local4, log_local5, log_local6, log_local7)</p> <p>Значение по умолчанию – log_local7)</p> <hr/> <p><b>Размер файла протоколирования событий</b></p> <p>Переменная FileMaxSize</p> <p>Значение: от 10 килобайт (значение по умолчанию – 10200 килобайт, если строка отсутствует или некорректна).</p>

	<p>Имя файла протоколирования: C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log.</p> <p>При достижении заданного значения данные копируются в файл upserver.log.bak, а файл upserver.log очищается. <a href="#">Пример файла с сообщениями.</a></p>
UPSRV	<p><b>Количество рабочих ниток в сервисе подготовки обновлений</b></p> <p>Переменная WorkThreadCount</p> <p>Значение: десятичное число от 1 до 10 (значение по умолчанию 2). Рекомендуемое значение - количество процессоров на компьютере + 1.</p> <p><b>Количество рабочих ниток в сервисе записи статистических данных в базу данных статистики</b></p> <p>Переменная StatThreadCount</p> <p>Значение: десятичное число от 1 до 10 (значение по умолчанию 1).</p> <p><b>Флаг отключения автоматического пересоздания рабочего сертификата</b></p> <p>Переменная DoNotCreateWorkCert</p> <p>Значение: false – отключено автоматическое пересоздание (значение по умолчанию)</p> <p>true – включено автоматическое пересоздание</p> <p><b>Максимальное количество хранимых примененных обновлений для каждого клиента</b></p> <p>Переменная MaxCountOfStorableUpdates</p> <p>Значение: десятичное число от 0 до 4294967295, значение 0 – обновления не удаляются (значение по умолчанию 0).</p> <p><b>Флаг удаления старых паролей к клиентским ключевым контейнерам</b></p> <p>Переменная DoNotClearOldPasswords</p> <p>Значение: false – удаляются автоматически старые пароли (значение по умолчанию)</p> <p>true – не удаляются автоматически старые пароли</p> <p><b>UDP порт, который используется для обмена уведомлениями с Клиентами управления</b></p> <p>Уведомления используются для отслеживания Клиентов управления, находящихся в сети, и оповещения их о существовании подготовленных обновлений.</p> <p>Переменная NotifyServerPort</p> <p>Значение: десятичное число от 0 до 65535 (значение по умолчанию 43010), значение 0 отключает механизм обмена уведомлениями.</p>
FTPServer	<p><b>Сетевой адрес для взаимодействия с сервисом продукта FileZilla Server</b></p> <p>Переменная Address</p> <p>Значение: локальный IP-адрес сервера FileZilla Server (значение по умолчанию 127.0.0.1).</p> <p><b>Сетевой порт для взаимодействия с сервисом продукта FileZilla Server</b></p> <p>Переменная Port</p> <p>Значение: порт сервиса FileZilla Server (значение по умолчанию 14147).</p> <p><b>Пароль для взаимодействия с сервисом продукта FileZilla Server</b></p> <p>Переменная Password</p> <p>Значение: строка, представляющая из себя пароль сервиса FileZilla Server (значение по умолчанию &lt;пустая строка&gt;).</p>
ClientInfo	<p><b>Максимальный размер лог сообщений VPN-продукта, хранящихся для каждого Клиента управления</b></p> <p>Переменная MaxVPNLogSize</p>



	<p>Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 25600).</p> <p><b>Максимальный размер лог сообщений FTP-сервера</b></p> <p>Переменная <code>MaxFTPLogSize</code></p> <p>Значение: десятичное число от 1024 до 921600 килобайт (значение по умолчанию 51200).</p>
	<p><b>Период анализа сообщений FTP-сервера</b></p> <p>Переменная <code>FTPLogReadPeriod</code></p> <p>Значение: целое число от 1 до 60 минут (значение по умолчанию 5).</p>
Notifications	<p><b>Максимальное время неактивности клиента</b></p> <p>Переменная <code>MaxNoActiveTime</code></p> <p>Значение: десятичное число от 0 до 4294967295 часов, значение 0 – отключает отслеживание максимального времени неактивности клиентов (значение по умолчанию 24).</p> <p><b>Максимальное время неактивности клиента для признания его находящимся не на связи</b></p> <p>Переменная <code>MaxNoOnlineTime</code></p> <p>Значение: десятичное число от 1 до 60 минут (значение по умолчанию 2).</p> <p><b>Минимальное время перед окончанием срока действия сертификата управляемого устройства</b></p> <p>Переменная <code>MinCertificateFireTime</code></p> <p>Значение: десятичное число от 0 до 4294967295 суток, значение 0 – отключает отслеживание минимального времени перед окончанием срока действия сертификатов управляемых устройств (значение по умолчанию 30).</p> <p>При наступлении этого времени дата окончания срока действия сертификата выделена красным цветом в таблице клиентов Сервера управления.</p>
UPCNS	<p><b>Флаг проверки целостности файлов продукта при старте приложения VPN UPServer console</b></p> <p>Переменная <code>NeedCheckProductFiles</code></p> <p>Значение: <code>true</code> – выполняется проверка целостности при каждом старте приложения, <code>false</code> – проверка целостности не выполняется (значение по умолчанию).</p>
DBServer	<p><b>Сетевой адрес для взаимодействия с сервисом продукта PostgreSQL Server</b></p> <p>Переменная <code>Address</code></p> <p>Значение: IP-адрес сервиса PostgreSQL Server (значение по умолчанию 127.0.0.1).</p> <p><b>Сетевой порт для взаимодействия с сервисом продукта PostgreSQL Server</b></p> <p>Переменная <code>Password</code></p> <p>Значение: порт сервиса PostgreSQL Server (значение по умолчанию 5432).</p> <p><b>Пароль для взаимодействия с сервисом продукта PostgreSQL Server</b></p> <p>Переменная <code>Port</code></p> <p>Значение: строка, представляющая из себя пароль сервиса PostgreSQL Server (значение по умолчанию 1234567890).</p>

HKEY\_LOCAL\_MACHINE\  
SOFTWARE\UPServer  
HKEY\_LOCAL\_MACHINE\  
SOFTWARE\Wow6432Node\UPServer

### **Режим работы создаваемых Клиентов управления**

Переменная ClientMode

Значение: windowless – безоконный режим работы Клиента управления (значение по умолчанию)

<пустая строка> – оконный режим работы Клиента управления (для отладки тестирования).

### **Запрос подтверждения у пользователя о начале обновления, устанавливаемый в пакете Клиента управления**

Переменная ClientUserAskMode

Значение: auto – необходимость запроса определяется на основе типа VPN-продукта (если установлен продукт Bel VPN Client - подтверждение запрашивается (значение по умолчанию)

never – подтверждение никогда не запрашивается, не смотря на тип VPN-продукта

always – подтверждение запрашивается всегда, не смотря на тип VPN-продукта

Если значение другое, то оно трактуется как auto.

### **Проверка исполняемых модулей при получении обновления**

Переменная ClientUpdateCheckMode

Значение: <пустая строка> – исполняемые модули не проверяются

none – исполняемые модули не проверяются

full – проверяются присланные в обновлении расширенные обновления и бинарные коды нового Клиента управления

Если значение отсутствует, то оно приравнивается к значению none.

Если значение другое, то оно приравнивается к full.

Исполняемые модули подписываются ЭЦП, для которой используется секретный сертификат, изданного компанией С-Терра. Проверка гарантирует, что исполняемые модули были созданы с использованием скриптов, созданных компанией С-Терра. Если администратор управляемых устройств использует свои скрипты, то такую проверку следует отключить.

Пример файла протоколирования:

```
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log file name:
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting FileMaxSize: 5120
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting SyslogEnable: false
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting SyslogSrvAddr:
127.0.0.1
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting SyslogFacility:
log_local7
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 Settings is read from file
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log

Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:WorkThreadCount: 2
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:MaxCountOfStorableUpdates:
1000
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:DoNotCreateWorkCert: false
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:DoNotClearOldPasswords: false
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:NotifyServerPort: 43010
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 ClientInfo:MaxVPNLogSize: 256 KB
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 ClientInfo:MaxFTPLogSize: 51200 KB
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 ClientInfo:FTPLogReadPeriod: 5 min
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 Notifications:MaxNoOnlineTime: 1
min
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 00002150 Server notify socket is
opened (any:43010)
Fri Feb 10 23:18:53 2012 NOTICE   upsrv 00001744 Module 4.0.12437 is started
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log file name:
```

```
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting FileMaxSize: 5120
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting SyslogEnable: false
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting SyslogSrvAddr:
127.0.0.1
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting SyslogFacility:
log_local7
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Settings is read from file
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Notifications:MaxNoActiveTime: 24
hours
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec
Notifications:MinCertificateFireTime: 30 days
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec UPCNS:NeedCheckProductFiles: false
Fri Feb 10 23:19:21 2012 NOTICE   upcns 00000aec Module 4.0.12437 is started
Fri Feb 10 23:19:24 2012 NOTICE   upcns 00000aec Module is stopped
```

## 17. Настройки Клиента управления

Настройки по умолчанию Клиента управления записаны на Сервере управления в файле:

C:\Documents and Settings\All Users\Application Data\UPServer\csettings.txt или

C:\ProgramData\UPServer\csettings.txt

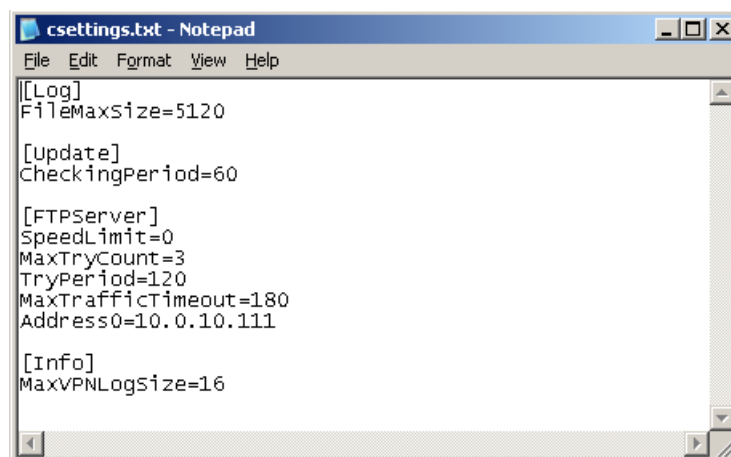


Рисунок 204

Для каждого клиента настройки Клиента управления можно изменить и сохранить в другом файле, а затем указать его в поле **UPAgent settings** (Рисунок 57) окна **Create new client** при создании клиента.

В файле настройки распределены между секциями – Log, Update, FTPServer, Info. Описание переменных в каждой секции представлено ниже. Несколько настроек выставляется при инсталляции (инициализации) Клиента управления в реестре

HKEY\_LOCAL\_MACHINE\SOFTWARE\UPAgent либо

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\UPAgent.

Секция	Описание
Log	<b>Флаг включения syslog протоколирования</b> Переменная SyslogEnable Значение: true – включено протоколирование false – выключено (значение по умолчанию – false).
	<b>Адрес Syslog-сервера</b> Переменная SyslogSrvAddr Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1)
	<b>Адрес источника сообщений</b> Переменная SyslogFacility Значение: log_kern, log_user, log_mail, log_daemon, log_auth, log_syslog, log_lpr, log_news, log_uucp, log_cron, log_authpriv, log_ftp, log_ntp, log_audit, log_alert, log_cron2, log_local0, log_local1, log_local2, log_local3, log_local4, log_local5, log_local6, log_local7 (значение по умолчанию)
	<b>Размер файла протоколирования событий</b>

Секция	Описание
	<p>Переменная <code>FileMaxSize</code></p> <p>Значение: от 10 килобайт (значение по умолчанию – 5120 килобайт, если строка отсутствует или некорректна).</p> <p>Имя файла протоколирования событий:</p> <p style="padding-left: 40px;">для ОС Windows - <code>C:\Program Files\UPAgent\upagent.log</code></p> <p style="padding-left: 40px;">для ОС Unix – <code>/var/log/upagent/upagent.log</code></p> <p>При достижении заданного значения данные копируются в файл <code>upagent.log.bak</code>, а файл <code>upagent.log</code> очищается.</p>
Update	<p><b>Период проверки новых обновлений на Сервере управления</b></p> <p>Переменная <code>CheckingPeriod</code></p> <p>Значение: от 60 до 86400 секунд (значение по умолчанию – 3600).</p>
	<p><b>Период между посылками нотификаций Серверу управления</b></p> <p>Переменная <code>NotifySendPeriod</code></p> <p>Значение: целое число от 1 до 3600 секунд (значение по умолчанию 60).</p>
	<p><b>Количество неудачных попыток соединения с Сервером управления перед тем, как заново попытаться подобрать параметры соединения</b> (например, использовать другой IP-адрес Сервера управления).</p> <p>Переменная <code>MaxFailedConnCount</code></p> <p>Значение: десятичное число от 0 до 200 секунд (значение по умолчанию 0);</p> <p style="padding-left: 40px;">значение 0 – не подбирать параметры соединения с Сервером управления при любом количестве неудачных попыток.</p>
	<p><b>UDP порт Клиента управления для обмена нотификациями с Сервером управления</b></p> <p>Переменная <code>NotifyClientPort</code></p> <p>Значение: целое число от 0 до 65535,</p> <p style="padding-left: 40px;">значение 0 – отключает механизм обмена нотификациями (значение по умолчанию 43011).</p> <p>Нотификации используются для механизма отслеживания нахождения Клиента управления на связи и оповещения его о существовании для них подготовленных обновлений.</p>
	<p><b>UDP порт Сервера управления для получения нотификаций от Клиента управления</b></p> <p>Переменная <code>NotifyServerPort</code></p>

Секция	Описание
	<p>Значение: целое число от 0 до 65535 (значение по умолчанию 43010), значение 0 – отключает механизм отсылки уведомлений.</p>
FTPServer	<p><b>Адрес FTP сервера</b> Переменная AddressX, где X любое десятичное число (0,1,2..) Количество таких переменных может быть больше одного, они будут использоваться в том порядке, в котором заданы. Числа должны быть уникальные в пределах секции. Значение: IP-адрес или DNS-имя, которое будет транслироваться в IP-адрес в момент создания соединения.</p> <p><b>Максимальное время ожидания соединения с FTP сервером</b> Переменная MaxConnectTimeout Значение: десятичное число от 0 до 300 секунд (значение по умолчанию 0, т.е. время ожидания определяется настройками ОС, под управлением которой работает Клиент управления).</p> <p><b>Максимальная скорость скачивания обновлений с Сервера управления</b> Переменная SpeedLimit Значение: от 512 до 4294967295 байт/секунду или 0 (значение 0 – ограничения нет, значение по умолчанию).</p> <p><b>Максимальное количество попыток скачать/получить данные с/на FTP сервер(а)</b> Переменная MaxTryCount Значение: целое число от 1 до 30 (значение по умолчанию 3).</p> <p><b>Период между попытками скачать/получить данные с/на FTP сервер(а)</b> Переменная TryPeriod Значение: целое число от 0 до 300 секунд (значение по умолчанию 120).</p> <p><b>Максимальное время отсутствия трафика между Клиентом управления и FTP-сервером, по истечении которого соединение считается разорванным</b> Переменная MaxTrafficTimeout Значение: целое число от 30 до 3600 секунд (значение по умолчанию 180).</p>
Info	<p><b>Максимальный размер сообщений продукта Bel VPN Gate/Client, пересылаемых на Сервер управления</b> Переменная MaxVPNLogSize Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 16).</p>

Секция	Описание
	<p><b>Период между сбором статистической информации на управляемом устройстве</b></p> <p>Переменная StatCollectPeriod</p> <p>Значение: десятичное число от 0 до 600 секунд (значение по умолчанию 5), значение 0 – сбор статистической информации не производится.</p>
	<p><b>Максимальный размер памяти на управляемом устройстве для сбора статистической информации. При достижении этого размера собранная статистическая информация пересылается на Сервер управления</b></p> <p>Переменная StatBufSize</p> <p>Значение: десятичное число от 1 до 2048 килобайт (значение по умолчанию 100).</p>
	<p><b>Период между посылками собранной статистической информации на Сервер управления</b></p> <p>Переменная StatSendPeriod</p> <p>Значение: десятичное число от 0 до 7200 минут (значение по умолчанию 10), значение 0 – отключает отслеживание по времени, действует только ограничение по размеру собранной статистической информации.</p>
	<p><b>Адрес и порт источника SNMP статистики</b></p> <p>Переменная StatSNMPAddr</p> <p>Значение: корректный IP-адрес и корректный порт, разделенные двоеточием (значение по умолчанию 127.0.0.1:161).</p>
	<p><b>Community-строка источника SNMP статистики</b></p> <p>Переменная StatSNMPCommunity</p> <p>Значение: строка, содержащая community (значение по умолчанию - public). Community-строка играет роль пароля при аутентификации сообщений SNMP.</p>
	<p><b>Период между перепосылками запросов к источнику SNMP статистики</b></p> <p>Переменная StatSNMPTimeout</p> <p>Значение: десятичное число от 1 до 100 сотых долей секунды (значение по умолчанию 10).</p>
	<p><b>Количество перепосылок запросов к источнику SNMP статистики</b></p> <p>Переменная StatSNMPRetries</p> <p>Значение: десятичное число от 0 до 5 раз (значение по умолчанию 0), значение 0 – статистика запрашивается только один раз (если в отведенное время ответ не приходит – повторных запросов не производится).</p>

Секция	Описание
StatVariables	<p><b>Флаг активности сбора статистики по загрузке процессора</b></p> <p>Переменная CPUUsage</p> <p>Значение:</p> <p>on – на Сервер управления будет посылаться параметр CPUUsage – средняя загрузка процессоров в процентах за время StatCollectPeriod (значение по умолчанию)</p> <p>off – статистика не собирается.</p>
	<p><b>Флаг активности сбора статистики по используемой памяти</b></p> <p>Переменная MemUsage</p> <p>Значение:</p> <p>on – на Сервер управления будут посылаться значения двух параметров и во вкладке Статистика UPWeb они будут отображены с именами:</p> <p>MemUsage – количество занятых байт в памяти</p> <p>MemFree - количество свободных байт в памяти</p> <p>(значение по умолчанию)</p> <p>off – статистика не собирается.</p>
	<p><b>Флаг активности сбора статистики по используемому дисковому пространству (диск, на котором установлен Клиент управления. Обычно для Windows - это диск C, для UNIX – примонтированный диск как /)</b></p> <p>Переменная DiskUsage</p> <p>Значение:</p> <p>on – на Сервер управления будут посылаться значения двух параметров:</p> <p>DiskUsage – количество занятых байт на диске</p> <p>DiskFree - количество свободных байт на диске</p> <p>(значение по умолчанию)</p> <p>off – статистика не собирается.</p>
	<p><b>Флаг активности сбора статистики по используемым сетевым интерфейсам</b></p> <p>Переменная NetUsage</p> <p>Значение:</p> <p>on – на Сервер управления будут посылаться значения двух параметров:</p> <p>NetInSpeed – среднее количество байт в секунду, полученных всеми интерфейсами, в период между замерами</p> <p>NetOutSpeed - среднее количество байт в секунду, отправленных со всех</p>



Секция	Описание																		
	<p>интерфейсов, в период между замерами (значение по умолчанию) off – статистика не собирается.</p> <p><b>Добавление переменной для сбора статистики</b> Запрос составляется в виде: SNMP:&lt;ID_SNMP&gt;=STATE [-n DISPLAYNAME] [-p COLLECTPERIOD] [-a SNMPADDR] [-c SNMPCOMMUNITY] [-t SNMPTIMEOUT] [-r SNMPRETRIES] [-ev ERROR_VALUE], где</p> <table> <tr> <td>&lt;ID_SNMP&gt; -</td><td>идентификатор запрашиваемой переменной (можно посмотреть в разделе «Мониторинг» пользовательской документации)</td></tr> <tr> <td>STATE -</td><td>флаг активности, значение on, off</td></tr> <tr> <td>DISPLAYNAME-</td><td>имя, под которым данная статистика будет посылаться на Сервер управления</td></tr> <tr> <td>COLLECTPERIOD-</td><td>период сбора статистики в секундах, если не задан, то используется значение StatCollectPeriod</td></tr> <tr> <td>SNMPADDR -</td><td>адрес и порт источника SNMP статистики, если не задан, то используется значение StatSNMPAddr</td></tr> <tr> <td>SNMPCOMMUNITY -</td><td>community-строка источника SNMP статистики, если не задана, используется значение StatSNMPCommunity</td></tr> <tr> <td>SNMPTIMEOUT -</td><td>период между перепосылками запросов к источнику SNMP статистики, если не задан, то используется StatSNMPTimeout</td></tr> <tr> <td>SNMPRETRIES -</td><td>количество перепосылок запросов к источнику SNMP статистики, если не задано, то используется значение StatSNMPRetries</td></tr> <tr> <td>ERROR_VALUE -</td><td>строка, которая будет использоваться в качестве значения статистики при ее неудачном сборе.</td></tr> </table> <p>Пример:</p>	<ID_SNMP> -	идентификатор запрашиваемой переменной (можно посмотреть в разделе «Мониторинг» пользовательской документации)	STATE -	флаг активности, значение on, off	DISPLAYNAME-	имя, под которым данная статистика будет посылаться на Сервер управления	COLLECTPERIOD-	период сбора статистики в секундах, если не задан, то используется значение StatCollectPeriod	SNMPADDR -	адрес и порт источника SNMP статистики, если не задан, то используется значение StatSNMPAddr	SNMPCOMMUNITY -	community-строка источника SNMP статистики, если не задана, используется значение StatSNMPCommunity	SNMPTIMEOUT -	период между перепосылками запросов к источнику SNMP статистики, если не задан, то используется StatSNMPTimeout	SNMPRETRIES -	количество перепосылок запросов к источнику SNMP статистики, если не задано, то используется значение StatSNMPRetries	ERROR_VALUE -	строка, которая будет использоваться в качестве значения статистики при ее неудачном сборе.
<ID_SNMP> -	идентификатор запрашиваемой переменной (можно посмотреть в разделе «Мониторинг» пользовательской документации)																		
STATE -	флаг активности, значение on, off																		
DISPLAYNAME-	имя, под которым данная статистика будет посылаться на Сервер управления																		
COLLECTPERIOD-	период сбора статистики в секундах, если не задан, то используется значение StatCollectPeriod																		
SNMPADDR -	адрес и порт источника SNMP статистики, если не задан, то используется значение StatSNMPAddr																		
SNMPCOMMUNITY -	community-строка источника SNMP статистики, если не задана, используется значение StatSNMPCommunity																		
SNMPTIMEOUT -	период между перепосылками запросов к источнику SNMP статистики, если не задан, то используется StatSNMPTimeout																		
SNMPRETRIES -	количество перепосылок запросов к источнику SNMP статистики, если не задано, то используется значение StatSNMPRetries																		
ERROR_VALUE -	строка, которая будет использоваться в качестве значения статистики при ее неудачном сборе.																		

Секция	Описание
	<pre>SNMP:1.3.6.1.4.1.9.9.171.1.3.1.1.0 =on -n ActiveTunCount -ev 0</pre>
<pre>HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\UP Agent</pre>	<p><b>Режим работы Клиента управления</b></p> <p>При инсталляции Клиента управления на управляемое устройство в ключе реестра HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent или HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\UPAgent выставляется режим работы, заданный по умолчанию. После инсталляции значение можно изменить.</p> <p>Переменная Mode</p> <p>Значение:</p> <p>windowless – безоконный режим работы Клиента управления (значение по умолчанию)</p> <p>&lt;пустая строка&gt; – оконный режим работы Клиента управления (для отладки и тестирования).</p> <p><b>Запрос подтверждения у пользователя о начале обновления</b></p> <p>Переменная UserAskMode</p> <p>Значение:</p> <p>auto – необходимость запроса определяется на основе типа VPN-продукта</p> <p>(подтверждение запрашивается, если на компьютере установлен продукт Bel VPN Client) (значение по умолчанию)</p> <p>never – подтверждение никогда не запрашивается, не смотря на тип VPN-продукта</p> <p>always – подтверждение запрашивается всегда, не смотря на тип VPN-продукта.</p> <p>Если значение другое, то оно трактуется как auto.</p> <p><b>Проверка исполняемых модулей при получении обновления</b></p> <p>Переменная UpdateCheckMode</p> <p>Значение:</p> <p>&lt;пустая строка&gt; – исполняемые модули не проверяются</p> <p>none – исполняемые модули не проверяются</p> <p>full – проверяются присланные в обновлении расширенные обновления и бинарные коды нового Клиента управления</p> <p>Если значение отсутствует, то оно приравнивается к значению none.</p>

Секция	Описание
	<p>Если значение другое, то оно приравнивается к full.</p> <p>Исполняемые модули подписываются ЭЦП, для которой используется секретный ключ сертификата, изданного компанией С-Терра. Проверка гарантирует, что исполняемые модули были созданы с использованием скриптов, созданных компанией С-Терра. Если администратор управляемых устройств использует свои скрипты, то такую проверку следует отключить.</p>

## 18. Описание интерфейса Сервера управления

Графический интерфейс приложения **VPN UPServer console** содержит следующие элементы.

### 18.1. Вкладка Clients

На Сервере управления во вкладке **Clients** отражается информация обо всех управляемых устройствах. Эта вкладка предназначена для создания, удаления учетных записей клиентов управляемых устройств, создания для них Клиентов управления, обновлений, приостановки работы с клиентом и т.д. Клиенты могут быть объединены в группы.

