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
Настройка СПДС «ПОСТ»
Версия 3.11

Руководство администратора

30.09.2014

Содержание

Продукт С-Терра КП 3.11

Назначение продукта

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

«Сервер безопасности CSP VPN Server. Версия 3.1/3.11/4.1»

«Клиент безопасности CSP VPN Client. Версия 3.1/3.11/4.1»

«Шлюз безопасности CSP VPN Gate. Версия 3.1/3.11/4.1»,

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

В данном документе описано управление продуктом CSP VPN Gate 3.1, установленным на СЗН «СПДС-USB-01», который далее будем называть СПДС (среда построения доверенного сеанса) или **СПДС «ПОСТ»**, или управляемое устройство. СПДС «ПОСТ» - среда построения доверенного сеанса для удаленного доступа к защищаемым ресурсам корпоративной сети. Настройка и управление СПДС «ПОСТ» осуществляется с использованием продукта С-Терра КП.

Подробно сам продукт СПДС «ПОСТ» описан в документах «Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1». СПДС «ПОСТ». Руководство администратора и «Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1». СПДС «ПОСТ». Руководство пользователя.

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 продукта CSP VPN Gate и его настроек, инсталлированном на управляемом устройстве.
- ***Клиент управления*** – клиентская часть продукта, устанавливается на управляемое устройство с инсталлированным продуктом CSP VPN Gate и предназначена для его управления.

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

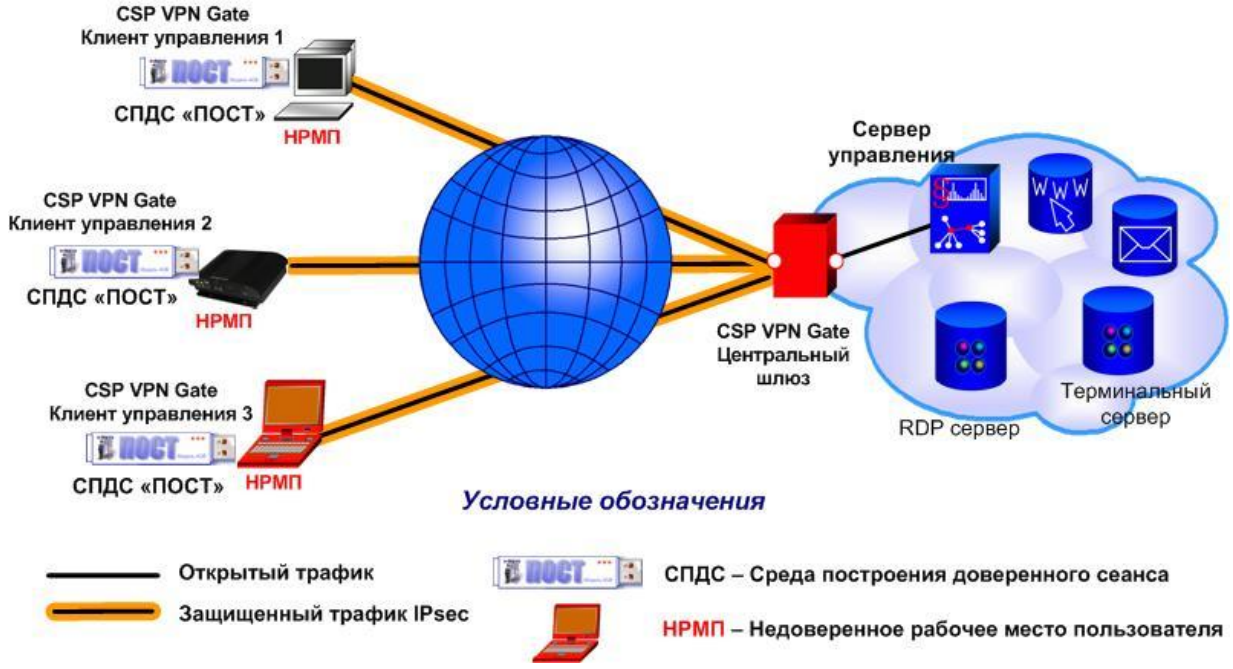


Рисунок 1

Сервер управления устанавливается на выделенный компьютер, размещенный в локальной сети, защищаемой шлюзом безопасности. На Сервере управления создаются настройки Клиента управления для каждого управляемого устройства и сами обновления.

