ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон: +7 (499) 940-9001
Факс: +7 (499) 940-9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный продукт
С-Терра КП
Версия 3.11

Руководство администратора

РЛКЕ.00006-02 90 03

22.01.2016

Содержание

1. Продукт С-Терра КП 3.11

1.1. Назначение продукта

Продукт С-Терра КП версии 3.11 предназначен для централизованного удаленного управления всей линии продуктов, производимых компанией «С-Терра СиЭсПи», а именно:

«Программного комплекса CSP VPN Server. Версия 3.1/3.11/4.0»

«Программного комплекса CSP VPN Client. Версия 3.1/3.11/4.0»

«Программного комплекса CSP VPN Gate. Версия 3.1/3.11/4.0»,

установленных на конечных устройствах, банкоматах, платежных терминалах, СЗН (специальном загрузочном носителе) «СПДС-USB-01» и др.

Далее продукты CSP VPN Server/CSP VPN Client/CSP VPN Gate будем именовать CSP VPN Agent.

Продукт С-Терра КП 3.11 состоит из двух частей:

- ***Сервер управления*** – серверная часть продукта, устанавливается на выделенный компьютер и предназначена для управления процессом обновления продуктов CSP VPN Agent и их настроек, инсталлированных на управляемых устройствах;
- ***Клиент управления*** – клиентская часть продукта, устанавливается на управляемое устройство с инсталлированным продуктом CSP VPN Agent и предназначена для его управления.

Общая схема использования продукта С-Терра КП 3.11

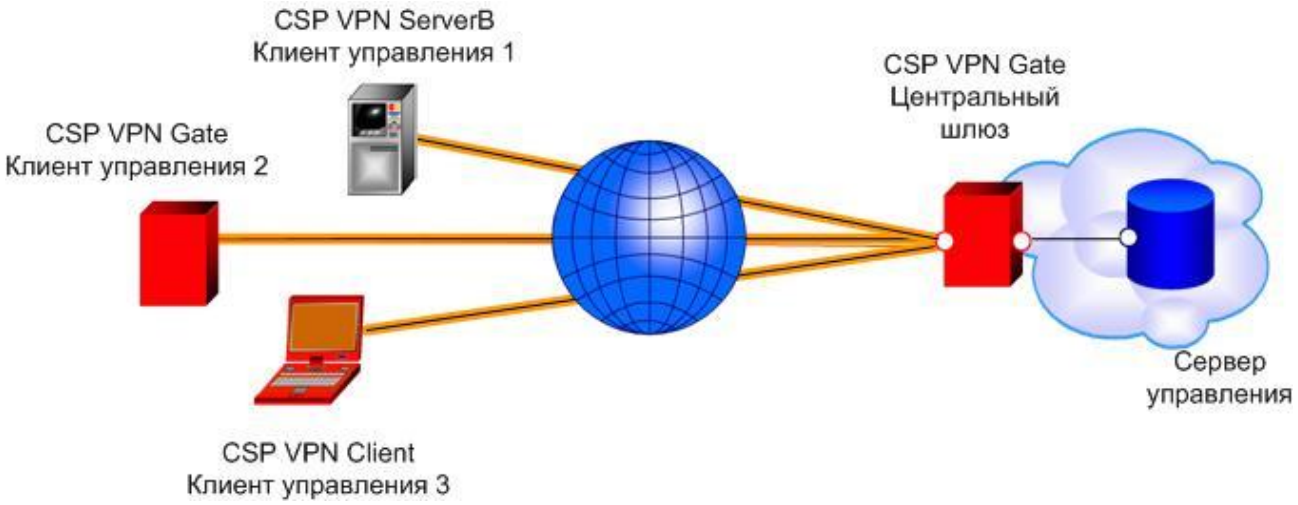

Рисунок 1

Сервер управления устанавливается на выделенный компьютер с ОС Windows Server 2003/2008, размещенный в защищенной локальной подсети. На Сервере управления создается Клиент управления для каждого управляемого устройства и сами обновления.

Созданный Клиент управления устанавливается на управляемое устройство, для которого он и был создан.

Все обмены между Сервером управления и Клиентом управления осуществляются по протоколу FTP и UDP (передаются нотификации). Этот трафик должен передаваться по защищенному IPsec-соединению.

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 CSP VPN Agent и ***Клиентом управления*** могут быть обновлены следующие данные:

- локальная политика безопасности, предписанная данному устройству (в текстовом виде или в виде cisco-like конфигурации)
- политика драйвера по умолчанию продукта CSP VPN Agent
- настройки драйвера продукта CSP VPN Agent
- предопределенные ключи продукта CSP VPN Agent
- локальные сертификаты продукта CSP VPN Agent, CA-сертификат, сертификаты партнеров, список отозванных сертификатов
- контейнеры с ключами сертификатов
- метод аутентификации партнеров
- настройки протоколирования событий продукта CSP VPN Agent
- лицензия на продукт CSP VPN Agent и КриптоПро CSP, в случае его использования
- Клиент управления
- 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 CSP VPN Agent
- локальная политика безопасности продукта CSP VPN Agent (в текстовом виде или в виде cisco-like конфигурации)
- настройки драйвера продукта CSP VPN Agent
- локальные сертификаты продукта CSP VPN Agent, списки отозванных сертификатов, CA 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 CSP VPN Agent на каждом устройстве
- запросы на локальные сертификаты
- имена предопределенных ключей продукта CSP VPN Agent
- настройки протоколирования событий продукта CSP VPN Agent
- журнал регистрации событий продукта CSP VPN Agent и Клиента управления
- информация о лицензиях продуктов CSP VPN Agent и КриптоПро CSP, в случае его использования.

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

- использование окон мастера для создания несложной политики безопасности продукта CSP VPN Agent управляемого устройства
- включение в систему управления уже работающего устройства с CSP VPN Agent
- управление устройством СПДС «ПОСТ» (продукт CSP VPN Gate, установленный на СЗН «СПДС-USB-01»)
- создание клонов клиента для устройства с CSP VPN Gate, отличающихся локальными сертификатами, лицензиями и т. д.
- изменение настроек готового проекта для CSP VPN Agent – утилита vpnmaker
- использование ГОСТ-сертификатов для подписывания обновлений.

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 С-Терра КП входят каталоги и файлы:

```
setup.exe
setup.ini
updater_server.cab
updater_server.msi
version.txt
FileZilla_Server-0_9_34.exe
vcredist_x86.exe
WINDOWS
LINUXRHEL5
SOLARIS
Additional
```


Note

Если на управляемом устройстве уже инсталлирован продукт CSP VPN Server/CSP VPN Client версии 3.1,3.11 то рекомендуется его деинсталлировать, а затем создать заново дистрибутив вместе с Клиентом 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.com.

Если на управляемом устройстве инсталлирован продукт CSP VPN Server/CSP VPN Client версии 3.0, то необходимо перейти на версию 3.1, 3.11 для сохранения полной функциональности продукта после выполнения обновления.

Note

Для управления шлюзом безопасности CSP VPN Gate на устройстве уже должен быть инсталлирован продукт CSP VPN Gate версии не ниже 3.1.

Note

Шлюз безопасности CSP VPN Gate версии 3.11 поставляется с инсталлированным Клиентом управления, который нужно инициализировать.

Note

Сервер управления помимо графического интерфейса имеет интерфейс управления на основе командной строки.

Note

Перед использованием продуктов компании «С-Терра СиЭсПи» и СКЗИ «КриптоПро CSP 3.6(R2)» в режиме КС1/КС2/КС3, изучите документ **«Правила пользования»**, входящий в комплект поставки.

Схема стенда

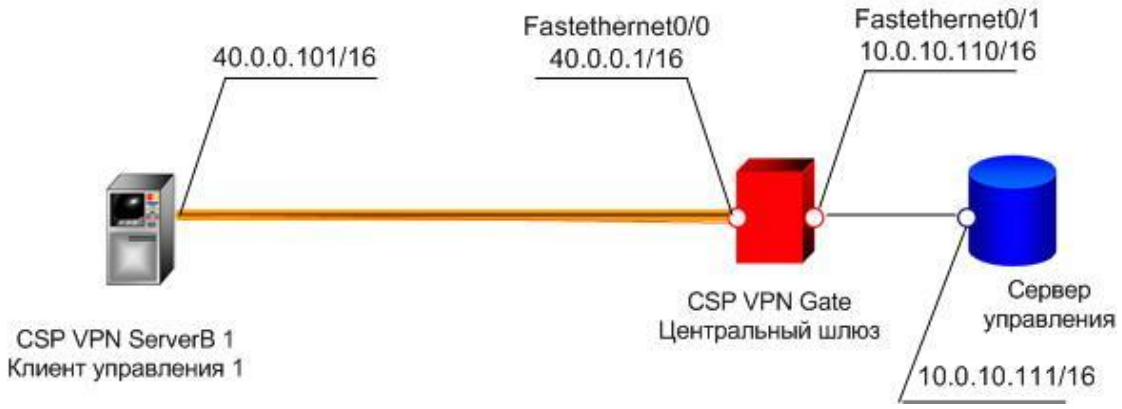

Рисунок 2

В дальнейшем описании документа приведены примеры для стенда (Рисунок 2), в который включен шлюз безопасности с установленным продуктом CSP VPN Gate, 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, построенному до шлюза безопасности.

2. Сценарии управления

Можно выделить два последовательных сценария обновления продукта CSP VPN Agent на управляемом устройстве.

Первый сценарий (при первом обращении к управляемому устройству):

для CSP VPN Gate - подготовка скриптов для инсталляции (инициализации) Клиента управления и настройки установленного продукта CSP VPN Gate, доставка и локальный запуск на управляемом устройстве

для CSP VPN Client/CSP VPN Server – подготовка дистрибутивов Клиента управления и CSP VPN Client/CSP VPN Server, доставка и локальная установка на управляемом устройстве.

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

Далее по тексту управляемые устройства будем называть клиентами, на которые устанавливается (установлен) продукт CSP VPN Agent и Клиент управления.

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

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: Для управляемых устройств, на которые планируется установить продукт CSP VPN Client/CSP VPN Server, на Сервере управления подготовьте дистрибутивы CSP VPN Client/CSP VPN Server и Клиента управления, доставьте и установите локально (см.раздел «Настройка и управление устройством с CSP VPN Server/CSP VPN Client») (а для CSP VPN Gate – подготовьте скрипты).

Шаг 4: Установленный Клиент управления автоматически выполнит проверку возможности устанавливать 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 будут созданы.

3. Установка Сервера управления

3.1. Инсталляция Сервера управления

Инсталляция Сервера управления осуществляется на выделенном компьютере с установленной ОС Windows Server 2003/2008.

1. Установите сначала СКЗИ «КриптоПро CSP 3.6(R2)», если планируется управлять устройствами с установленным продуктом CSP VPN Agent (cp) 3.1/3.11, использующим СКЗИ «КриптоПро CSP 3.6(R2)», или с установленным продуктом С-Терра Agent (cp,st) 4.0, или если для проверки обновлений планируется использовать ГОСТ-сертификаты. СКЗИ потребуется для генерации случайных чисел, используемых при создании ключевых пар на управляемых устройствах.
2. Для инсталляции Сервера управления запустите файл `setup.exe` из состава дистрибутива. Появится окно с запросом на установку необходимых компонент, нажмите кнопку Установить (Рисунок 3).

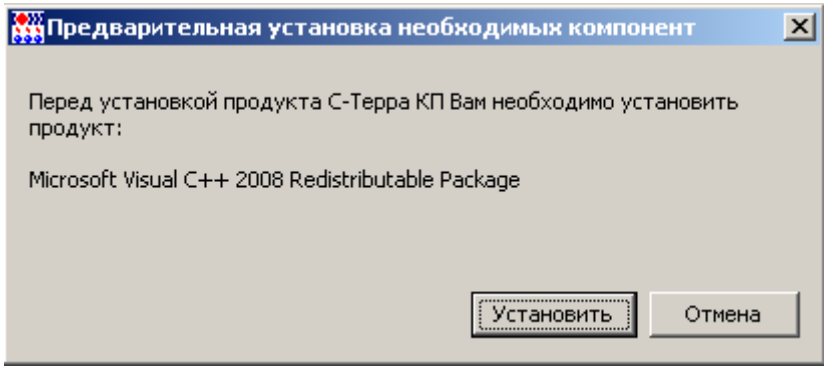

Рисунок 3

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

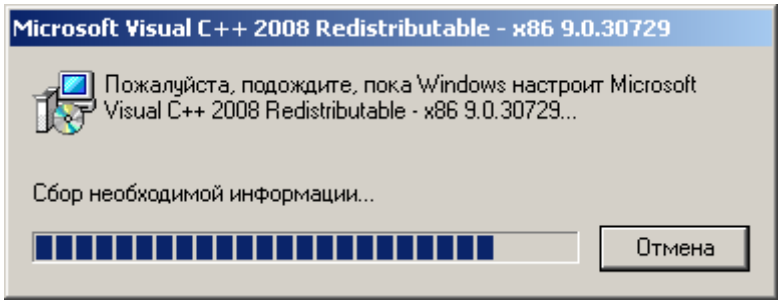

Рисунок 4

Далее появляется приглашение к инсталляции продукта С-Терра КП (Рисунок 5), нажмите кнопку Next.

Рисунок 5

Папку, в которую будет установлен Сервер управления, оставьте без изменений (Рисунок 6).

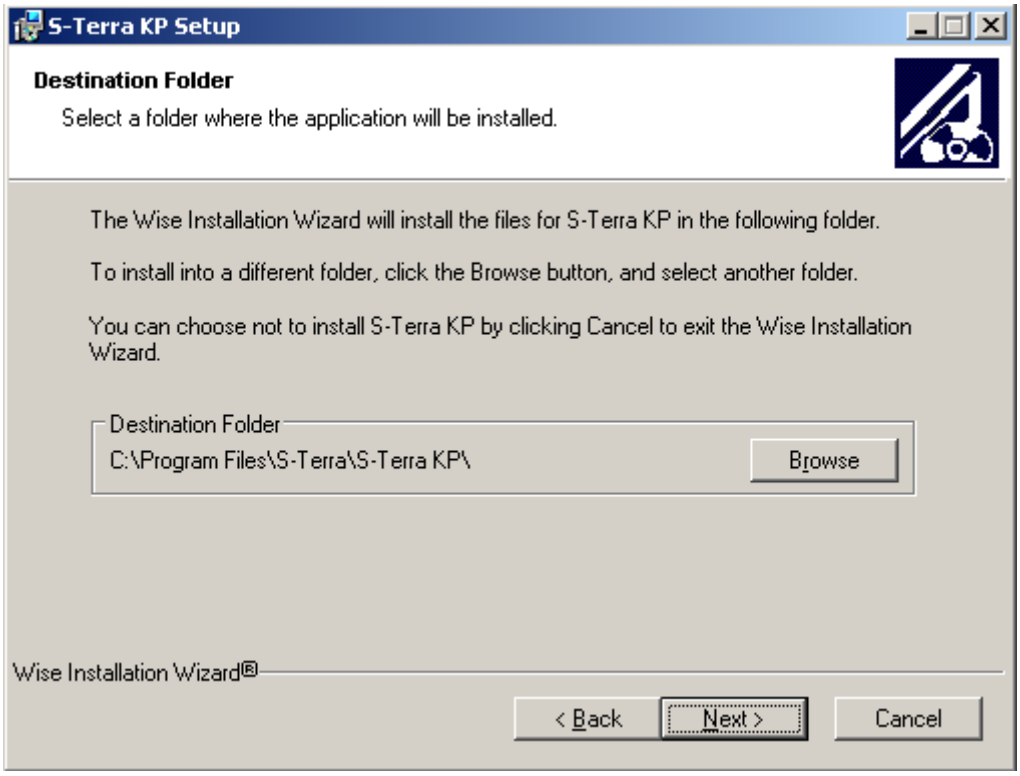

Рисунок 6

Подтвердите готовность к инсталляции – нажмите кнопку Next (Рисунок 7), после чего начнется процесс инсталляции.

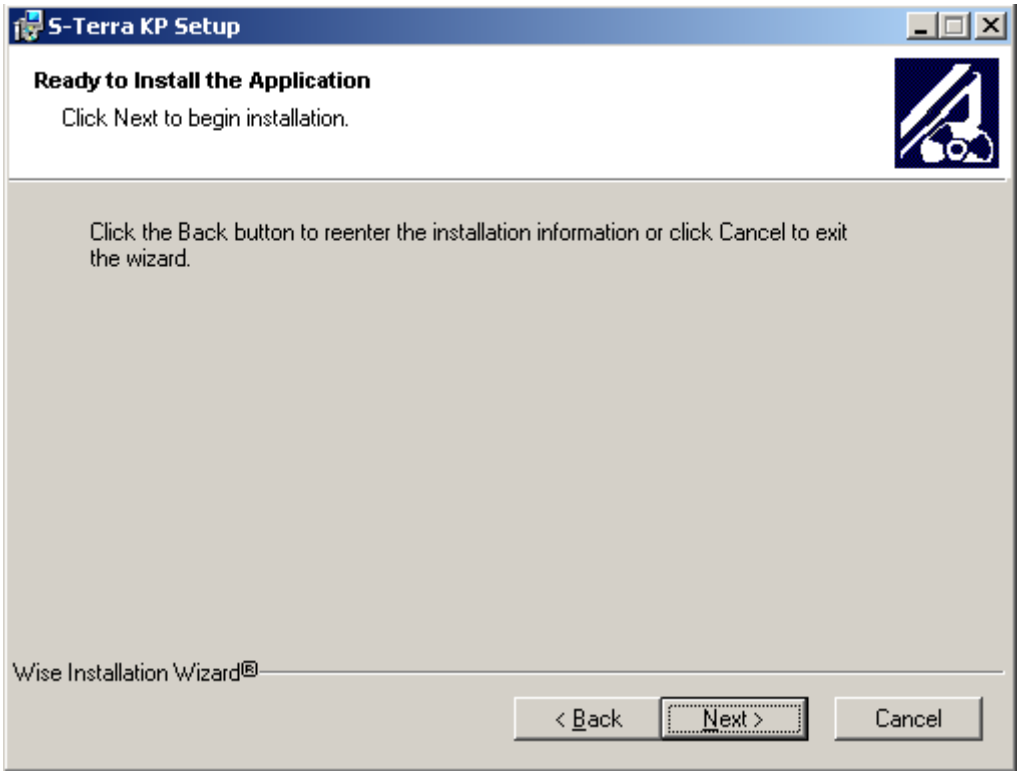

Рисунок 7

Далее появится окно с приглашением к инсталляции продукта FileZilla Server (Рисунок 8). Примите условия лицензионного соглашения – нажмите кнопку I Agree.

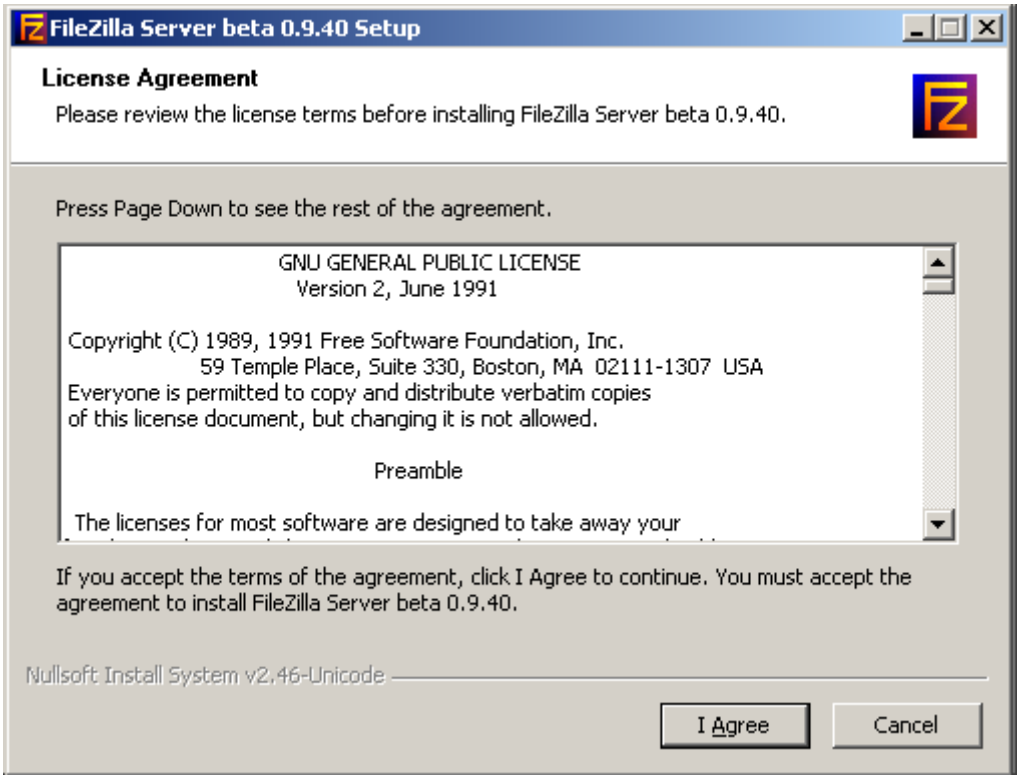

Рисунок 8

В следующем окне (Рисунок 9) предлагается выбрать компоненты для инсталляции. Оставьте настройки по умолчанию и нажмите кнопку Next.

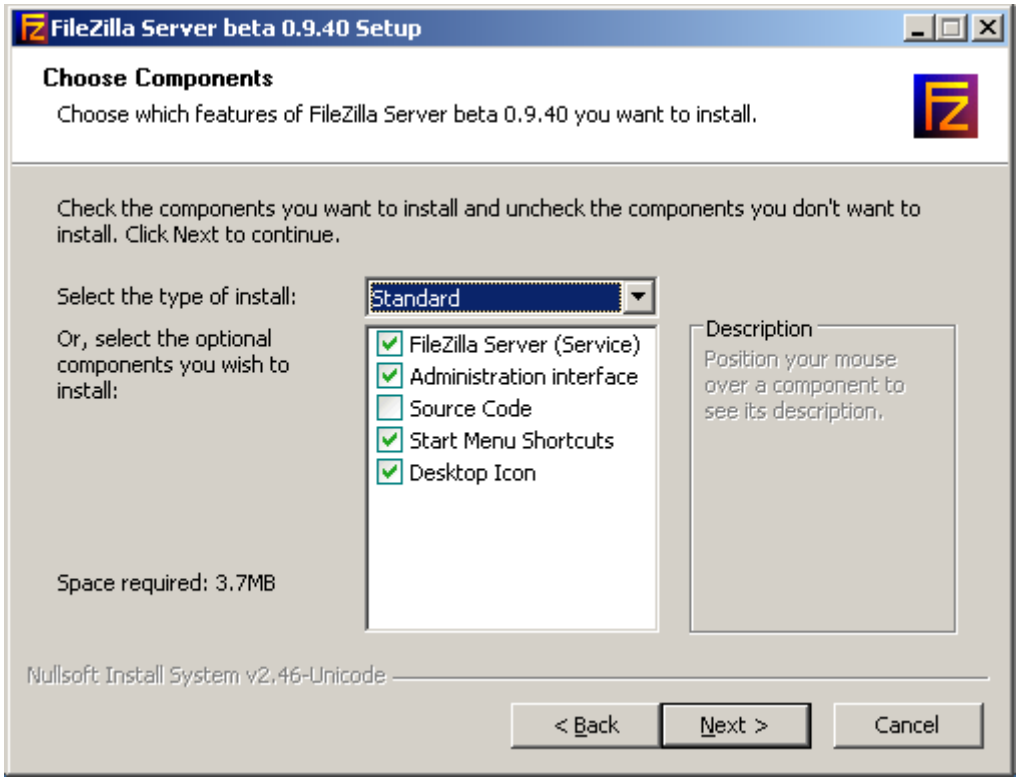

Рисунок 9

Укажите папку, в которую будет установлен продукт FileZilla Server (Рисунок 10).

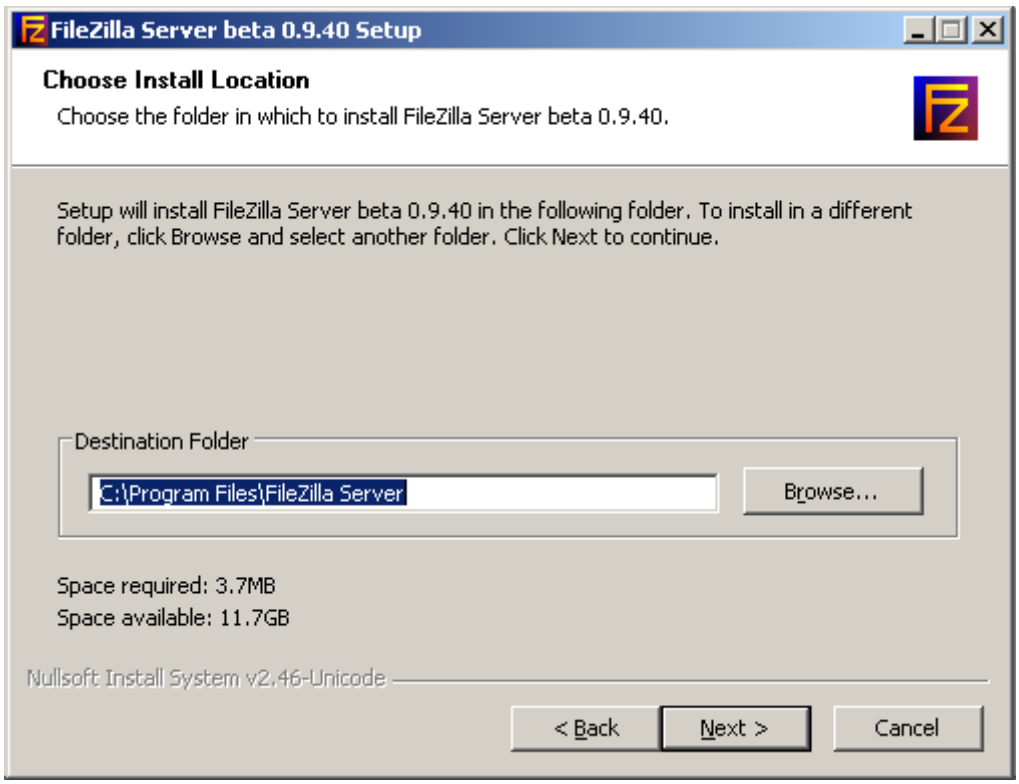

Рисунок 10

В окне выбора настроек для запуска сервиса продукта FileZilla Server оставьте значения по умолчанию и нажмите кнопку Next (Рисунок 11).

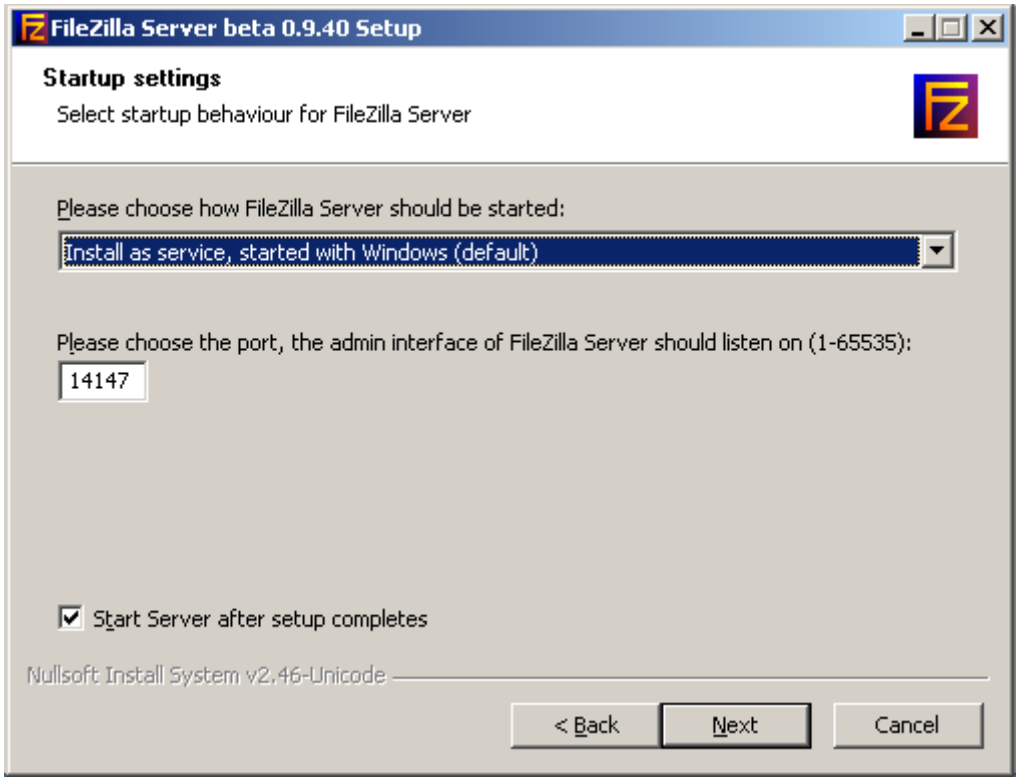

Рисунок 11

В окне с настройками старта консоли управления продуктом FileZilla Server оставьте значения по умолчанию и нажмите кнопку Install (Рисунок 12), после чего запустится процесс установки.

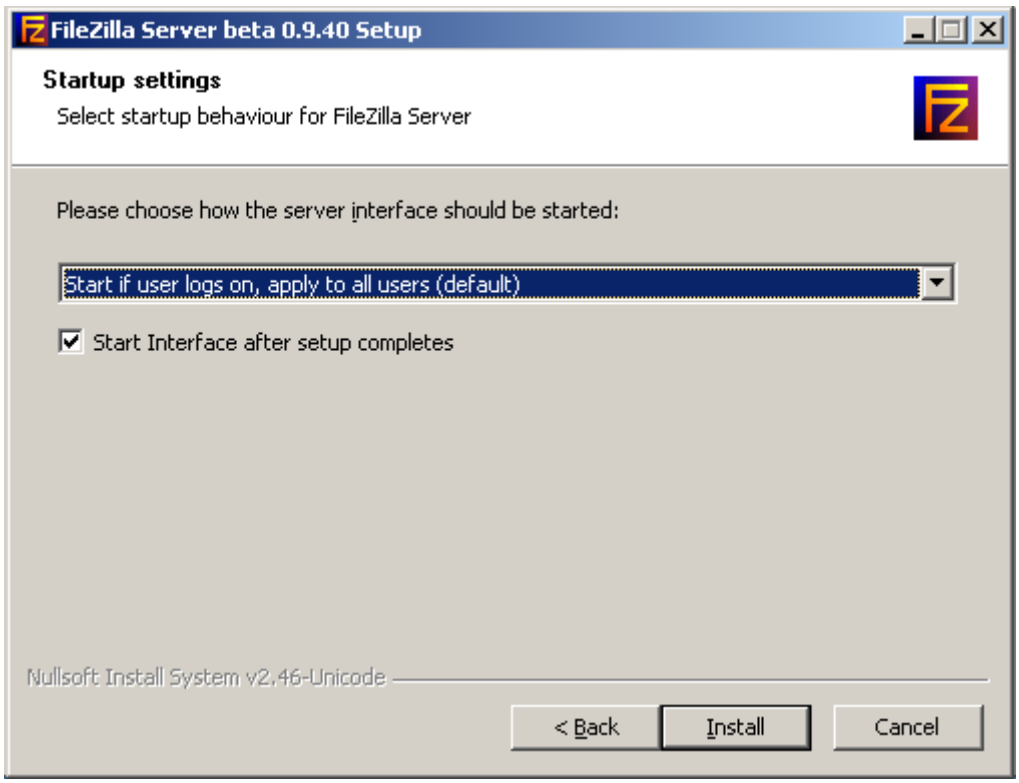

Рисунок 12

По завершению процесса установки нажмите кнопку Close (Рисунок 13).

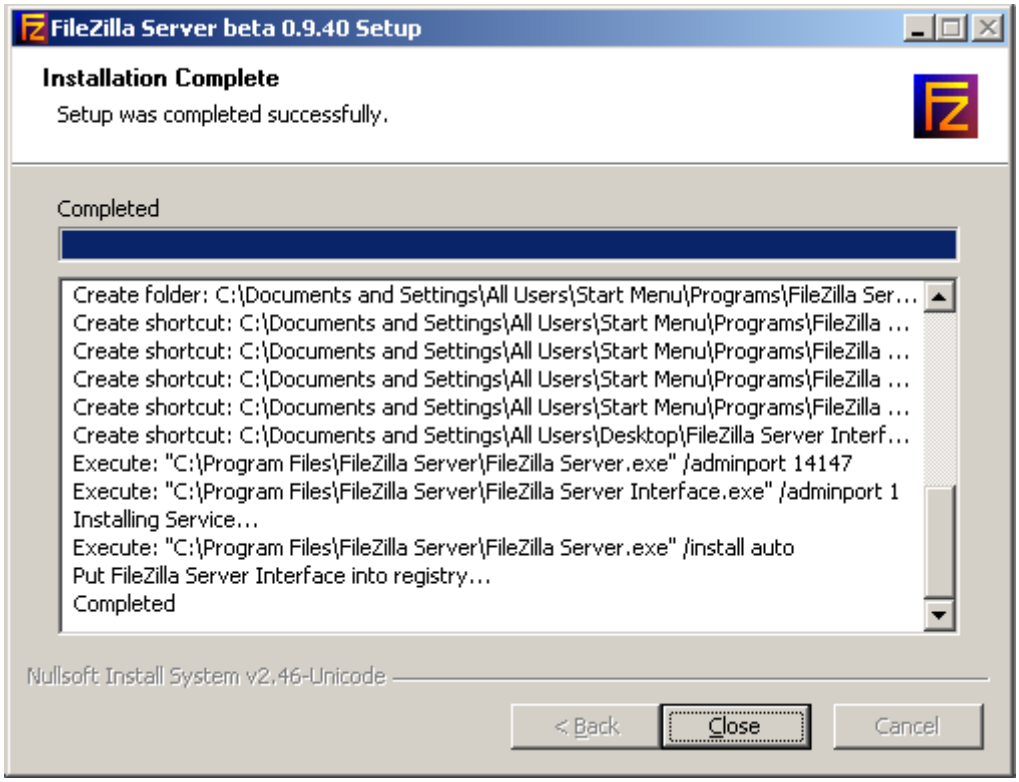

Рисунок 13

Запустится консоль управления продуктом FileZilla Server (Рисунок 14), нажмите кнопку OK.

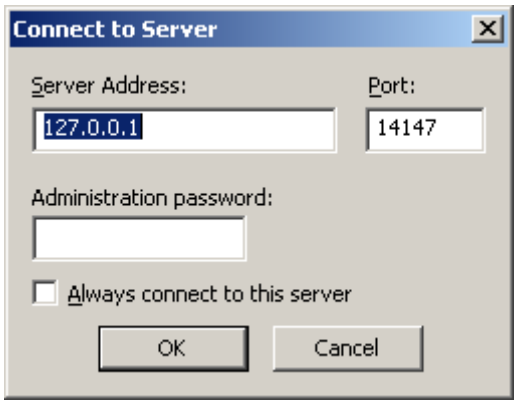

Рисунок 14

Далее должно произойти установление соединения с FTP-сервером **FileZilla Server** (Рисунок 15).

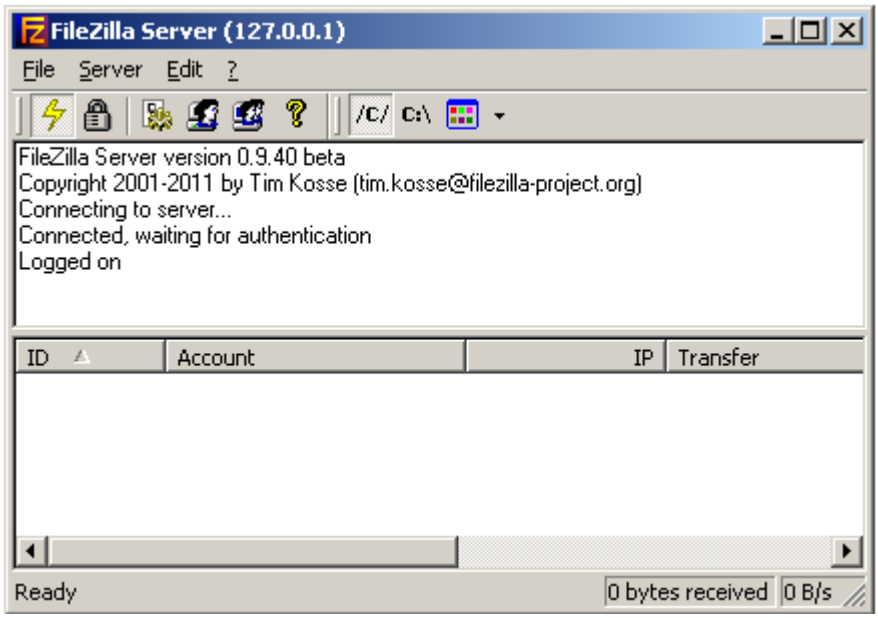

Рисунок 15

После успешного соединения можно закрыть окно консоли продукта **FileZilla Server**. После установки всех компонент происходит запуск сервиса, который может продолжаться около двух минут, т.к. проверяется целостность программной части продукта. Закончите установку продукта Сервер управления, нажав кнопку Finish (Рисунок 16).

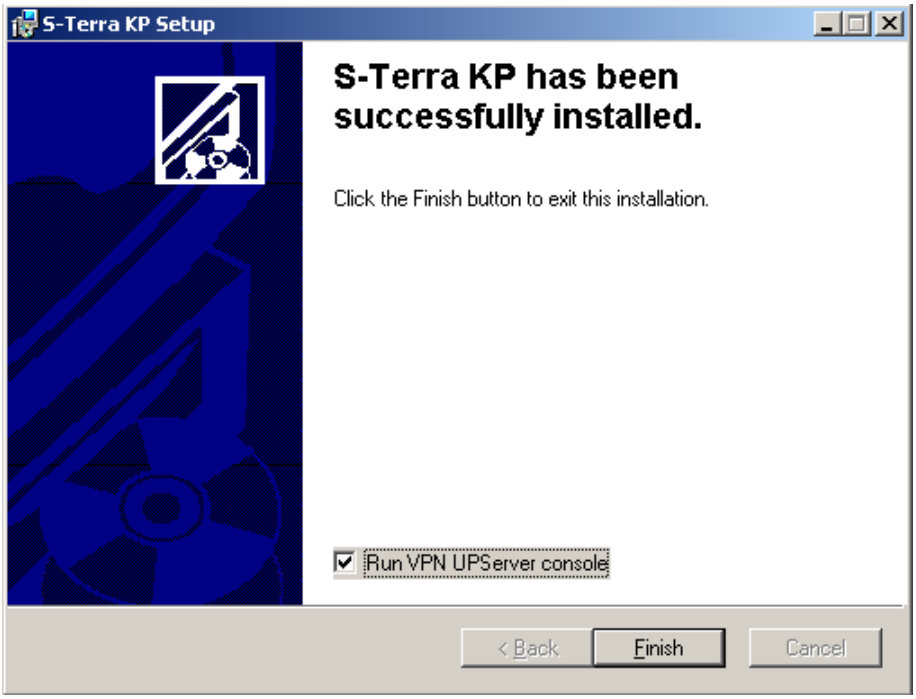

Рисунок 16

4. Настройка Сервера управления

4.1. Настройка механизма идентификации и аутентификации в Сервер управления

Для настройки механизма идентификации и аутентификации при доступе к Серверу управления выполните следующее:

1. Закройте окно **VPN UPServer console**.
2. Скопируйте утилиту `authmgr.exe` из состава дистрибутива С-Терра КП в любой каталог, например, в каталог установки Сервера управления `C:\Program Files\UPServer`, и запустите ее.
3. В окне с предупреждением (Рисунок 17) дайте утвердительный ответ.

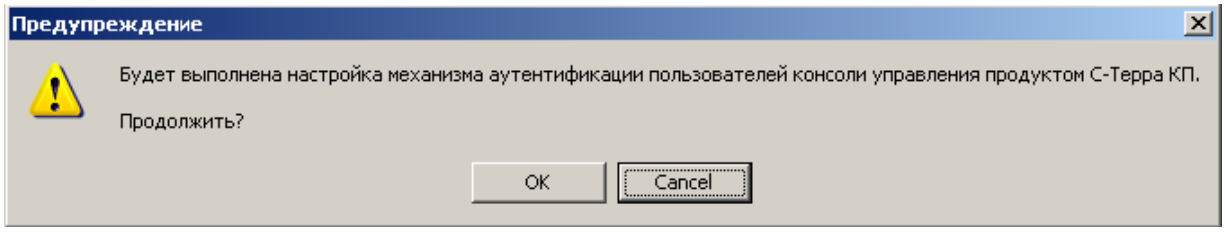

Рисунок 17

4. Настройка завершена, нажмите OK (Рисунок 18).

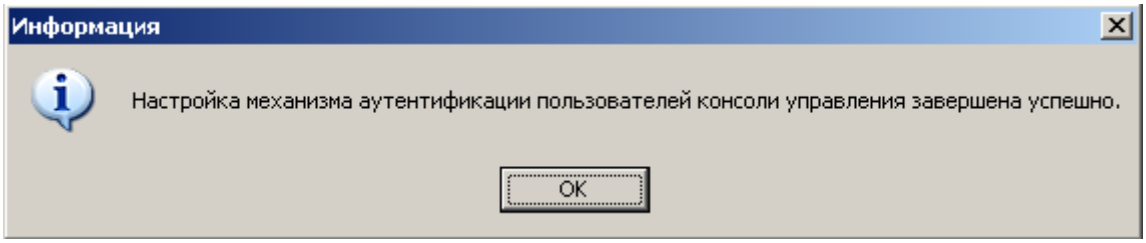

Рисунок 18

5. Запустите консоль Сервера управления - **VPN UPServer Console** (`Пуск-Программы-S-Terra-S-Terra KP-VPN UPServer Console`).
6. Появится окно **UPServer login** для ввода идентификатора администратора и его пароля (Рисунок 19). Назначать уполномоченного администратора может только суперпользователь. Поэтому сначала введите идентификатор суперпользователя - superuser.и назначьте ему пароль, нажав кнопку Change...

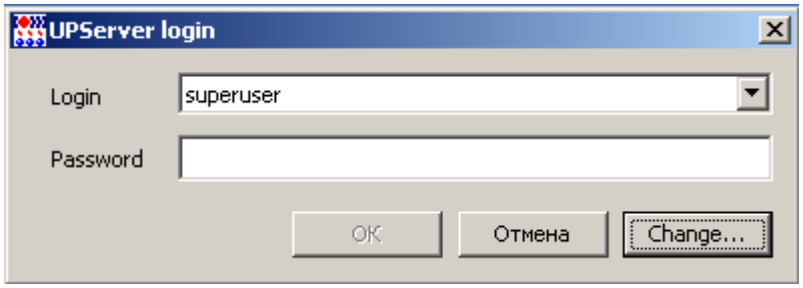

Рисунок 19

7. Затем в окне **UPServer user list** нажмите кнопку Add и в окне **UPServer user** задайте идентификатор и пароль уполномоченного администратора, нажмите OK в двух окнах (Рисунок 20).

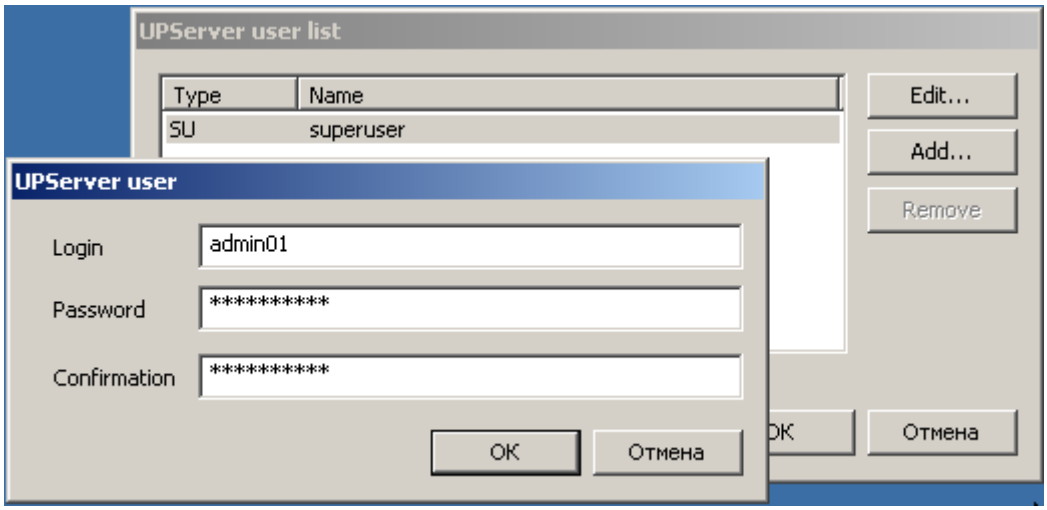

Рисунок 20

8. При запуске Сервера управления появится окно логина, введите идентификатор уполномоченного администратора и его пароль (Рисунок 21).

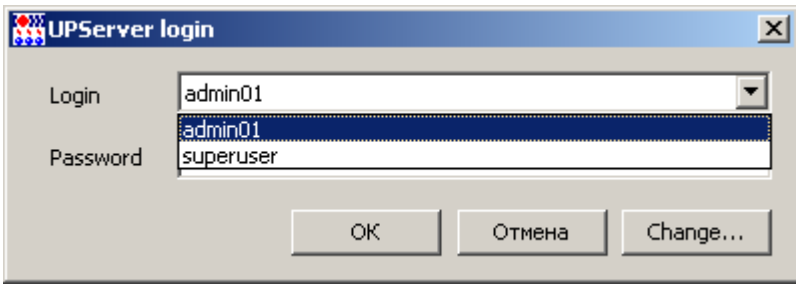

Рисунок 21

9. После нажатия кнопки OK запустится консоль Сервера управления - **VPN UPServer Console** (Рисунок 22)**.** При трех общих неуспешных попытках ввода идентификатора и пароля уполномоченного администратора окно консоли Сервера управления не будет открыто, а появится сообщение о количестве неуспешных попыток ввода логина.

4.2. Настройка Сервера управления

Начальная настройка Сервера управления производится во вкладке **Settings**, а настройка и управление клиентами – во вкладке **Clients** (Рисунок 22).

Меню графического интерфейса описано в главе «Описание интерфейса Сервера управления».

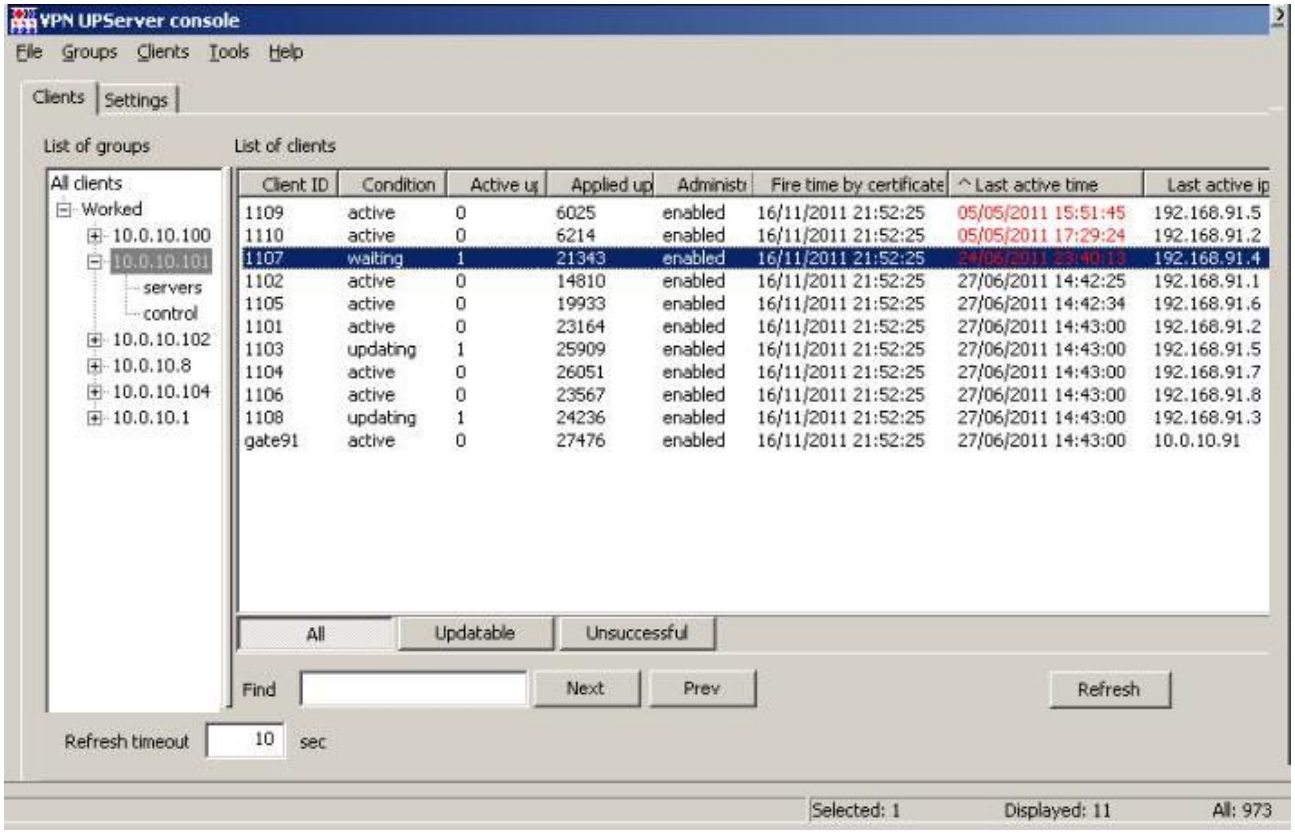

Рисунок 22

При первом запуске приложения **VPN UPServer Console** выводится предупреждение о необходимости задать настройки продукта ***Сервер управления*** (Рисунок 23).

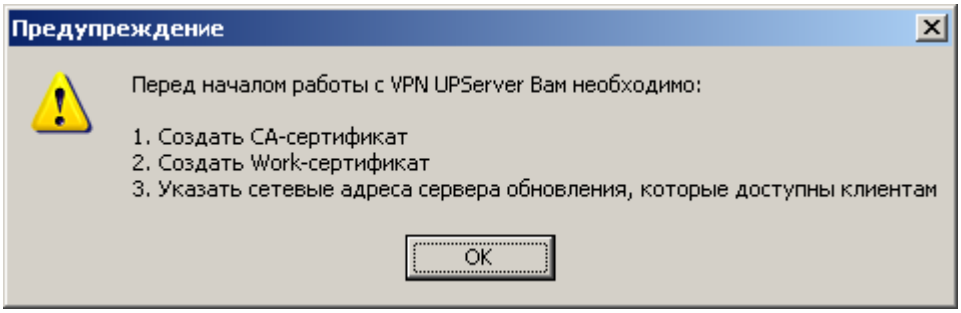

Рисунок 23

Нажмите кнопку OK, откроется окно настроек продукта Сервер управления (Рисунок 24). Во вкладке **Settings** введите данные лицензии, создайте CA-сертификат и рабочий сертификат (work certificate) Сервера управления, а также задайте сетевые адреса Сервера управления.

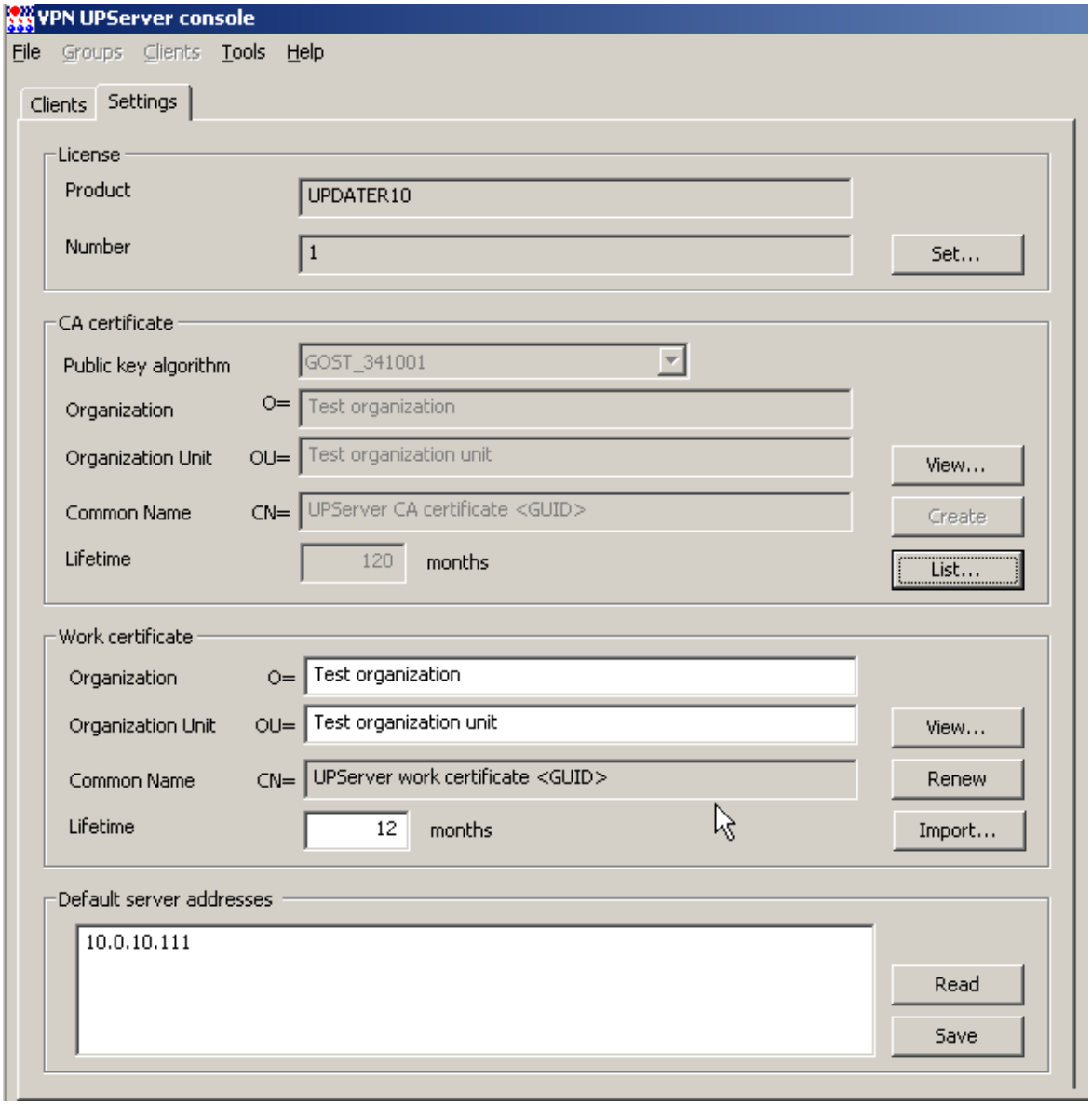

Рисунок 24

4.2.1. Ввод лицензии

Для ввода лицензии на продукт Сервер управления нажмите кнопку Set…(Рисунок 24).

В появившемся окне **Set license** (Рисунок 25):

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

`UPDATER10` – продукт будет работать с количеством Клиентов управления не более 10

`UPDATER100` – продукт будет работать с количеством Клиентов управления не более 100

`UPDATER500` – 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 с пятью Клиентами управления и не больше.

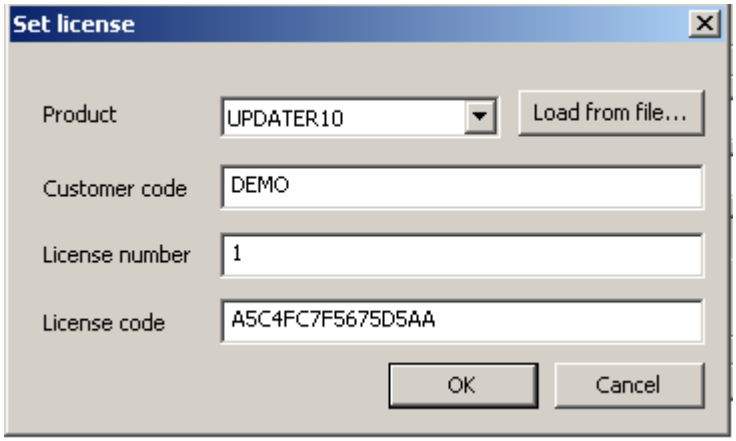

Рисунок 25

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 24) нажмите кнопку Create и заполните поля в окне **Create new CA certificate**, например, следующими значениями (Рисунок 26):

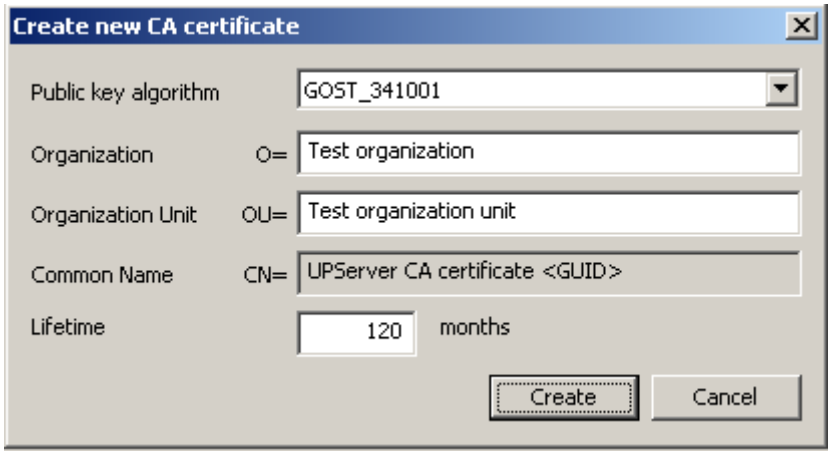

Рисунок 26

где

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

`RSA` - длина открытого ключа – 2048 бит

GOST_341001 (`ГОСТ Р 34.10-2001`) – длина открытого ключа – 512 бит, для использования этого алгоритма на Сервере управления должен быть установлен СКЗИ «КриптоПро CSP 3.6(R2)»

Organization – название организации

Organization Unit – название отдела в организации

Common Name – имя владельца сертификата, заполняется автоматически

Lifetime – срок действия сертификата в месяцах.

2. После этого нажмите кнопку Create, будет выдано **Предупреждение** (Рисунок 27), нажмите OK.

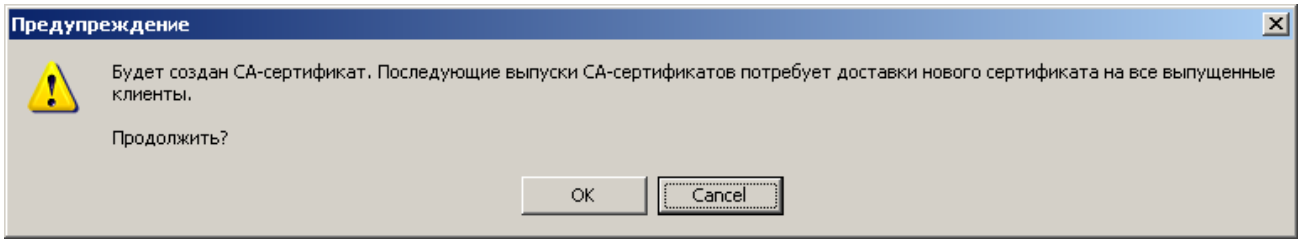

Рисунок 27

3. В процессе создания CA сертификата может быть выдано окно с запросом носителя для размещения контейнера с секретным ключом. Выберите Реестр и нажмите OK.

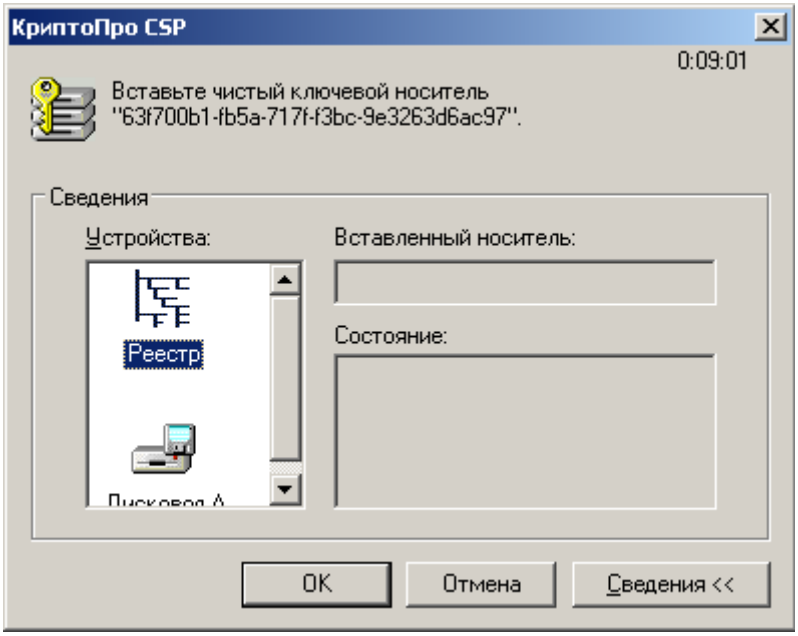

Рисунок 28

4. Если на сервере не установлен аппаратный ДСЧ, например, ПАК «Соболь» или Аккорд-АМДЗ, (что обязательно для режима КС2 «КриптоПро CSP»), то появляется окно для биологической инициализации ДСЧ – понажимайте клавиши или перемещайте указатель мыши.

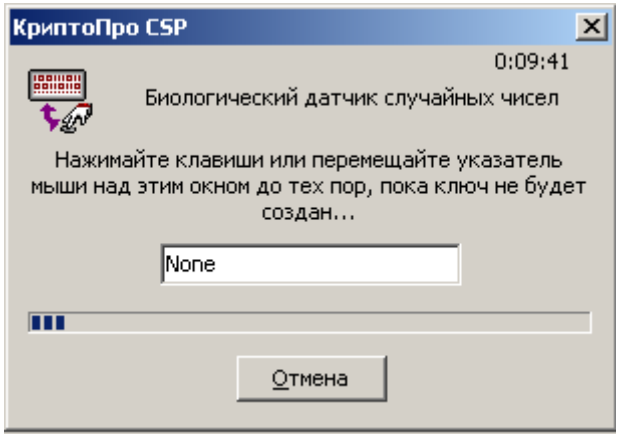

Рисунок 29

5. Введите пароль на контейнер с секретным ключом CA сертификата и подтвердите его.

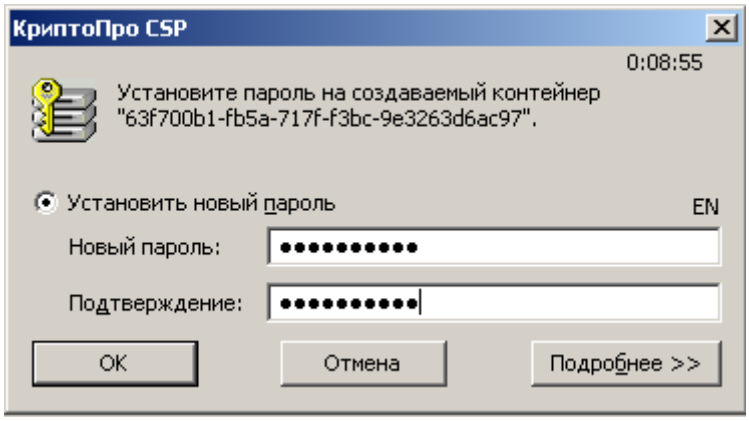

Рисунок 30

6. CA сертификат создан и хранится в сертификатном хранилище операционной системы, нажмите OK.

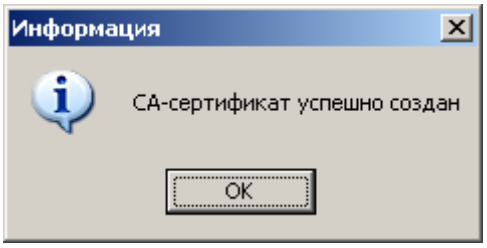

Рисунок 31

Note

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

Можно создать два CA сертификата (Рисунок 32), например, один с использованием алгоритма RSA, а другой - алгоритма GOST для генерации открытого ключа. Если у сертификата скоро истечет срок действия, можно заранее создать новый CA сертификат. Выбор из списка актуального для работы сертификата осуществляется его выделением и нажатием кнопки Set default. В результате напротив этого сертификата в столбце Active появится звездочка (*).

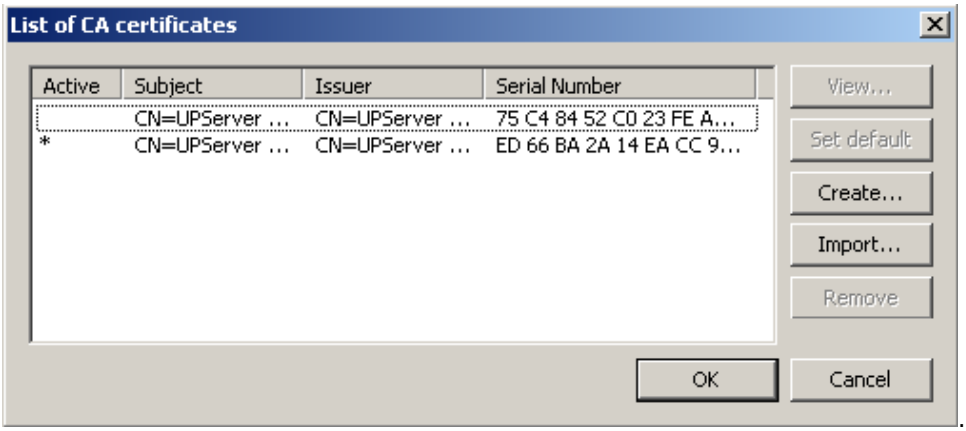

Рисунок 32

4.2.3. Создание рабочего сертификата

1. В группе **Work certificate** (Рисунок 24) заполните поля рабочего (локального) сертификата Сервера управления и нажмите кнопку Create. Перед созданием будет выдано **Предупреждение** (Рисунок 33):

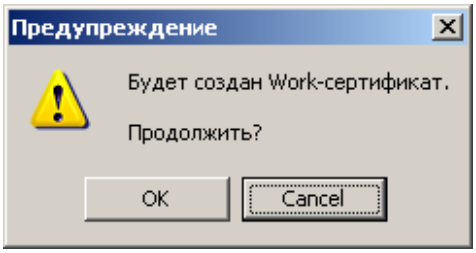

Рисунок 33

2. Если поля заполнены верно – нажмите кнопку OK. Возможен запрос ключевого носителя для размещения контейнера с секретным ключом рабочего сертификата (Рисунок 34).

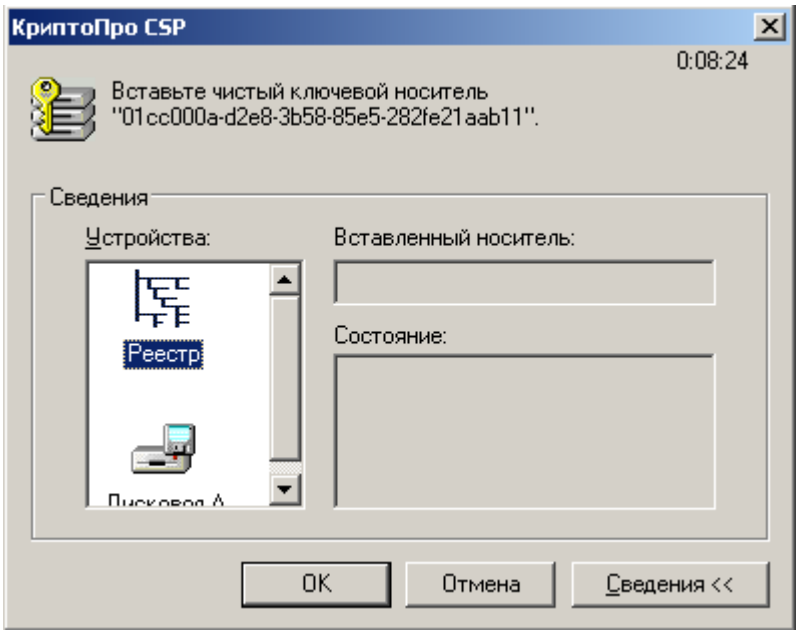

Рисунок 34

3. Если на сервере не установлен аппаратный ДСЧ, например, ПАК «Соболь» или Аккорд-АМДЗ, (что обязательно для режима КС2 «КриптоПро CSP»), то появляется окно для биологической инициализации ДСЧ – понажимайте клавиши или перемещайте указатель мыши.

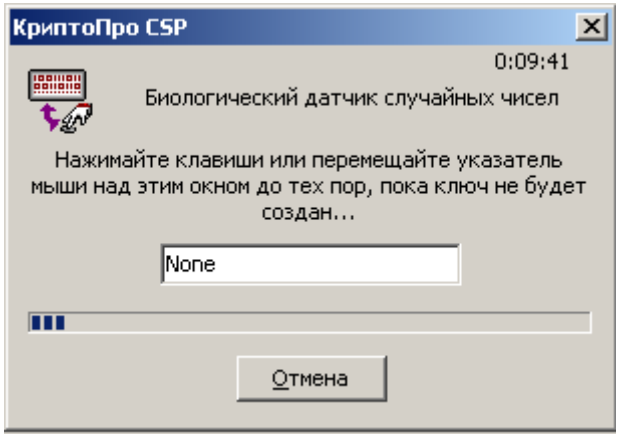

Рисунок 35

4. Введите пароль на контейнер с секретным ключом рабочего сертификата и подтвердите его.

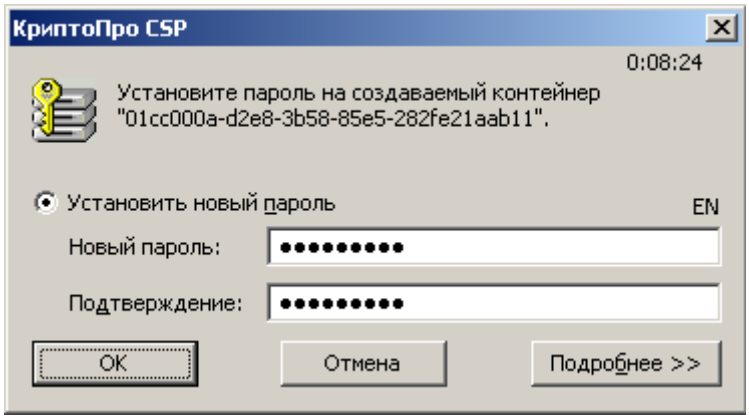

Рисунок 36

5. Введите пароль на контейнер с секретным ключом соответствующего CA сертификата.

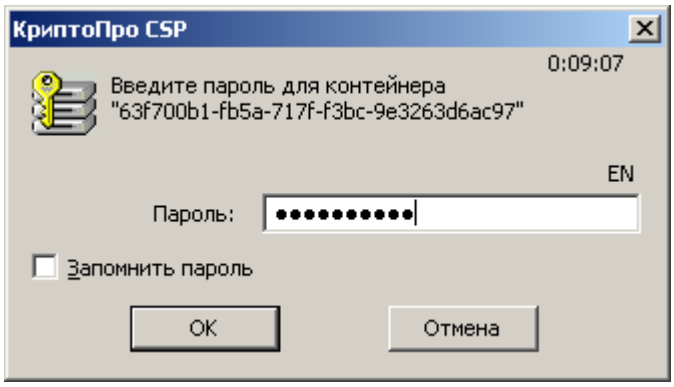

Рисунок 37

6. 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 38).

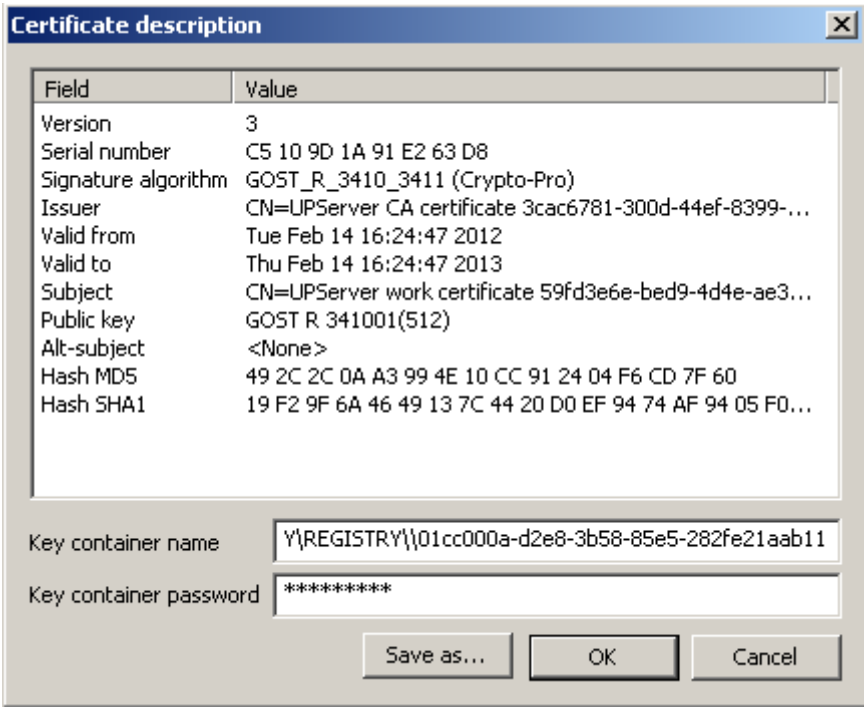

Рисунок 38

7. После успешного создания сертификата будет выдано подтверждение, нажмите кнопку OK (Рисунок 39).

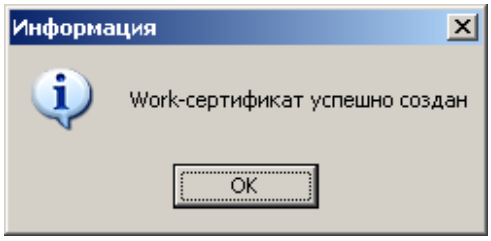

Рисунок 39

После этого кнопка Create в группе **Work certificate** изменится на Renew (Рисунок 24).

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

4.2.4. Задание адресов Сервера управления

1. В группе **Default server addresses** (Рисунок 24) 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.
2. **После задания адресов обязательно нажмите кнопку** Save, появится предупреждение (Рисунок 40).
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.

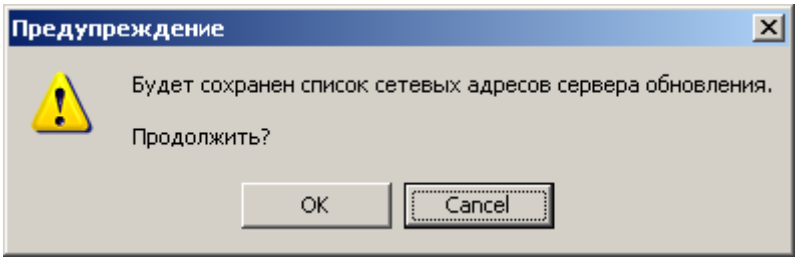

Рисунок 40

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**, создайте учетную запись для шлюза CSP VPN Gate, защищающего подсеть с Сервером управления, и учетные записи для каждого управляемого устройства, дистрибутивы Клиентов управления и CSP VPN Agent.

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 41) Сервера управления, интерфейс которой описан в разделе «Описание интерфейса Сервера управления». Во вкладке **Clients** отражается информация обо всех управляемых устройствах. ***Шлюз*** безопасности, защищающий подсеть с Сервером управления, будем называть ***центральным***. Приведем сценарий для настройки центрального шлюза.

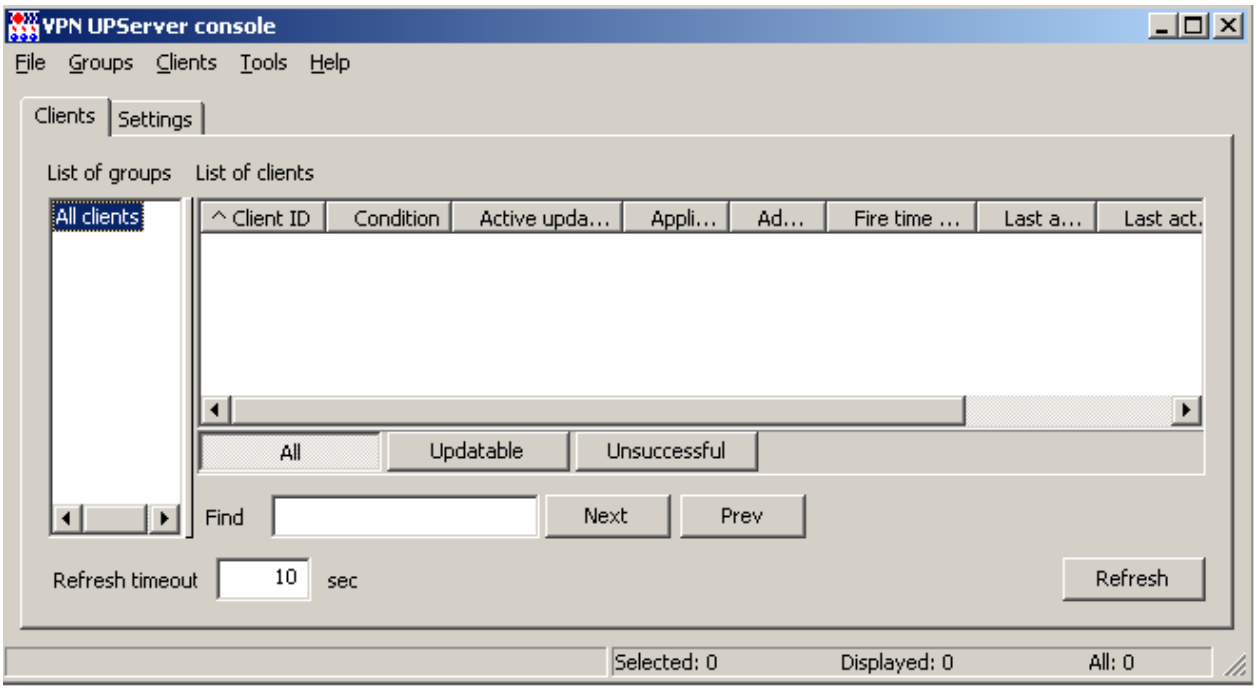

Рисунок 41

5.1. Создание учетной записи клиента для центрального шлюза

1. В меню ***Clients*** выберите предложение ***Create*** (Рисунок 42).