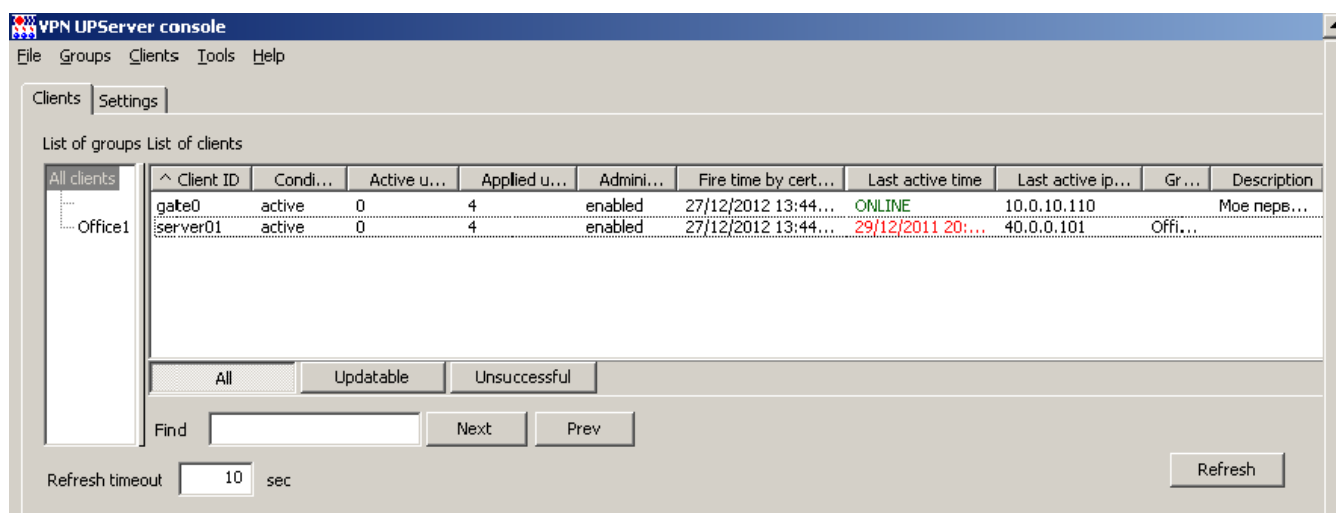


Рисунок 205

Описание вкладки **Clients**.

Параметр	Описание
List of groups	дерево групп клиентов, объединенных администратором по территориальному или организационному признаку расположения управляемых устройств
List of clients	таблица со списком клиентов, входящих в выделенную группу. Столбцы таблицы имеют следующие значения:
Client ID	уникальный идентификатор клиента
Condition	состояние Клиента управления, может принимать следующие значения: <b>new</b> – Клиент управления зарегистрирован на Сервере управления и еще ни разу не выходил на связь по сети <b>active</b> – Клиент управления готов к приему обновлений <b>waiting</b> – обновление для клиента создано и выложено на FTP-сервер и ожидается, что Клиент управления начнет его скачивание <b>updating</b> – Клиент управления применяет обновление (в данном состоянии Клиент управления находится с момента, когда он обнаружил обновление на Сервере управления и до момента, когда он его применил или отвергнул) <b>failed</b> – Клиент управления не смог применить очередное обновление (в этом состоянии клиент продолжает работу на предыдущем комплекте обновления, попытки по применению обновления не предпринимаются, пока администратор не изменит это состояние на active, отменив неуспешное обновление). Ошибка детектируется на основании невозможности скачать то же обновление с Сервера управления при примененном обновлении
Active updates	количество еще непримененных обновлений
Applied updates	количество успешно примененных обновлений

Administrative state	административное состояние обслуживания Клиента управления, может принимать следующие значения:  <b>enabled</b> – Клиент управления обслуживается  <b>disabled</b> – Клиент управления не обслуживается (все его обращения к серверу игнорируются)
Fire time by certificates	ближайшая дата и время истечения срока действия одного из сертификатов, размещенных в базе продукта Bel VPN Gate/Client 4.1
Last active time	время последнего действия, может принимать следующие значения:  <b>дата и время</b> последнего удачного FTP-соединения клиента (когда клиент успешно аутентифицировался на FTP-сервере)  <b>ONLINE</b> – в данный момент клиент находится на связи
Last active ip-address	IP-адрес клиента, с которого было осуществлено последнее удачное FTP-соединение
Group	имя группы, к которой принадлежит клиент
Description	произвольная строка, вносимая администратором, для описания клиента

Допускается **сортировка по столбцам** таблицы клиентов. Значком **^** метится столбец, по которому сортируются данные, если данные в таком столбце одинаковые, то они сортируются по **Client ID**.

Вкладка **Clients** имеет следующие **кнопки управления**:

Кнопка, поле	Описание
All	в таблице отображаются все клиенты группы
Updatable	в таблице отображаются только те клиенты, которые имеют хотя бы одно непримененное обновление или находятся в состоянии <b>ne active</b>
Unsuccessful	в таблице отображаются клиенты в состоянии <b>failed</b> (не смогли применить очередное обновление)
Find	поле для ввода строки, по которой будет происходить поиск клиентов в таблице, содержащих данную строку в любом поле. Если такой клиент найден - он выделяется в списке клиентов.
Next	кнопка запуска поиска следующего клиента, относительно выделенного, удовлетворяющего заданной строке в поле Find. Аналогично нажатию клавиши <b>F3</b>
Prev	кнопка запуска поиска предыдущего клиента, относительно выделенного, удовлетворяющего заданной строке в поле Find. Аналогично нажатию клавиш <b>Shift-F3</b>
Refresh timeout	поле, в котором задается период времени в секундах обновления информации в таблице клиентов
Refresh	кнопка для принудительного обновления информации в таблице клиентов. Нажатие кнопки дает команду для сбора информации обо всех существующих клиентах. Так как процесс сбора информации может быть долгим, то ожидание по кнопке <b>Refresh</b> производится только для выделенных на данный момент клиентов. Отображение обновленной информации для всех остальных клиентов будет произведено позднее, по мере получения полной информации. Аналогично нажатию клавиши <b>F5</b>

Нижняя строка вкладки **Clients** отражает:

**Selected** – количество выделенных на данный момент клиентов

**Displayed** – количество отображаемых на данный момент клиентов

**All** – количество всех клиентов на Сервере управления.

## 18.2. Меню File

Меню **File** включает одно предложение:

**Exit** – завершает работу консоли управления (обслуживание клиентов при этом не завершается).

## 18.3. Меню Groups

Меню **Groups** содержит следующие элементы:

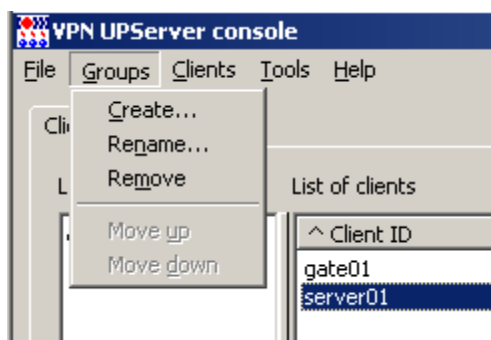


Рисунок 206

**Create...** - вызывает окно **Create new group** создания новой группы (группа создается как подгруппа выделенной группы), в котором надо задать имя группы (Рисунок 207).

**Parent group name** – имя группы, в которой создается подгруппа

**Group name** – имя создаваемой подгруппы.

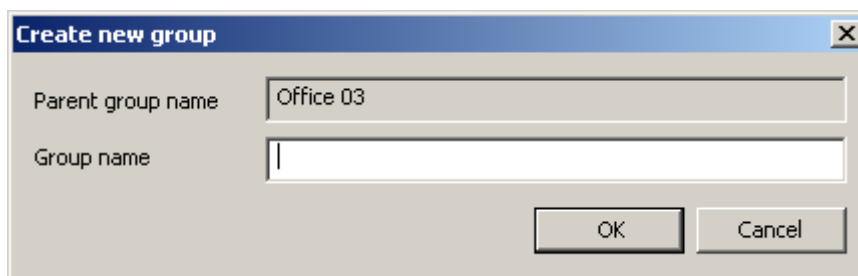


Рисунок 207

**Rename...** - вызывает окно переименования выделенной группы, в котором задается новое имя группы (Рисунок 208).

**Parent group name** – имя группы, в которой переименовывается подгруппа

**Group name** – новое имя подгруппы.

При переименовании группы все входящие в нее клиенты и группы сохраняются.

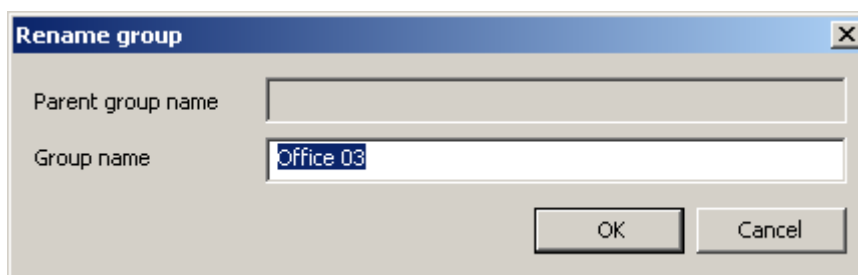


Рисунок 208

**Remove** – удаляет выделенную группу; при этом все клиенты и подгруппы, входящие в нее, перемещаются в группу уровнем выше.

**Move up** – перемещает выделенную группу в списке вверх, сохраняя уровень группы в дереве

**Move down** – перемещает выделенную группу в списке вниз, сохраняя уровень группы в дереве.

## 18.4. Меню Clients

Меню **Clients** содержит следующие элементы:

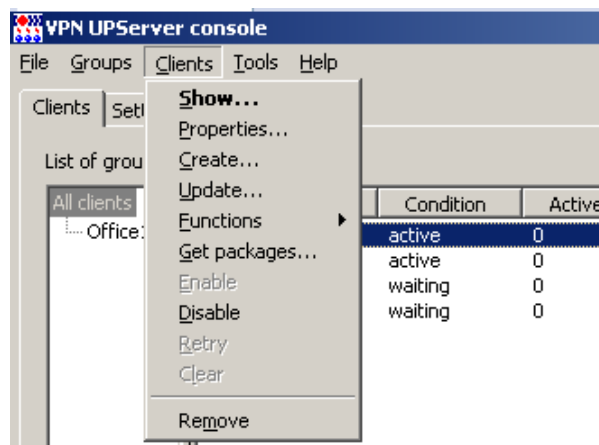


Рисунок 209

**Show...** – вызывает окно отображения параметров существующего клиента (Рисунок 154)

**Properties...** - вызывает окно **Client properties** с информацией об управляемом устройстве и следующими полями:

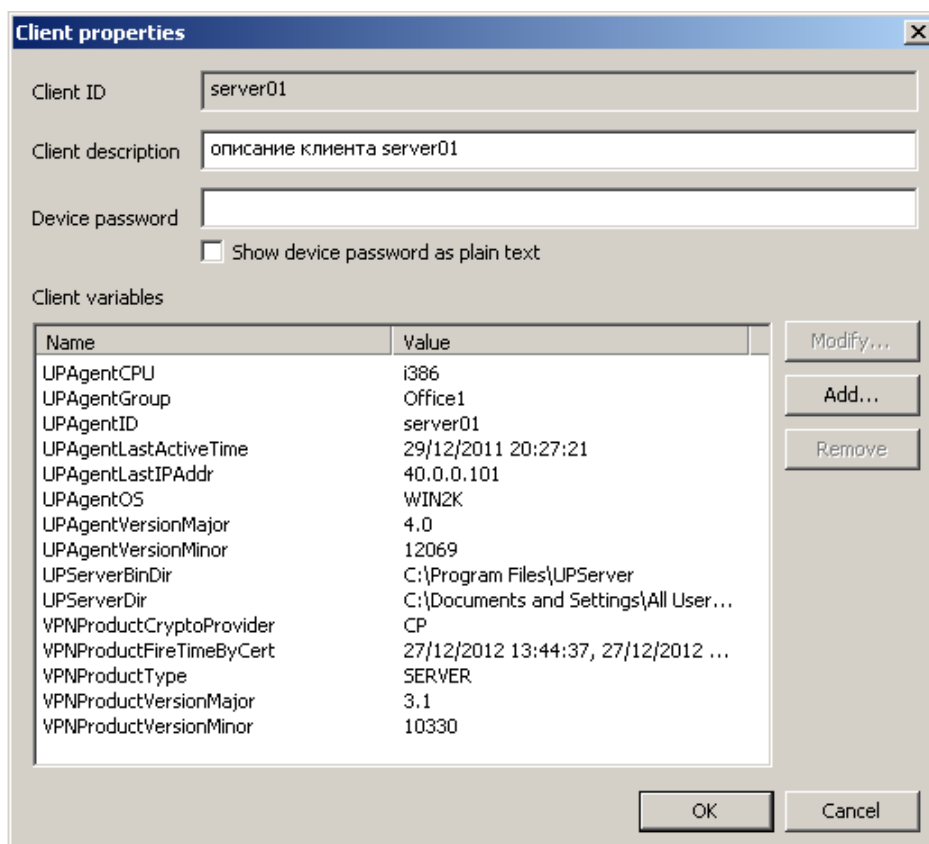


Рисунок 210

**Client ID** - идентификатор клиента

**Client description** – введенная администратором в это поле информация будет отображена в поле *Description* вкладки **Clients** (Рисунок 205)

**Device password** – в данной версии это поле не используется

**Show device password as plain text** – в данной версии этот флаг не используется

**Client variables** – список переменных, описывающих клиента, которые передаются скрипту *cook.bat* при его запуске в процессе подготовки расширенного обновления. Список переменных может быть дополнен администратором, используя кнопку **Add**. Все добавляемые переменные должны начинаться с префикса *EX\_*.

**Create...** – вызывает окно **Create new client** создания нового клиента (Рисунок 85)

**Update...** – вызывает окно **Update client** создания обновления для существующего клиента (Рисунок 211) со следующими полями:

**Client ID** – идентификатор клиента

**Creation time** – дата и время, когда создаваемое обновление будет доступно для скачивания Клиентом управления

**Product package** – имя инсталляционного файла Bel VPN Gate/Client 4.1 (который был создан с помощью продукта Bel VPN Client 4.1 AdminTool) или имя файла с данными продукта Bel VPN Gate/Client 4.1, созданного с помощью окна **VPN data maker**, вызываемого кнопкой **E**

Кнопка **E** – вызывает окно **VPN data maker** (Рисунок 58) для задания политики безопасности и настроек продукта Bel VPN Gate/Client 4.1

**UPAgent folder** – имя каталога, в котором расположен инсталляционный файл Клиента управления (заполняется, если надо установить новую версию Клиента управления)

**UPAgent settings** – имя файла с настройками Клиента управления (заполняется, если надо обновить настройки Клиента управления) (см. главу «[Настройки Клиента управления](#)»)

**Extended data** – путь к каталогу, в котором расположены расширенные данные и скрипты обновления

**Send current UPServer CA certificates to client** – установка флажка для пересылки клиенту вместе с обновлением актуального списка CA сертификатов Сервера управления.

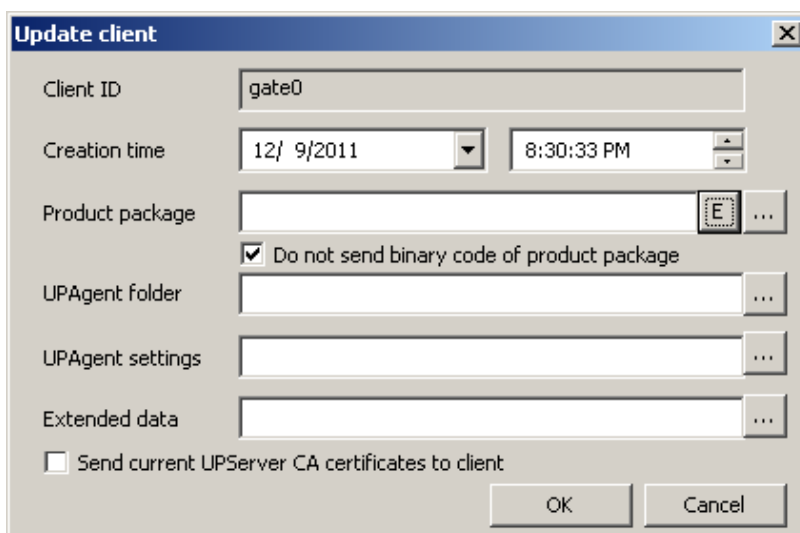


Рисунок 211

**Functions** – вызывает подменю (Рисунок 212):

**Key pairs** – позволяет задать действия с ключевой парой на управляемом устройстве:



**Generate...** – создать ключевую пару на управляемом устройстве. При выборе этого предложения появляется окно **Make key pair** (Рисунок 106) для задания параметров ключевой пары и запроса на сертификат.

**Remove...** – удалить ключевую пару с управляемого устройства, при этом появляется окно **Remove container** (Рисунок 213) для задания параметров удаляемой ключевой пары:

**Creation time** – дата и время, когда Сервер управления сделает доступным для скачивания Клиентом управления пакет обновления, содержащий данные для удаления ключевой пары на управляемом устройстве. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания

**Container name** – имя контейнера на управляемом устройстве, который будет удален. Поле является обязательным для заполнения. В выпадающем списке присутствуют имена существующих, но не используемых VPN-продуктом контейнеров

**Container password** – пароль контейнера, который будет использоваться при удалении. Если это поле не задано, то пароль считается пустым.

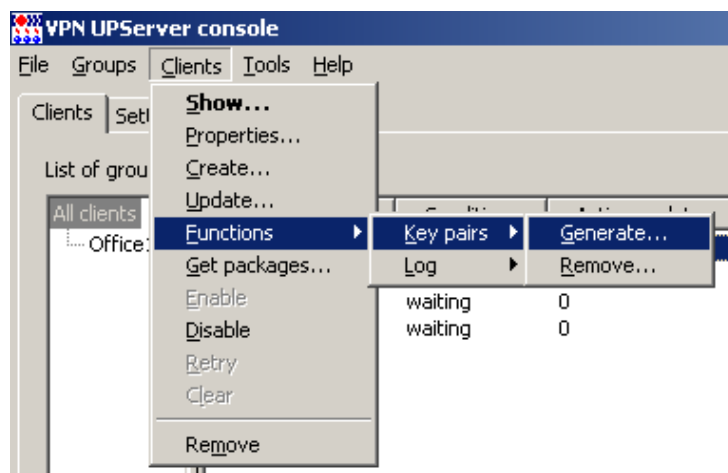


Рисунок 212

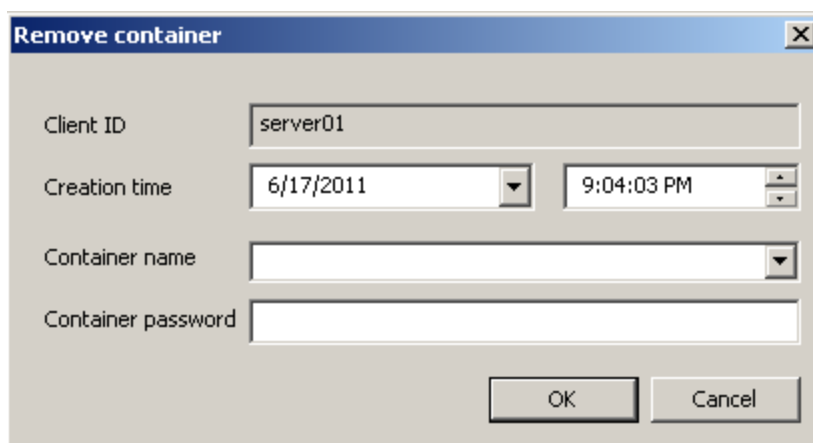


Рисунок 213

**Log** – позволяет задать настройки протоколирования событий на управляемом устройстве, при этом возможны два действия (Рисунок 214):

**Setup...** – задать параметры протоколирования в окне **Setup log** (Рисунок 215):

**Creation time** – дата и время, когда пакет обновления с настройками протоколирования на управляемом устройстве, будет доступен для скачивания. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания

**State** – состояние системы протоколирования:

ON – включить пересылку syslog сообщений в стандартную систему протоколирования операционной системы Windows

OFF – выключить пересылку syslog сообщений в стандартную систему протоколирования операционной системы Windows

Эта настройка работает только для управляемых устройств с ОС Windows. Для устройств с ОС Unix эта настройка не применяется, журналирование на таких устройствах включено по умолчанию и не может быть отключено.

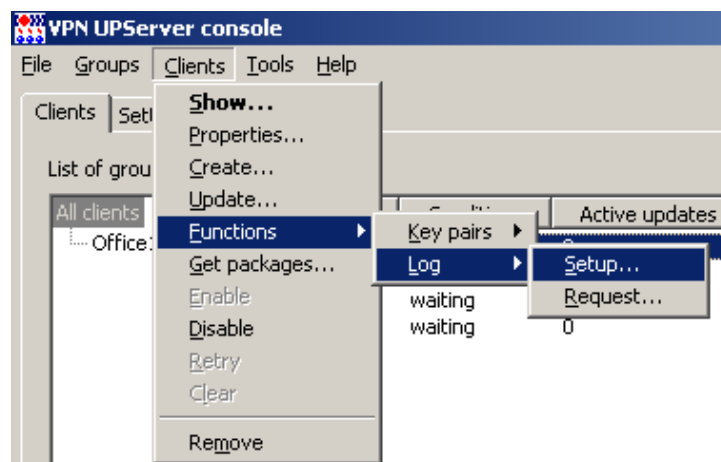


Рисунок 214

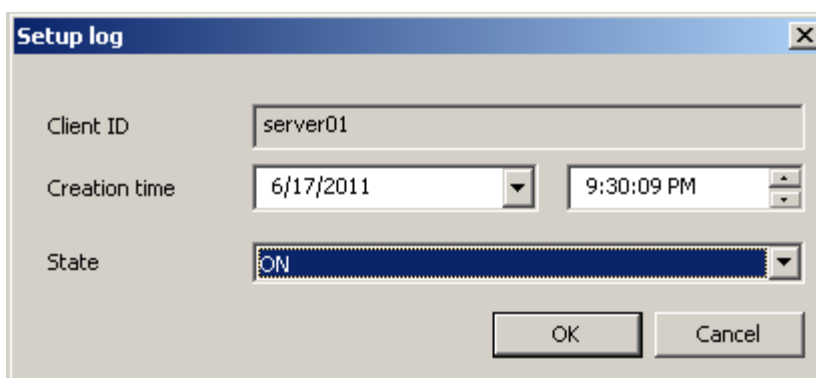


Рисунок 215

**Request...** – запросить данные из системы протоколирования на управляемом устройстве, заполнив в окне **Request log** (Рисунок 216) поле:

**Creation time** – дата и время, когда пакет обновления с запросом данных протоколирования syslog канала, будет доступен для скачивания. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания.

**Get packages...** – вызывает окно запроса каталога, в который будут сохранены инициализационные дистрибутивы для управляемого устройства

**Enable** – включает механизм обмена данными с клиентом

**Disable** – выключает механизм обмена данными с клиентом

**Retry** – снимает признак неудачного обновления, вследствие чего обновление будет скачено Клиентом управления еще раз, без каких либо изменений

**Clear** – удаляет все непримененные обновления для клиента (предназначено для отмены неудачных обновлений)

**Remove** – удаляет информацию о клиенте с Сервера управления.

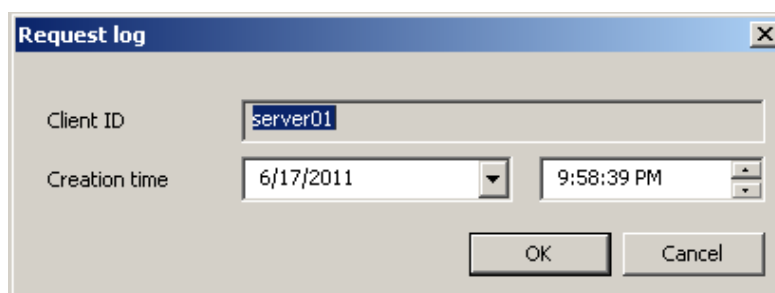


Рисунок 216

## 18.5. Меню Tools

Меню **Tools** содержит предложения [VPN data maker](#), [VPN data converter](#), [UPFlash creator](#), [Statistic DB editor](#) (Рисунок 217):

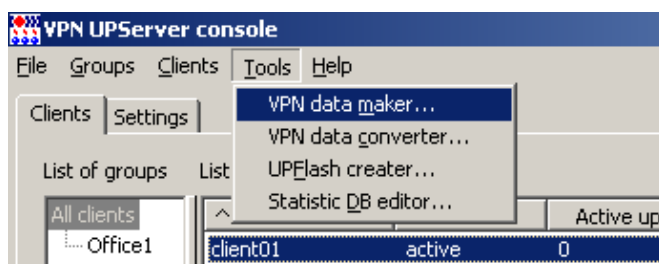


Рисунок 217

Предложение **VPN data maker** вызывает одноименное окно **VPN data maker** для задания настроек продукта Bel VPN Gate/Client 4.1 для нового проекта (Рисунок 218). Сделать это можно с использованием:

- [вкладка данного окна](#)
- или [окон мастера](#), вызываемого кнопкой [Run Wizard](#).