Дистрибутив Клиента управления размещен на СПДС «ПОСТ», при получении настроек Клиент управления устанавливается на управляемое устройство.

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.

Возможности продукта С-Терра КП

На СПДС «ПОСТ» с установленным продуктом CSP VPN Gate, КриптоПро CSP 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 Gate
- настройки драйвера продукта CSP VPN Gate
- локальные сертификаты продукта CSP VPN Gate, CA-сертификат, сертификаты партнеров, список отозванных сертификатов
- контейнеры с ключами сертификатов
- настройки протоколирования событий продукта CSP VPN Gate
- лицензия на продукт CSP VPN Gate и КриптоПро CSP
- 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 Gate
- локальная политика безопасности продукта CSP VPN Gate (в текстовом виде или в виде cisco-like конфигурации)
- настройки драйвера продукта CSP VPN Gate
- локальные сертификаты продукта CSP VPN Gate, 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 Gate на каждом устройстве
- запросы на локальные сертификаты
- настройки протоколирования событий продукта CSP VPN Gate
- журнал регистрации событий продукта CSP VPN Gate и Клиента управления
- информация о лицензиях продуктов CSP VPN Gate и КриптоПро CSP.

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

- использование окон мастера для создания несложной политики безопасности продукта CSP VPN Gate для управляемого устройства
- управление устройством СПДС «ПОСТ»
- создание клонов клиента для устройства с CSP VPN Gate, отличающихся локальными сертификатами, лицензиями и т.д.
- изменение настроек готового проекта для CSP VPN Gate – утилита vpnmaker
- автоматизация процесса управления устройствами - утилита upmgr
- использование ГОСТ-сертификатов для подписывания обновлений.

Характеристика продукта С-Терра КП

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 CA сертификата Сервера управления. CA сертификат Сервера управления устанавливается на каждый Клиент управления во время первой 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_40.exe
vcredist_x86.exe
WINDOWS
```