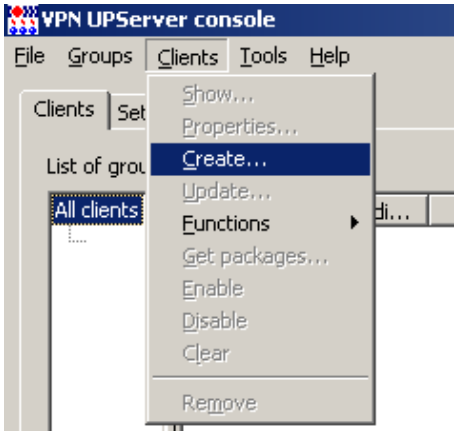

Рисунок 42

Появившееся окно **Create new client** (Рисунок 43) 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>,<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∈[1..9], или “LPTx”, где x∈[1..9]

Product package – имя файла дистрибутива CSP VPN Agent (который был создан с помощью продукта CSP VPN Server AdminTool/CSP VPN Client AdminTool) или имя файла с настройками продукта CSP VPN Agent, созданного с помощью окна **VPN data maker**, вызываемого кнопкой E

Кнопка E – вызывает окно **VPN data maker** (Рисунок 44) для задания политики безопасности и настроек продукта CSP VPN Agent.

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»).

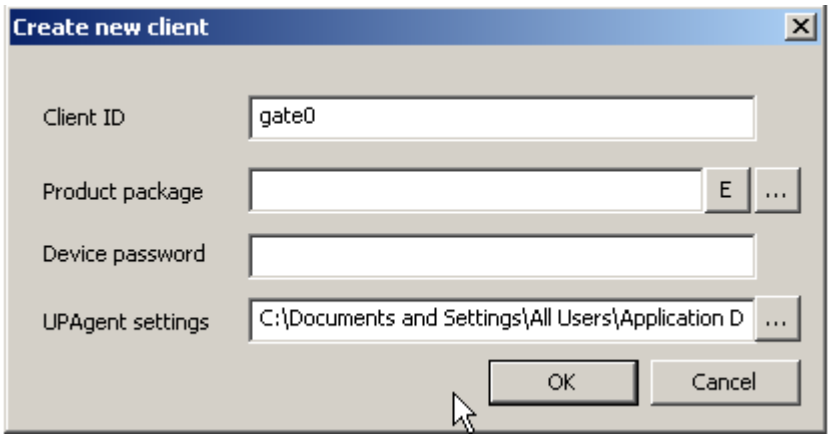

Рисунок 43

2. В поле **Client ID** введите идентификатор клиента, например, `gate0`.
3. Поле **UPAgent settings** оставьте без изменений, в нем указан файл с настройками Клиента управления.
4. В поле **Product package** нажмите кнопку E, появится окно **VPN data maker** (Рисунок 44).

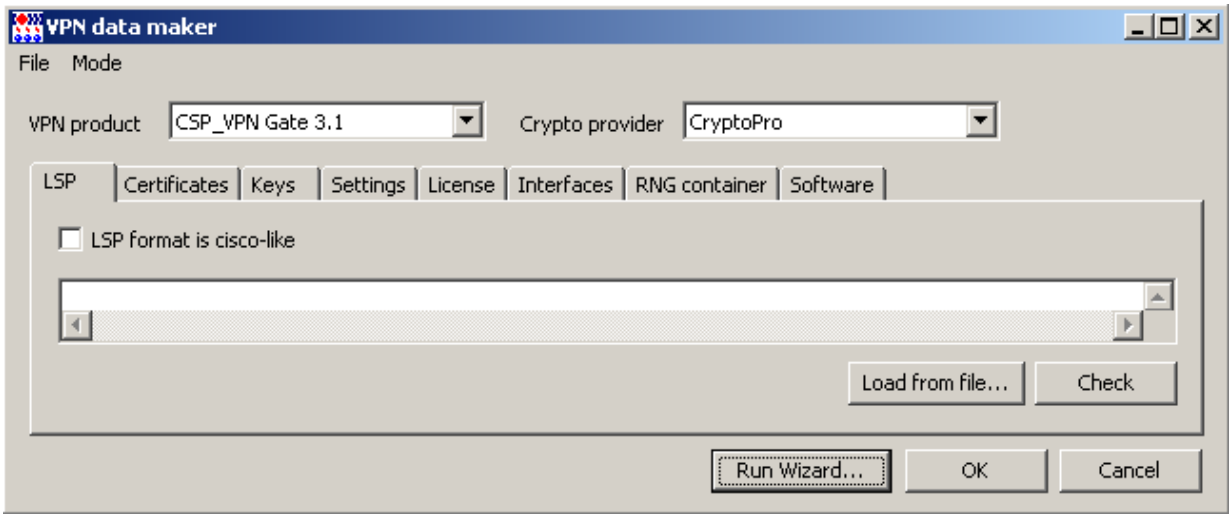

Рисунок 44

5. В окне **VPN data maker** выберите продукт CSP VPN Gate 3.1 и криптопровайдера CryptoPro (Рисунок 44).

6. Далее нужно задать политику безопасности для шлюза и другие настройки. Сложную политику можно задать во вкладке **LSP** (Рисунок 44) 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 взаимодействующих сторон (Рисунок 45). Интерфейс этого окна описан в разделе «Задание политики и настроек с использованием мастера».

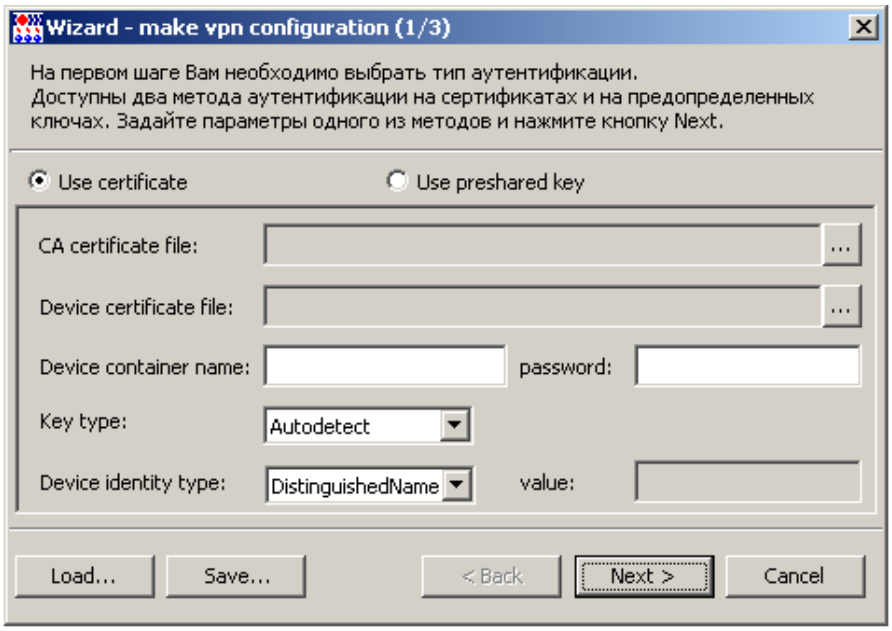

Рисунок 45

7. Выберите аутентификацию с использованием предопределенного ключа (Рисунок 46). ы
   В поле **Key name** введите имя ключа, например, `key0`. Введите значение ключа с клавиатуры. В качестве идентификатора устройства оставьте значение `Default` (IP-адрес устройства, на котором установлен CSP VPN Gate). Нажмите кнопку Next.

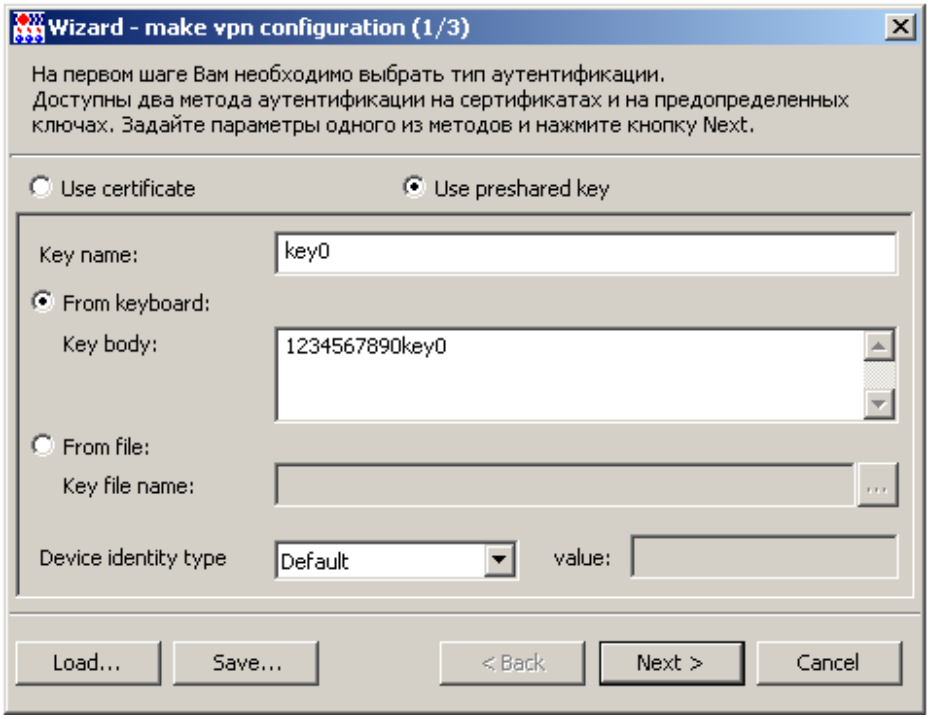

Рисунок 46

8. В следующем окне задайте правило фильтрации, по которому центральный шлюз будет пропускать трафик от управляемых устройств к Серверу управления и обратно. При этом трафик между управляемыми устройствами и центральным шлюзом должен быть защищенным (Рисунок 47). Для создания правила нажмите кнопку Add.

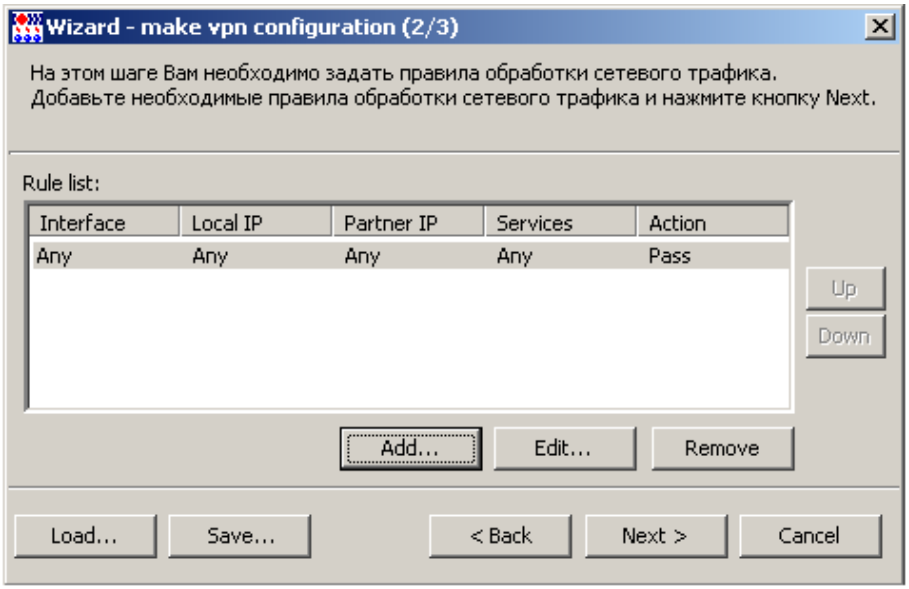

Рисунок 47

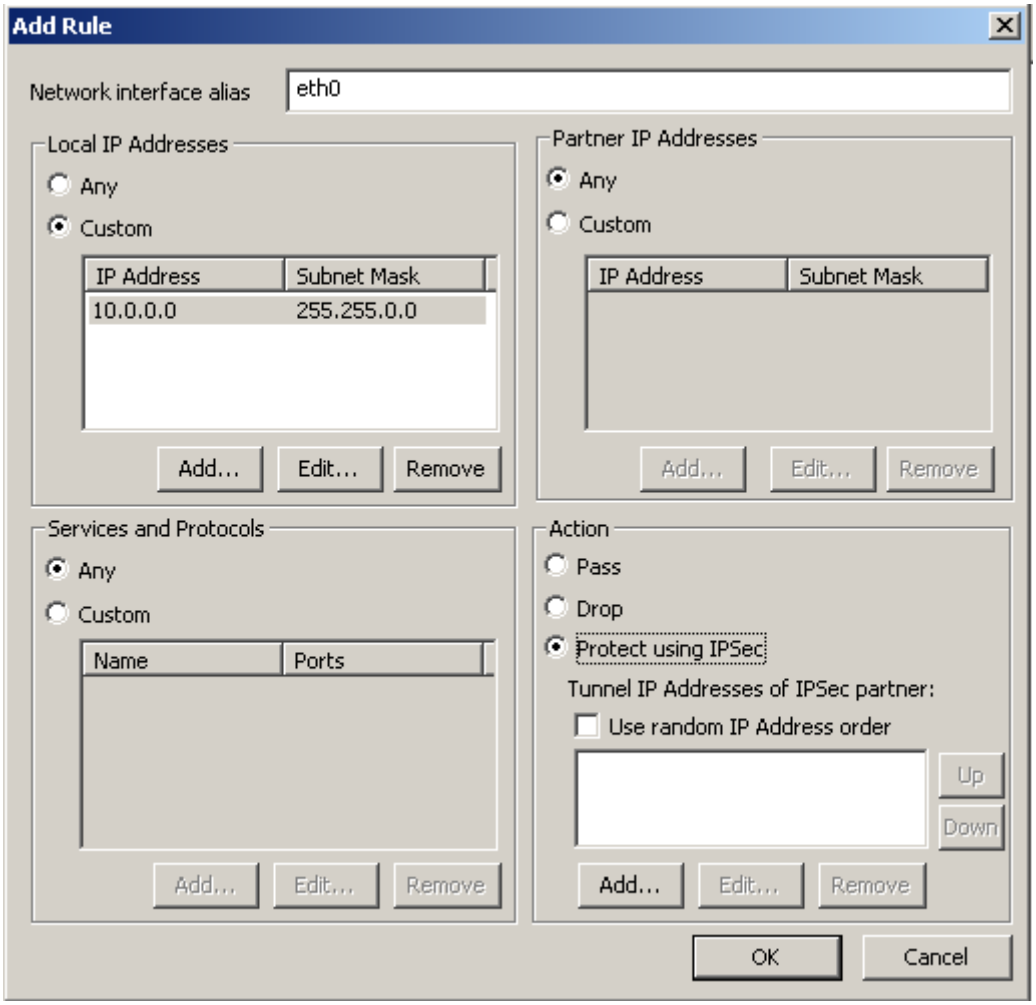

Рисунок 48

9. Создаваемое правило привяжите к интерфейсу шлюза с логическим именем, например, `eth0`, который смотрит во внешнюю сеть (Рисунок 2). В области **Local IP Addresses** (Рисунок 48) 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 Addresse**s поставьте переключатель в положение Any. В области **Action** - переключатель в положение ***Protect using IPsec***, не указывая адрес IPsec партнера (адрес любой).
10. После нажатия кнопки OK появится предупреждение (Рисунок 49). Нажмите кнопку Yes.

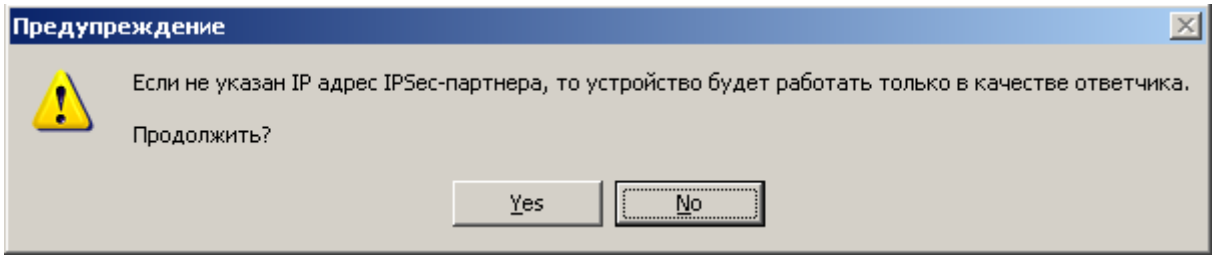

Рисунок 49

11. Увеличьте приоритет созданного правила (Рисунок 50), нажав кнопку Up.

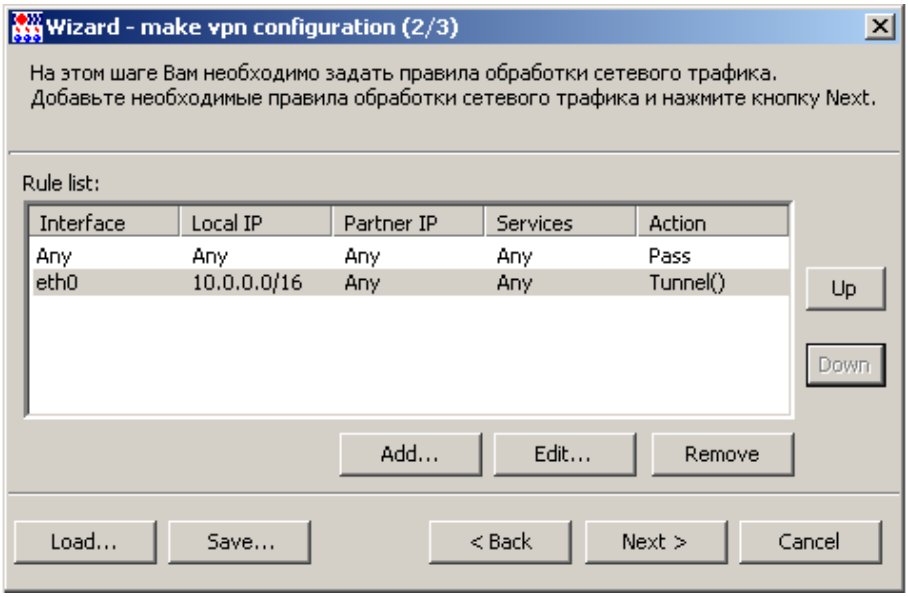

Рисунок 50

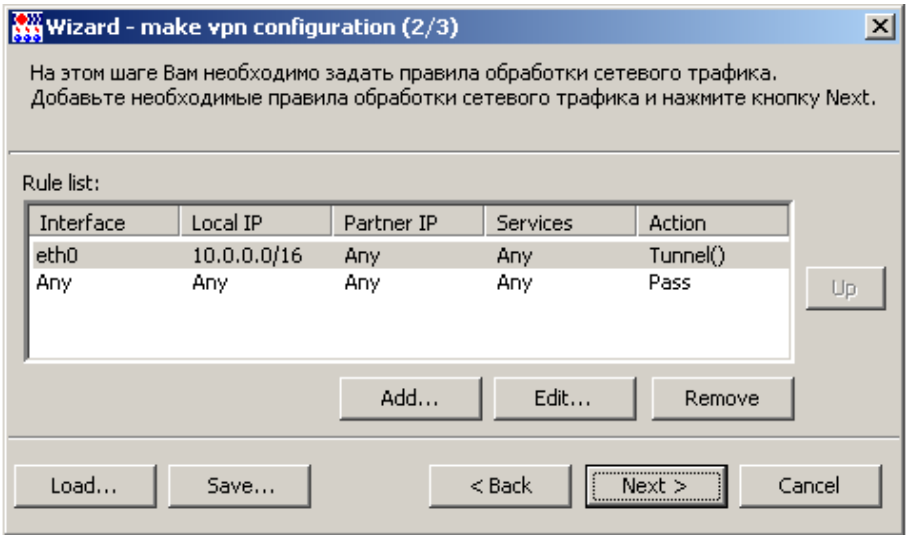

Рисунок 51

12. Нажмите кнопку Next (Рисунок 51).
13. Введите данные лицензии на продукт CSP VPN Gate и серийный номер лицензии на продукт криптопровайдера (КриптоПро CSP 3.6) (Рисунок 52). Если на шлюзе лицензия на КриптоПро CSP 3.6 уже задана и не требуется ее замена, то поле **Serial number** оставьте пустым.

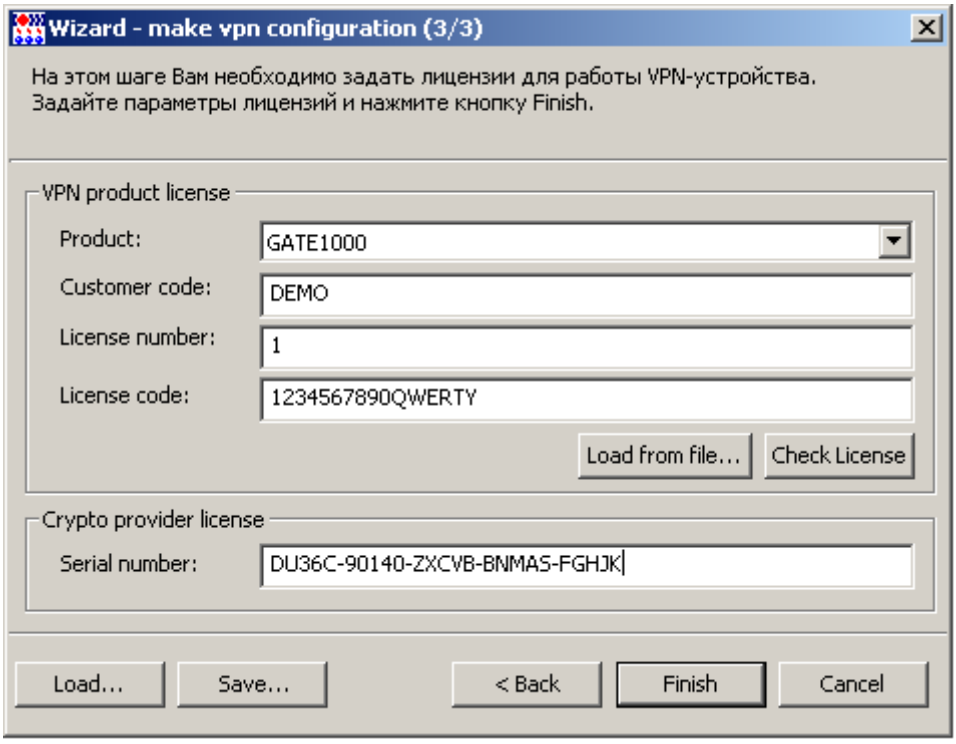

Рисунок 52

14. Сохраните введенные данные в окнах мастера, нажав кнопку Save...(Рисунок 52), и укажите имя файла-проекта в любом созданном вами каталоге (Рисунок 53).

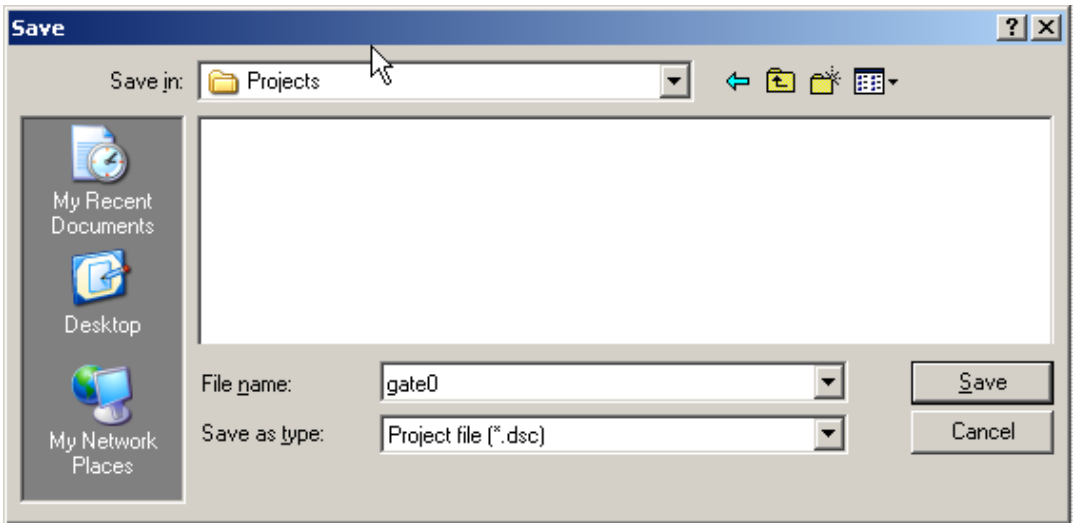

Рисунок 53

15. В окне мастера нажмите кнопку Finish (Рисунок 52). Все введенные данные будут отражены во вкладках проекта (Рисунок 54), за исключением вкладки **Interfaces**.

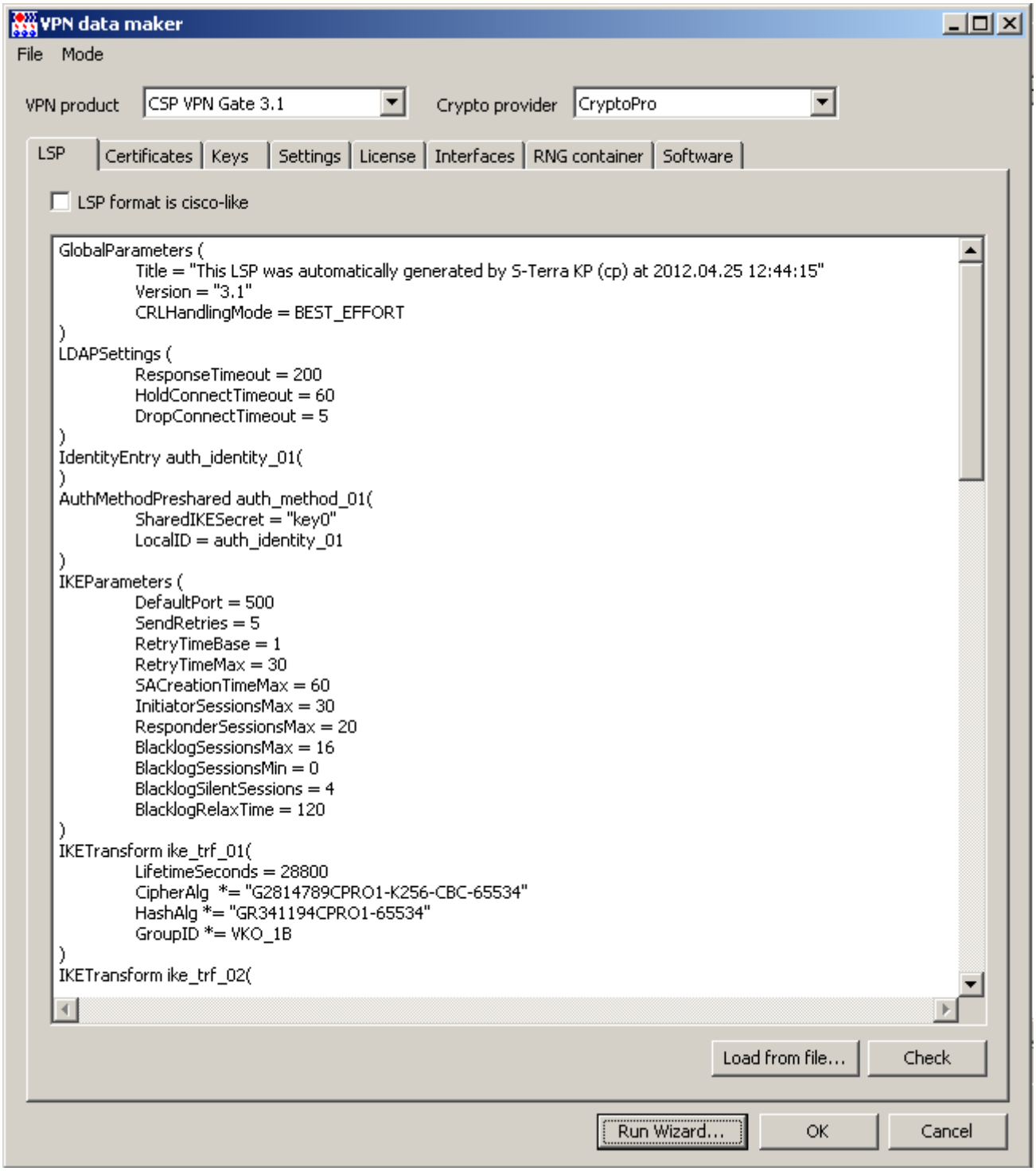

Рисунок 54

16. 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_mgr show` – для CSP VPN Gate 3.1, 3.11

    утилиту `/opt/VPNagent/bin/if_show` – для S-Terra Gate 4.0.

    Во вкладке **Interfaces** установите флажок **Network interface aliases**, нажмите кнопку Add и в окне **Network interface alias** введите логическое и физическое имя интерфейсов (Рисунок 55).

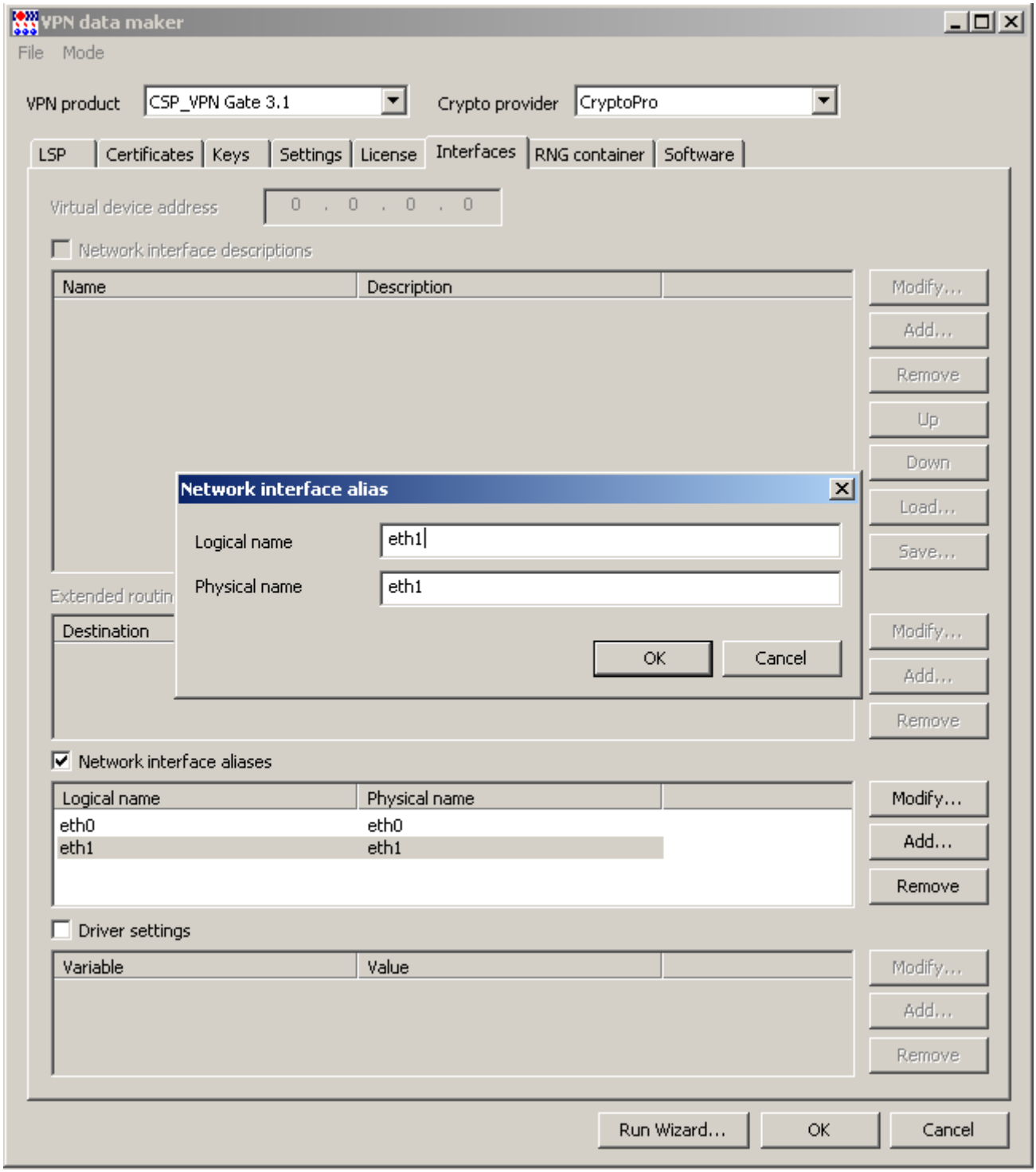

Рисунок 55

Note

Адреса сетевых интерфейсов шлюза, заданные через cisco-like консоль, игнорируются Сервером управления. Для корректного задания адресов рекомендуется пользоваться средствами операционной системы.

17. Во вкладке **Interfaces** нажмите кнопку OK, появится окно с настройками нового клиента (Рисунок 56), опять нажмите кнопку OK.

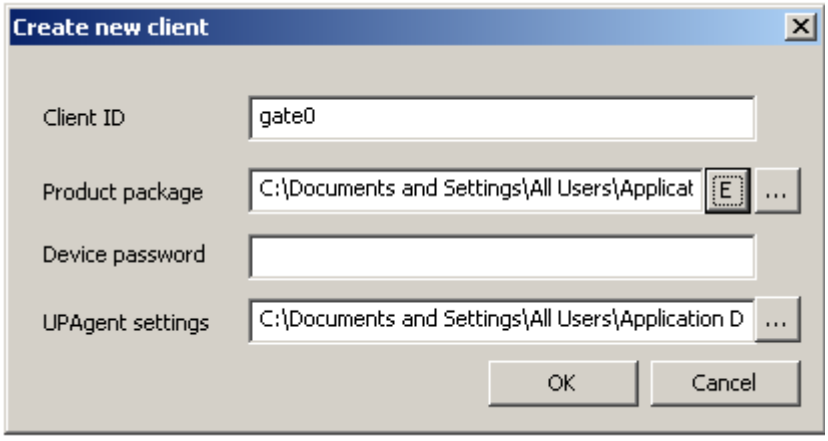

Рисунок 56

18. На Сервере управления в таблице клиентов появился новый клиент – `gate0`. Переведите его в активное состояние, выбрав в контекстном меню предложение ***Enable*** (Рисунок 57).

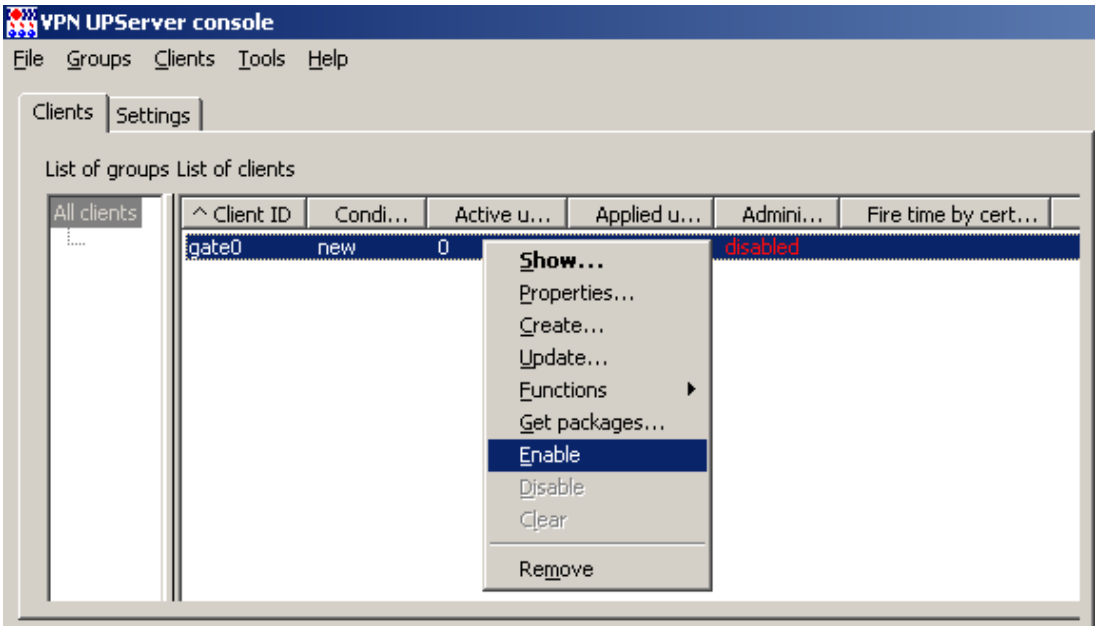

Рисунок 57

5.2. Подготовка скриптов для Клиента управления и CSP VPN Gate

1. Для установки Клиента управления, дистрибутив которого размещен на шлюзе в каталоге `/packages`, и обновления настроек CSP VPN Gate следует подготовить два скрипта. Для клиента `gate0` выберите предложение ***Get packages*** в контекстном меню (Рисунок 58).

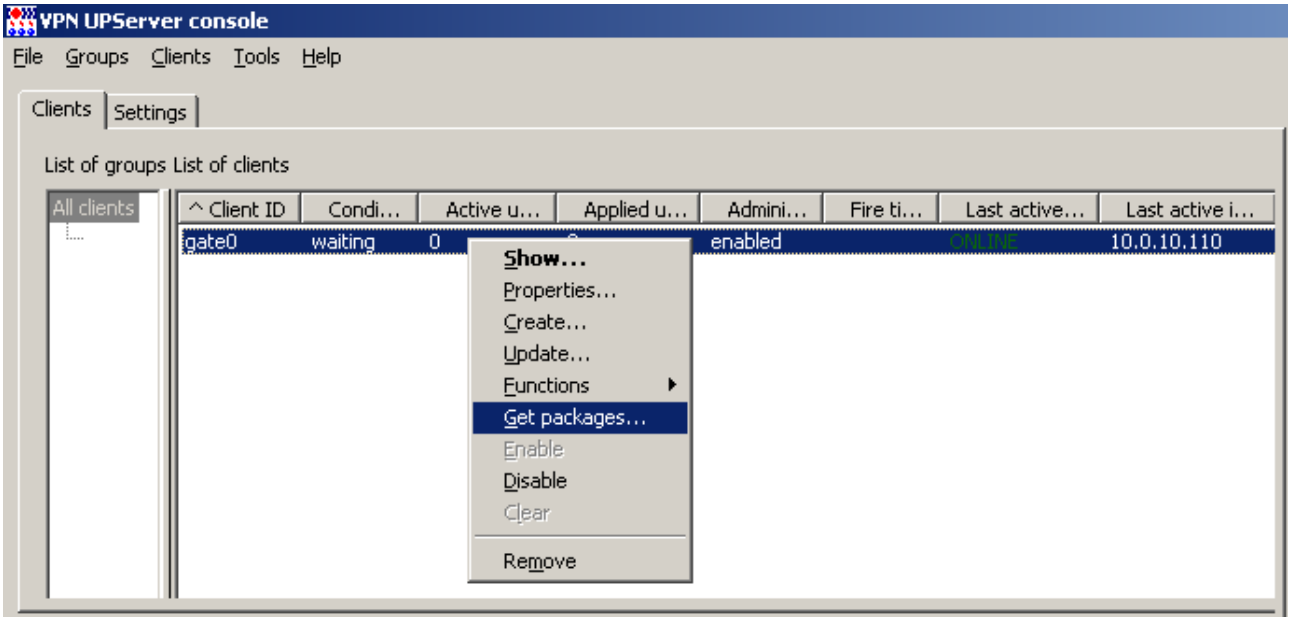

Рисунок 58

2. В открывшемся окне укажите каталог для сохранения скриптов (Рисунок 59).

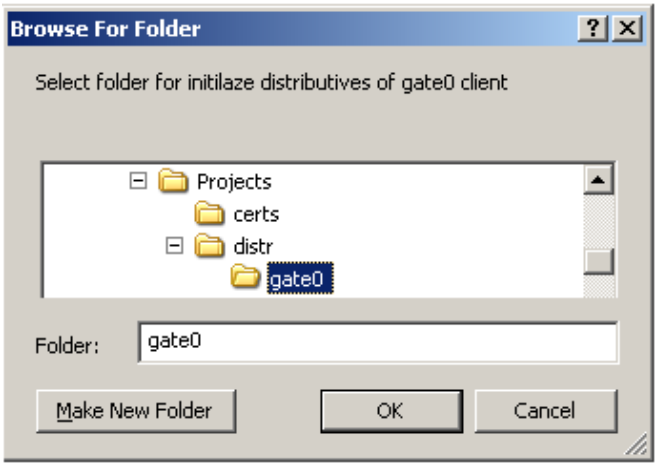

Рисунок 59

В указанный каталог будут сохранены два файла (Рисунок 60), (Рисунок 61):

- `setup_upagent.sh` – скрипт, содержащий данные для Клиента управления
- `setup_product.sh` – скрипт, содержащий настройки для продукта CSP VPN Gate.

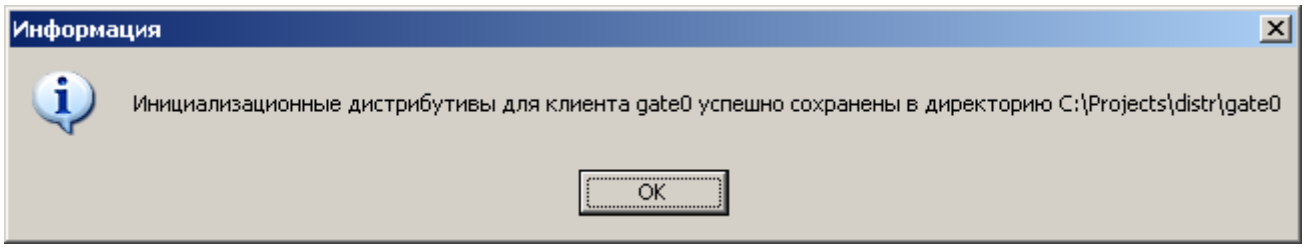

Рисунок 60

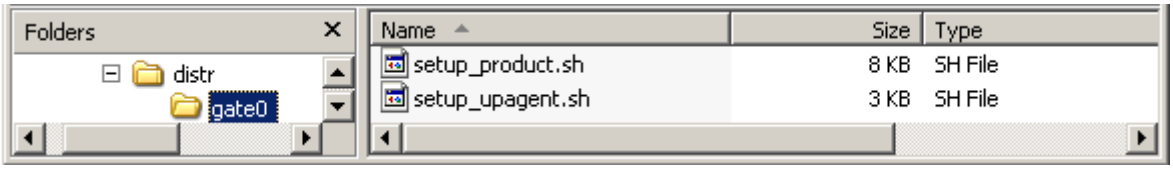

Рисунок 61

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 CSP VPN Gate версии 3.1 поставляется на устройстве без инсталлированного Клиента управления. Для версии 3.11 CSP VPN Gate поставляется вместе с инсталлированным Клиентом управления, требуется инициализировать Клиента управления.

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

Установка созданных скриптов осуществляется локально, так как Клиент управления на этом устройстве еще не инсталлирован (инициализирован). 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 Configuration
   - 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 62).

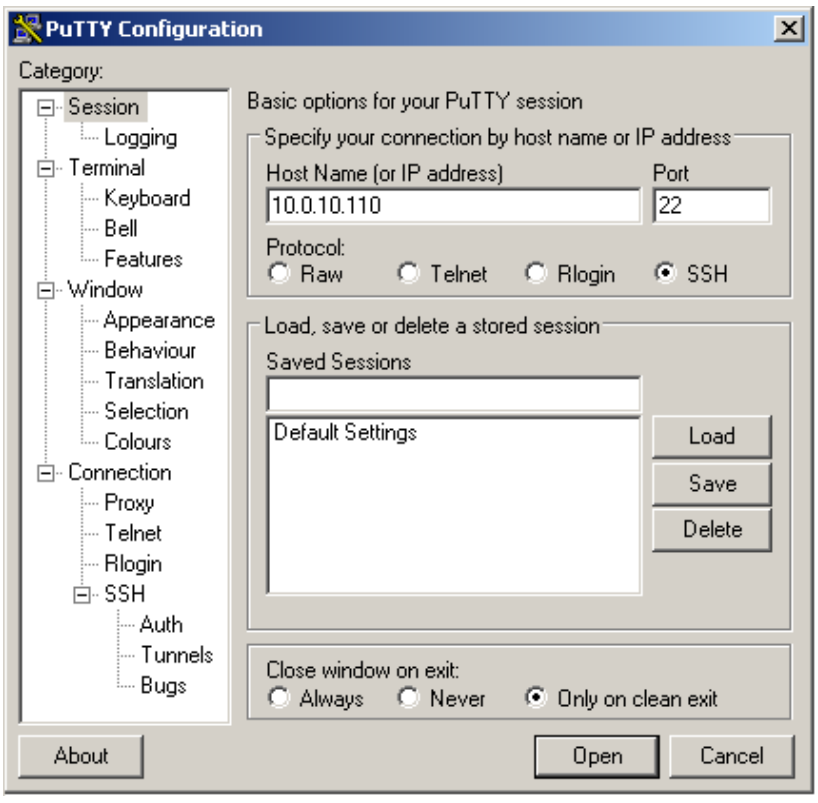

Рисунок 62

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 63).

Рисунок 63

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:

```
[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 Red Hat Enterprise Linux 5
C:\Program Files\S-Terra\S-Terra KP\upagent\LINUXRHEL5\vpnupagent.tar

для ОС Solaris 10
C:\Program Files\ S-Terra\S-Terra KP\
UPServer\upagent\SOLARIS\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
```

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

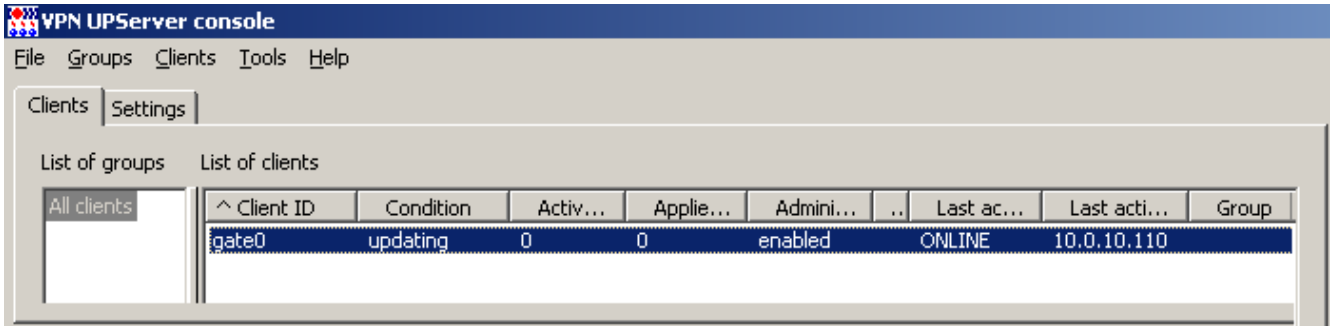

Рисунок 64

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

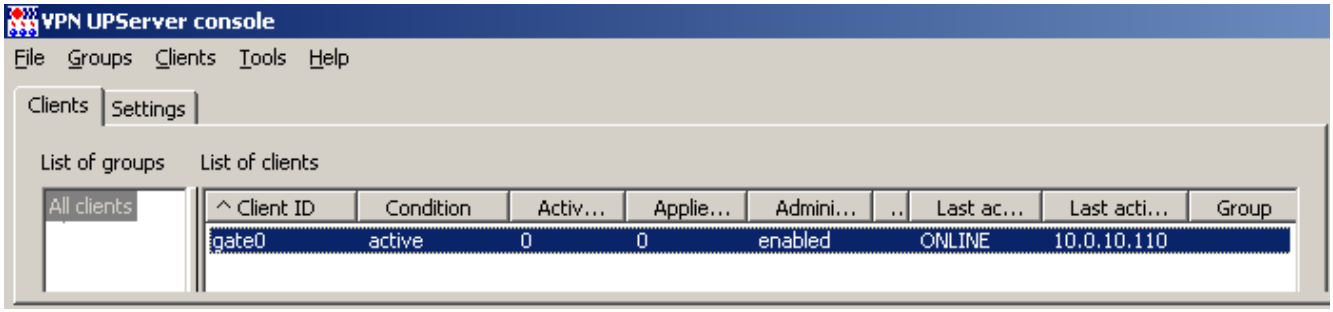

Рисунок 65

6. Настройка и управление устройством с CSP VPN Server/CSP VPN Client

6.1. Создание клиента на Сервере управления

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

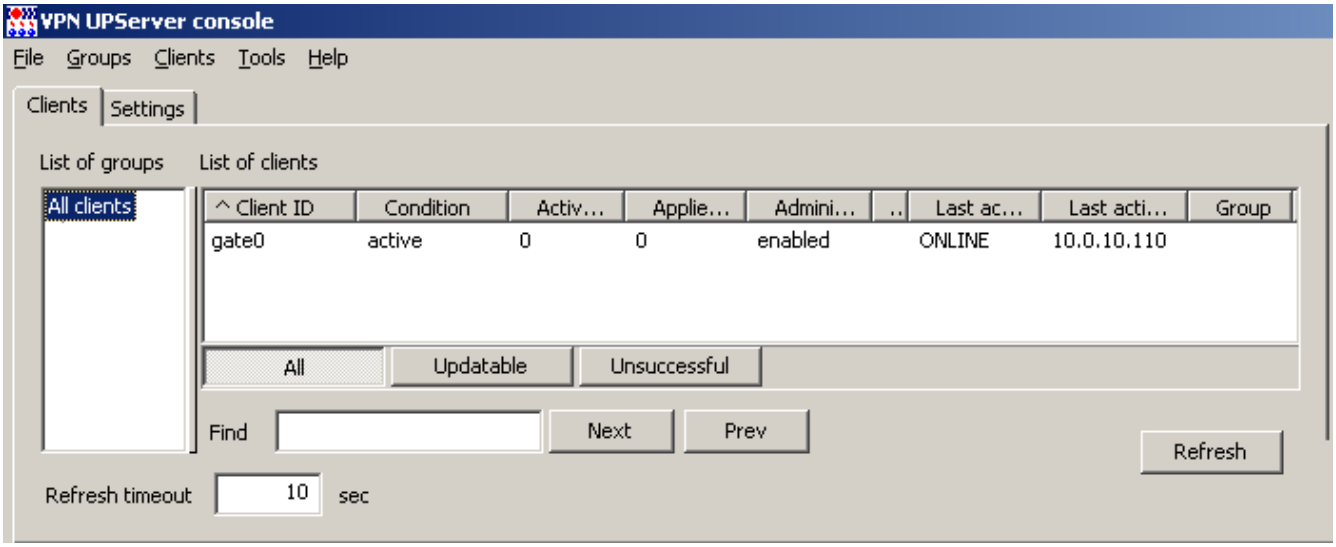

Рисунок 66

1. Для создания группы выделите группу All clients, а в меню ***Groups*** выберите предложение ***Create*** (Рисунок 67).

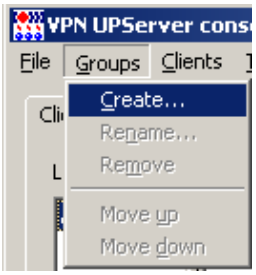

Рисунок 67

В поле **Group name** введите имя группы, например, Office1, в которой будут созданы в дальнейшем клиенты (Рисунок 68), и нажмите OK.

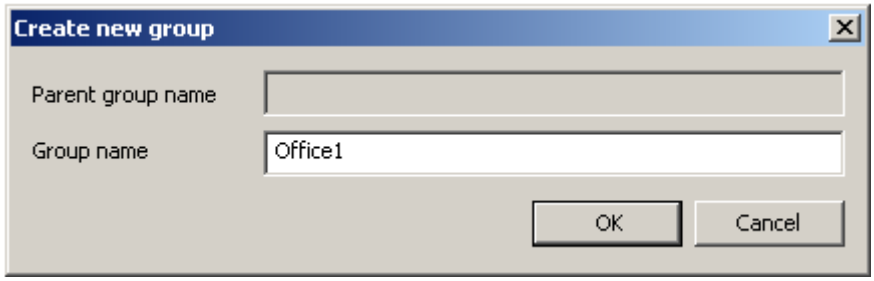

Рисунок 68

2. В меню ***Clients*** выберите предложение ***Create*** (Рисунок 69).

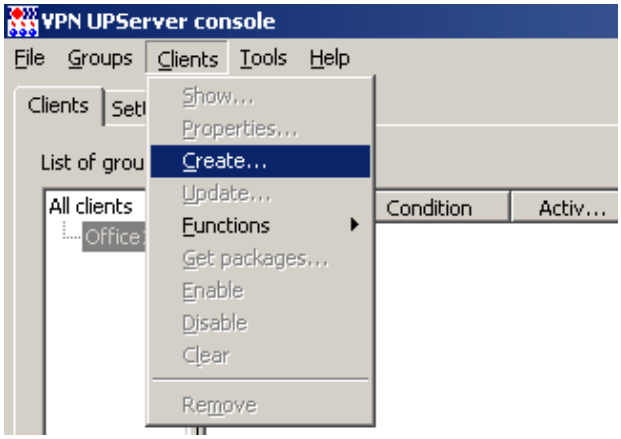

Рисунок 69

3. В окне создания нового клиента **Create new client** введите идентификатор клиента, например, `server01`, а в поле **Product package** нажмите кнопку E (Рисунок 70).

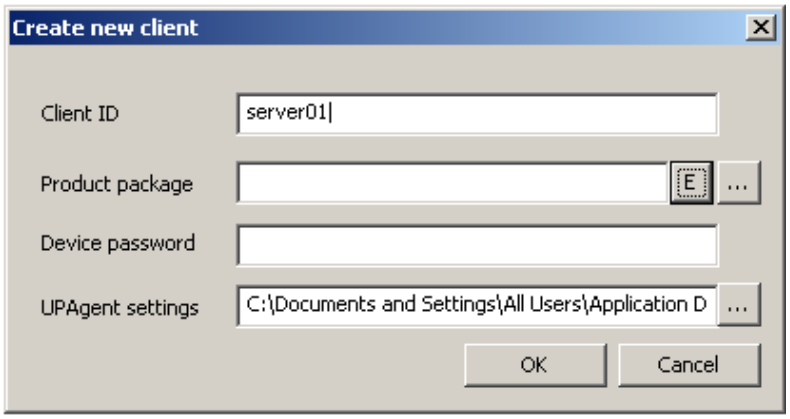

Рисунок 70

4. В окне **VPN data maker** (Рисунок 71) задайте политику безопасности и все настройки продукта, например, CSP VPN Server 3.1, выбрав его в поле **VPN product**, а в поле **Crypto provider** – CryptoPro. Политику и настройки можно ввести во вкладки или загрузить из файла, а можно воспользоваться окнами мастера, нажав кнопку Run Wizard…

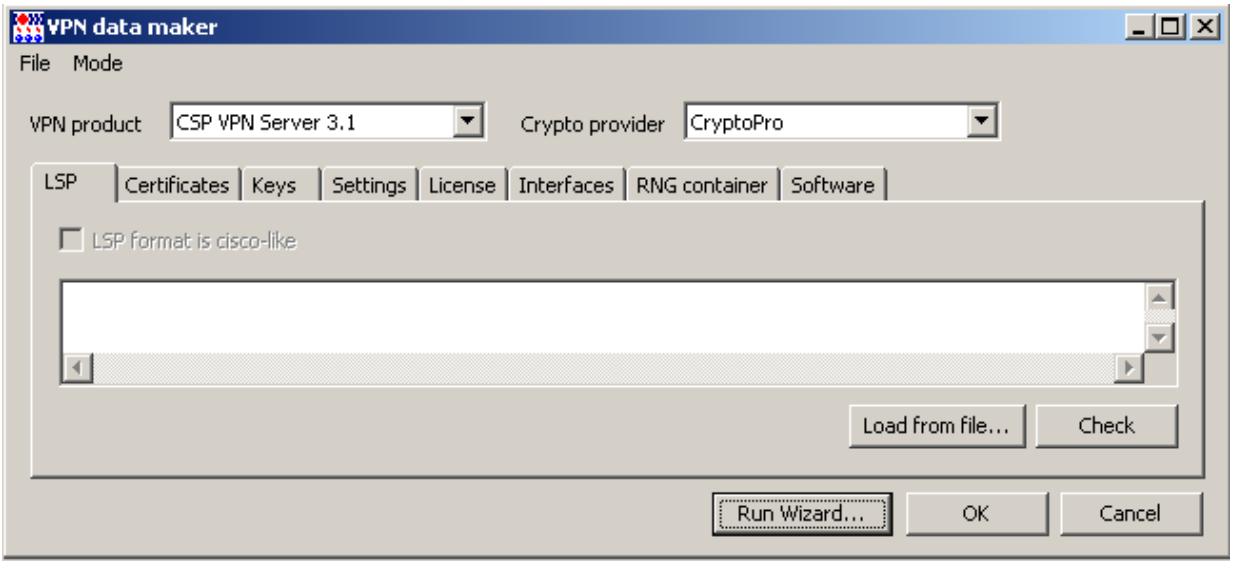

Рисунок 71

5. Выберите метод аутентификации такой же как и у партнера - шлюза CSP VPN Gate, введите такое же значение ключа (Рисунок 72).

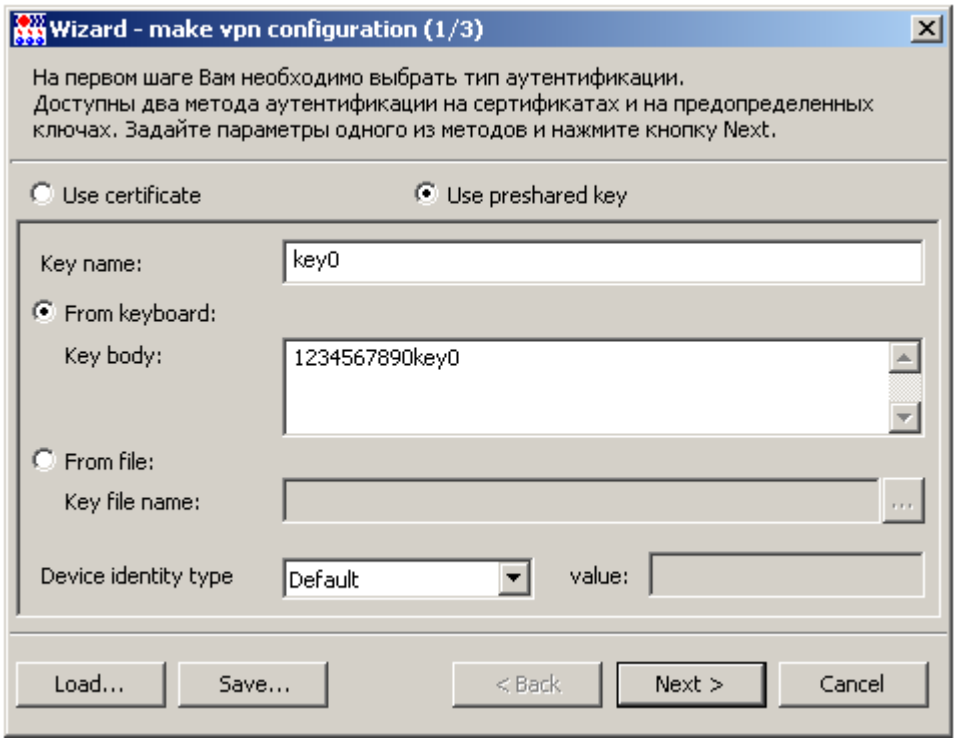

Рисунок 72

6. В следующем окне задайте правило для создания соединения с Сервером управления, при этом соединение с центральным шлюзом должно быть защищенным, для этого нажмите кнопку Add (Рисунок 73).

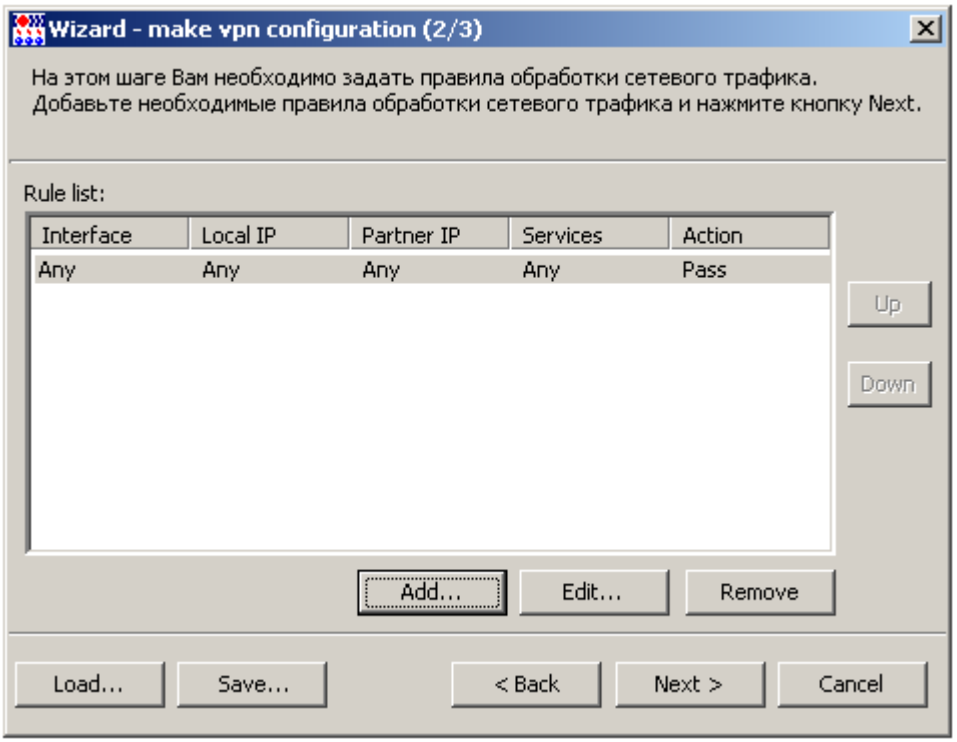

Рисунок 73

7. В поле **Network interface alias** (Рисунок 74) 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 IPsec-партнера задайте адрес интерфейса шлюза 40.0.0.1, защищающего подсеть с Сервером управления. Нажмите кнопку OK.

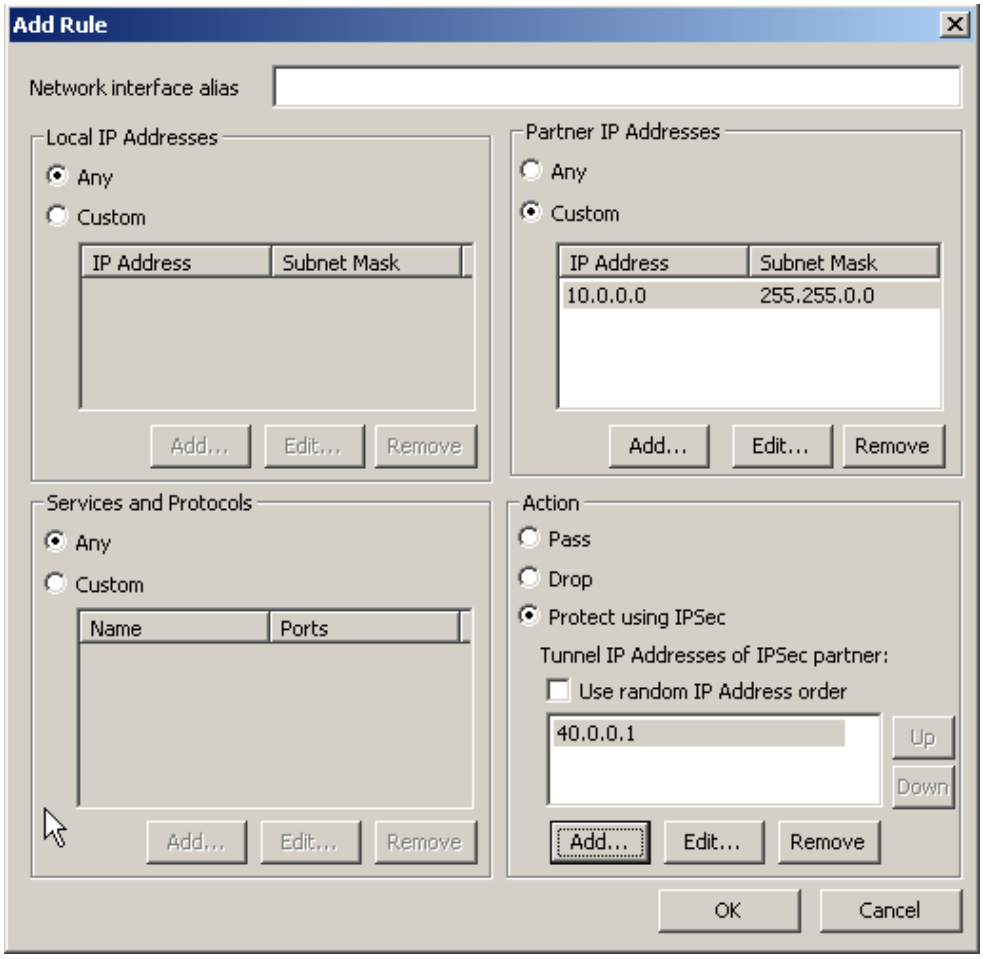

Рисунок 74

8. Увеличьте приоритет созданного правила, используя кнопку Up (Рисунок 75), затем нажмите Next.

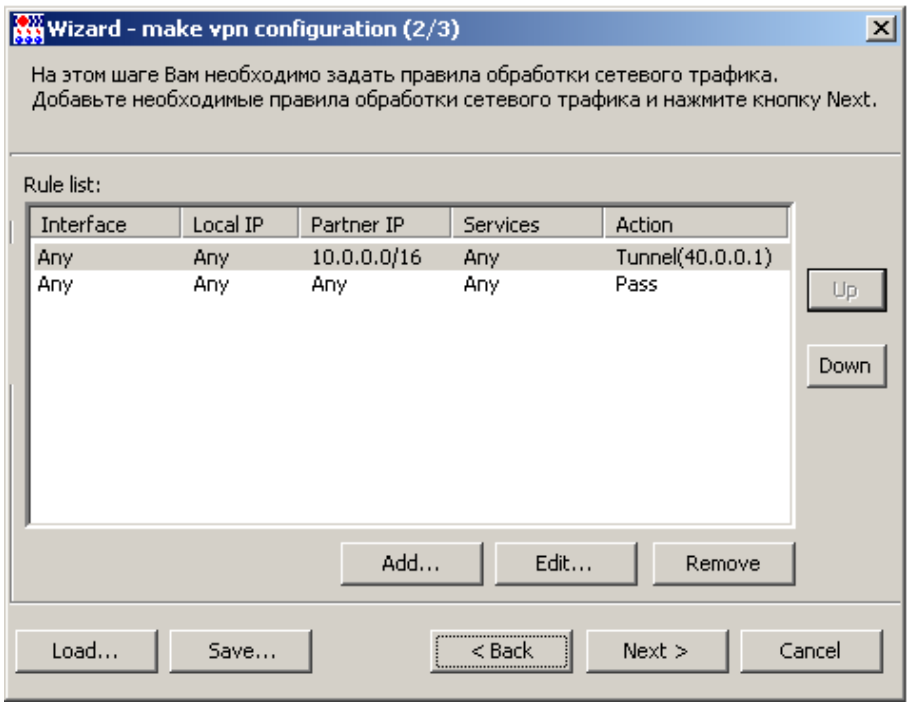

Рисунок 75

9. Введите данные лицензии на продукт CSP VPN Server 3.1 (Рисунок 76).

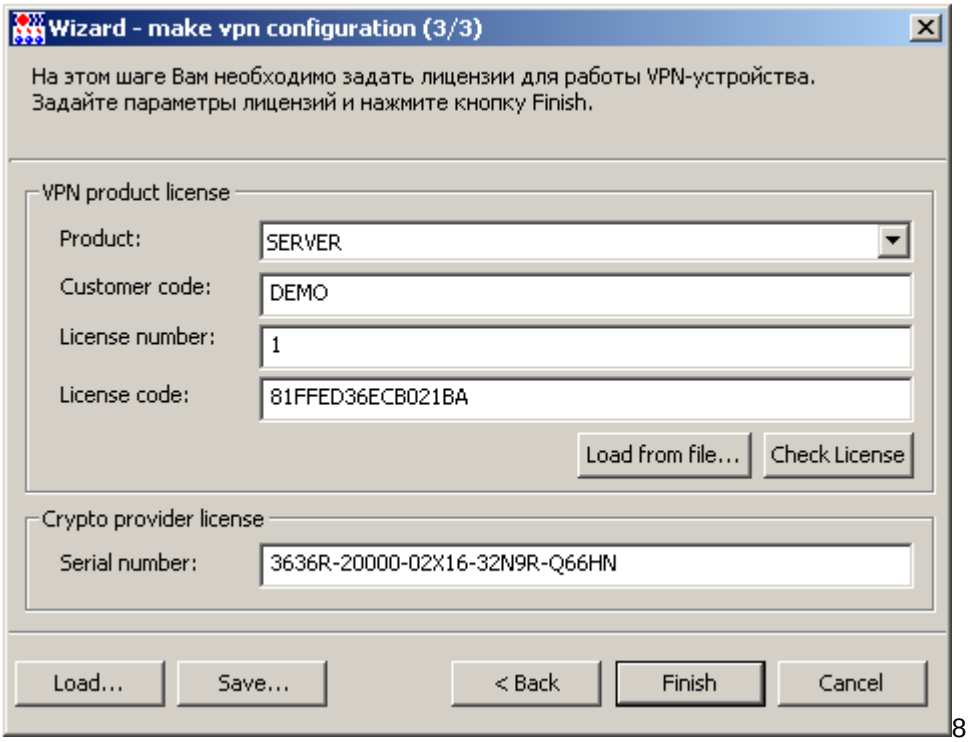

Рисунок 76

10. Сохраните все введенные данные, нажав кнопку Save…, и укажите имя файла-проекта в любом созданном вами каталоге (Рисунок 77).

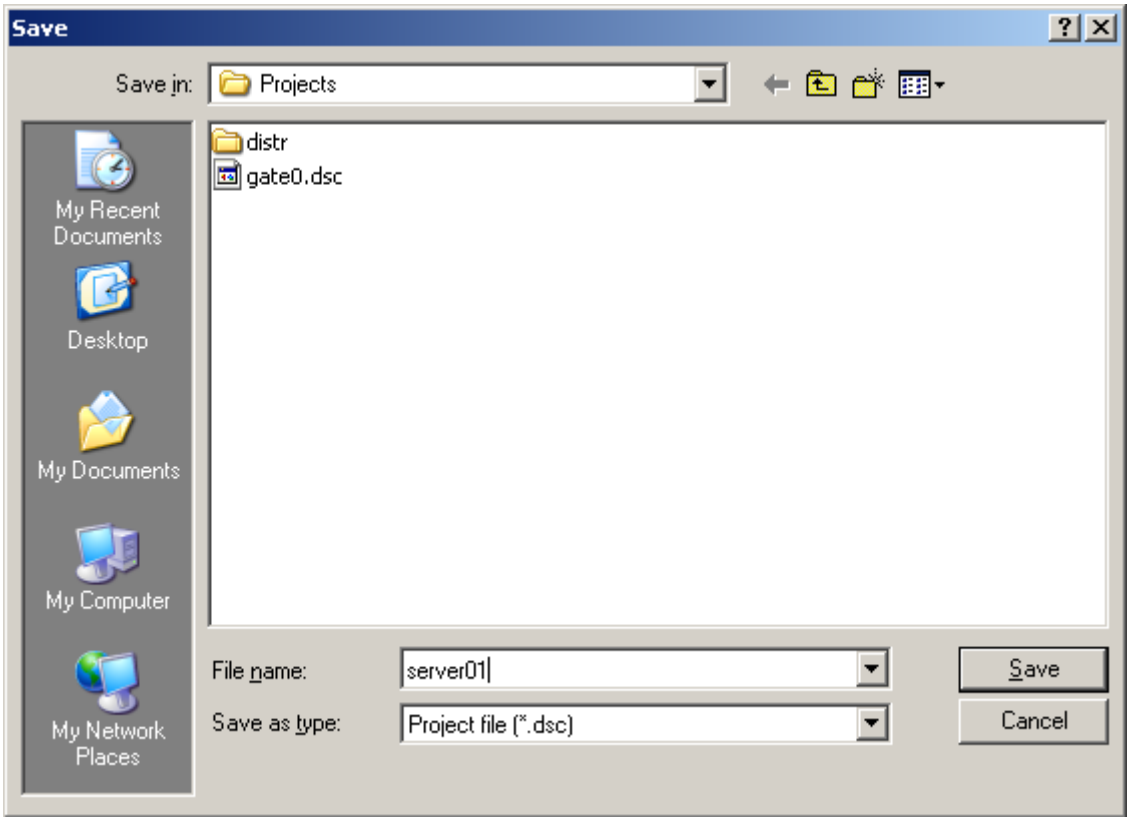

Рисунок 77

11. В окне мастера нажмите кнопку Finish (Рисунок 76). Все введенные данные будут отражены во вкладках проекта (Рисунок 78). Нажмите кнопку OK.

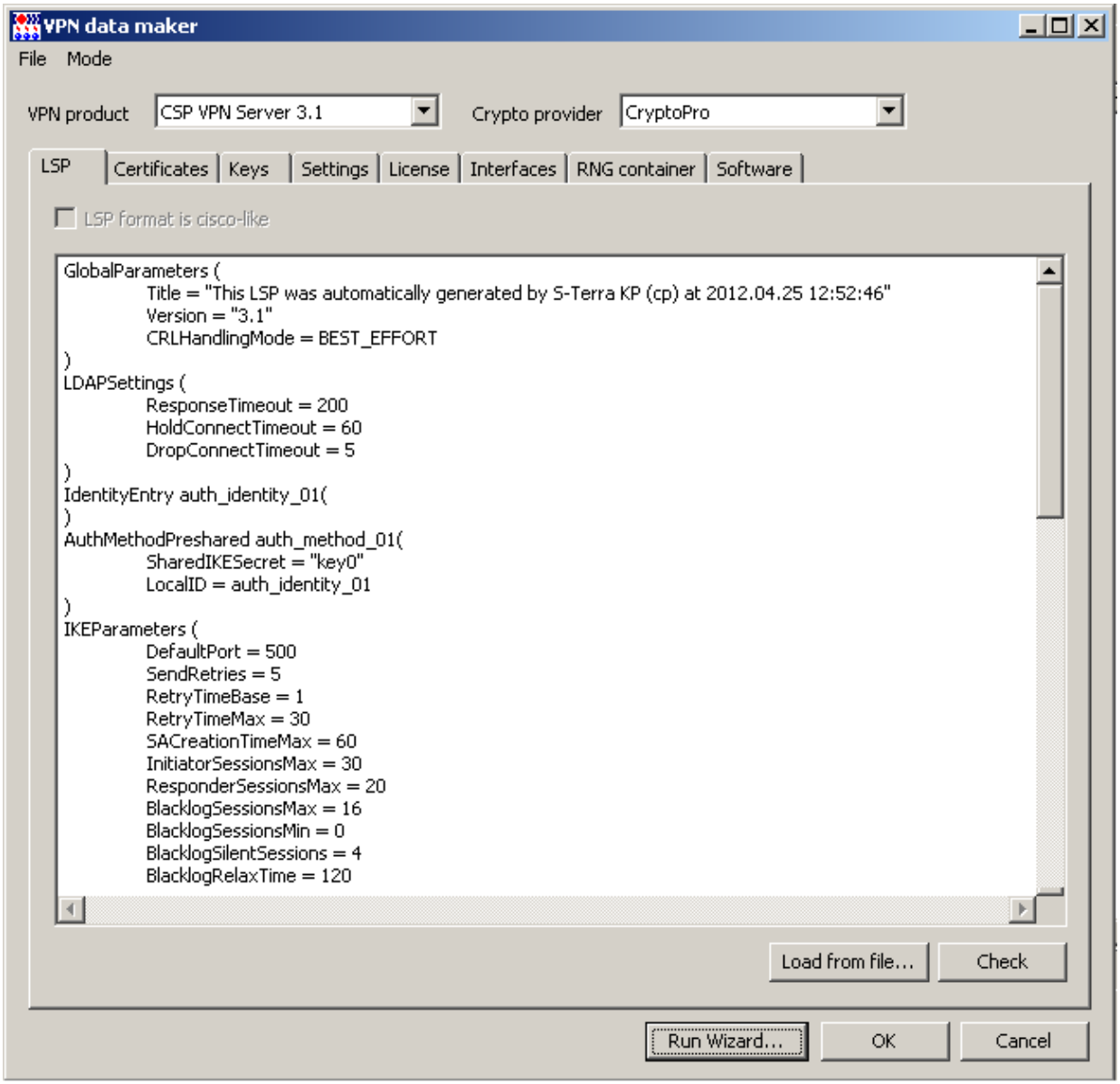

Рисунок 78

12. В окне создания нового клиента server01 также нажмите OK (Рисунок 79).

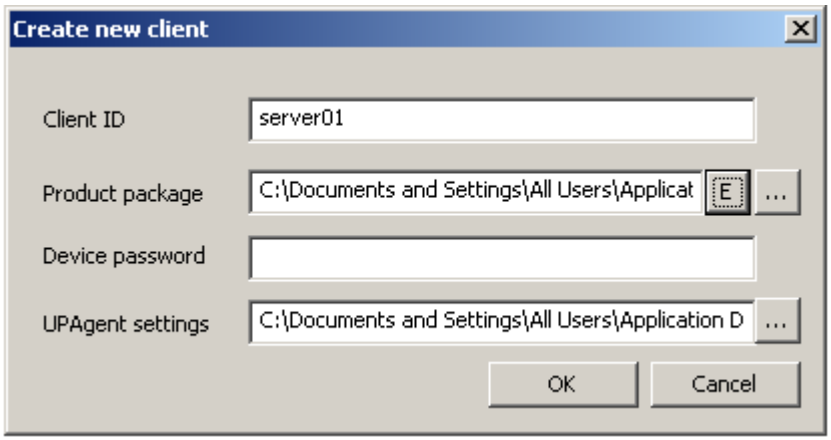

Рисунок 79

13. Созданного клиента переведите в активное состояние, выбрав в контекстном меню предложение ***Enable*** (Рисунок 80). 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**.