Созданный проект можно [сохранить в файл](#) и использовать при создании обновления для клиента (указать созданный файл в поле **Product package** окна **Update client**).

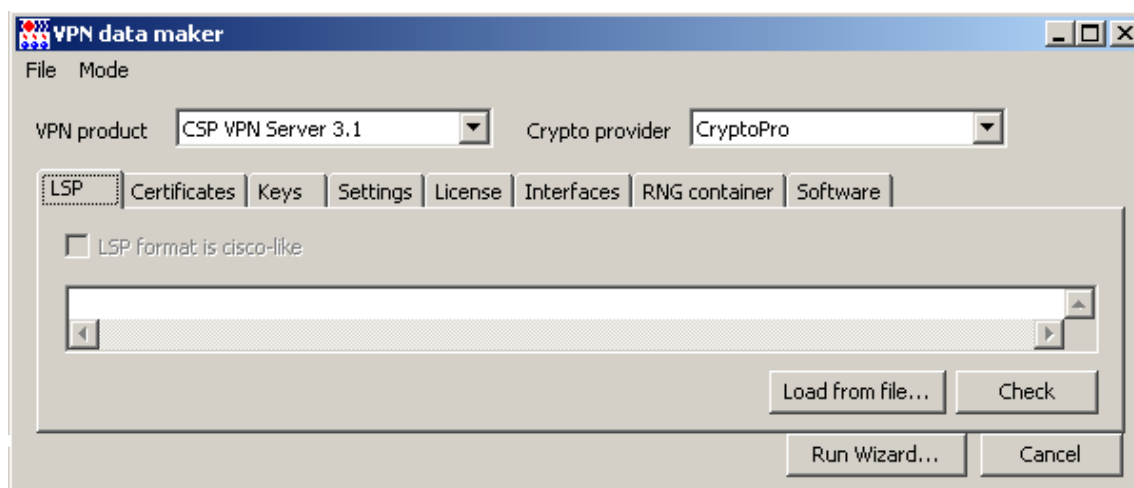


Рисунок 218

### 18.5.1. Задание политики и настроек с использованием вкладок

**VPN product** только в режиме шаблона проекта – выпадающий список, из которого выбирается продукт, для которого далее задаются все настройки во вкладках:

Bel VPN Client 4.1

**Crypto provider** – выпадающий список с используемым криптопровайдером в продукте:

Avest – криптопровайдер ЗАО «Авест»

**LSP** – вкладка для задания локальной политики безопасности продукта Bel VPN Gate/Client, предписанной управляемому устройству (Рисунок 218):

**LSP format is cisco-like** – установка этого флажка говорит о том, что локальная политика безопасности задана в формате cisco-like

**Load from file...** - нажатие этой кнопки вызывает окно для загрузки LSP из файла

**Check** – запускает процесс проверки синтаксиса LSP. В этой версии продукта проверка синтаксиса LSP в виде cisco-like формата не производится

**Run Wizard...** – вызывает **окно мастера** задания настроек.

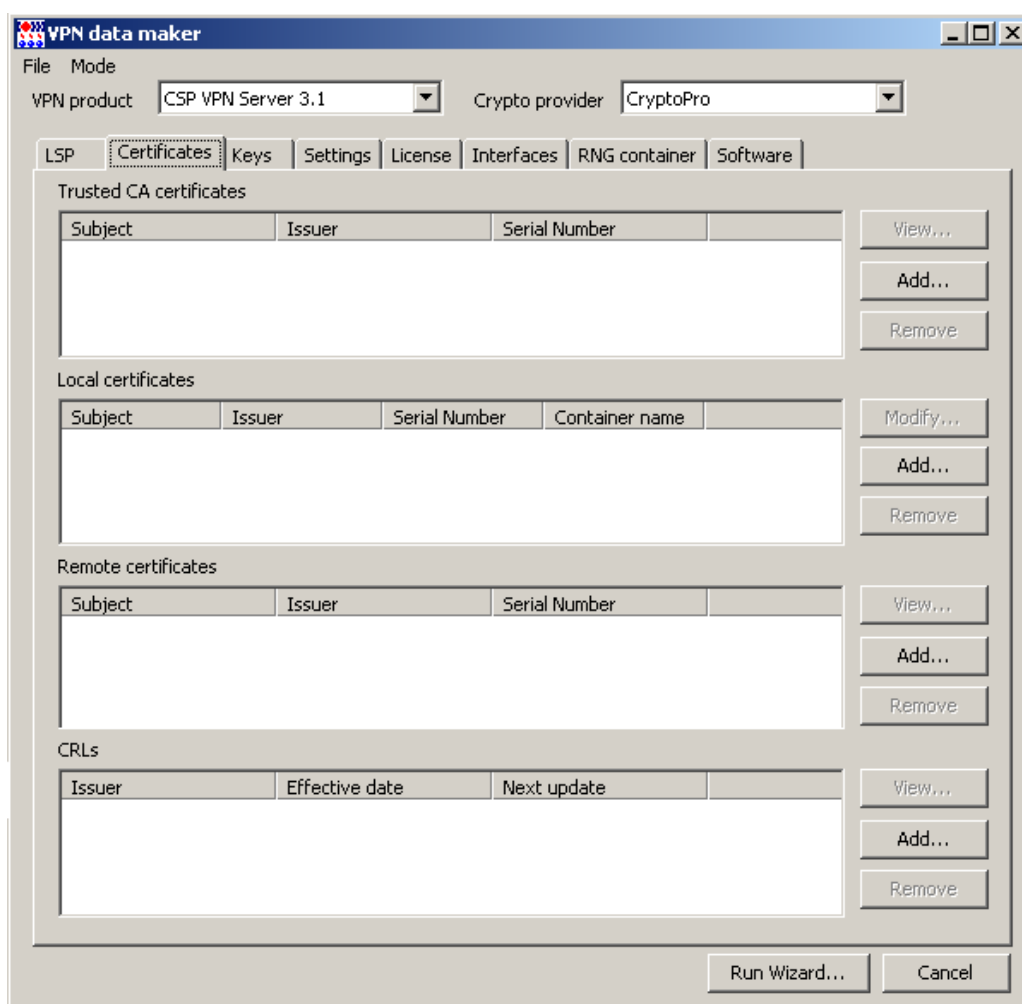


Рисунок 219

**Certificates** – вкладка для задания CA, локальных, партнерских и списков отозванных сертификатов для продукта Bel VPN Gate/Client 4.1 (Рисунок 219).

**Keys** – вкладка для задания предопределенных ключей для работы продукта Bel VPN Gate/Client 4.1 с партнерами (Рисунок 220).

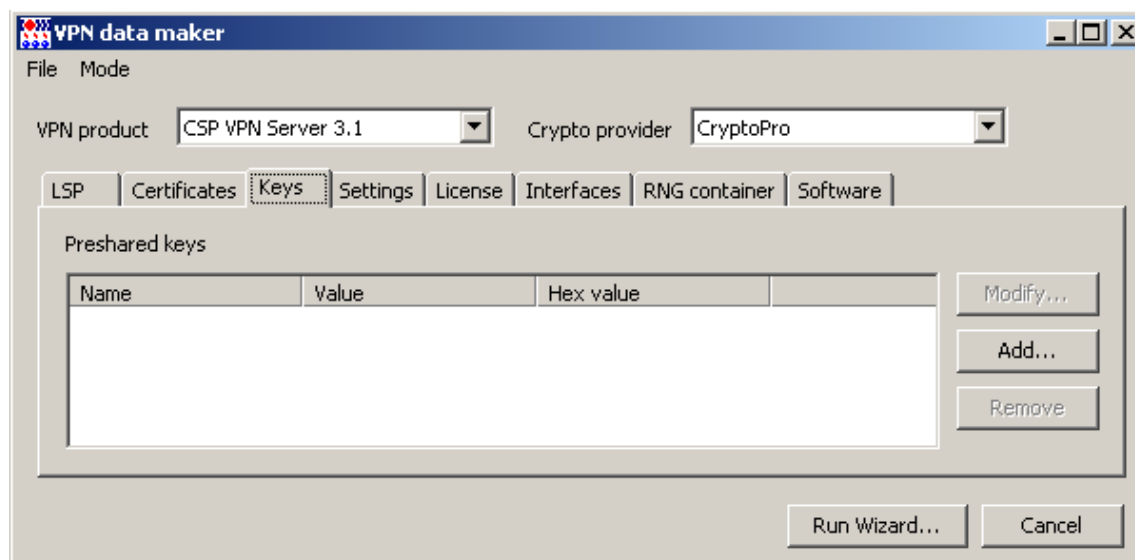


Рисунок 220

**Settings** – вкладка для задания настроек управляемого устройства.

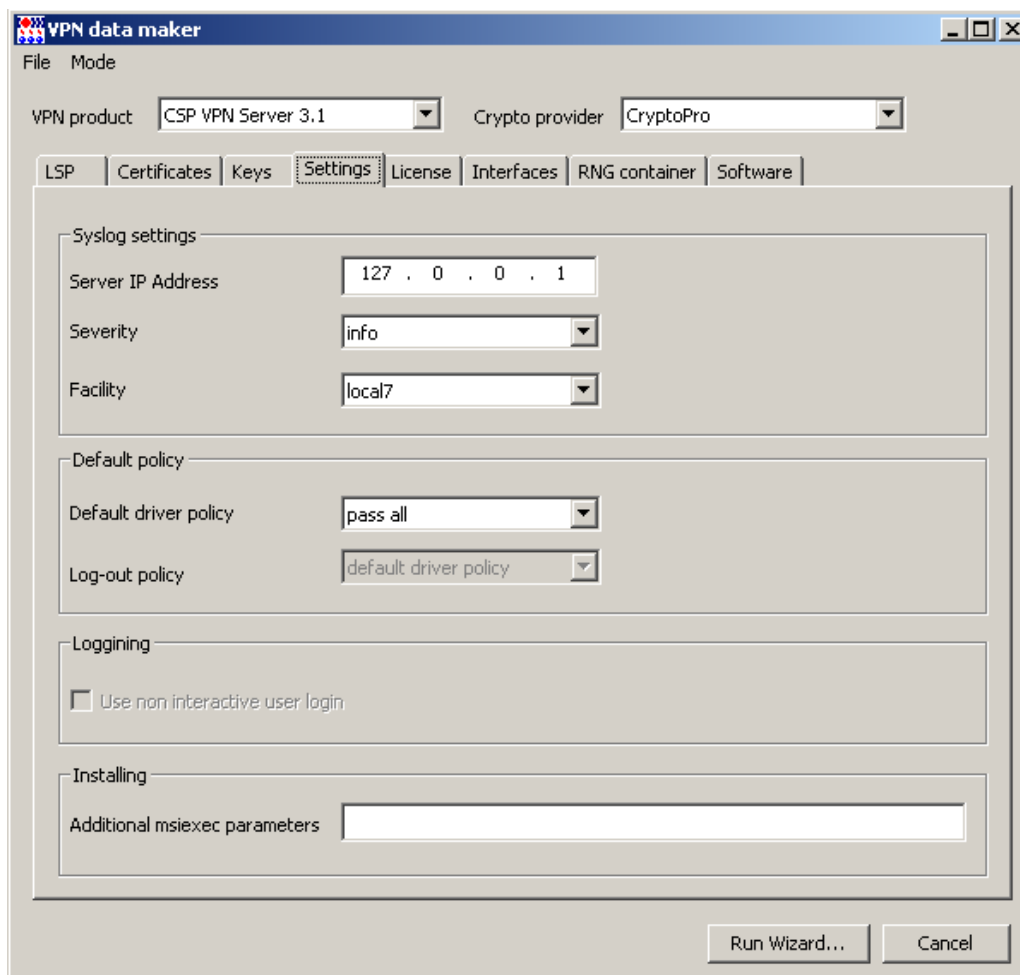


Рисунок 221

**License** – вкладка для ввода данных лицензии на продукт Bel VPN Gate/Client 4.1.

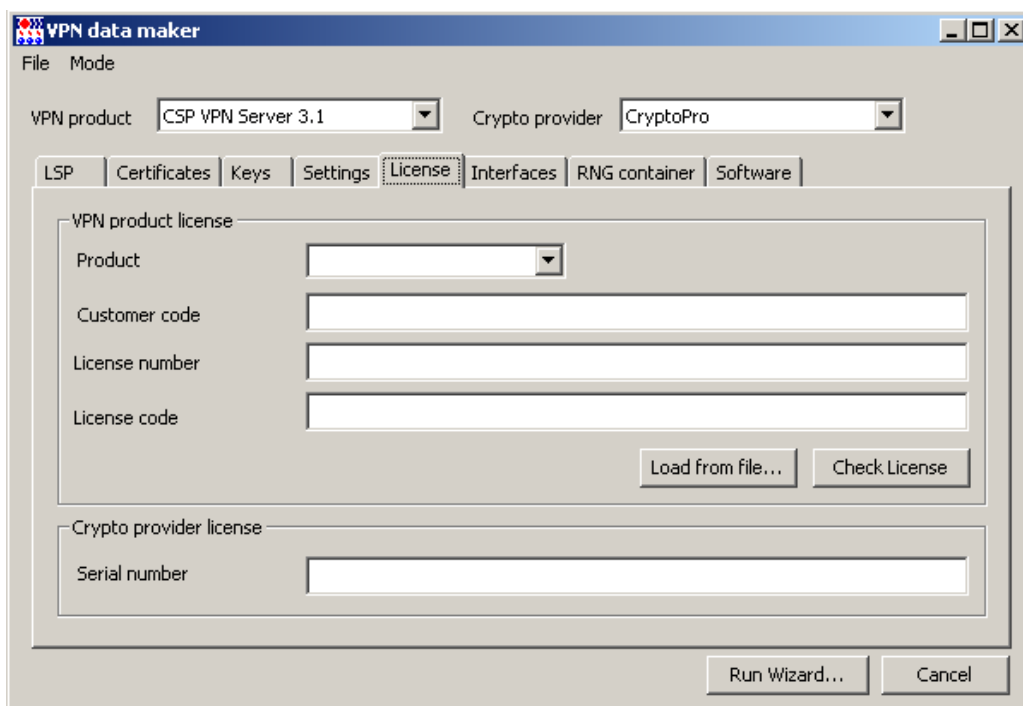


Рисунок 222

**Interfaces** – вкладка для задания настроек сетевых интерфейсов управляемого устройства.

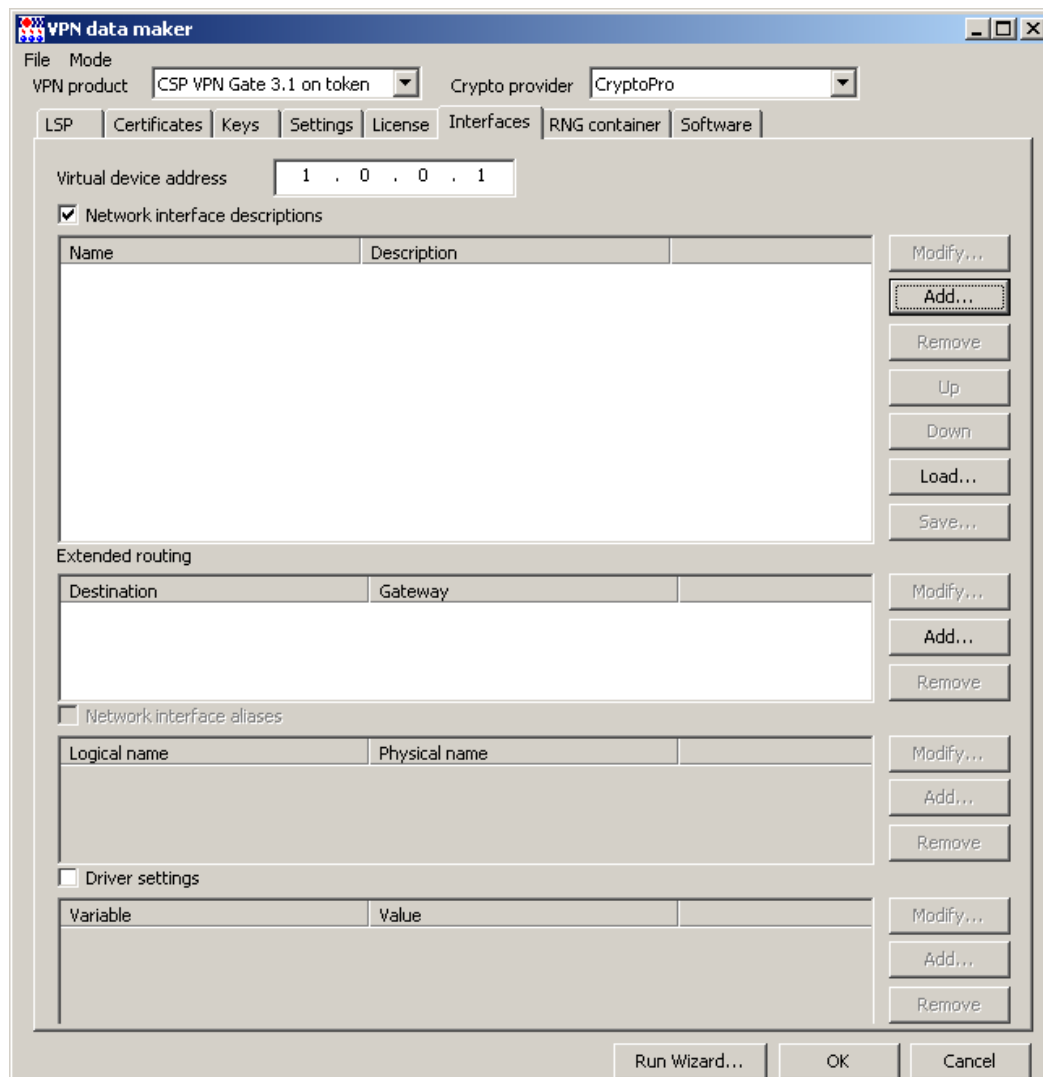


Рисунок 223

**Virtual device address** – поле доступно только для продукта Bel VPN Gate 4.1 on token. В это поле вносится адрес, с которым будут приходить пакеты к партнерам от СПДС «ПОСТ», подключенному к любому компьютеру или терминалу (описано в разделе «Настройка СПДС «ПОСТ»).

**Network interface description** – этот раздел доступен только для продукта Bel VPN Gate 4.1 on token, в котором можно задать интерфейсы и сетевые настройки. Эти же настройки можно задать в профайлах и загрузить по кнопке [Load](#). Редактирование настроек выполняется в окне **Edit connection**, появляющемся при нажатии кнопки [Add](#).

#### Окно Edit connection

В этом окне настраиваются для СПДС «ПОСТ» профили как проводных соединений (Ethernet) так и беспроводных (Wi-Fi). Для настройки соединения с мобильной сетью WiMAX см. примечание в разделе «Проводное соединение».

#### Проводное соединение (Ethernet)

Для настройки проводного соединения следует установить в поле «Connection type» значение «Wired».

**Connection type** – тип соединения: «Wired» – проводное соединение, «Wireless» – беспроводное соединение Wi-Fi.

**Connection ID** – идентификатор соединения, свободное текстовое поле.

**Method** – метод получения IP-адреса для соединения: «Auto» – автоматическое получение адреса по протоколу DHCP, «Manual» – задание адресов вручную.

**Edit connection**

Connection type: **Wired**

Connection ID:

Method: **Auto**

DHCP client ID:

Interface addresses

Address	Mask	Gateway
<input type="text"/>		

DNS servers:

Search domains:

MTU:

MAC address:

☒ Autoconnect

Connection check: **true**

Speed test: **true**

Рисунок 224

**DHCP client ID** – идентификатор клиента, передается на сервер DHCP при запросе адреса. Свободное текстовое поле.

**Interface addresses** – область для задания IP-адресов интерфейса. Доступна только при настройке вручную.

**DNS servers** – список IP-адресов DNS серверов. Если в поле **Method** установлено значение «Auto», то перечисленные здесь адреса добавляются к списку полученному от сервера DHCP. IP-адреса в списке разделяются двоеточием или запятой или пробелом.

**Search domains** – список DNS суффиксов по-умолчанию, которые используются при разрешении доменных имён. Формат поля – список доменных имён, разделенных двоеточием или запятой или пробелом.

**MTU** – MTU соединения, значение по-умолчанию – 0. Допустимые значения 0-65535.

**MAC address** – MAC адрес сетевой платы, для которой описывается соединение. Формат - шесть пар шестнадцатеричных символов без разделителя или разделенных двоеточием или запятой или пробелом. Поле можно оставить пустым, тогда соединение будет устанавливаться с использованием первой попавшейся сетевой карты в компьютере, но это может привести к невозможности установления соединения, если в компьютере установлено несколько сетевых карт.

**Autoconnect** – пытаться или нет установить соединение автоматически при старте сеанса работы пользователя.

**Connection check** – скрипт для проверки возможности установления соединения с удалённым сервером. Выбор из списка фиксированных значений, с возможностью редактирования.

**Speed test** – скрипт для проверки качества (скорости) соединения. Выбор из списка фиксированных значений, с возможностью редактирования.

**Примечание:**

Для настройки соединения с мобильной сетью типа WiMAX так же следует использовать настройки проводного соединения и (обязательно) в поле **Connection ID** указывать значение «wimax». Это связано с тем, что модемы работающие в такой сети работают в режиме эмуляции проводного Ethernet соединения, но для правильной настройки модема требуется отличать его от обычного проводного соединения, что делается по полю **Connection ID**.

### **Беспроводное соединение Wi-Fi**

Во вкладке **General** задаются общие настройки для беспроводного соединения, такие же как и описанные в разделе проводного соединения. Во вкладке **WiFi settings** задаются специфичные настройки для беспроводного соединения. Эта вкладка изменяется в зависимости от настройки оборудования и безопасности сети. Некоторые настройки имеют очень специальное техническое значение и не описываются даже в документации на Network Manager, а дается ссылка на документацию wpa\_supplicant (это утилита для настройки беспроводной сети).



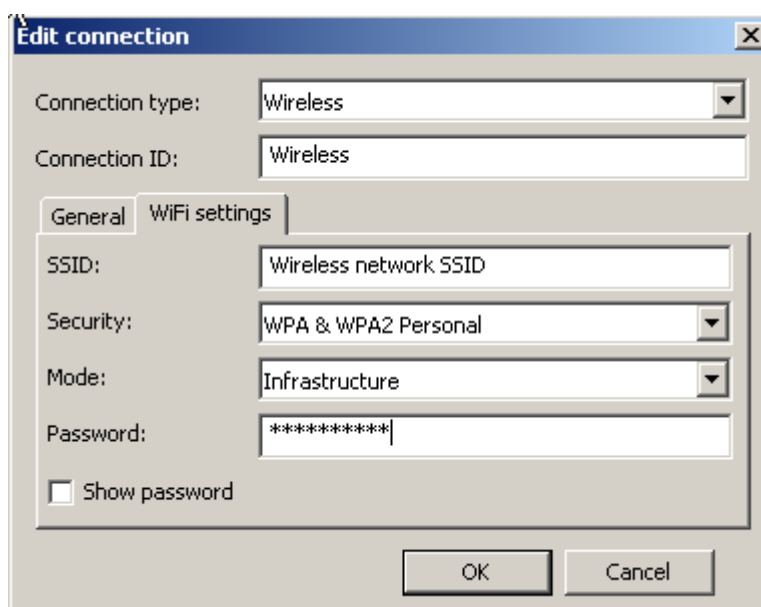


Рисунок 225

**SSID** – идентификатор беспроводной сети. Свободное текстовое поле.

**Security** – базовый алгоритм безопасности сети. Предустановленный список значений: «None» – открытая сеть, «WEP 40/128-bit key (hex or ASCII)» и «WEP 128-bit passphrase» – варианты защиты сети по алгоритму WEP, различаются способом задания ключа (в настоящий момент объявлены устаревшими, т.к. используют криптографические алгоритмы недостаточной стойкости), «WPA & WPA2 Personal» – сеть защищена с помощью алгоритма WPA с использованием разделяемого ключа, «WPA & WPA2 Enterprise» – аутентификация пользователя в сети производится с помощью сервера RADIUS с использованием протокола EAP, предназначено для использования в корпоративных сетях.

**Mode** – режим настройки сети: «Infrastructure» – доступ к сети обеспечивается через точку доступа, «Ad-hoc» – децентрализованная самоорганизующаяся беспроводная сеть, не имеющая постоянной структуры, нет точек доступа.

**Band** – поле доступно, если в поле **Mode** выбрано значение «Ad-hoc». Диапазон работы беспроводной сети: «Automatic» – нет предпочтения, «A (5 GHz)» и «B/G (2,4 GHz)».

**Channel** – поле доступно, если в поле **Mode** выбрано значение «Ad-hoc». Номер канала в выбранном диапазоне. Свободное текстовое поле, можно вводить только цифры.