```
LINUXRHEL5
Additional
```

Note

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

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

В дальнейшем описании документа приведены примеры для стенда (Рисунок 2), в который включен шлюз безопасности с установленным продуктом CSP VPN Gate (центральный шлюз), защищающий подсеть с Сервером управления и RDP-сервером. В стенде присутствует компьютер (IP-адрес 10.0.232.24/16) с недоверенным рабочим местом пользователя (НРМП). Для построения доверенного сеанса связи с RDP-сервером используется СПДС «ПОСТ», который вставляется в USB-порт устройства с НРМП. Первоначальная настройка СПДС «ПОСТ» осуществляется локально, а дальнейшие обновления настроек будут осуществляться удаленно централизованно с Сервера управления. Взаимодействие между СПДС «ПОСТ» и Сервером управления осуществляется по защищенному каналу IPsec, построенному до центрального шлюза. В качестве RDP-сервера используется компьютер с ОС Windows XP и разрешенным удаленным доступом к этому компьютеру.

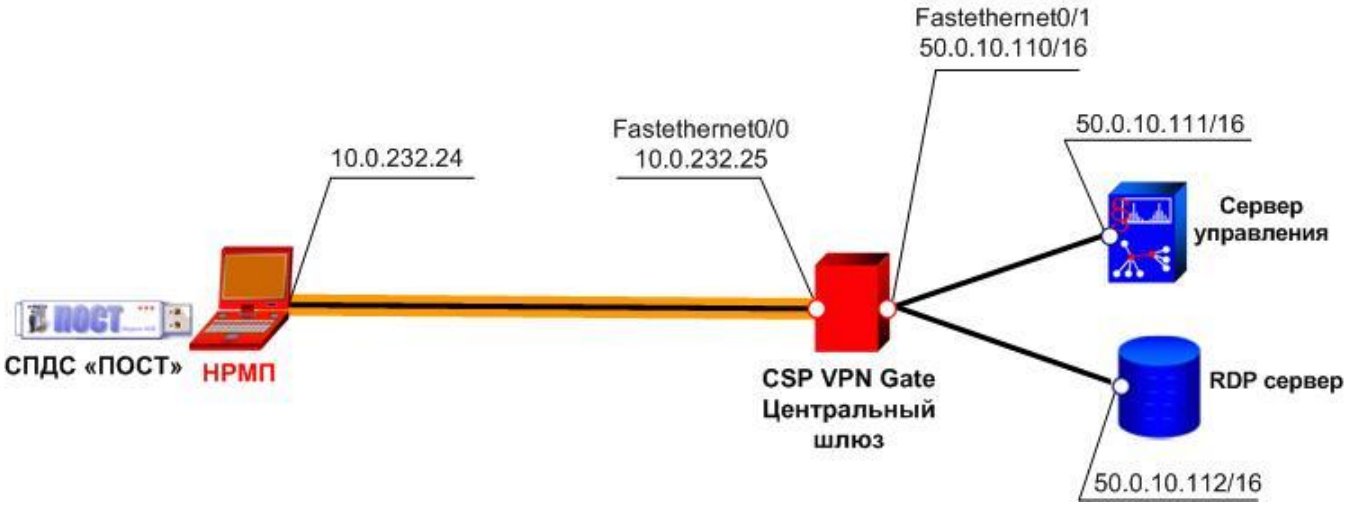


Рисунок 2

Сценарии управления

Можно выделить два последовательных сценария обновления настроек продукта CSP VPN Gate на управляемом устройстве (СПДС «ПОСТ»).

Первый сценарий (при первом обращении к управляемому устройству):

подготовка скриптов на Сервере управления для инсталляции Клиента управления и настройки установленного продукта CSP VPN Gate, доставка и локальный запуск на управляемом устройстве.

Второй сценарий (все последующие взаимодействия с управляемым устройством):

создание обновлений на Сервере управления и передача на управляемое устройство по защищенному IPsec соединению.

Далее по тексту управляемые устройства будем называть клиентами, на которых установлен продукт CSP VPN Gate и Клиент управления.

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

Ниже описаны два сценария по шагам.