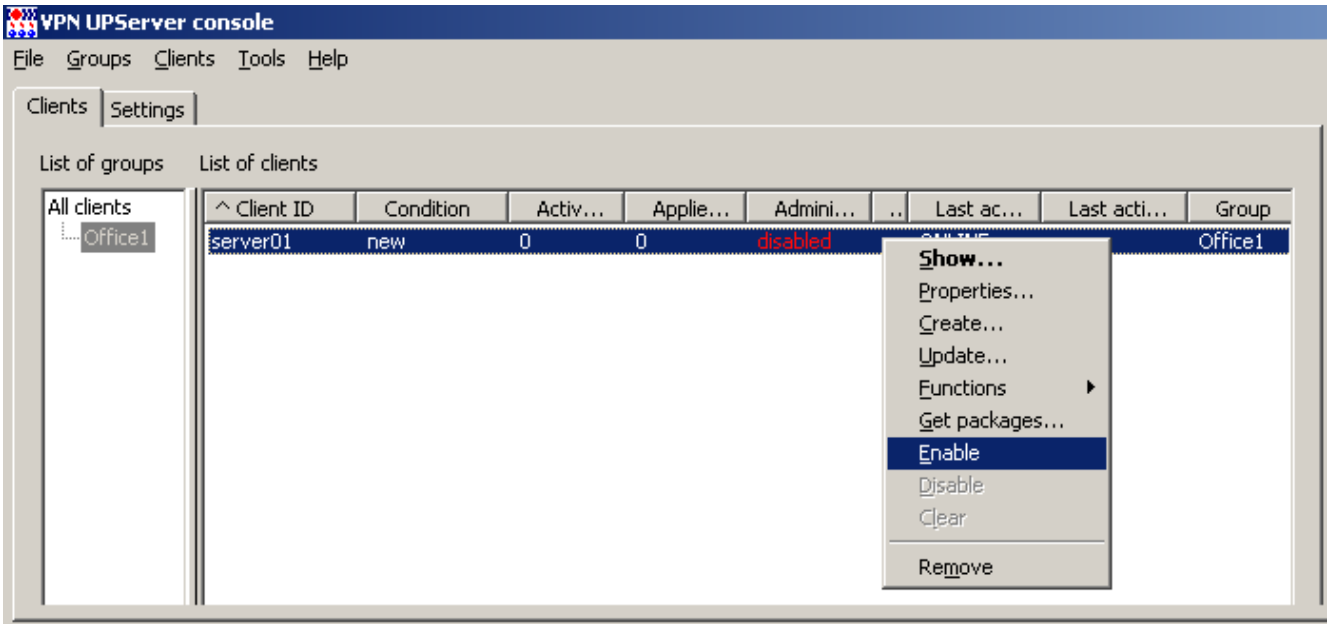

Рисунок 80

6.2. Создание дистрибутивов Клиента управления и CSP VPN Server/CSP VPN Client

1. Для создания дистрибутивов Клиента управления и CSP VPN Server для клиента server01 выберите предложение ***Get packages*** (Рисунок 81).

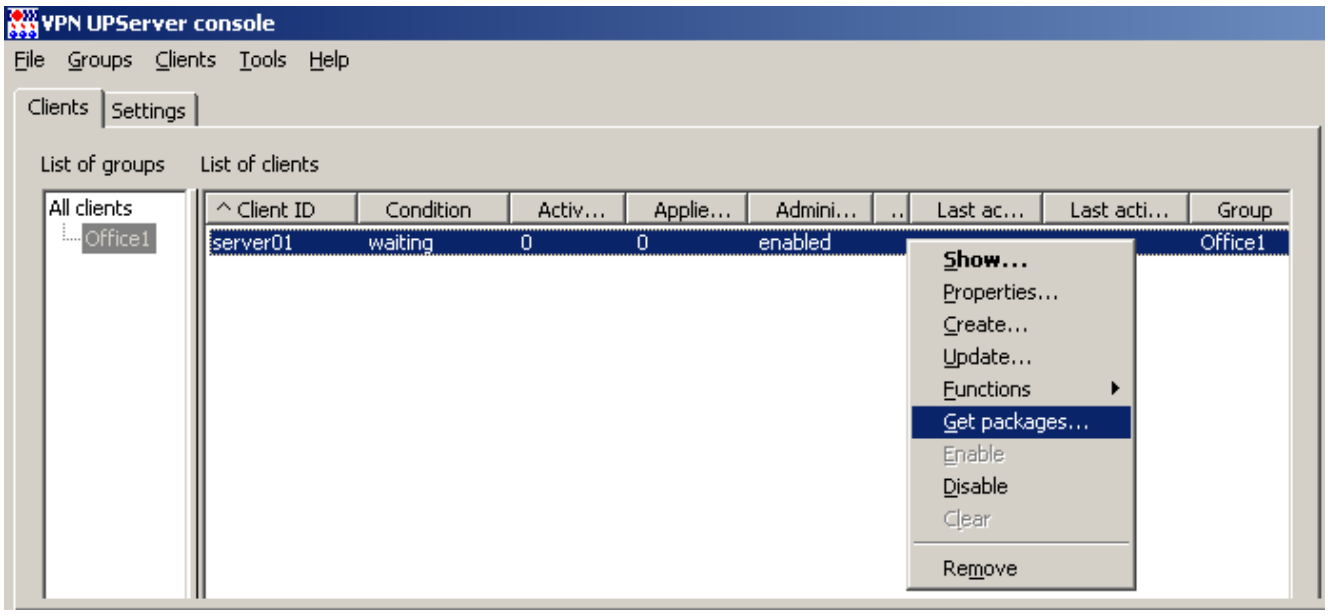

Рисунок 81

2. Укажите каталог для сохранения дистрибутивов (Рисунок 82) и нажмите OK.

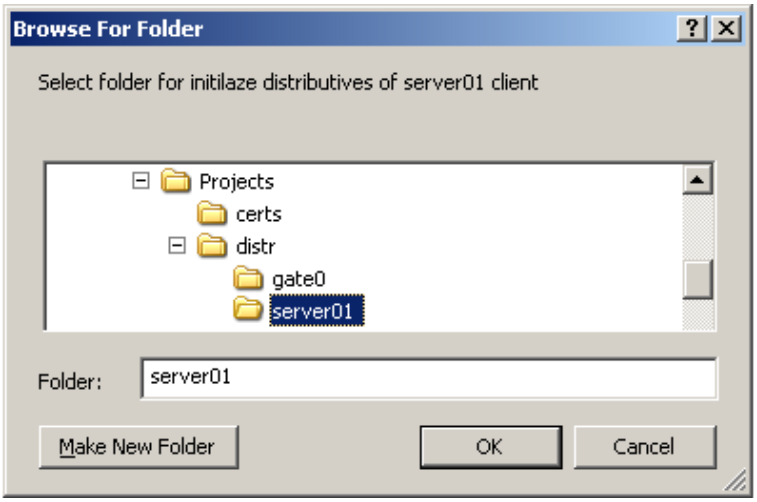

Рисунок 82

3. В указанный каталог будут сохранены два файла (Рисунок 83):

   `setup_product.exe` – дистрибутив продукта CSP VPN Server

   `setup_upagent.exe` – дистрибутив продукта VPN UPAgent (Клиент управления).

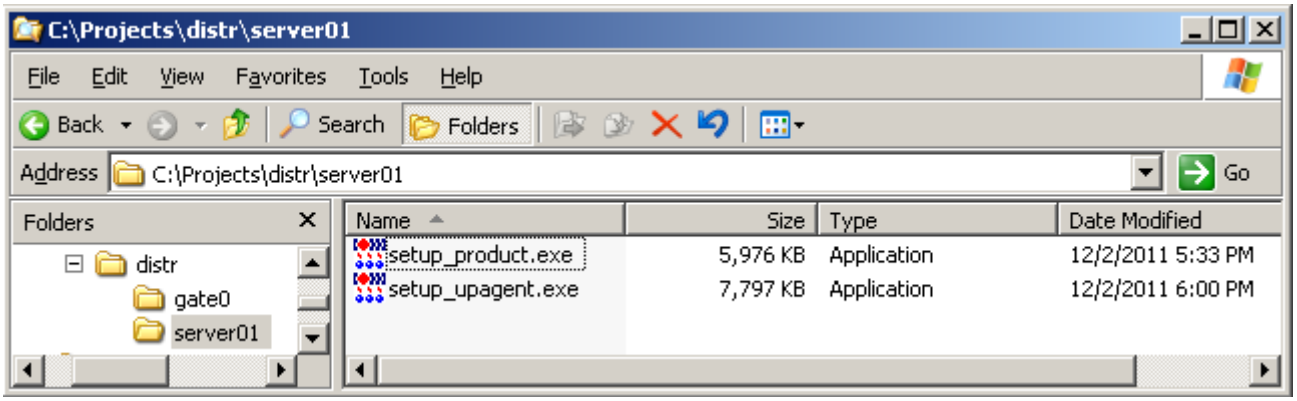

Рисунок 83

6.3. Инсталляция Клиента управления и CSP VPN Server/CSP VPN Client

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

сначала `setup_product.exe`

затем `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 CSP VPN Server/CSP VPN Client описан в документе («Сервер безопасности CSP VPN Server. Версия 3.1. Руководство администратора»/«Клиент безопасности CSP VPN Client. Версия 3.1. Руководство администратора»).
2. Инсталляция Клиента управления (продукт VPN Upagent) запускается программой `setup_upagent.exe`. В появившемся окне (Рисунок 84) нажмите кнопку Да.

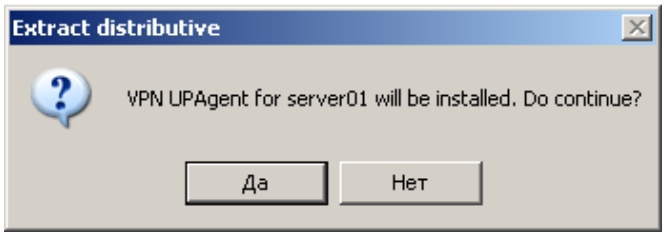

Рисунок 84

Для продолжения инсталляциии нажмите кнопку Next.

Рисунок 85

Выберите каталог для инсталляции Клиента управления (Рисунок 86).

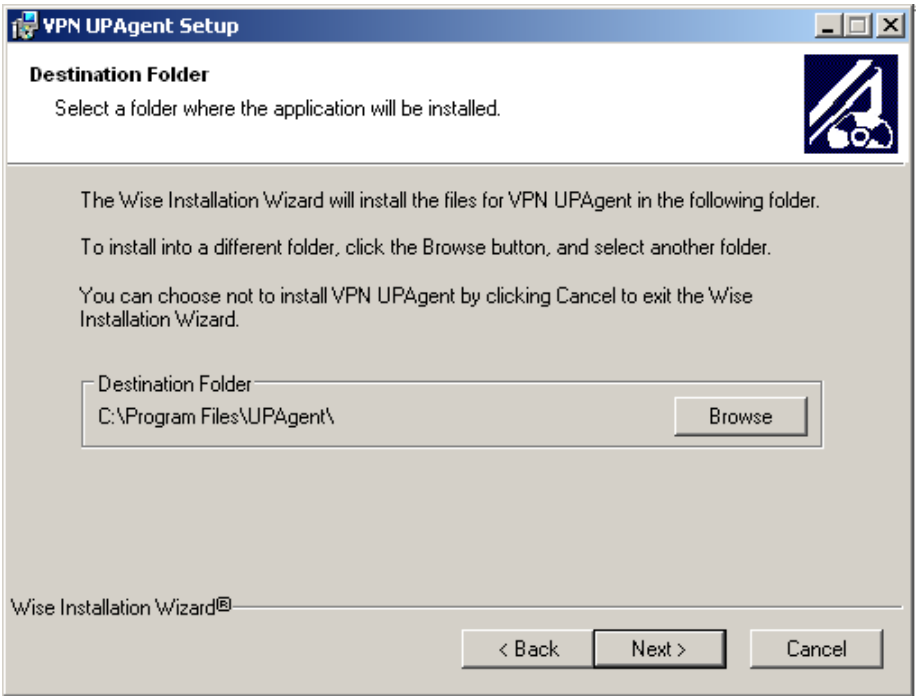

Рисунок 86

В следующем окне подтвердите готовность к установке и нажмите кнопку Next.

По завершению инсталляции нажмите кнопку Finish (Рисунок 87).

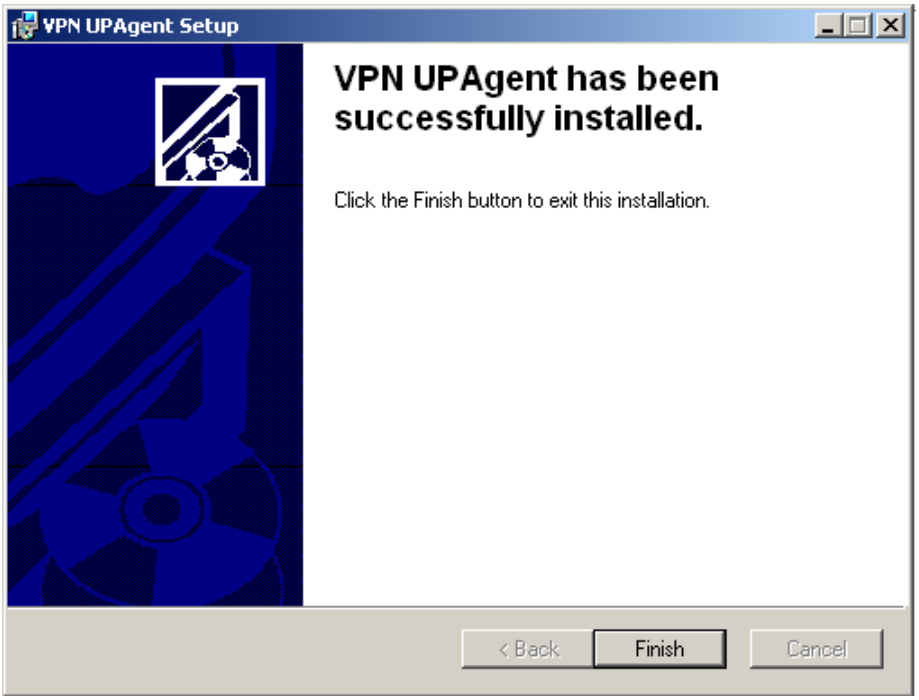

Рисунок 87

3. По завершению установки Клиент управления попытается установить связь с Сервером управления. Этот процесс можно наблюдать в консоли управления продуктом FileZilla Server на Сервере управления (Рисунок 88).

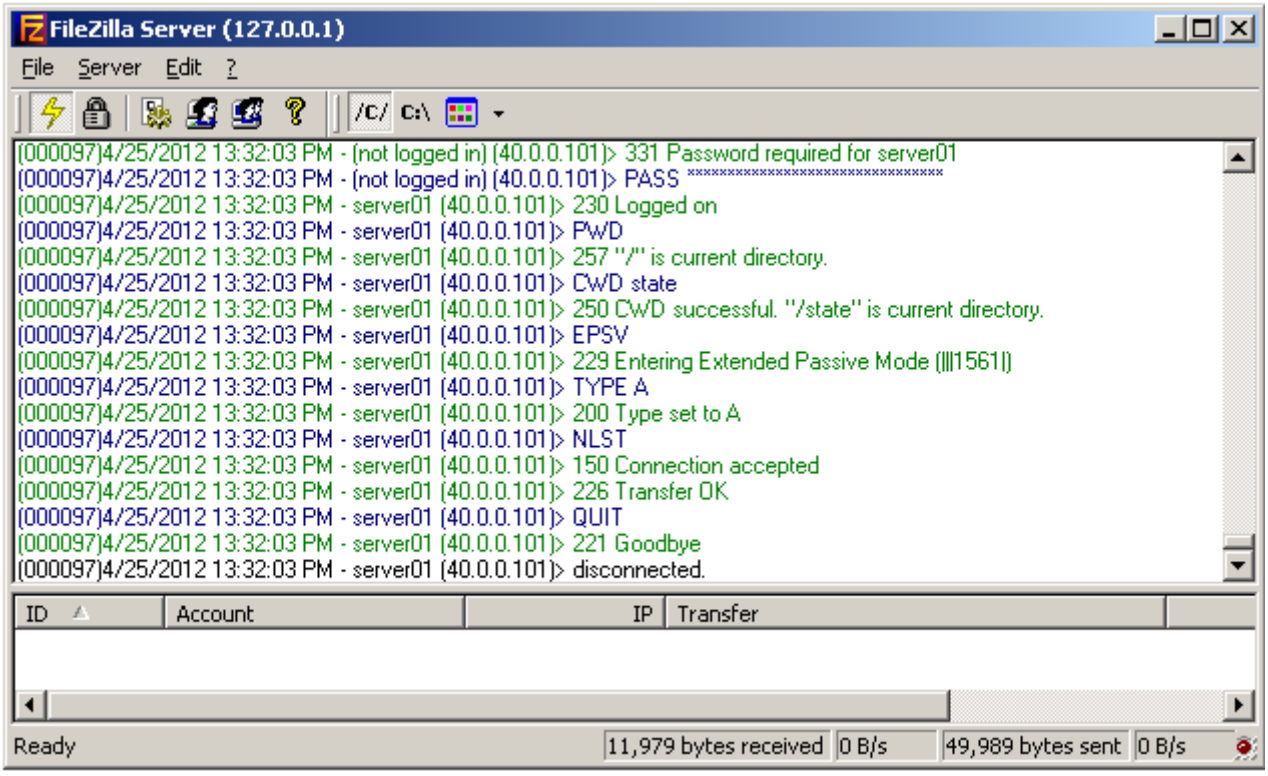

Рисунок 88

4. 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 89).

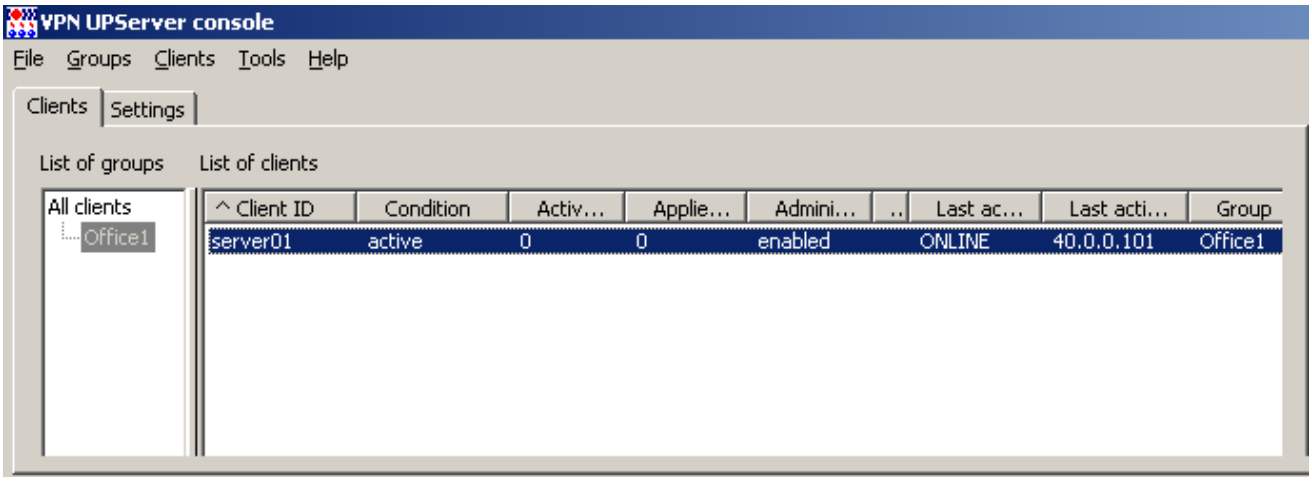

Рисунок 89

7. Сценарий перехода на аутентификацию с использованием сертификатов

Предположим, что на управляемом устройстве установлен Клиент управления, продукты CSP VPN Server и КриптоПро CSP 3.6. На центральном шлюзе также установлен Клиент управления и продукт CSP VPN Gate с криптографией КриптоПро CSP 3.6. 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 создастся 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 CA и локальный сертификат для клиента
4. на Сервере управления подготовьте обновление, включающее новый локальный сертификат, CA 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. Настройка ДСЧ на клиенте с ОС Windows (КриптоПро CSP)

Для возможности использовать «Исходный материал», на управляемом устройстве запустите КриптоПро CSP 3.6 (Рисунок 90), во вкладке **Оборудование** нажмите кнопку Настроить ДСЧ. В открывшемся окне предложение «КриптоПро Исходный Материал» переместите в верхнюю строку, как первый датчик случайных чисел и нажмите кнопку ОК. Если такого ДСЧ нет – добавьте его.

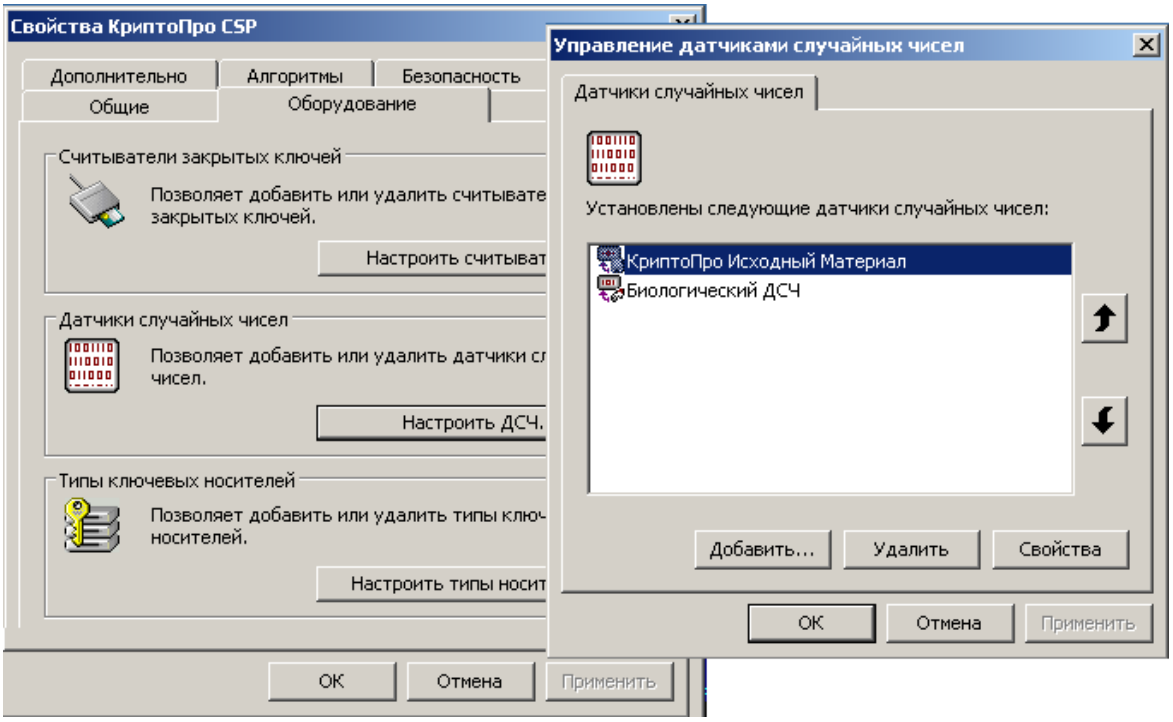

Рисунок 90

7.2. Настройка ДСЧ на клиенте с CSP VPN Gate (КриптоПро CSP)

На шлюзе безопасности, использующем СКЗИ «КриптоПро CSP 3.6» класса КС1, настройка ДСЧ, называемого «КриптоПро Исходный Материал», осуществляется автоматически при инсталляции Клиента управления локально (скрипт `setup_upagent.sh` вызывает другой скрипт `/packages/VPNUPAgent/install.sh`):

```
/opt/cprocsp/sbin/ia32/cpconfig -hardware rndm -add cpsd -name 'CPSD RNG' -
level 1
/opt/cprocsp/sbin/ia32/cpconfig -hardware rndm -configure cpsd -add string
/db1/kis_1 /var/opt/cprocsp/dsrf/db1/kis_1
/opt/cprocsp/sbin/ia32/cpconfig
```

При использовании «КриптоПро CSP 3.6» класса КС2 дополнительно автоматически выполняются команды:

```
touch /var/opt/cprocsp/dsrf/db1/kis_1
touch /var/opt/cprocsp/dsrf/db2/kis_1

/etc/init.d/vpngate stop
/etc/init.d/cprocsp restart
/etc/init.d/vpngate start
```

Последние 3 команды приведут к разрыву защищенных соединений, поэтому инсталляцию Клиента управления надо выполнять локально, а не удаленно и эти команды можно заменить перезагрузкой шлюза.

7.3. Настройка ДСЧ на клиенте с CSP VPN Gate (S-Terra)

На шлюзе безопасности, использующем СКЗИ «S-Terra», автоматически добавляется в файл `/etc/S-Terra/skzi.conf` описание источника случайных чисел из внешней гаммы:

```
RNG=/opt/VPNagent/lib/libConsBioRNG.so,/opt/VPNagent/lib/libExtGammaRNG.so
ExtGammaPath=/var/s-terra/gamma
```

7.4. Настройка ДСЧ на клиенте с CSP VPN Server (S-Terra)

На сервере безопасности, использующем СКЗИ «S-Terra» нужно добавить в файл `C:\Program Files\S-Terra Server\skzi.conf` описание источника случайных чисел из внешней гаммы (добавляемая часть выделена жирным шрифтом):

```
RNG=C:\Program Files\S-Terra Server\ConsBioRNG.dll,C:\Program Files\S-Terra
Server\ExtGammaRNG.dll
ExtGammaPath=c:\gamma
```

7.5. Настройка ДСЧ на клиенте с CSP VPN Client (S-Terra)

На клиенте безопасности, использующем СКЗИ «S-Terra» нужно добавить в файл `C:\Program Files\S-Terra Client\skzi.conf` описание источника случайных чисел из внешней гаммы (добавляемая часть выделена жирным шрифтом):

```
RNG=C:\Program Files\S-Terra Client\ConsBioRNG.dll,C:\Program Files\S-Terra
Client\ExtGammaRNG.dll
ExtGammaPath=c:\gamma
```


7.6. Создание обновления с параметрами ключевой пары и запроса на сертификат

1. На управляемом устройстве с ОС Windows в «КриптоПро CSP» должен быть инсталлирован считыватель, например, Реестр.
2. 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 91).

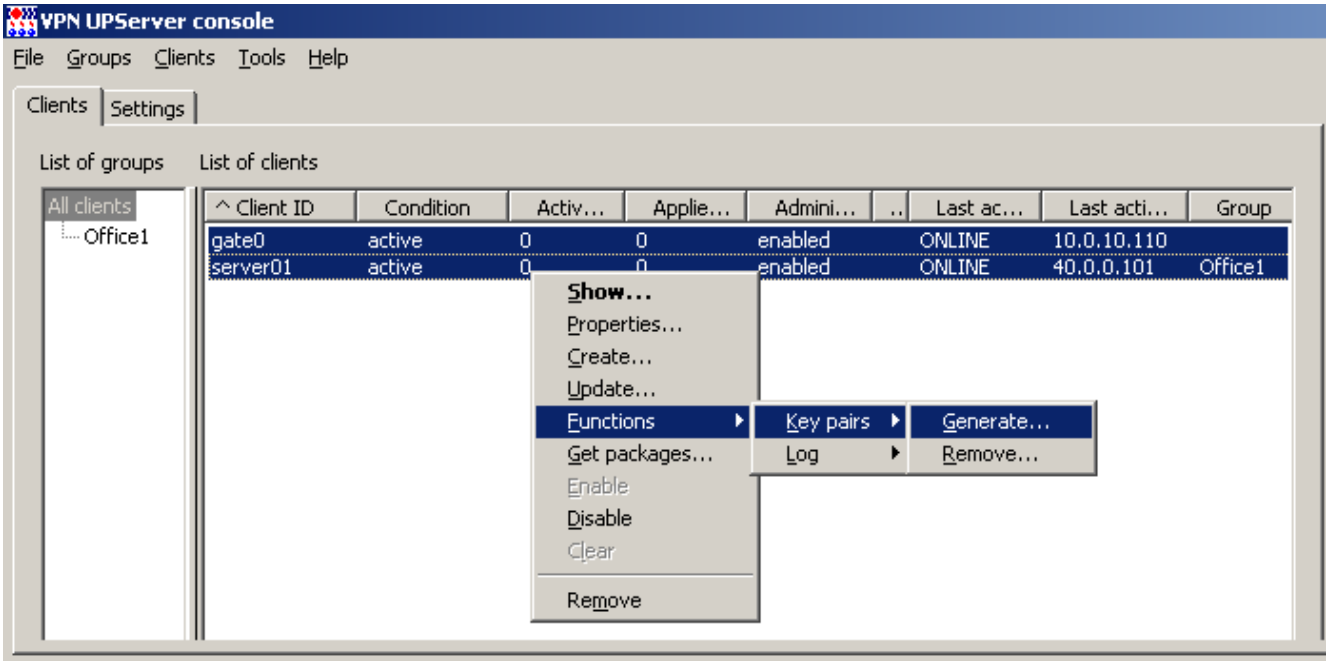

Рисунок 91

3. В открывшемся окне (Рисунок 92) заполните только два поля – задайте пароль на контейнер и его подтверждение, в который будет размещена ключевая пара для локального сертификата.

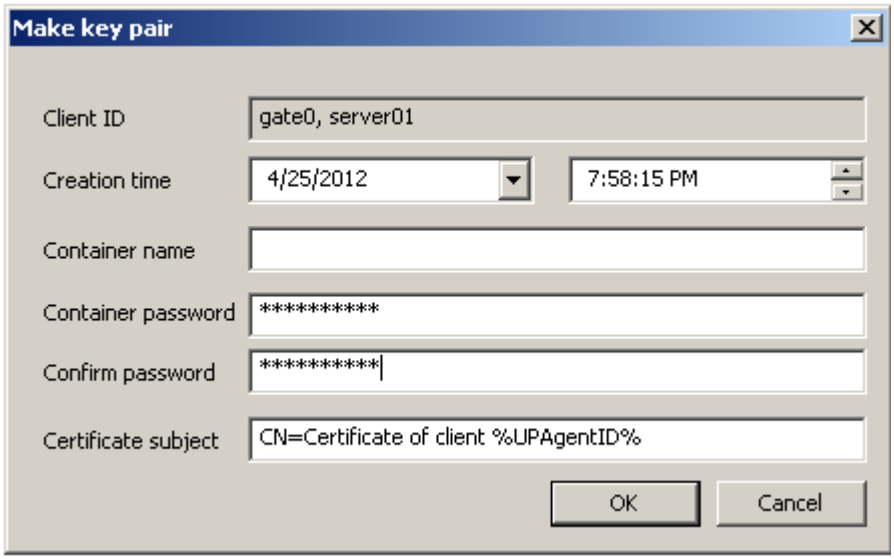

Рисунок 92

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 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 инсталлировано несколько считывателей. Например,

  `\\.\HDIMAGE\HDIMAGE\\cont1`

  `\\.\REGISTRY\cont1` *или* `REGISTRY\\cont2`

  `\\.\FAT12_A\cont3` или `FAT12_A\cont4`

- **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).

4. При нажатии кнопки OK предлагается выполнить «биологическую» инициализацию ДСЧ – понажимайте клавиши или перемещайте указатель мыши (Рисунок 93). Если на Сервере управления установлен аппаратный ДСЧ, то данное окно не выводится.

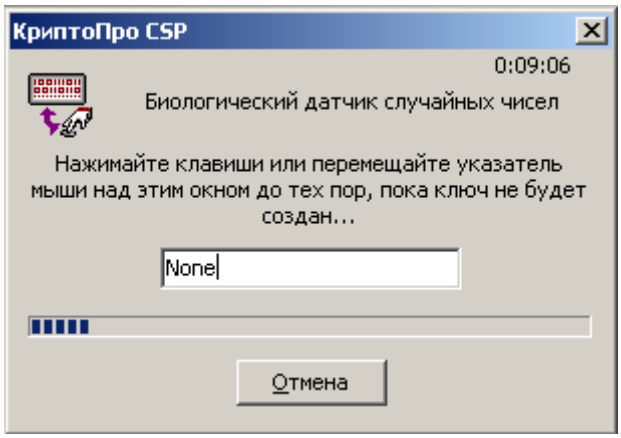

Рисунок 93

5. После этого в таблице появятся новые обновления с параметрами ключевых пар и контейнеров для данных клиентов (Рисунок 94). Количество активных обновлений (столбец Active updates) увеличится на единицу.

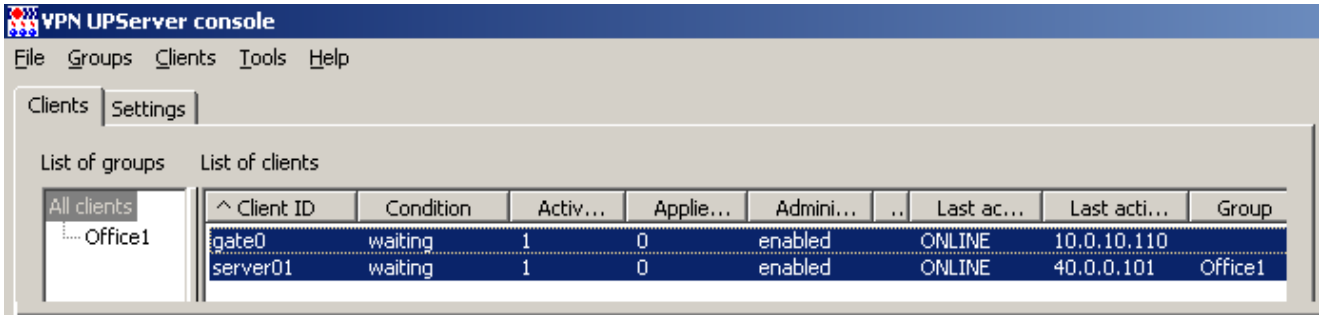

Рисунок 94

6. Через некоторое время обновления будут применены на устройствах, что отразится в таблице на Сервере управления (Рисунок 95). Количество успешных примененных обновлений увеличится на единицу, а количество готовых к скачиванию - уменьшится на единицу.

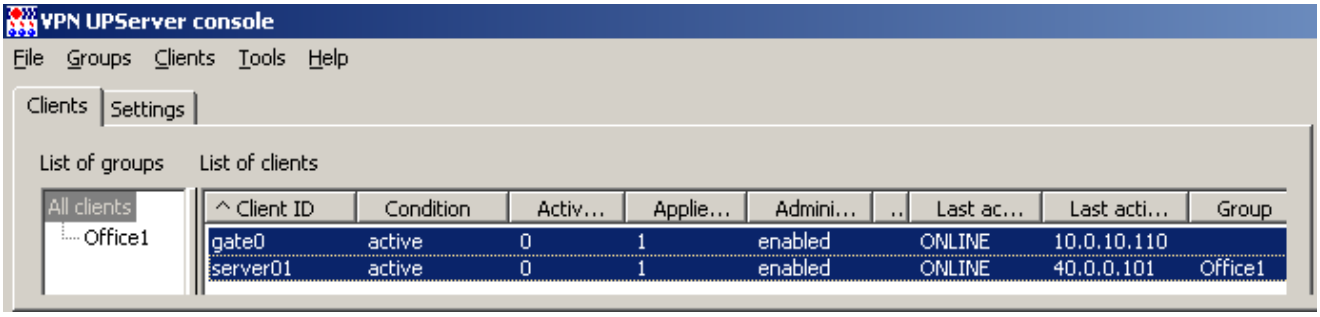

Рисунок 95

7.7. 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 96).

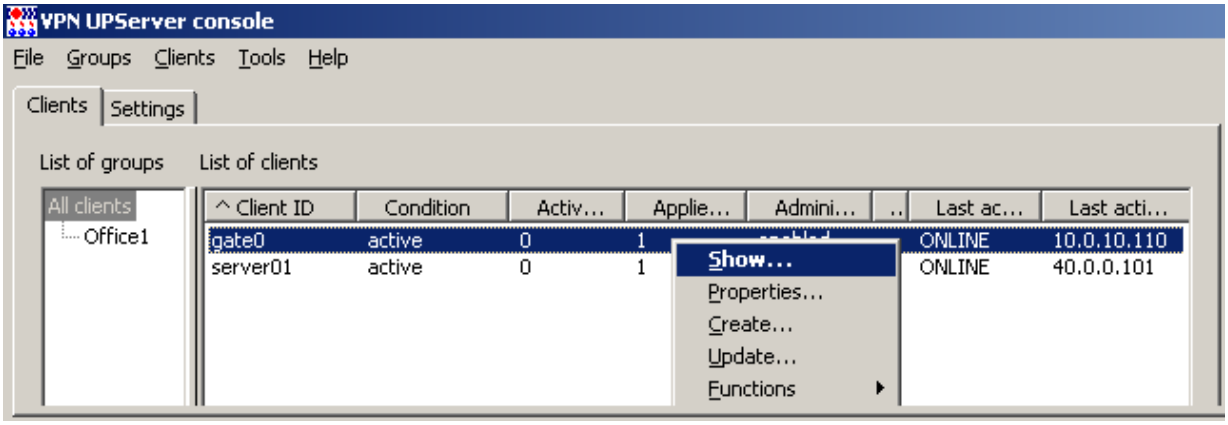

Рисунок 96

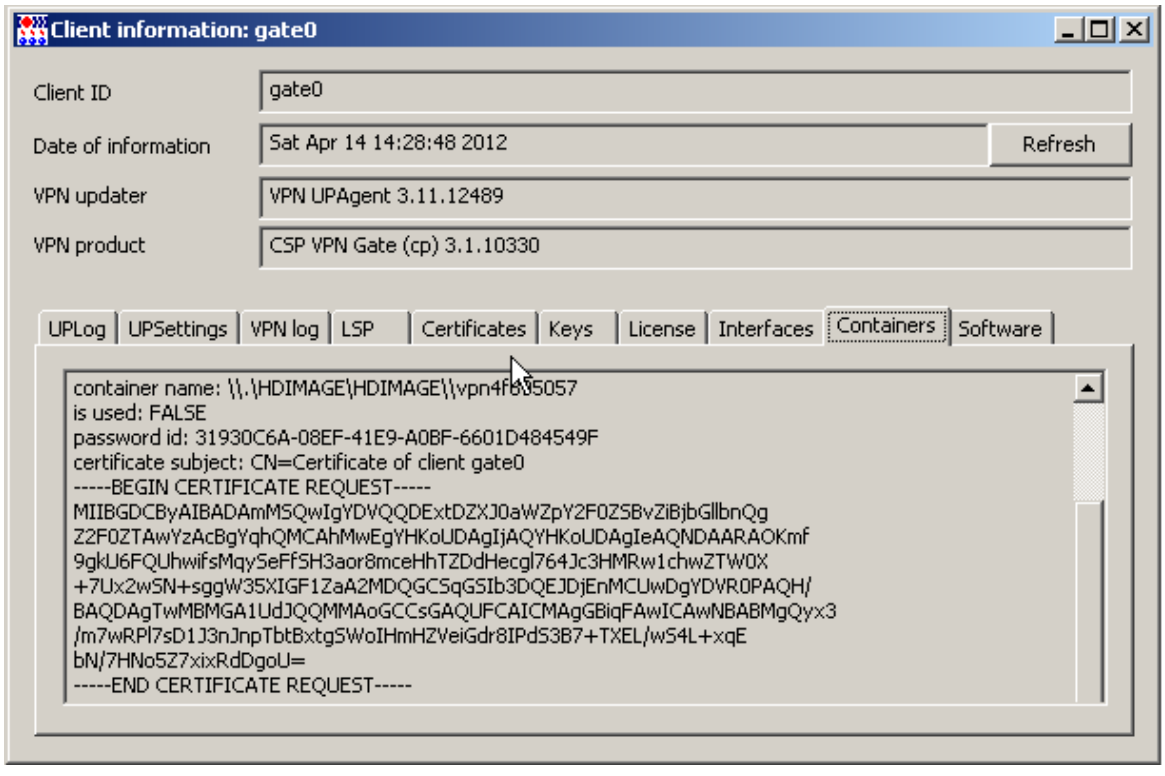

Рисунок 97

Во вкладке **Containers** для `gate0` появилась запись о созданном контейнере (Рисунок 97):

- **container name** – имя созданного контейнера
- **is used: FALSE** – признак того, что контейнер еще не используется продуктом CSP VPN Gate, 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.

Для клиента `server01` контейнер размещен в Registry управляемого устройства (Рисунок 98).

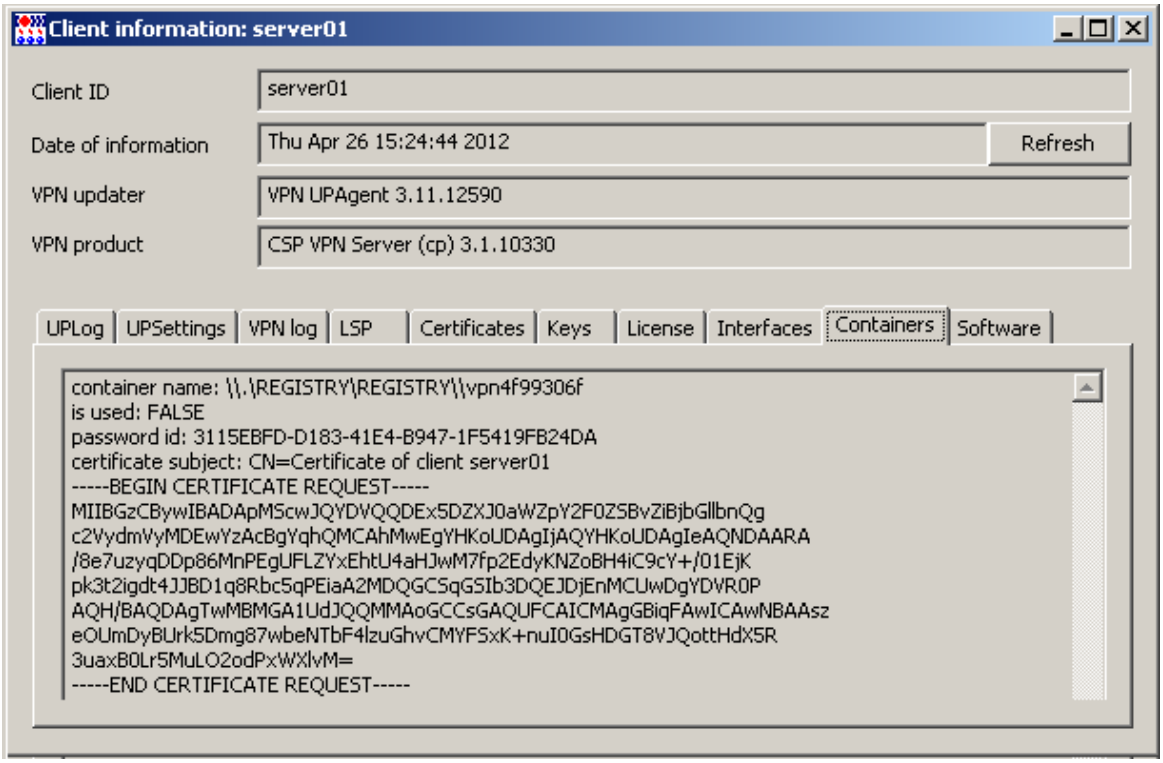

Рисунок 98

7.8. Создание сертификата

Запрос на сертификат скопируйте из вкладки **Containers**, отошлите в Центр сертификации, используя, например, средства Microsoft Windows CA (Рисунок 102).

1. На Сервере управления запустите `Microsoft Internet Explorer`, в поле `Address` укажите адрес Удостоверяющего Центра и утилиту `certsrv (Certificate Service)`.

   Для целей тестирования можно настроить Удостоверяющий Центр на Сервере управления (настройку УЦ см. в документе «Приложение» к Программному комплексу CSP VPN Gate). В этом случае наберите `http://127.0.0.1/certsrv/`.

2. В появившемся окне высвечивается имя Удостоверяющего Центра – в нашем случае S-Terra CA. Выберите предложение `Request a certificate`.

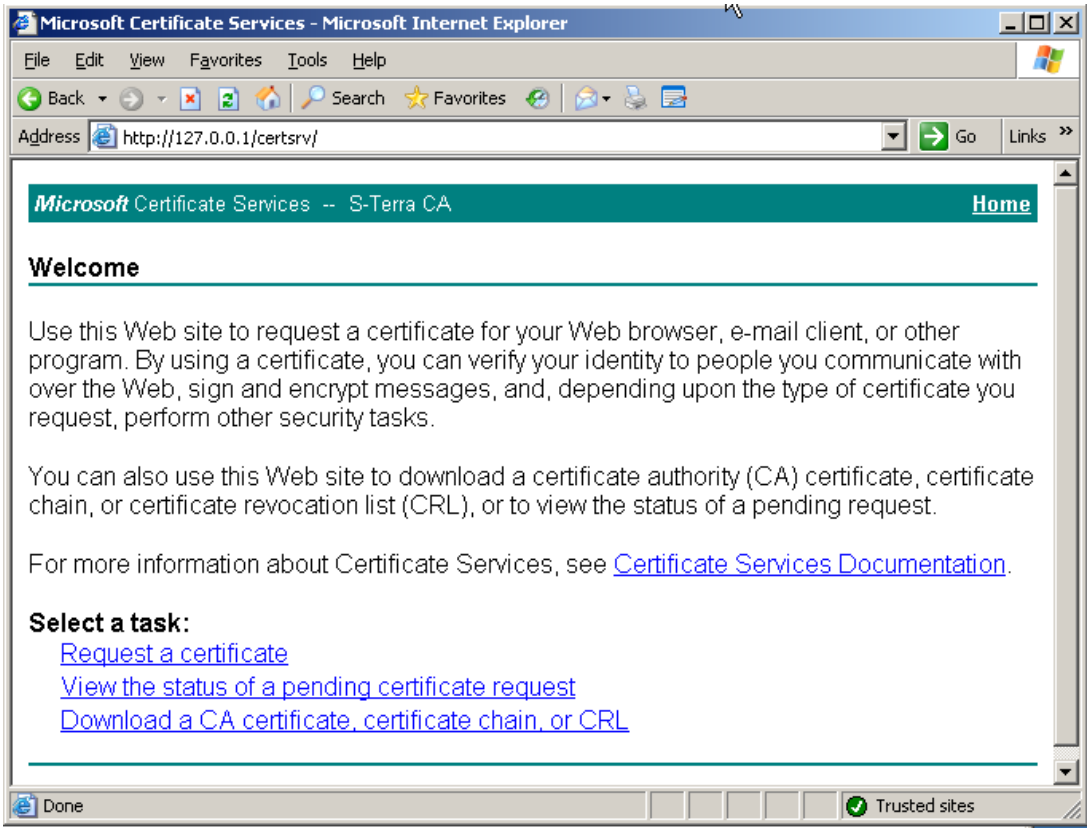

Рисунок 99

3. Далее выберите форму расширенного запроса – предложение "`advanced certificate request`".

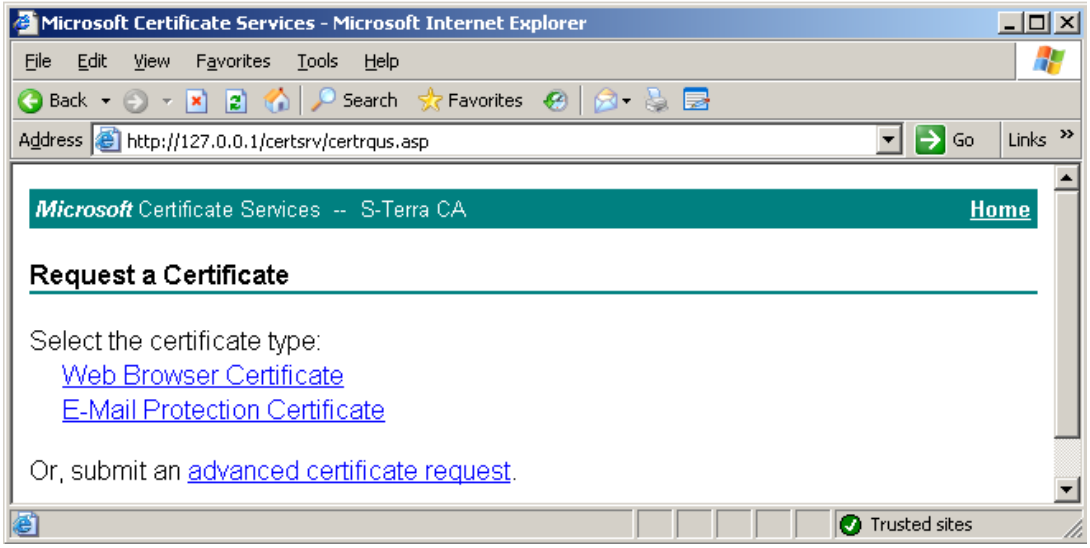

Рисунок 100

4. Чтобы вставить скопированный в буфер запрос выберите предложение "`Submit a certificate request …`".

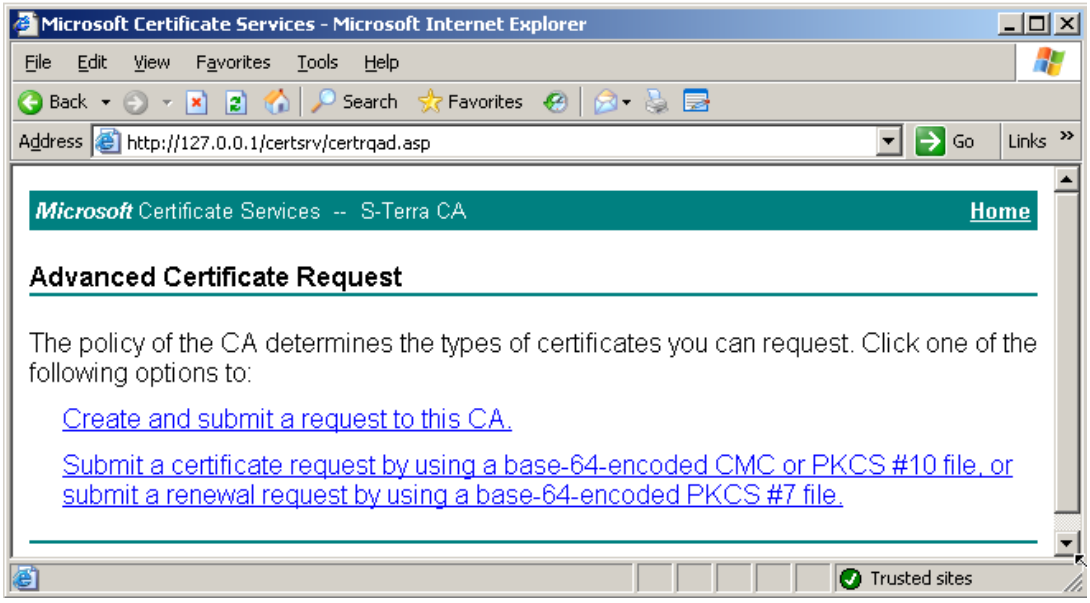

Рисунок 101

5. Вставьте скопированный запрос и нажмите кнопку Submit.

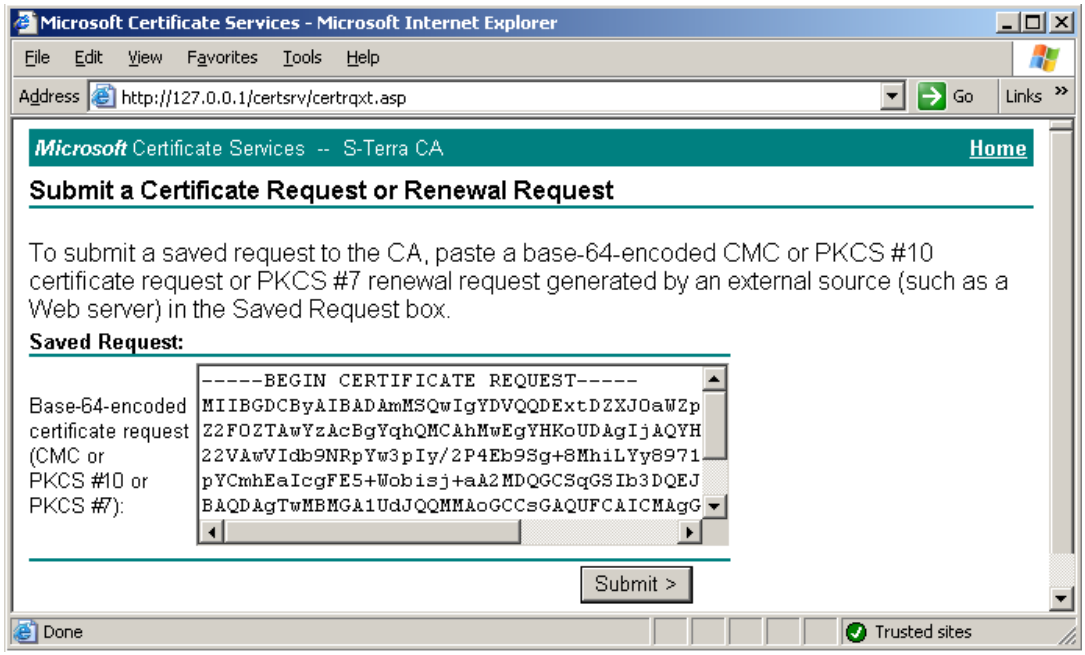

Рисунок 102

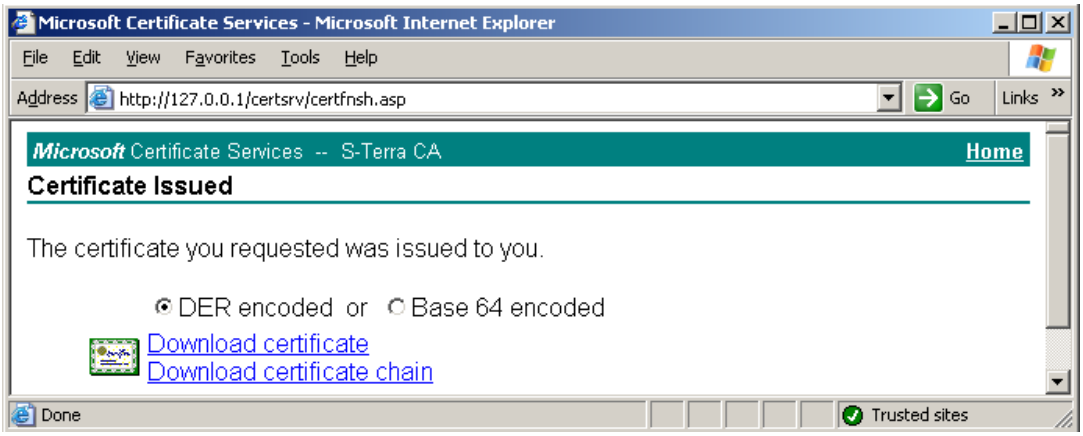

Рисунок 103

6. Выбрав предложение «`Download certificate`», сохраните локальный сертификат для gate0 на Сервере управления. Также сохраните в файл CA сертификат.
7. Также вставьте запрос и для server01 и получите сертификат. Для сохранения локального и CA сертификата в одном файле можно выбрать предложение `Download certificate chain` (Рисунок 103), сохранив в формате PKCS#7.
8. Два созданных локальных сертификата для клиентов gate0 и server01, а также CA сертификат сохранены на Сервере управления (Рисунок 104).

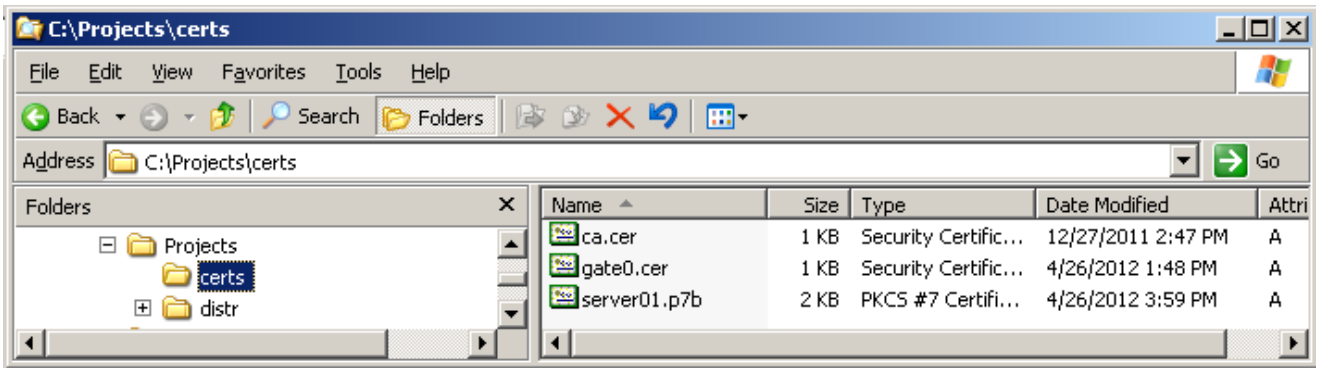

Рисунок 104

7.9. Создание обновления с новым сертификатом для шлюза

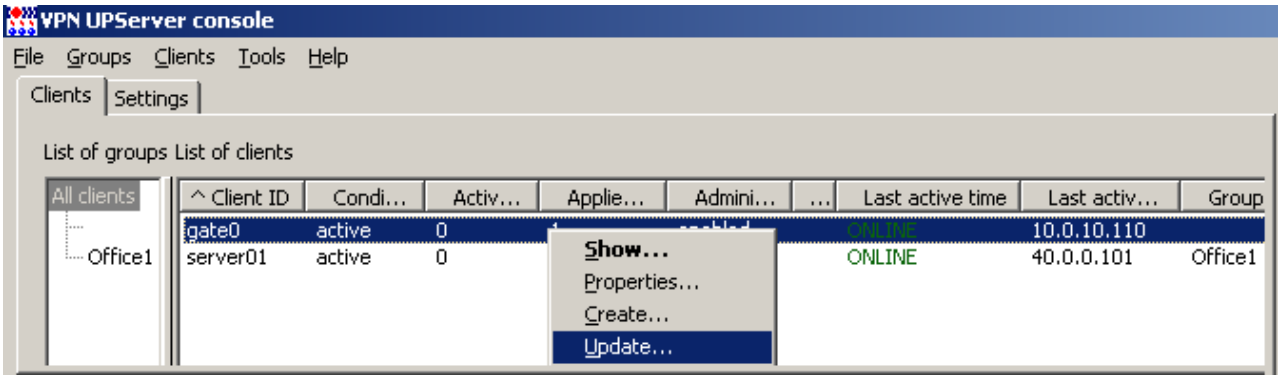

Рисунок 105

1. На Сервере управления в контекстном меню выберите предложение ***Update*** (Рисунок 105).
2. В открывшемся окне **Update client** нажмите кнопку E (Рисунок 106).

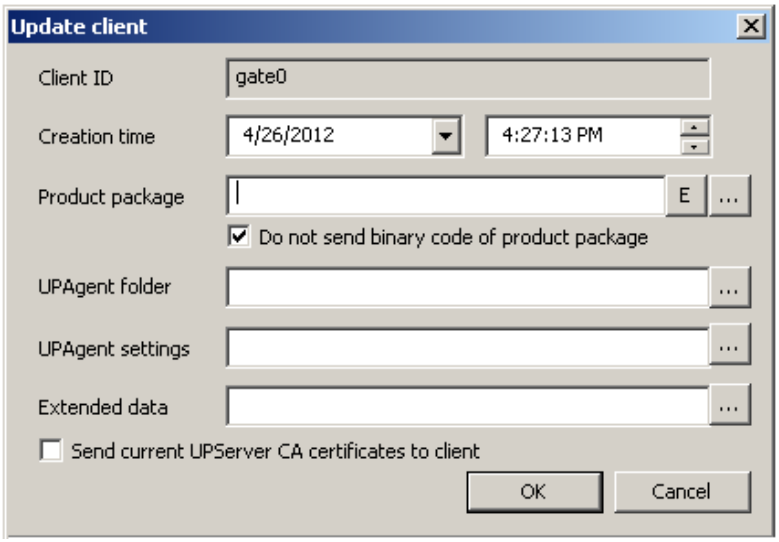

Рисунок 106

3. В окне **VPN data maker** перейдите во вкладку **Certificates** (Рисунок 107) и в области Trusted CA certificates нажмите кнопку Add.

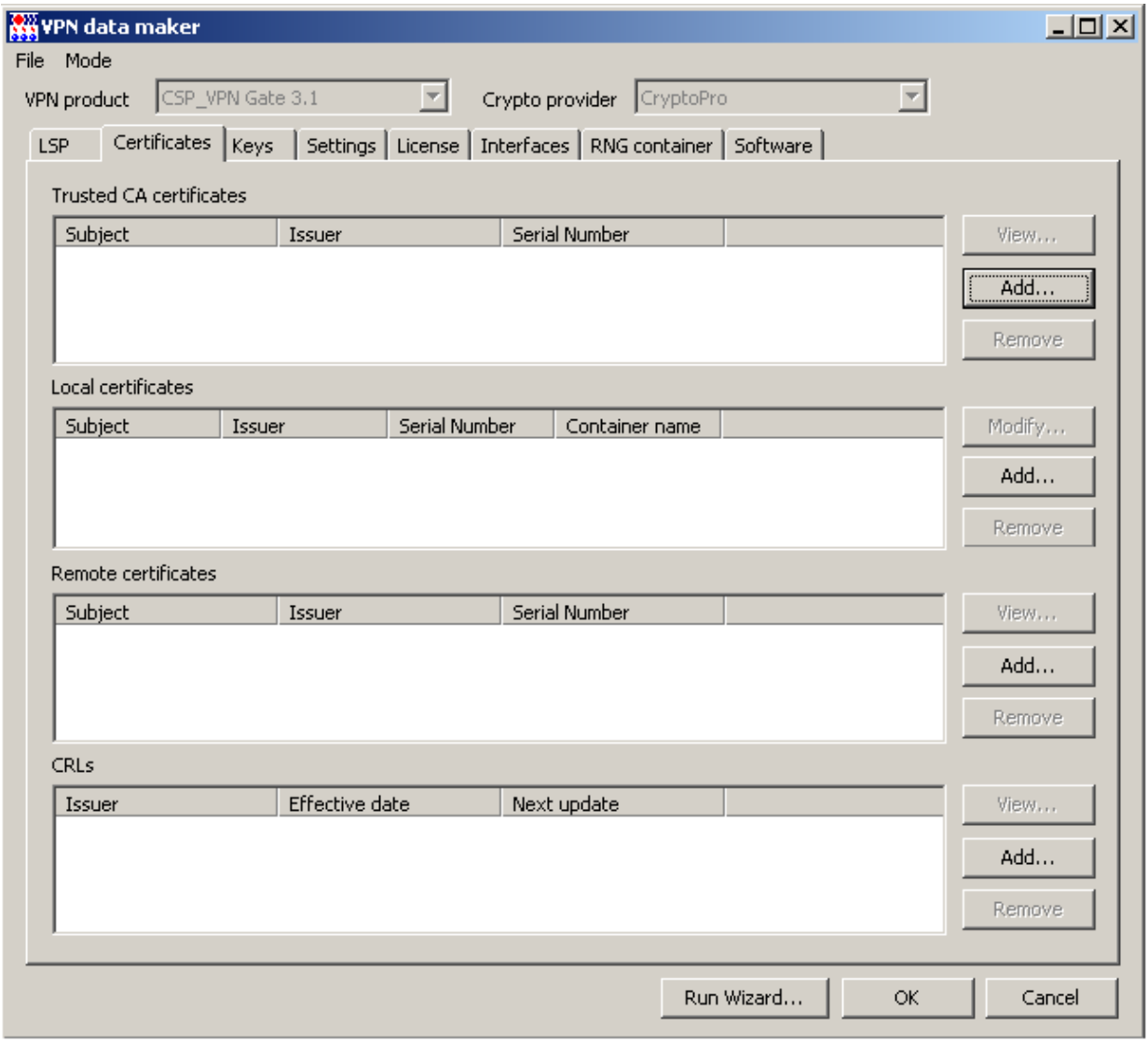

Рисунок 107

4. В открывшемся окне выберите файл с CA сертификатом

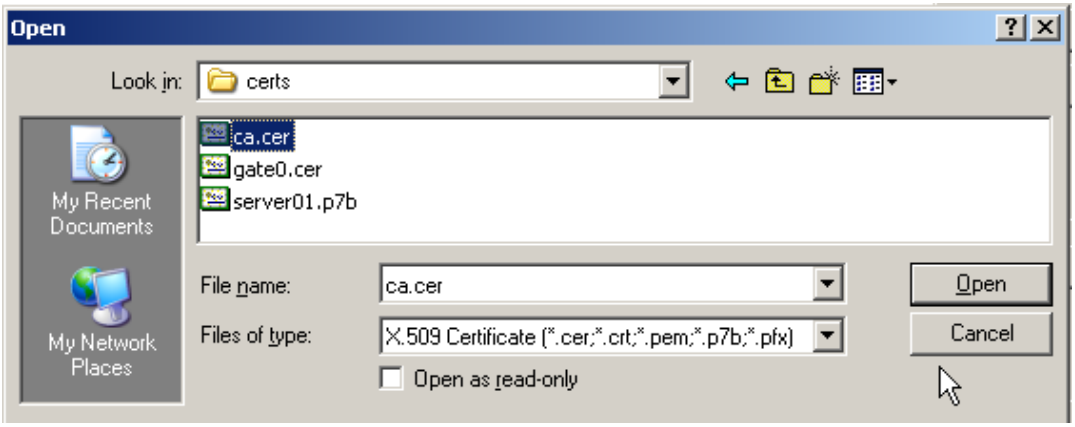

Рисунок 108

5. В следующем окне выберите CA сертификат (Рисунок 109).

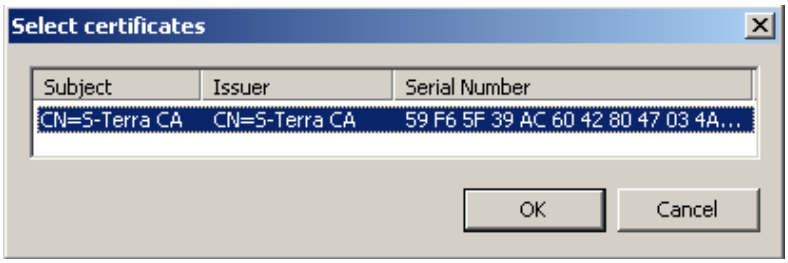

Рисунок 109

6. В разделе **Local certificates** нажмите кнопку Add (Рисунок 110).

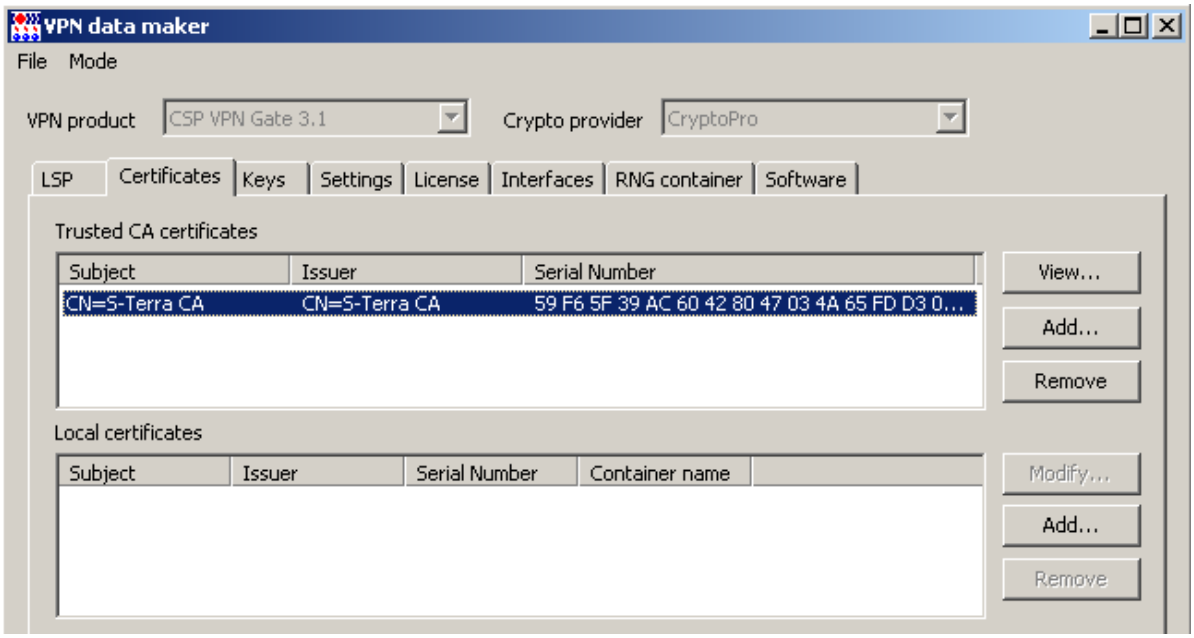

Рисунок 110

7. В открывшемся окне укажите файл с локальным сертификатом для клиента gate0.

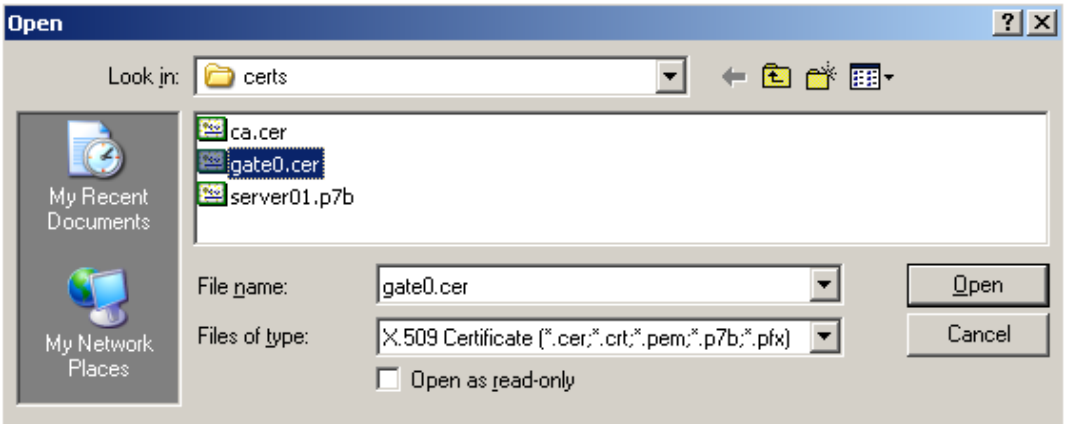

Рисунок 111

8. Выберите нужный сертификат и нажмите OK.

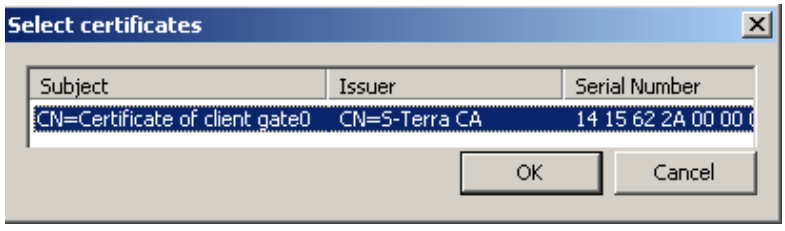

Рисунок 112

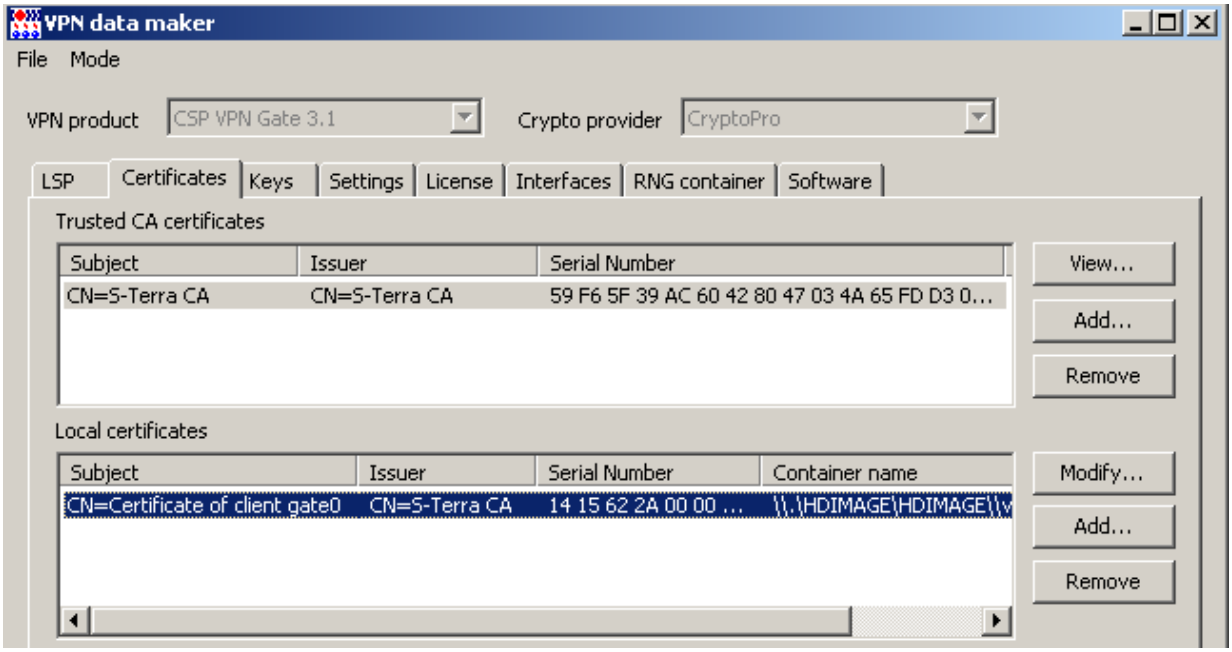

Рисунок 113

9. Для центрального шлюза в политике безопасности к методу аутентификации с использованием предопределенного ключа добавьте аутентификацию с использованием сертификатов. Для этого во вкладке **LSP** добавьте структуру **AuthMethodGOSTSign auth_method_02**, а в структуру `IKERule` добавьте имя метода аутетификации - **auth_method_02** (Рисунок 114):

```
AuthMethodGOSTSign auth_method_02(
    LocalID = IdentityEntry( DistinguishedName = USER_SPECIFIC_DATA )
    LocalCredential = CertDescription( Subject *=
COMPLETE,"CN=Certificate of client gate0" )
    SendRequestMode = AUTO
    SendCertMode = AUTO
)

IKERule ike_rule(
    DoNotUseDPD = FALSE
    DPDIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01,auth_method_02
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
    DoAutopass = TRUE
)
```

10. Нажмите кнопку OK (Рисунок 114).

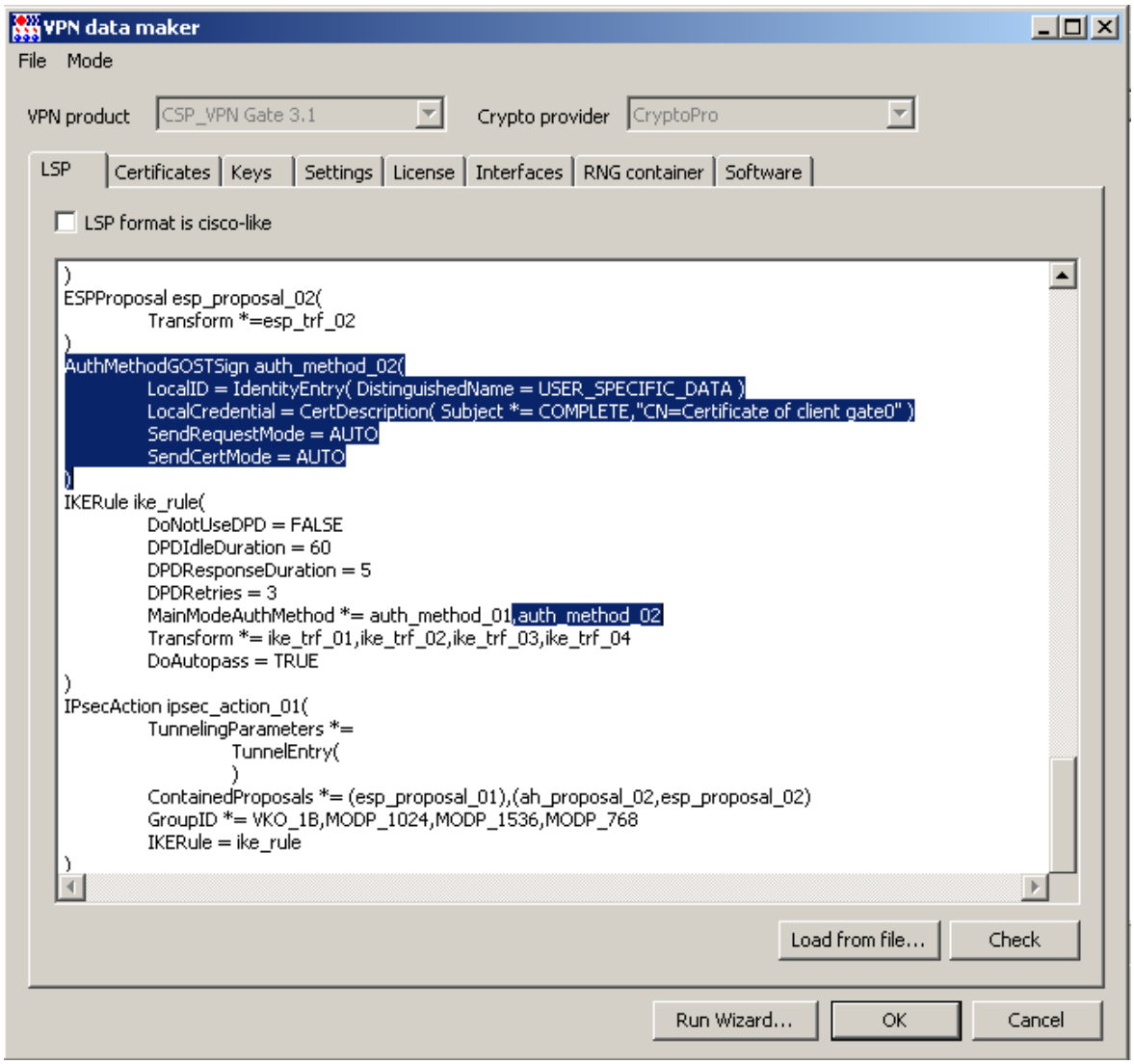

Рисунок 114

11. Файл с данными для продукта CSP VPN Gate создан (Рисунок 115), нажмите OK.

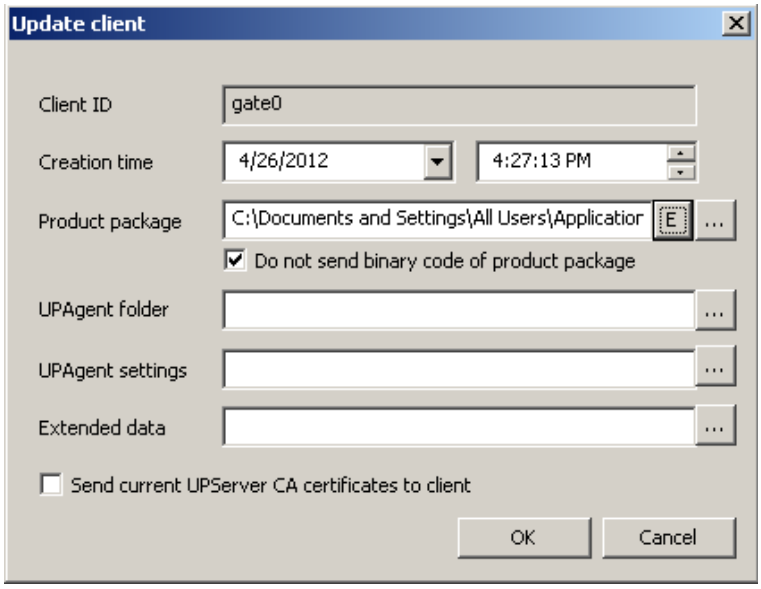

Рисунок 115

12. Обновление для gate0 подготовлено для скачивания (Рисунок 116).