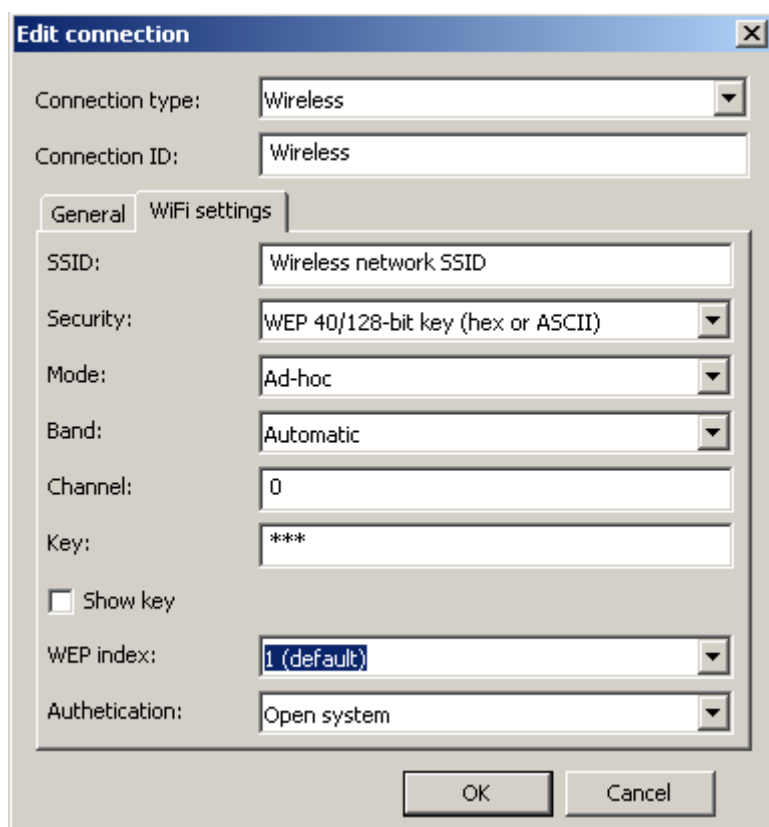


Рисунок 226

**Key** – поле доступно, если в поле **Security** выбран один из вариантов WEP. Ключ доступа к беспроводной сети, защищённой с помощью алгоритма WEP. Допустимые значения зависят от выбранного варианта в поле «Security»: «WEP 40/128-bit key (hex or ASCII)» – длина ключа фиксирована ровно 5 или 13 символов, или второй вариант - ровно 10 или 26 шестнадцатеричных цифр, «WEP 128-bit passphrase» – нет ограничений, но перед доставкой профиля на СПДС «ПОСТ» вычисляется хеш введённого ключа, который и используется в дальнейшем, и обратно получить исходный ключ не представляется возможным (так работает Network Manager, если сказать другими словами, то исходный ключ в профиле сохраняется пока профиль находится в продукте S-Terra КП, а на СПДС «ПОСТ» передается хеш этого ключа).

**Show key** – Доступно только при выборе одного из вариантов WEP в поле **Security**. Флажок, который позволяет показать открытым текстом ключ доступа к сети.

**WEP index** – поле доступно, если в поле **Security** выбран один из вариантов WEP. Задаёт используемый индекс ключа WEP. Выбор из списка предустановленных значений: «1 (default)», «2», «3» и «4». **Примечание:** Редактор позволяет задать до четырёх ключей, переключая значения в этом поле.

**Authentication** – выбор алгоритма аутентификации пользователя для доступа к сети. Допустимые значения зависят от выбранного варианта в поле **Security**: для любого из вариантов WEP – «Open system» и «Shared key»; для «WPA & WPA2 Enterprise» – «LEAP», «Tunneled TLS» и «Protected EAP (PEAP)»; с другими значениями поля **Security** данное поле не используется.

**Anonymous ID** – фальшивое имя пользователя, передаваемое открытым текстом и используемое на первой фазе аутентификации пользователя, для сокрытия истинного имени. Доступно только при выборе в поле **Security** значения «WPA & WPA2 Enterprise», а в поле **Authentication** - значения «Tunneled TLS» или «Protected EAP (PEAP)».

**Username** – имя пользователя для входа в сеть. Доступно только при выборе в поле **Security** значения «WPA & WPA2 Enterprise».

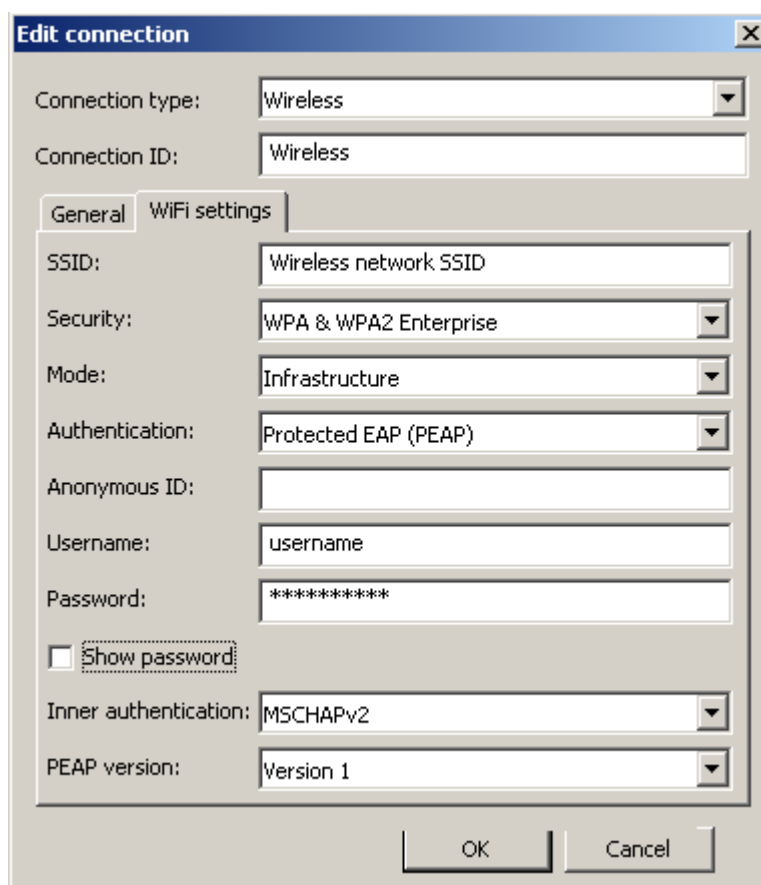


Рисунок 227

**Password** – пароль пользователя для входа в сеть. Доступно только при выборе в поле **Security** значения «WPA & WPA2 Enterprise».

**Show password** – флажок, который позволяет показать открытым текстом пароль доступа к сети. Доступно только при выборе одного из вариантов WPA в поле **Security**.

**Inner authentication** – протокол аутентификации второй фазы. Выбор из списка предустановленных значений зависит от значения, установленного в поле **Authentication** – для «Tunneled TLS»: «PAP», «CHAP», «MSCHAP» или «MSCHAPv2»; для «Protected EAP (PEAP)»: «MSCHAPv2» или «MD5». С другими значениями поле **Authentication** не используется.

**PEAP version** – версия протокола PEAP: «Version 0» и «Version 1».

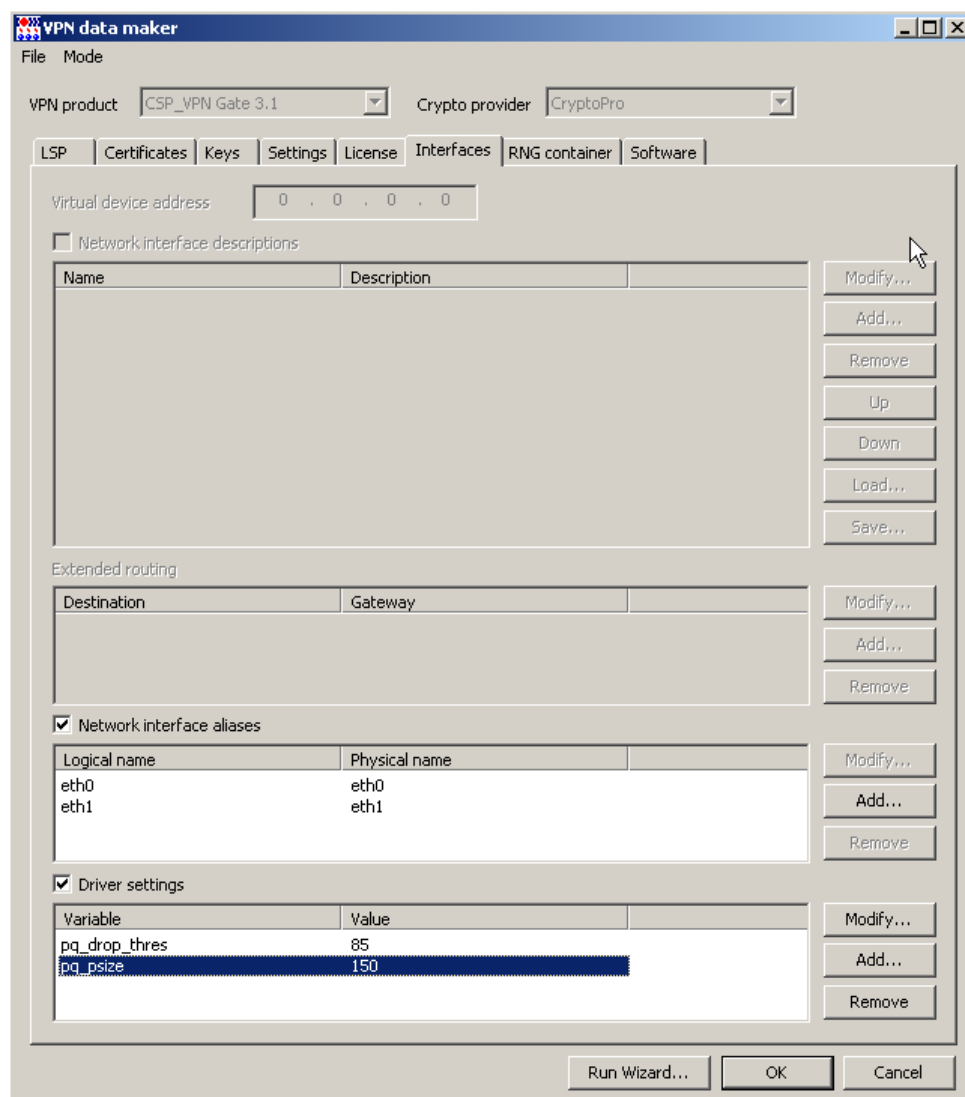


Рисунок 228

**Network interface aliases** – установка этого флажка позволяет добавлять, модифицировать, удалять логические и физические имена сетевых интерфейсов

**Driver settings** – установка флажка позволяет изменить настройки IPsec драйвера, установленные по умолчанию (Рисунок 229). Эти настройки имеются только у продукта Bel VPN Gate 4.1. Описание этих настроек (утилита `drv_mgr`) см. в документе «Специализированные команды», входящем в состав «Руководства администратора Программный комплекс Bel VPN Gate 4.1».

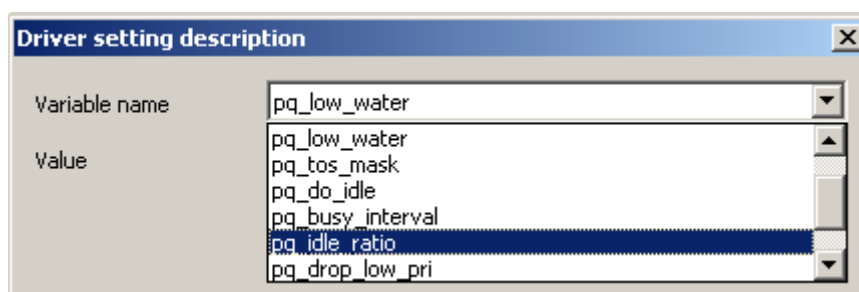


Рисунок 229

**RNG container** – вкладка задания местоположения криптографического (RNG) контейнера, содержащего инициализационные данные для датчика случайных чисел (ДСЧ).

При создании дистрибутива продукта Bel VPN Client 4.1 надо указать имя каталога для нового контейнера, если указанного каталога нет - он будет создан. При создании обновления для этих продуктов указывается уже существующий RNG контейнер. Для продукта Bel VPN Gate 4.1 процедура инициализации выполняется только один раз, поэтому в этой вкладке указывается уже существующий RNG контейнер, как при создании дистрибутива, так и при создании обновления.

В этой вкладке может использоваться подстановка %INSTALLDIR%, которая означает каталог, в который установлен Bel VPN Gate/Client. Значения по умолчанию – каталоги Bel VPN Client 4.1, Bel VPN Gate 4.1.

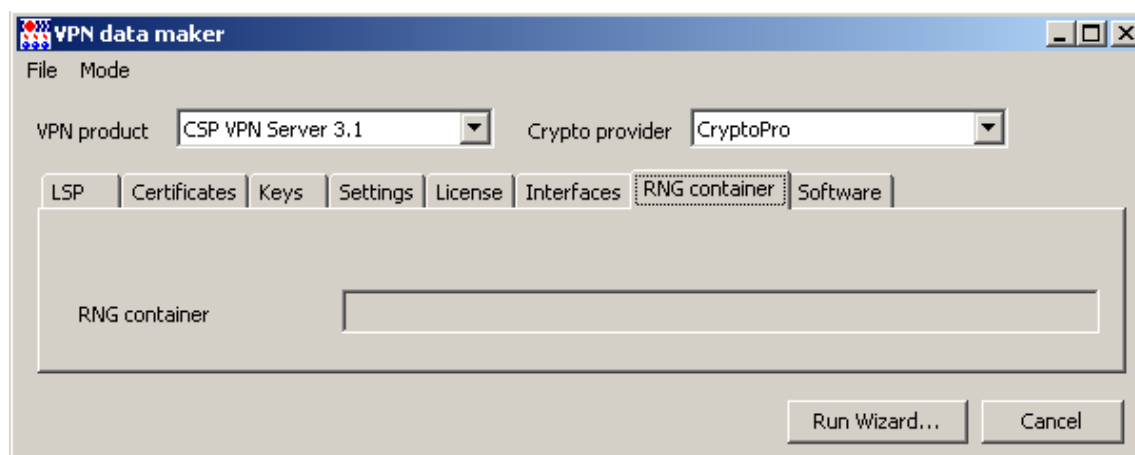


Рисунок 230

**Software** – вкладка для задания настроек дополнительных продуктов, установленных на управляемом устройстве (Рисунок 231).

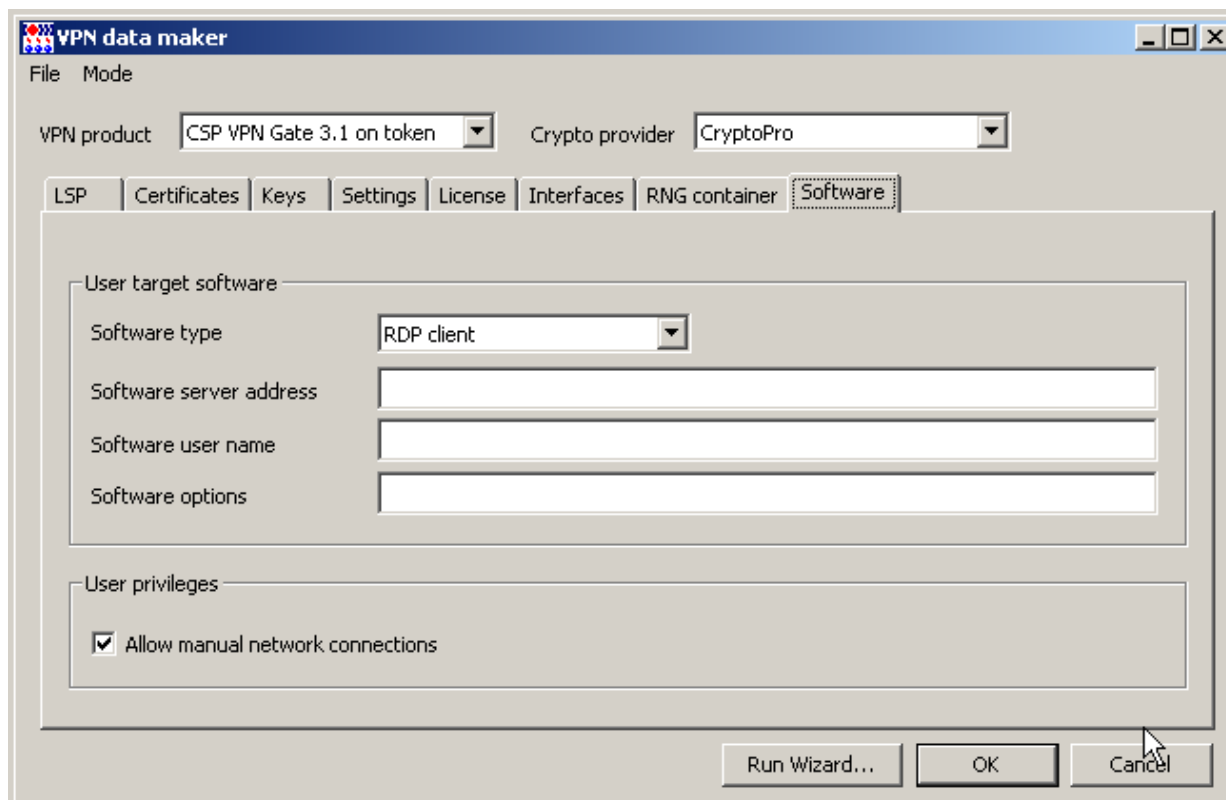


Рисунок 231

### Сохранение и загрузка настроек продукта

Меню **File** окна **VPN data maker** содержит два предложения (Рисунок 232):

**Load** – загружает настройки из файла данных продукта Bel VPN Gate/Client 4.1.

**Save as** – сохраняет в файл данные продукта Bel VPN Gate/Client 4.1, отраженные во вкладках окна **VPN data maker**.

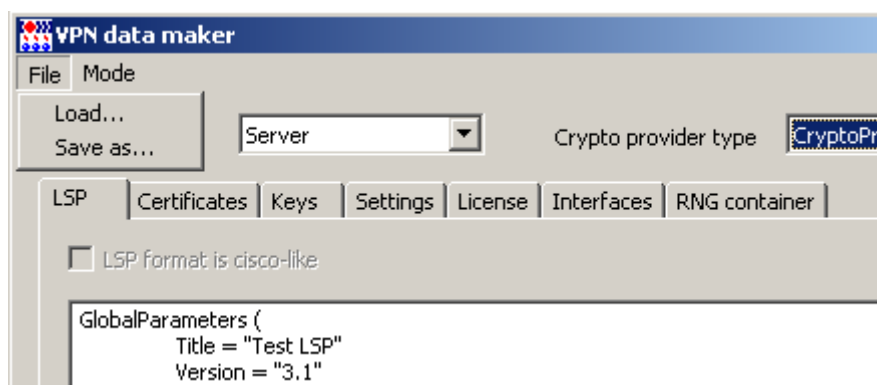


Рисунок 232

### 18.5.2. Задание политики и настроек с использованием мастера

При нажатии кнопки **Run Wizard** в окне **VPN data maker** появляется первое окно мастера для задания сертификатов и предопределенных ключей (Рисунок 233).

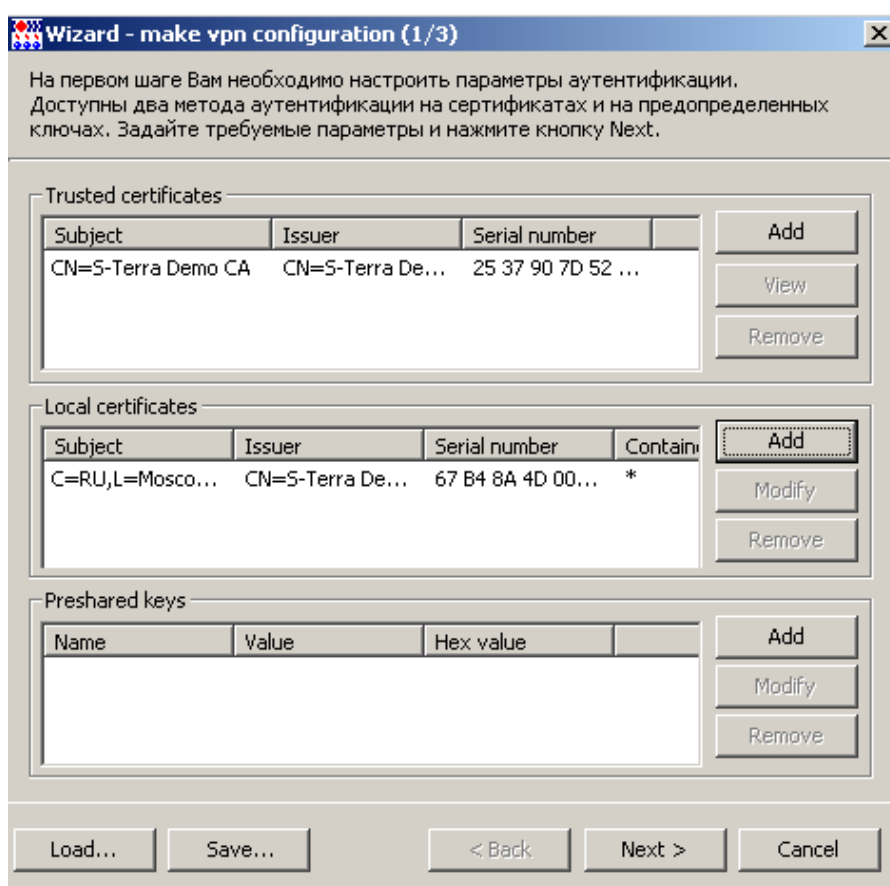


Рисунок 233

При добавлении локального сертификата появляется окно для задания имени контейнера с секретным ключом локального сертификата и пароля к нему (Рисунок 234). Если на управляемом устройстве есть запрос на сертификат и контейнер к нему, то достаточно указать в качестве контейнера и пароля «\*», при применении обновления они будут сопоставлены с локальным сертификатом.

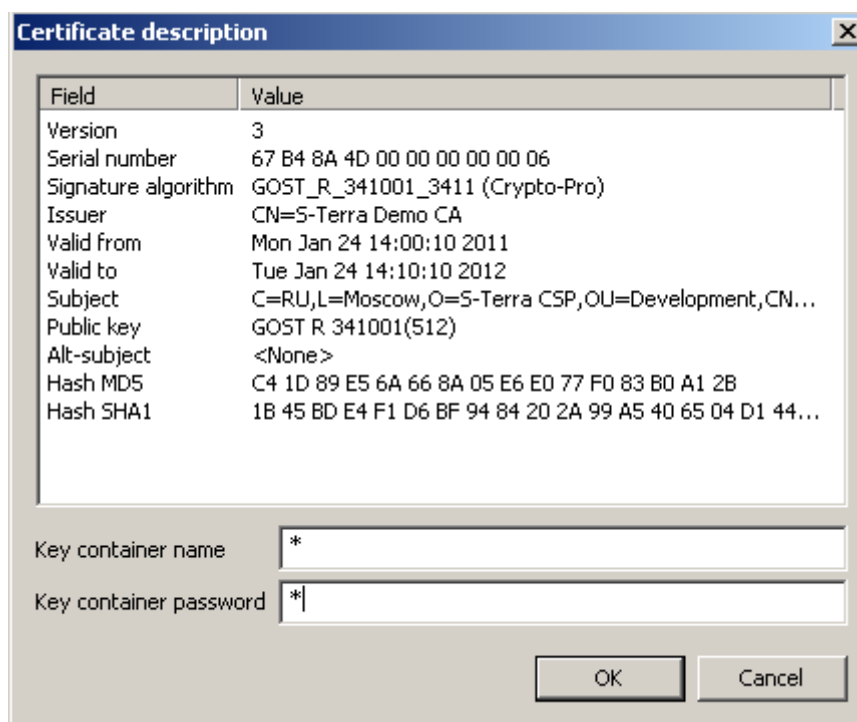


Рисунок 234

Во втором окне мастера задаются правила фильтрации и защиты трафика. Задание правил и ввода лицензионной информации были описаны в разделе [«Настройка и управление центральным шлюзом»](#).

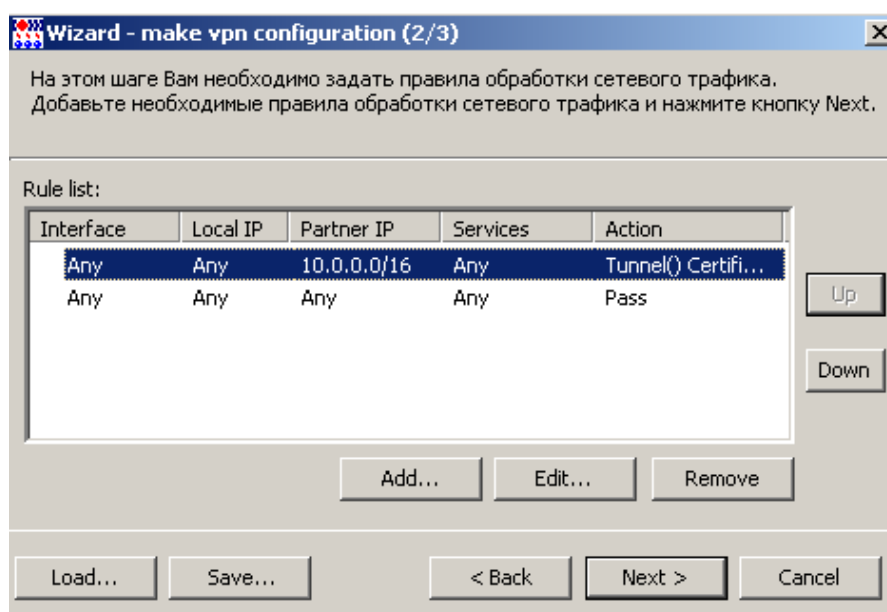


Рисунок 235

В окне задания правила в разделе **Action** кнопка [Advanced settings](#) предназначена для задания расширенных настроек правила (Рисунок 236).