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: На Сервере управления подготовьте скрипты для настройки центрального шлюза, доставьте их и запустите локально (см. раздел «Настройка и управление центральным шлюзом»).

Шаг 3: Для управляемого устройства СПДС «ПОСТ» создайте локальный сертификат (контейнер с секретным ключом запишите на СПДС «ПОСТ»), настройте политику безопасности, подготовьте скрипты для инсталляции Клиента управления и инициализации CSP VPN Gate. Скрипты запишите на СПДС «ПОСТ» (см.раздел «Настройка и управление СПДС «ПОСТ»).

Шаг 4: Подключите СПДС «ПОСТ» к компьютеру пользователя, выполните с него загрузку ОС, в административном режиме проведите инициализацию и тестовую проверку (см. раздел «Инициализация СПДС «ПОСТ»).

Шаг 5: Передайте пользователю подготовленный СПДС «ПОСТ», с которого он осуществляет загрузку и в режиме пользователя получает доступ к RDP, Web или другим серверам защищаемого сегмента корпоративной сети.

Сценарий последующих обновлений

Шаг 1: На Сервере управления сформируйте обновление для СПДС «ПОСТ». В заданное время автоматически будет создан пакет обновления, который сразу будет доступен для скачивания.

Шаг 2: Пользователь, перейдя в административный режим работы СПДС «ПОСТ», предоставляет Клиенту управления возможность проверки наличия доступных для него обновлений и загрузки их с Сервера управления. Можно задать подряд несколько обновлений с указанием времени создания каждого, и они будут применены в том порядке, в котором были созданы.

Установка и настройка Сервера управления

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 Gate (ср) 3.1/3.11/4.0, использующим СКЗИ «КриптоПро CSP 3.6», или для проверки обновлений планируется использовать ГОСТ-сертификаты, или 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 сообщение о необходимости установки продукта Microsoft Visual C++ Redistributable Package, нажмите кнопку Установить (Рисунок 3).