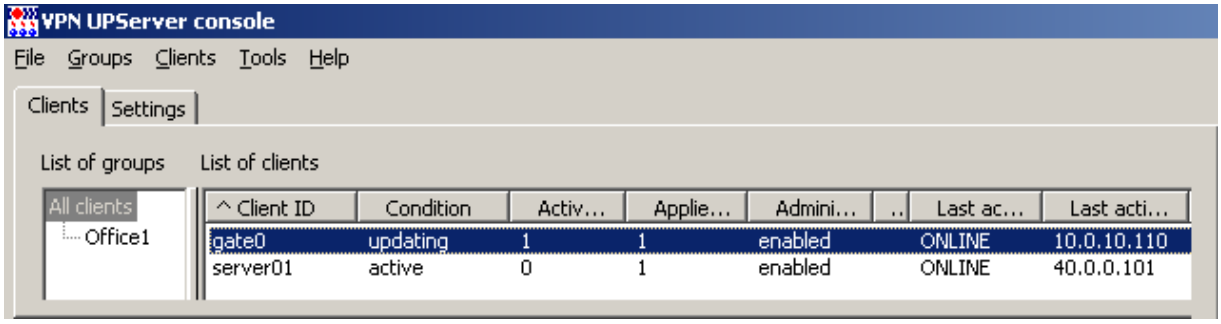

Рисунок 116

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 сертификат зарегистрированы в продукте и используются (Рисунок 117).

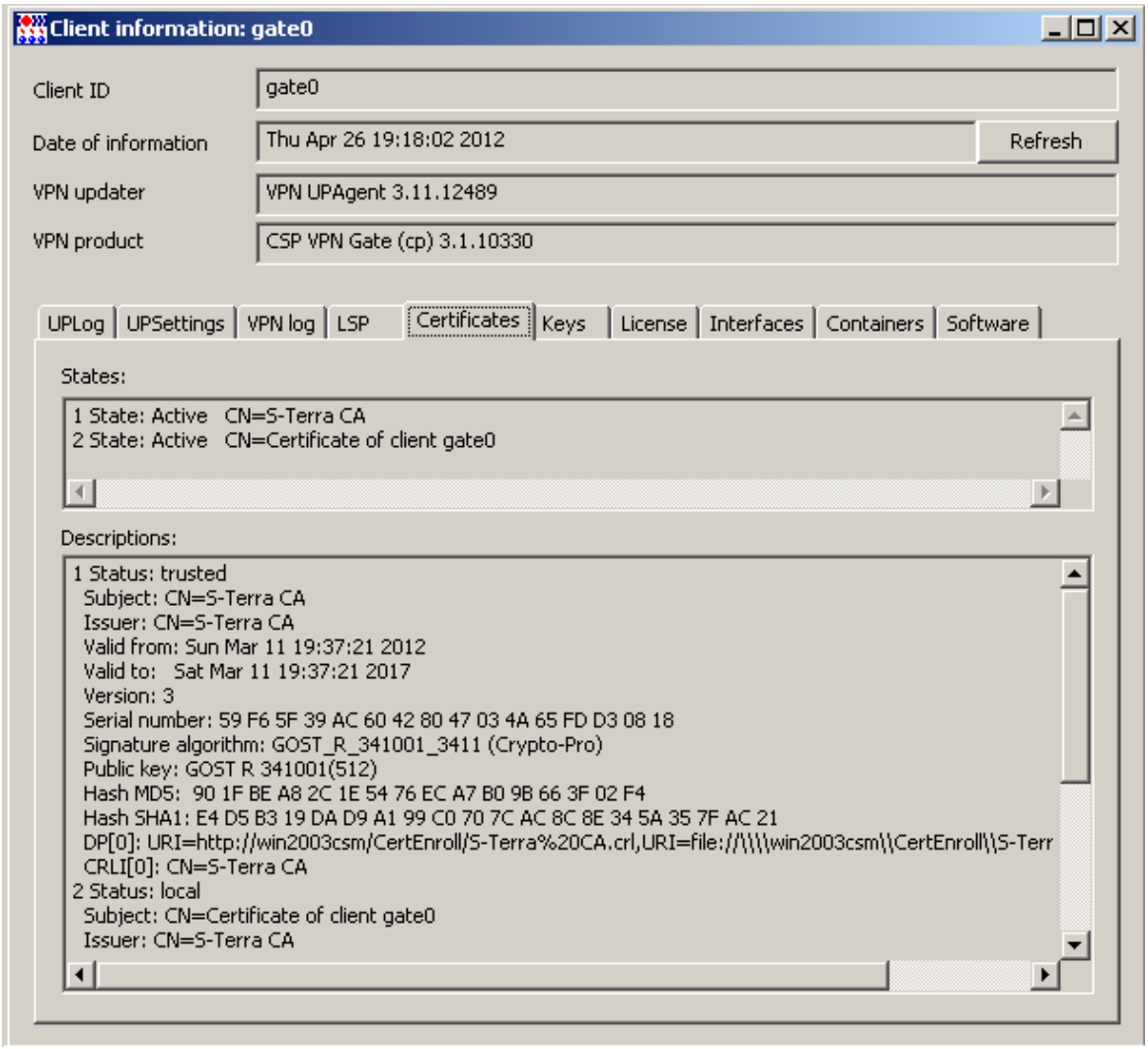

Рисунок 117

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

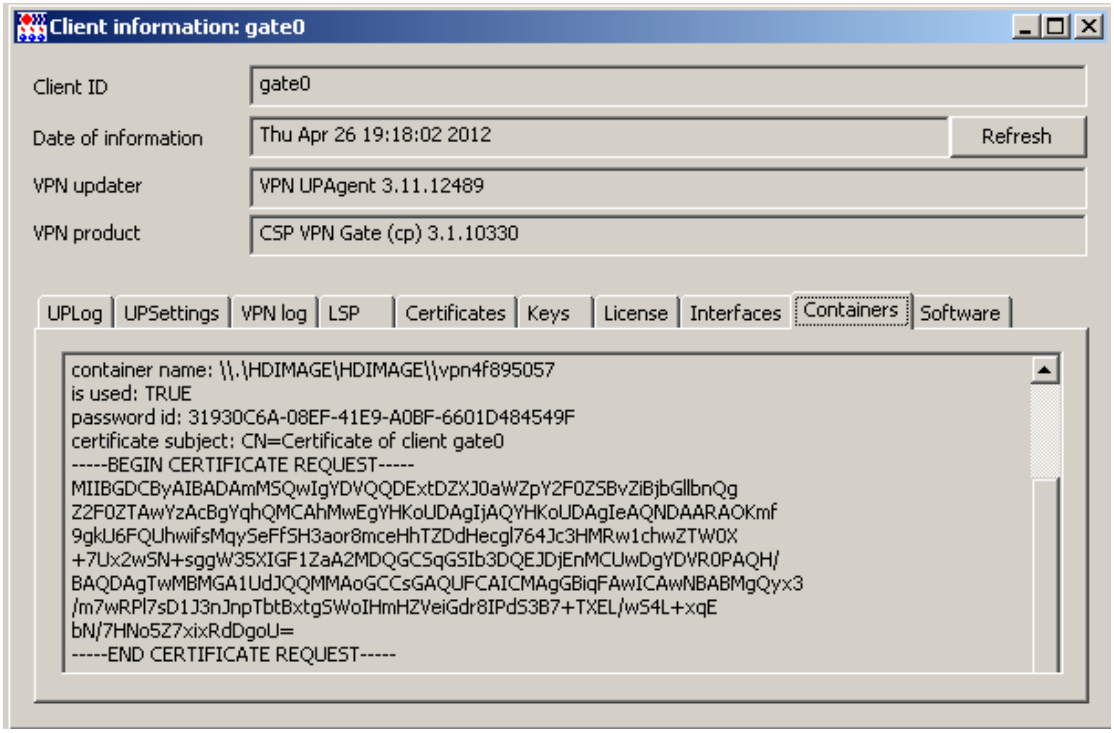

Рисунок 118

7.10. Создание обновления с новым сертификатом для сервера

Обратите внимание, что на момент замены сертификата на клиенте с CSP VPN Agent, его партнеры уже должны быть настроены на работу с новым сертификатом на CSP VPN Agent.

1. Создание обновления для сервера выполняется также как и для центрального шлюза – в контекстном меню выберите предложение ***Update*** (Рисунок 119).

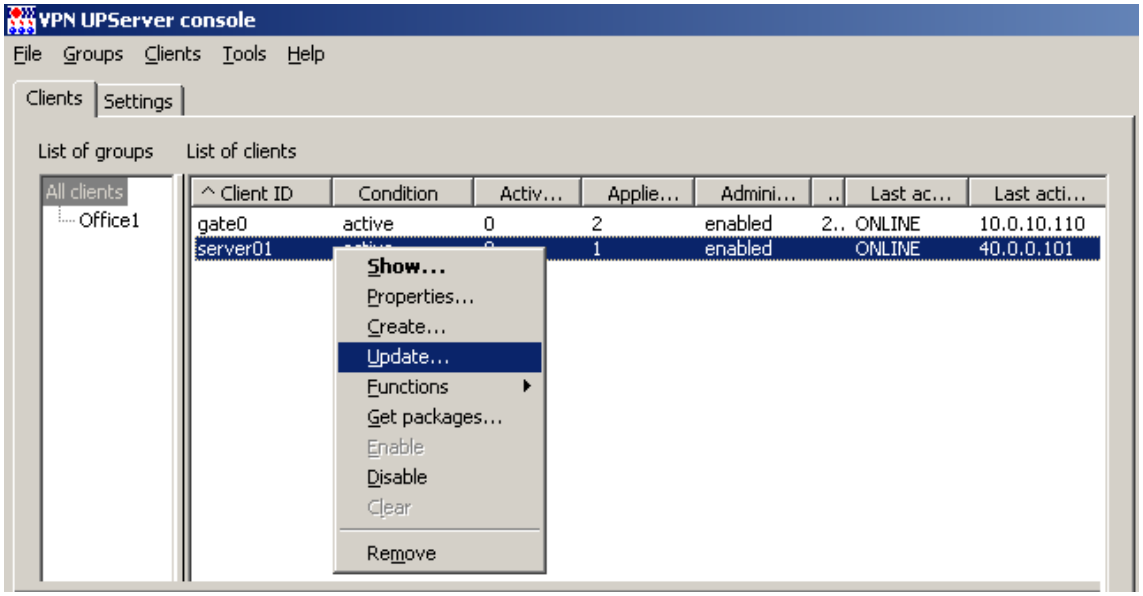

Рисунок 119

2. В следующем окне нажмите кнопку E для вызова окна для ввода данных (Рисунок 120).

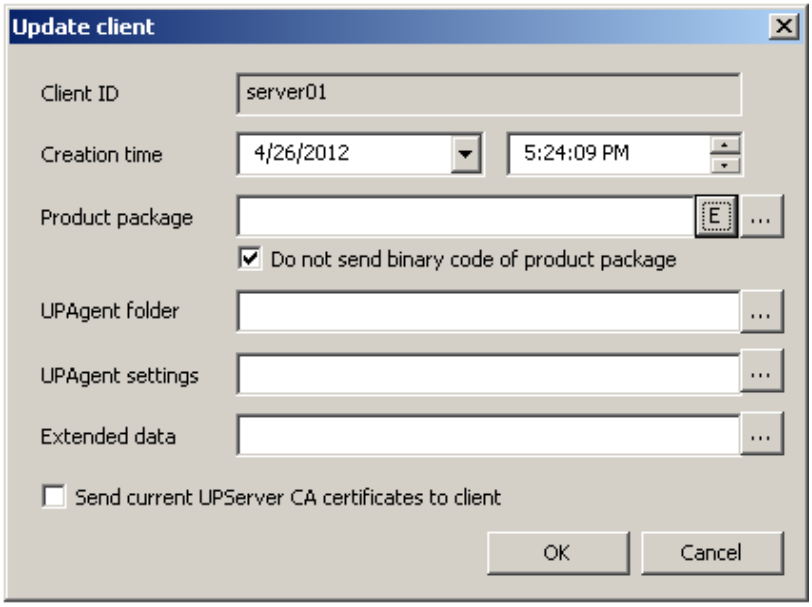

Рисунок 120

3. Появится окно **VPN data maker** с текущими настройками продукта CSP VPN Server. Для перехода на аутентификацию с использованием сертификатов в этом случае воспользуемся окнами мастера – нажмите кнопку Run Wizard.

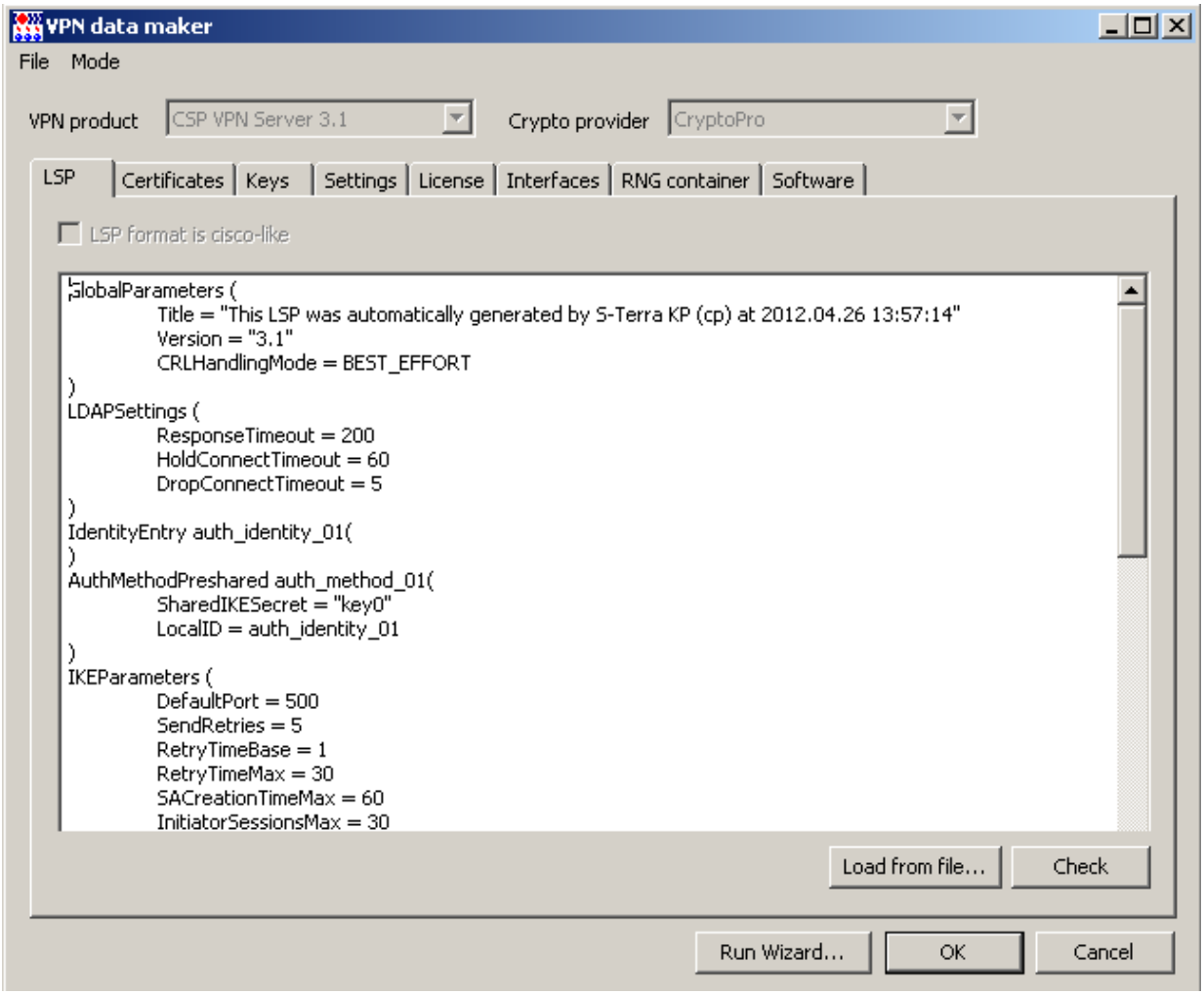

Рисунок 121

4. В первом окне мастера поставьте переключатель в положение **Use certificate**. В поле **CA certificate file** нажмите кнопку … .

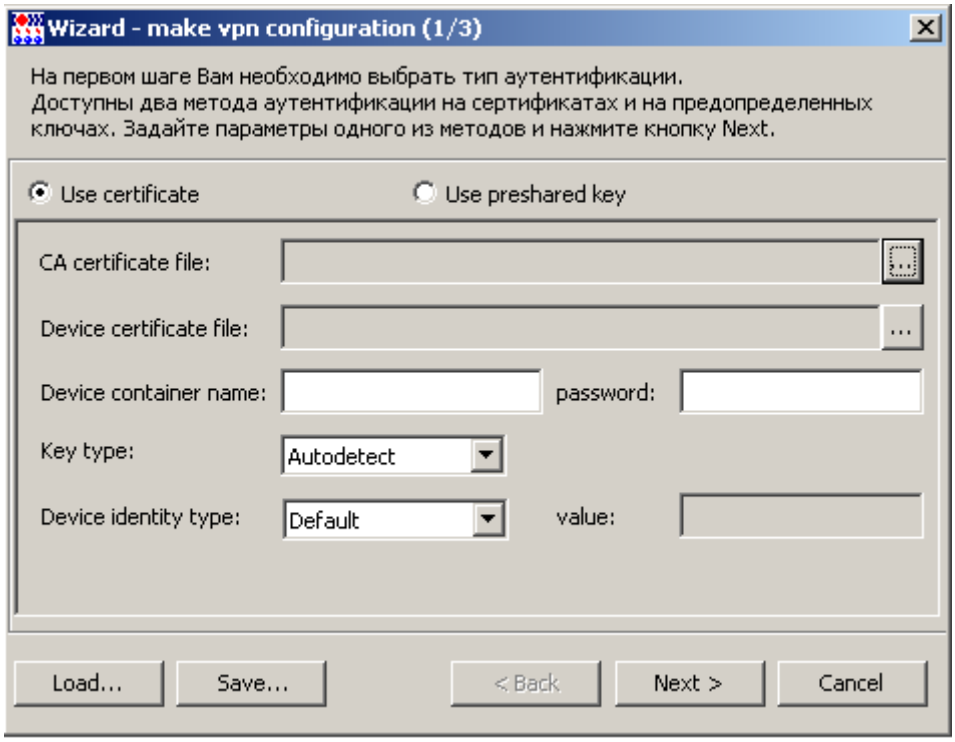

Рисунок 122

5. Выберите файл, в котором лежат два сертификата - CA сертификат и локальный сертификат для server01.

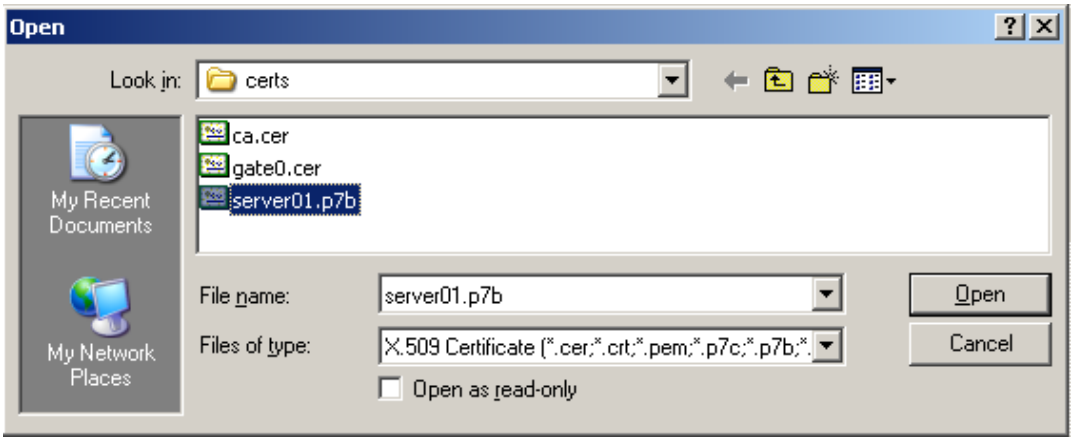

Рисунок 123

6. В открывшемся окне укажите CA сертификат и нажмите OK.

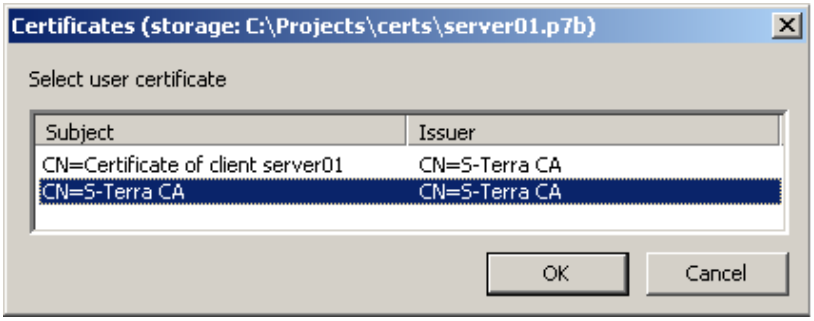

Рисунок 124

7. В строке **Device certificate file** опять нажмите кнопку ...

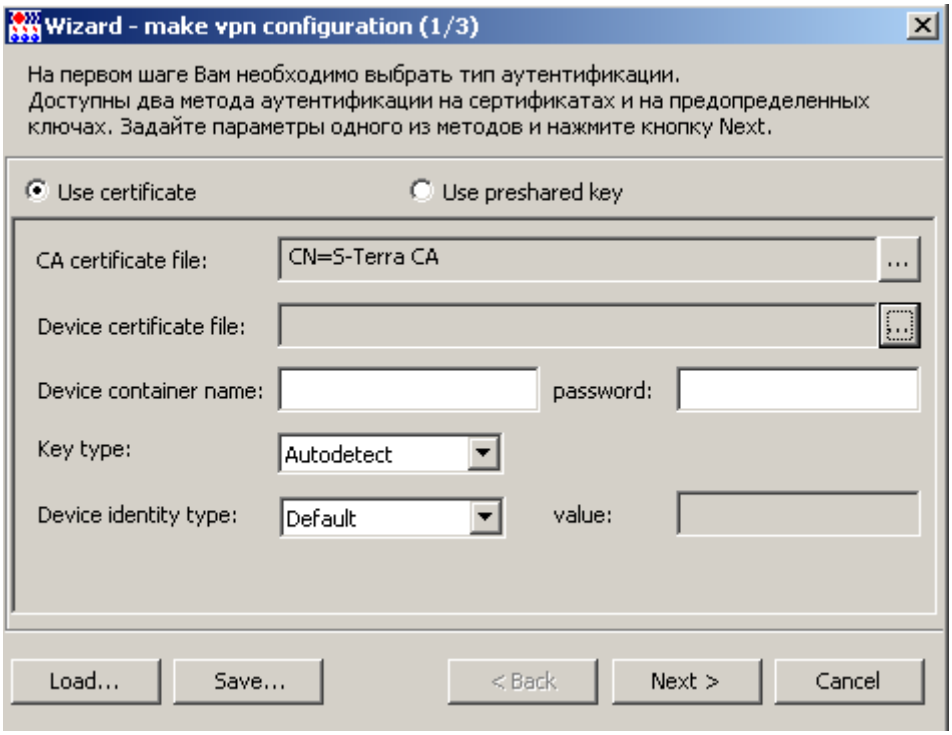

Рисунок 125

8. И укажите тот же файл с сертификатами.

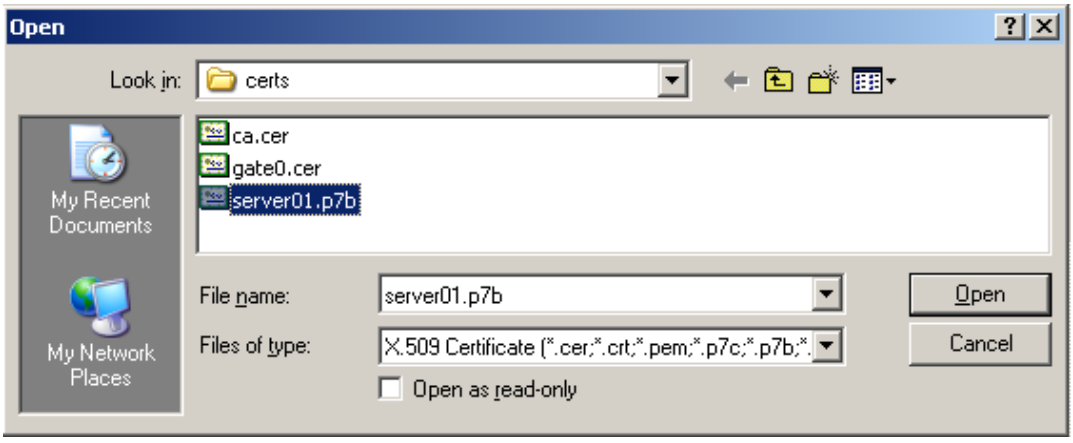

Рисунок 126

9. В открывшемся окне укажите локальный сертификат для управляемого устройства server01 и нажмите OK.

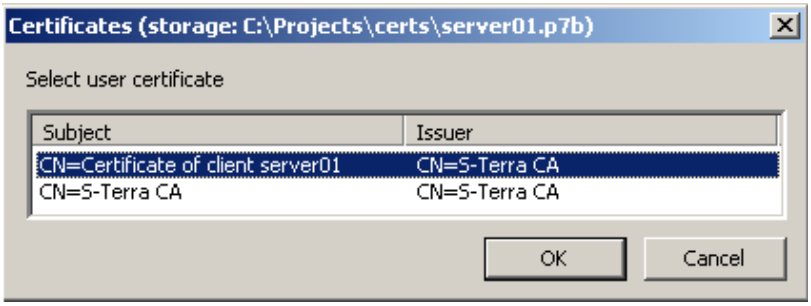

Рисунок 127

10. Первое окно мастера заполнено не только полями с сертификатами, но и автоматически заполняются поля с именем контейнера и паролем к нему. Эти данные сохраняются при создании запроса на сертификат.

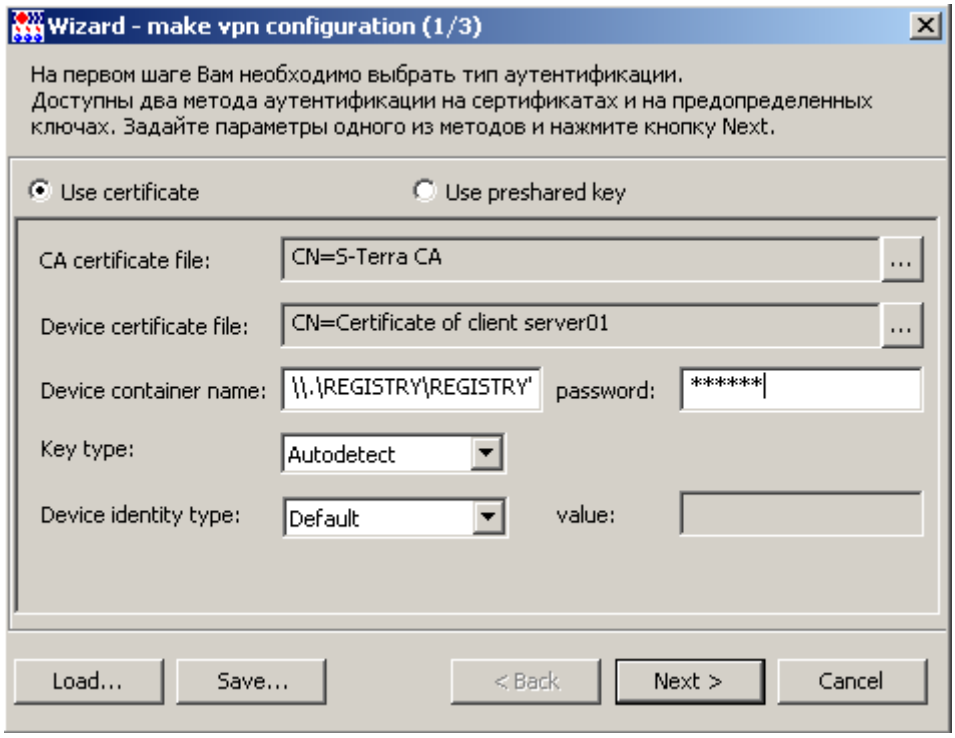

Рисунок 128

11. В поле **Device identity type** измените тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Укажите значение `Distinguished Name` – в качестве идентификатора партнеру будет высылаться значение поля Subject из локального сертификата управляемого устройства, показываемое в поле **Device identity value**, если оно задано в сертификате. Нажмите кнопку Next.

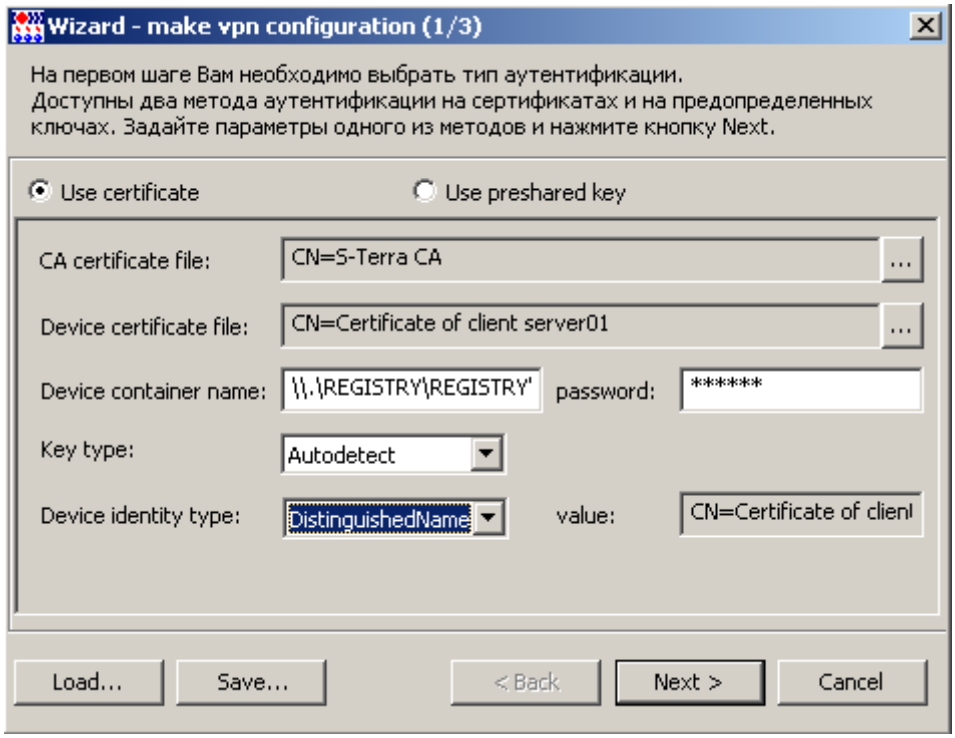

Рисунок 129

12. В следующем окне правила оставьте без изменения, нажмите кнопку Next.

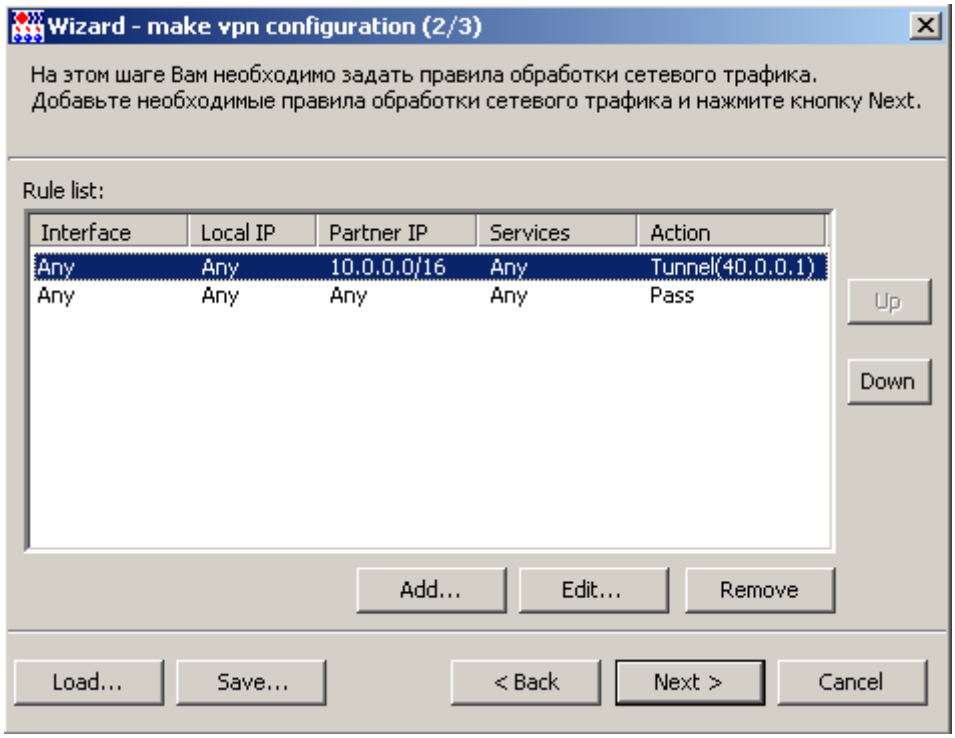

Рисунок 130

13. Данные лицензий оставьте без изменений и нажмите кнопку Finish.

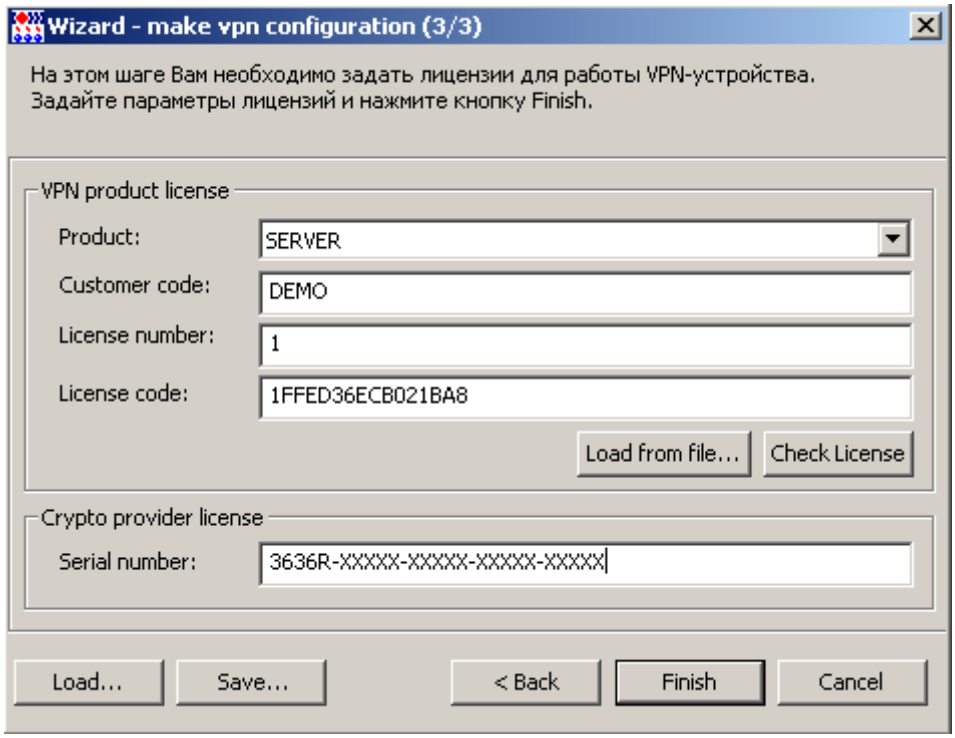

Рисунок 131

14. Далее появляется окно **VPN data maker**, в котором все вкладки настроены на аутентификацию с использованием сертификатов, в том числе и политика **LSP**. Нажмите кнопку OK.

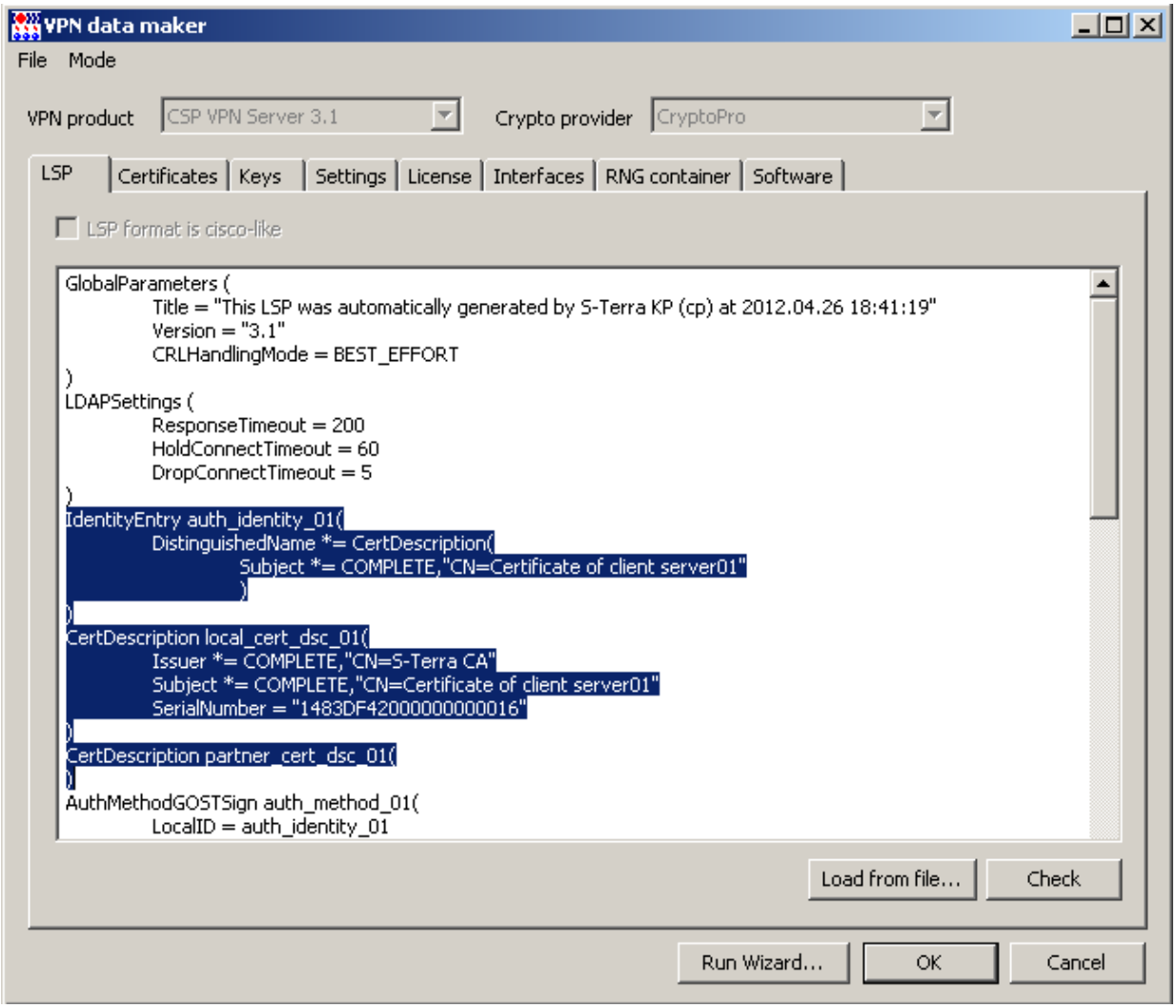

Рисунок 132

15. В следующем окне опять нажмите OK.

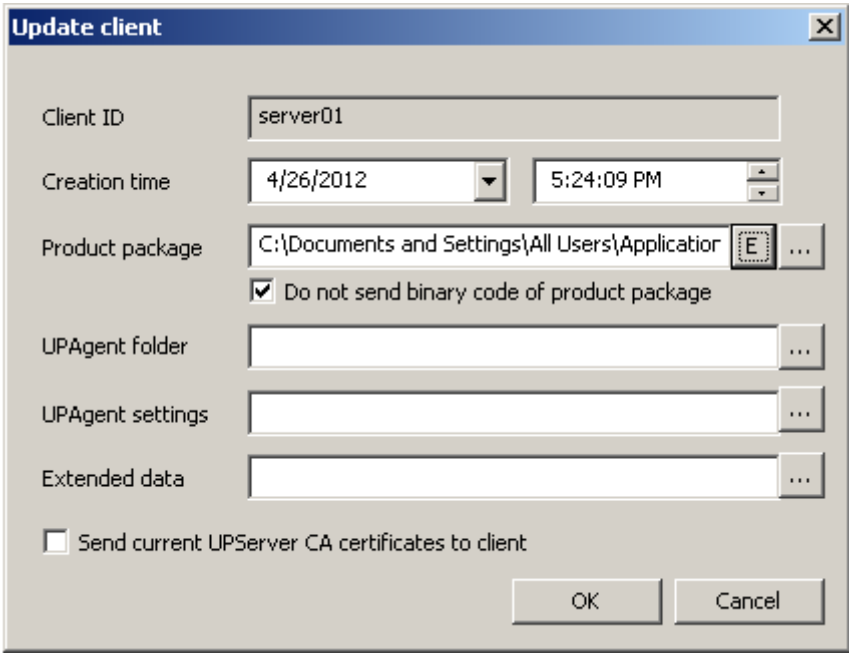

Рисунок 133

16. Обновление с сертификатами для server01 подготовлено и готово для скачивания Клиентом управления (Рисунок 134).

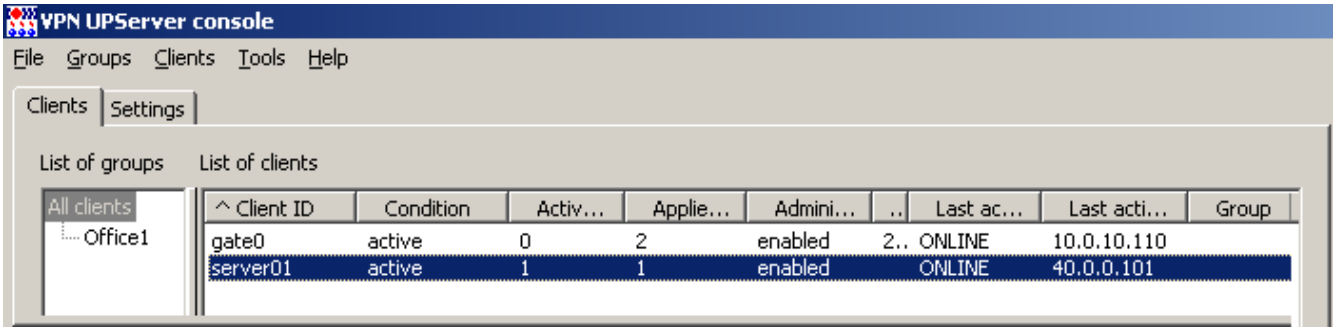

Рисунок 134

17. После его применения на управляемом устройстве во вкладке **Certificates** видно, что на устройстве в продукте CSP VPN Server зарегистрировано три сертификата – CA, локальный и сертификат партнера (Рисунок 135).

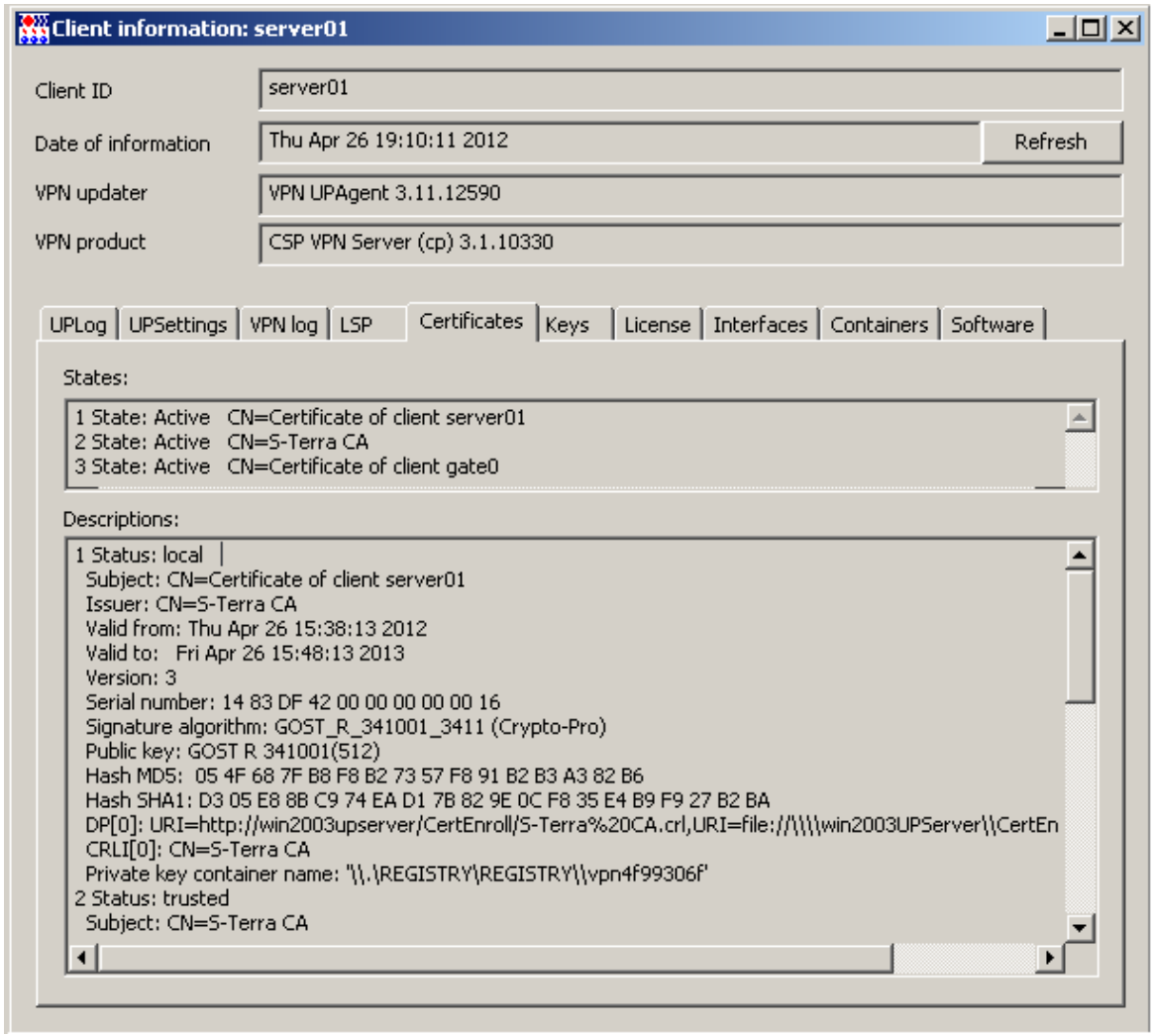

Рисунок 135

8. Сценарий неудачного обновления клиента

1. Для получения неудачного обновления клиента укажите неверный адрес Сервера управления в настройках Клиента управления. Для этого во вкладе **Settings** измените, например, адрес 10.0.10.111 на адрес 10.0.10.112 и нажмите кнопку Save (Рисунок 135).

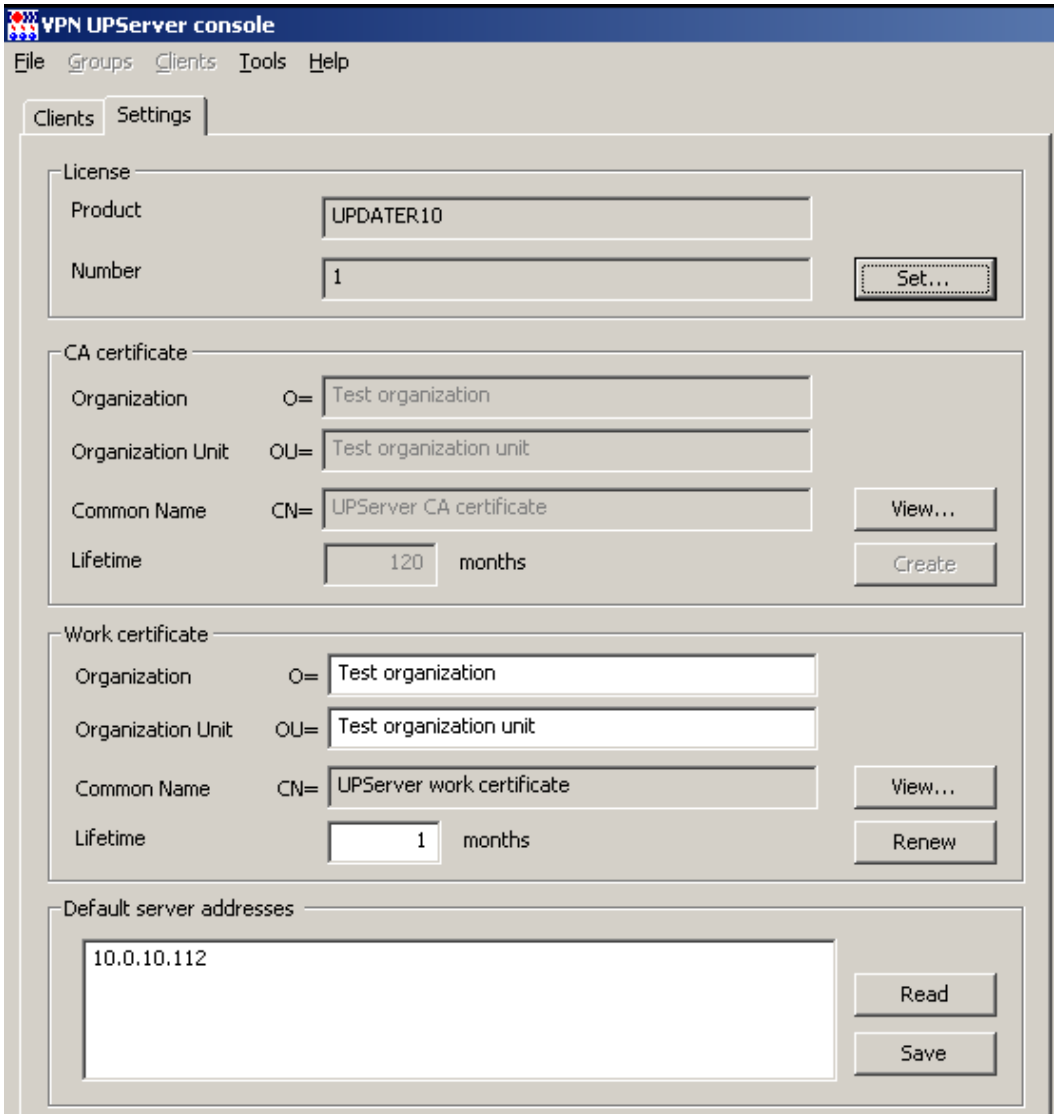

Рисунок 136

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

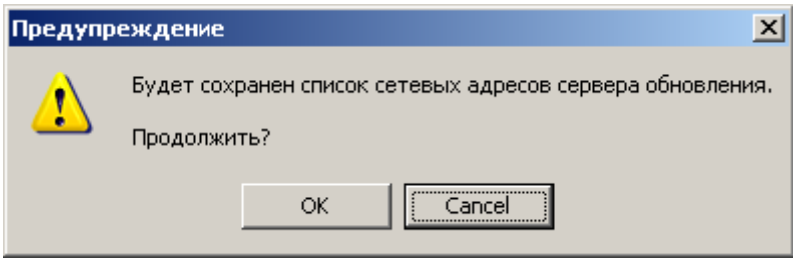

Рисунок 137

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

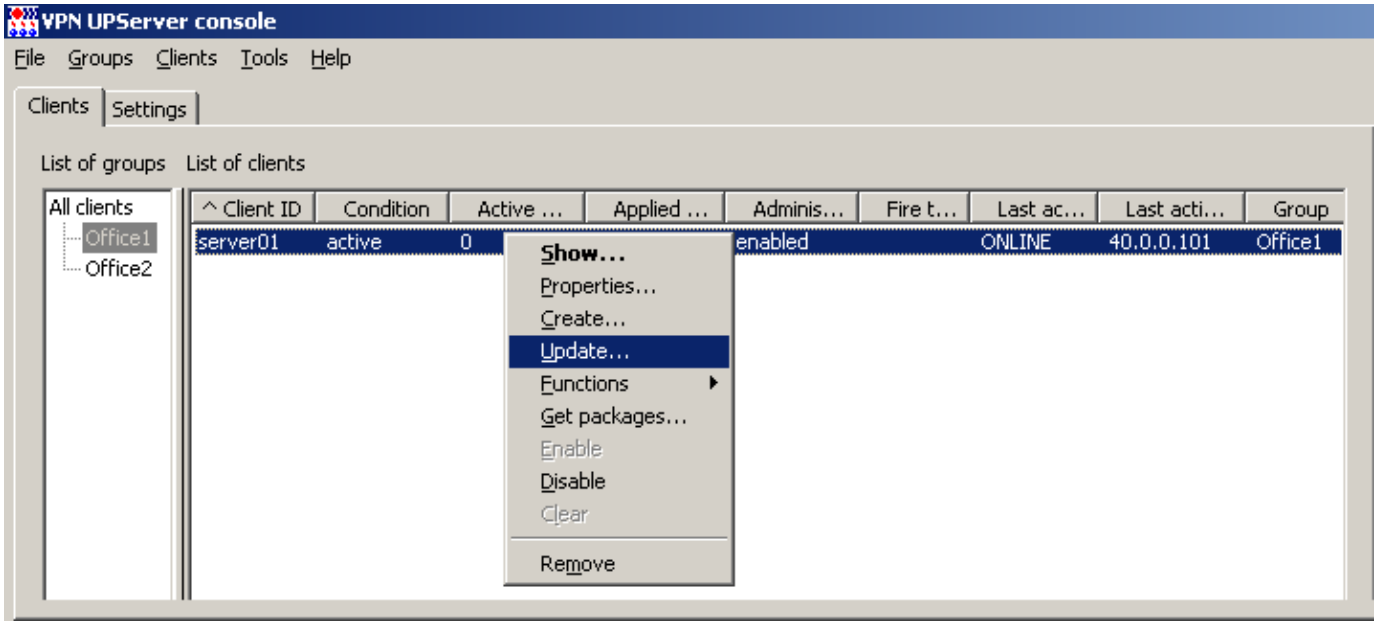

Рисунок 138

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".

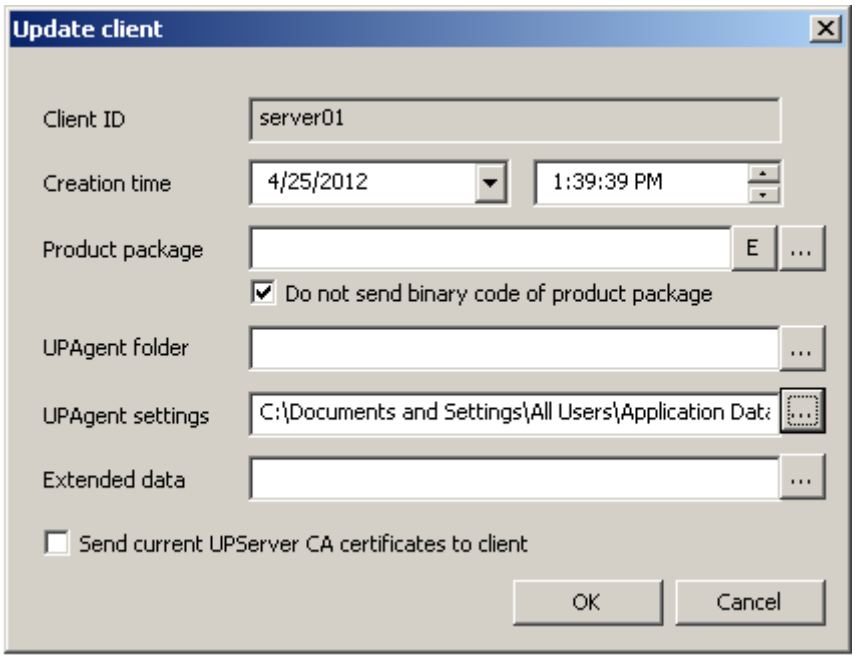

Рисунок 139

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

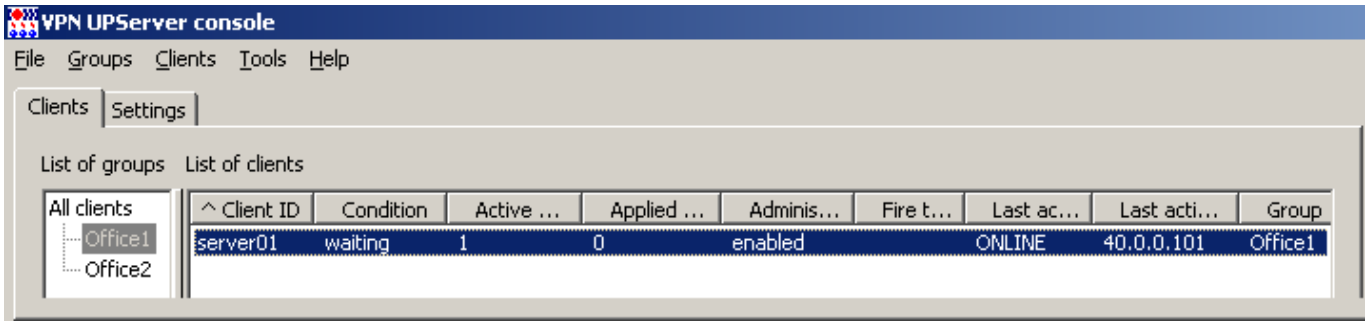

Рисунок 140

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

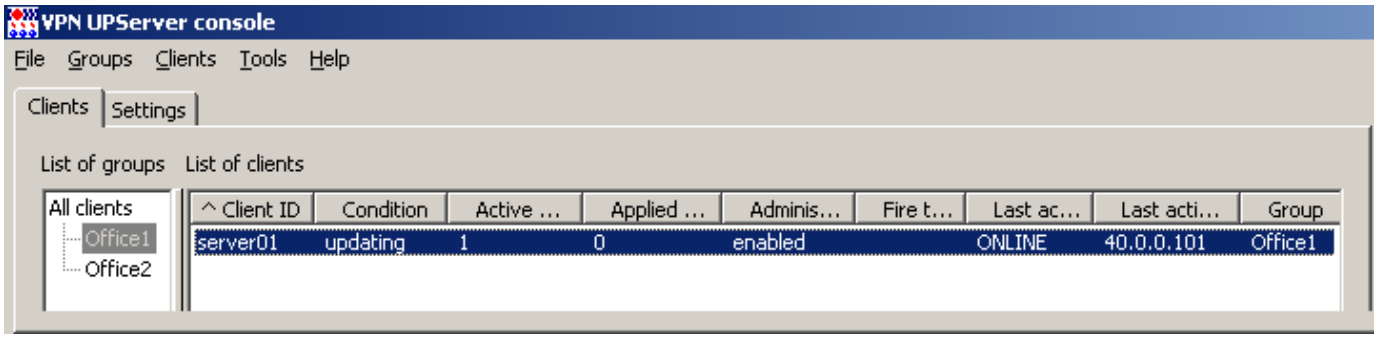

Рисунок 141

7. По истечении некоторого времени (если настройки по умолчанию не менялись, то примерно через 6 минут) состояние изменится с **updating** на **failed**.

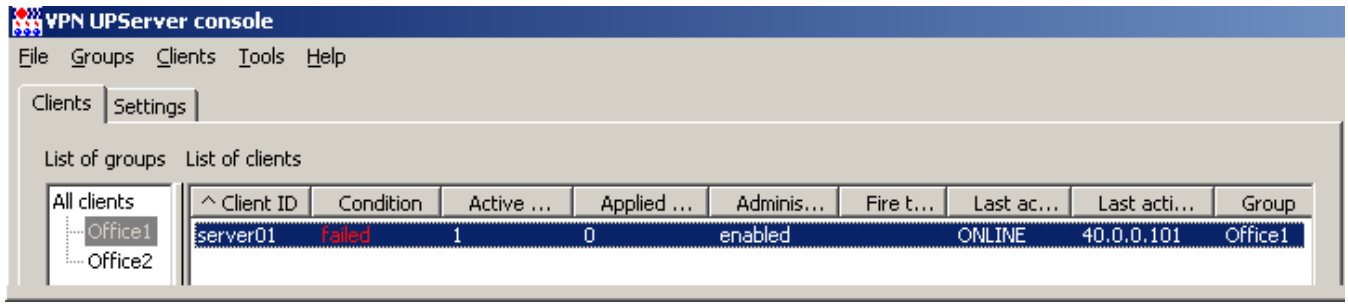

Рисунок 142

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 144).

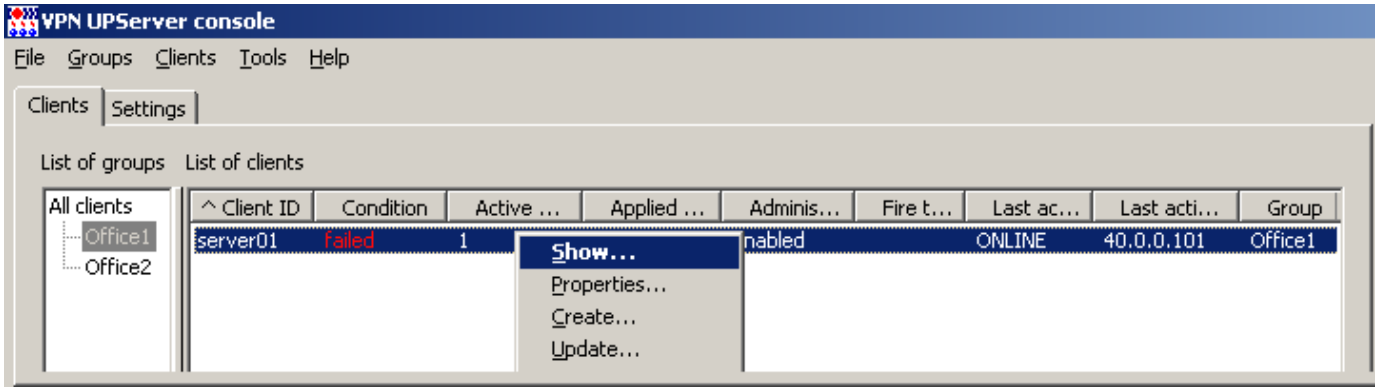

Рисунок 143

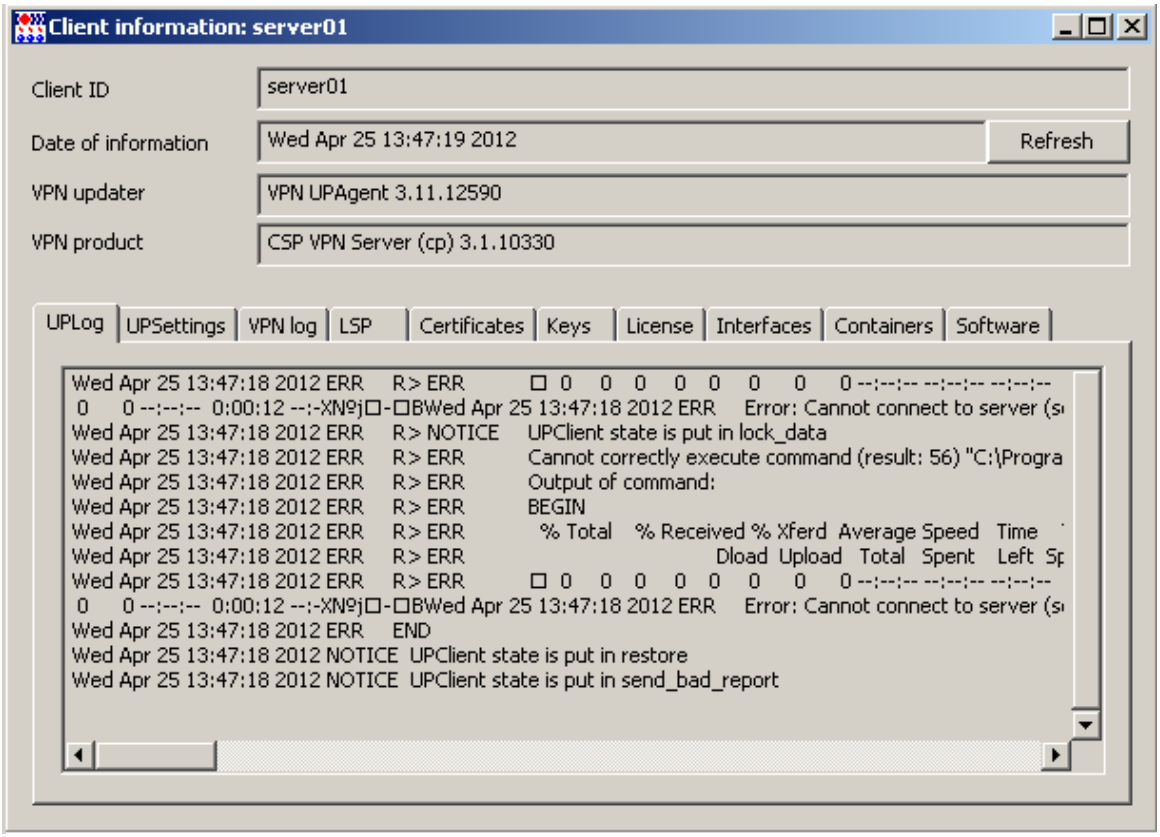

Рисунок 144

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

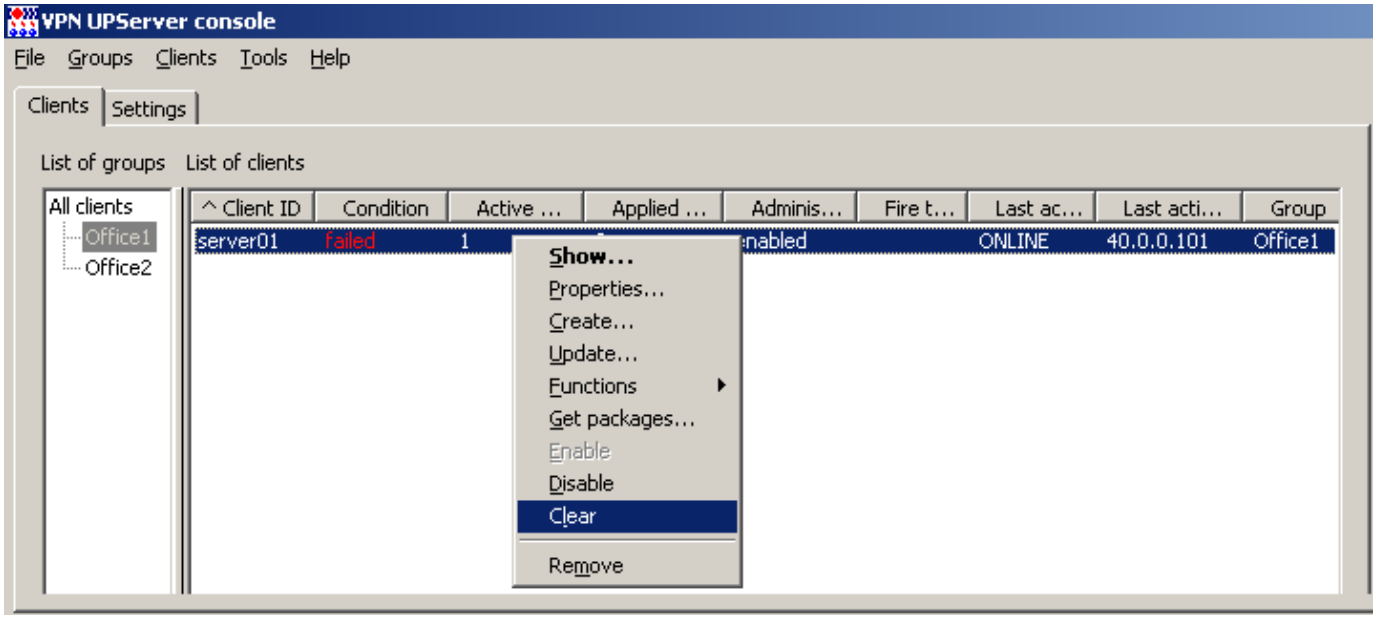

Рисунок 145

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

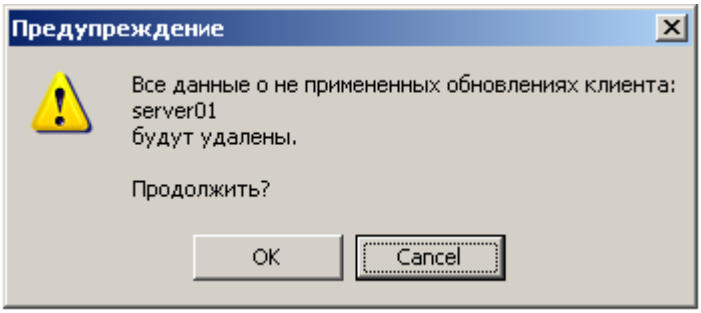

Рисунок 146

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.

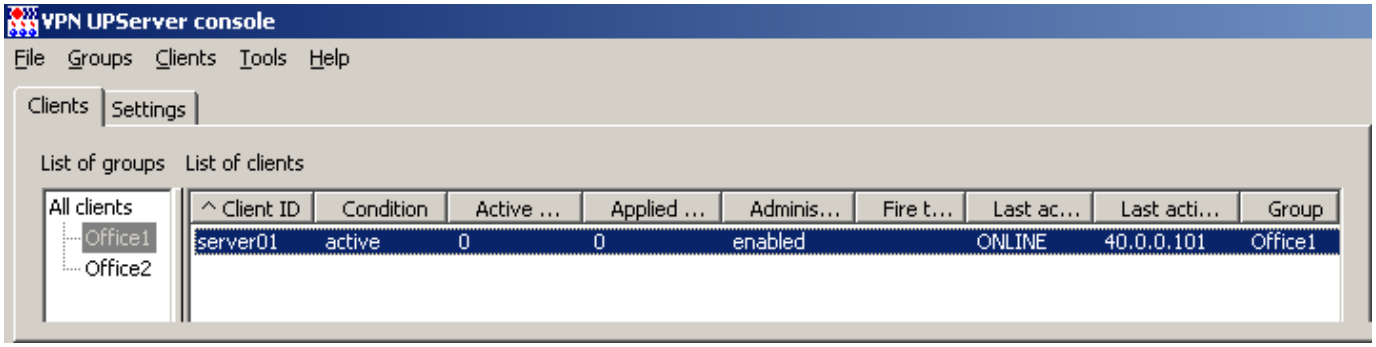

Рисунок 147

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

9. Информация о клиенте на Сервере управления

1. Посмотреть параметры VPN-продукта, Клиента управления на управляемом устройстве после проведенного обновления можно на Сервере управления с помощью предложения ***Show*** меню ***Clients*** (или контекстного меню).

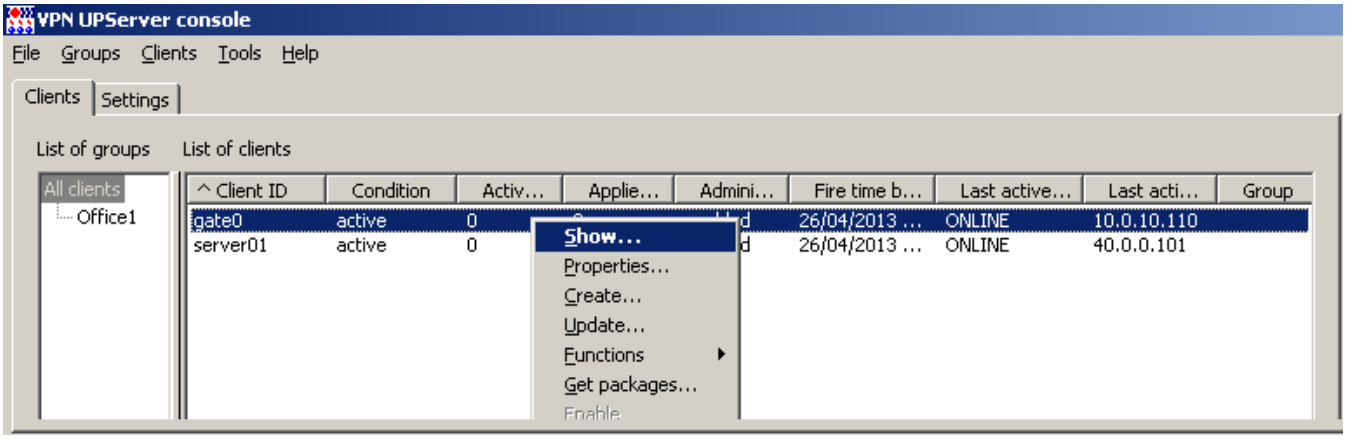

Рисунок 148

2. В результате будет выдано окно с разными вкладками (Рисунок 149), в которых отражена информация о проведенных обновлениях, настройках Клиента управления, действующей в данный момент политике безопасности на клиенте, используемых предопределенных ключах или сертификатах, об интерфейсах клиента, таблице маршрутизации и т.п.
3. Во вкладке **UPLog** ведется лог событий по обновлению клиента.

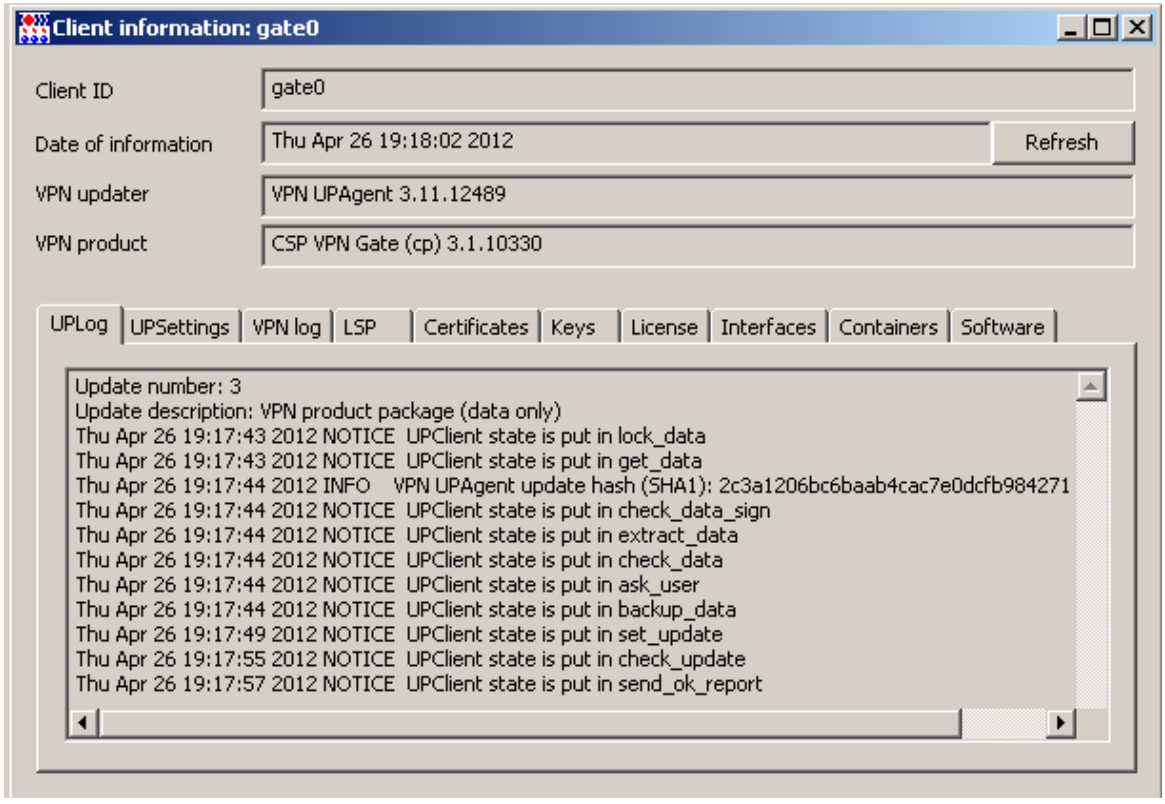

Рисунок 149

4. Во вкладке **UPSettings** (Рисунок 150) отражены настройки Клиента управления. Описание этих настроек дано в главе «Настройки Клиента управления».

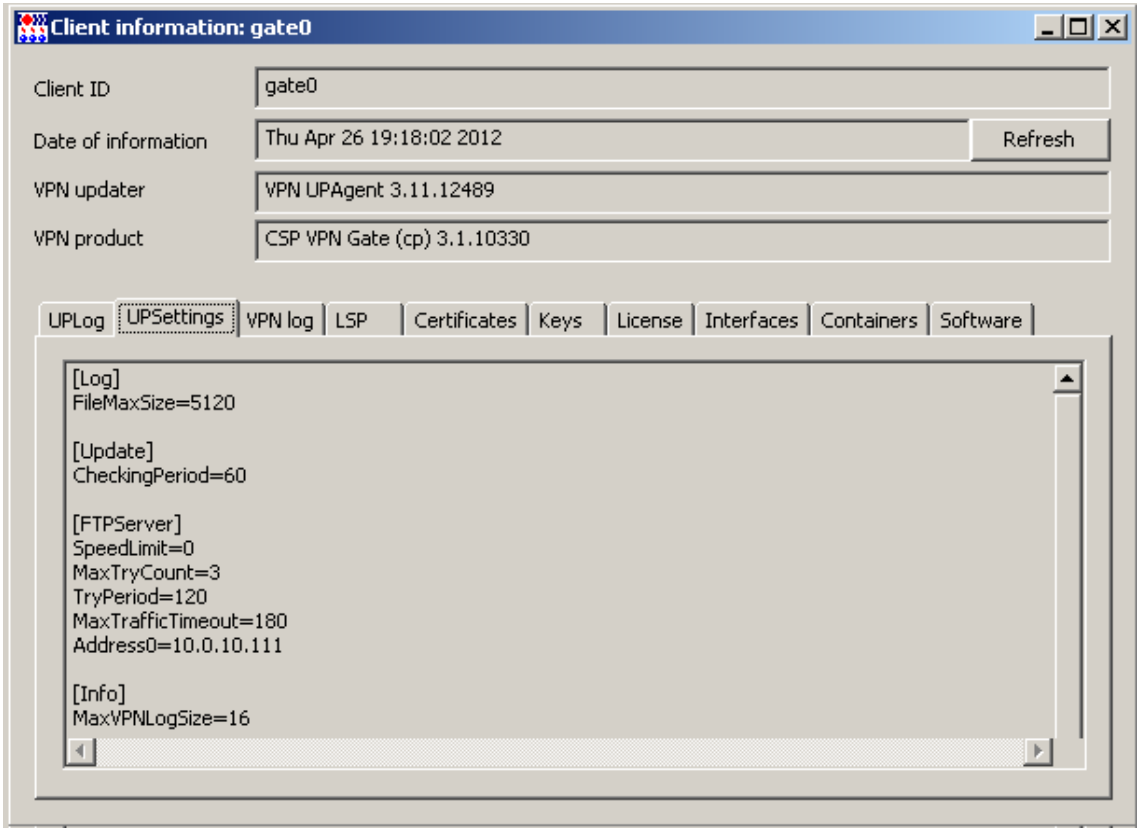

Рисунок 150

5. Во вкладке **VPN log** отражается протоколирование событий, связанных с работой VPN-продукта CSP VPN Agent, и настройки syslog-клиента.