Рисунок 236

В первой вкладке **IKE settings** расширенных настроек представлен упорядоченный список алгоритмов, который предлагается партнеру для согласования, который может использоваться для защиты трафика при создании ISAKMP соединения (Рисунок 237).

**IKE proposals** – упорядоченный список IKE предложений по приоритету. В верхней строчке находится предложение с наивысшим приоритетом.

**Encryption** – предлагаемые алгоритмы шифрования пакетов. Предлагаются следующие белорусские криптографические алгоритмы:

- СТБ 34.101.31-2011 (подразделы 6.3, 6.5 раздела 6);
- ГОСТ 28147-89.

Также предлагается международный алгоритм шифрования AES-256.

**Integrity** – предлагаемые алгоритмы проверки целостности пакетов. Предлагаются следующие белорусские криптографические алгоритмы:

- СТБ 34.101.31-2011 (раздел 6.9)
- СТБ 1176.1-99.

Также предлагается международный алгоритм SHA1.

**Group** – параметры выработки общего сессионного ключа по алгоритму Диффи-Хеллмана:

*BELTDH* – протокол формирования общего ключа на основе эллиптических кривых согласно СТБ 34.101.66-2014 (приложение А).



*MODP\_768* – группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана)

*MODP\_1024* – группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана)

*MODP\_1536* – группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

**Enable Aggressive Mode** – установка этого флажка позволяет использовать агрессивный режим обмена информацией о параметрах защиты и установления ISAKMP SA. В этом режиме партнеру высылается только первая IKE политика из списка, имеющая самый высокий приоритет. При выборе этого режима выдается об этом предупреждение. Если для аутентификации используется предопределенный ключ и выбран тип идентификатора *KeyID*, то должен использоваться только режим Aggressive. При отсутствии этого флажка используется основной режим - партнеру высылаются все IKE политики для выбора и согласования.

**LifeTime (sec)** – время в секундах, в течение которого ISAKMP SA будет существовать. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 28800, которое выставлено при открытии нового проекта. Значение 0 означает, что время действия SA не ограничено. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

**LifeTime (Kb)** – указывает объем данных в килобайтах, который могут передать стороны во всех IPsec SA, созданных в рамках одного ISAKMP SA. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 0, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

**IPsec SA** – количество IPsec SA, созданных в рамках одного ISAKMP SA. Значение 0 означает, что количество IPsec SA не ограничено.

**Certificate (send)** – задает логику отсылки локального сертификата на запрос партнера в процессе первой фазы IKE. В своем запросе партнер может указать какому CA сертификату он доверяет. Если такой сертификат не найден, то он не отсылается. Возможные значения:

*AUTO* – автоматически определяется, когда необходима отсылка локального сертификата партнеру (значение по умолчанию).

*NEVER* – сертификат не высылается.

*ALWAYS* – сертификат высылается всегда.

*CHAIN* – сертификат высылается всегда, причем в составе с цепочкой доверительных CA. Имеется ввиду цепочка сертификатов, построенная от локального сертификата до CA, который удовлетворяет описанию, присланному партнером в запросе. В общем случае это CA, удовлетворяющий запросу партнера, произвольное количество промежуточных CA и локальный сертификат.

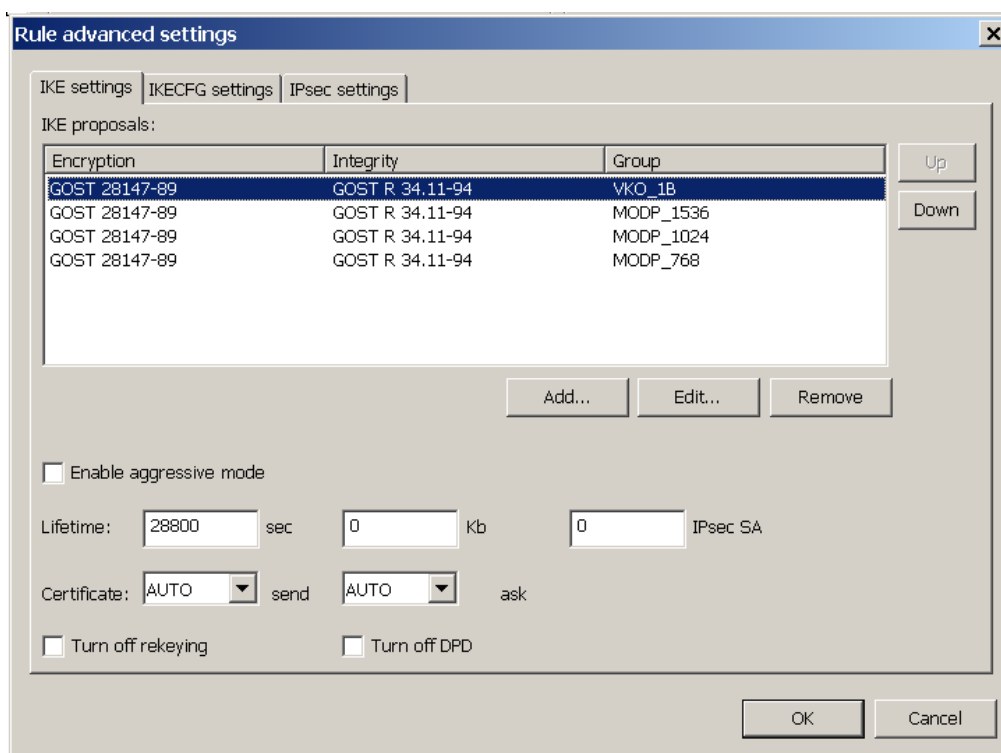


Рисунок 237

**Certificate (ask)** – задает логику отсылки запроса на сертификат партнера. Возможные значения:

*AUTO* – запрос высылается, если возможный сертификат партнера отсутствует (значение по умолчанию).

*NEVER* – запрос не высылается.

*ALWAYS* – запрос высылается всегда.

**Turn off rekeying** – установка этого флажка приводит к тому, что заблаговременная смена ключевого материала (сессионного ключа) не проводится.

**Turn off DPD** – установка этого флажка отключает использование протокола DPD для проверки IKE соединения.

Во второй вкладке **IKECFG settings** (Рисунок 238) задаются данные для использования протокола IKECFG.

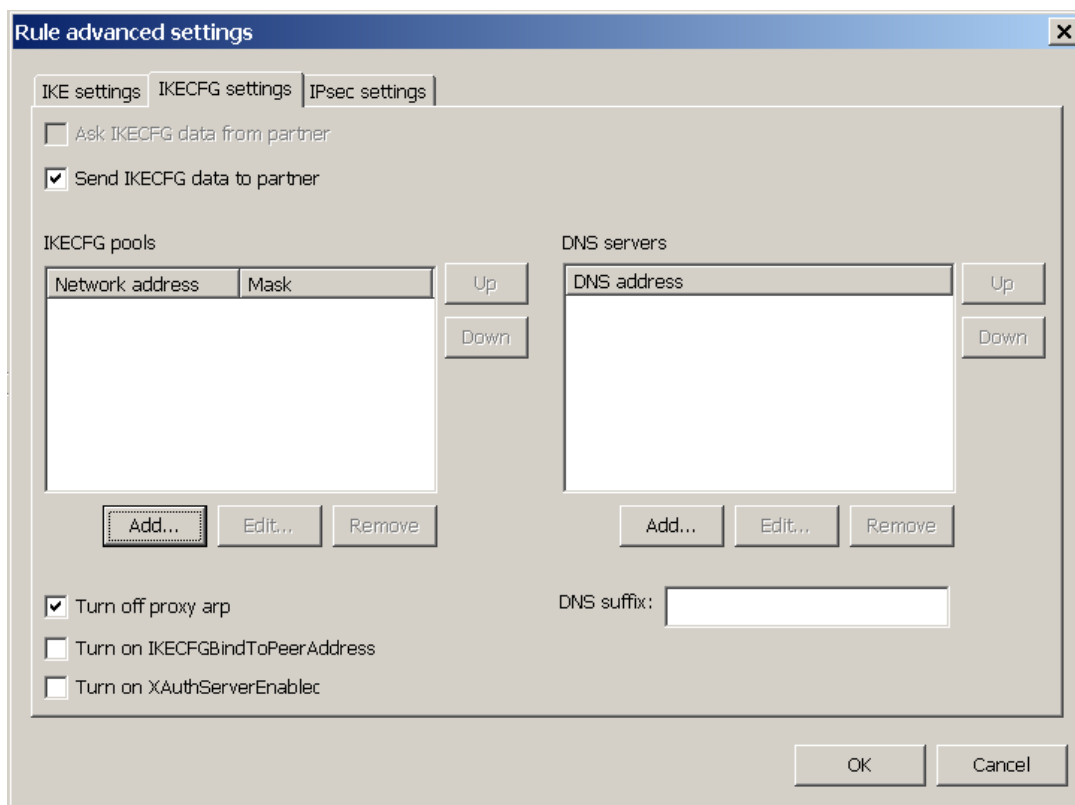


Рисунок 238

**Ask IKECFG data from partner** – при установке этого флажка у партнера будут запрашиваться данные по протоколу IKECFG – адрес из пула, адреса DNS серверов, DNS суффиксы (для продуктов Bel VPN Client 4.1).

**Send IKECFG data to partner** – при установке этого флажка партнеру будут передаваться данные по протоколу IKECFG: адрес из пула, адреса DNS серверов, DNS суффиксы (для продуктов Bel VPN Gate 4.1).

**IKECFG pools** – в этом поле следует задать адреса IKECFG пулов (для продуктов Bel VPN Gate 4.1).

**DNS servers** – в этом поле следует задать адреса DNS серверов (для продуктов Bel VPN Gate 4.1).

**DNS suffix** – в этом поле следует задать DNS суффикс (для продуктов Bel VPN Gate 4.1).

**Turn off proxy arp** –

*при установке этого флажка - адреса не проксируются*

*при снятии флажка - при неустановленном флажке Bel VPN Gate выступает в роли ProхуARP для указанного множества адресов пула. Если IP-адрес не попадает ни в одну из защищаемых локальных подсетей, проху-арп запись не создается, и это не считается ошибкой*

**Turn on IKECFGBindToPeerAddress** –

*при установке этого флажка - IKECFG сервер будет идентифицировать клиентов по IP-адресу и порту партнера (видимые гейту, по которым построен ISAKMP SA)*

*при снятии флажка - идентификация клиентов осуществляется по ID первой фазы IKE).*

**Turn on XauthServerEnable** –

*при установке этого флажка – Bel VPN Gate выступает в роли XAuth-сервера. Для данного IKE правила шлюз требует поддержку метода аутентификации с использованием XAuth. После успешного построения ISAKMP SA, Bel VPN Gate инициирует XAuth-сессию.*

*при снятии флажка – Bel VPN Gate работает в обычном режиме, XAuth-обмены не проводятся.*

В третьей вкладке **IPsec settings** (Рисунок 239) задаются параметры, которые используются при защите трафика. Партнеру направляется список наборов преобразований, по протоколу IKE происходит согласование и выбор конкретного набора преобразований, который будет использоваться для защиты трафика одного SA.

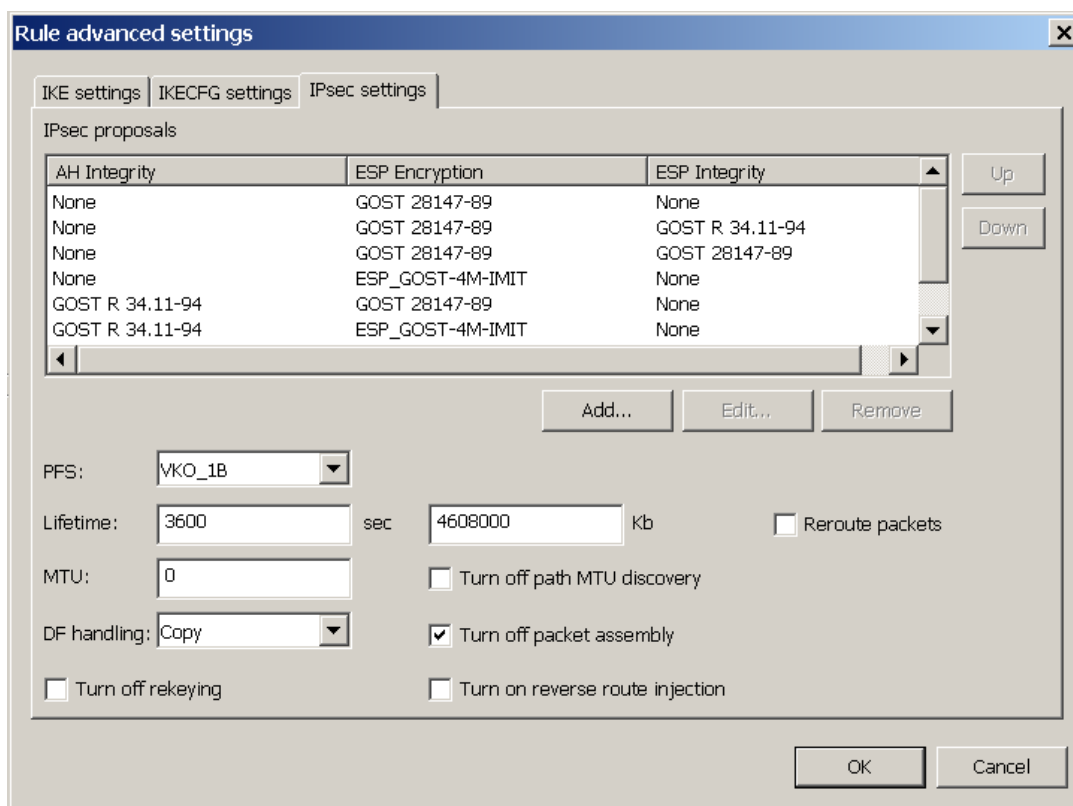


Рисунок 239

**IPsec Proposals** – упорядоченный по приоритету список наборов преобразований, высылаемых партнеру для согласования. При помощи кнопок Up и Down выполняется упорядочивание списка по приоритету. В верхней строчке находится набор преобразований с наивысшим приоритетом.

**AH Integrity** – предлагаемые алгоритмы проверки целостности пакета по протоколу AH. Имеются следующие значения:

- *None* – алгоритм проверки целостности не применяется;
- *СТБ 34.101.31-2011 (раздел 6.6)* – белорусский криптографический алгоритм;
- *СТБ 1176.1-99* – белорусский криптографический алгоритм;
- *ГОСТ 28147-89* – белорусский криптографический алгоритм;
- *SHA1* – международный криптографический алгоритм.

**ESP Integrity** – предлагаемые алгоритмы проверки целостности пакета по протоколу ESP. Имеются следующие значения:

- *None* – алгоритм проверки целостности не применяется;
- *СТБ 34.101.31-2011 (раздел 6.6)* – белорусский криптографический алгоритм;
- *СТБ 1176.1-99* – белорусский криптографический алгоритм;
- *ГОСТ 28147-89* – белорусский криптографический алгоритм;
- *SHA1* – международный криптографический алгоритм.

**ESP Encryption** – предлагаемые алгоритмы шифрования пакетов по протоколу ESP:

- *None* – алгоритм шифрования ESP не применяется;

- *Null* – алгоритм применять, но не шифровать;
- *СТБ 34.101.31-2011* (раздел 6.4) – белорусский криптографический алгоритм;
- *ГОСТ 28147-89* – белорусский криптографический алгоритм;
- *AES-256* – международный криптографический алгоритм.

**PFS**– параметры выработки ключевого материала, высылаемые партнеру для согласования:

*No PFS* – опция PFS не включена и при согласовании новой SA новый обмен по алгоритму Диффи-Хеллмана для выработки общего сессионного ключа не выполняется. Ключевой материал заимствуется из первой фазы IKE.

Выбранный параметр означает, что при согласовании новой SA выполняется новый обмен ключами по алгоритму Диффи-Хеллмана в рамках IPsec. Может использоваться один из параметров:

*BELTDH* – используется алгоритм Диффи-Хеллмана на эллиптических кривых по СТБ 34.101.66-2014 (Приложение А).

*MODP\_768* – группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана).

*MODP\_1024* – группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана).

*MODP\_1536* – группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

**LifeTime (sec)** – время в секундах, в течение которого IPsec SA будет существовать.

Возможное значение – целое число из диапазона 1..2147483647. Рекомендуемое значение – 3600, которое выставлено при открытии нового проекта. Пустая строка и значение 0, которое означает неограниченное время жизни IPsec SA, – недопустимы, при создании инсталляционного файла будет выдано сообщение об ошибке.

**LifeTime (Kb)** – указывает объем данных в килобайтах, который могут передать стороны в рамках одной IPsec SA. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 4608000, которое выставлено при открытии вкладки. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

**Reroute packets** – повторная маршрутизация пакета:

*при установке этого флажка* – исходящий пакет после цикла обработки не отправляется в драйвер сетевого интерфейса, а направляется для повторной маршрутизации. Такой пакет может попасть на повторную обработку IPsec драйвером, так что правила фильтрации должны учитывать и пропускать такие пакеты. Устанавливать данный флажок имеет смысл для SA, заменяющих адрес назначения. Если по ходу обработки пакета адрес назначения не изменился, флаг reroute packets игнорируется.

*при снятии флажка* – пакет не будет подвергаться повторной маршрутизации/

**MTU** – задает значение MTU для IPsec SA, создаваемых по данному правилу, значение MTU используется только для исходящих пакетов и для последнего SA, примененного к пакету (в случае вложенного IPsec значение MTU для внутреннего SA игнорируется). Значение - целое число из диапазона 1..65535, рекомендуется устанавливать значение MTU не менее 670 байт, значение 0 означает, что MTU определяется автоматически.

**Turn off path MTU discovery**

*при установке этого флажка* - отключается алгоритм "Path MTU Discovery" (выявление максимального размера пакета, проходящего на всем пути от отправителя к получателю без фрагментации) для IPsec SA, создаваемых по данному правилу. ICMP-сообщения не обрабатываются, значение MTU вычисляется только из локальной конфигурации. *при снятии флажка* - обрабатываются ICMP-сообщения типа destination unreachable/fragmentation needed, приходящих в ответ на IPsec-пакеты. На основе этих сообщений вычисляется эффективное значение MTU трассы.

**DF handling** – задает алгоритм формирования DF ( Don't Fragment) бита внешнего IP-заголовка для туннельного режима IPsec:

*COPY* – копировать DF бит из внутреннего заголовка во внешний заголовок

*SET* – всегда устанавливать DF бит внешнего заголовка в 1

**CLEAR** – всегда сбрасывать DF бит внешнего заголовка в 0.

**Turn off packet assembly** – сборка пакета из IP-фрагментов перед инкапсуляцией в IPsec:

*при установке этого флажка* – пакет не подвергается сборке

*при снятии флажка* – пакет будет собран из IP-фрагментов перед инкапсуляцией в IPsec. Рекомендуется устанавливать при работе по защищенному соединению с предыдущими версиями Шлюза безопасности. В транспортном режиме IPsec сборка пакетов перед инкапсуляцией производится всегда.

**Turn off rekeying** – задает режим "мягкой" смены ключевого материала:

*при установке этого флажка* – заблаговременная смена ключевого материала (rekeying) не проводится. При отсутствии подходящего IPsec соединения, новый IPsec SA создается только по запросу из ядра – при наличии исходящего IP-пакета, либо по инициативе партнера. В результате, во время создания нового IPsec SA IP-трафик приостанавливается, а при интенсивном трафике возможна потеря пакетов.

*при снятии флажка* – заблаговременно, незадолго до окончания действия IPsec соединения, на его основе (с теми же параметрами) проводится IKE-сессия (Quick Mode) по созданию нового IPsec SA – rekeying. Rekeying не проводится, если за время существования старого SA под его защитой не было никакого трафика.

**Turn on reverse route injection** – включение механизма RRI:

*при установке этого флажка* – после установления защищенного соединения с удаленным партнером, при включенном механизме RRI, в системную таблицу маршрутизации автоматически добавляется запись об обратном маршруте

*при снятии флажка* – механизм RRI выключен, при создании SA по этому IPsec правилу дополнительных действий не предпринимается.

### 18.5.3. Конвертирование политики

При выборе предложения **vpn data converter** появляется окно **VPN data converter** для преобразования политики безопасности из одной версии продукта в другую, из текстового представления (LSP) в cisco-like формат или наоборот.

При переходе на управляемом устройстве с одной версии продукта на другую и для перевода отлаженной политики безопасности в другую версию, можно использовать окно **VPN data converter**. Конвертирование отлаженной работающей политики применимо и для настройки другого управляемого устройства с другой версией продукта Bel VPN Gate/Client.

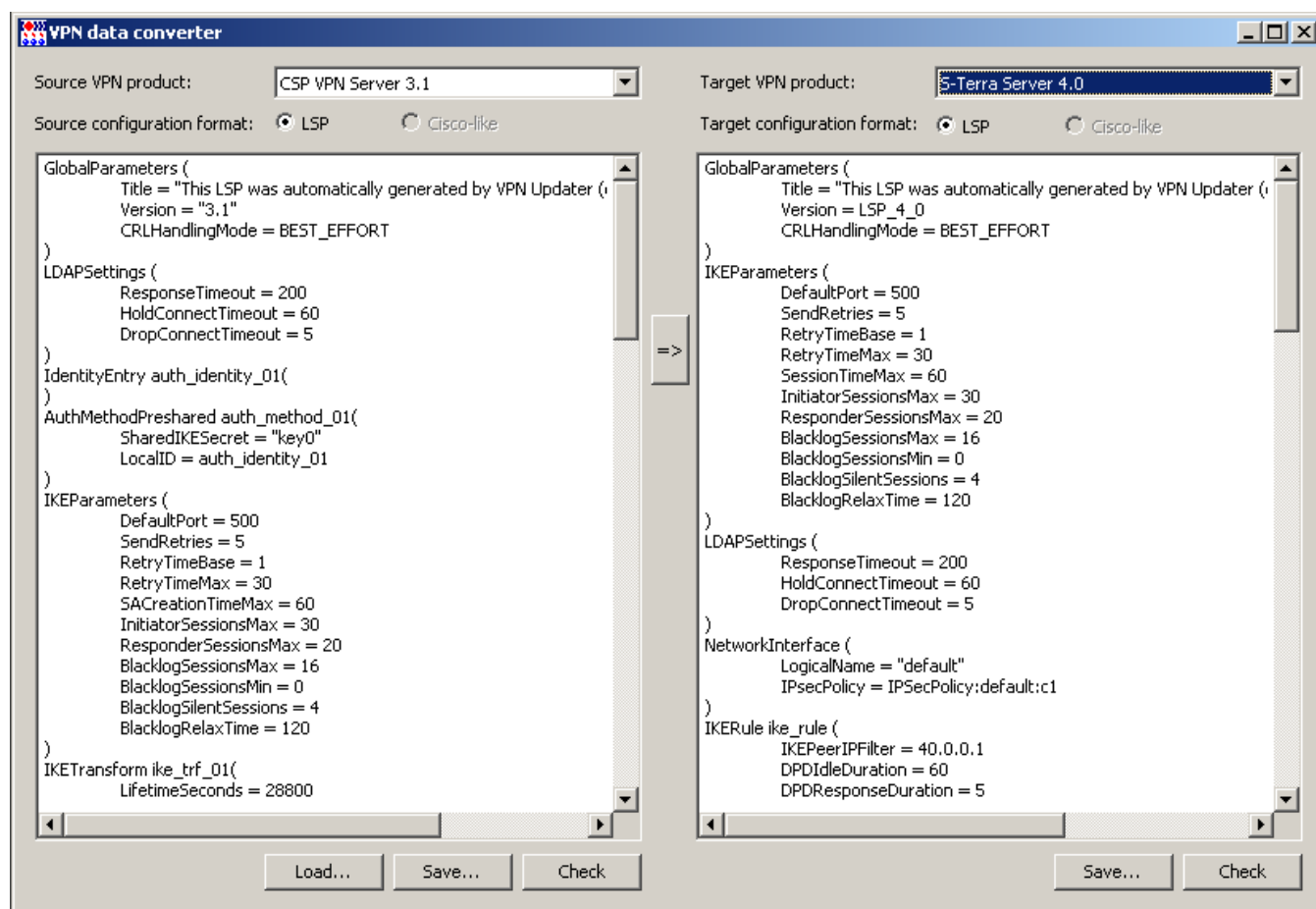


Рисунок 240

#### 18.5.4. Создание носителя с образом диска

При выборе предложения **UPFlash creator** появляется окно **UPFlash creator** для создания USB Flash, который можно использовать для восстановления образа Bel VPN Gate 4.1 на шлюзах или изменения версии образа.

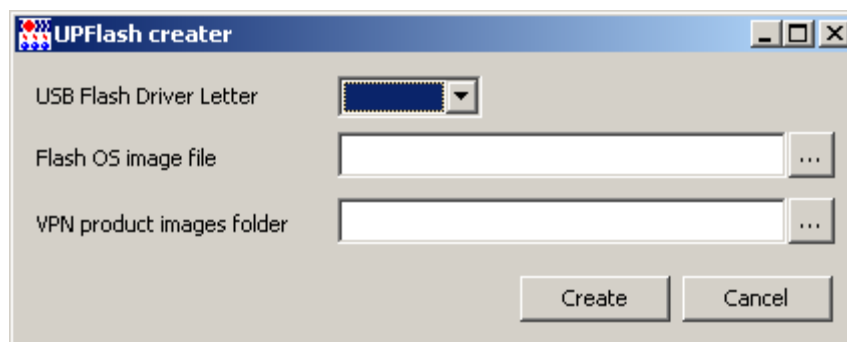


Рисунок 241

**USB Flash Driver Letter** – имя диска, которым представляется USB Flash носитель. На этот носитель будут записаны данные, позволяющие использовать этот USB Flash носитель как загрузочный для шлюзов.

**Flash OS image file** – образ операционной системы, которая будет использоваться как базовая для загрузки с создаваемого USB Flash носителя. Данный файл можно будет скачать с сайта компании или запросить в службе поддержки

**VPN product images folder** – каталог с образами шлюзов. Эти образы будут скопированы на USB Flash носитель и будут использованы для загрузки на шлюзы. Данные файлы можно будет скачать с сайта компании или запросить в службе поддержки.

## 18.5.5. Редактирование настроек базы данных

При выборе предложения **Statistic DB editor** появляется окно **Statistic DB editor...** для редактирования настроек базы данных, которая используется для хранения статистических данных об управляемых устройствах.

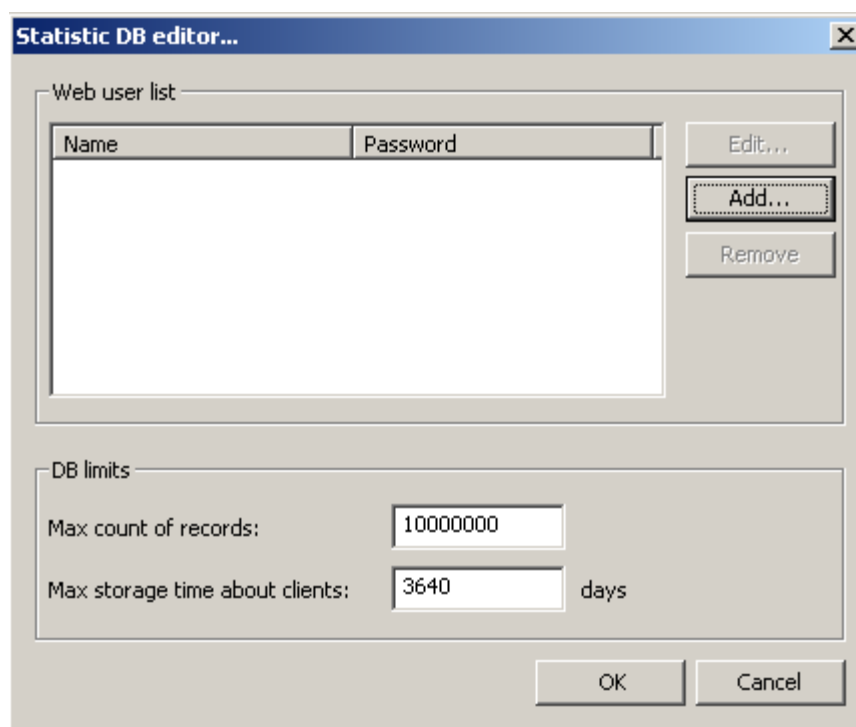


Рисунок 242

**Web user list** – список пользователей базы данных статистики, которые могут работать с данными базы данных через Web браузер, заходя на сервер под именами и паролями заданными в этом списке. (адрес для доступа к базе данных статистики [https://АДРЕС\\_СЕРВЕРА:8443/](https://АДРЕС_СЕРВЕРА:8443/))

**Max count of records** – максимальное количество записей статистики, полученных от всех управляемых устройств (по умолчанию каждое устройство присылает около 5000 записей в час)

**Max storage time about clients** – максимальное количество дней, которое будет храниться информация о действиях администратора, связанных с изменениями имен клиентов или групп клиентов (добавление/удаление/переименование клиентов или групп клиентов).

## 18.6. Меню Help

В меню **Helps** предложение **About VPN UPSever console** выводит информацию о продукте.

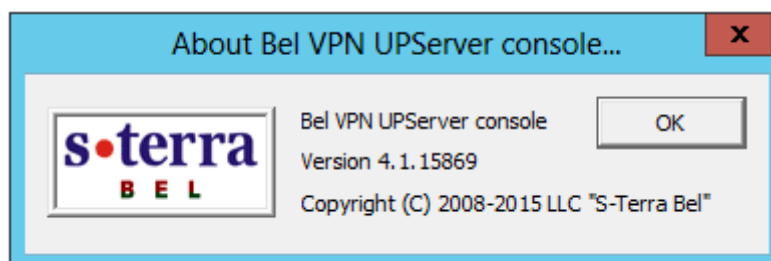


Рисунок 243





## 19. Протоколирование событий

---

### 19.1. Сервер управления

Все сообщения о протоколируемых событиях Сервера управления по умолчанию записываются в файл:

`C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log.`

### 19.2. Клиент управления

На управляемом устройстве все сообщения о протоколируемых событиях Клиента управления по умолчанию записываются в файл:

для ОС Windows - `C:\Program Files\UPAgent\upagent.log`

для ОС Unix - `/var/log/upagent/upagent.log`

Эти же сообщения передаются на Сервер управления и их можно посмотреть во вкладке **Uplog** окна **Client information**, вызываемом выделением клиента в таблице и предложением **Show** в контекстном меню.

### 19.3. Продукт Bel VPN Gate/Client

На управляемом устройстве все сообщения от продукта **Bel VPN Gate/Client** передаются Клиентом управления на Сервер управления и их можно посмотреть во вкладке **VPNlog** окна **Client information**, вызываемом выделением клиента в таблице и предложением **Show** в контекстном меню.

Кроме того, на управляемом устройстве все сообщения о протоколируемых событиях работы продукта **Bel VPN Gate 4.1** передаются на локальный syslog-сервер:

- в файл `/var/log/cspvpngate.log` для аппаратных платформ с жестким диском
- в файл `/tmp/cspvpngate.log` для аппаратных платформ с флеш-диск

Протоколирование работы некоторых утилит и сервисов передается в специальные файлы. Все сообщения и настройка syslog-клиента и сервера описаны в документе «Программно-аппаратный комплекс Bel VPN Gate 4.1. Протоколирование событий».

А для продуктов **Bel VPN Client 4.1** просмотр сообщений, посылаемых на локальный хост, осуществляется с использованием продукта Kiwi Syslog Daemon.

## 20. UPWEB - система учета, анализа и отображения статистических показателей VPN-агентов

### 20.1. Создание пользователя для работы со статистикой

Перед тем, как запустить систему UPWeb, создайте пользователя, который будет иметь право доступа к базе данных для работы со статистикой. В меню **Tools** выберите предложение **Statistic DB editor** (Рисунок 244).

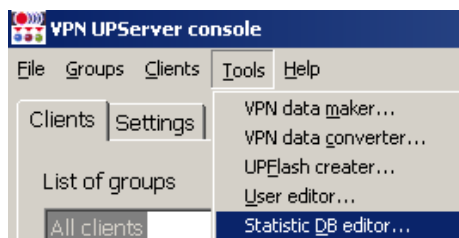


Рисунок 244

В окне **Statistic DB editor** (Рисунок 245) создайте пользователя и назначьте ему пароль, как было описано в разделе «[Редактирование настроек базы данных](#)».

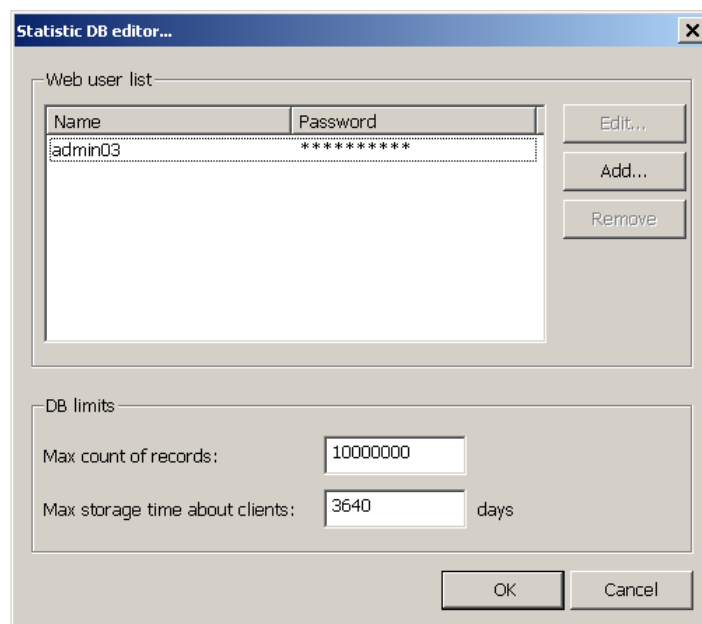


Рисунок 245

### 20.2. Запуск системы UPWeb

На Сервере управления запустите интернет-браузер и в поле для ввода URL укажите <https://127.0.0.1:8443/login.zul> (Рисунок 246).

Введите логин и пароль пользователя для доступа к базе данных статистики, нажмите кнопку **Вход**.

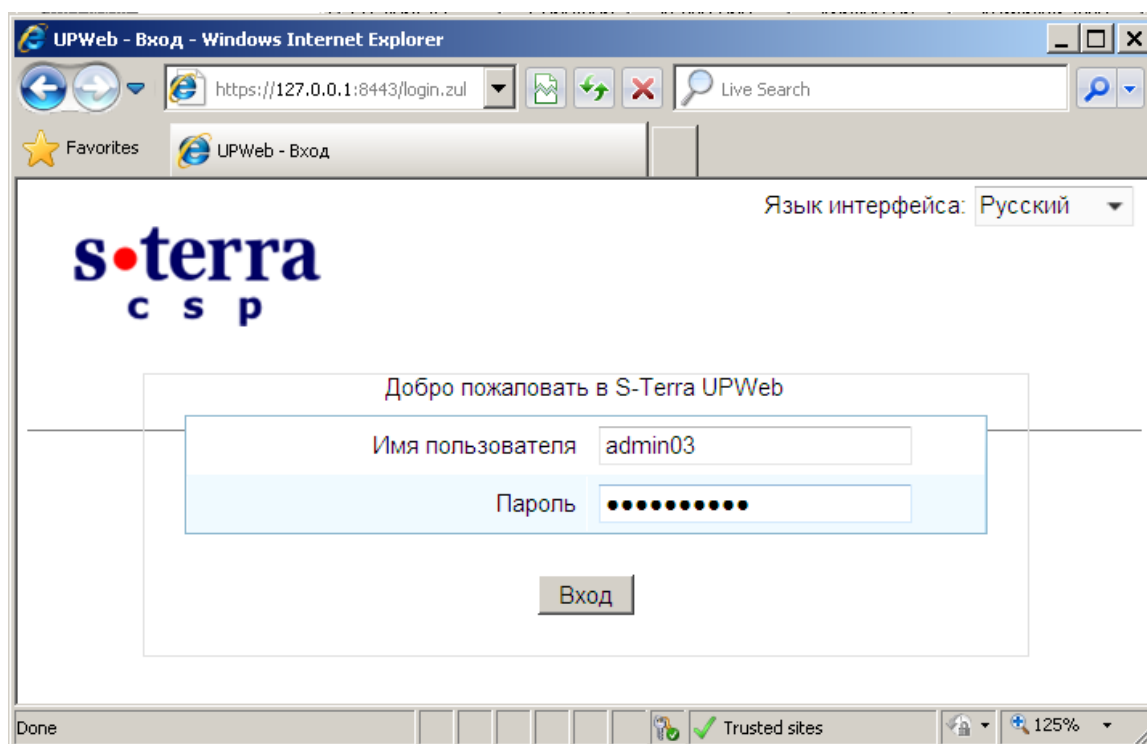


Рисунок 246

Откроется окно с главной вкладкой **Статистика**, в которой отражены все клиенты и значения переменных статистики для них (Рисунок 247).

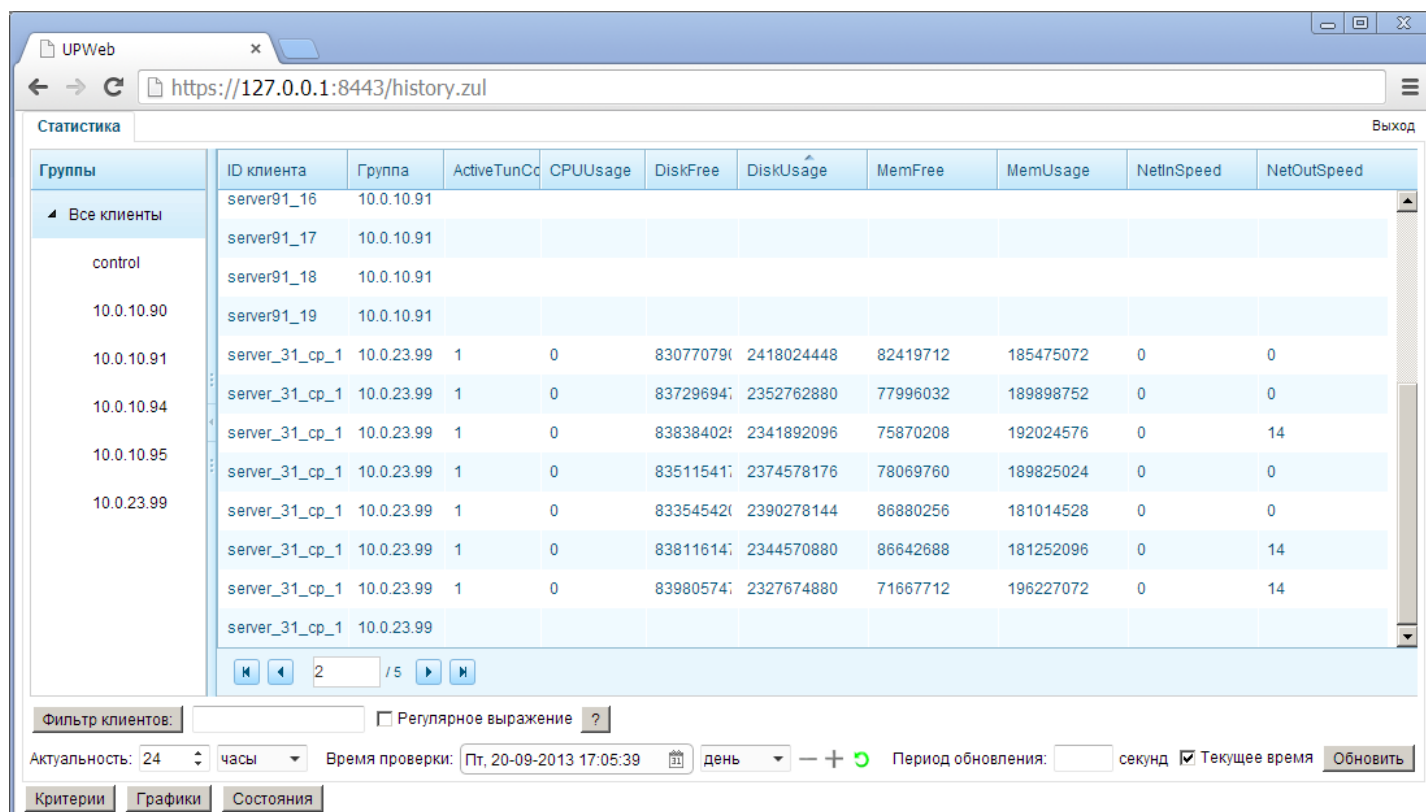


Рисунок 247

## 20.3. Переменные статистики

В настройках Клиента управления в секции [StatVariables](#) включено 4 переменных для сбора статистики на каждом управляемом устройстве: CPUUsage, MemUsage, DiskUsage, NetUsage.

В ответ на запрос CPUUsage будет прислано значение одной переменной:

CPUUsage – средняя занятость процессоров в процентах за время StatCollectPeriod.

В ответ на запрос MemUsage будут присланы значения двух переменных:

MemUsage – количество занятых байт в памяти

MemFree – количество свободных байт в памяти.

В ответ на запрос DiskUsage будут присланы значения двух переменных:

DiskUsage – количество занятых байт на диске

DiskFree – количество свободных байт на диске

В ответ на запрос NetUsage будут присланы значения двух переменных:

NetInSpeed – среднее количество байт в секунду, полученных всеми интерфейсами в период между замерами

NetOutSpeed – среднее количество байт в секунду, отправленных со всех интерфейсов в период между замерами.

Во вкладке **Статистика** переменные статистики имеют значения, равные последним полученным данным от клиентов за заданный диапазон времени - на момент времени, указанный в поле Время проверки, за период времени, указанный в поле Актуальность.

Для задания новой переменной статистики составьте запрос согласно разделу [«Добавление переменной для сбора статистики»](#) в секции StatVariables. Создайте обновление с новыми настройками Клиента управления для управляемых устройств.

Только к вкладке **Статистика** применяется кнопка [Фильтрация по имени](#), флажок Регулярное выражение, поля Актуальность, Время проверки, Период обновления, Текущее время.

Для кнопок [Критерии](#), [Графики](#), [Снимки](#) будут открываться отдельные вкладки, в которых задаются все настройки.

## 20.4. Основные возможности

Основные возможности, которые можно получить, используя главную вкладку **«Статистика»**:

- сортировка клиентов по возрастанию или убыванию значения какого-либо параметра статистики на текущий момент времени
- фильтрация клиентов по имени за заданный интервал времени с получением значений всех переменных статистики (кнопка [Фильтрация клиентов](#))
- фильтрация клиентов по значению переменных за заданный интервал времени для указанных клиентов (кнопка [Критерии](#))
- построение графика изменения значения переменных статистики в заданный интервал времени (кнопка [Графики](#))
- снятие снимка графического интерфейса с изображением всех вкладок в заданный момент времени (кнопка [Снимки](#)).

## 20.5. Фильтрация клиентов по имени и времени

Во вкладке Статистика можно фильтровать клиентов по имени за заданный интервал времени, сортировать по значениям переменных статистики, отслеживать последние значения, собирать статистику за определенный период.

**Задание интервала времени для фильтрации и сортировки**

Поля **Актуальность** и **Время проверки** задают интервал времени.

**Время проверки** – задает окончание интервала времени.

**Актуальность** – задает время актуальности значений переменных в годах, месяцах, днях, часах, минутах, секундах.

Если от значения **Время проверки** вычесть значение **Актуальность** получится начало интервала времени.

**Текущее время** – флажок, если он установлен, то при нажатии кнопки **Обновить** выставляется текущее время в поле **Время проверки**.

Кнопка **Обновить** – повторное обновление последних значений переменных статистики за заданный период времени.

**Период обновления** – интервал времени между автоматическими обновлениями переменных в таблице и дереве групп клиентов:

- если этот интервал не задан или равен нулю, то кнопка **Обновить** один раз обновляет содержимое таблицы. Использование данной кнопки имеет смысл, если значение **Время проверки** находится в будущем;
- если этот интервал не нулевой, то по нажатию кнопки **Обновить** происходит обновление таблицы и одновременный запуск периодического таймера – для симуляции "автоматического" нажатия кнопки **Обновить** через заданный интервал времени – **Период обновления**;
  - ♦ об автоматическом нажатии кнопки Обновить сигнализирует измененный цвет текста "Период обновления" – синий.

### Задание регулярного выражения для имени

Рядом с кнопкой **Фильтрация по имени** - поле для ввода признака фильтрации по имени (шаблон ID клиента):

- если поле пустое – фильтрация клиентов не осуществляется, показывается весь список
- если поле непустое – рассматривается как подстрока в имени клиента для поиска, регистр символов не учитывается;
- если поле непустое и установлен флажок **Регулярное выражение** – строка в поле рассматривается как регулярное выражение, регистр символов не учитывается. В регулярном выражении используются следующие символы для фильтрации клиентов по имени:
  - ♦ символ \* соответствует тому, что любое количество предшествующих символов должны присутствовать в имени, в том числе и нулевое;
  - ♦ символ ? соответствует тому, что один предшествующий символ должен присутствовать в имени, или нулевое количество;
  - ♦ если в начале выражения находится символ ^, то это означает, что имя клиента должно начинаться с символов, следующих за символом ^. Отсутствие символа ^ в начале эквивалентно указанию символа \* в начале выражения;
  - ♦ если в конце выражения указан символ \$, то имя клиента должно заканчиваться символами, предшествующими символу \$. Отсутствие символа \$ в конце эквивалентно указанию символа \* в конце выражения;

Кнопка **?** показывает подсказку для создания регулярного выражения.

### Сценарий 1

Сортировать и отображать клиентов, имеющих наибольшее или наименьшее значение какой-либо переменной статистики на текущий момент времени (Рисунок 248).

- Шаг 1:** В поле **Актуальность** установите период, за который интересующая переменная статистики будет собрана со всех отслеживаемых клиентов;
- установление большого периода актуальности замедляет выбор статистики из базы данных.*
- Шаг 2:** Установите **Время проверки** в будущее время либо флажок **Текущее время**;
- при установленном флажке **Текущее время** нажатие кнопки **Обновить** приводит к выставлению текущего времени в поле **Время проверки**.*

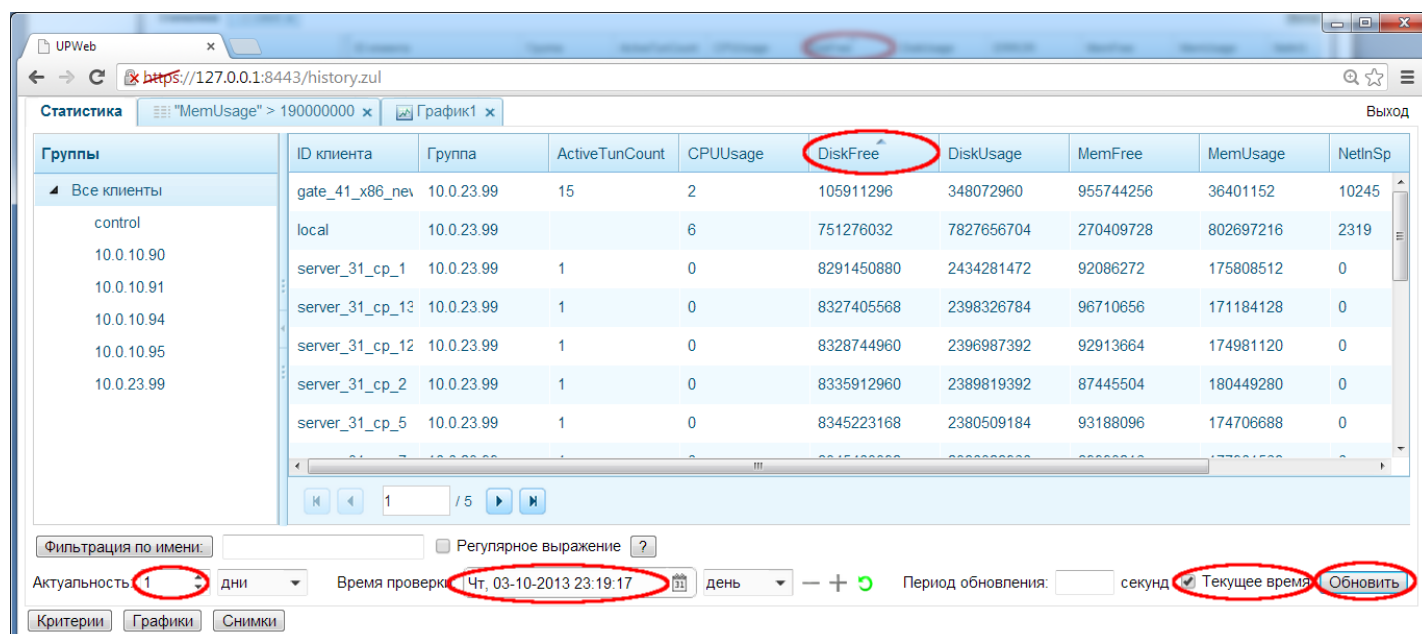


Рисунок 248

**Шаг 3:** Нажмите кнопку **Обновить** – будет выполнен запрос к базе данных и обновлена информация о клиентах и переменных статистики, присылаемых клиентами;

*на момент обновления в базе данных могут быть зарегистрированы новые клиенты или удалены старые, список переменных статистики, присылаемых клиентами, может быть также изменён.*

**Шаг 4:** Нажмите на заголовок столбца интересующей переменной, значения будут отсортированы по возрастанию или убыванию.

**Шаг 5:** Если дальше нажимать кнопку **Обновить** – информация о клиентах и переменных из базы данных будет обновляться, при этом:

*порядок сортировки клиентов будет сохранен;  
если список клиентов большой - размещается на нескольких страницах.*

## Сценарий 2

Отображать последние значения параметров статистики клиентов (Рисунок 249).

**Шаг 1:** В поле **Актуальность** установите период, за который интересующая переменная статистики будет собрана со всех отслеживаемых клиентов.

**Шаг 2:** Установите **Время проверки** в будущее время либо флажок **Текущее время**.

**Шаг 3:** Отсортируйте клиентов по ID клиента, нажав мышкой на надпись "ID клиента".

**Шаг 4:** При необходимости отфильтруйте клиентов по имени, установив **шаблон ID клиента**, и нажмите кнопку **Фильтрация по имени**.