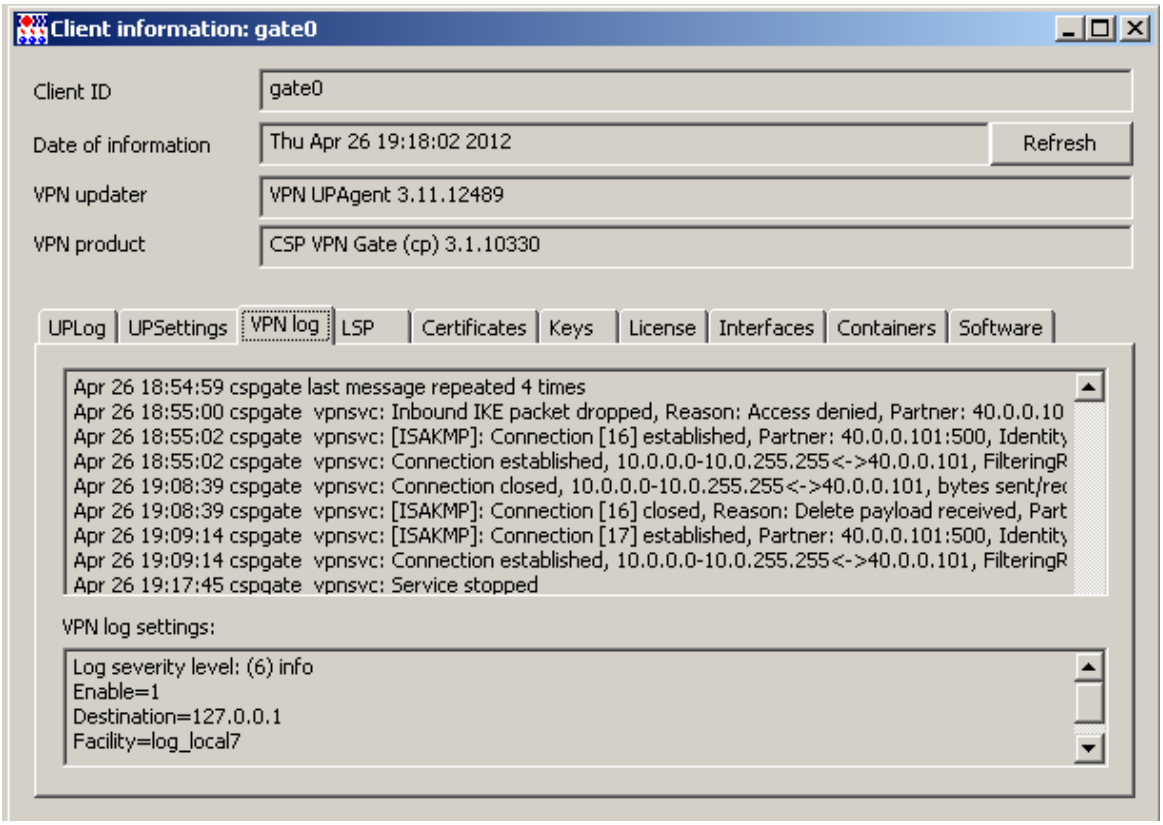

Рисунок 151

6. Вкладка **LSP** показывает загруженную политику безопасности на управляемом устройстве в виде текстового файла и в виде cisko-like конфигурации, а также политику по умолчанию (Рисунок 152).

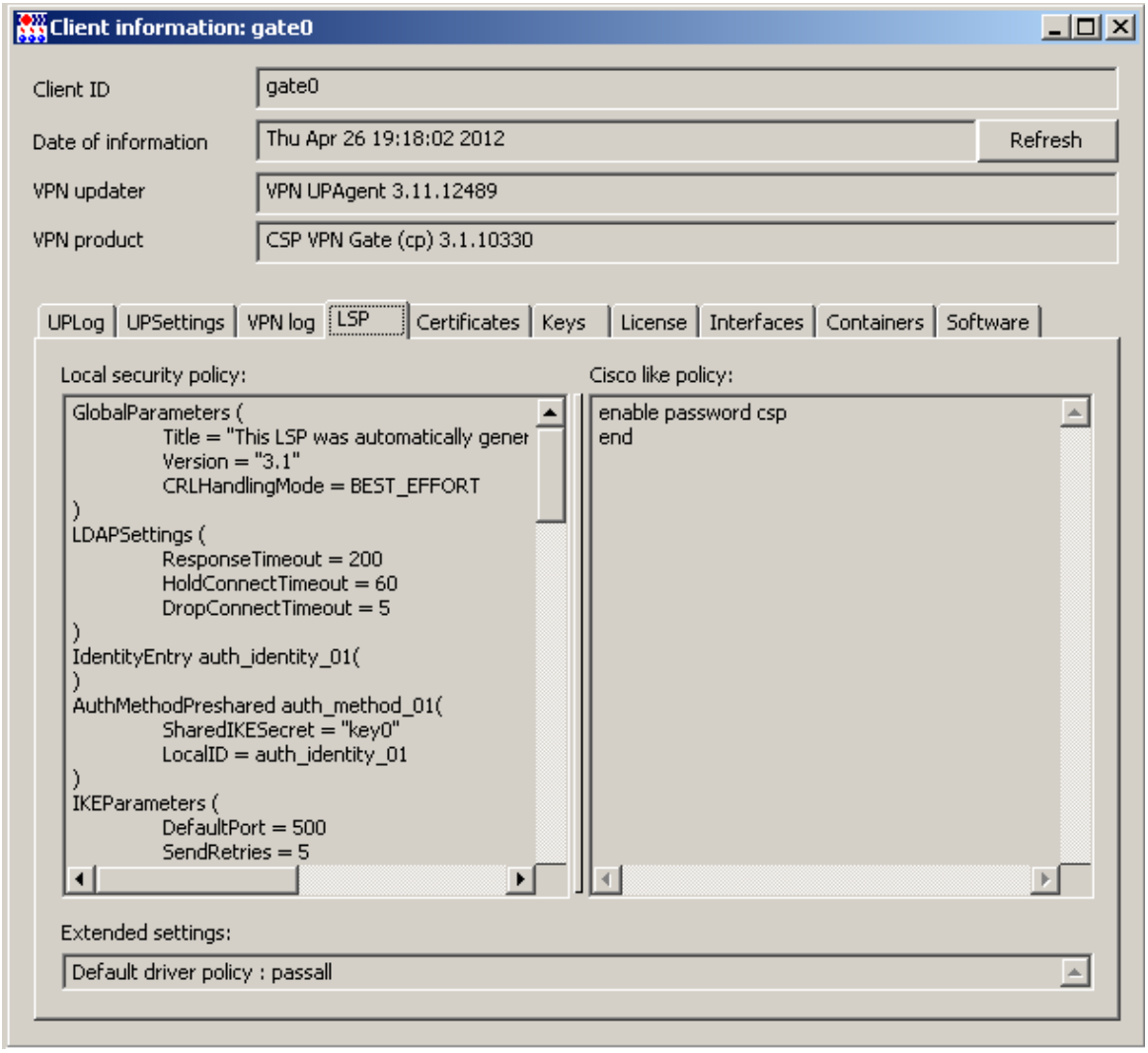

Рисунок 152

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

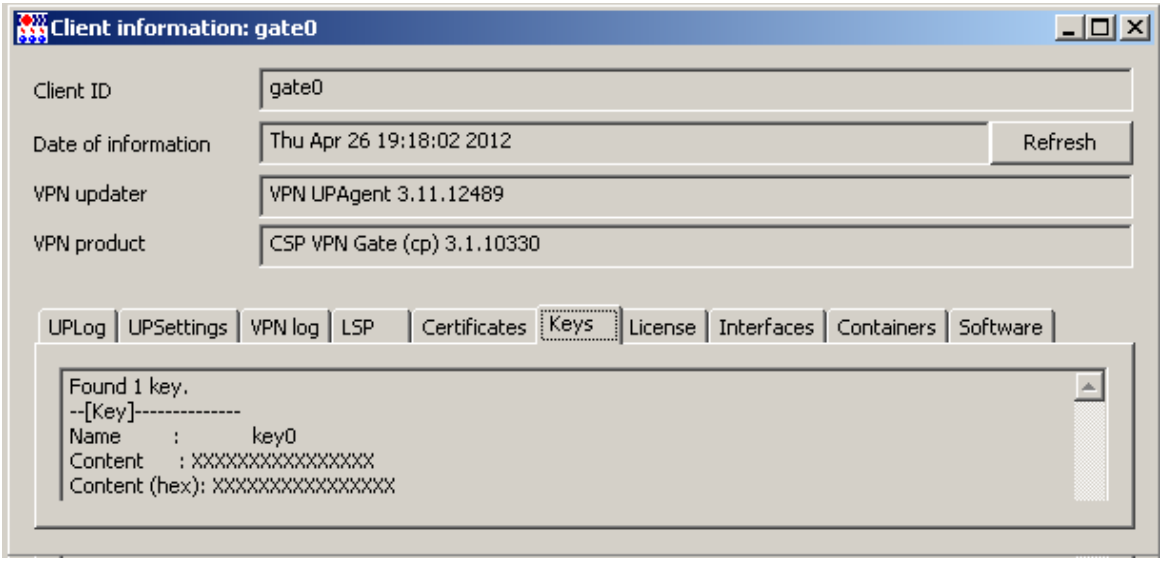

Рисунок 153

8. Вкладка **Certificates** показывает все зарегистрированные в продукте CSP VPN Agent сертификаты и их статус.

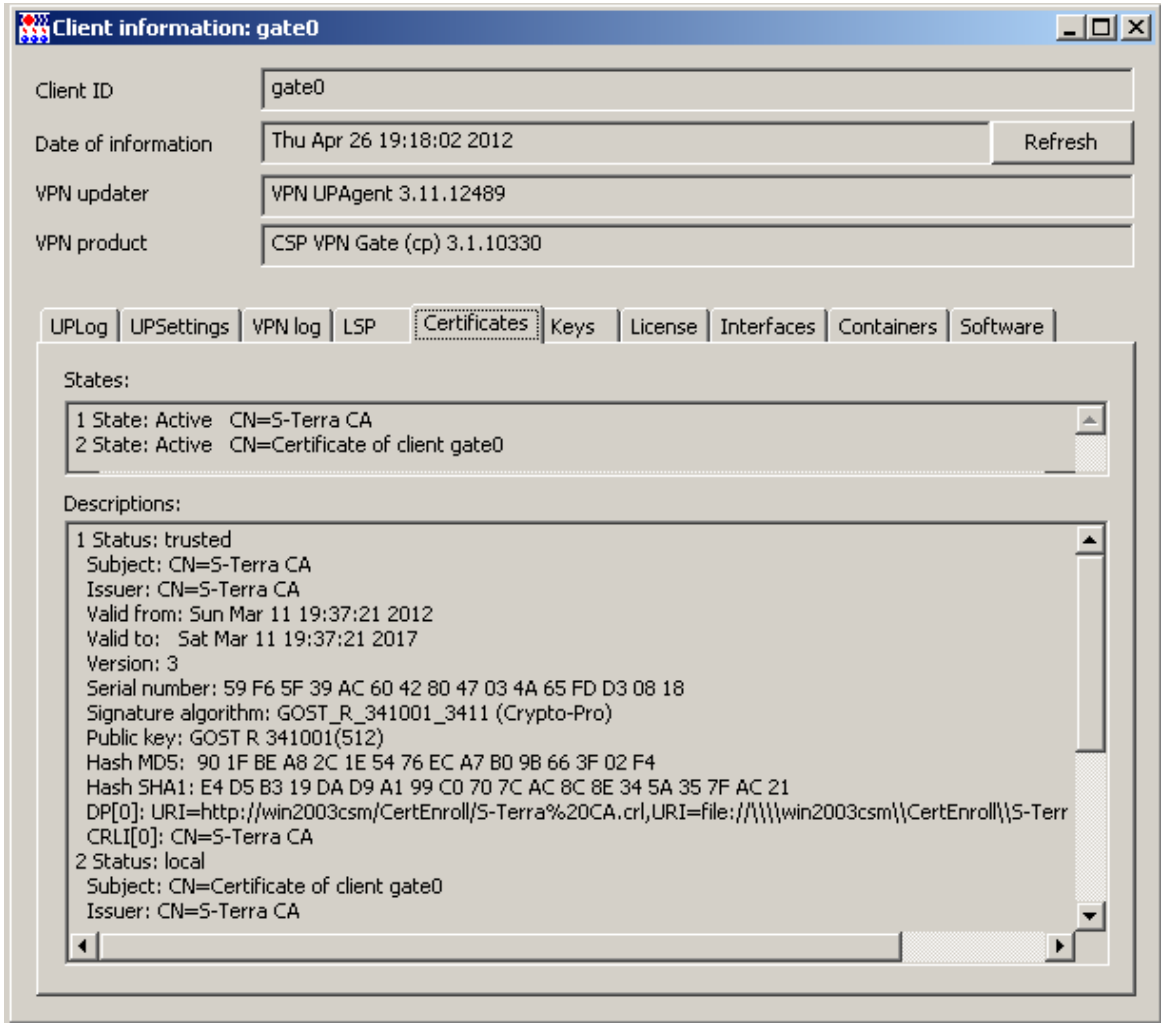

Рисунок 154

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

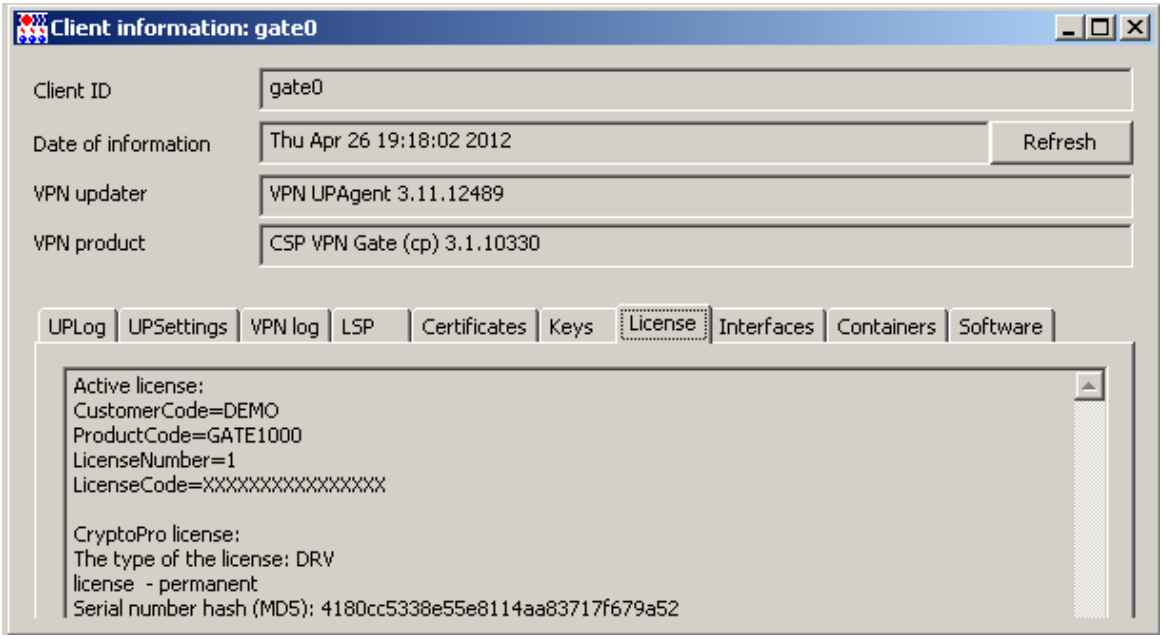

Рисунок 155

10. Вкладка **Interfaces** содержит информацию обо всех сетевых интерфейсах управляемого устройства, а раздел Driver settings показывает настройки IPsec драйвера (для продуктов CSP VPN Gate 3.1,3.11, S-Terra Gate 4.0 и S-Terra Server 4.0).

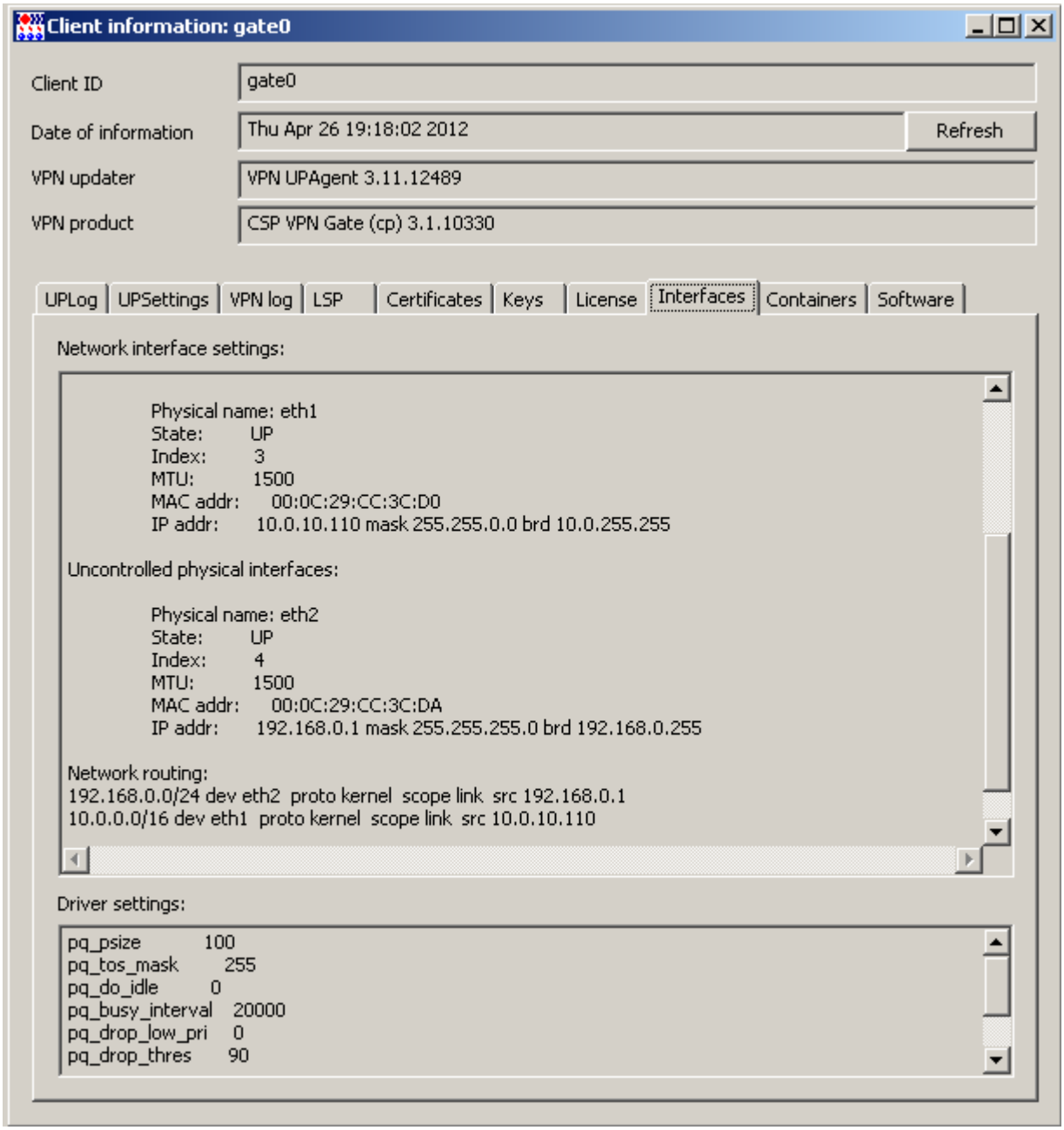

Рисунок 156

11. Для устройства с установленным продуктом CSP VPN Server во вкладке Interfaces будет показана еще и таблица маршрутизации (Рисунок 157).

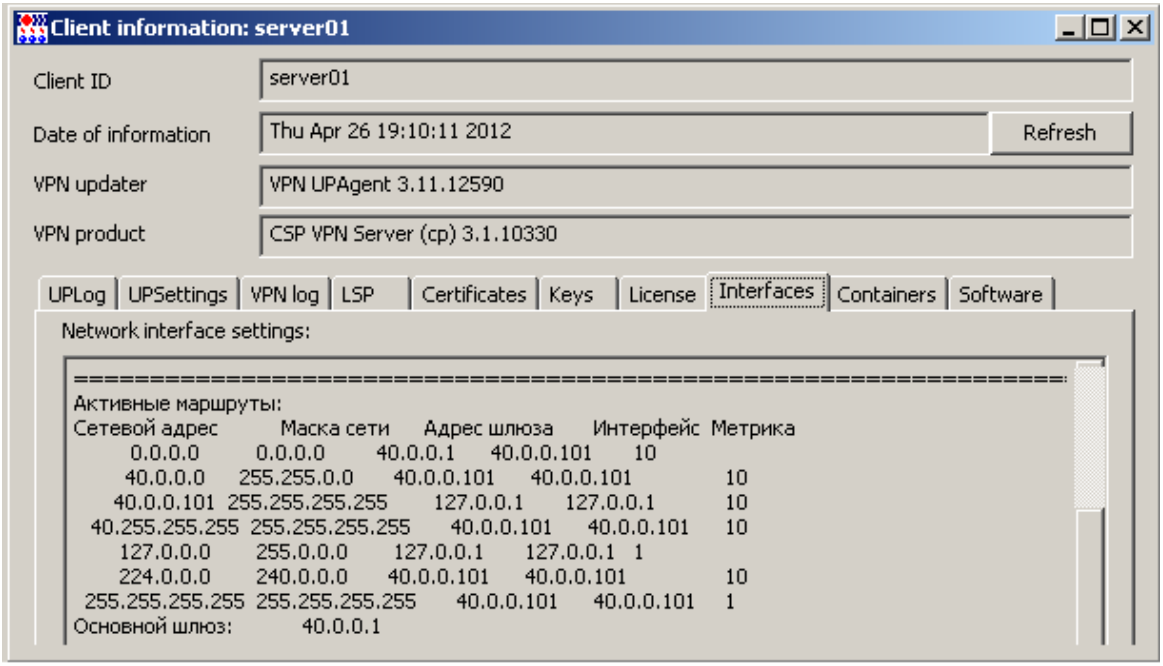

Рисунок 157

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

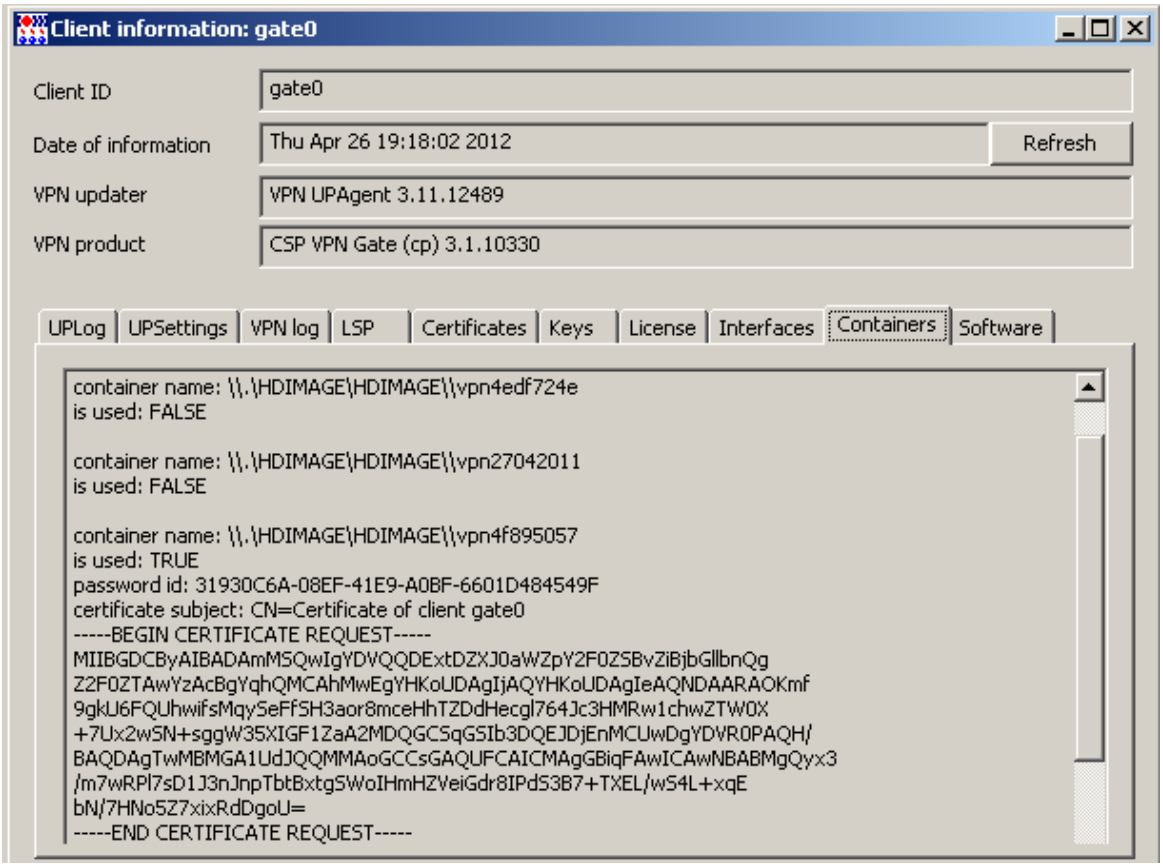

Рисунок 158

13. Вкладка Software используется только для продукта CSP VPN Gate on token и описана в разделе «Настройка и управление СПДС «ПОСТ».

10. Действия пользователя при обновлении

Сценарий обновления на управляемом устройстве зависит от настройки «Режим запроса подтверждения у пользователя о начале обновления» на Клиенте управления. По умолчанию эта настройка имеет значение **auto**:

для CSP VPN Client всегда будет запрашиваться разрешение на применение обновления

для CSP VPN Server и CSP VPN Gate такое разрешение не запрашивается.

При получении обновления Клиент управления проверяет на управляемом устройстве тип установленного VPN-продукта, и при наличии CSP VPN Client на панель состояния операционной системы выводится иконка в виде красного флажка и сообщение с просьбой запустить процесс обновления (Рисунок 159).

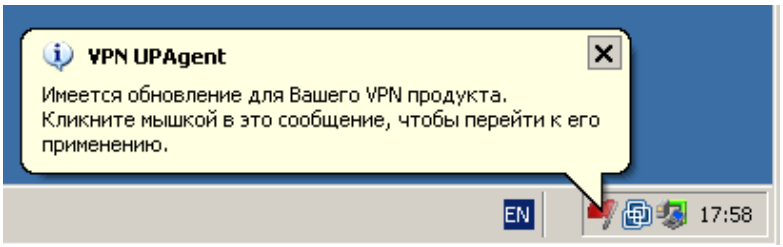

Рисунок 159

Двойное нажатие мышки на этой иконке или теле сообщения приводит к появлению окна **VPN UPAgent** с отображением процесса обновления (Рисунок 160). При нажатии кнопки Применить процесс обновления запустится. В ОС Windows Vista и более новых версиях, нижеприведенные окна будут отображаться в специальном режиме работы ОС, в зависимости от настроек Службы обнаружения интерактивных служб windows.

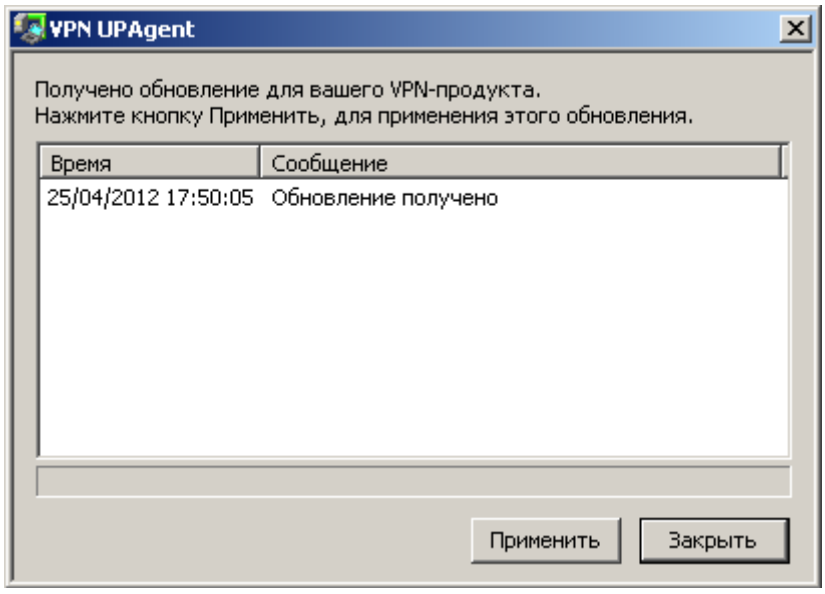

Рисунок 160

Если пароль логина в продукт CSP VPN Client не пустой, то в процессе обновления может запрашиваться пароль для изменения данных в базе продукта CSP VPN Client (Рисунок 161). Необходимо задать пароль и нажать кнопку ОК. При отказе задать пароль - обновление будет считаться неуспешным (все данные будут возвращены в прежнее состояние, сообщение о неудачном обновлении будет отправлено администратору).

Рисунок 161

В окне **VPN UPAgent** отображаются все этапы обновления продукта. При удачном завершении процесса обновления будет выдана строка «Изменения применены успешно».

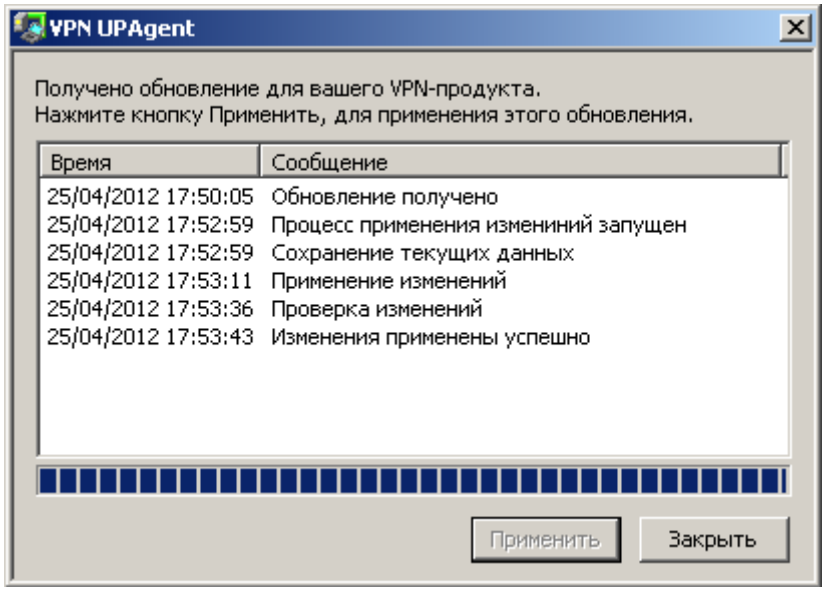

Рисунок 162

А над иконкой с красным флажком появится сообщение «Обновление применено». Через некоторое время это сообщение и иконка исчезнут.

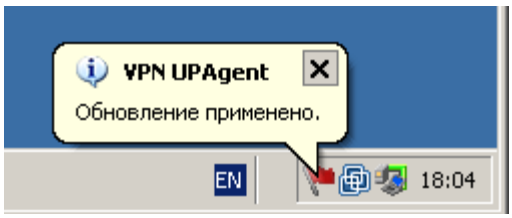

Рисунок 163

При неуспешном обновлении в окне **VPN UPAgent** появится строка «Изменения не применены».

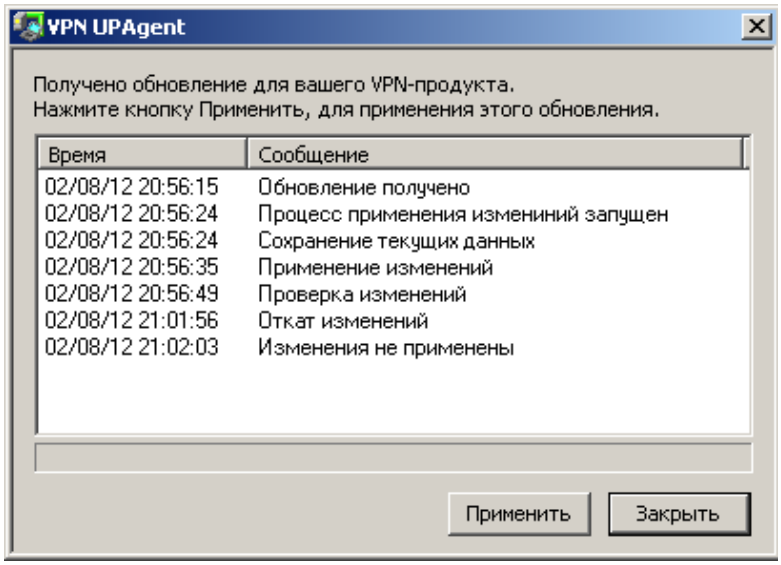

Рисунок 164

А над красным флажком появится сообщение «Обновление не применено». Окно и сообщение через некоторое время исчезнут.

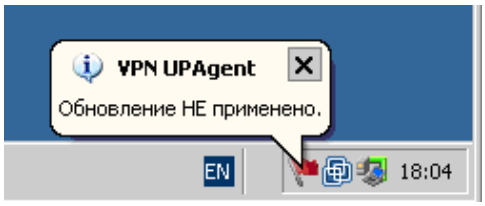

Рисунок 165

11. Сценарий выполнения расширенного обновления

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

```
hostname
```

Для этого надо создать обновление, например, для клиента server01, 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 server01, в контекстном меню выберите предложение ***Update***.

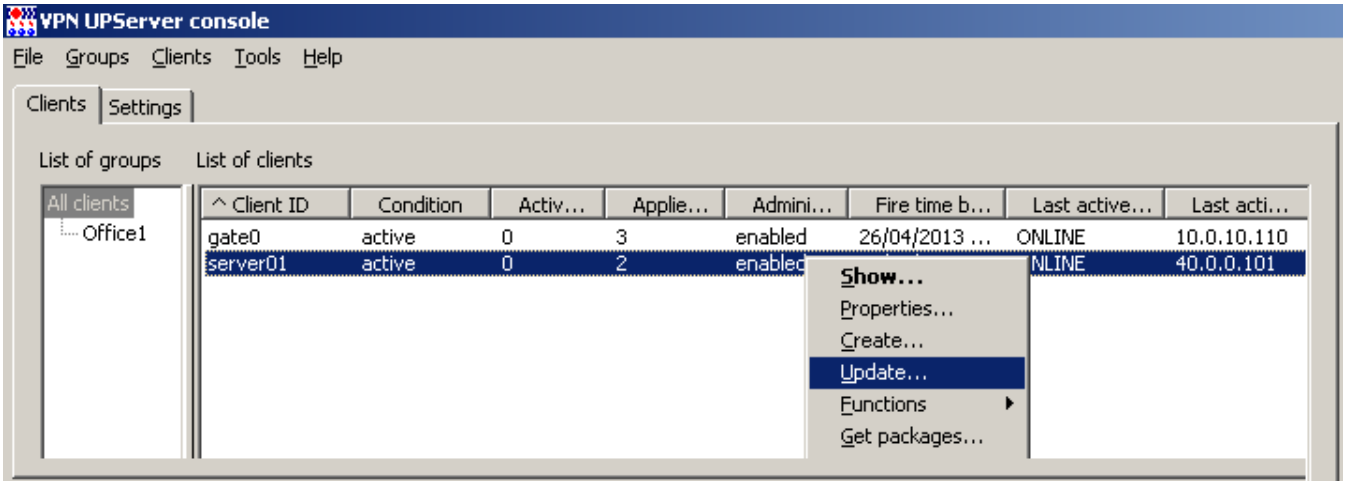

Рисунок 166

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

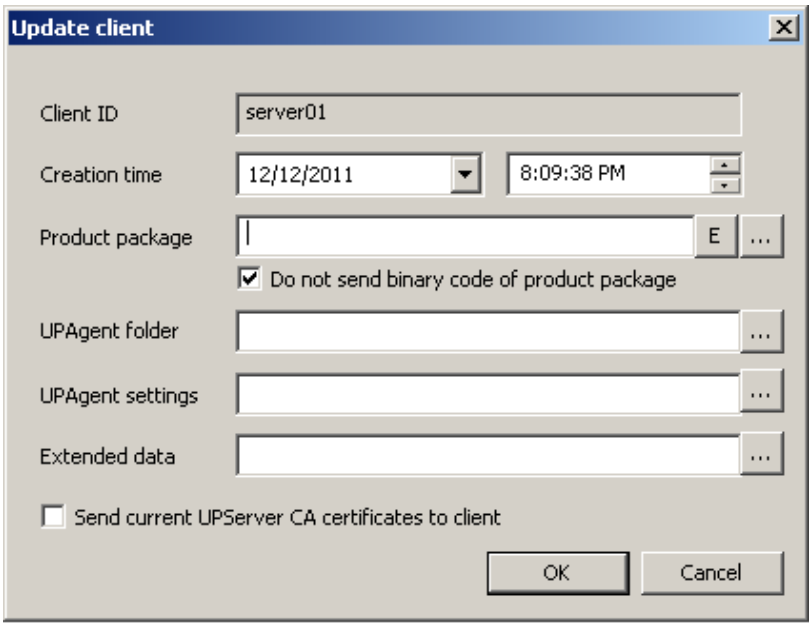

Рисунок 167

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 (CP,SC,ST)

`UPAgentGroup` – идентификатор группы, к которой принадлежит UPAgent

`UPAgentOS` – тип операционной системы, для которой был собран UPAgent (WIN2K,SOLARIS,LINUXRHEL5)

`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 CSP VPN Agent, 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. В поле **Extended data** внесите каталог `C:\test` с файлом `update.bat` и нажмите ОК.

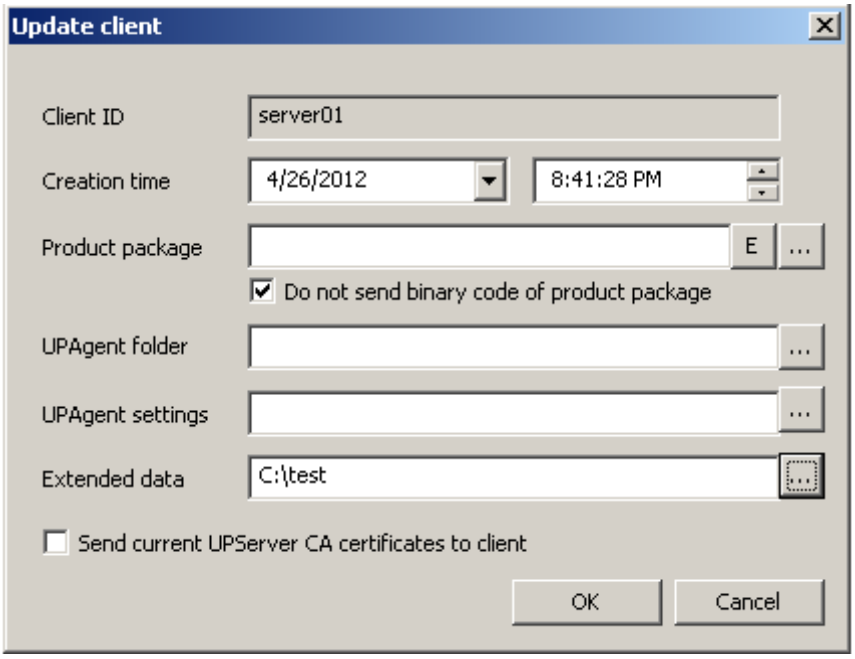

Рисунок 168

5. После нажатия OK будет создано обновление для клиента server01, которое будет скачено Клиентом управления и применено.

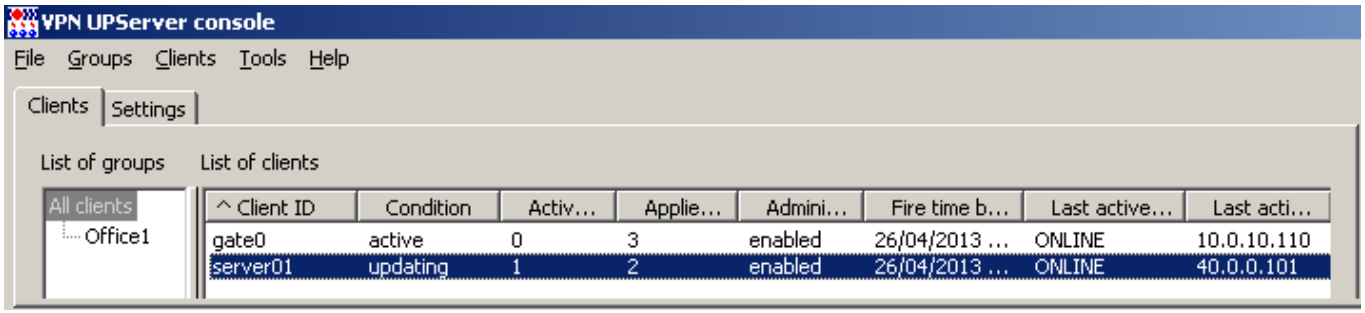

Рисунок 169

6. Результат применения команды **hostname** можно увидеть во вкладке **Uplog** для данного клиента на Сервере управления. В данном примере – это «ServerKP».

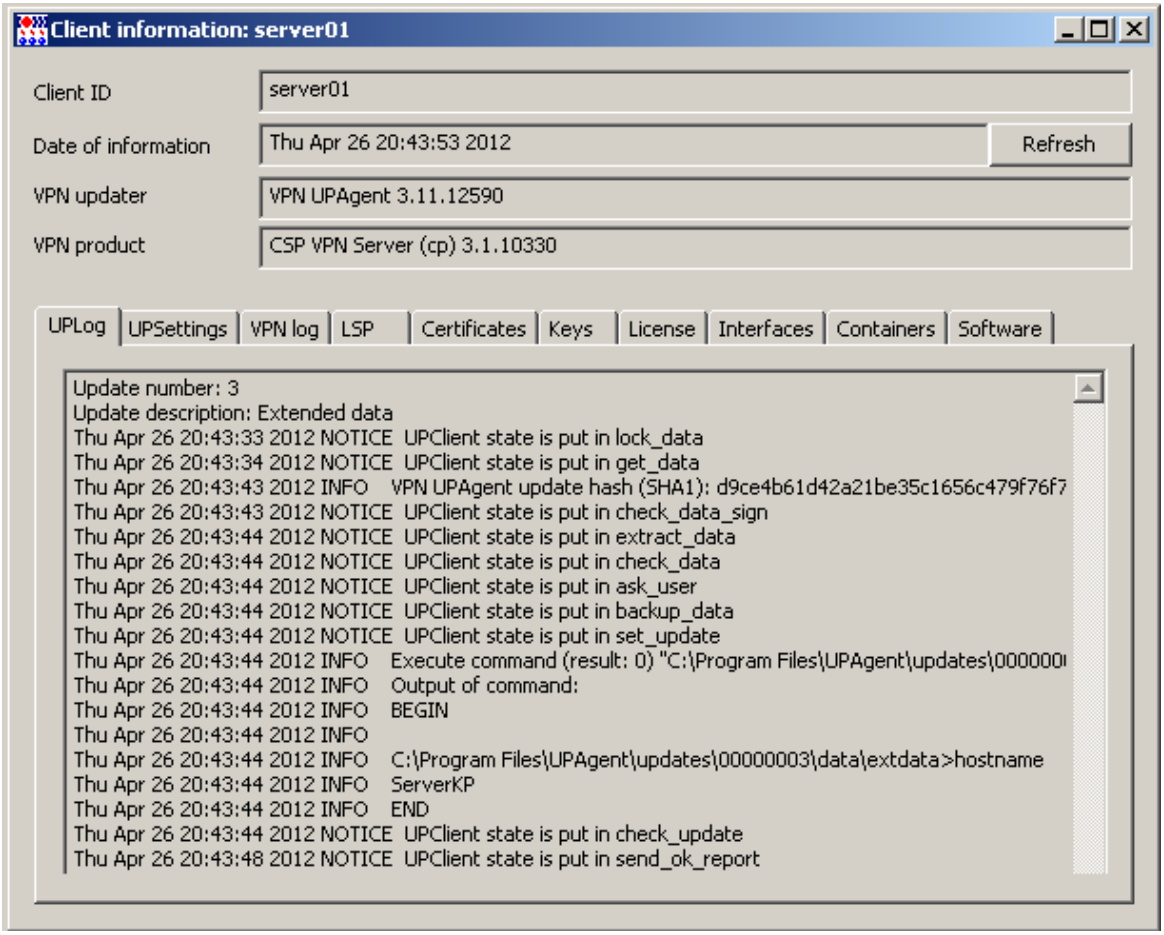

Рисунок 170

12. Настройка и управление СПДС «ПОСТ»

В этом разделе описано управление продуктом CSP VPN Gate, установленным на специальном загрузочном носителе (СЗН) «СПДС-USB-01», который далее будем называть СПДС (среда построения доверенного сеанса) или СПДС «ПОСТ», или управляемое устройство. Подробно сам продукт СПДС «ПОСТ» описан в документе «Программный комплекс «Шлюз безопасности CSP VPN Gate.Версия 3.1» СПДС ПОСТ». СПДС «ПОСТ» - среда построения доверенного сеанса связи для удаленного защищенного доступа к корпоративным ресурсам сети.

Общая схема использования продукта С-Терра КП 3.11 с СПДС «ПОСТ»

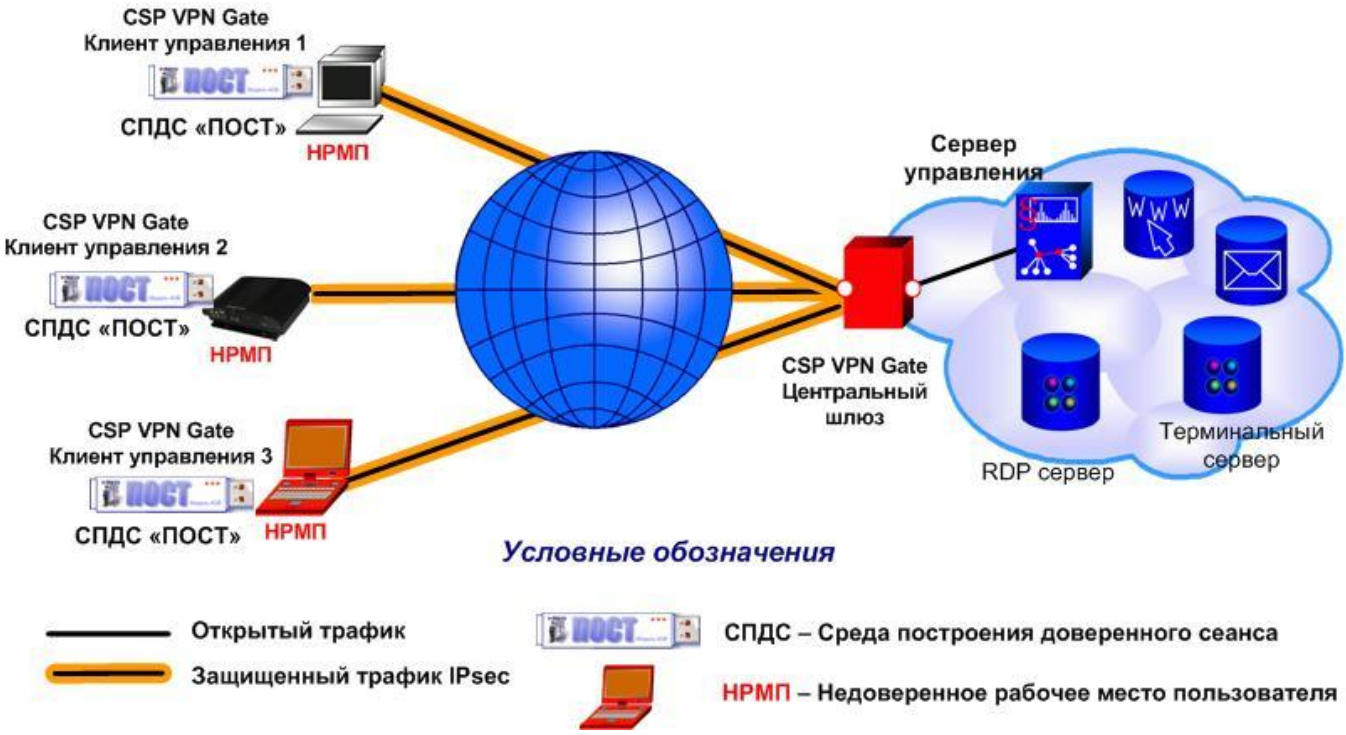

Рисунок 171

Настройка СПДС «ПОСТ» будет описана для следующей схемы стенда (Рисунок 172). В стенд включен центральный шлюз CSP VPN Gate, защищающий подсеть с Сервером управления и RDP-сервером, и компьютер, которому мы не доверяем (НРМП). Имеется устройство СПДС «ПОСТ» с установленной ОС и продуктом CSP VPN Gate. Требуется настроить СПДС «ПОСТ» для защищенного взаимодействия с Сервером управления и RDP-сервером. Недоверенный компьютер следует настроить на загрузку с СПДС «ПОСТ». Настройка СПДС «ПОСТ» должна осуществляться с Сервера управления.

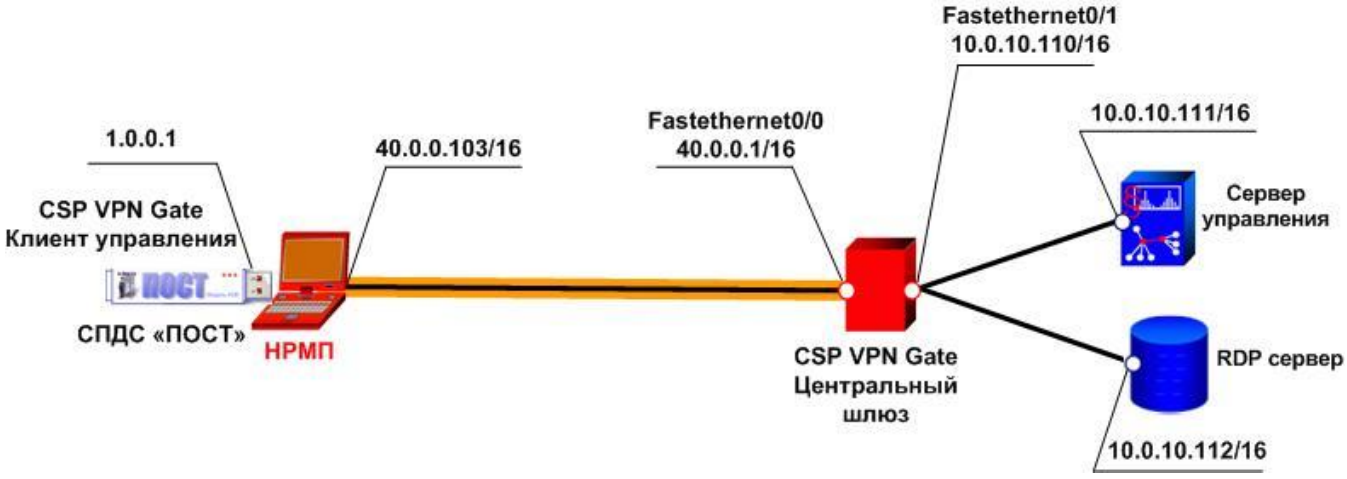

Рисунок 172

12.1. Установка SPDS Editor

На Сервере управления установите продукт SPDS Editor, дистрибутив которого размещен на сайте компании по адресу http://s-terra.com/documents/R311/SPDSEditor/SPDSEditor.rar.

Из загруженного архива запустите файл `SPDSEditor\setup.exe` и в появляющихся окнах нажимайте кнопку Next.

Рисунок 173

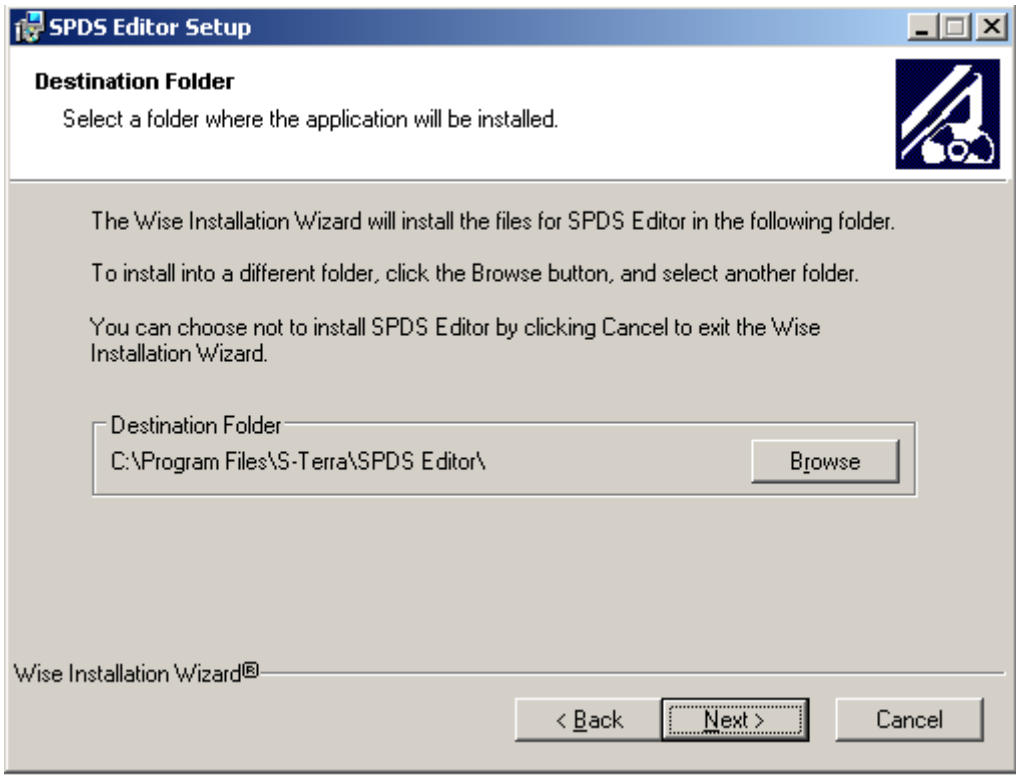

Рисунок 174

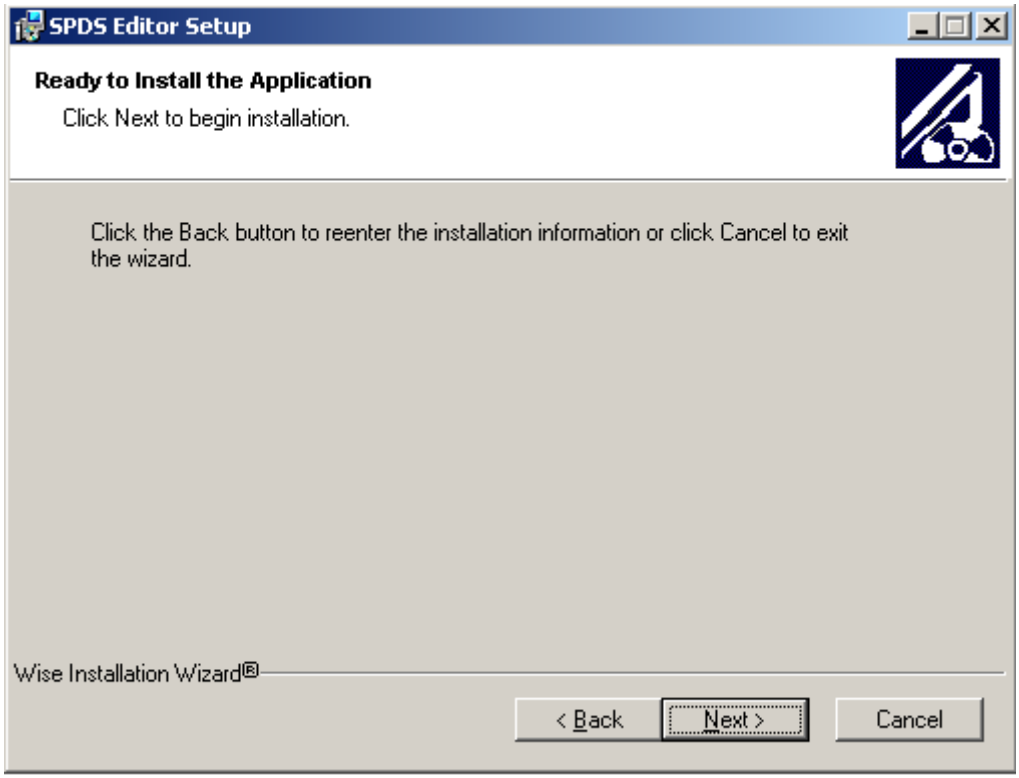

Рисунок 175

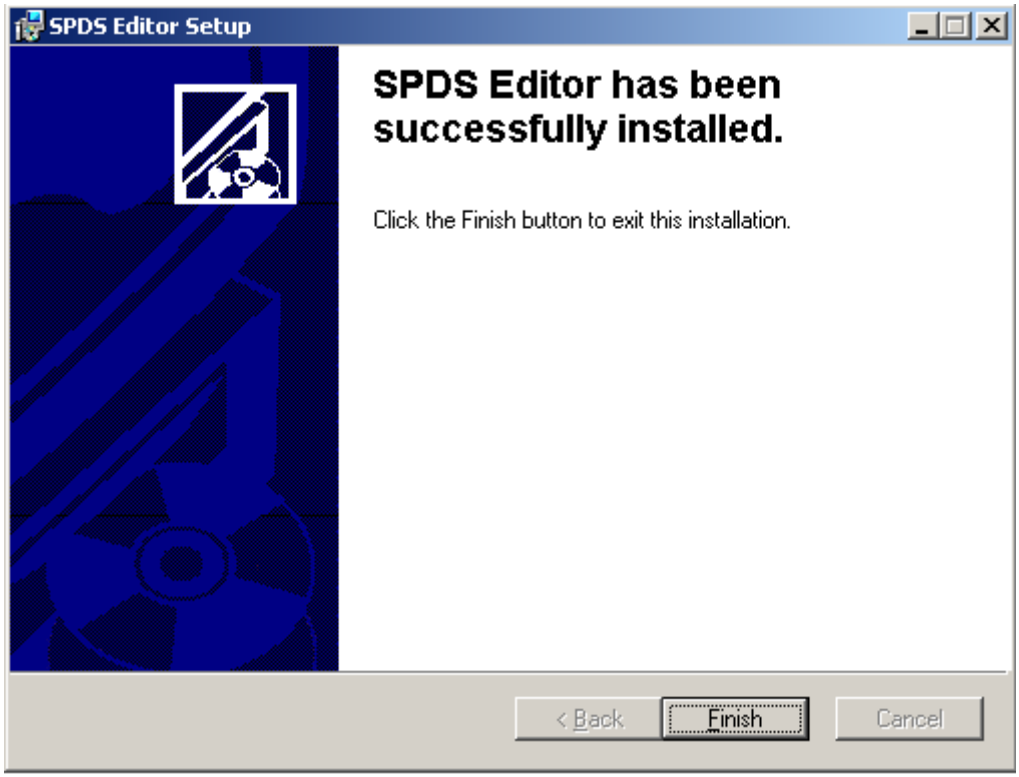

Рисунок 176

Если появится предупреждение 25001 о необходимости установки драйвера CCID, то из каталога `SPDSEditor\Additional` дистрибутива запустите один из размещенных в нем файлов.

12.2. Создание ключевой пары и запроса на сертификат СПДС «ПОСТ»

1. Запустите установленный SPDS Editor – `Пуск-Программы-S-Terra-SPDS Editor-SPDS Editor` (Рисунок 177).

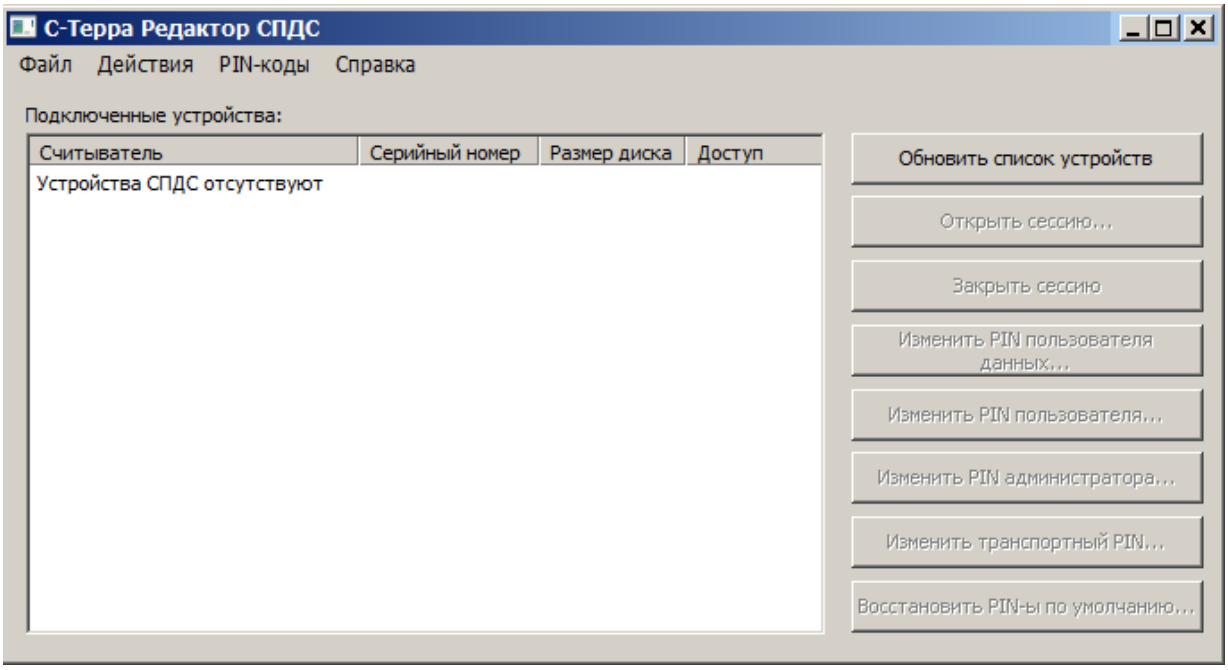

Рисунок 177

Кнопки окна **С-Терра Редактор СПДС** имеют следующие значения:

Кнопка Обновить список устройств – обновляет список доступных устройств в списке устройств.

Кнопка Открыть сессию… - открывает Раздел данных выбранного устройства на запись.

Кнопка Закрыть сессию… - закрывает Раздел данных выбранного устройства от записи.

Кнопка Изменить PIN пользователя данных… - позволяет изменить PIN пользователя Раздела данных выбранного устройства. Этот PIN необходим пользователю для открытия Раздела данных на запись.

Кнопка Изменить PIN пользователя… - позволяет изменить PIN пользователя выбранного устройства. Этот PIN необходим пользователю для аутентификации при загрузке с устройства или для открытия Раздела данных на запись.

Кнопка Изменить PIN администратора… - позволяет изменить PIN администратора выбранного устройства. Этот PIN необходим администратору для изменения PIN устройства (PIN пользователя, PIN пользователя данных, Траспортный).

Кнопка Изменить транспортный PIN… - позволяет изменить транспортный PIN выбранного устройства. Этот PIN необходим для возможности низкоуровневых операций над устройством.

Кнопка Восстановить PIN-ы по умолчанию… - отменяет установленные администратором значения PIN (PIN пользователя, PIN пользователя данных, PIN администратора) и возвращает им заводские значения.

Заводские значения:

PIN пользователя данных - 12345678

PIN пользователя - 12345678

PIN администратора – 12345678

Транспортный PIN – случайное число.

2. Вставьте СПДС «ПОСТ» в USB-разъем Сервера управления.
3. Распознанное устройство появится в окне **С-Терра Редактор СПДС**.
4. Измените заводское значение PIN пользователя данных, нажав кнопку Изменить PIN пользователя данных (Рисунок 178)

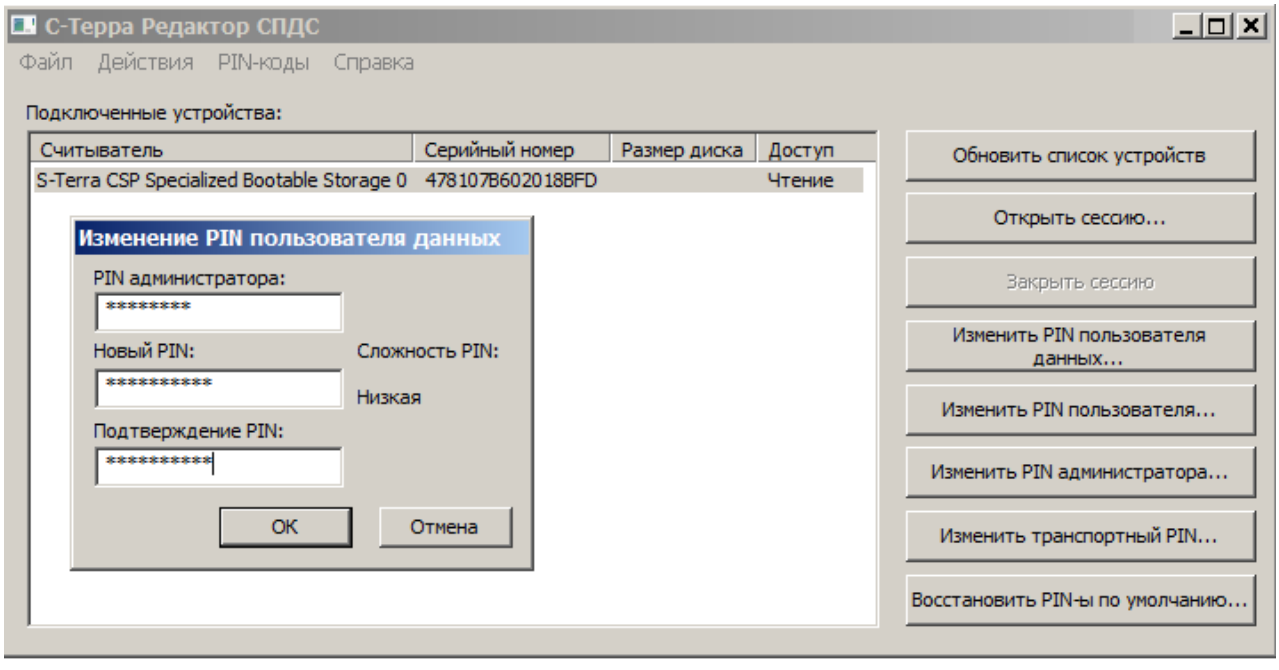

Рисунок 178

5. Нажмите кнопку «Открыть сессию» для открытия Раздела данных на запись.
6. В окне **Авторизация** введите PIN пользователя и нажмите ОК (Рисунок 179).

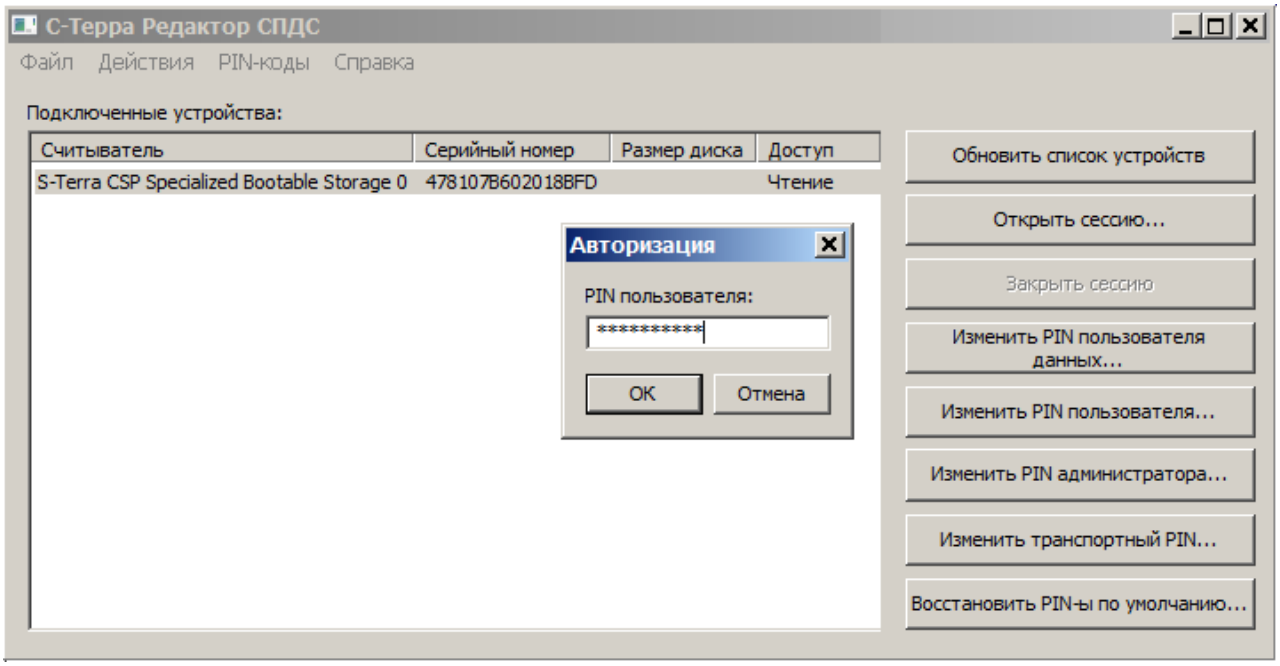

Рисунок 179

7. Устройство СПДС «ПОСТ» готово для записи (Рисунок 180).

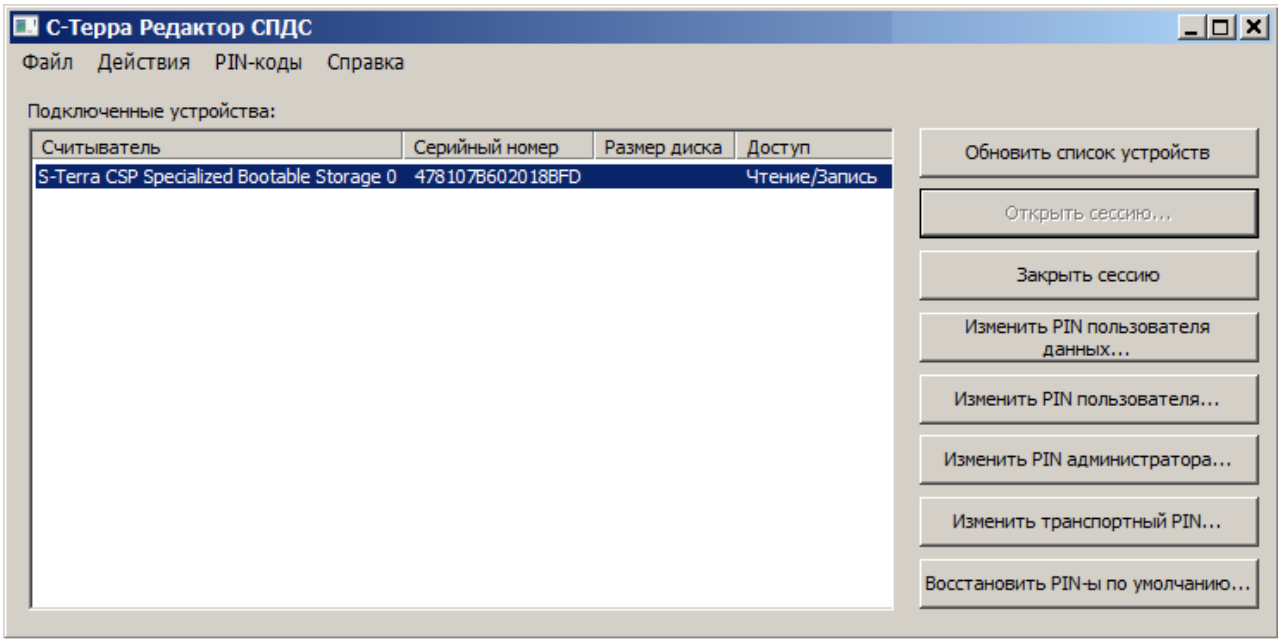

Рисунок 180

8. Далее в СКЗИ «КриптоПро CSP 3.6» инсталлируйте считыватель «Все считыватели смарт-карт».

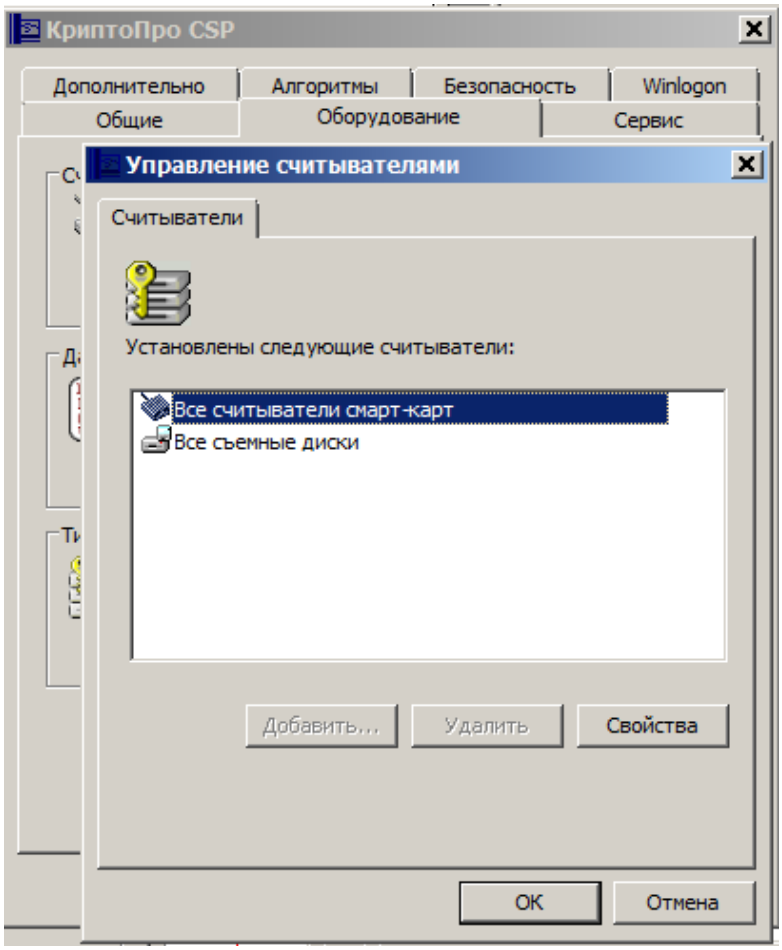

Рисунок 181

9. Далее следует создать ключевую пару и запрос на локальный сертификат СПДС «ПОСТ». Как было описано ранее, можно использовать средства Microsoft Windows CA. На Сервере управления запустите `Microsoft Internet Explorer`, в поле `Address` укажите адрес Удостоверяющего Центра и утилиту `certsrv (Certificate Service)`.

   Для целей тестирования можно настроить Удостоверяющий Центр на Сервере управления (настройка УЦ описана в документе «Приложение» к Программному комплексу CSP VPN Gate). В этом случае наберите `http://127.0.0.1/certsrv/`.

10. В появившемся окне высвечивается имя Удостоверяющего Центра – в нашем случае S-Terra CA. Выберите предложение `Request a certificate`.

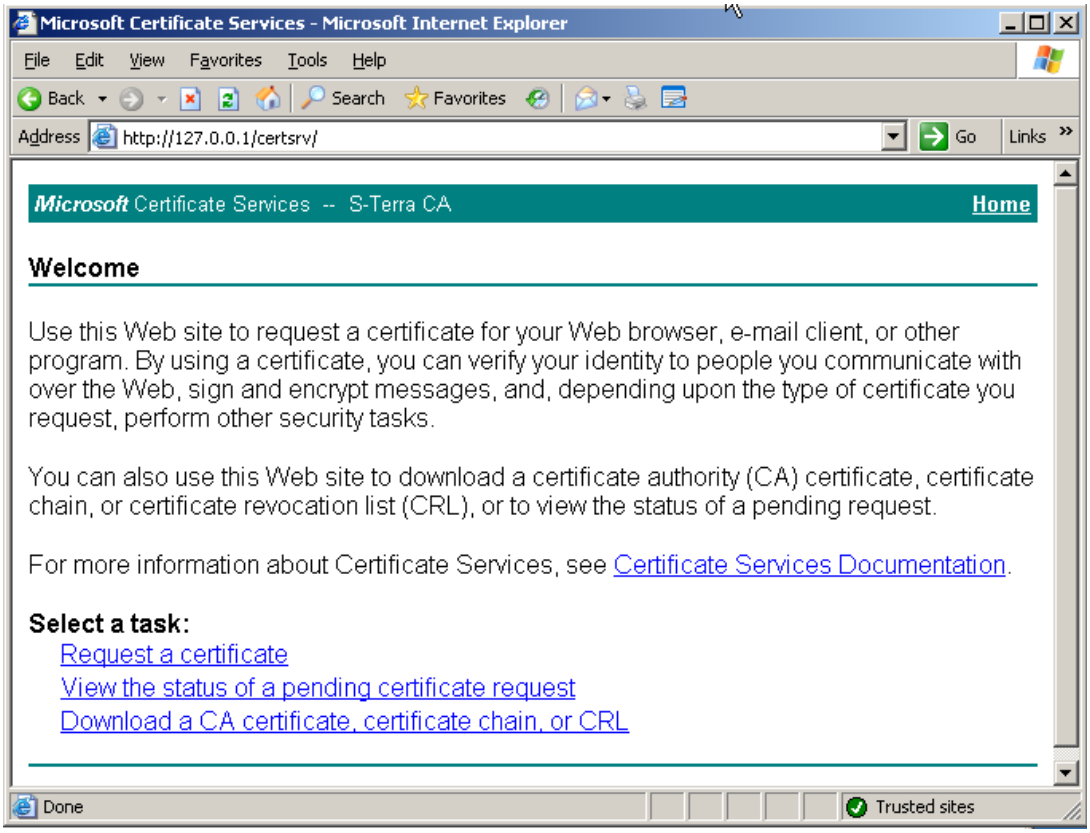

Рисунок 182

11. Далее выберите форму расширенного запроса – предложение "`advanced certificate request`".

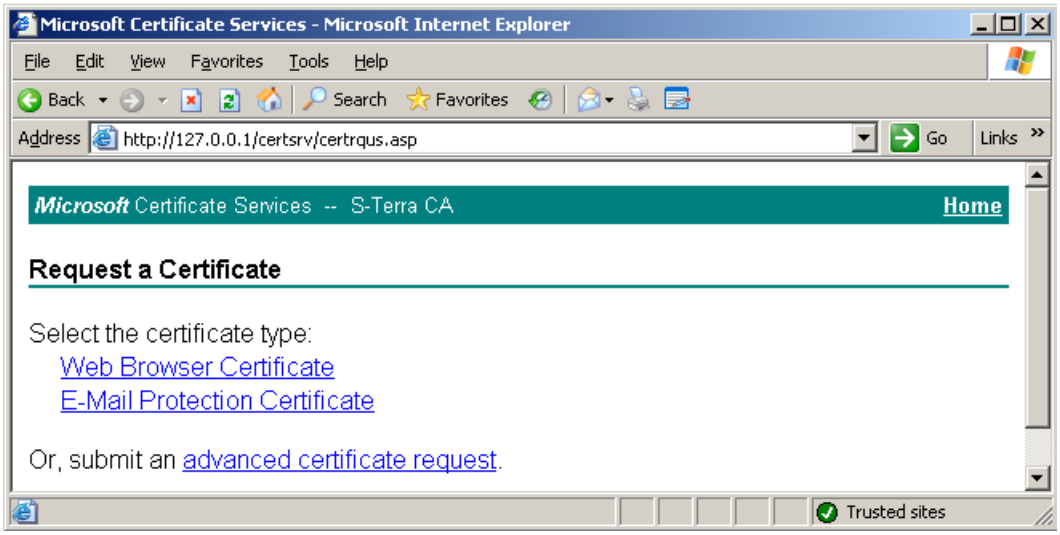

Рисунок 183

12. Для получения формы выберите предложение "`Create and submit a request to this CA`".

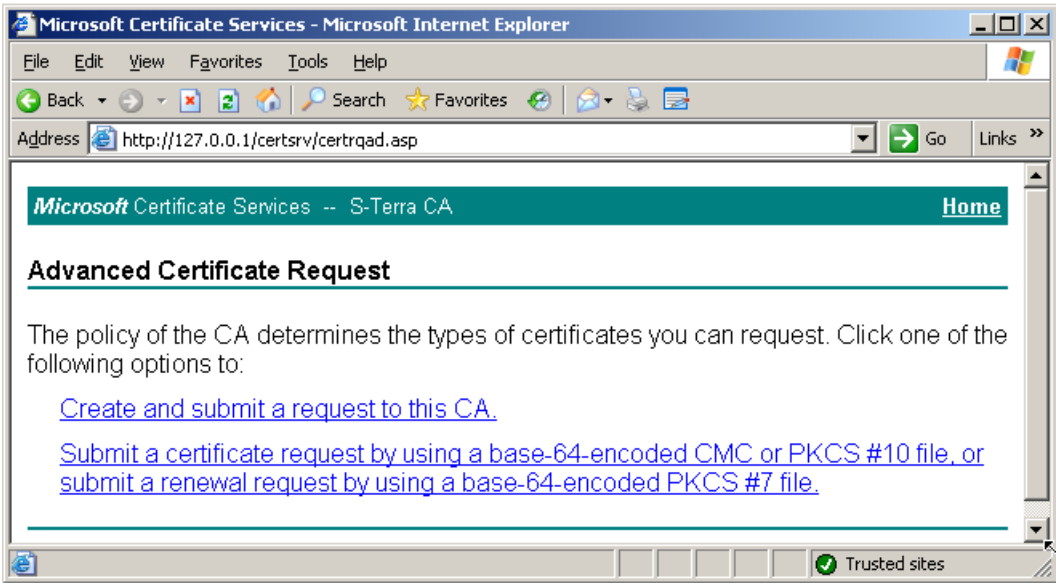

Рисунок 184

13. Заполните форму расширенного запроса (Рисунок 185). Дадим некоторые пояснения для ее заполнения:

- в разделе **Identifying Information** (Информация о Владельце Сертификата) внесите данные о владельце сертификата. Во всех полях этого раздела разрешается использовать не только латинские, но и русские буквы, кроме поля Country/Region, оно всегда содержит значение RU.
- в разделе **Type of Certificate Needed** (Тип требуемого сертификата) из выпадающего списка выберите предложение ***IPSec Certificate***
- в разделе **Key Options** (Опции создания ключей) выбираются опции для создания ключевой пары и размещения секретного ключа. Рекомендуется сделать следующий выбор:
  - Поставьте переключатель в положение ***Create new key set*** (Создать установки для нового секретного ключа)
  - CSP (Тип Криптопровайдера) – из выпадающего списка выберите ***Crypto-Pro GOST R 34.10-2001 Cryptographic Service provider***
  - Key Usage (Использование ключей) – для выбора типа ключа поставьте переключатель в положение ***Both*** (для подписи и обмена)
  - Key Size (Размер ключа) – размер ключа. При выборе алгоритма GOST R 34.10-2001 длина ключа всегда ***512***
  - поставьте переключатель в положение ***Automatic key container name***, чтобы имя контейнера с секретным ключом задавалось автоматически
  - ***Mark keys as exportable*** – поставьте флажок, чтобы можно было скопировать контейнер с секретным ключом
- в разделе **Additional Options** (Дополнительные опции):
  - request Format - ***CMC***
  - Hash Algorithm – выбрать ***GOST R 34.11-94***

14. Нажмите кнопку Submit.

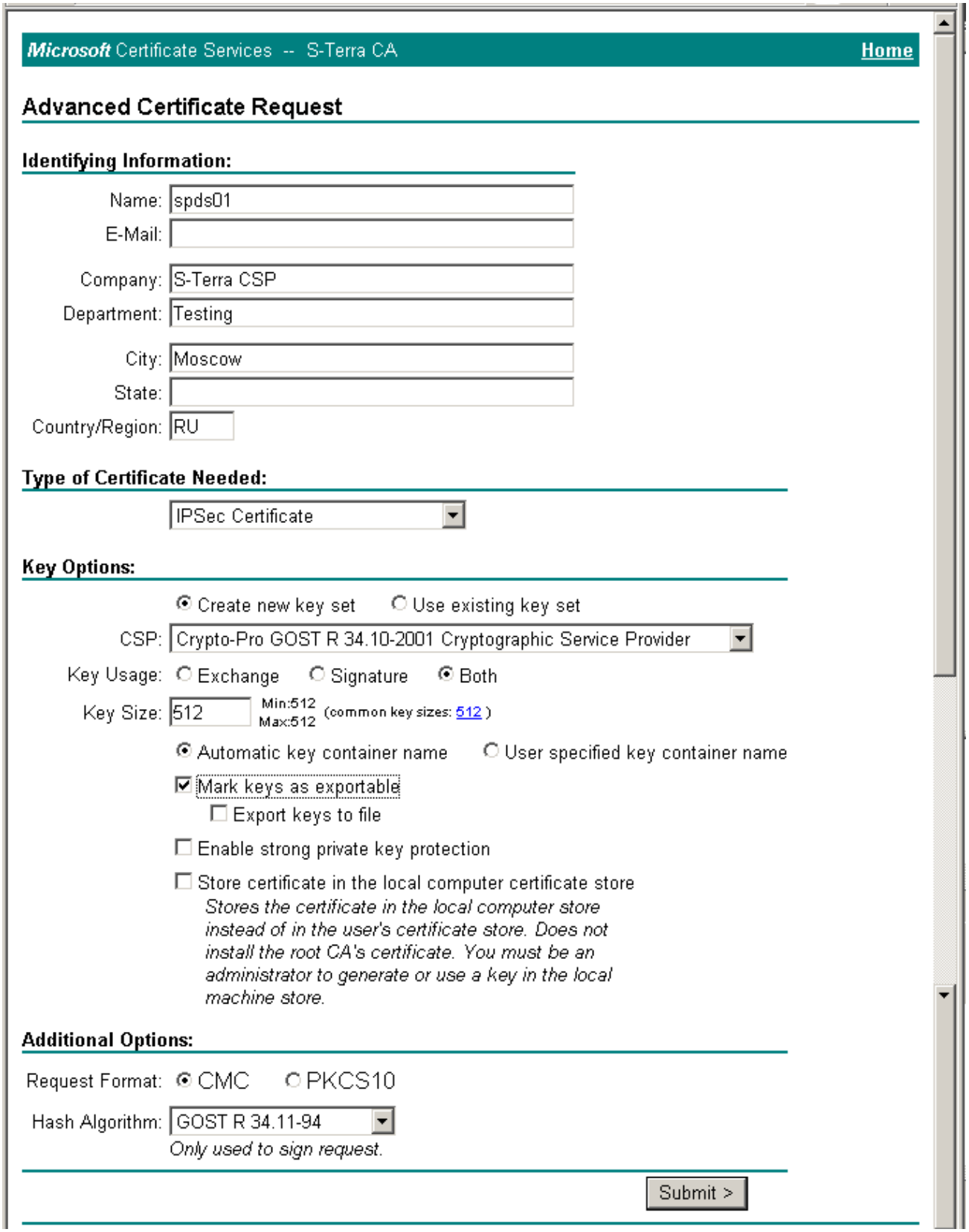

Рисунок 185

15. На следующем предупреждении нажмите кнопку Yes.

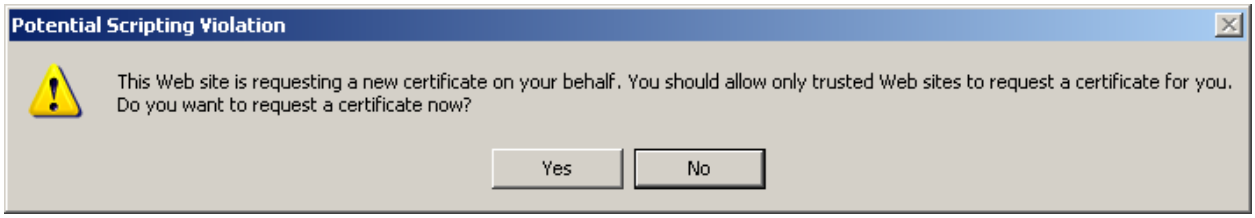

Рисунок 186

16. В следующем окне укажите ключевой носитель, соответствующий СПДС «ПОСТ», и нажмите OK.

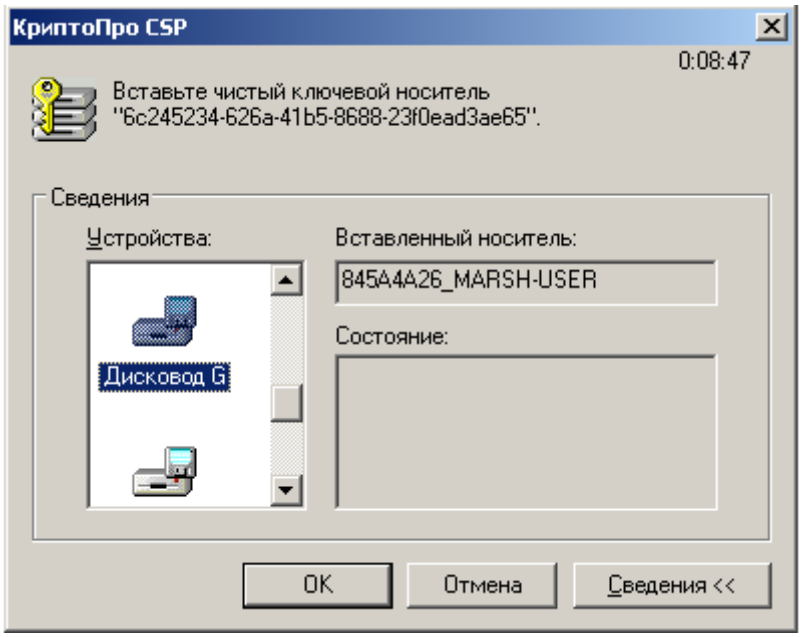

Рисунок 187

17. Если используется биологический ДСЧ, то нажимайте клавиши или перемещайте указатель мыши, если используется аппаратный генератор ДСЧ, то это окно не появляется.

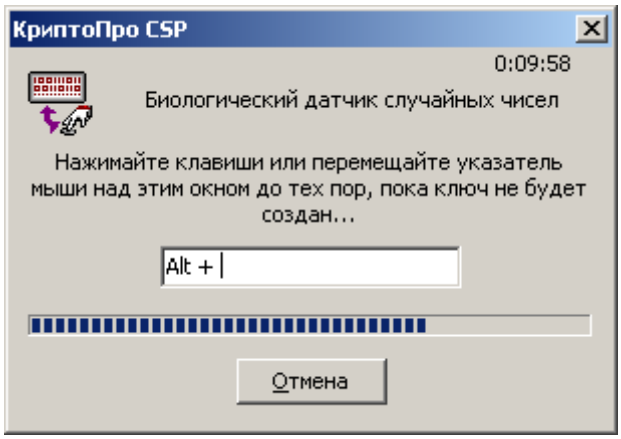

Рисунок 188

18. В окне запроса пароля поля оставьте пустыми, чтобы можно скопировать контейнер при инициализации устройства СПДС (Рисунок 189).

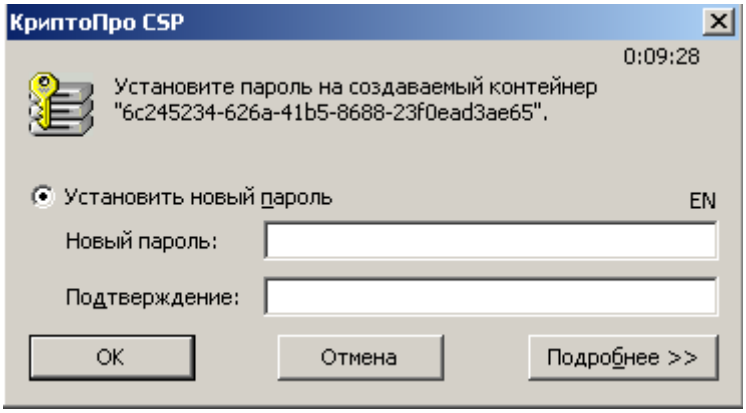

Рисунок 189

19. Если на Удостоверяющем Центре сертификаты выпускаются автоматически при получении запроса, то появляется окно с предложением установить сертификат. В этом случае выберите предложение `Install this certificate`.

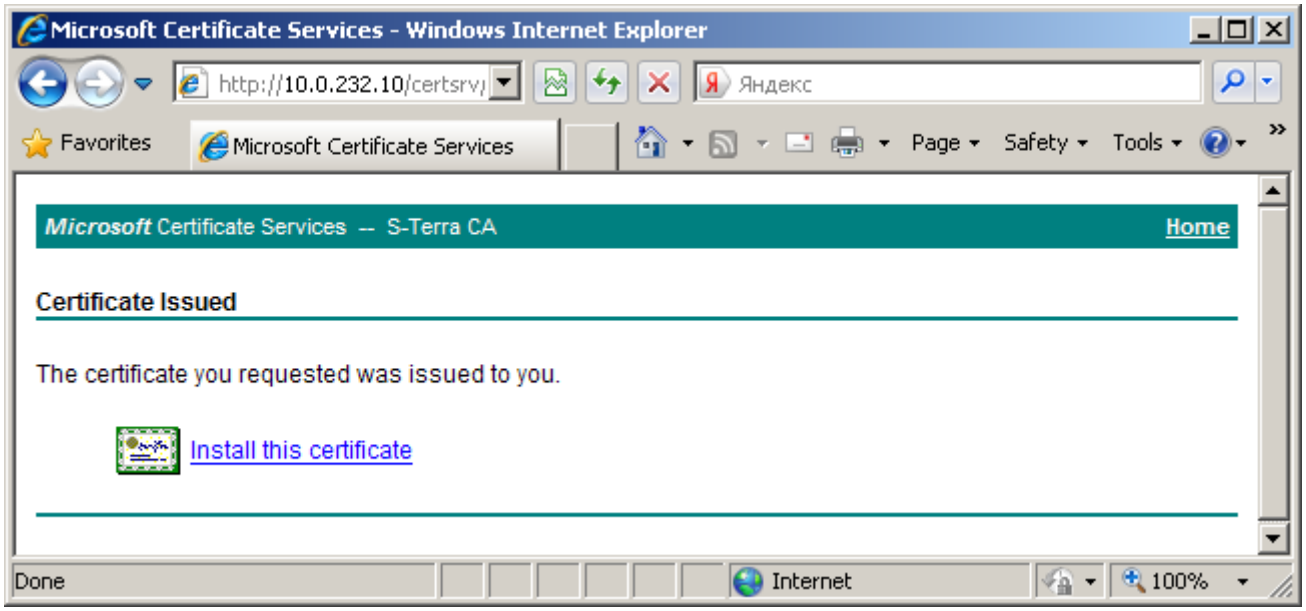

Рисунок 190

В результате сертификат будет записан на СПДС «ПОСТ» в тот же контейнер, что и ключевая пара.

20. Экспортируйте локальный сертификат из контейнера в файл на Сервер управления, так как он будет необходим для настройки СПДС «ПОСТ».
21. Также экспортируйте CA сертификат в файл на Сервер управления.

12.3. Создание настроек для СПДС «ПОСТ»

На устройстве СПДС «ПОСТ» установлена ОС и продукт CSP VPN Gate. Для настройки СПДС нужно создать два скрипта для инициализации CSP VPN Gate, создания политики безопасности и настроек. Все это выполняется на Сервере управления.

1. На Сервере управления запустите консоль **UPServer Console** (`Пуск-Программы-S-Terra-S-Terra KP-VPN UPServer Console`). Во вкладке **Clients** в контекстном меню (правая кнопка мыши) выберите предложение ***Create*** для создания учетной записи клиента для устройства СПДС «ПОСТ».

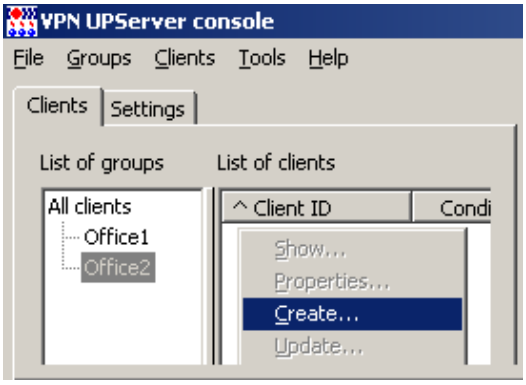

Рисунок 191

2. В окне создания нового клиента **Create new client** в поле **Client ID** укажите идентификатор клиента для СПДС «ПОСТ», например, `spds01` и нажмите кнопку E.

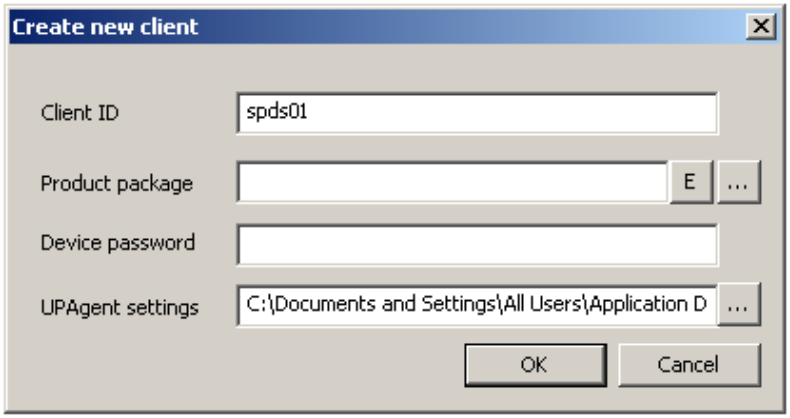

Рисунок 192

3. В окне **VPN data maker** выберите продукт **CSP VPN Gate 3.1 on token** и криптопровайдера CryptoPro. Нажмите кнопку Run Wizard, чтобы использовать окна мастера.

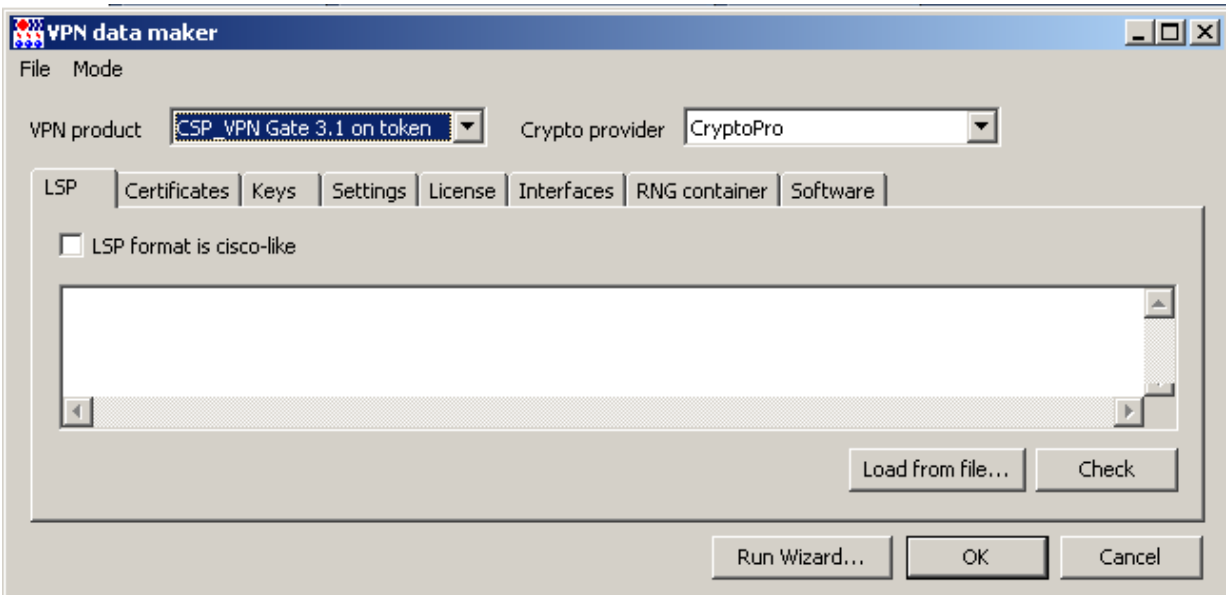

Рисунок 193

4. В первом окне мастера выберите метод аутентификации сторон с использованием сертификатов (Рисунок 194):

   В поле **CA certificate file** нажмите кнопку [...], в открывшемся окне выберите файл с CA сертификатом. Обязательный параметр.

   В поле **Device certificate file** нажмите кнопку [...], в открывшемся окне выберите файл с локальным сертификатом для СПДС. Обязательный параметр.

   В поле **Device container name** отображается местоположение и имя ключевого контейнера, с которым он будет скопирован на СПДС во время инициализации CSP VPN Gate.

   В поле **Device container password** укажите пароль к контейнеру, который будет скопирован при инициализации.

   В поле **Key type** установите значение Autodetect – тип ключа будет определяться автоматически при первом обращении к контейнеру секретного ключа.

   В поле **Device identity type** укажите тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Укажите значение Distinguished Name – в качестве идентификатора партнеру будет высылаться значение поля Subject из локального сертификата управляемого устройства, показываемое в поле Device identity value, если оно задано в сертификате.

   В поле **Device identity value** показывается значение поля Subject из локального сертификата. Нажмите кнопку Next.

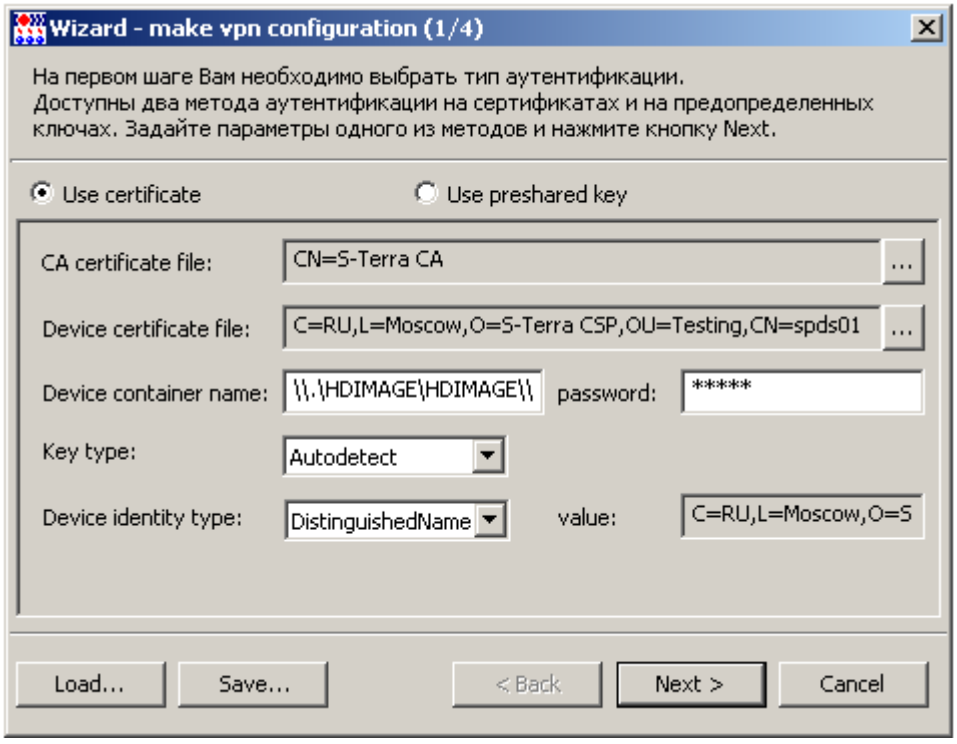

Рисунок 194

5. Во втором окне мастера (Рисунок 195) задайте правило, которое будет пропускать трафик от СПДС «ПОСТ» к Серверу управления и другим ресурсам в защищаемой подсети 10.0.0.0/16. Трафик между СПДС «ПОСТ» и центральным шлюзом должен защищаться по протоколу IPsec, для этого нажмите кнопку Add.

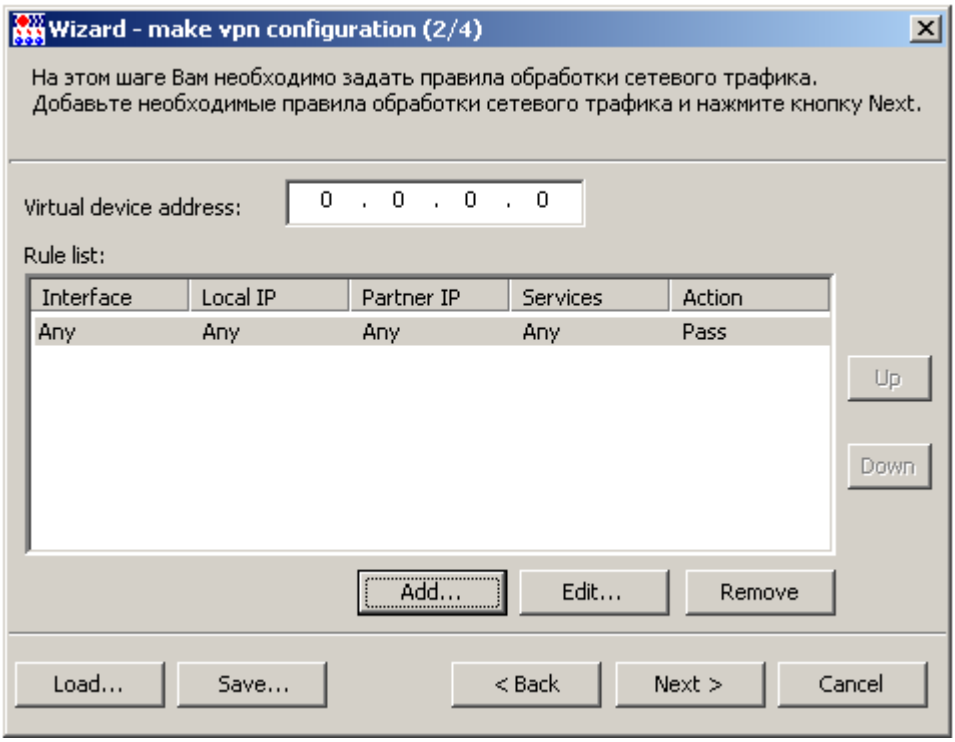

Рисунок 195

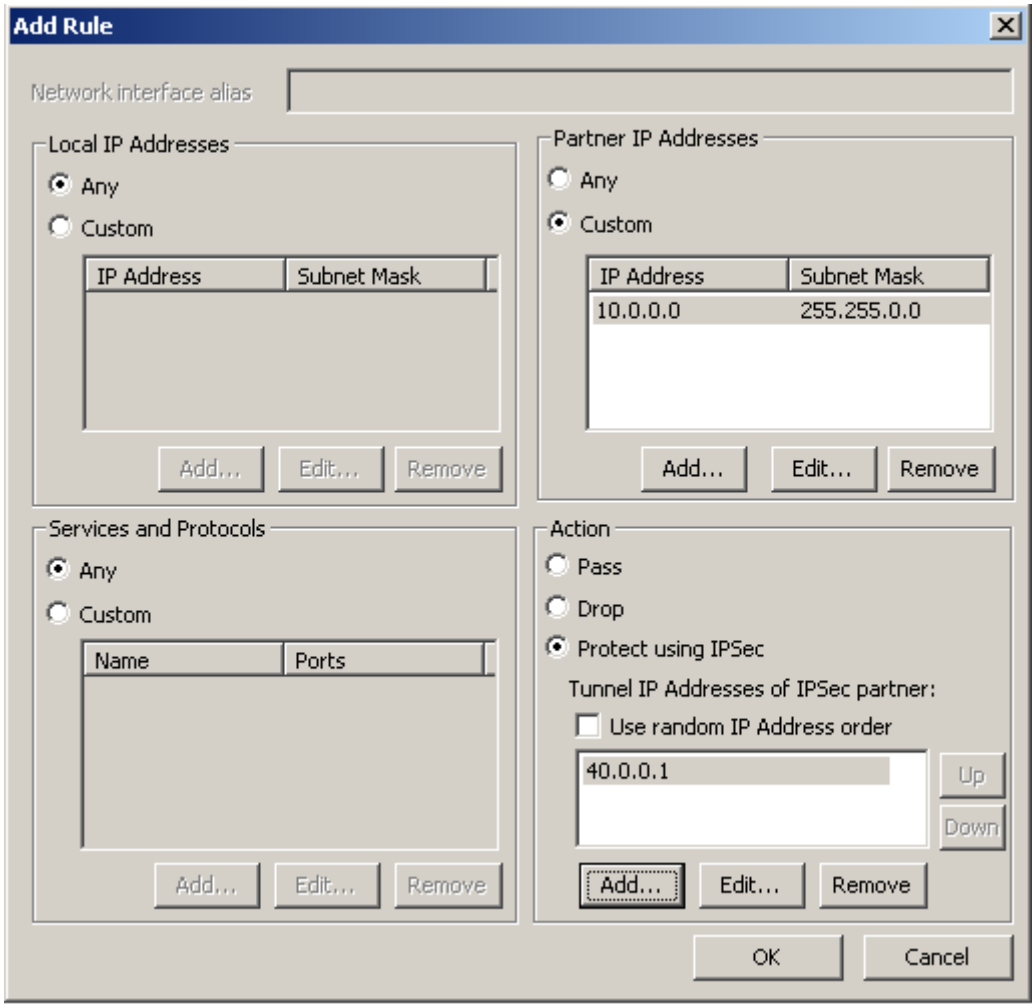

Рисунок 196

6. В окне **Add Rule** (Рисунок 196) укажите следующее:
   - в области **Local IP Addresses** поставьте переключатель в положение Any
   - в области **Partner IP Addresses** – в положение Custom и укажите адрес всей подсети Сервера управления, например, 10.0.0.0/16
   - в области **Services and Protocol** – положение Any
   - в области **Action** – укажите IPsec-партнера, с которым будет построено защищенное соединение. В нашем случае – это адрес интерфейса шлюза 40.0.0.1, защищающего подсеть с Сервером управления.

   Нажмите кнопку OK.
7. Увеличьте приоритет созданного правила, используя кнопку Up(Рисунок 197).
8. В поле **Virtual device address** укажите виртуальный адрес, с которым будут приходить пакеты от СПДС «ПОСТ» в защищаемую подсеть с Сервером управления и другими защищаемыми ресурсами, например, 1.0.0.1. Нажмите кнопку Next.

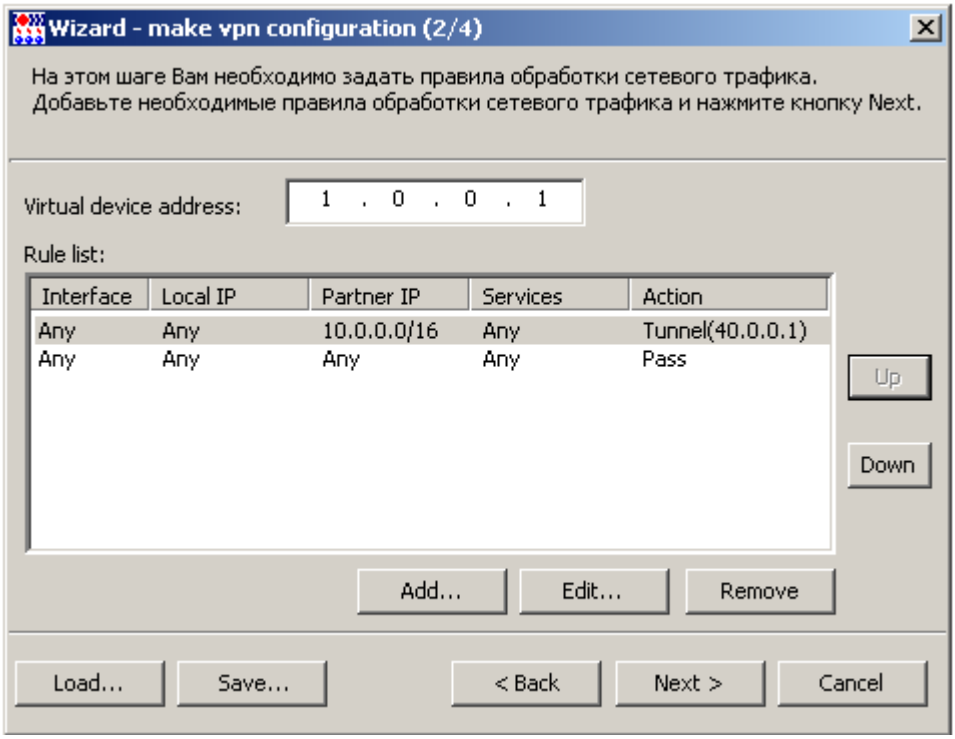

Рисунок 197

9. В третьем окне мастера (Рисунок 198) укажите настройки целевого ПО, установленного на СПДС «ПОСТ», и сетевые настройки. Выберите клиента (Web-client,RDP-client,Other), в качестве которого будет выступать СПДС «ПОСТ», и адрес защищаемого сервера, к которому осуществляется удаленный доступ с СПДС «ПОСТ». Укажите имя пользователя, который будет иметь доступ к серверу. Сетевые настройки можно подготовить заранее, записав в файлы, и указать каталог в поле **Folder of network profiles**. Если сетевые настройки не указывать, то пользователю самому придется выполнять их.

   Если СПДС «ПОСТ» выступает в качестве RDP клиента, то поставьте переключатель в это положение и укажите адрес RDP-сервера, например, 10.0.10.112 (в той же подсети, что и Сервер управления). Для целей тестирования в качестве RDP-сервера может выступать хост с установленной ОС Windows XP и установленной настройкой для общего доступа (Система-Удаленные сеансы-Разрешить удаленный доступ к этому компьютеру).

   Для поля **Folder of network profiles** в качестве примера подготовлены профайлы с сетевыми настройками, которые можно выбрать из каталога: `C:\Documents and Settings\All Users\Application Data\UPServer\NetworkManager\Sample of profiles` или задать свои. Сетевые настройки соединения можно будет задать позже в окне VPN data maker во вкладке Interfaces.

Нажмите кнопку Next.

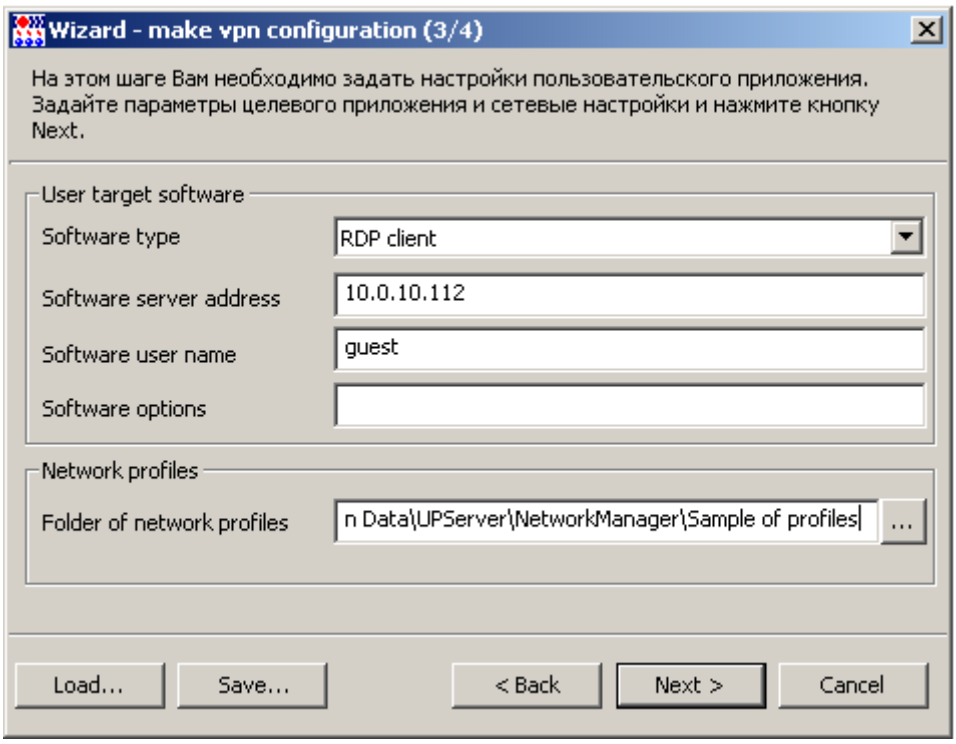

Рисунок 198

10. В следующем окне укажите лицензионные данные на продукт CSP VPN Gate 3.1 и СКЗИ «КриптоПро CSP 3.6».

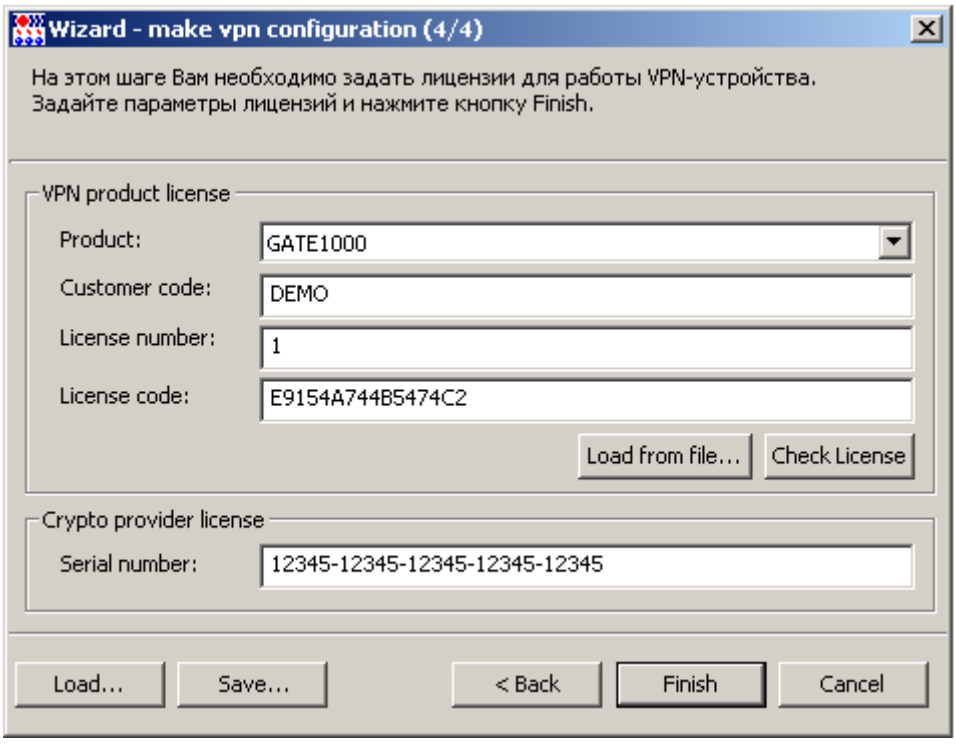

Рисунок 199

11. Далее нажмите кнопку Save для сохранения данных проекта (Рисунок 200).

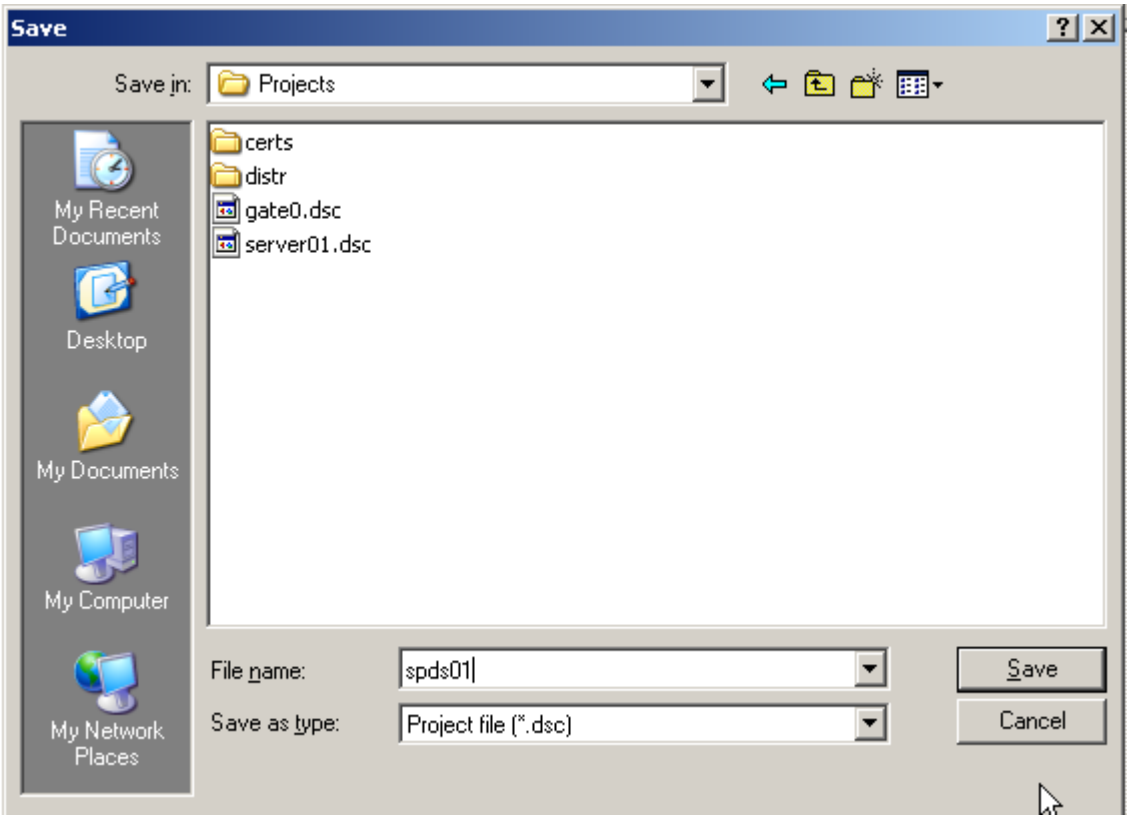

Рисунок 200

12. Затем нажмите кнопку Finish (Рисунок 199).
13. В появившемся окне **VPN data maker** перейдите во вкладку **Interfaces** для задания сетевых настроек соединений, если они не были заданы ранее с использованием профайлов, в противном случае - нажмите кнопку OK.

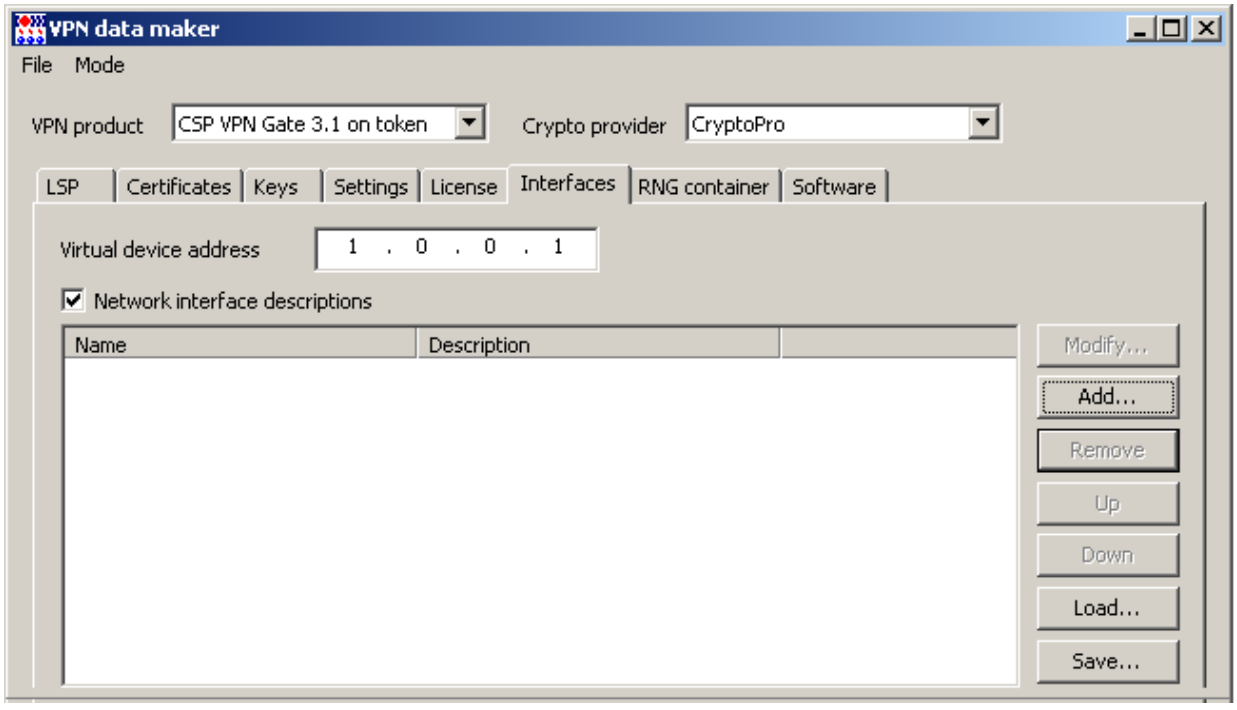

Рисунок 201

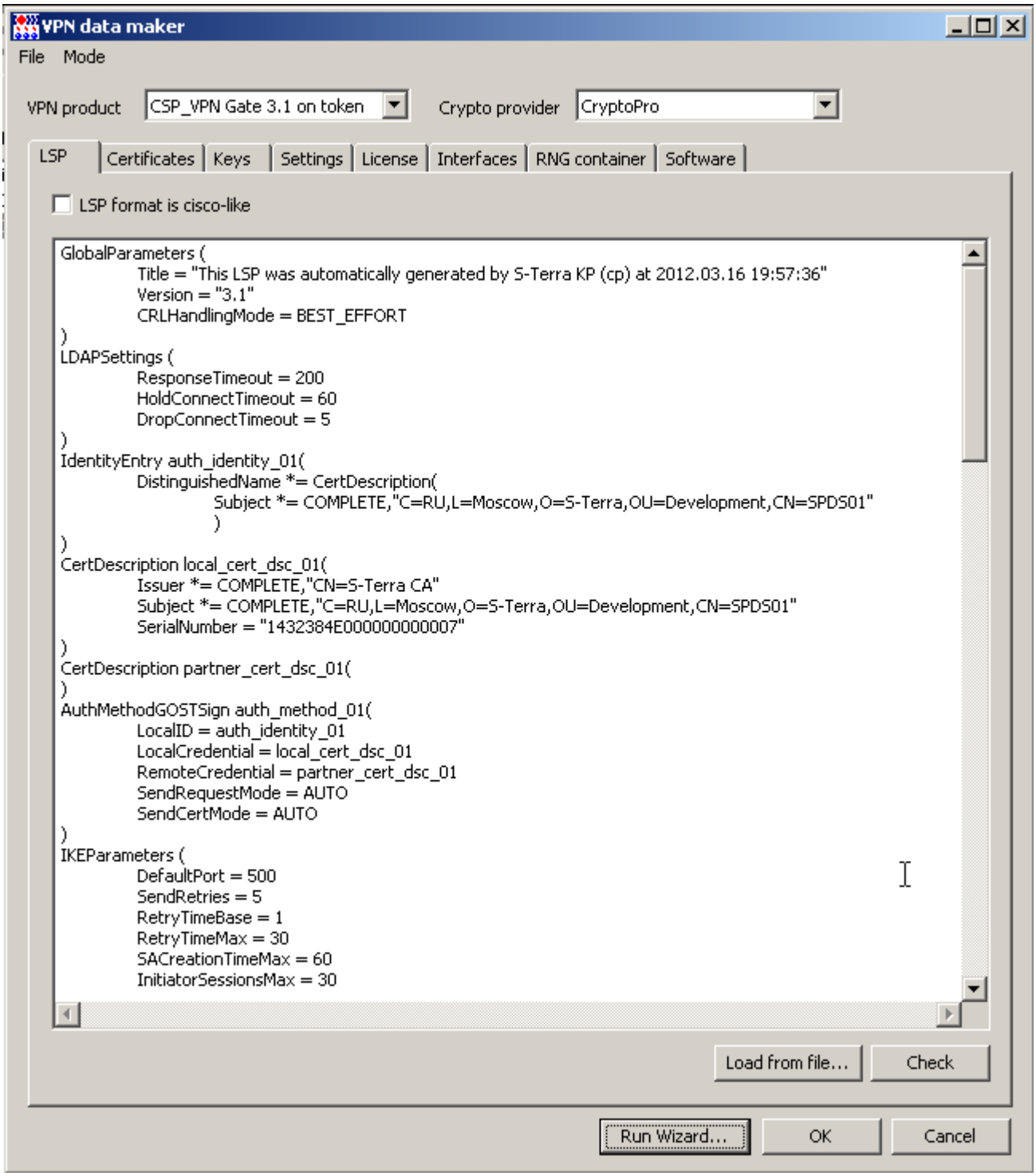

Рисунок 202

14. В окне создания нового клиента также нажмите кнопку OK (Рисунок 203).

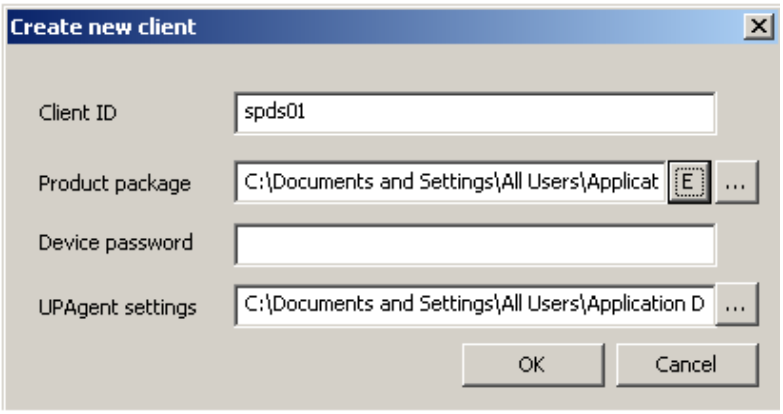

Рисунок 203

15. На Сервере управления выделите строку с новым клиентом и в контекстном меню выберите предложение ***Enable***, чтобы активировать клиента (Рисунок 204).

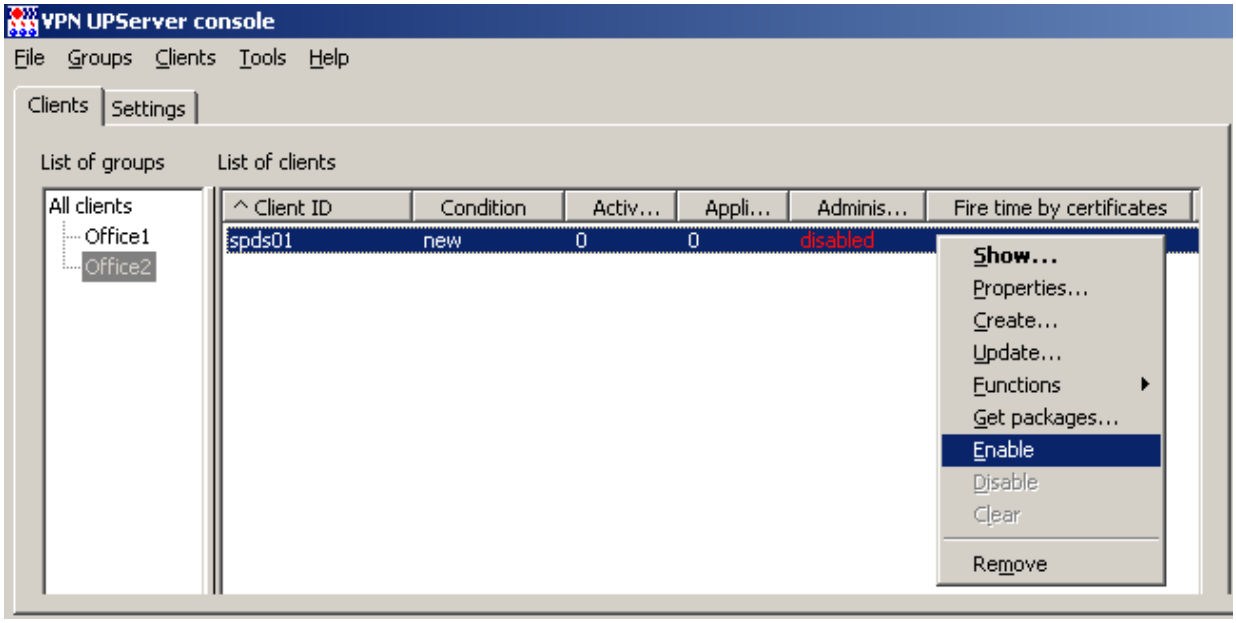

Рисунок 204

Note

На всех устройствах, через которые будет проходить трафик от СПДС «ПОСТ», должен быть прописан обратный маршрут до адреса 1.0.0.1.

16. На центральном шлюзе в таблицу маршрутизации внесите маршрут для доступа к адресу 1.0.0.1:

```
route add -host 1.0.0.1 gw 40.0.0.1
```

12.4. Подготовка скриптов для Клиента управления и CSP VPN Gate

1. Для инсталляции Клиента управления, дистрибутив которого размещен на СПДС «ПОСТ» в каталоге `/packages`, и инициализации CSP VPN Gate следует подготовить два скрипта. В таблице выделите клиента `spds01` и в контекстном меню выберите предложение ***Get packages*** .

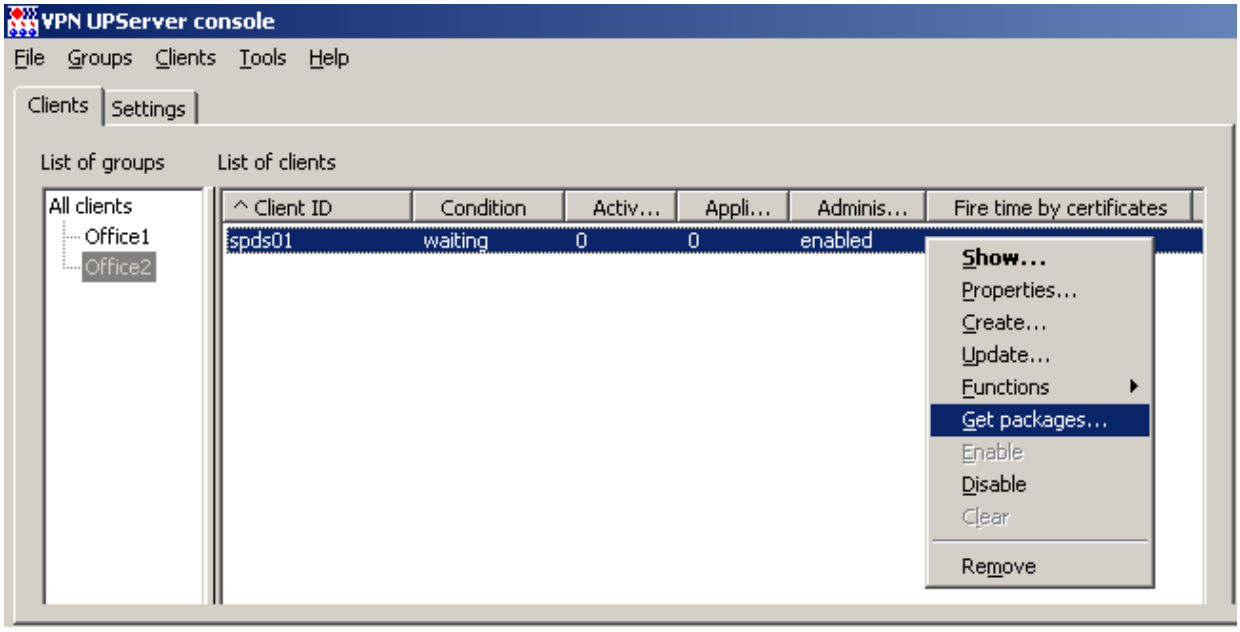

Рисунок 205

2. В открывшемся окне укажите каталог на Сервере управления, в который будут сохранены скрипты.

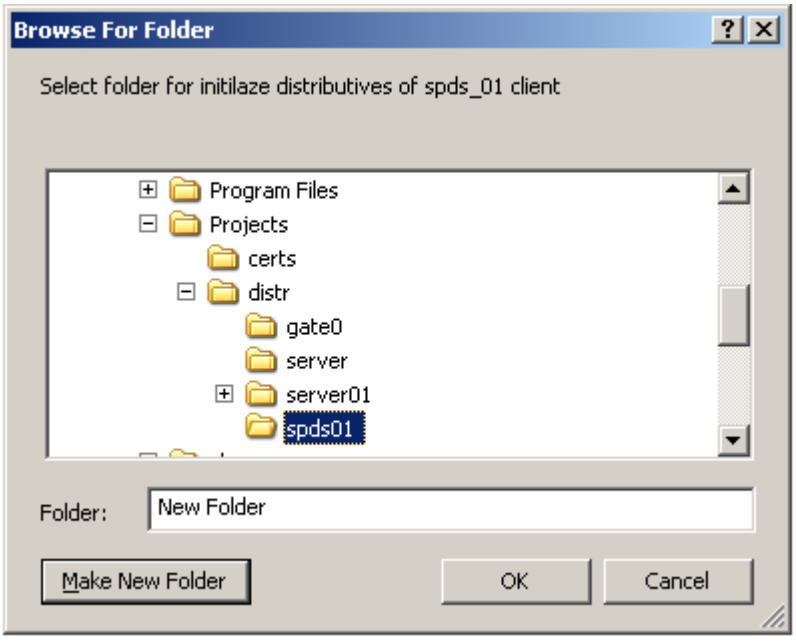

Рисунок 206

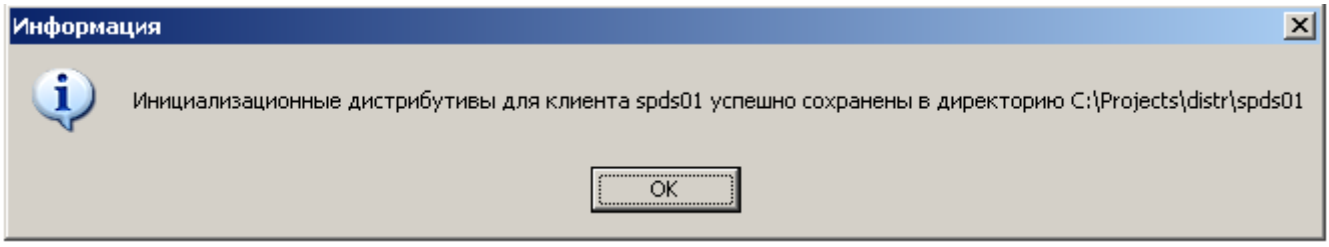

Рисунок 207

3. Два файла будут сохранены в указанный каталог:
   - `setup_product.sh` – скрипт для инициализации продукта CSP VPN Gate
   - `setup_upagent.sh` – скрипт, содержащий данные для Клиента управления.

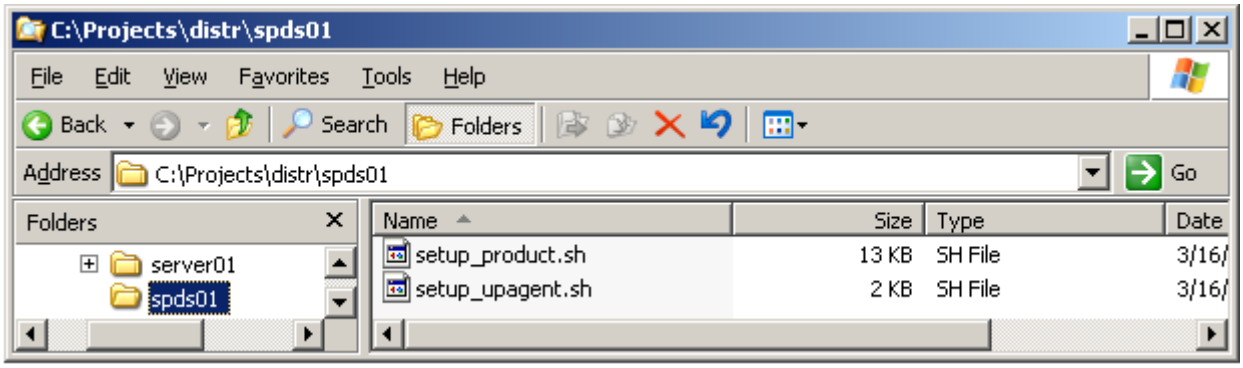

Рисунок 208

4. Созданные файлы перенесите на СПДС «ПОСТ» в каталог `customization`.

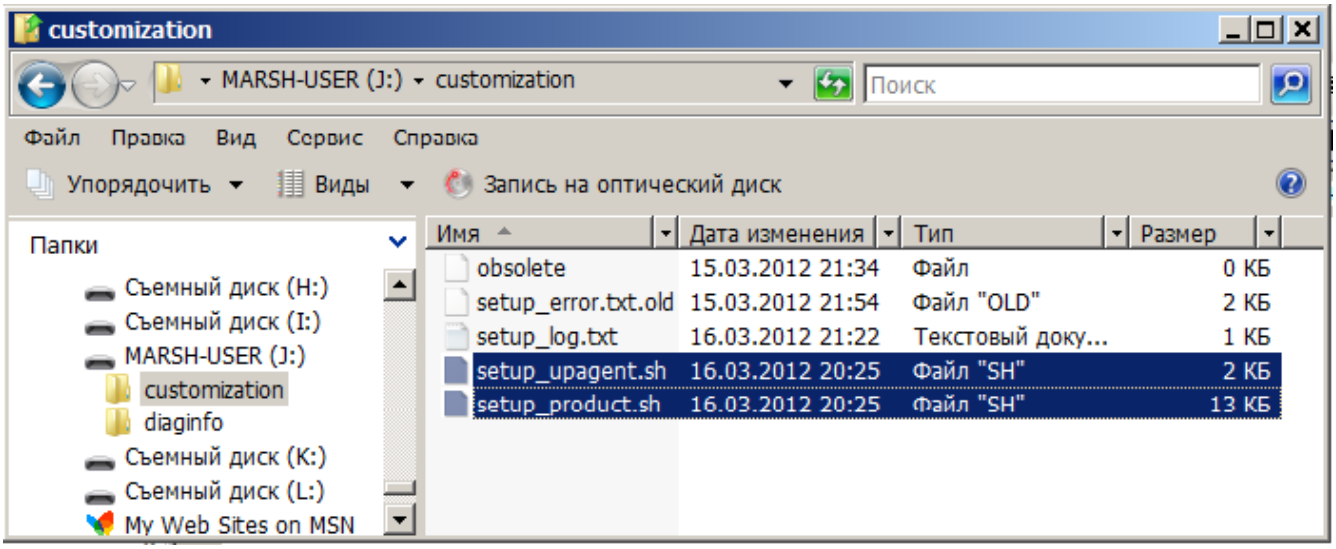

Рисунок 209

5. Закройте сессию с СПДС «ПОСТ», нажав кнопку «Закрыть сессию» в редакторе СПДС, закройте приложение и выньте СПДС «ПОСТ» из USB-разъема.

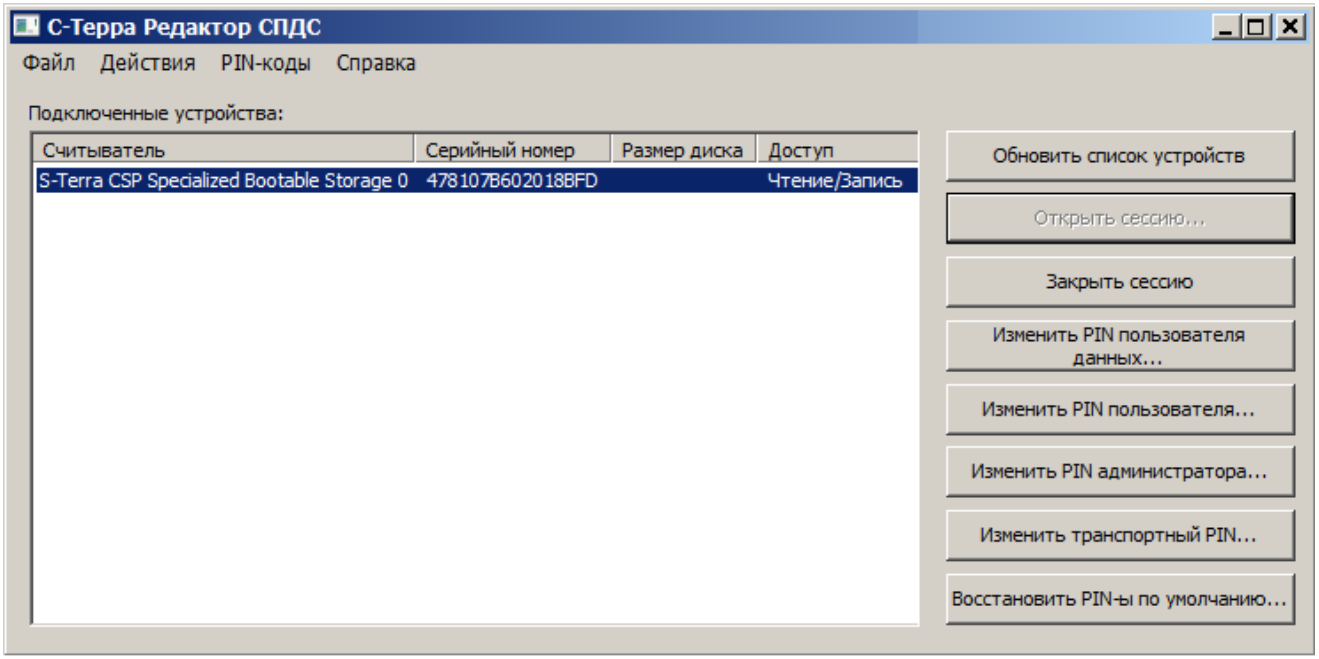

Рисунок 210

12.5. Инициализация СПДС

Далее СПДС «ПОСТ» следует инициализировать. Эта процедура должна осуществляться администратором, так как данные инициализации хранятся на устройстве в незащищенном виде.

1. Вставьте СПДС «ПОСТ» в USB-разъем компьютера, который будет загружаться с этого устройства.
2. Включите компьютер, войдите в программу BIOS и выполните настройку для загрузки компьютера с СПДС «ПОСТ» (см.документ «СПДС «ПОСТ». Руководство пользователя», раздел «Настройка BIOS») – выберите первым, например, предложение S-Terra Boot Partition.
3. При загрузке с СПДС «ПОСТ» появятся следующие предложения:

```
Loading …
Серийный номер устройства СПДС-USB: 1234567890123456
Введите PIN пользователя:
XXXXXXXX <Enter>
```

4. Введите PIN пользователя. При вводе неверного PIN предоставляется еще 4 попытки для ввода, после чего устройство будет заблокировано аппаратными средствами. Разблокировка выполняется только администратором.
5. Осуществляется проверка целостности файлов на СПДС «ПОСТ».

```
Проверка целостности файлов:
```

6. Появляется заставка СПДС»ПОСТ».

Рисунок 211

7. Далее появляется окно (Рисунок 212) или (Рисунок 213) для выбора режима работы. Предлагается выбрать Режим клиента или Административный режим. При первом запуске выберите `Административный режим`.

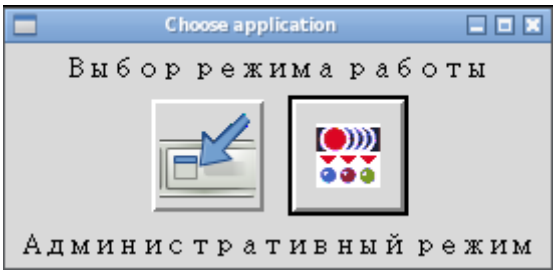

Рисунок 212

Рисунок 213

8. После этого продукт CSP VPN Gate будет инициализирован, а Клиент управления установлен на СПДС «ПОСТ». Выполняется проверка функционирования - Клиент управления устанавливает соединение с Сервером управления и проверяет наличие обновлений.
9. Получив нулевое обновление, Клиент управления загружает его и состояние клиента `spds01` меняется на `active`, он готов для принятия обновлений.

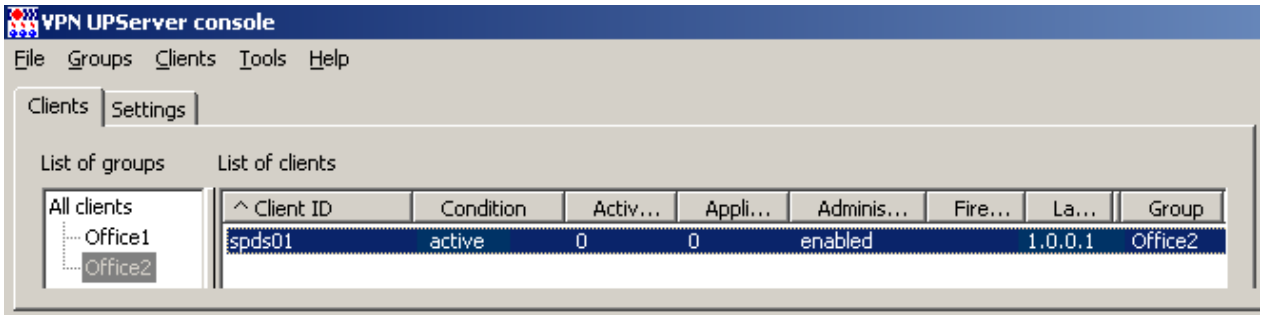

Рисунок 214

10. Устройство СПДС «ПОСТ» после этого выключится и будет готово для эксплуатации пользователем.

12.6. Эксплуатация СПДС «ПОСТ» пользователем

1. Администратор передает устройство СПДС «ПОСТ» пользователю, который вставляет его в терминальное устройство или компьютер, который настроен для загрузки с СПДС «ПОСТ».
2. После загрузки появляется большая заставка (Рисунок 211), а затем предлагается выбрать режим работы, выберите Режим клиента, например, «Клиент RDP».

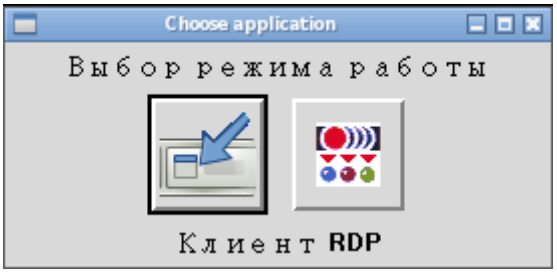

Рисунок 215

3. Далее осуществляется защищенный доступ к удаленному серверу в соответствии с заданными настройками, для нашего стенда - это RDP-сервер. При доступе предлагается ввести имя и пароль пользователя для его аутентификации. В соответствии с регламентом на RDP-сервере будут открыты соответствующие папки для работы данного пользователя.

   Таким образом, можно получить удаленное защищенное рабочее место, подключив СПДС «ПОСТ» к любому недоверенному компьютеру, настроенному на загрузку с него.

4. Получение обновлений для СПДС «ПОСТ» с Сервера управления осуществляется только в Административном режиме. Завершив работу в Режиме клиента и закрыв все приложения, снова загрузите компьютер с СПДС «ПОСТ» и перейдите в Административный режим. Клиент управления скачает обновление, применит его и выключит компьютер. Далее можно продолжать работу в Режиме клиента.

13. Сценарий создания клонов клиента CSP VPN Gate

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

13.1. Создание базового проекта

1. Задайте настройки (конфигурацию) продукта CSP VPN Gate для базового проекта `gate_base.pvd`, который будет использоваться для клонирования. Для этого в меню ***Tools*** выберите предложение ***VPN data maker*** (Рисунок 216).

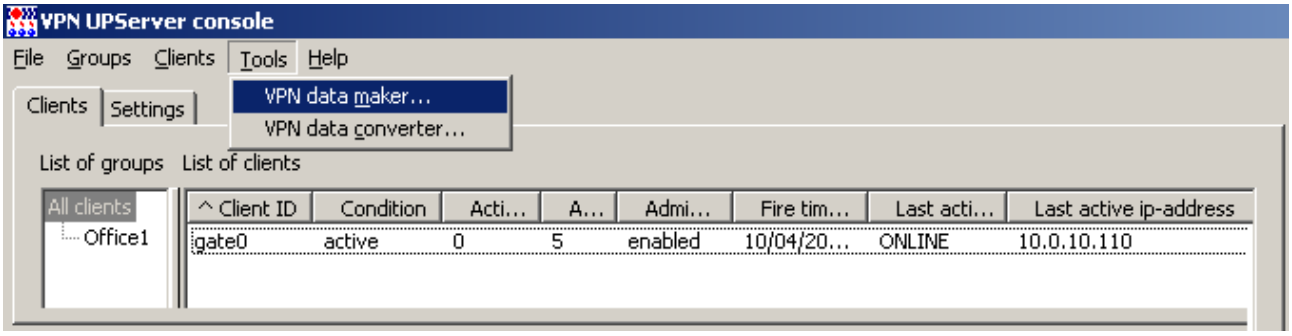

Рисунок 216

2. Выберите продукт CSP VPN Gate 3.1 и CryptoPro, нажмите кнопку Run Wizard.

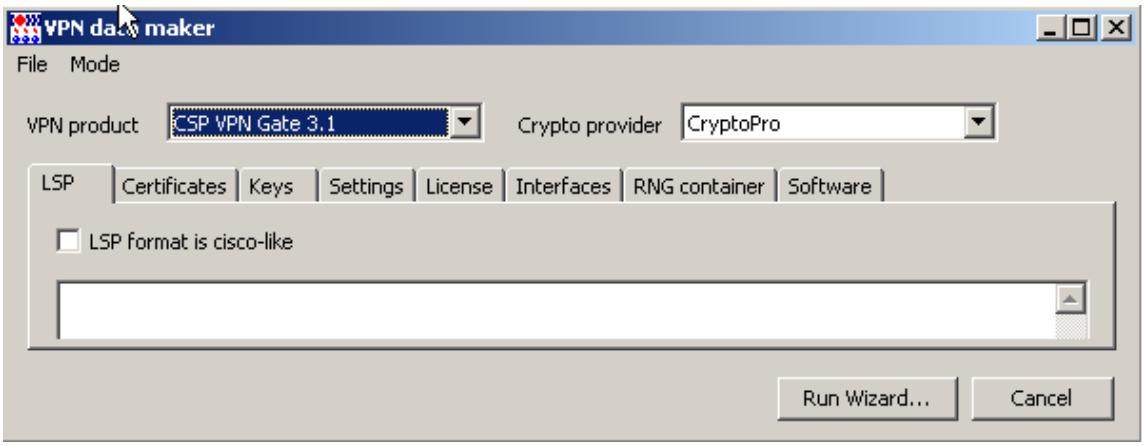

Рисунок 217

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

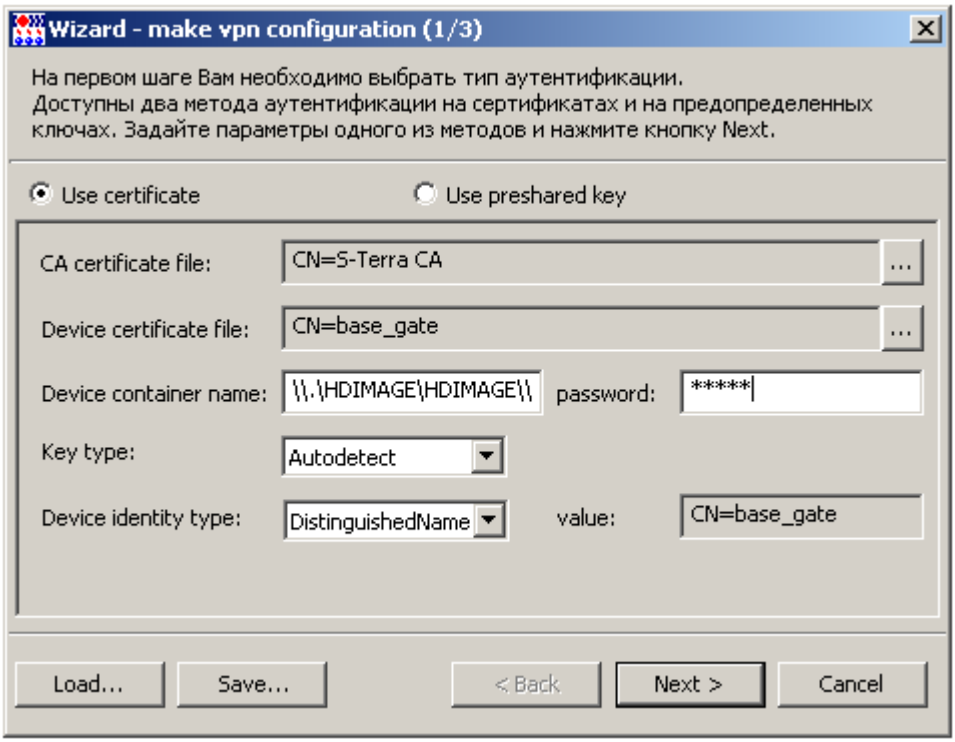

Рисунок 218

4. Создайте правило для защиты трафика между управляемым устройством и центральным шлюзом.