**Шаг 5:** Установите **Период обновления** (автообновления) в значение, отличное от нуля.

**Шаг 6:** Нажмите кнопку **Обновить** – информация о клиентах и переменных из базы данных будет обновляться, при этом:

*текст "Период обновления" будет изменен на синий – значит запущен таймер автообновления;  
порядок сортировки клиентов будет сохранен.*

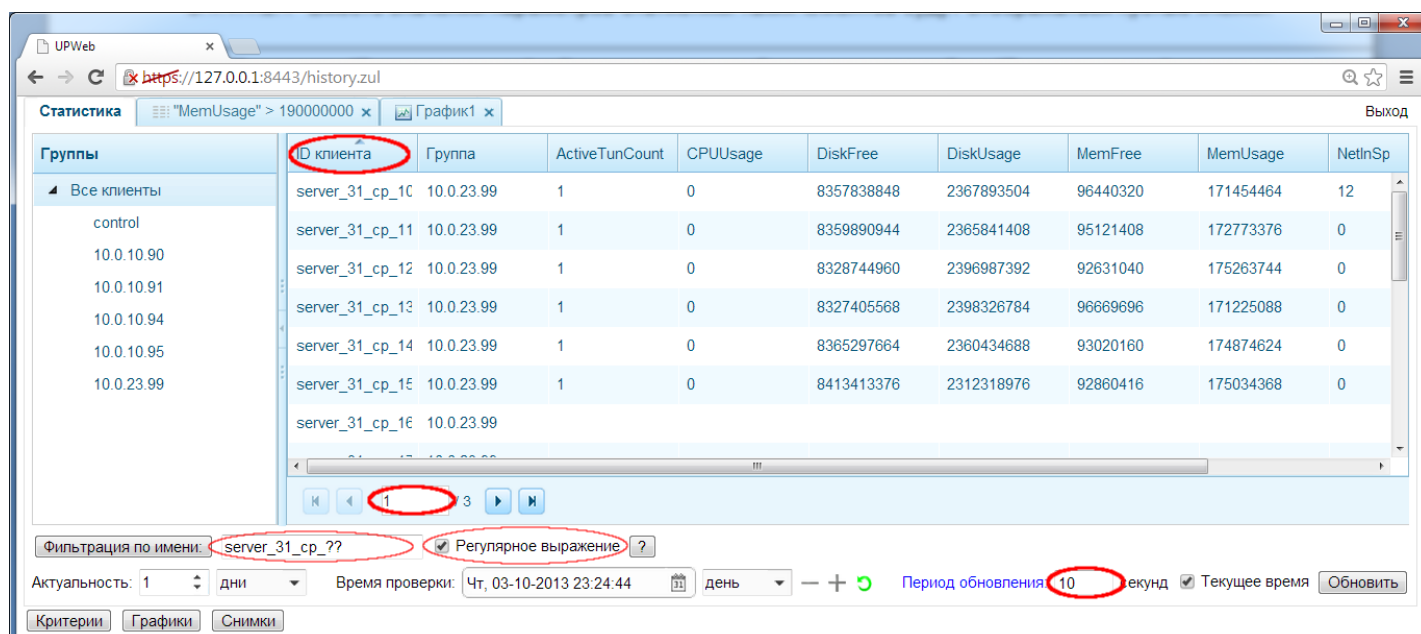


Рисунок 249

### Сценарий 3

Отслеживать активность клиентов по сбору статистики за определенный период времени (Рисунок 250).

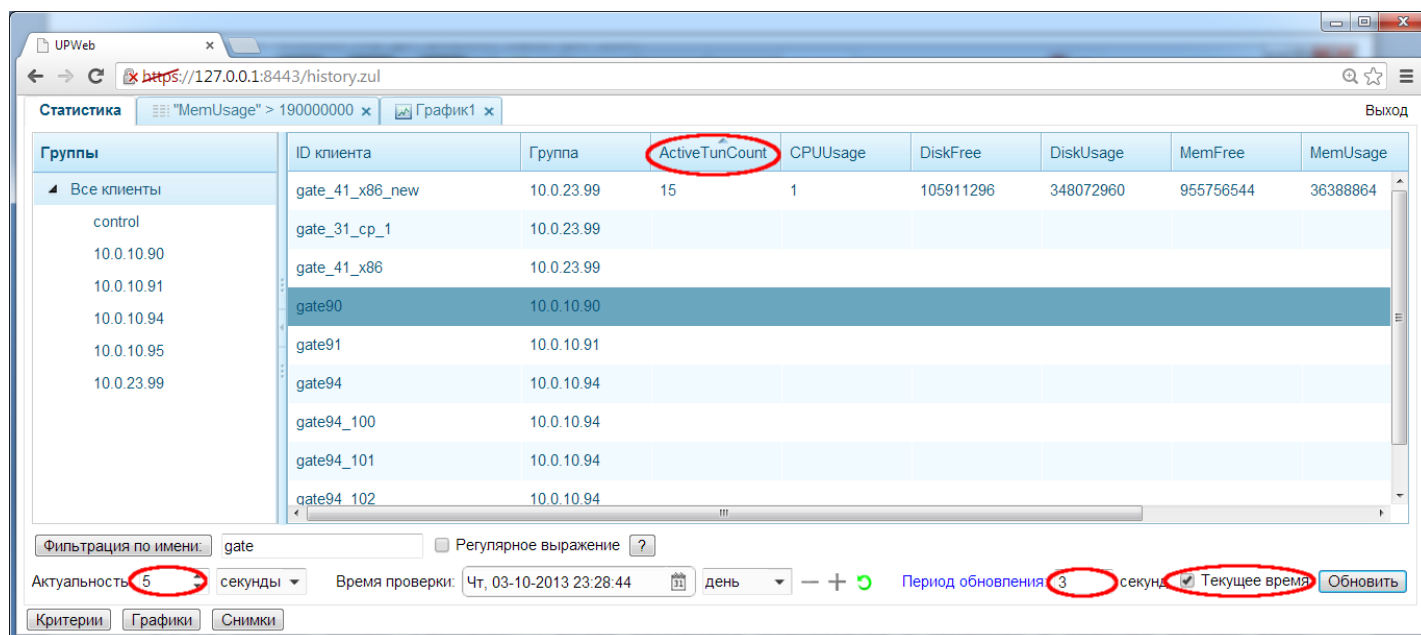


Рисунок 250

- Шаг 1:** В поле **Актуальность** установите период, за который интересующая переменная статистики будет собрана со всех отслеживаемых клиентов.
- Шаг 2:** Установите флажок **Текущее время**.
- Шаг 3:** Нажмите на заголовок столбца интересующей переменной, значения будут отсортированы по возрастанию или убыванию.
- Шаг 4:** Нажмите кнопку **Обновить** – информация будет обновляться, цвет надписи "Период обновления" будет изменен на синий - запущен таймер автообновления. Если какой-либо клиент не присылал статистику за заданный период – ячейка в таблице будет пустая.



**Сценарий 4**

Посмотреть историю значений переменных статистики для клиентов.

- Шаг 1:** В поле **Время проверки** установите значение в прошлое.
- Шаг 2:** Поле **Период обновления** очистите.
- Шаг 3:** Нажмите кнопку **Обновить** – информация о клиентах будет обновлена и остановлен таймер автообновления.
- Шаг 4:** Изменяя значение **Актуальность** и отсортировывая переменные по значению, можно узнать как изменялись переменные статистики в прошлом.

**20.6. Фильтрация по значениям переменных статистики (критерии)****Сценарий 5**

Показать всех клиентов с используемой памятью свыше 110 000 000 байт в течение определенного времени.

- Шаг 1:** Нажмите кнопку **Критерии**, а затем **Добавить**, откроется окно для создания нового критерия (Рисунок 251).

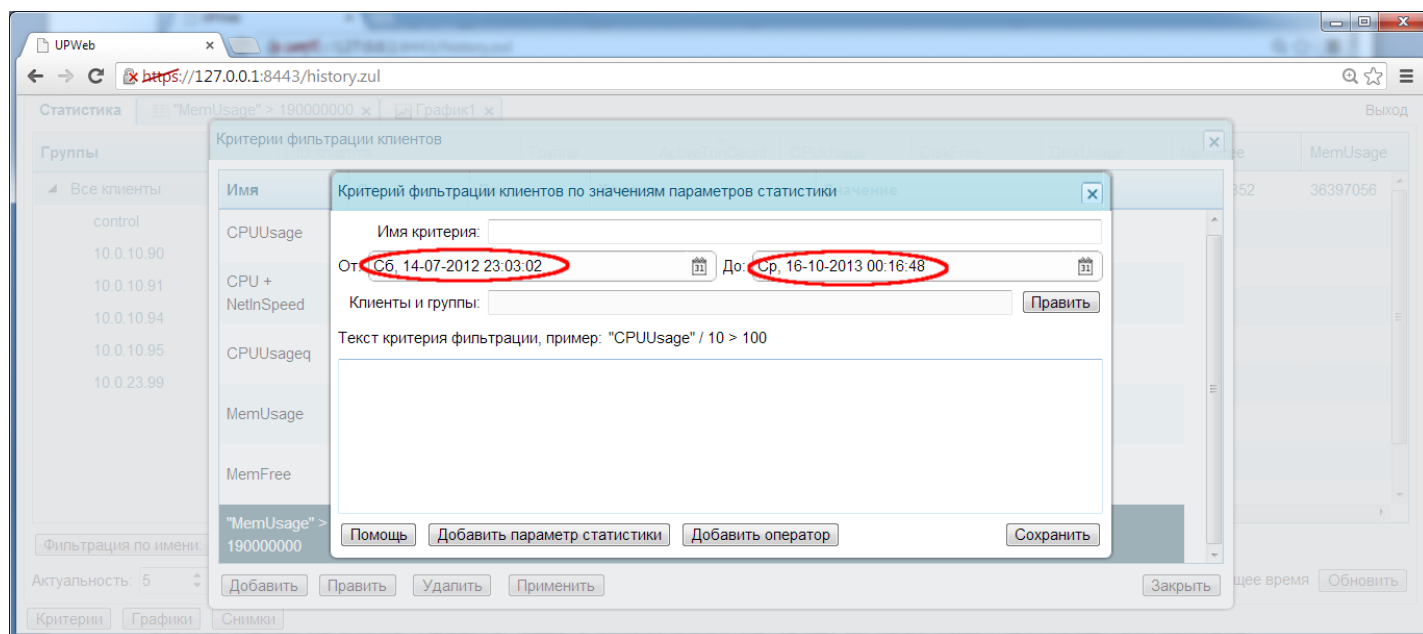




Рисунок 251

- Шаг 2:** Задайте интересующий интервал времени в полях **От** и **До**:  
*задавайте интервал небольшим для уменьшения времени поиска клиентов.*
- Шаг 3:** Нажмите кнопку **Править** для задания списка клиентов, среди которых будет производиться выборка.
- Шаг 4:** В окне **Выберите клиента или группу** в левой части перечислены все доступные клиенты, в правой – выбранные клиенты (Рисунок 252). Используя голубые горизонтальные стрелки, сделайте выбор клиентов для применения критерия.

Для поиска клиентов в левой части можно использовать поле **Клиенты**, введя в него часть имени клиента, или применить **Регулярное выражение** также как и при фильтрации по имени. Если ни одного клиента не найдено – текст в поле **Клиенты** становится красным. В противном случае – найденный клиент будет выделен. Нажатие на кнопку  вызывает процедуру поиска следующего выделенного клиента, нажатие на кнопку  – предыдущего. При достижении конца списка, поиск продолжается с начала.

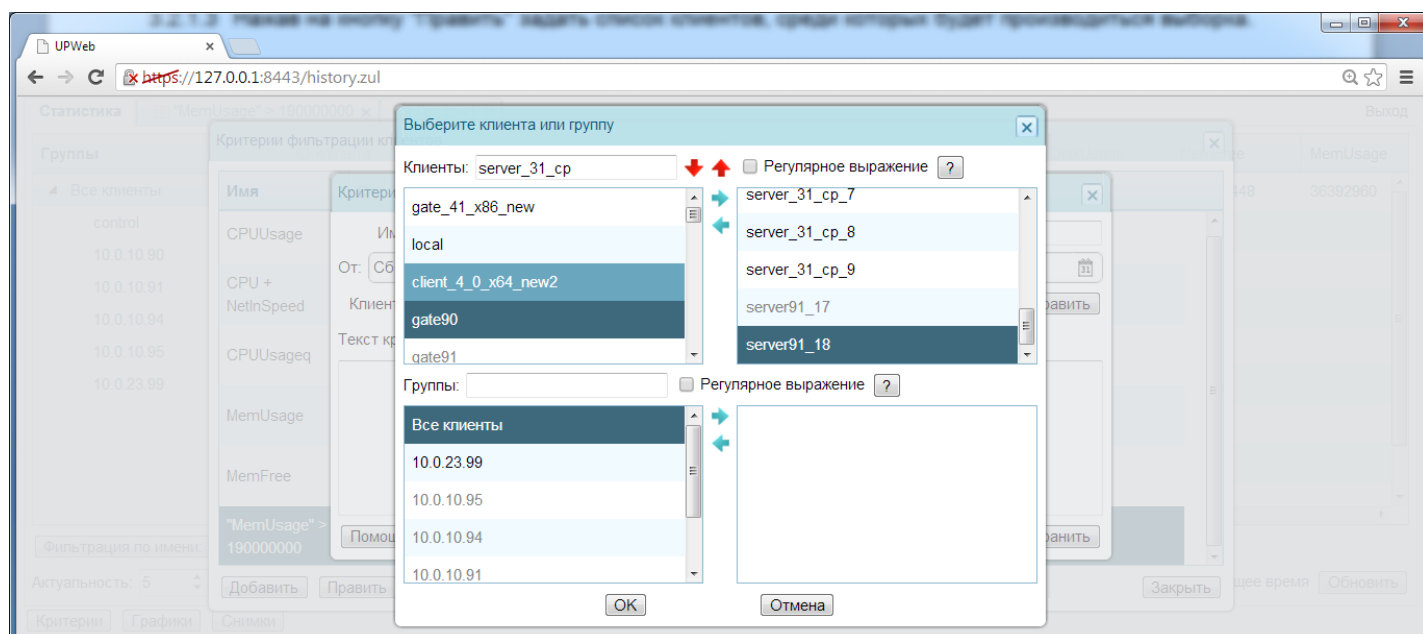


Рисунок 252

**Шаг 5:** Нажмите кнопку **Добавить параметр статистики**, выберите переменную статистики MemUsage (Рисунок 253).

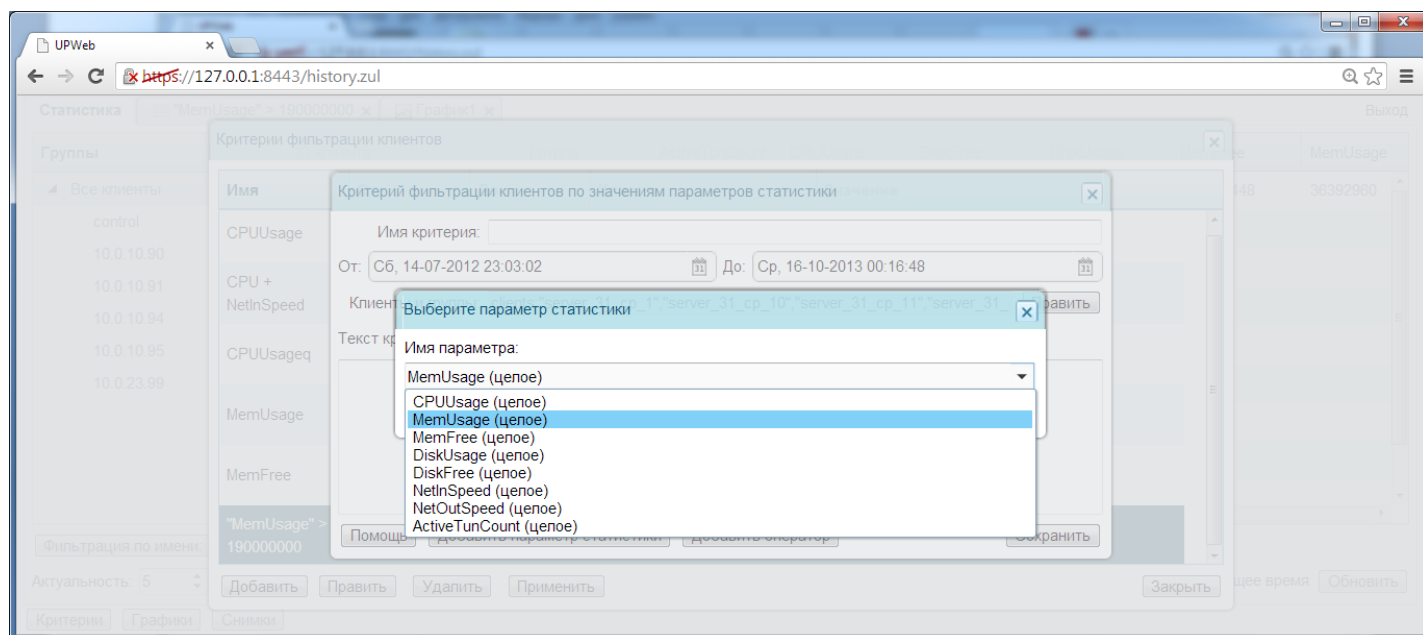


Рисунок 253

**Шаг 6:** Завершите текст критерия, добавив к переменной MemUsage ее значение ">110000000", нажмите кнопку **Сохранить** (Рисунок 254).

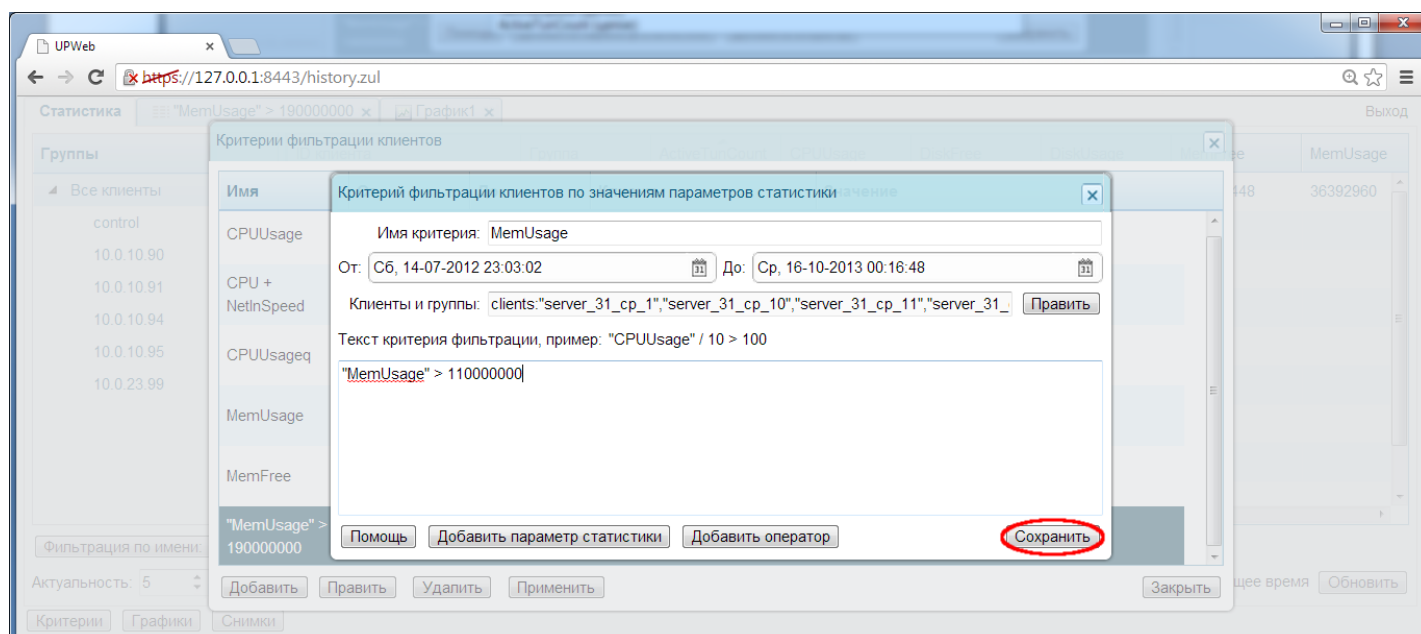


Рисунок 254

**Шаг 7:** В окне **Критерии фильтрации клиентов** выберите созданный критерий и нажмите кнопку **Применить**.

**Шаг 8:** Результатом применения критерия будет таблица клиентов, удовлетворяющих критерию - потребление памяти должно превышать 110000000 единиц в какой-либо момент времени заданного интервала (Рисунок 255).

*Замечание: некоторые значения MemUsage, отображаемые в этой таблице могут быть меньше 110000000, так как в таблице отображены значения клиентов на момент проверки, которые могут быть меньше максимальных значений на заданном интервале.*

ID клиента	Группа	ActiveTunCount	CPUUsage	DiskFree	DiskUsage	MemFree	MemUsage	NetInSpeed	NetOutSpeed
server_31_cp_13	10.0.23.99	1	0	8327335936	2398396416	96681984	171212800	0	0
server_31_cp_10	10.0.23.99	1	4	8357740544	2367991808	96108544	171786240	839	812
server_31_cp_3	10.0.23.99	1	0	8400039936	2325692416	95244288	172650496	0	0
server_31_cp_11	10.0.23.99	1	0	8359788544	2365943808	95133696	172761088	0	14
server_31_cp_6	10.0.23.99	1	0	8345337856	2380394496	95035392	172859392	0	0
server_31_cp_9	10.0.23.99	1	0	8355975168	2369757184	94441472	173453312	12	8
server_31_cp_5	10.0.23.99	1	0	8345120768	2380611584	93200384	174694400	12	8
server_31_cp_14	10.0.23.99	1	0	8365199360	2360532992	92483584	175411200	0	0
server_31_cp_15	10.0.23.99	1	0	8413327360	2312404992	92319744	175575040	0	0

Рисунок 255

## 20.7. Построение графиков

Можно построить графики зависимостей значений переменных статистики от времени.

### Сценарий 6

Построить графики зависимостей значений параметров "CPUUsage" и "NetInSpeed" от времени для клиентов "server\_31\_cp\_11" и "server\_31\_cp\_12" за заданный интервал и определить даты, когда выполняется условие "CPUUsage" > 10 с одновременным значением "NetInSpeed" > 120.