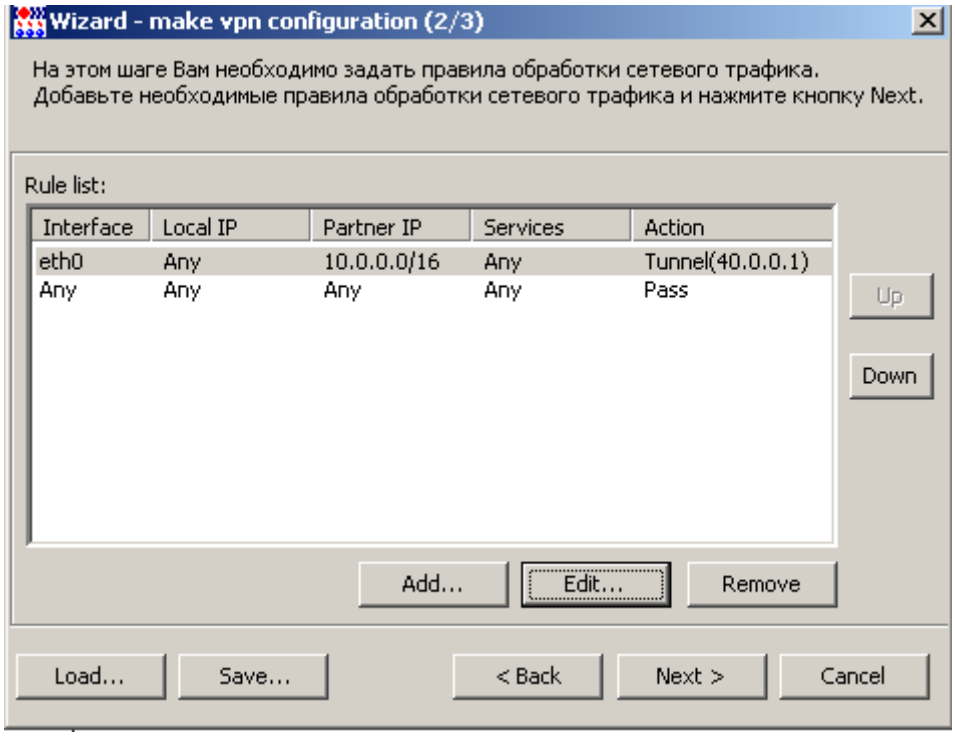

Рисунок 219

5. Введите данные лицензий на CSP VPN Gate и КриптоПро, нажмите кнопку Finish.

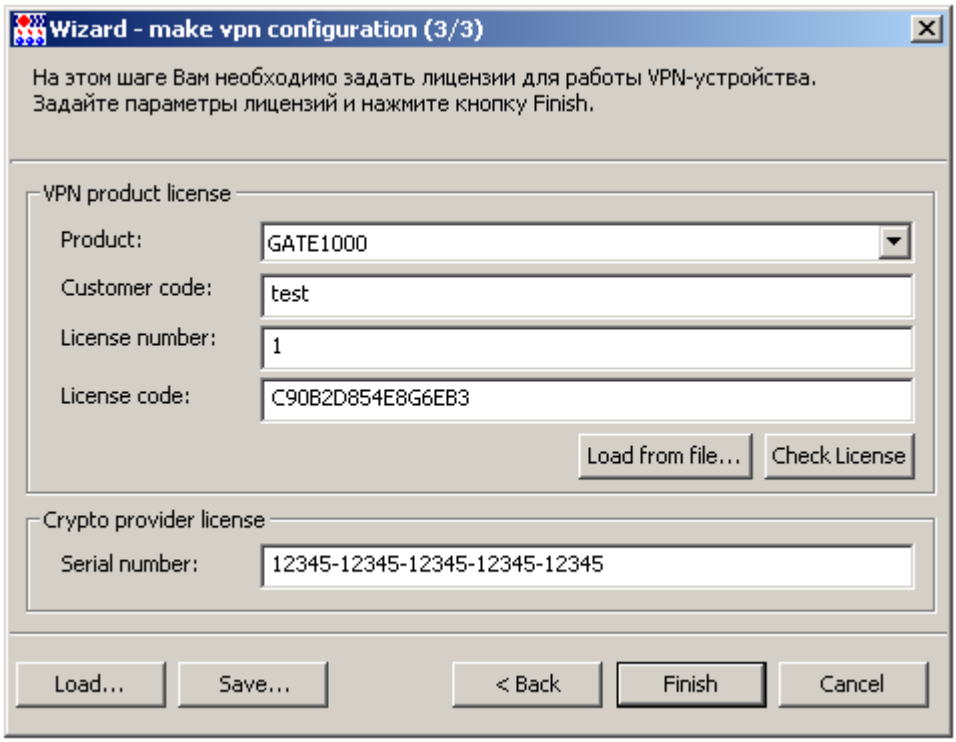

Рисунок 220

6. 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 221):

```
IdentityEntry auth_identity_01(
    DistinguishedName *= CertDescription(
          Subject *= COMPLETE,"CN=base_gate"
          )
)
CertDescription local_cert_dsc_01(
    Issuer *= COMPLETE,"CN=S-Terra CA"
    Subject *= COMPLETE,"CN=base_gate"
    SerialNumber = "202172E7000000000012"
)
CertDescription partner_cert_dsc_01(
)
AuthMethodGOSTSign auth_method_01(
    LocalID = auth_identity_01
    LocalCredential = local_cert_dsc_01
    RemoteCredential = partner_cert_dsc_01
    SendRequestMode = AUTO
    SendCertMode = AUTO
)
```

заменить на строки:

```
IdentityEntry auth_identity_01(
    DistinguishedName *= USER_SPECIFIC_DATA
)
CertDescription partner_cert_dsc_01(
)
AuthMethodGOSTSign auth_method_01(
    LocalID = auth_identity_01
    RemoteCredential = partner_cert_dsc_01
    SendRequestMode = AUTO
    SendCertMode = AUTO
)
```


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.

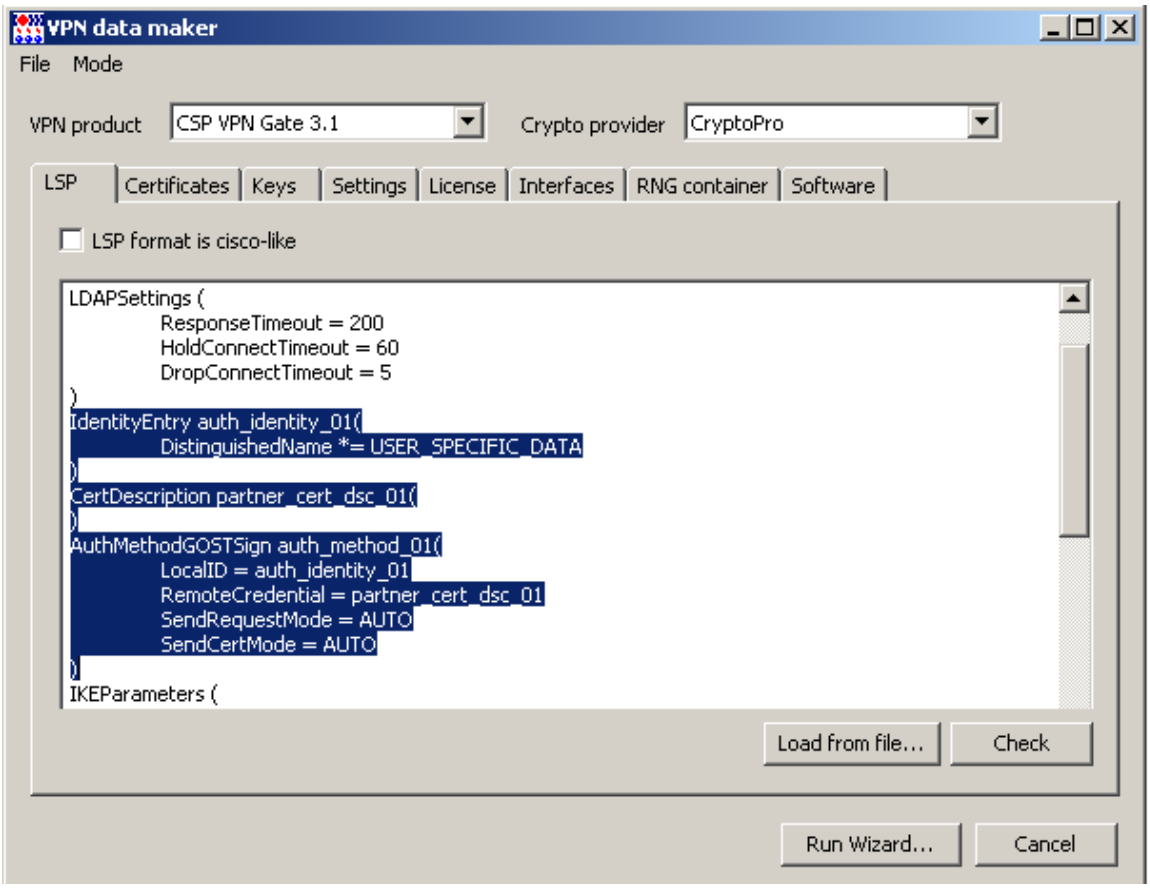

Рисунок 221

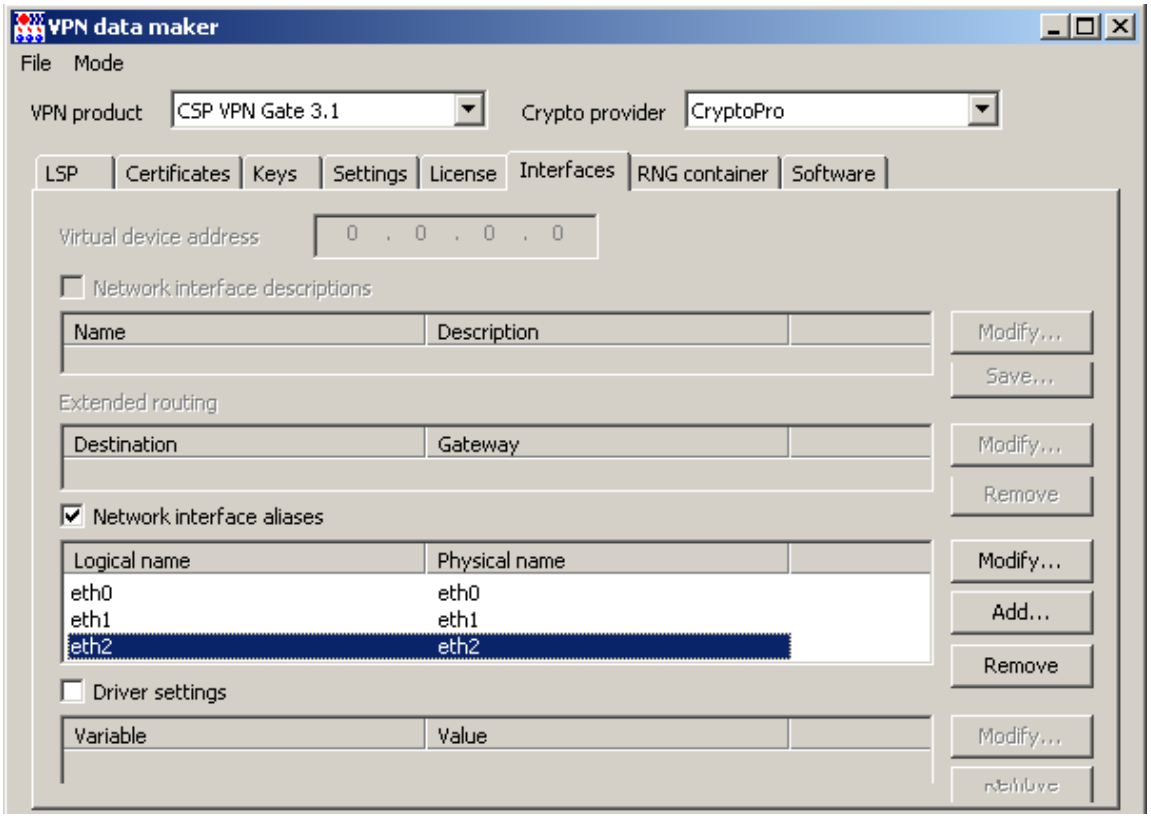

Рисунок 222

7. Далее во вкладке ***Interfaces*** задайте алиасы сетевых интерфейсов. Допустим, на устройствах, на которые будут устанавливаться клоны, имеется 3 сетевых интерфейса с логическими именами – `eth0, eth1, eth2` (Рисунок 222).

8. Получен базовый проект, сохраните его в файл на Сервере управления, выбрав в меню ***File*** предложение ***Save as….***

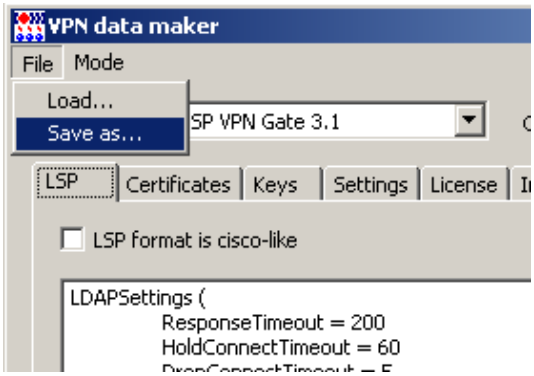

Рисунок 223

9. Сохраните в каталоге `Clone` под именем, например, `base_gate.vpd`.

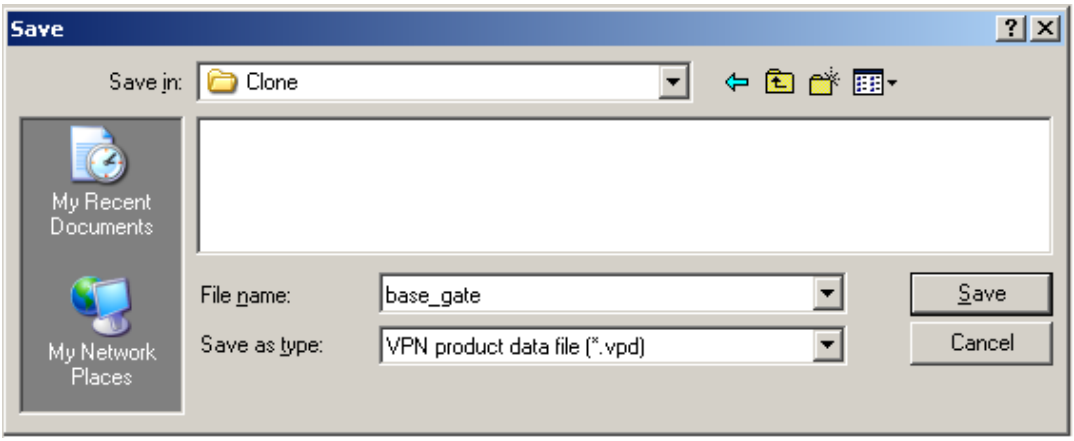

Рисунок 224

13.2. Подготовка материалов для клонов

Далее следует подготовить материал для создания клонов базового проекта – для каждого управляемого устройства создайте локальный сертификат, политику безопасности (LSP), файлы с лицензиями на CSP VPN Gate и КриптоПро CSP, сохранив все это на Сервере управления.

1. Получите утилиту `cryptcp` вместе с лицензией для тестирования с сайта компании КРИПТО-ПРО по адресу http://www.cryptopro.ru/products/other/cryptcp. Разместите ее в каталоге КриптоПро и зарегистрируйте лицензию:

```
C:\Program Files\Crypto Pro\CSP\cryptcp -sn XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

2. Подключите USB-флеш к Серверу управления. Узнайте имя доступной USB-флеш, на которую будут записываться подготовленные скрипты и контейнер, выполнив команду:

```
"C:\Program Files\Crypto Pro\CSP\csptest.exe" -enum -provtype gost2001 -info -
type PP_ENUMREADERS
```

В результате будут выданы имена доступных считывателей, например:

```
    0x0102  REGISTRY        ?aano?
    0x0102  FAT12_E         Aeneiaia E
    0x0102  FAT12_A         Aeneiaia A
```


3. 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" -exprt -CA http://10.0.10.111/certsrv -dm
```

- При создании случайных последовательностей можно избежать интерактивных запросов, если заранее сгенерить их с использованием ПАК «Аккорд-АМДЗ» или электронного замка «Соболь», а затем в КриптоПро CSP настроить ДСЧ на «Исходный материал».
- При задании команды в ОС Windows пароль в ней задать невозможно – будет запрашиваться интерактивно (Рисунок 225). Обязательно задайте пустой пароль.

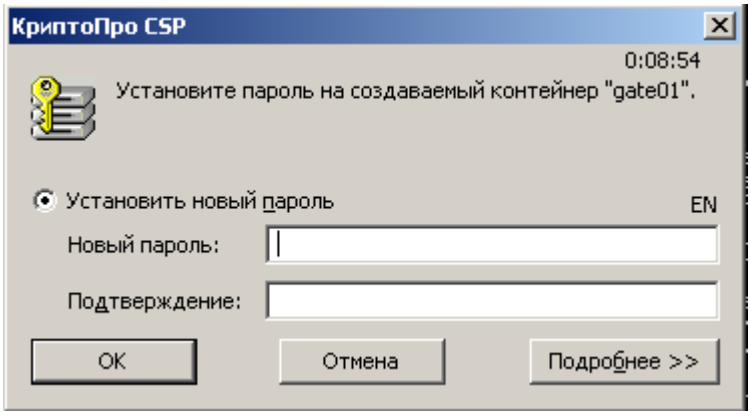

Рисунок 225

- Утилиту `cryptcp` можно использовать в ОС Unix, которая входит в состав пакета КриптоПро. При создании ключевой пары и контейнера можно избежать интерактивного задания пароля:

```
/opt/cprocsp/bin/ia32/cryptcp -creatcert -dn "CN=gate01" -both -km -cont
'\\.\FLASH\gate01' -exprt -pin "" -CA "http://10.0.10.111/certsrv" -dm -enable-
install-root
```

4. 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
```

5. Создайте файл `C:\Clone\st_gate01.lic` с лицензией на продукт CSP VPN Gate, например::

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

6. Создайте файл `C:\Clone\cp_gate01.lic` с лицензией на продукт КриптоПро CSP, например:

```
LicenseSerialNumber=12345-12345-12345-12345-12345
```

7. Создайте файл алиасов сетевых интерфейсов `C:\Clone\ia_gate01.txt`, например:

```
eth0=eth0
eth1=eth1
eth2=eth2
```

8. 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 12345 -ifaliases
C:\Clone\ia_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.

9. 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
```

10. Создайте два скрипта для настройки CSP 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, содержащий данные для настройки продукта CSP VPN Gate

`setup_upagent.sh` – скрипт, содержащий данные для инсталляции (инициализации) продукта VPN UPAgent.

11. Скопируйте дистрибутив Клиента управления с Сервера управления `C:\Program Files\S-Terra\S-Terra KP\upagent\<OS>\vpnupagent.tar` на USB-флеш.

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

13.3. Настройка управляемого устройства

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

```
ifconfig eth0 40.0.0.102/16
ifconfig eth1 192.168.0.1/24
/bin/ni_saveif_all.sh
```

2. Вставьте в USB-порт управляемого устройства подготовленный USB-флеш и выполните его монтирование, например:

```
mount /dev/sda1 /mnt
```

3. Убедитесь, что контейнеры на USB-флеш доступны для КриптоПро CSP посредством команды `csptest`.

```
/opt/cprocsp/bin/ia32/csptest -keyset -u -machinekeyset -enum_containers -
verifycontext
```

4. 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
```

5. Запустите скрипт для инсталляции Клиента управления (VPN UPAgent):

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

6. Запустите скрипт для настройки CSP VPN Gate:

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

7. Выполните окончательную инициализацию продукта CSP VPN Gate:

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

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

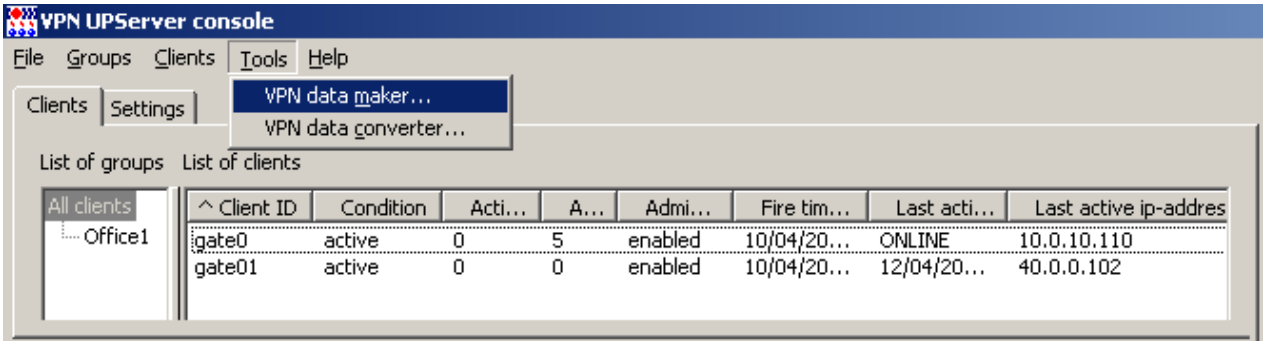

Рисунок 226

8. 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 40.0.0.1
```

14. Сценарий включения в систему управления работающего устройства с CSP VPN Agent

Имеется устройство с установленной ОС и продуктом CSP VPN Agent, которое настроено сторонними методами и включено, например, в подсеть 40.0.0.0/16 с адресом 40.0.0.104. 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 CSP VPN Gate - `work_gate02`.

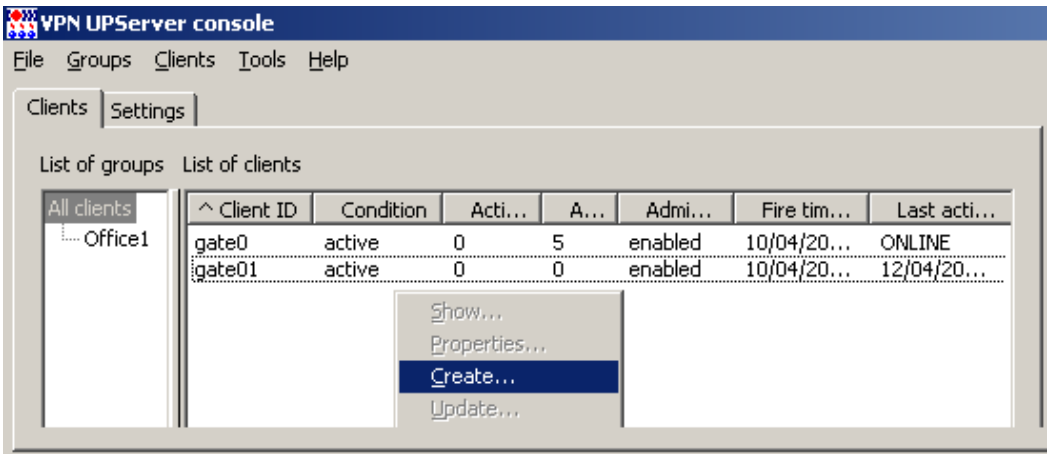

Рисунок 227

2. Введите уникальное имя клиента и нажмите кнопку E.

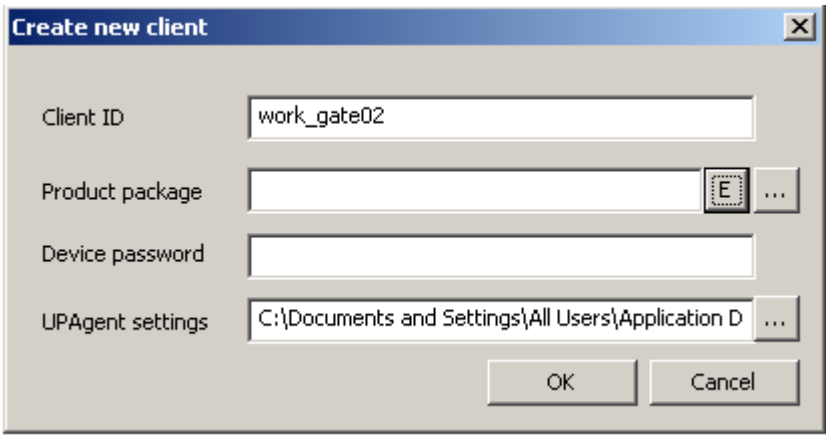

Рисунок 228

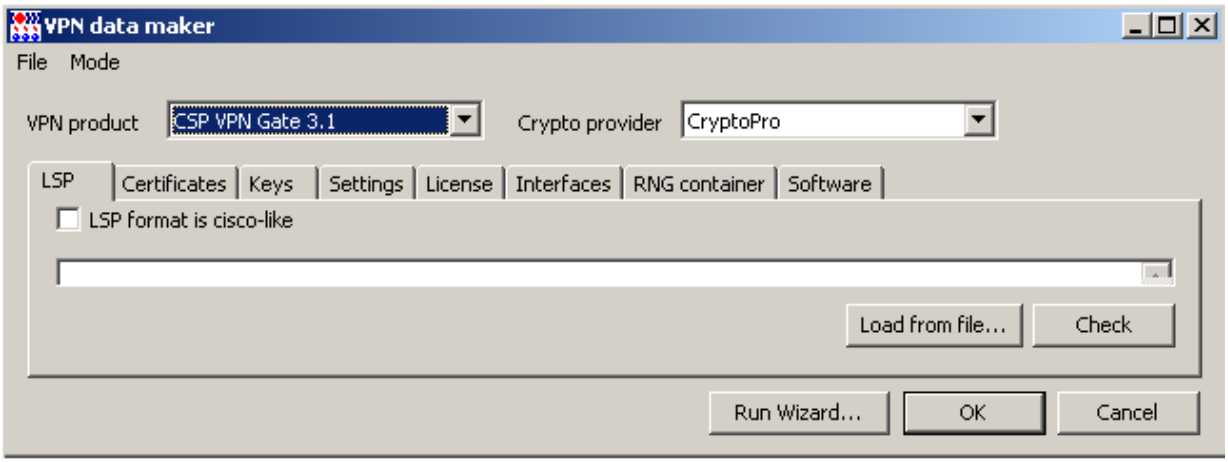

Рисунок 229

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

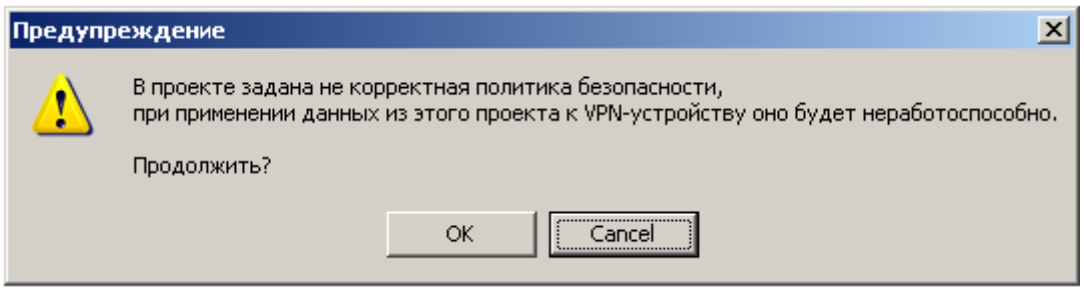

Рисунок 230

5. В следующем предупреждении также нажмите OK.

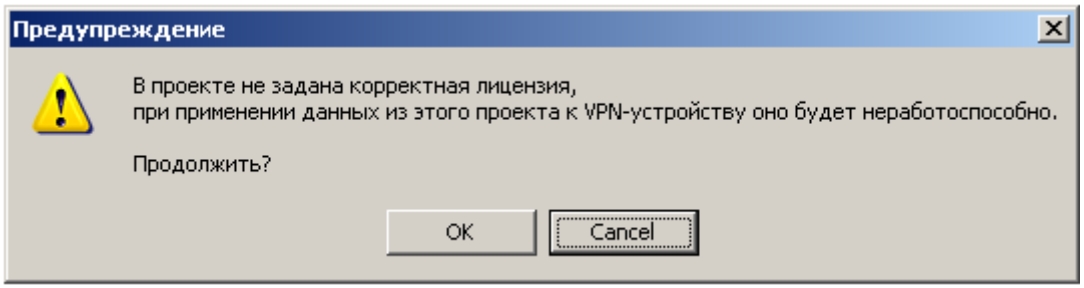

Рисунок 231

6. В окне создания клиента нажмите OK.

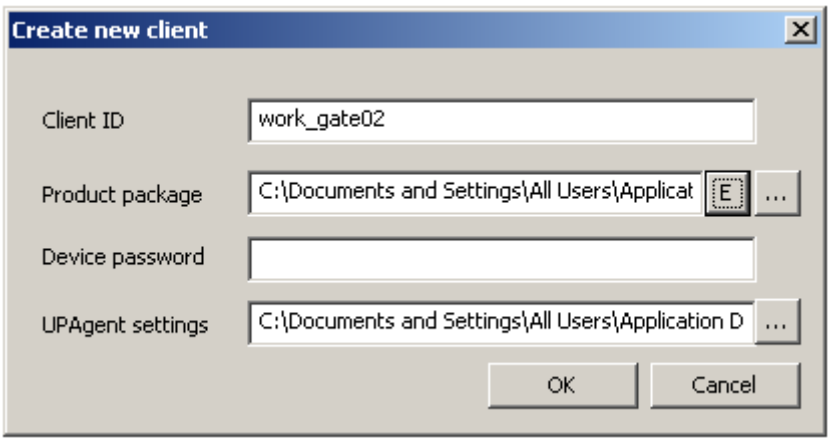

Рисунок 232

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

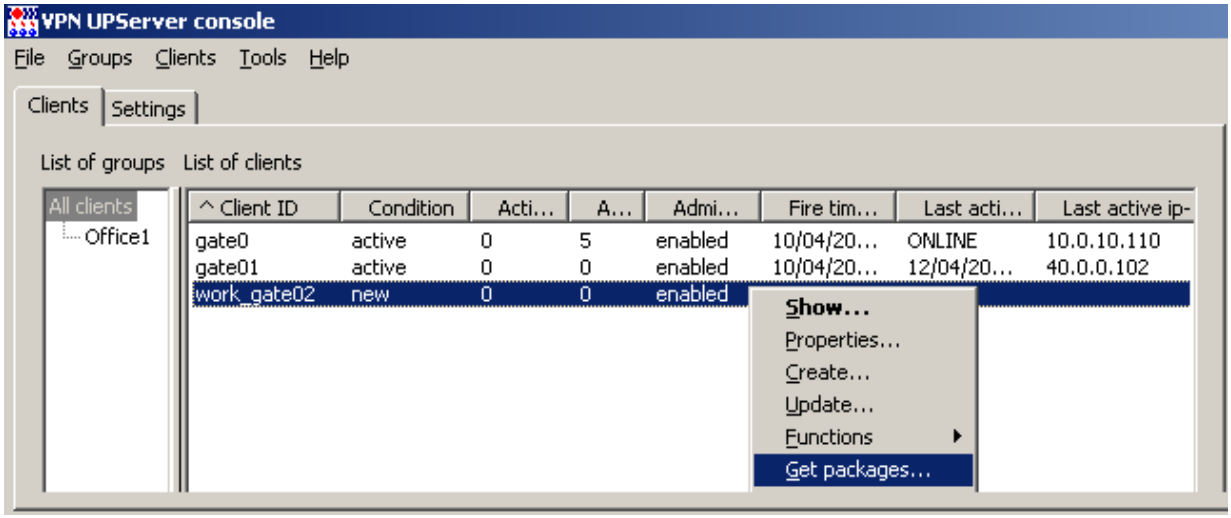

Рисунок 233

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

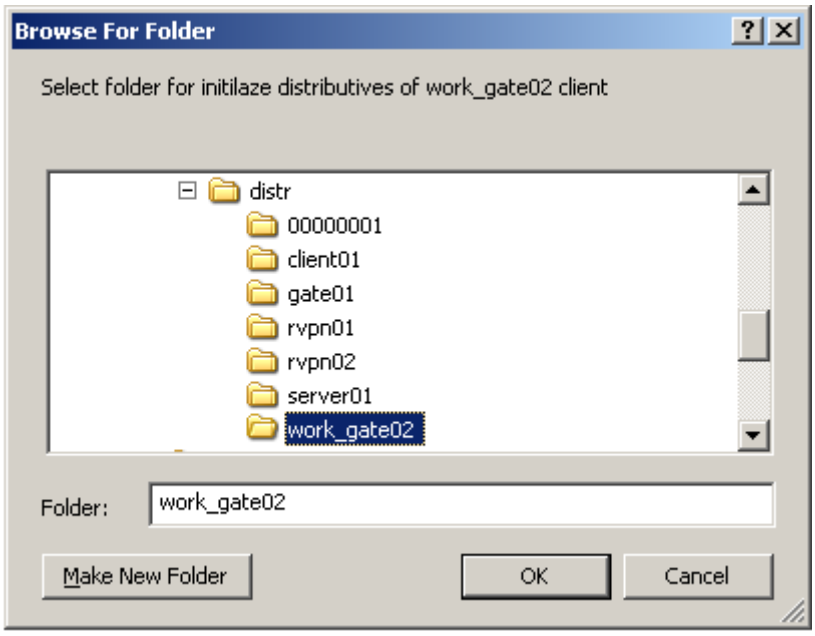

Рисунок 234

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

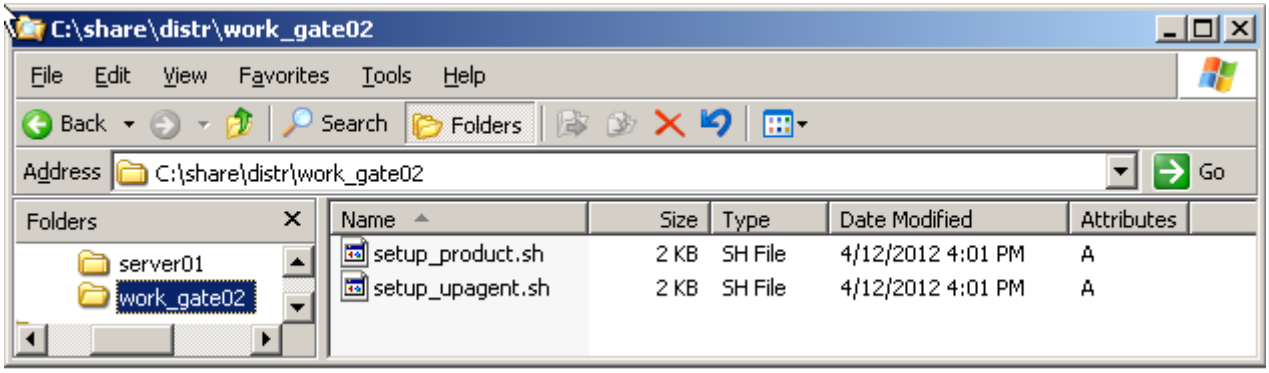

Рисунок 235

10. Доставьте скрипт `setup_upagent.sh` на работающий шлюз с адресом 40.0.0.104, например, с использованием утилиты `pscp` в предварительно созданный каталог `/tmp`:

```
pscp setup_upagent.sh root@40.0.0.104:/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@40.0.0.104:/tmp/work_gate02.vpd C:\Projects
```

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

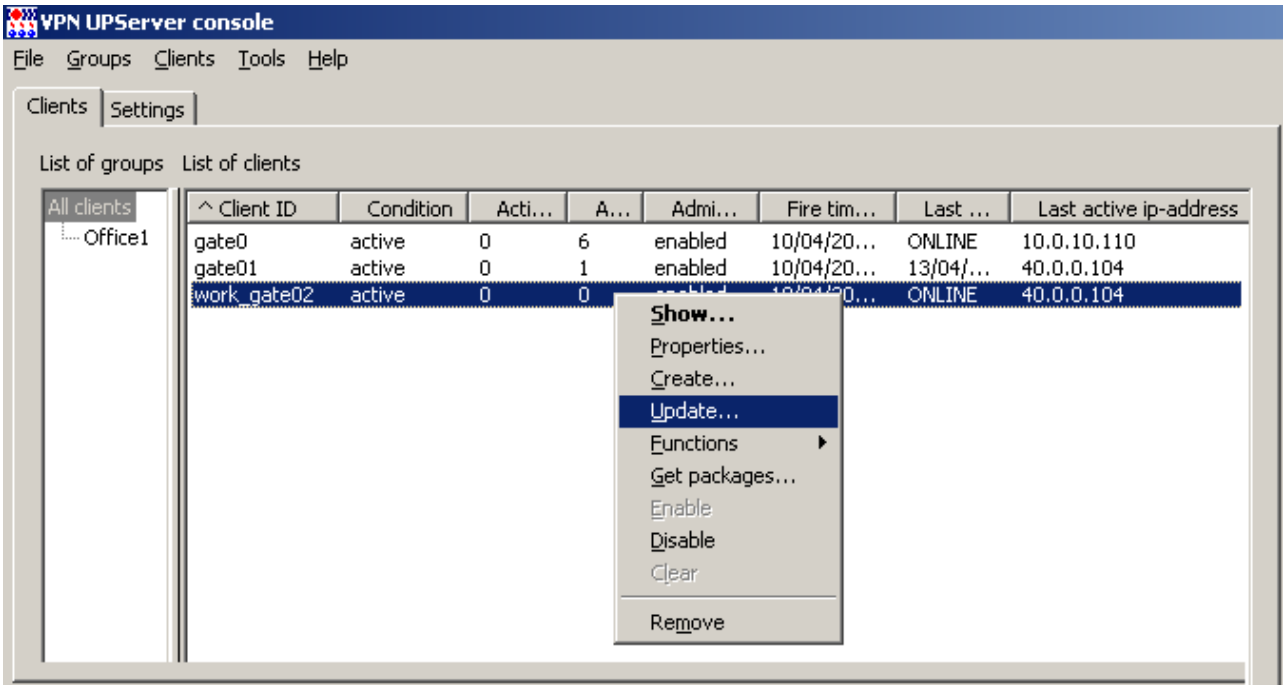

Рисунок 236

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

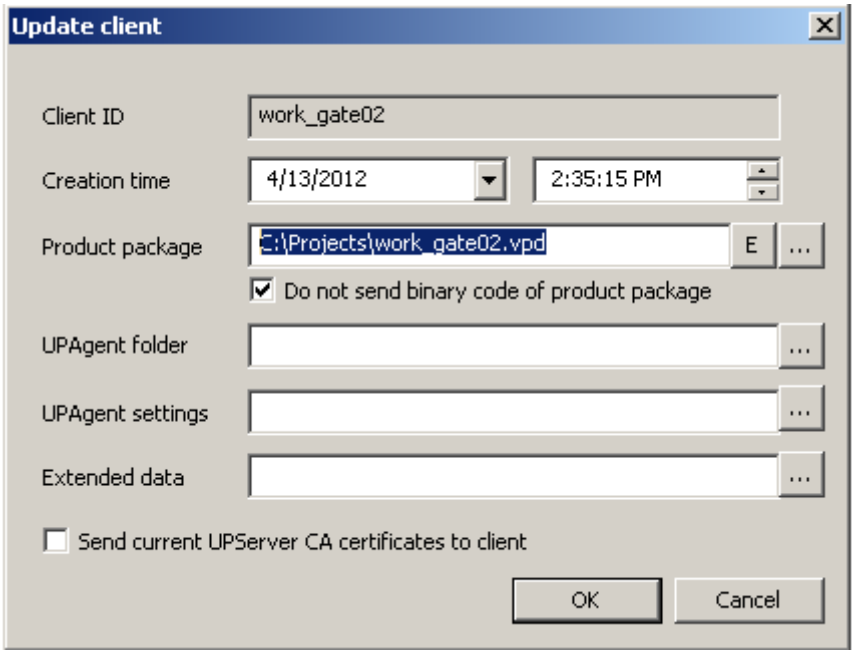

Рисунок 237

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

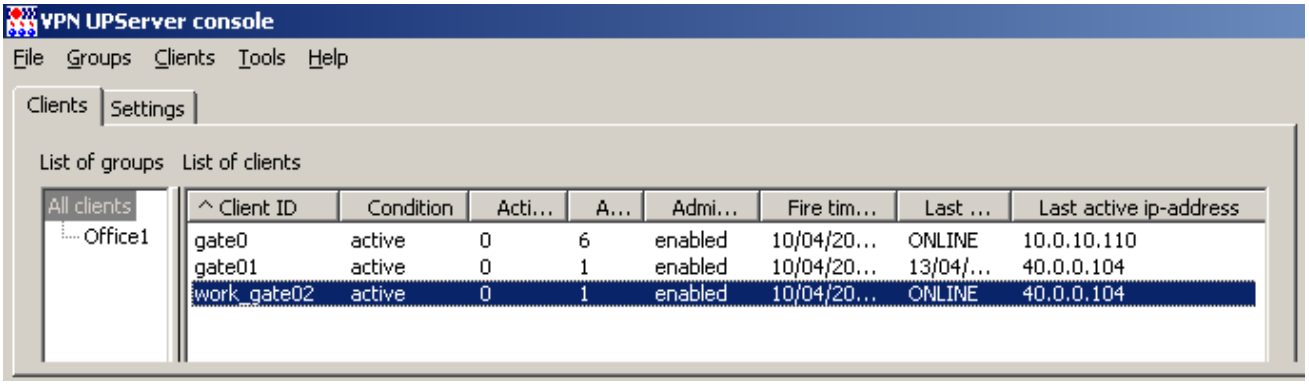

Рисунок 238

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 осуществлялось сторонними методами.

15. 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***.

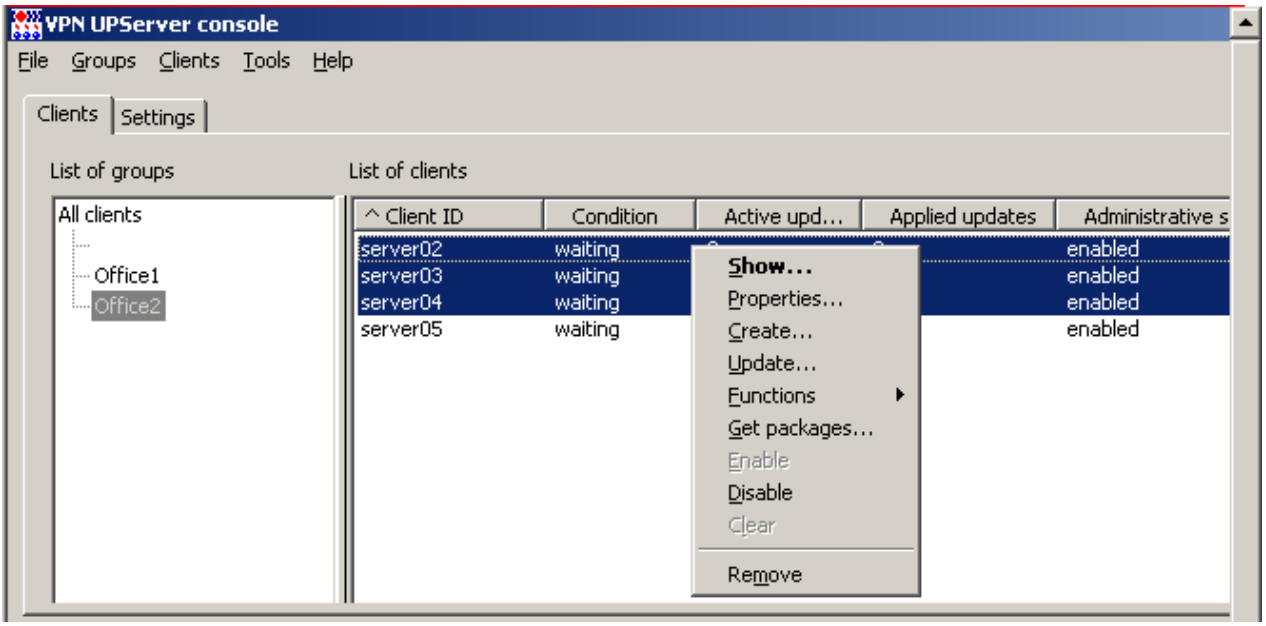

Рисунок 239

Каждый клиент на Сервере управления создается отдельно и для каждого клиента скрипты (дистрибутивы) Клиента управления и CSP VPN Agent 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 предопределенных 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.

15.1. Создание шаблона проекта

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

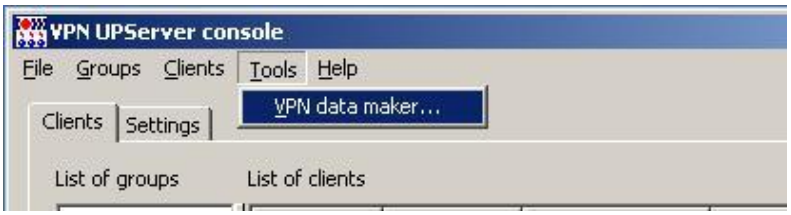

Рисунок 240

2. В открывшемся окне **VPN data maker** заполните необходимые вкладки (или используйте Run Wizard) для настройки продукта CSP VPN Agent.

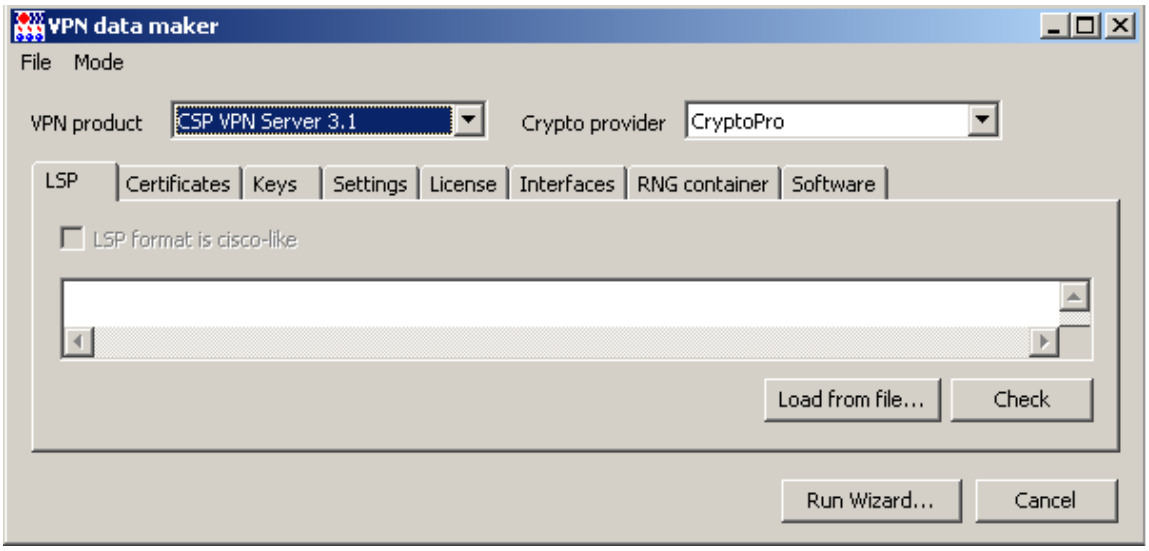

Рисунок 241

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

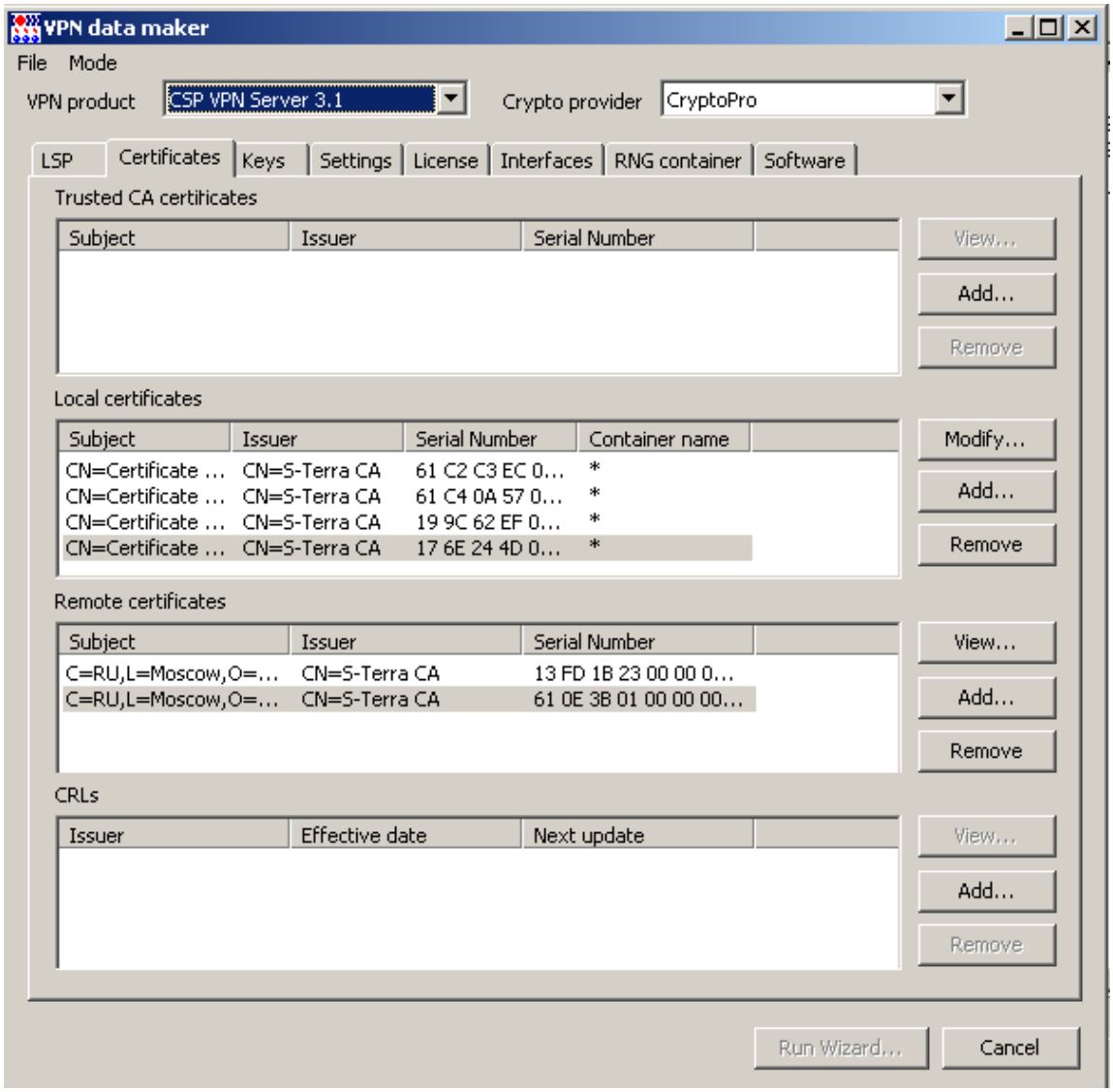

Рисунок 242

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.

Use this container name and this password as default – при установке этого флажка и при указании в полях «*», для групповой операции добавления сертификатов это окно будет появляться только один раз.

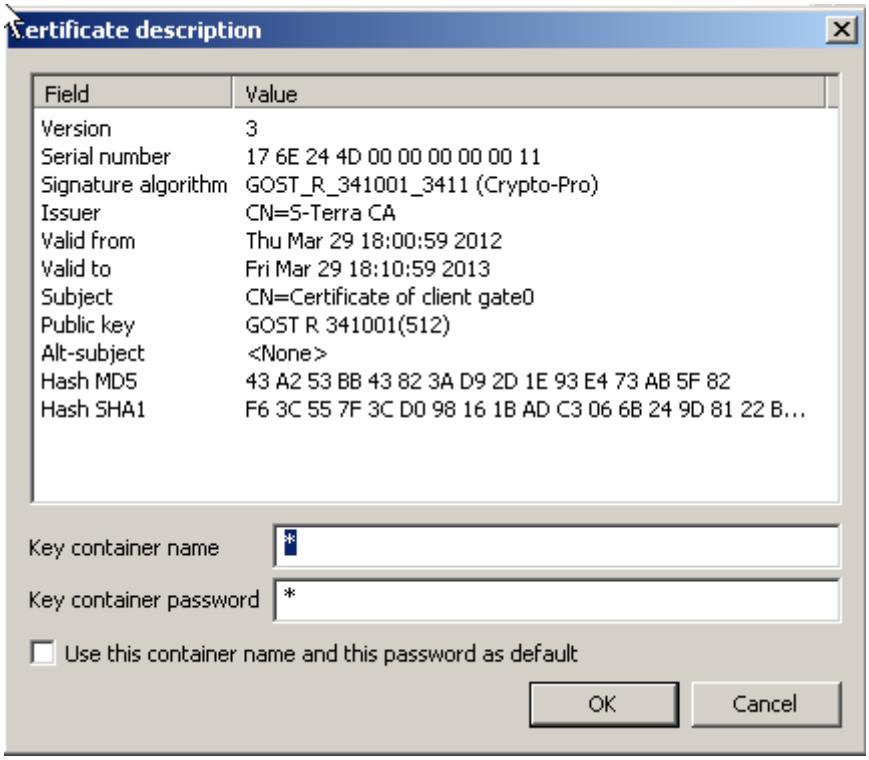

Рисунок 243

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

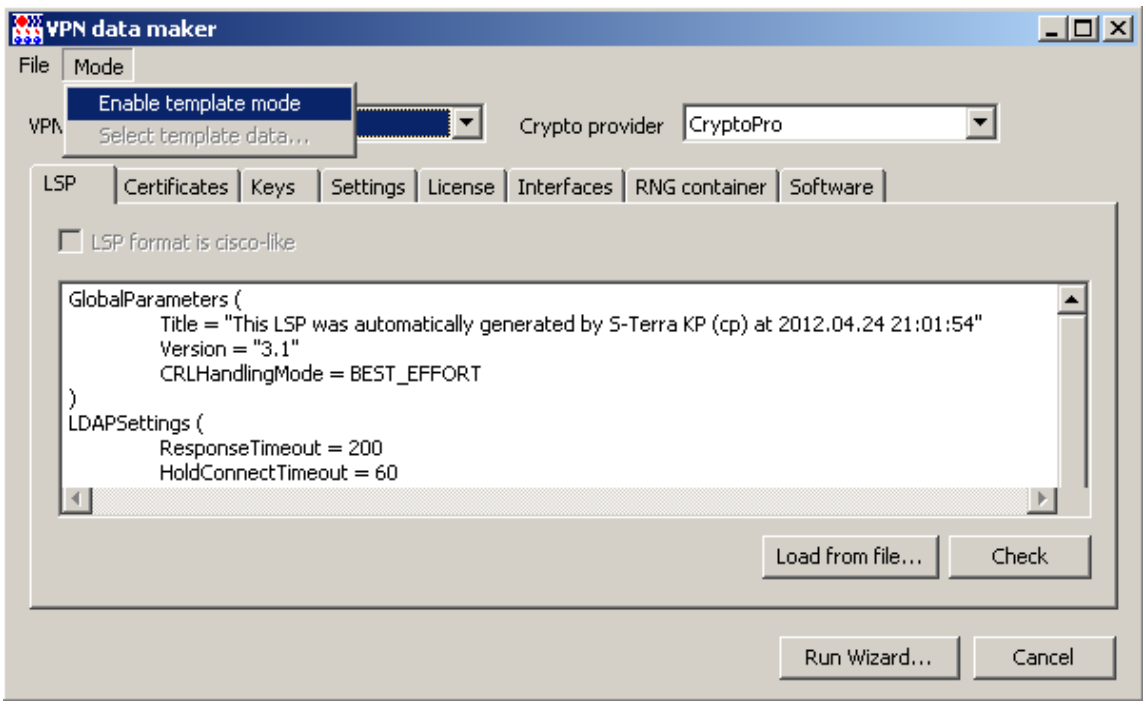

Рисунок 244

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

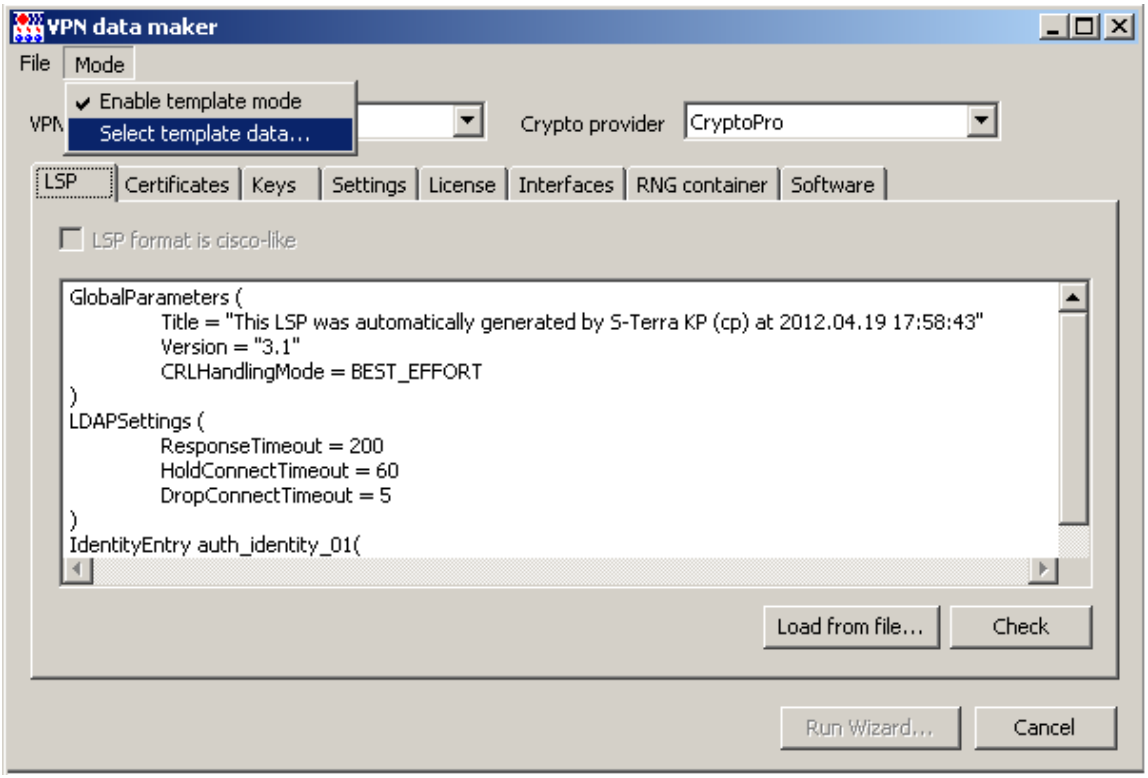

Рисунок 245

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

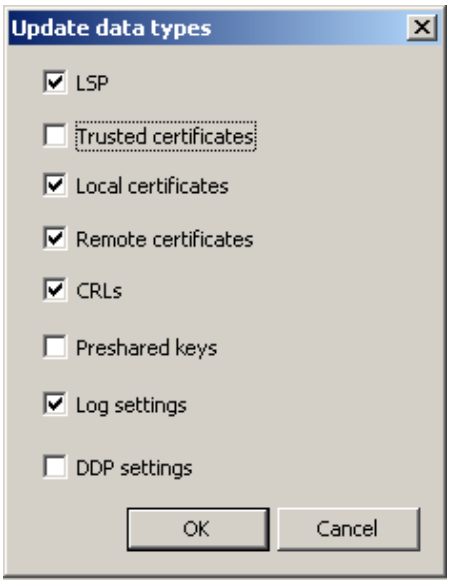

Рисунок 246

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***.

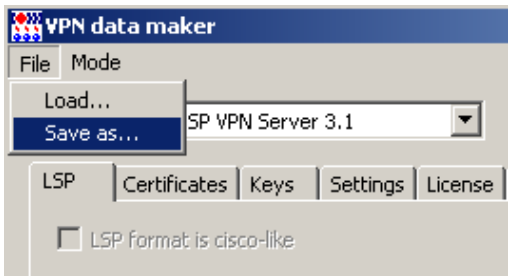

Рисунок 247

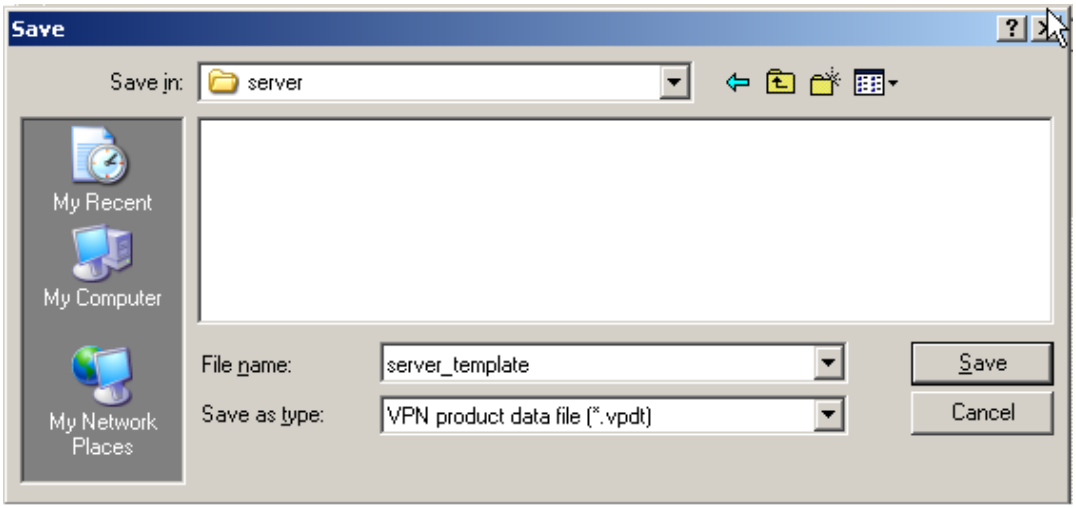

Рисунок 248

15.2. 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***.

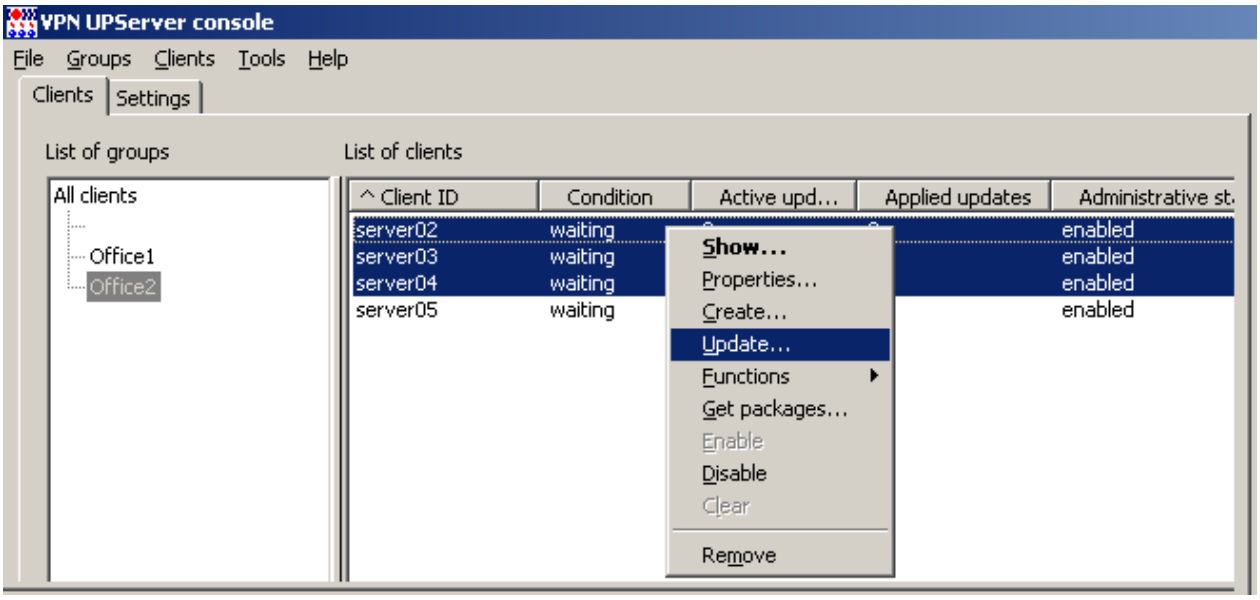

Рисунок 249

2. В открывшемся окне **Update clients** в поле **Product package** нажмите кнопку [...] и в стандартном окне открытия файла укажите файл с шаблоном проекта, например, `server_template.vpdt`.

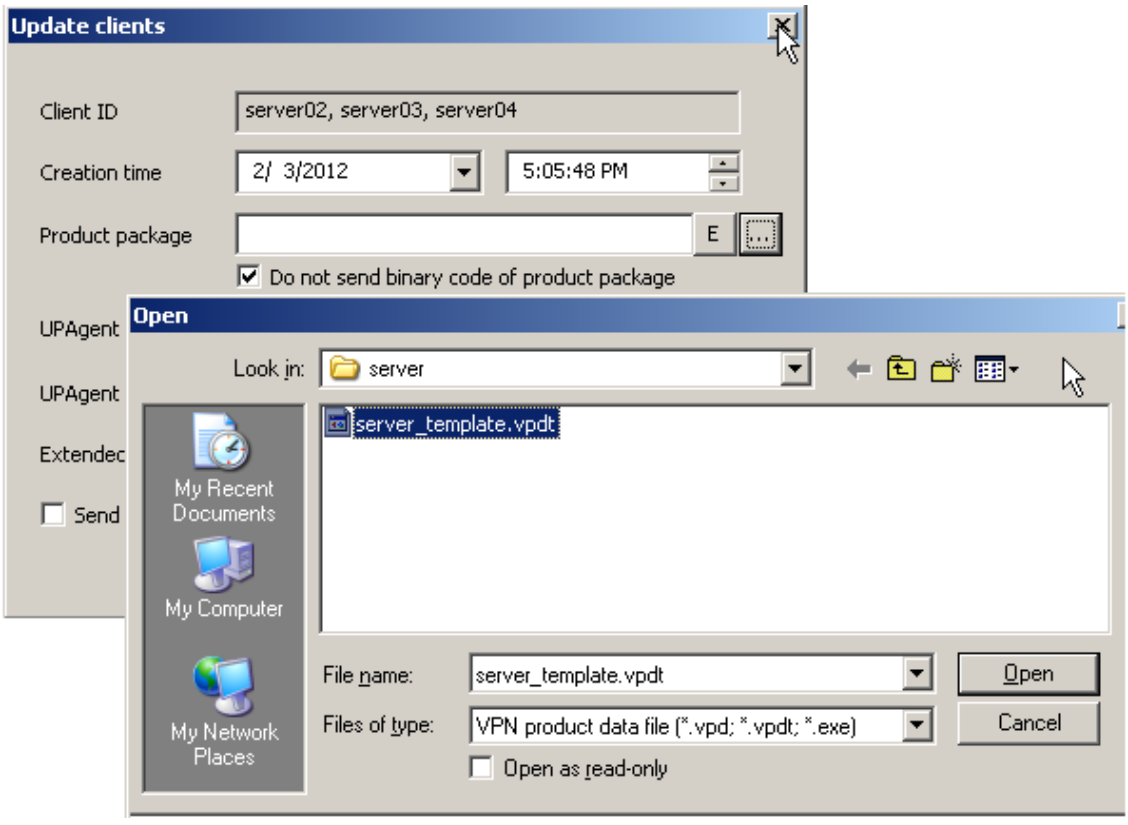

Рисунок 250

3. 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.

16. Утилита upmgr

Утилита `upmgr.exe` является технологической утилитой, вызываемой при работе с графической консолью Сервера управления. Утилита размещена в каталоге продукта – `C:\Program Files\S-Terra\S-Terra KP`.

Команды утилиты `upmgr.exe`:

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

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

upmgr remove -i CLIENT_ID

upmgr get -i CLIENT_ID -d PRODUCT_DIR [-ask_user_mode ASK_USER_MODE] [-
check_mode CHECK_MODE]

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]

upmgr clear -i CLIENT_ID

upmgr disable -i CLIENT_ID

upmgr enable -i CLIENT_ID

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

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

upmgr show_cert

upmgr renew_cert [-expired_only]

upmgr check_files
```

где:

`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];
`SECTION_NAME`	имя секции данных о клиенте. `Например, ”---VPN PRODUCT---”, ”---LSP---”, ”---LICENSE---” и т.п.`
`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 CSP VPN Server/CSP VPN Client, который был создан с помощью продукта CSP VPN Server/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
`PRODUCT_DIR`	каталог, в который будут сохранены дистрибутивы для Клиента управления;

ASK_USER_MODE	режим запроса подтверждения у пользователя о начале обновления, устанавливаемый в пакете Клиента управления, может принимать значения: auto – подтверждение запрашивается, если установлен CSP 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 Если значение другое, то оно приравнивается к full.
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
CREATION_TIME	формат: hh:mm. 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 Клиентом управления сразу после создания обновления (если параметры не указаны, то используются текущая дата и время);
OLD_CLIENT_GROUP	имя группы, которая должна быть заменена на CLIENT_GROUP (формат PARENT0/PARENT1[/NAME][*]);
CLIENT_DESC	произвольная строка для описания клиента, вносимая в поле Descrition
FILE	имя файла, в котором указана строка с переменной и ее значением, описывающая свойства клиента, которая передается скрипту cook.bat при его запуске в процессе подготовки расширенного обновления. Формат строки: _ex_имя_переменной=значение_переменной
-expired_only	рабочий сертификат Сервера управления пересоздается, если у него истек срок действия.
check_files	проверка целостности файлов Сервера управления.

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

Команда ***show*** выводит информацию, аналогичную таблице клиентов (Рисунок 66). Если не указывать ключ `-i`, то выводится краткая информация обо всех клиентах, при указании ключа `-i` – выводится расширенная информация для указанного клиента.

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

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

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]
```

Создание нового клиента с идентификатором "`client02`", с именем дистрибутива продукта CSP VPN Server "`e:\share\test_pkg.exe`":

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

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

```
upmgr remove -i CLIENT_ID
```

Удаление клиента с идентификатором "` client02`":

```
upmgr.exe remove -i client02
```

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

```
upmgr get -i CLIENT_ID -d PRODUCT_DIR [-ask_user_mode ASK_USER_MODE] [-
check_mode CHECK_MODE]
```

Получение 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*** 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]
```

Создание для клиента с идентификатором "`client02`" обновления данных продукта CSP VPN Agent, находящихся в дистрибутиве этого продукта "`e:\share\test_pkg.exe`":

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

Если вместо ключа `-p` указать ключ `-pd`, то Клиенту управления будут пересылаться только данные, без бинарных кодов продукта CSP VPN Agent.

Команда ***clear*** позволяет отменить все неприменeнные обновления для клиента.

```
upmgr clear -i CLIENT_ID
```

Удаление всех неприменeнных обновлений для клиента с идентификатором "`00000002`":

```
upmgr.exe clear -i client02
```

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

```
upmgr disable -i CLIENT_ID
```

Запрет всех сетевых обменов с клиентом с идентификатором "client02":

```
upmgr disable -i client02
```

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

```
upmgr enable -i CLIENT_ID
```

Разрешение сетевых обменов с клиентом с идентификатором "client02":

```
upmgr.exe enable -i client02
```

Команда ***set_group*** изменяет группу у заданных клиентов.

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

Включает клиента "client02" в группу "Moscow/Office01":

```
upmgr.exe set_group –g Moscow/Office01 –i client02
```

Команда ***set_prop*** добавляет описание свойств у заданного клиента.

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

Клиенту client01 добавить в описание свойство «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\S-Terra KP\prop_client02.txt"
```

В файле prop_client02.txt записана строка – «может работать с токеном= eToken NG-FLASH»

Команда ***show_cert*** запускает стандартную GUI программу операционной системы для отображения рабочего сертификата Сервера управления.

```
upmgr show_cert
```

Показать рабочий сертификат Сервера управления:

```
upmgr.exe show_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
```

Пересоздать рабочий сертификат Сервера управления только в том случае, если у него истек срок действия. Команда работает только для RSA-сертификатов, так как перевыпуск ГОСТ-сертификатов требует интерактивного участия администратора.

```
upmgr.exe renew_cert -expired_only
```

Команда ***check_files*** запускает проверку целостности файлов Сервера управления

```
upmgr check_files
```


17. Утилита vpnmaker

Утилита `vpnmaker` является технологической утилитой, вызываемой при работе с графической консолью Сервера управления для внесения изменений в готовый проект. Утилита размещена в каталоге продукта `C:\Program Files\S-Terra\S-Terra KP`.

Назначение – изменение данных в готовых проектах, создание 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.

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.

Старые ключи из проекта удаляются. Можно добавить несколько ключей

`-lic LIC_FILE` — полный путь к текстовому файлу с лицензией на продукт. Пример файла:

```
[license]
```



```
CustomerCode=bank
ProductCode=GATE100
LicenseNumber=1
LicenseCode=6E7AAAECBBB478B8
```

`-cryptolic CRYPTO_LIC_FILE` полный путь к текстовому файлу с лицензией криптопровайдера. Пример файла:

```
LicenseSerialNumber=1282349167838947
```

`-cert CERT_FILE` полный путь к файлу с сертификатом (расширение `.cer`, `.p7b`, `.pfx`). Для этого сертификата можно указать дополнительные параметры:

`-certpwd PWD` пароль, которым защищен файл с сертификатом.

`-certnum NUM` порядковый номер сертификата (нужен, если файл содержит несколько сертификатов).

`-certkey KEY_CONT` имя контейнера с секретным ключом сертификата (сам контейнер – у клиента).

`-certkeypwd KEY_PWD` пароль, защищающий ключевой контейнер.

`-trust` этот флаг должен выставляться у CA-сертификатов, которым мы доверяем.

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.

`-ifdesc IF_FILE` полный путь к текстовому файлу с описанием виртуального адреса и роутинга. Параметр может быть только для CSP VPN Gate on token (СПДС «ПОСТ»). Пример файла:

```
VirtualDeviceAddress=23.24.24.24

[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

DGA – default gateway address
VDA – virtual device address
```

`-ifaliases IF_FILE` полный путь к текстовому файлу с описанием алиасов интерфейсов. Пример файла:

```
FastEthernet1/0 = eth1
FastEthernet1/1 = eth2,eth3
default   =  *
```

По этой информации формируется файл `ifaliases.cf` (для продуктов версии 4.0) или информация сохраняется в базе продукта (для версий 3.X). Если не определен алиас `default`, он автоматически добавляется в виде `default = *`.

`-targetsoft TARGETSOFT_FILE` полный путь к текстовому файлу с описанием типа и параметров целевого программного обеспечения на

управляемом устройстве. Параметр применяется только для CSP VPN Gate on token. Пример файла:

```
TARGET=rdp
SERVER=192.168.15.1:5444
USER=guest
OPTIONS=
```

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 устройств.

Параметры режима **make_template**

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

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

18. Настройки Сервера управления

Администратор Сервера управления может задать некоторые настройки в файле:

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

`c:\ProgramData\UPServer\ssettings.txt`

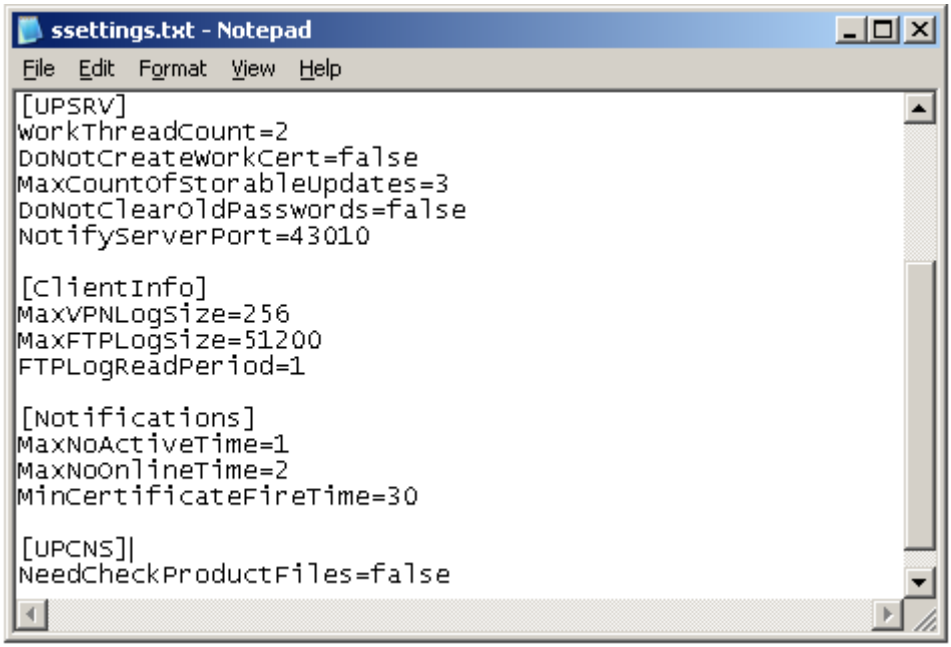

Рисунок 251

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.`

Администратор может управлять следующими настройками.

Секция	Описание
`Log`	***Флаг включения syslog протоколирования*** Переменная `SyslogEnable` Значение: `true` - включено протоколирование `false` - выключено (значение по умолчанию – `false`).
	Адрес Syslog-сервера Переменная `SyslogSrvAddr` Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1)
	Адрес источника сообщений Переменная `SyslogFacility` Значение: строка (значение по умолчанию – `log_local7`)
	Размер файла протоколирования событий Переменная `FileMaxSize` Значение: от 10 килобайт (значение по умолчанию - 10200 килобайт, если строка отсутствует или некорректна). Имя файла протоколирования: `C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log.` При достижении заданного значения данные копируются в файл `upserver.log.bak`, а файл `upserver.log` очищается. Пример файла с

	сообщениями.
UPSRV	***Количество рабочих ниток в сервисе подготовки обновлений*** Переменная `WorkThreadCount` Значение: десятичное число от 1 до 10 (значение по умолчанию 2). Рекомендуемое значение - количество процессоров на компьютере + 1.
	Флаг отключения автоматического пересоздания рабочего сертификата Переменная `DoNotCreateWorkCert` Значение: `false` – отключено автоматическое пересоздание (значение по умолчанию) `true` – включено автоматическое пересоздание
	Максимальное количество хранимых примененных обновлений для каждого клиента Переменная `MaxCountOfStorableUpdates` Значение: десятичное число от 0 до 4294967295, значение 0 – обновления не удаляются (значение по умолчанию 0).
	Флаг удаления старых паролей к клиентским ключевым контейнерам Переменная `DoNotClearOldPasswords` Значение: `false` – удаляются автоматически старые пароли (значение по умолчанию) `true` – не удаляются автоматически старые пароли
	UDP порт, который используется для обмена нотификациями с Клиентами управления Нотификации используются для отслеживания Клиентов управления, находящихся на связи, и оповещения их о существовании подготовленных обновлений. Переменная `NotifyServerPort` Значение: десятичное число от 0 до `65535` (значение по умолчанию 43010), значение 0 отключает механизм обмена нотификациями.
FTPServer	***Сетевой адрес для взаимодействия с сервисом продукта FileZilla Server*** Переменная `Address` Значение: локальный IP-адрес сервера FileZilla Server (значение по умолчанию 127.0.0.1).
	Сетевой порт для взаимодействия с сервисом продукта FileZilla Server Переменная `Port` Значение: порт сервиса FileZilla Server (значение по умолчанию 14147).
	Пароль для взаимодействия с сервисом продукта FileZilla Server Переменная `Password` Значение: строка, представляющая из себя пароль сервиса FileZilla Server (значение по умолчанию `<пустая строка>`).
ClientInfo	***Максимальный размер лог сообщений VPN-продукта, хранящихся для каждого Клиента управления*** Переменная `MaxVPNLogSize` Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 256).
	Максимальный размер лог сообщений FTP-сервера Переменная `MaxFTPLogSize` Значение: десятичное число от 1024 до 921600 килобайт (значение по умолчанию 51200).

	Период анализа сообщений FTP-сервера Переменная `FTPLogReadPeriod` Значение: целое число от 1 до 60 минут (значение по умолчанию 5).
`Notifications`	***Максимальное время неактивности клиента*** Переменная `MaxNoActiveTime` Значение: десятичное число от 0 до 4294967295 часов, значение 0 – отключает отслеживание максимального времени неактивности клиентов (значение по умолчанию 24).
	Максимальное время неактивности клиента для признания его находящимся не на связи Переменная `MaxNoOnlineTime` Значение: десятичное число от 1 до 60 минут (значение по умолчанию 2).
	Минимальное время перед окончанием срока действия сертификата управляемого устройства Переменная `MinCertificateFireTime` 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). При наступлении этого времени дата окончания срока действия сертификата выделена красным цветом в таблице клиентов Сервера управления.
`UPCNS`	***Флаг проверки целостности файлов продукта при старте приложения VPN UPServer console*** Переменная `NeedCheckProductFiles` Значение: `true` – выполняется проверка целостности при каждом старте приложения `false` – проверка целостности не выполняется (значение по умолчанию)
`UPCNS_Wizard`	***Время жизни ISAKMP SA в секундах для задания в настройках управляемых устройств при использовании окон мастера*** Переменная `IKE_LifetimeSec` Значение: десятичное число от 0 до 2147483647 секунд значение 0 означает, что данная переменная в конфигурации (настройках) управляемого устройства не задается (используется значение по умолчанию, заданное в LSP для данного продукта CSP VPN Gate) значение по умолчанию - 28800 (используется, когда в файле `ssettings.txt` отсутствует строка с данной переменной).
	Время жизни ISAKMP SA в килобайтах (количество обработанного трафика) для задания в настройках управляемых устройств при использовании окон мастера Переменная `IKE_Lifetime`KB Значение: десятичное число от 0 до 2147483647 килобайт значение 0 означает, что данная переменная в конфигурации (настройках) управляемого устройства не задается значение по умолчанию – 0.
	Количество IPsec SA, созданных в рамках одного ISAKMP SA, для задания в настройках управляемых устройств при использовании окон мастера Переменная `IKE_Lifetime`Keys Значение: десятичное число от 0 до 2147483647 значение 0 означает, что данная переменная в настройках управляемого устройства не задается значение по умолчанию - 0.

Время жизни IPsec SA в секундах для задания в настройках управляемых устройств при использовании окон мастера

Переменная `IPSEC_LifetimeSec`

Значение: десятичное число от 0 до 2147483647 секунд

значение 0 означает, что данная переменная в настройках управляемого устройства не задается

значение по умолчанию - 3600.

Время жизни IPsec SA в килобайтах (количество обработанного трафика) для задания в настройках управляемых устройств при использовании окон мастера

Переменная `IPSEC_Lifetime`KB

Значение: десятичное число от 0 до 2147483647 килобайт

значение 0 означает, что данная переменная в настройках управляемого устройства не задается

значение по умолчанию - 4608000.

Наименование группы для выработки ключевого материала для IPsec SA, высылаемое партнеру для согласования, при задании настроек управляемых устройств в окнах мастера

Переменная `IPSEC_Group`

Значение: `NONE` - при согласовании новой SA новый обмен по алгоритму Диффи-

Хеллмана или VKO для выработки общего сессионного ключа не выполняется. Ключевой материал заимствуется из первой фазы IKE.

`VKO_1B` – при согласовании новой SA выполняется новый обмен ключами по алгоритму VKO ГОСТ Р 34.10-2001 в рамках IPsec (значение по умолчанию)

`MODP_768` – при согласовании новой SA выполняется новый обмен ключами по алгоритму Диффи-Хеллмана в рамках IPsec (768-битовый вариант алгоритма Диффи-Хеллмана)

`MODP_1024` - 1024-битовый вариант алгоритма Диффи-Хеллмана

`MODP_1536` – 1536-битовый вариант алгоритма Диффи-Хеллмана.

Включение комбинированного алгоритма шифрования вложений IPsec ESP на основе ГОСТ 28147-89 - G2814789CPRO1-K288-CNTMAC-253, который используется при создании политики безопасности для CSP VPN Agent версии 3.11. При включении этого алгоритма вместе с шифрованием выполняется и проверка целостности пакетов.

Переменная `IPSEC_UseExtendedAlg_3_11`

Значение: `true` – включение алгоритма

`false` – выключение алгоритма.

Режим обработки списков отозванных сертификатов (CRL) для задания в настройках управляемых устройств при использовании окон мастера

Переменная `EXSET_CRLHandlingMode`

Значение: `DISABLE` – при проверке сертификата CRL не обрабатывается

`OPTIONAL` – CRL используется только в случае, если он был предустановлен или получен (и обработан) в процессе IKE обмена и является действующим

`BEST_EFFORT` – CRL используется при проверке сертификата только в том случае, если он является действующим. Этот режим отличается от режима OPTIONAL тем, что CRL может быть получен посредством протокола LDAP (если он настроен) (значение по умолчанию)

`ENABLE` – для успешной проверки сертификата обрабатывается CRL.

`HKEY_LOCAL_MACHINE\SOFTWARE\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 и 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 CSP 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 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.

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
```

19. 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`

`c:\ProgramData\UPServer\csettings.txt`

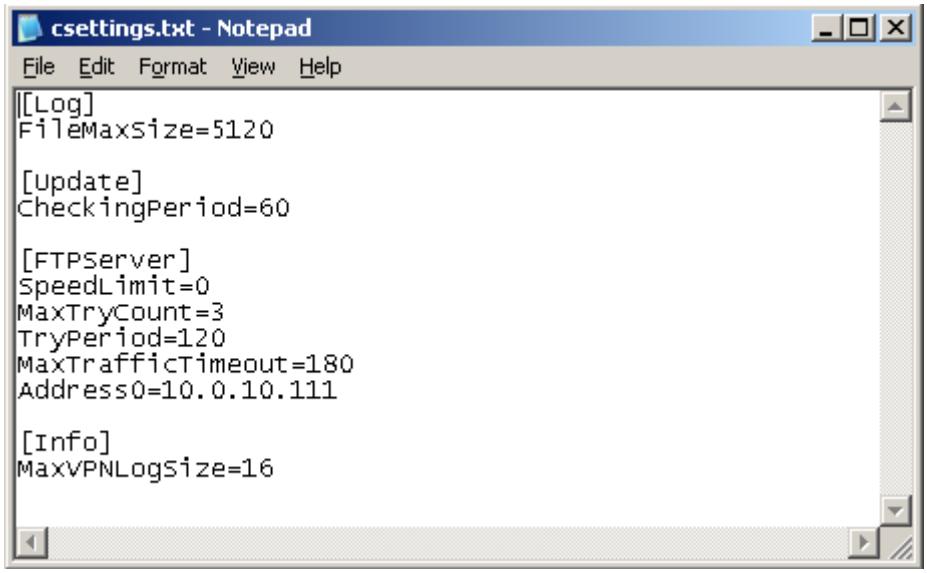

Рисунок 252

Для каждого клиента настройки Клиента управления можно изменить и сохранить в другом файле, а затем указать его в поле **UPAgent settings** (Рисунок 43) 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`.

Секция	Описание
`Log`	***Флаг включения syslog протоколирования*** Переменная `SyslogEnable` Значение: `true` - включено протоколирование `false` - выключено (значение по умолчанию – `false`).
	Адрес Syslog-сервера Переменная `SyslogSrvAddr` Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1)
	Адрес источника сообщений Переменная `SyslogFacility` Значение: строка (значение по умолчанию – `log_local7`)
	Размер файла протоколирования событий Переменная `FileMaxSize` Значение: от 10 килобайт (значение по умолчанию - 5120 килобайт, если строка отсутствует или некорректна). Имя файла протоколирования событий: для ОС Windows - `C:\Program Files\UPAgent\upagent.log` для ОС Unix – `/var/log/upagent/upagent.log`

	При достижении заданного значения данные копируются в файл `upagent.log.bak`, а файл `upagent.log` очищается.
`Update`	***Период проверки новых обновлений на Сервере управления*** Переменная `CheckingPeriod` Значение: от 60 до 86400 секунд (значение по умолчанию - 3600).
	Период между посылками нотификаций Серверу управления Переменная `NotifySendPeriod` Значение: целое число от 1 до 3600 секунд (значение по умолчанию 60).
	UDP порт Клиента управления для обмена нотификациями с Сервером управления Переменная `NotifyClientPort` Значение: целое число от 0 до 65535, 0 - отключает механизм обмена нотификациями (значение по умолчанию 43011). Нотификации используются для механизма отслеживания нахождения Клиента обновления на связи и оповещения его о существовании для них подготовленных обновлений.
	UDP порт Сервера управления для получения нотификаций от Клиента управления Переменная `NotifyServerPort` Значение: целое число от 0 до 65535 (значение по умолчанию 43010), значение 0 отключает механизм отсылки нотификаций.
`FTPServer`	***Адрес FTP сервера*** 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.
	Максимальное время ожидания соединения с FTP сервером Переменная `MaxConnectTimeout` Значение: десятичное число от 0 до 3600 секунд (значение по умолчанию 0), значение 0 отключает время ожидания соединения с FTP-сервером..
	Ограничение скорости скачивания обновлений с Сервера управления Переменная `SpeedLimit` Значение: от 512 до 4294967295 байт/секунду или 0 (0 – ограничения нет, значение по умолчанию).
	Максимальное количество попыток скачать/получить данные с/на FTP сервер(а) Переменная `MaxTryCount` Значение: целое число от 1 до 30 (значение по умолчанию 3).
	Период между попытками скачать/получить данные с/на FTP сервер(а) Переменная `TryPeriod` Значение: целое число от 0 до 300 секунд (значение по умолчанию 120).
	Максимальное время отсутствия трафика между Клиентом управления и FTP-сервером, по истечении которого соединение считается разорванным Переменная `MaxTrafficTimeout` Значение: целое число от 30 до 3600 секунд (значение по умолчанию 180).
`Info`	***Максимальный размер сообщений продукта CSP VPN Agent,***

	пересылаемых на Сервер управления Переменная `MaxVPNLogSize` Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 16).
`HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent`	***Режим работы Клиента управления*** При инсталляции Клиента управления на управляемое устройство в ключе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent` выставляется режим работы, заданный по умолчанию. После инсталляции значение можно изменить. Переменная `Mode` Значение: `windowless` – безоконный режим работы Клиента управления (значение по умолчанию) `<пустая строка>` – оконный режим работы Клиента управления (для отладки и тестирования).
	Запрос подтверждения у пользователя о начале обновления Переменная `UserAskMode` Значение: `auto` – необходимость запроса определяется на основе типа VPN-продукта (подтверждение запрашивается, если на компьютере установлен продукт CSP VPN Client) (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 `UpdateCheckMode` 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 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.

20. Описание интерфейса Сервера управления

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

20.1. 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.

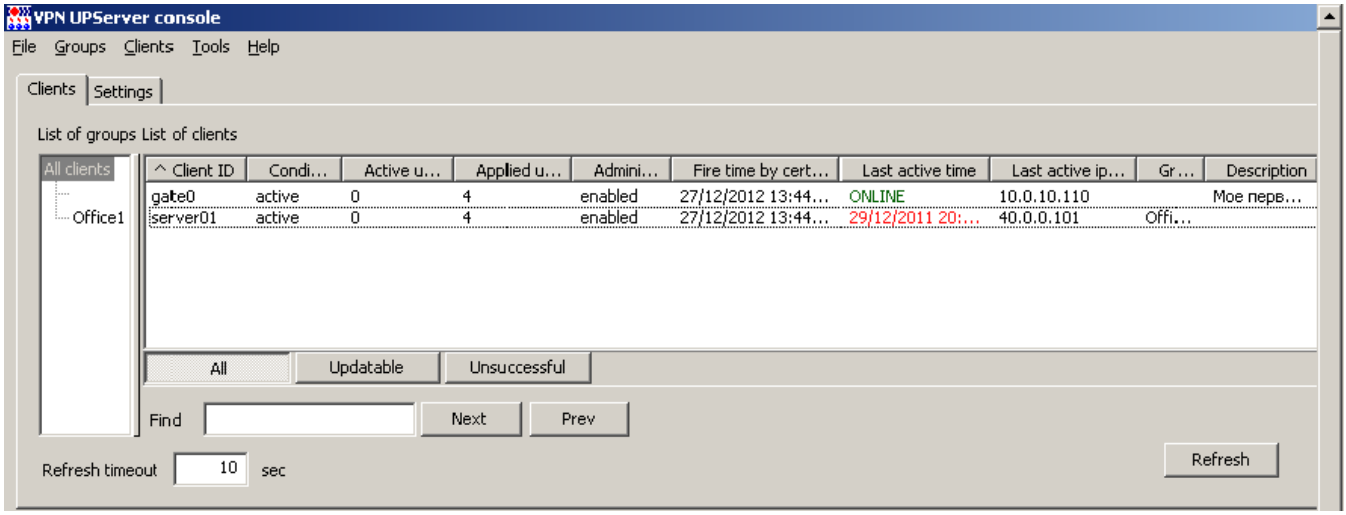

Рисунок 253

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: **new** – Клиент управления зарегистрирован на Сервере управления и еще ни разу не выходил на связь по сети **active** – Клиент управления готов к приему обновлений **waiting** – обновление для клиента создано и выложено на FTP-сервер и ожидается, что Клиент управления начнет его скачивание **updating** – 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) **failed** – 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 неприменных обновлений
Applied updates	количество успешно примененных обновлений

Administrative state	административное состояние обслуживания Клиента управления, может принимать следующие значения: **enabled** – Клиент управления обслуживается **disabled** – 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 CSP VPN Agent/S-Terra Agent
Last active time	время последнего действия, может принимать следующие значения: **дата и время** последнего удачного FTP-соединения клиента (когда клиент удачно аутентифицировался на FTP-сервере) **ONLINE** – 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 **не active**
Unsuccessful	в таблице отображаются клиенты в состоянии **failed** (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 **F3**
Prev	кнопка запуска поиска предыдущего клиента, относительно выделенного, удовлетворяющего заданной строке в поле Find. Аналогично нажатию клавиш **Shift-F3**
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 долговременным, то ожидание по кнопке **Refresh** 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 **F5**

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.

20.2. Меню File

Меню ***File*** включает одно предложение:

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

20.3. Меню Groups

Меню ***Groups*** содержит следующие элементы:

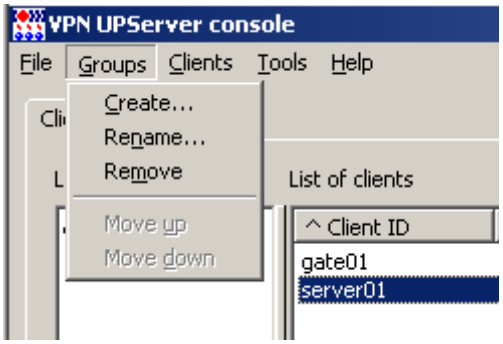

Рисунок 254

Create… - вызывает окно **Create new group** создания новой группы (группа создается как подгруппа выделенной группы), в котором надо задать имя группы (Рисунок 255).

Parent group name – имя группы, в которой создается подгруппа

Group name – имя создаваемой подгруппы.

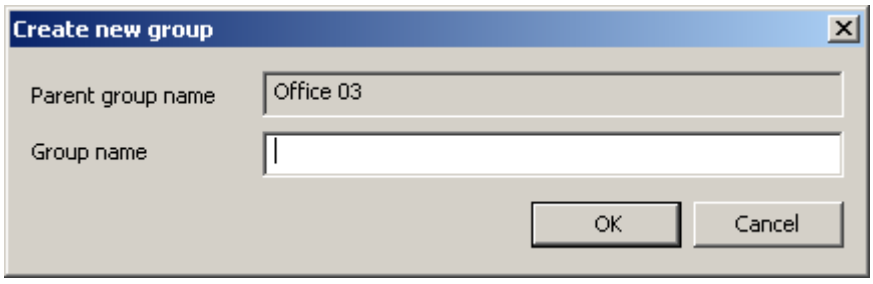

Рисунок 255

Rename… - вызывает окно переименования выделенной группы, в котором задается новое имя группы (Рисунок 256).

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.

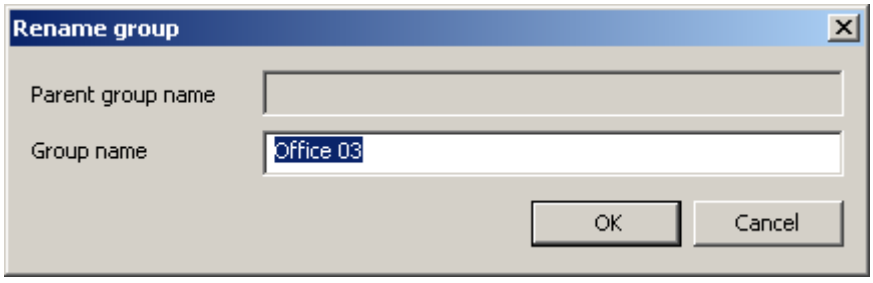

Рисунок 256

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.

20.4. Меню Clients

Меню ***Clients*** содержит следующие элементы:

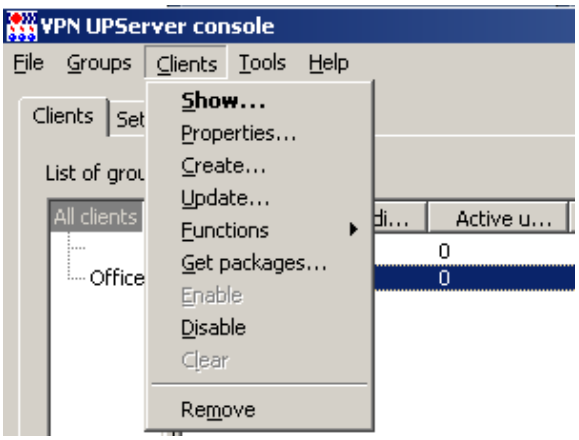

Рисунок 257

Show… – вызывает окно отображения параметров существующего клиента (Рисунок 149)

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

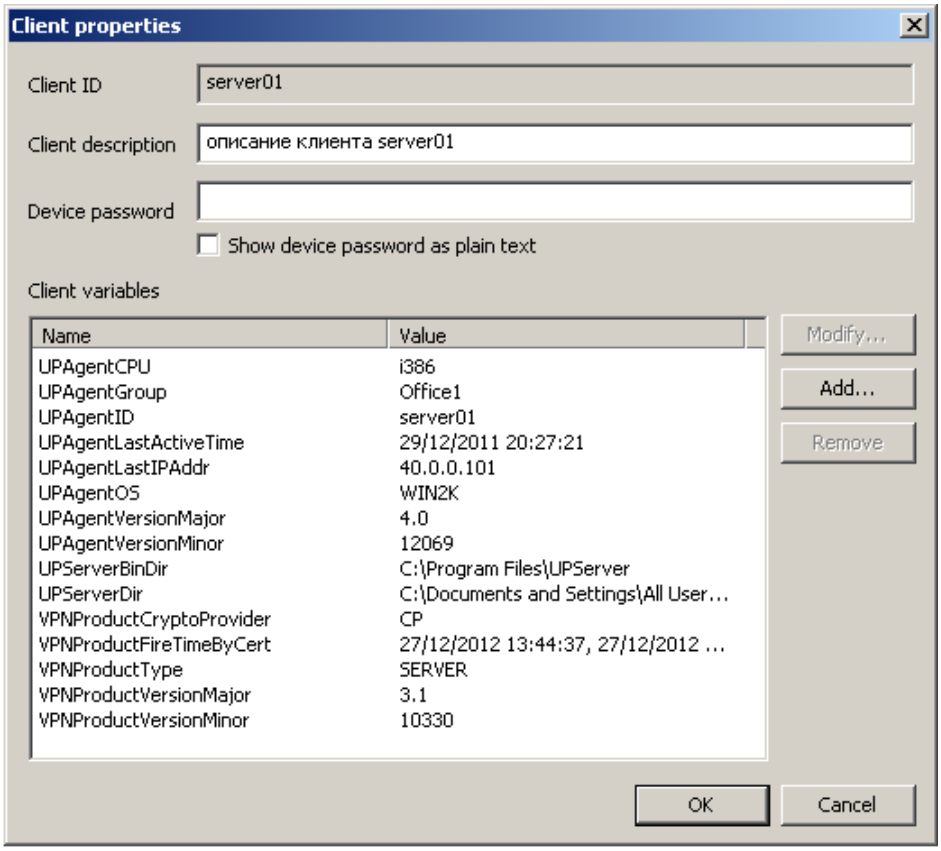

Рисунок 258

Client ID - идентификатор клиента

Client description – введенная администратором в это поле информация будет отображена в поле `Description` вкладки **Clients** (Рисунок 253)

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 70)

Update… – вызывает окно **Update client** создания обновления для существующего клиента (Рисунок 259) со следующими полями:

Client ID – идентификатор клиента

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

Product package – имя файла дистрибутива CSP VPN Agent (который был создан с помощью продукта CSP VPN Server AdminTool/CSP VPN Client AdminTool) или имя файла с данными продукта CSP VPN Agent, созданного с помощью окна **VPN data maker**, вызываемого кнопкой E

Кнопка E – вызывает окно **VPN data maker** (Рисунок 44) для задания политики безопасности и настроек продукта CSP VPN Agent

UPAgent folder – имя каталога, в котором расположен дистрибутив 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.

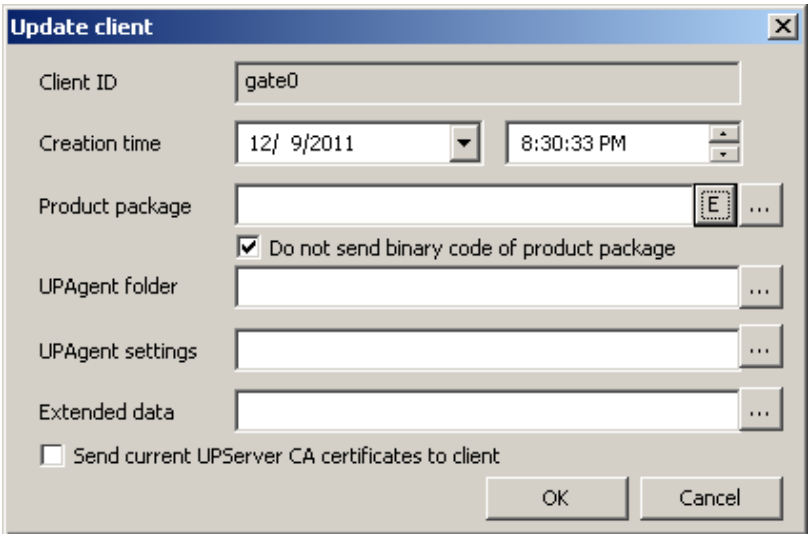

Рисунок 259

Functions – вызывает подменю (Рисунок 260):

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 92) для задания параметров ключевой пары и запроса на сертификат.

Remove… -удалить ключевую пару с управляемого устройства, при этом появляется окно **Remove container** (Рисунок 261) 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.

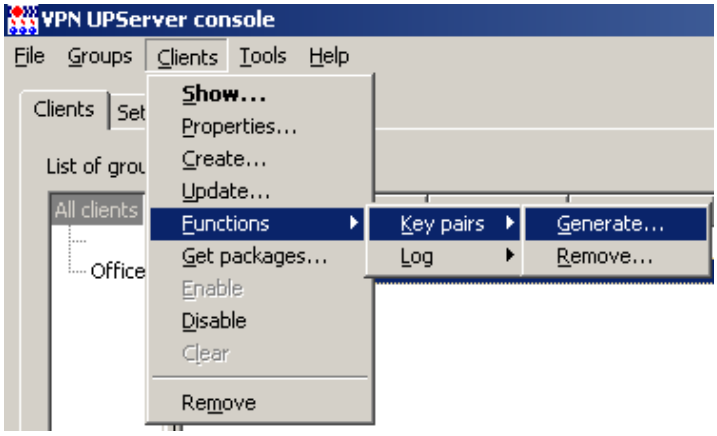

Рисунок 260

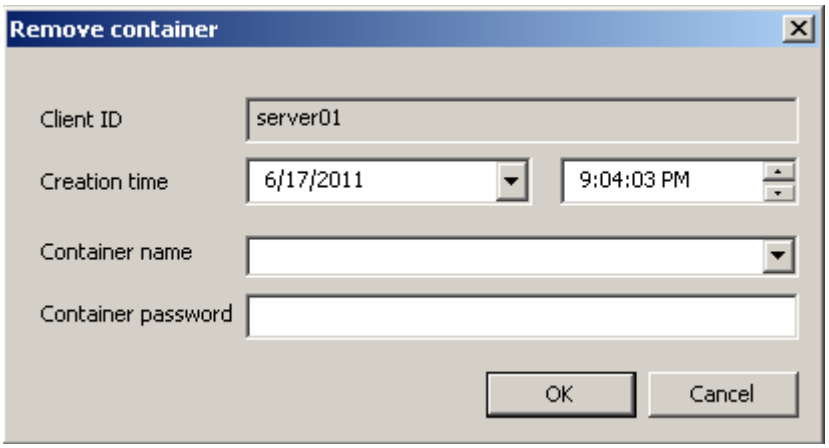

Рисунок 261

Log – позволяет задать настройки протоколирования событий на управляемом устройстве, при этом возможны два действия (Рисунок 262):

Setup… - задать параметры протоколирования в окне **Setup log** (Рисунок 263):

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.

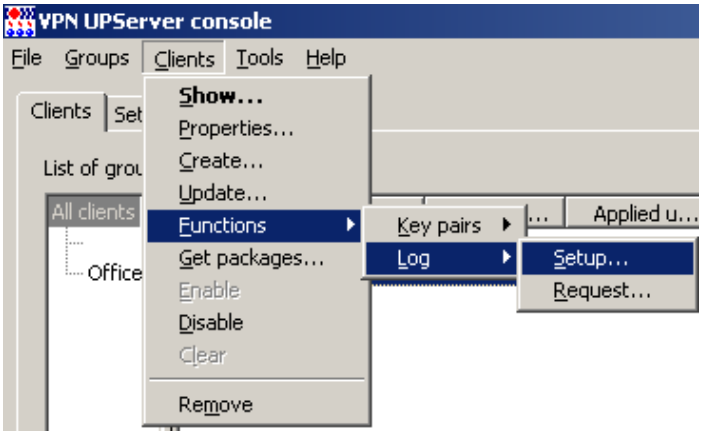

Рисунок 262

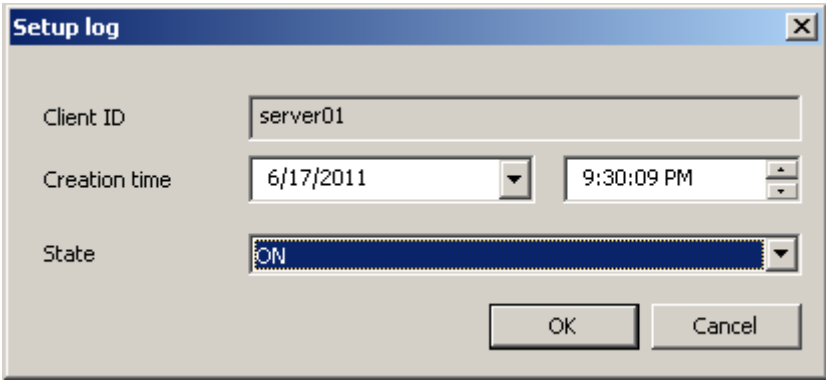

Рисунок 263

Request… - запросить данные из системы протоколирования на управляемом устройстве, заполнив в окне **Request log** (Рисунок 264) 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

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

Remove – удаляет информацию о клиенте с Сервера управления.

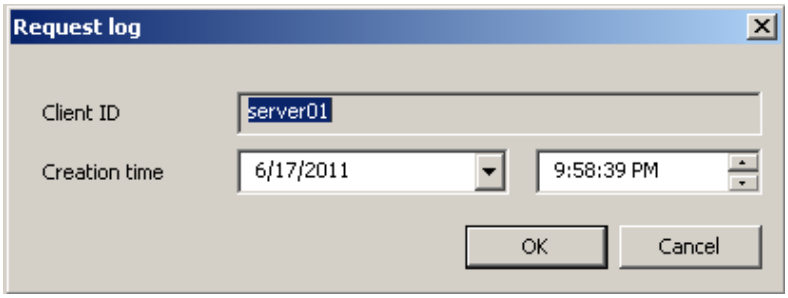

Рисунок 264

20.5. Меню Tools

Меню ***Tools*** содержит два предложения VPN data maker и VPN data converter (Рисунок 265):

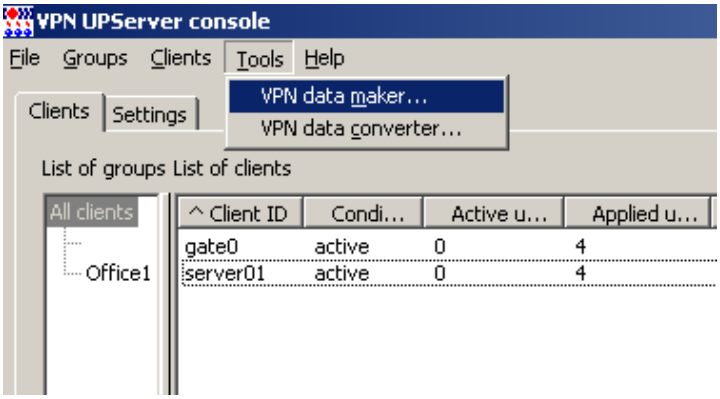

Рисунок 265

Предложение ***VPN data maker*** вызывает одноименное окно **VPN data maker** для задания настроек продукта CSP VPN Agent для нового проекта (Рисунок 266). Сделать это можно с использованием:

- вкладок 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**).

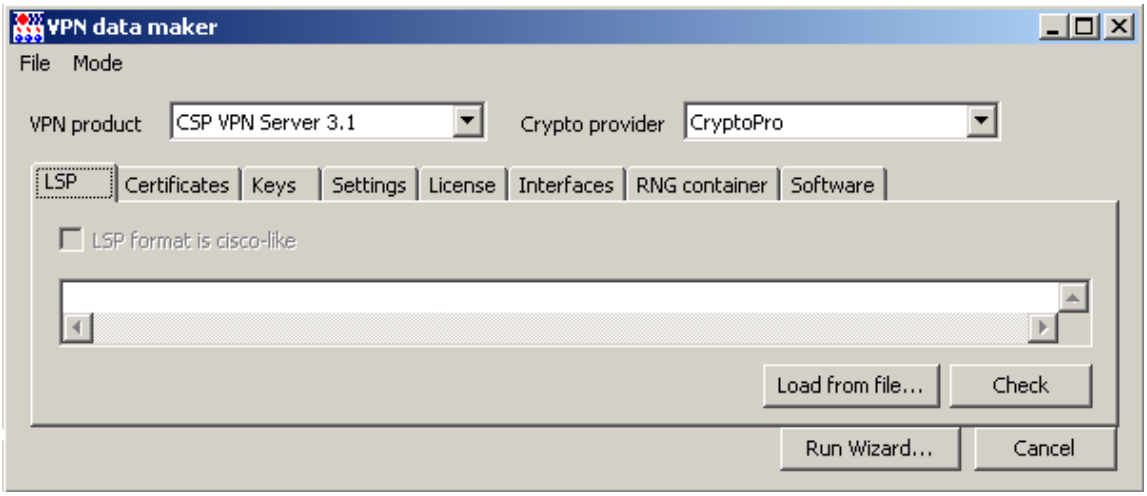

Рисунок 266

20.5.1. 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:

```
CSP VPN Client 3.1
CSP VPN Server 3.1
CSP VPN Gate 3.1
CSP VPN Gate 3.1 on token
CSP VPN Client 3.11
CSP VPN Server 3.11
CSP VPN Gate 3.11
CSP VPN Gate 3.11 on token
S-Terra Client 4.0
S-Terra Server 4.0
S-Terra Gate 4.0
```

Crypto provider – выпадающий список с используемым криптопровайдером в продукте:

`CryptoPro` – КриптоПро CSP 3.6 компании Крипто-Про
`SignalCOM` – Крипто-КОМ CSP 3.2 компании Сигнал-КОМ
`S-Terra` – криптография от компании С-Терра СиЭсПи

LSP – вкладка для задания локальной политики безопасности продукта CSP VPN Agent, предписанной управляемому устройству (Рисунок 266):

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.

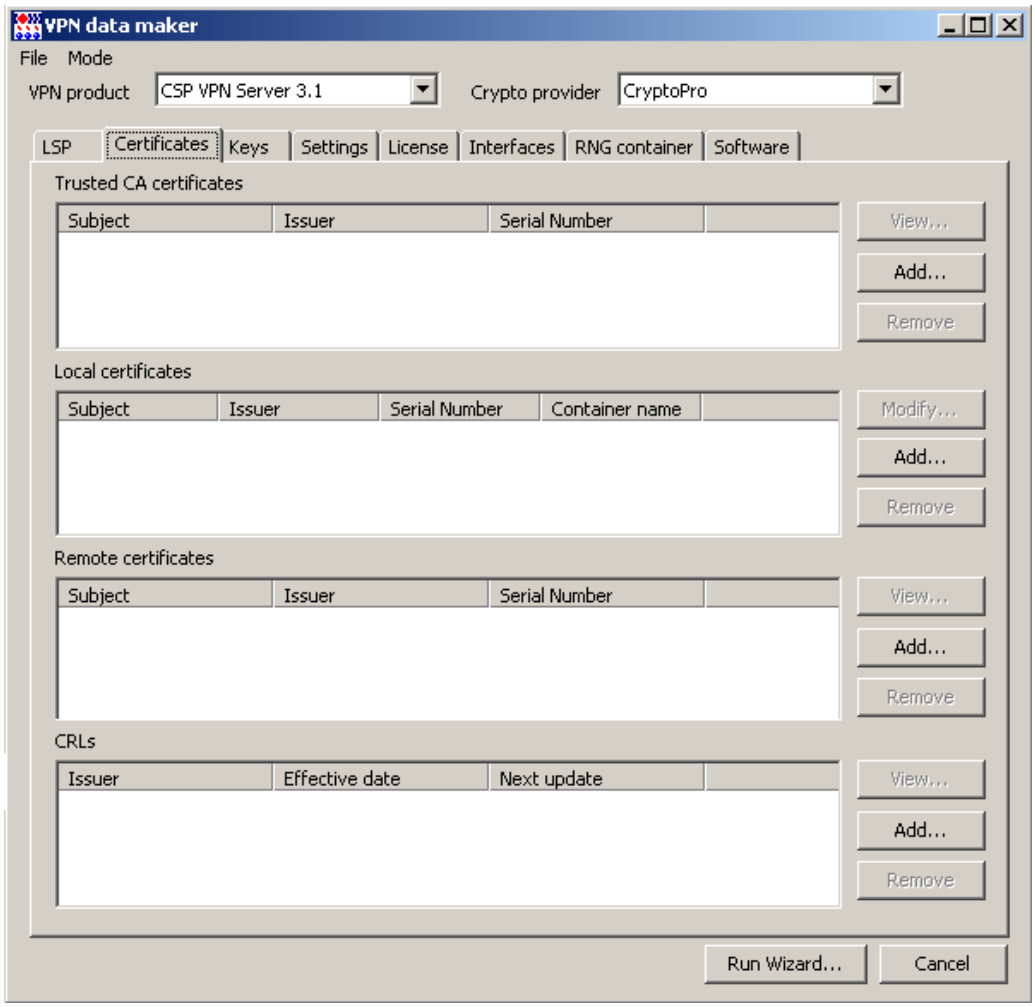

Рисунок 267

Certificates – вкладка для задания CA, локальных, партнерских и списков отозванных сертификатов для продукта CSP VPN Agent (Рисунок 267).

Keys – вкладка для задания предопределенных ключей для работы продукта CSP VPN Agent с партнерами (Рисунок 268).

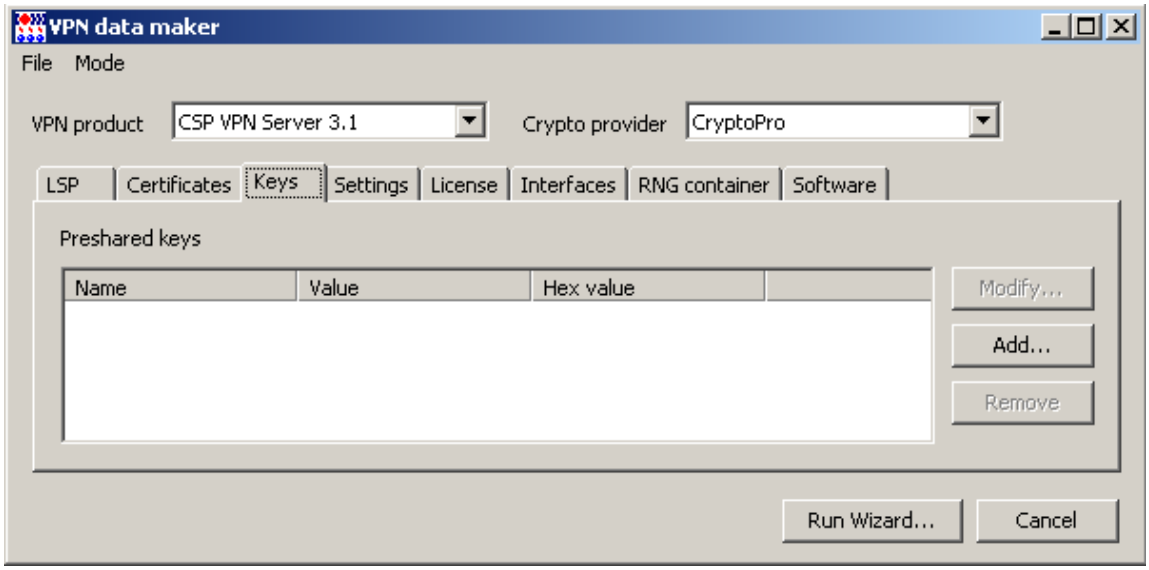

Рисунок 268

Settings – вкладка для задания настроек управляемого устройства.

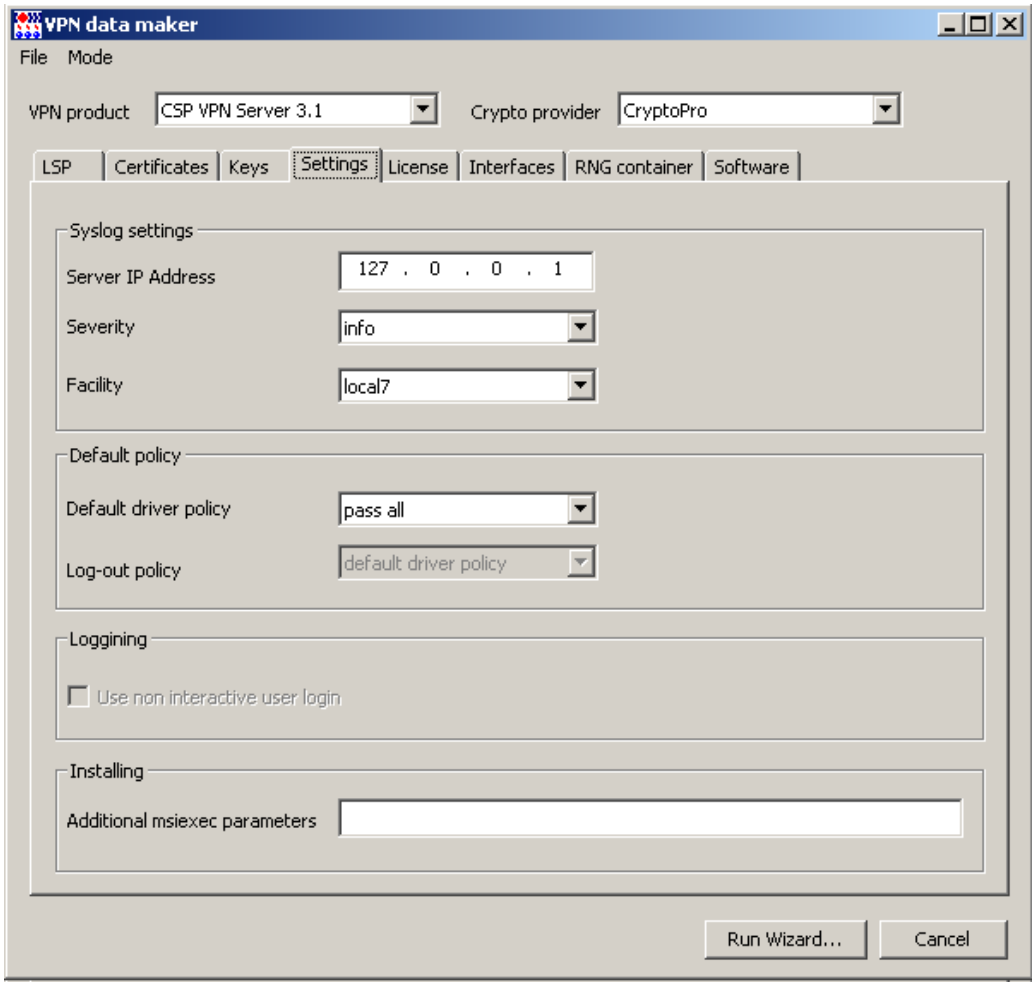

Рисунок 269

License – вкладка для ввода данных лицензии на продукт CSP VPN Agent.

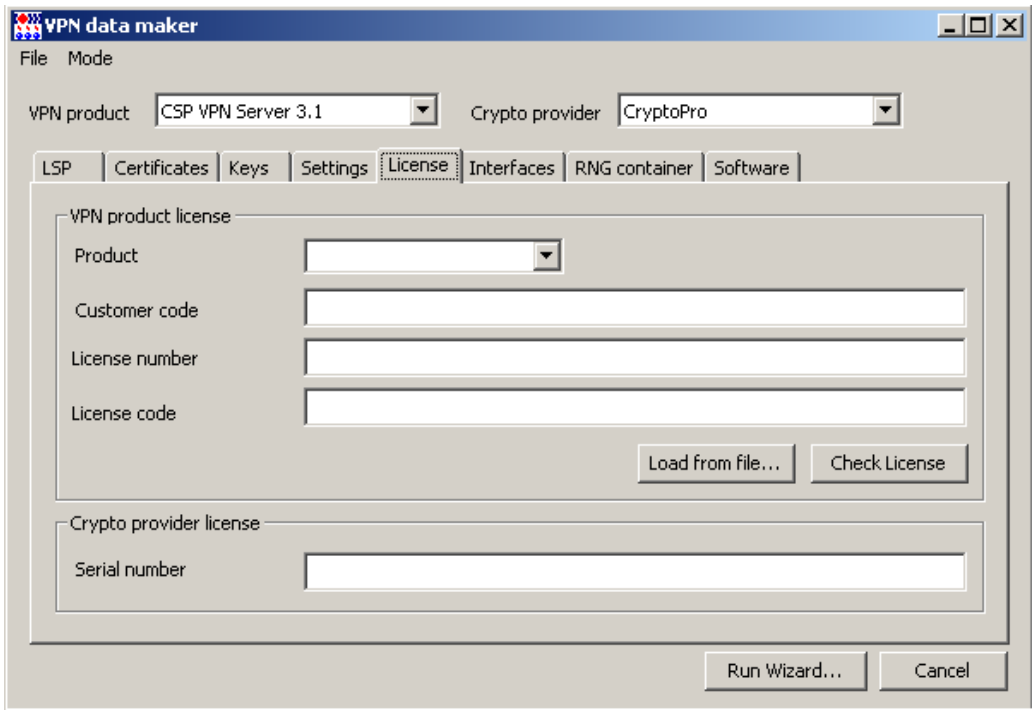

Рисунок 270

Interfaces – вкладка для задания настроек сетевых интерфейсов управляемого устройства.

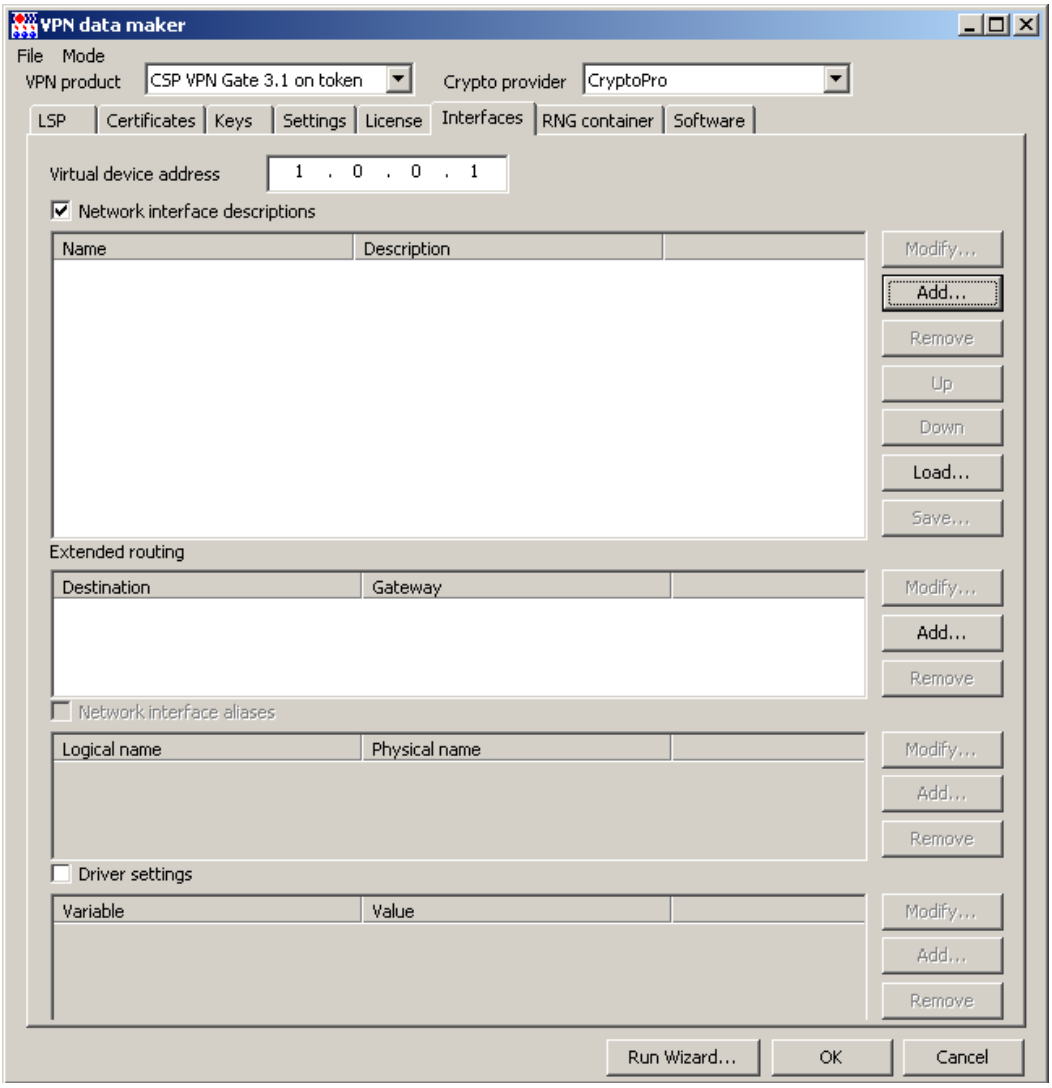

Рисунок 271

Virtual device address – поле доступно только для продукта CSP VPN Gate 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 CSP VPN Gate 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 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.

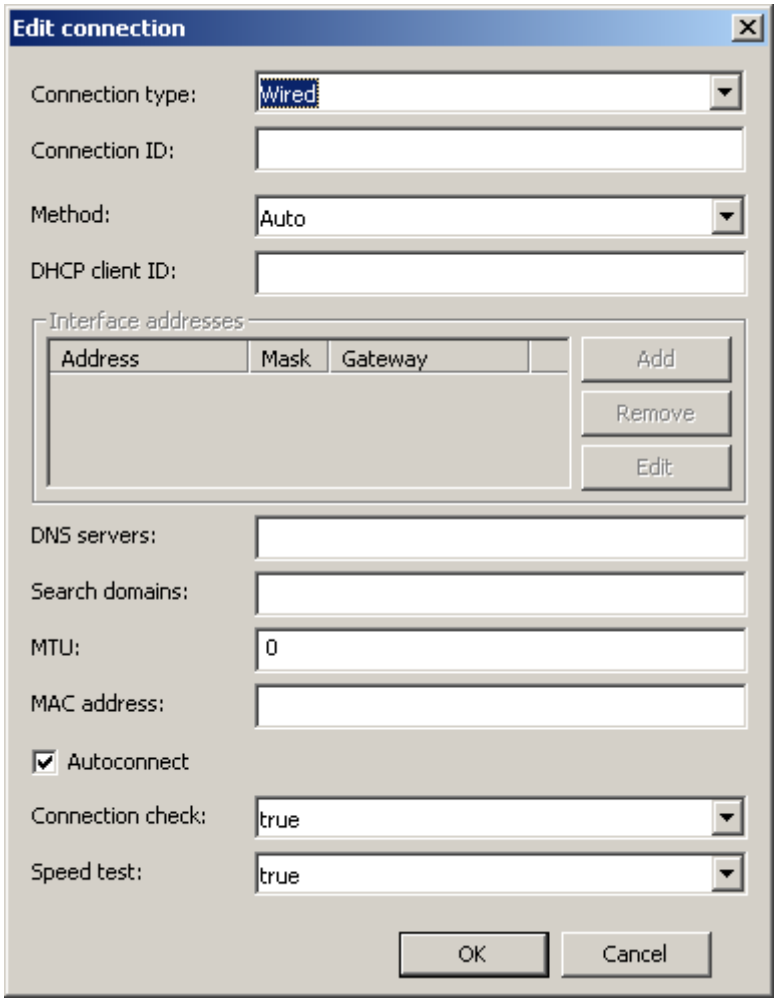

Рисунок 272

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 разделются 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).

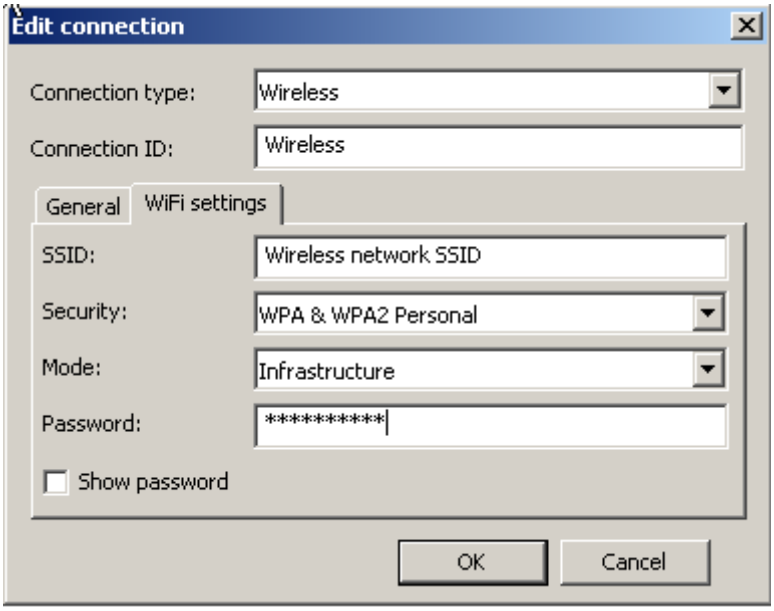

Рисунок 273

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.

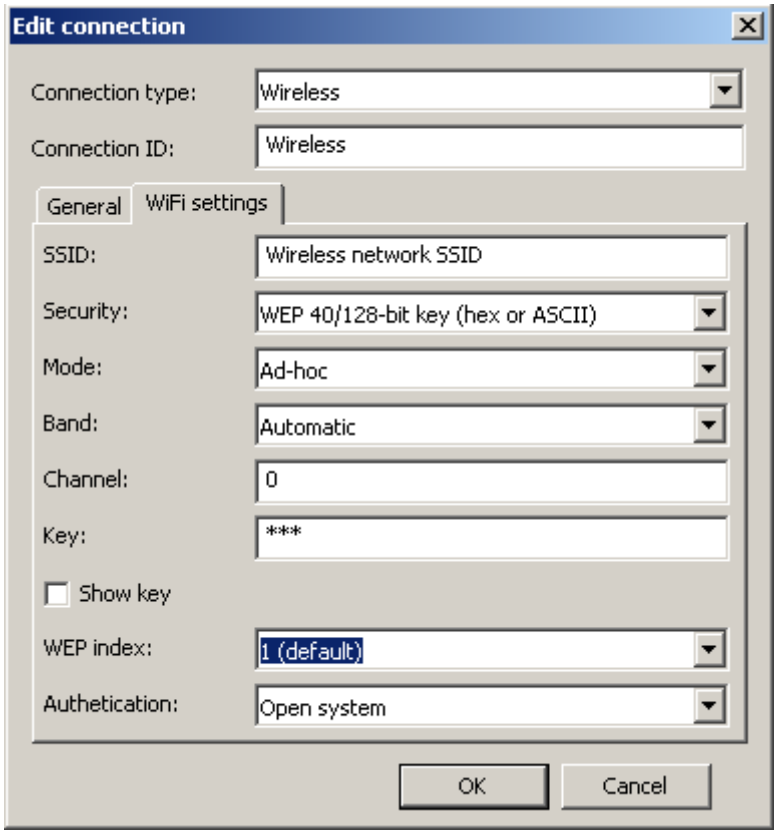

Рисунок 274

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. Задает 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».

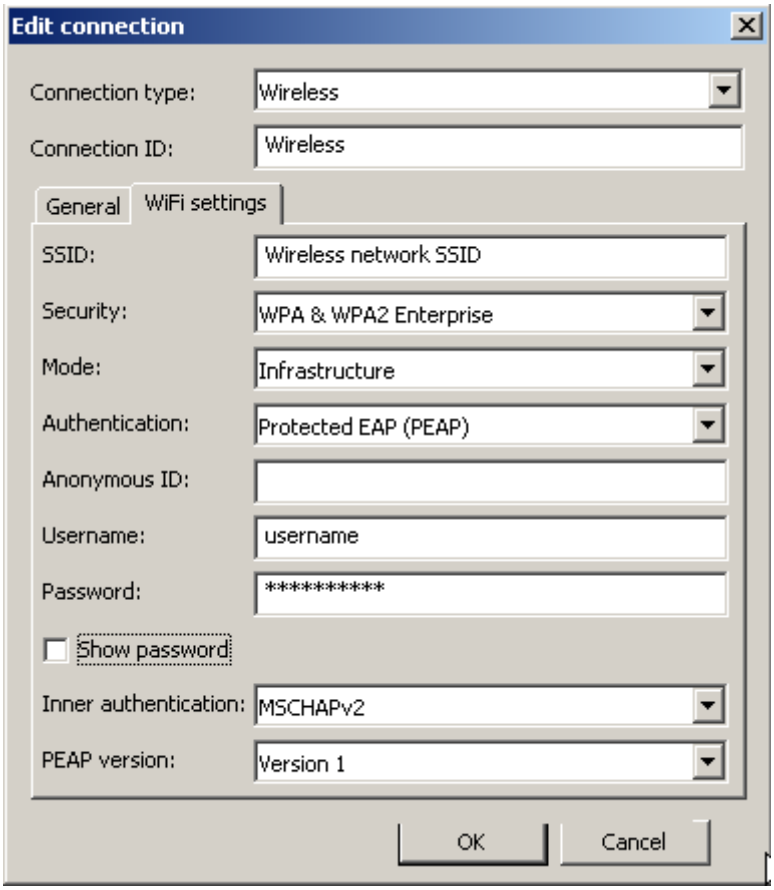

Рисунок 275

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».

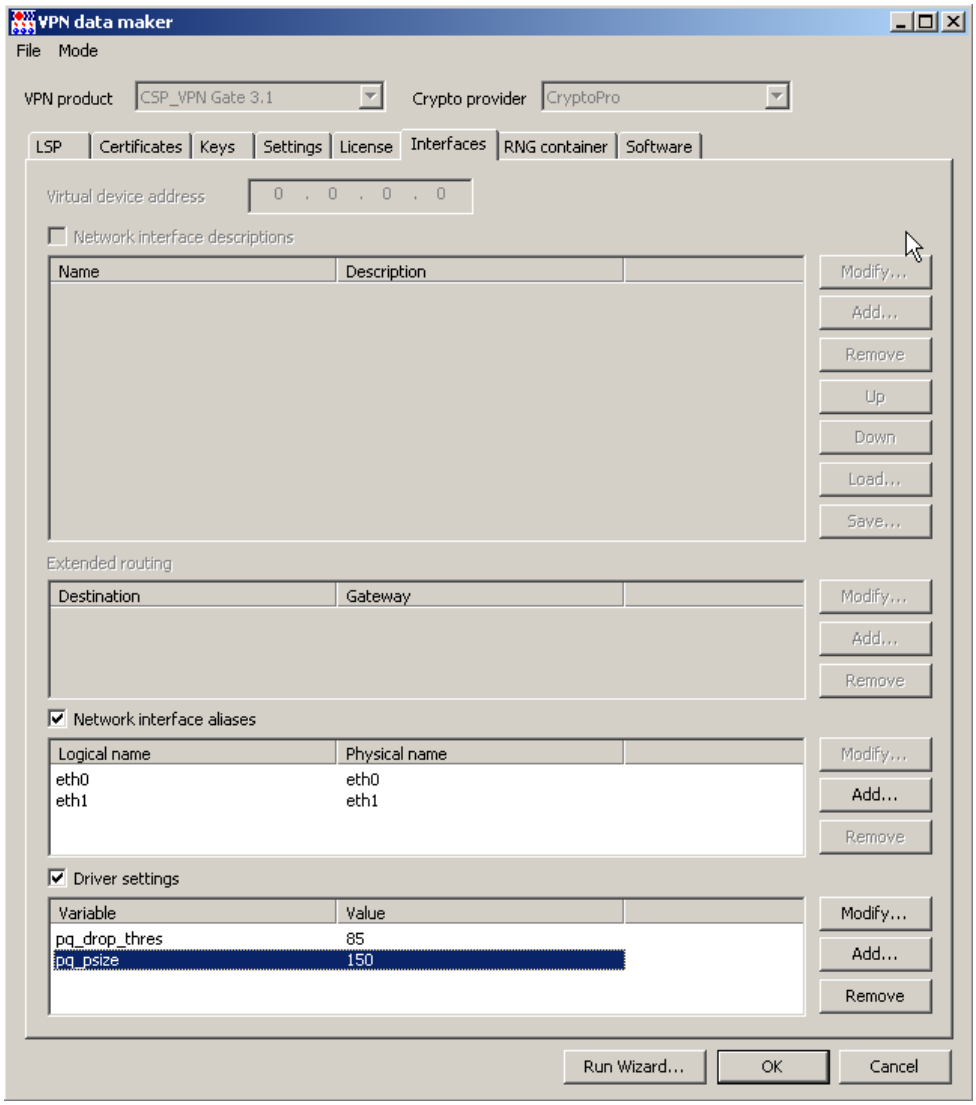

Рисунок 276

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

Driver settings – установка этого флажка позволяет изменить настройки IPsec драйвера, установленные по умолчанию (Рисунок 277). Эти настройки имеются только у продукта CSP VPN Gate. Поэтому описание этих настроек (утилита drv_mgr) см. в документе «Специализированные команды», входящем в состав «Руководства администратора Программный комплекс CSP VPN Gate».

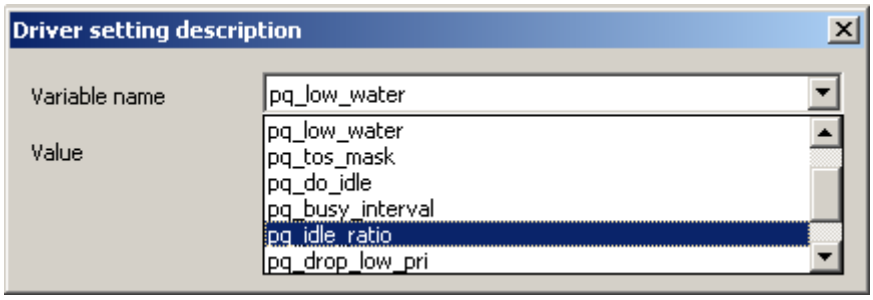

Рисунок 277

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

контейнер представляет собой каталог, поэтому имя контейнера – имя каталога (Рисунок 278). Используется только для криптопровайдера SignalCOM.

При создании дистрибутива продукта `CSP VPN Client/CSP VPN Server` 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 CSP VPN Gate 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 CSP VPN Agent. Значения по умолчанию – каталоги CSP VPN Client, CSP VPN Server, CSP VPN Gate.

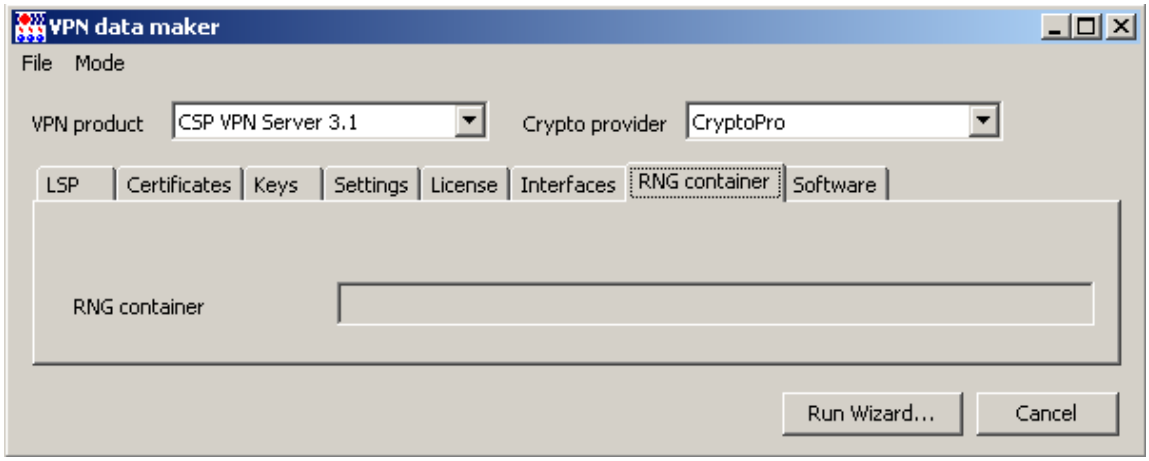

Рисунок 278

Software – вкладка для задания настроек дополнительных продуктов, установленных на управляемом устройстве (Рисунок 279). Эта вкладка доступна для редактирования только для продукта CSP VPN Gate, установленного на СЗН «СПДС-USB-01», т.е. при настройке СПДС «ПОСТ.

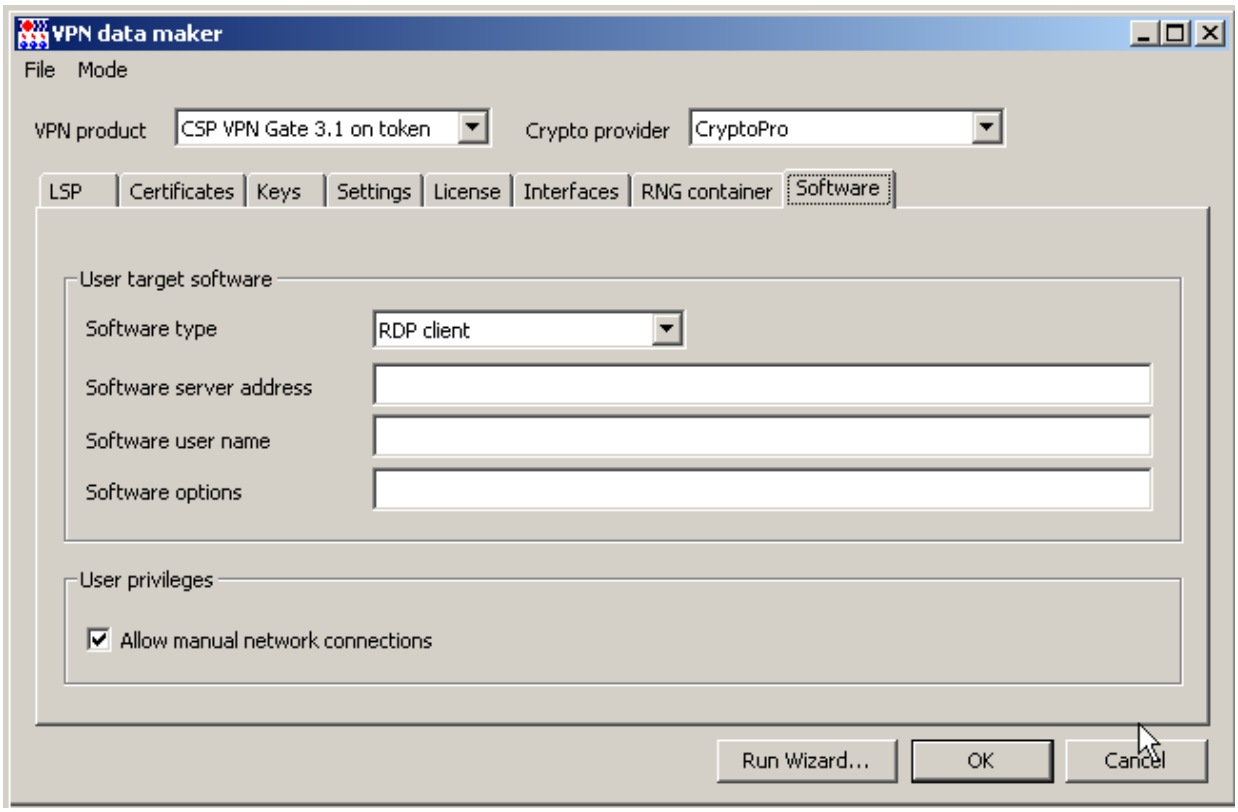

Рисунок 279

Сохранение и загрузка настроек продукта

Меню ***File*** окна **VPN data maker** содержит два предложения (Рисунок 280):

Load – загружает настройки из файла данных продукта CSP VPN Agent

Save as – сохраняет в файл данные продукта CSP VPN Agent, отраженные во вкладках окна **VPN data maker.**

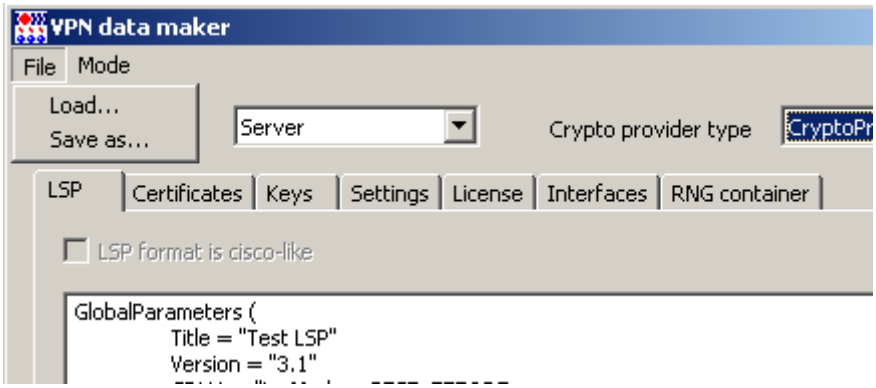

Рисунок 280

20.5.2. Задание политики и настроек с использованием мастера

При нажатии кнопки Run Wizard в окне **VPN data maker** появляется окно мастера создания несложной политики безопасности и настроек для управляемого устройства (Рисунок 281).

При выборе аутентификации с использованием сертификатов доступны следующие поля (все поля подробно описаны в документе «Программный комплекс CSP VPN Client/CSP VPN Server. Руководство администратора»).:

CA certificate file – здесь отражается поле Subject корневого сертификата Удостоверяющего Центра (Trusted CA Certificate). Для этого в конце поля нажмите кнопку [...], в открывшемся окне выберите файл с CA сертификатом. Обязательный параметр.

Device certificate file – здесь отражается поле Subject локального сертификата управляемого устройства. Для этого разместите на Сервере управления файл с локальным сертификатом и в конце поля нажмите кнопку [...], в открывшемся окне выберите данный файл. Обязательный параметр.

Device container name – уникальное имя контейнера с ключевой парой, размещенного на управляемом устройстве. При указании локального сертификата это поле заполняется автоматически.

Device container password – пароль к контейнеру. При использовании eToken в этом поле нужно указать PIN-код к токену

Key type – тип секретного ключа, хранящегося в контейнере, имеет три значения:

- Autodetect – тип ключа будет определяться автоматически при первом обращении к контейнеру секретного ключа. Определение типа ключа основано на проверке соответствия открытого ключа локального сертификата и секретного ключа в контейнере. Значение по умолчанию.
- Signature – ключ для подписи
- Exchange – ключ для обмена.

Device identity type – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Поле содержит выпадающий список со следующими значениями:

- Default – в качестве идентификатора партнеру будет высылаться действительный IP-адрес управляемого устройства

- Distinguished Name – в качестве идентификатора партнеру будет высылаться значение Subject из локального сертификата управляемого устройства, показываемое в поле Device identity value, если оно задано в сертификате
- Email – в качестве идентификатора партнеру будет высылаться значение поля E-mail расширения локального сертификата, показываемое в поле Device identity value, если оно там задано
- FQDN – в качестве идентификатора партнеру будет высылаться значение доменного имени управляемого устройства, считываемое из поля DNS расширения локального сертификата и показываемое в поле Device identity value, если оно там задано
- IPV4Addr – в качестве идентификатора партнеру будет высылаться первый IP-адрес, указанный в расширении сертификата, и показываемый в поле Device identity value, если он там задан.

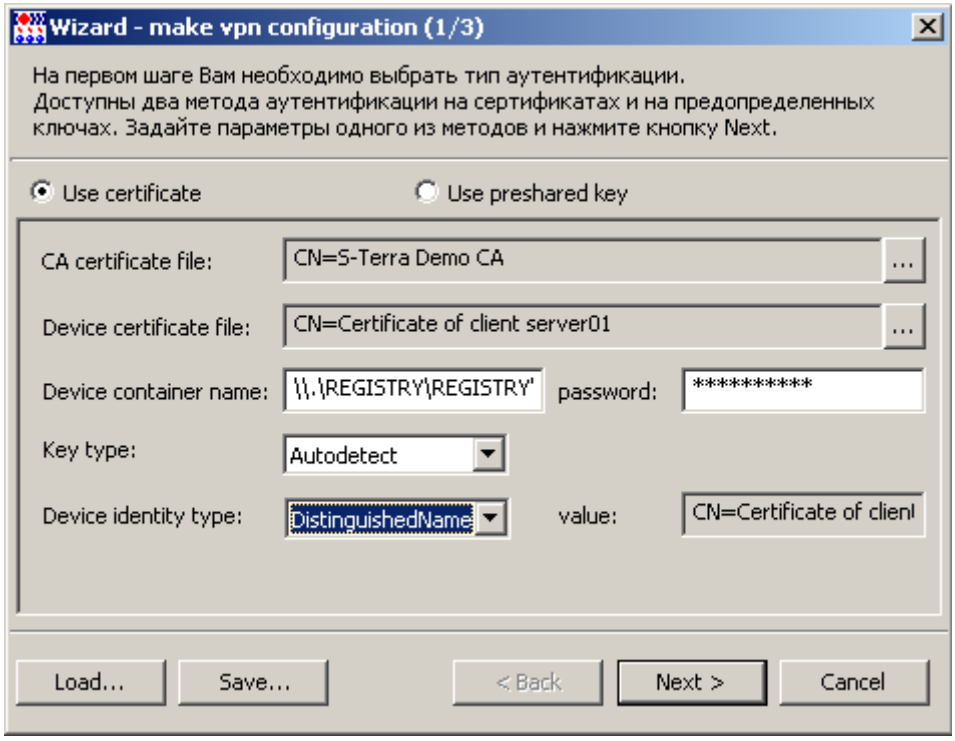

Рисунок 281

При выборе аутентификации с использованием предопределенного ключа доступны следующие поля (Рисунок 282):

Key name –имя предопределенного ключа. Обязательный параметр.

Значение предопределенного ключа можно ввести в двух полях:

From keyboard – значение вводится с клавиатуры. Если предопределенный ключ задан несколькими строками, то каждый перенос в теле ключа будет представлен двумя символами 0x0D 0x0A (символ возврата и перевода каретки) и тогда при подготовке предопределенного ключа для партнера должны быть использованы эти символы.

From file – значение ключа считывается из файла с именем, указанным в поле **Key file name**

Device identity type – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Может принимать следующие значения:

- Default – в качестве идентификатора партнеру будет высылаться действительный IP-адрес управляемого устройства

- IPV4Addr – в качестве идентификатора партнеру будет высылаться IP-адрес, который нужно задать в поле Device identity value.

После ввода аутентификационной информации нажмите кнопку Next. Во втором окне мастера (Рисунок 282) задайте правила фильтрации и защиты трафика между Сервером управления и управляемым устройством.

Задание правил и ввода лицензионной информации были описаны в разделе «Настройка и управление центральным шлюзом» и «Настрока и управление устройством с CSP VPN Server/CSP VPN Client».

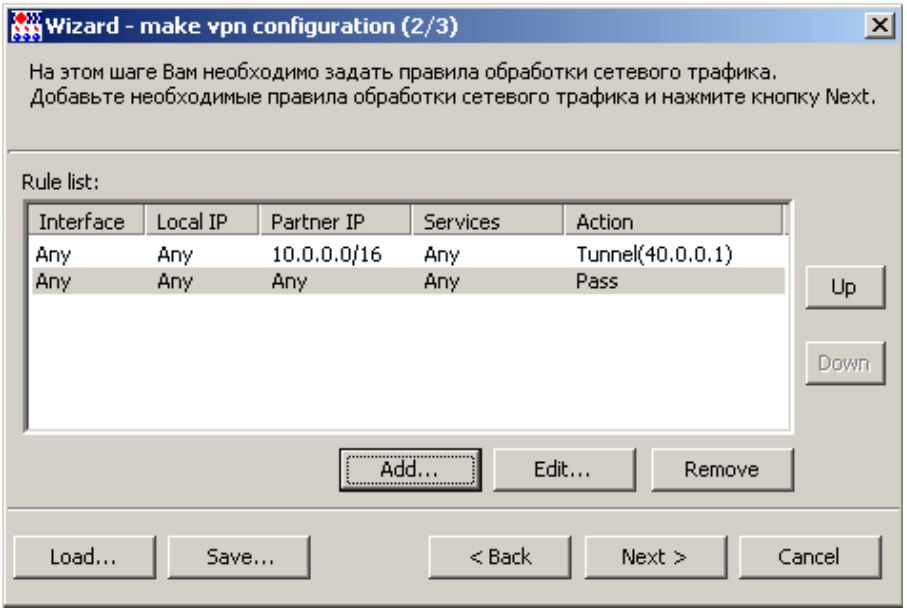

Рисунок 282

20.5.3. 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 CSP VPN Agent.

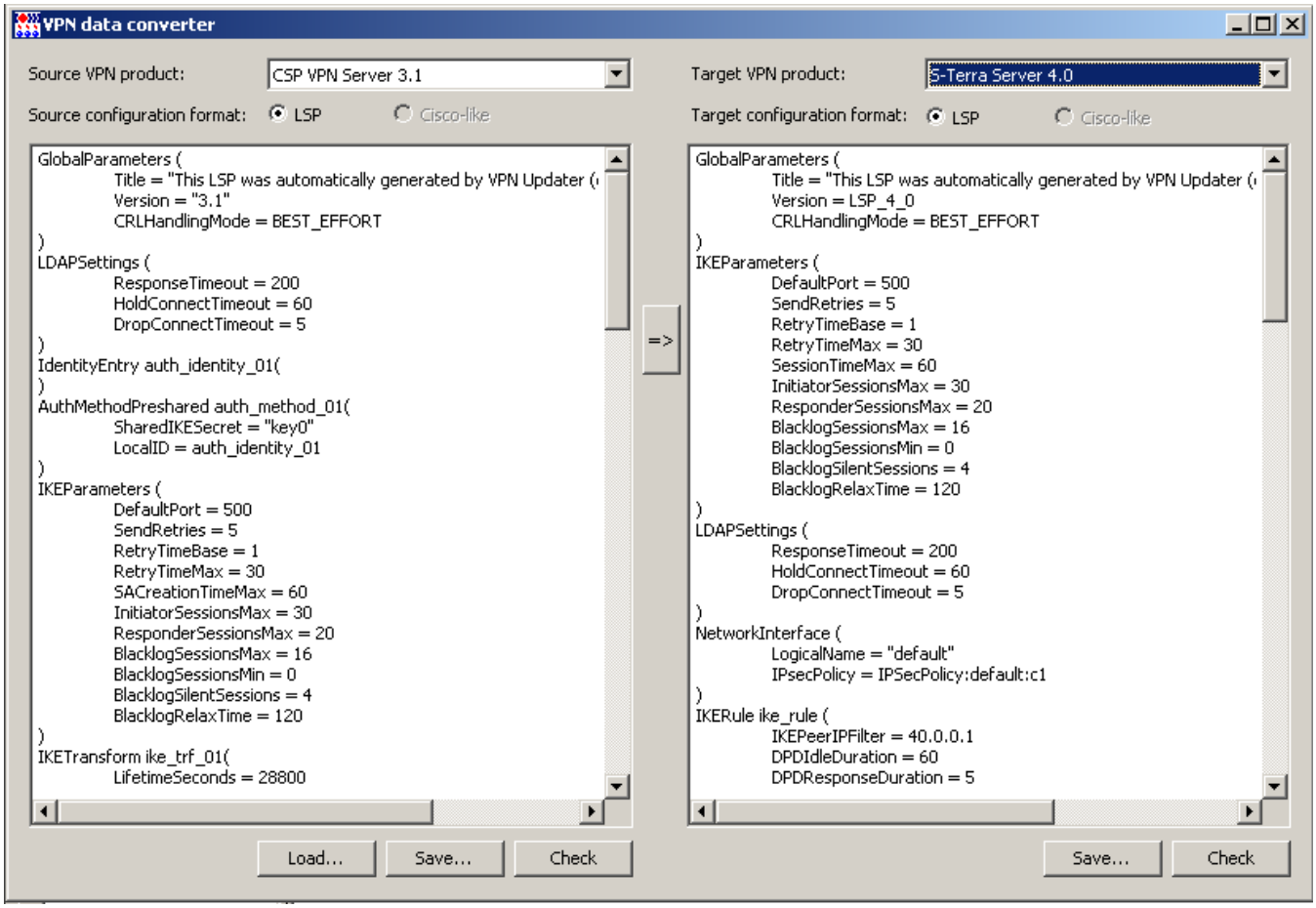

Рисунок 283

20.6. Меню Help

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

Рисунок 284

21. Протоколирование событий

21.1. 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.`

21.2. 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.

21.3. Продукт CSP VPN Agent

На управляемом устройстве все сообщения от продукта **CSP VPN Agent** 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 **CSP VPN Gate** 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-диском

Протоколирование работы некоторых утилит и сервисов передается в специальные файлы. Все сообщения и настройка syslog-клиента и сервера описаны в документе «Программный комплекс CSP VPN Gate. Версия 3.11. Протоколирование событий».

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