**Шаг 1:** Нажмите кнопку **Графики**, откроется окно **Параметры графика** (Рисунок 256).

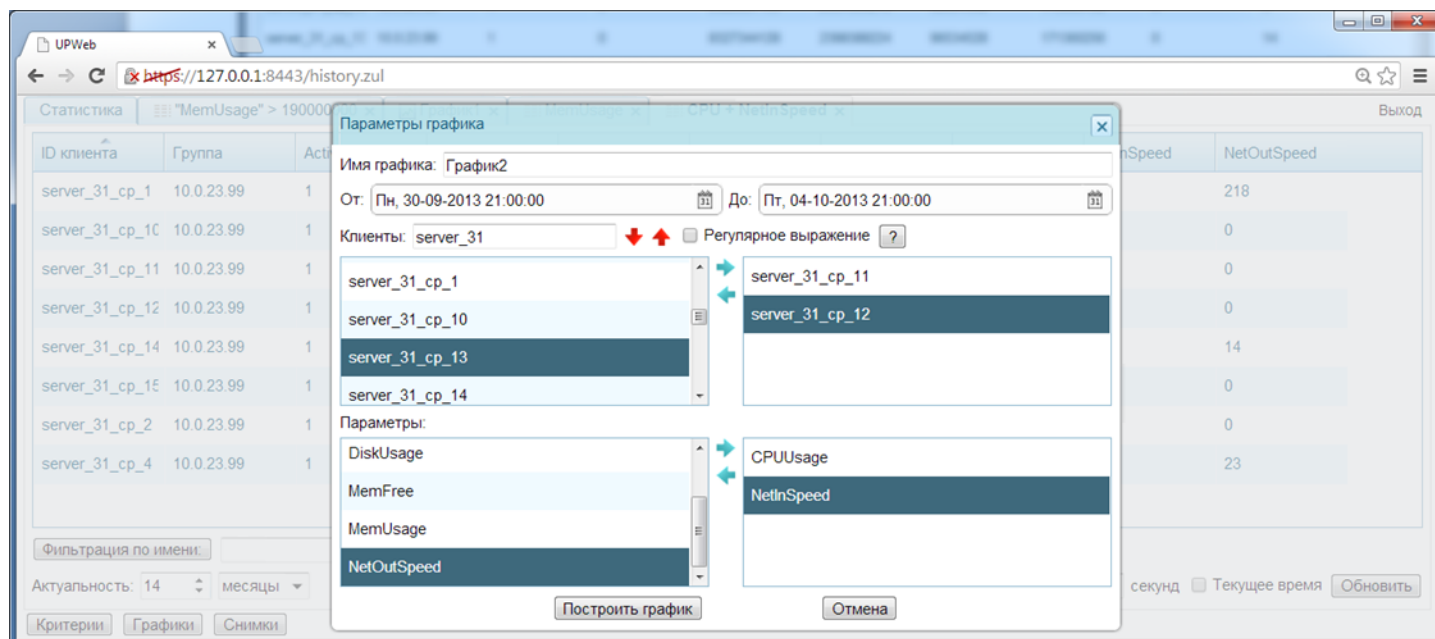


Рисунок 256

**Шаг 2:** Задайте список клиентов: "server\_31\_cp\_11" и "server\_31\_cp\_12".

**Шаг 3:** Задайте список параметров "CPUUsage" и "NetInSpeed".

**Шаг 4:** Задайте интервал времени **От** и **До**.

**Шаг 5:** Нажмите кнопку **Построить график**.

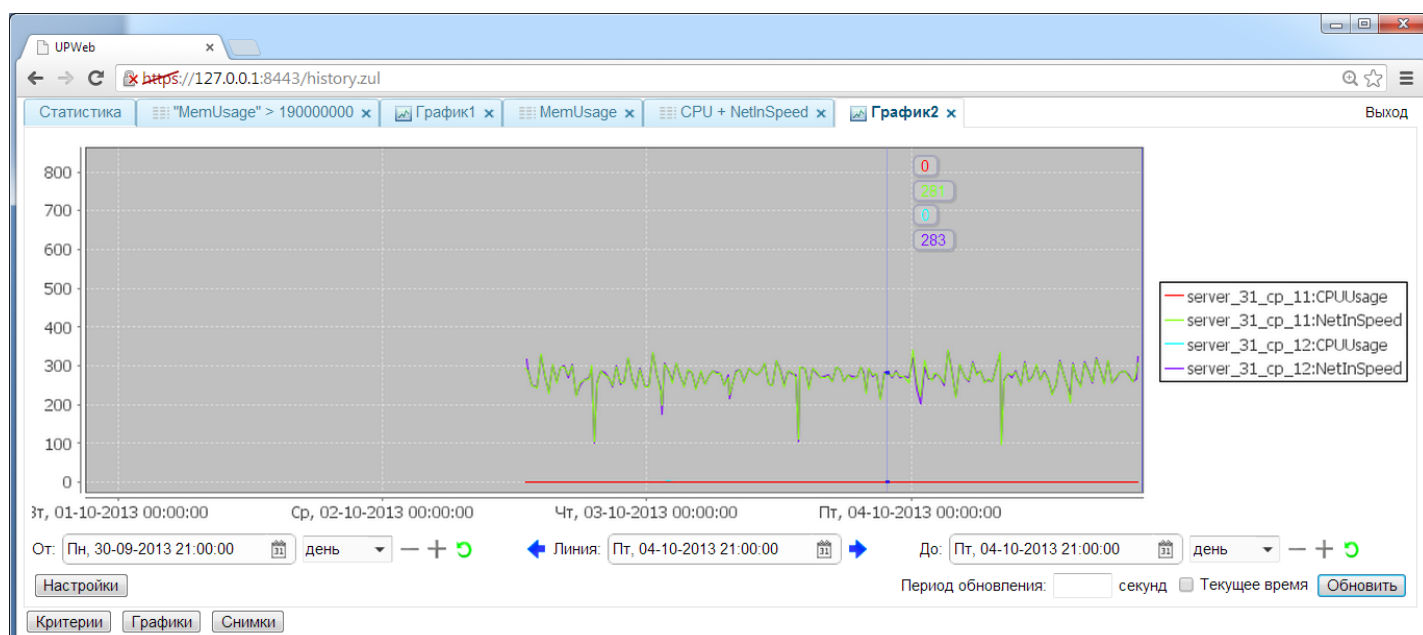


Рисунок 257

*Замечание. Значения переменных на графиках усреднены по времени - заданный временной интервал разбит на некоторое количество под-интервалов, на каждом из которых вычислено среднее значение каждой переменной.*

**Шаг 6:** Нажмите кнопку **Настройки**, откроется окно **Настройки графиков**.

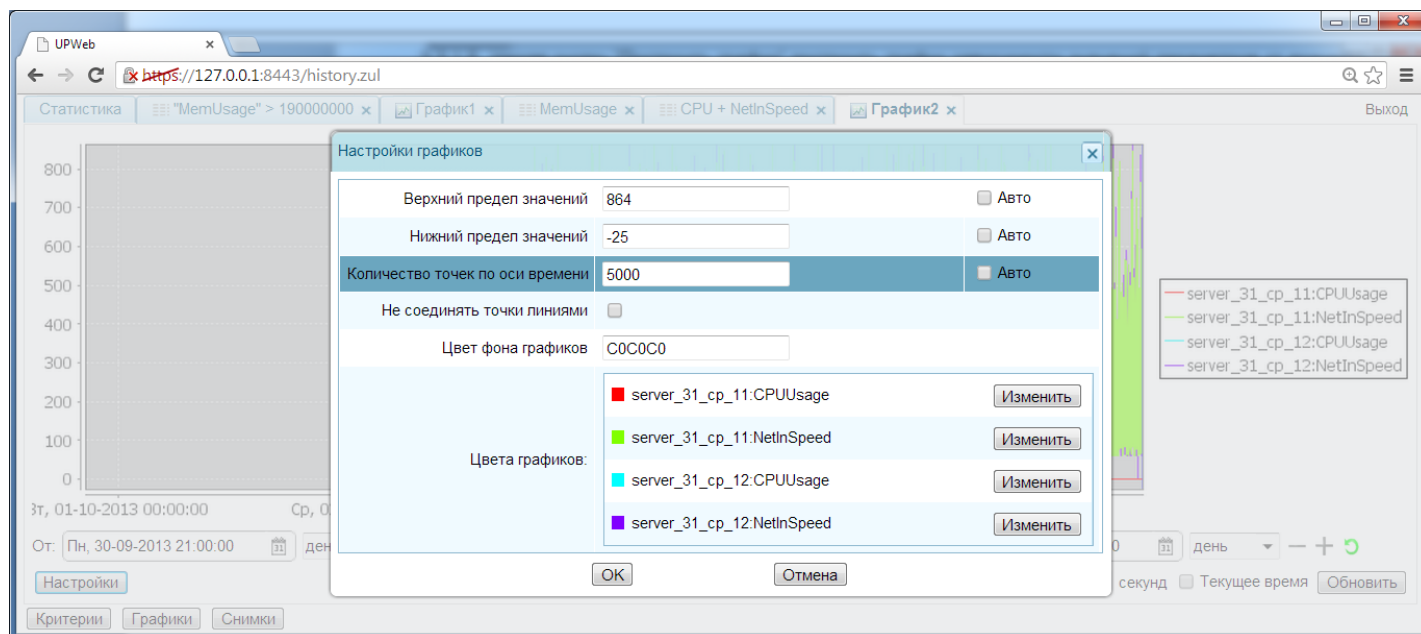


Рисунок 258

**Шаг 7:** Количество подинтервалов - точек по оси времени - автоматически определяется в зависимости от разрешения картинки графиков. Если вручную задать это количество, например, 5000, отключив при этом автоматическое масштабирование по оси значений переменных, то получим следующие графики (Рисунок 259).

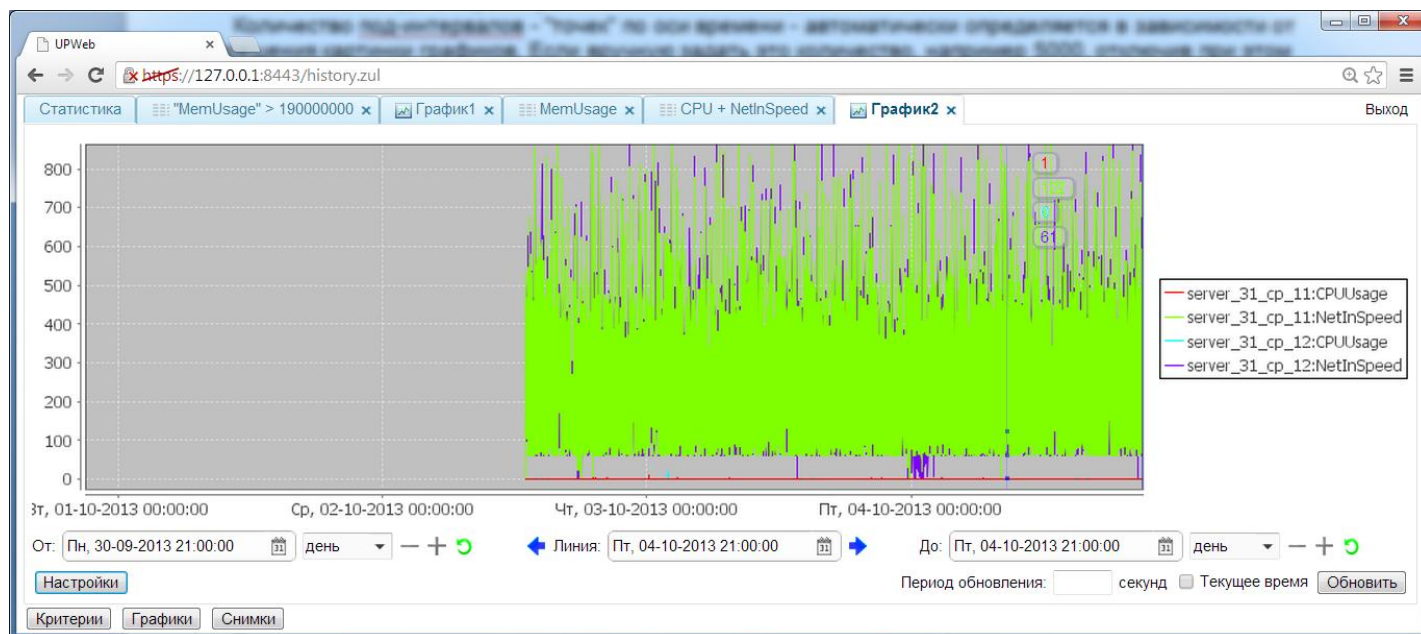


Рисунок 259

На графиках видно, что большую часть времени среднее значение переменной "NetInSpeed" превышает 120 единиц для обоих клиентов "server\_31\_cp\_11" и "server\_31\_cp\_12".

Однако, из совмещенных графиков не видно, в какие моменты времени значение переменной "CPUUsage" превышает 10 единиц. Построим отдельный график для значений "CPUUsage".

**Шаг 8:** Нажмите кнопку **Графики**, откроется окно настройки нового графика, удалите "NetInSpeed" из списка выбранных переменных клиентов (Рисунок 260).

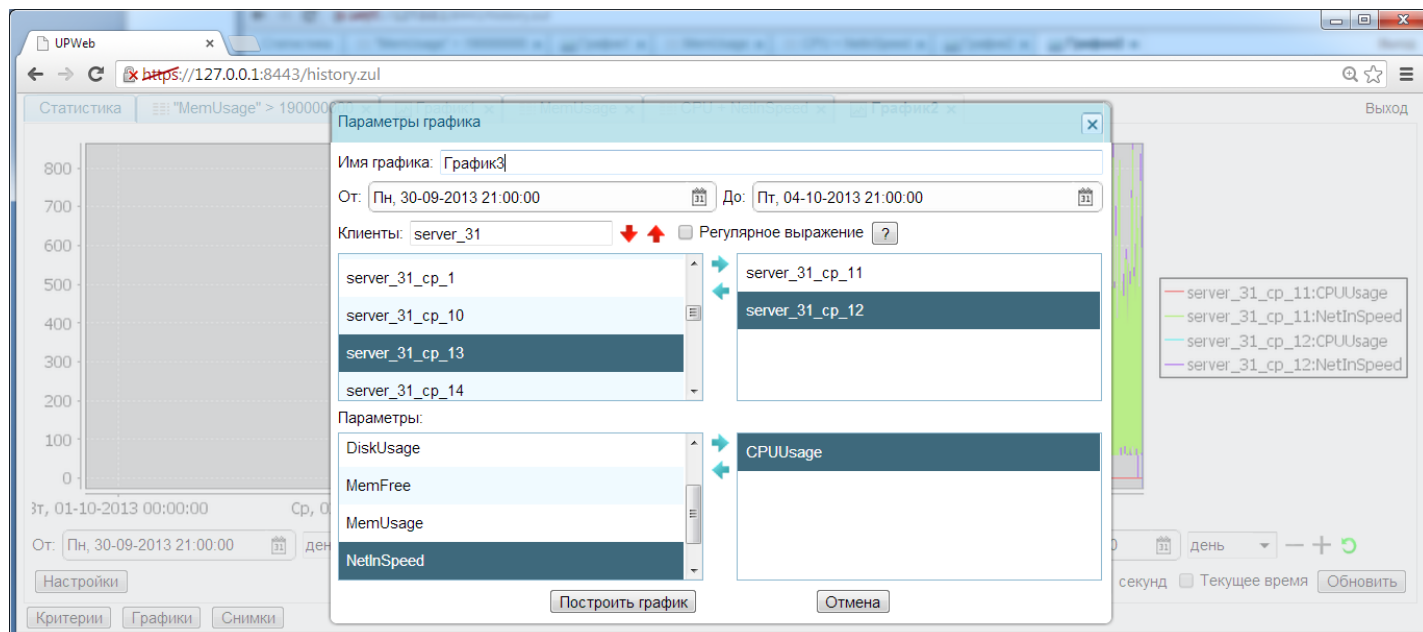


Рисунок 260

**Шаг 9:** Нажмите кнопку **Построить график**, получился новый график зависимости "CPUUsage" от времени (Рисунок 261).

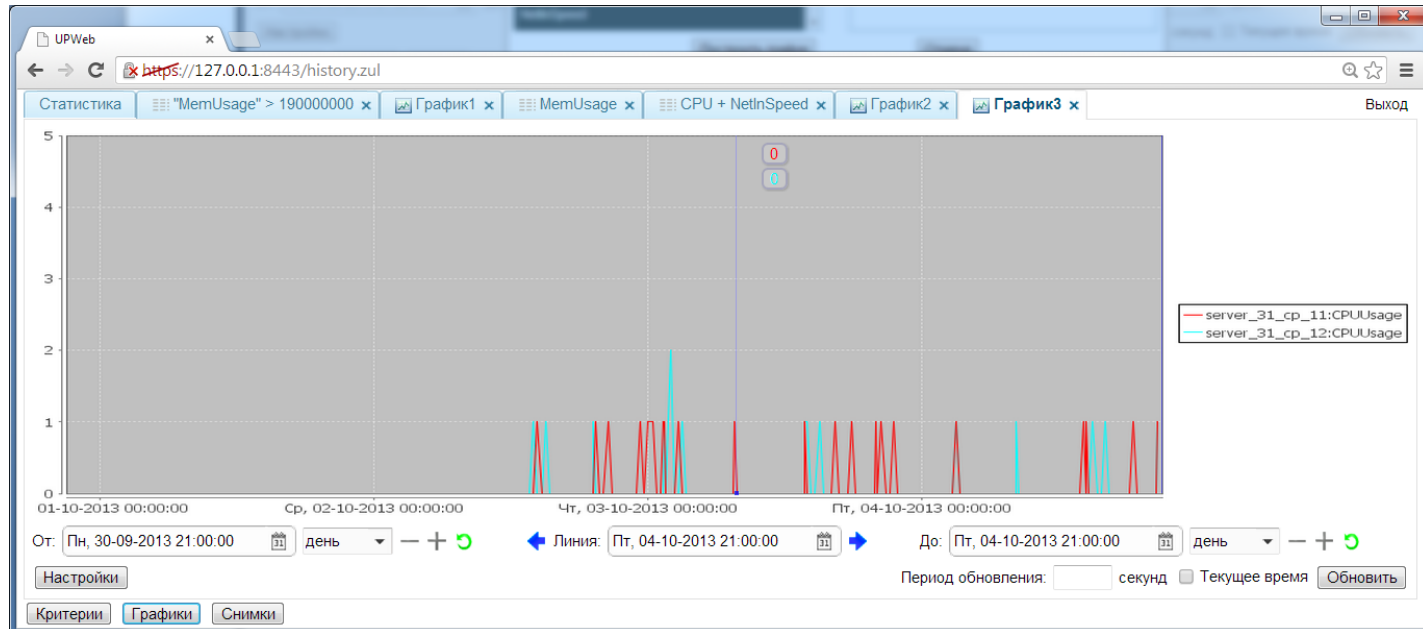


Рисунок 261

**Шаг 10:** Усредненные значения "CPUUsage" не позволяют определить время, когда значение "CPUUsage" превышает 10 единиц, поэтому нажмите кнопку **Настройки**, в открывшемся окне **Настройки графиков** увеличьте количество точек по оси времени до 7000, и получите измененный график (Рисунок 262).



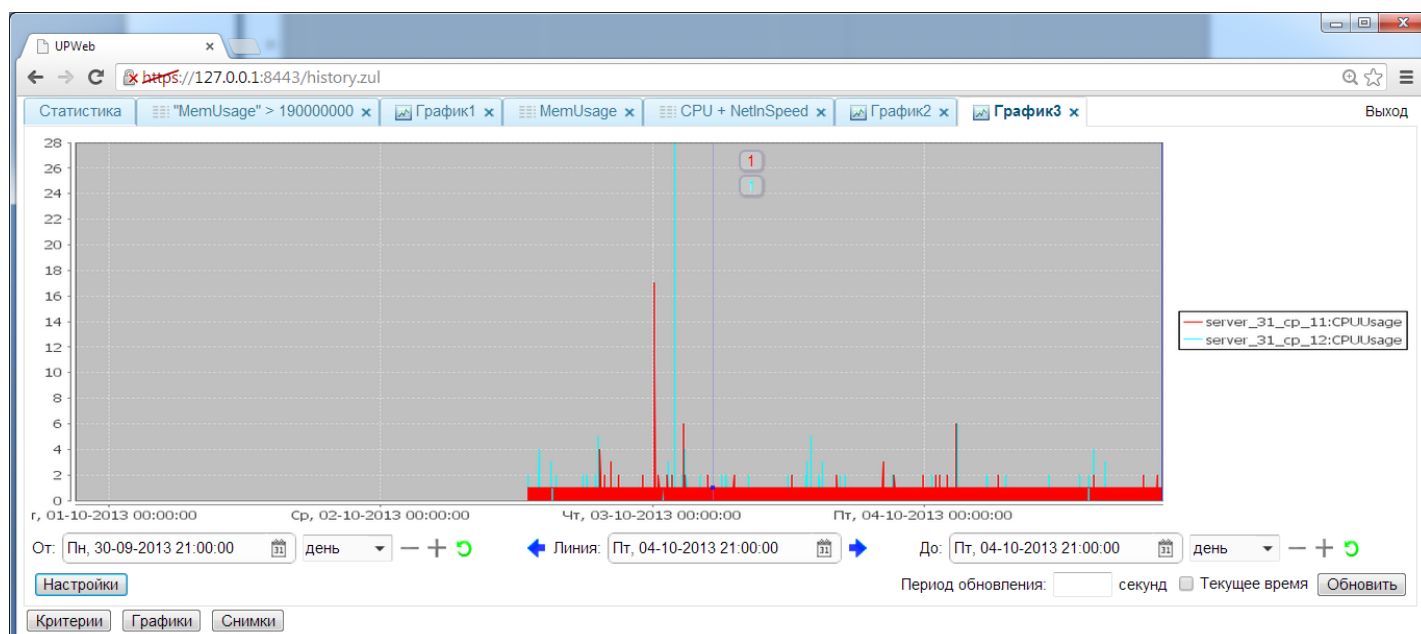


Рисунок 262

**Шаг 11:** Изменяя значения **От** и **До** на графике, отключив "соединение точек линиями" в настройках графиков, можно получить следующую картину, из которой видны значения времени, когда выполняется условие "CPUUsage" > 10 (Рисунок 263).

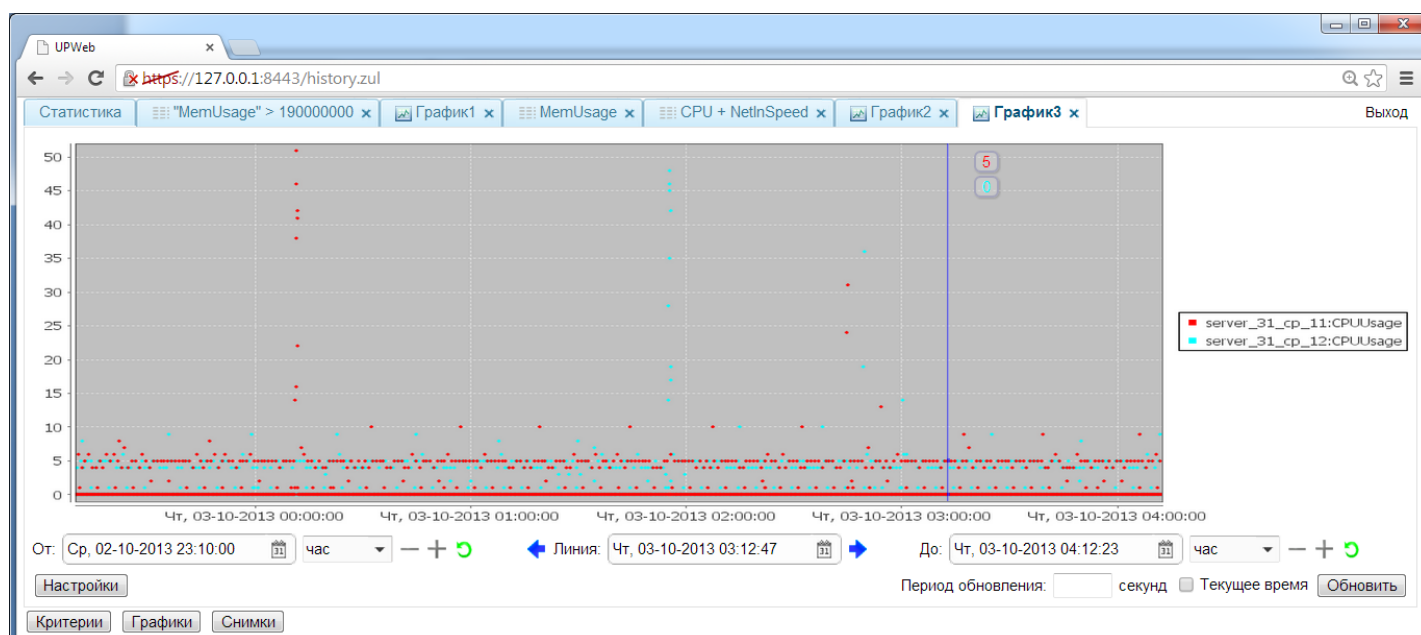


Рисунок 263

## 20.8. Снимки

Снимок пользовательского интерфейса – это значение всех настроек и открытых закладок на какой-либо момент времени. Это состояние сохраняется в базе данных и может быть восстановлено в любой момент времени (Рисунок 264). При загрузке снимка текущие открытые закладки будут закрыты.

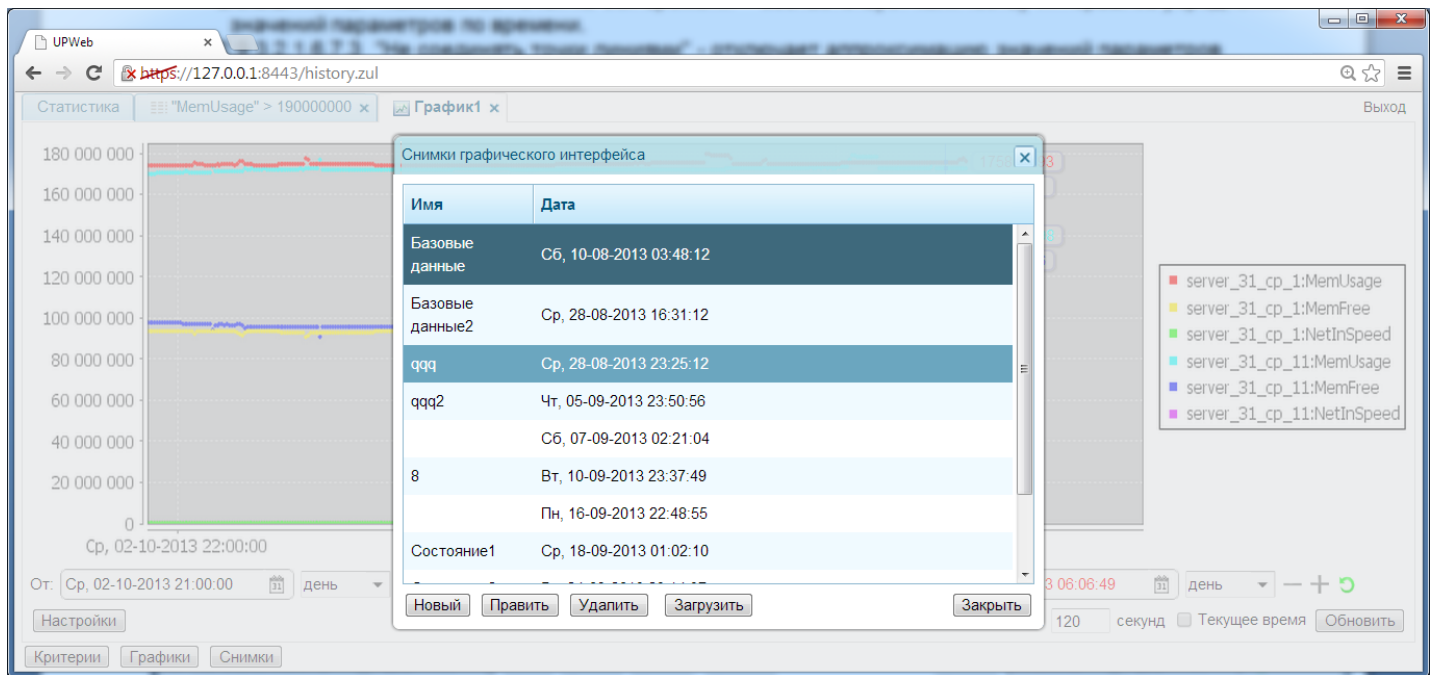


Рисунок 264