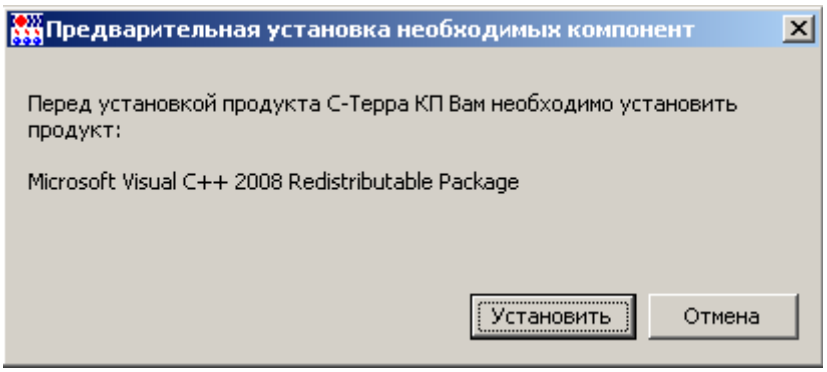


Рисунок 3

Выполняется сбор информации для Microsoft Visual C++ и подготовка к инсталляции (Рисунок 4).

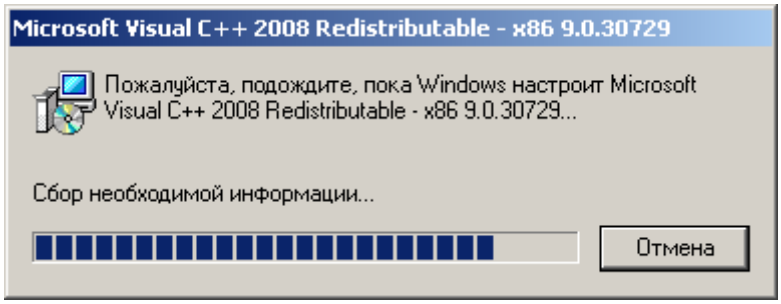


Рисунок 4

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).

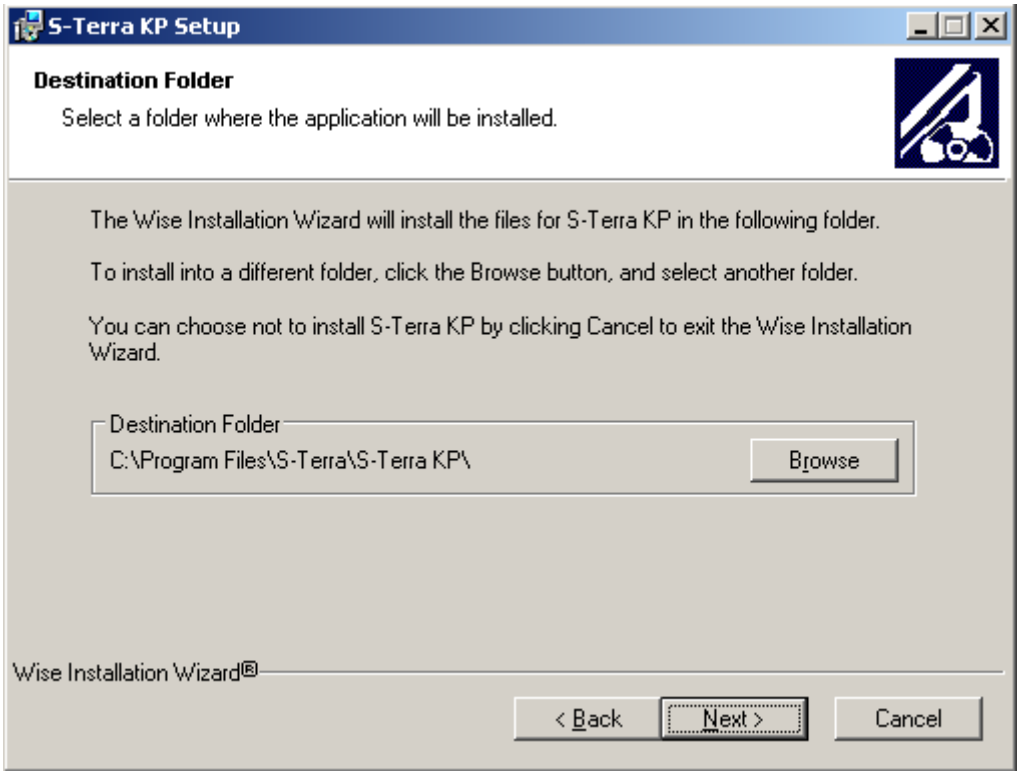


Рисунок 6

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

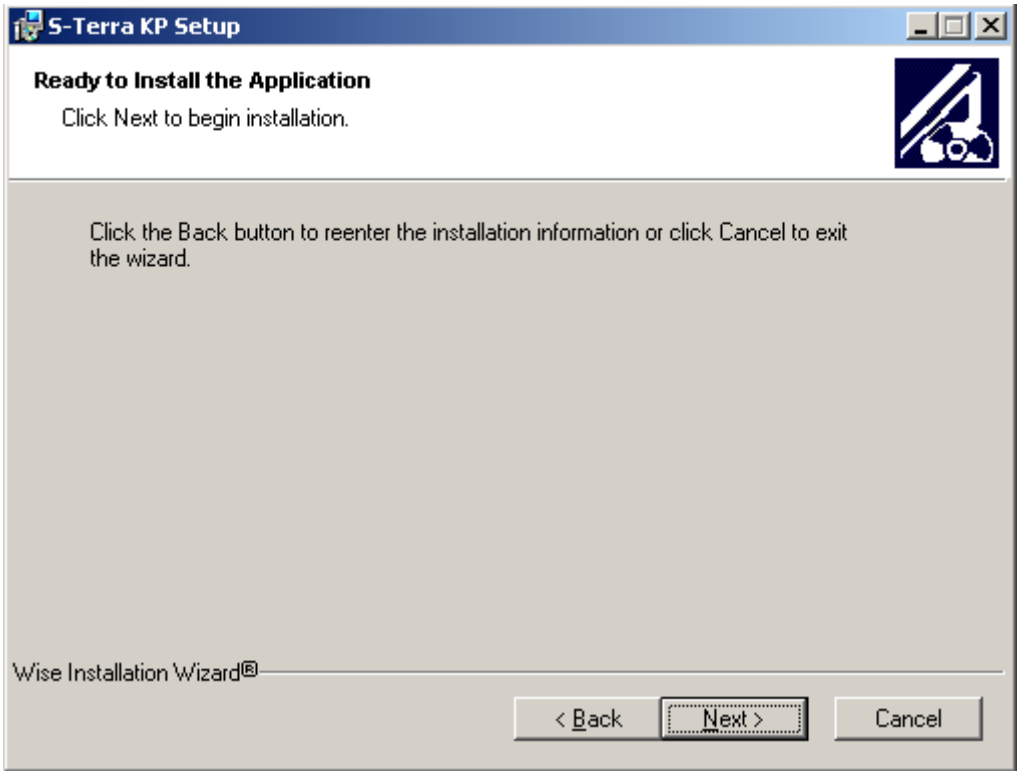


Рисунок 7

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

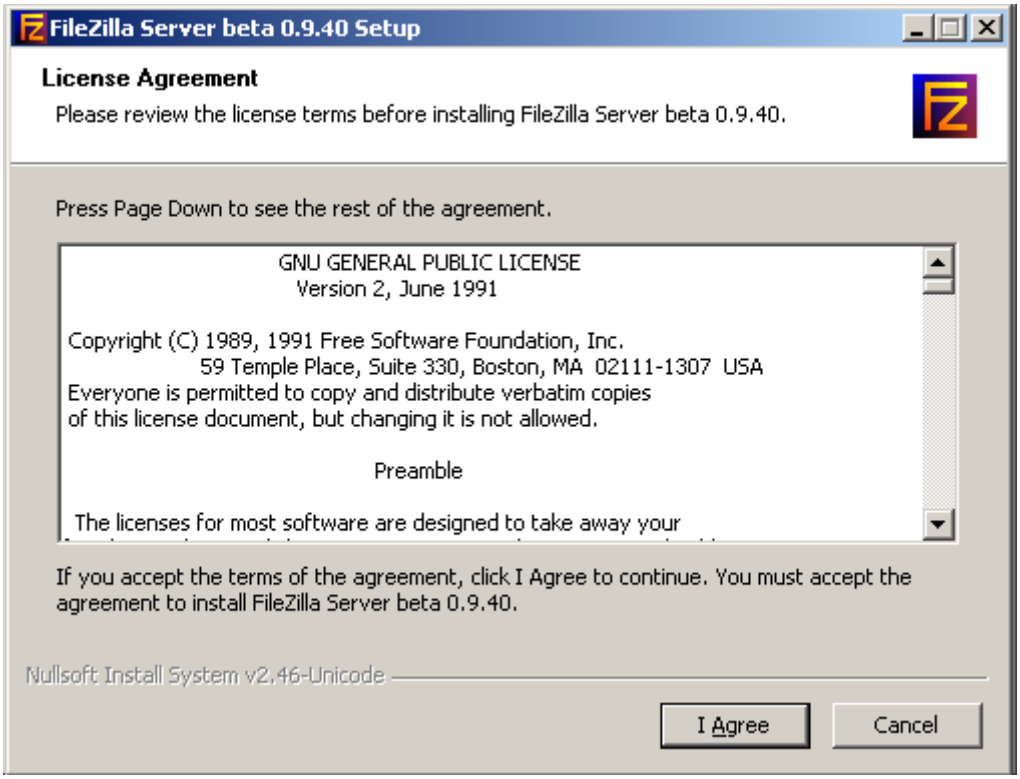


Рисунок 8

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

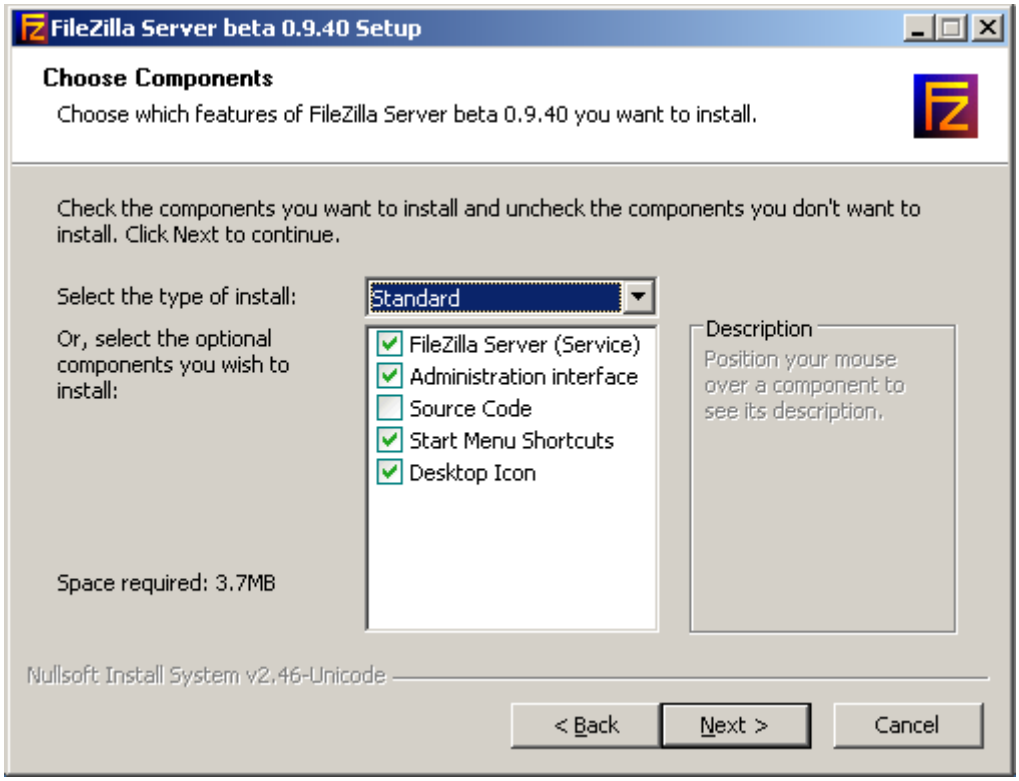


Рисунок 9

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

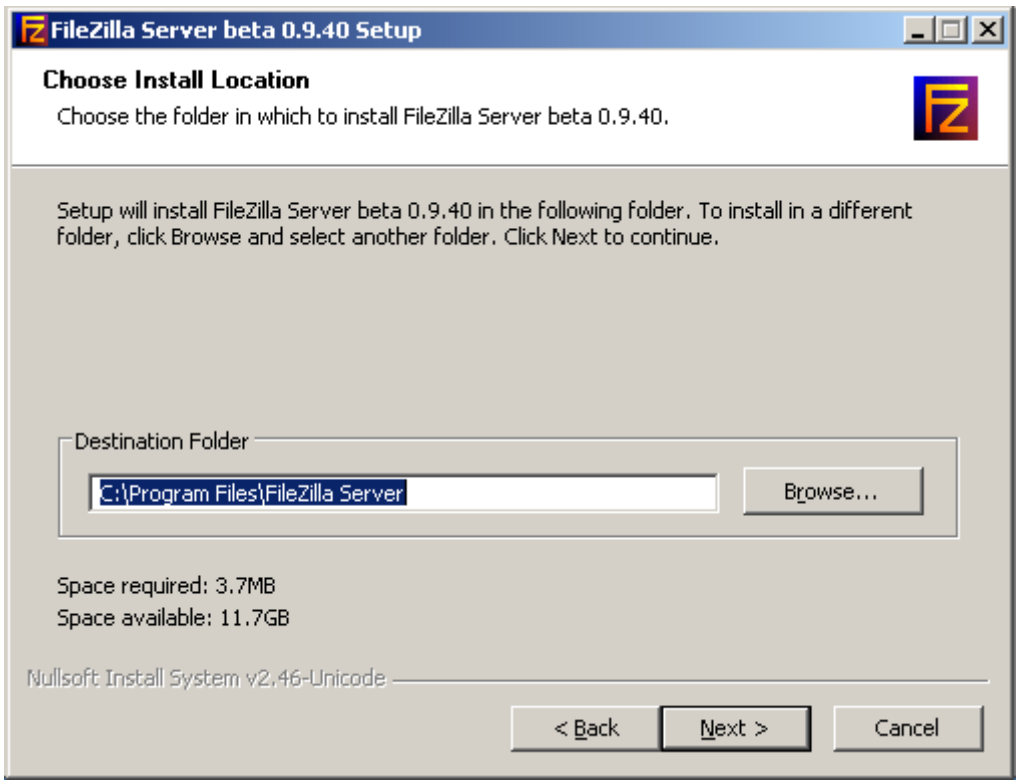


Рисунок 10

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

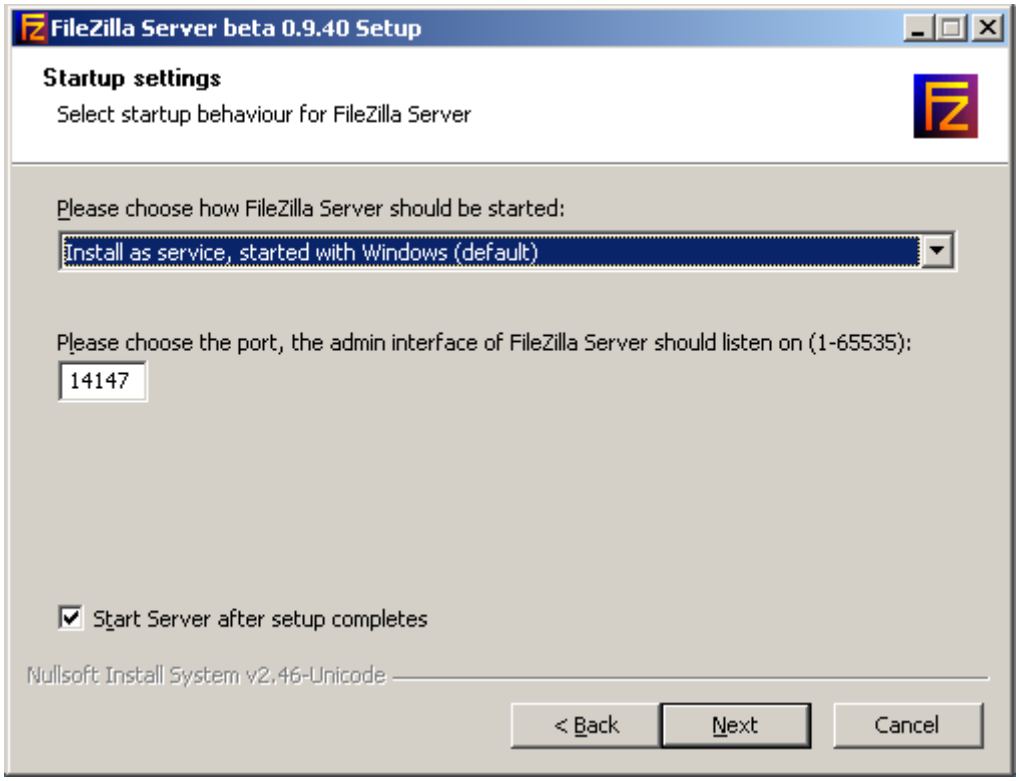


Рисунок 11

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.

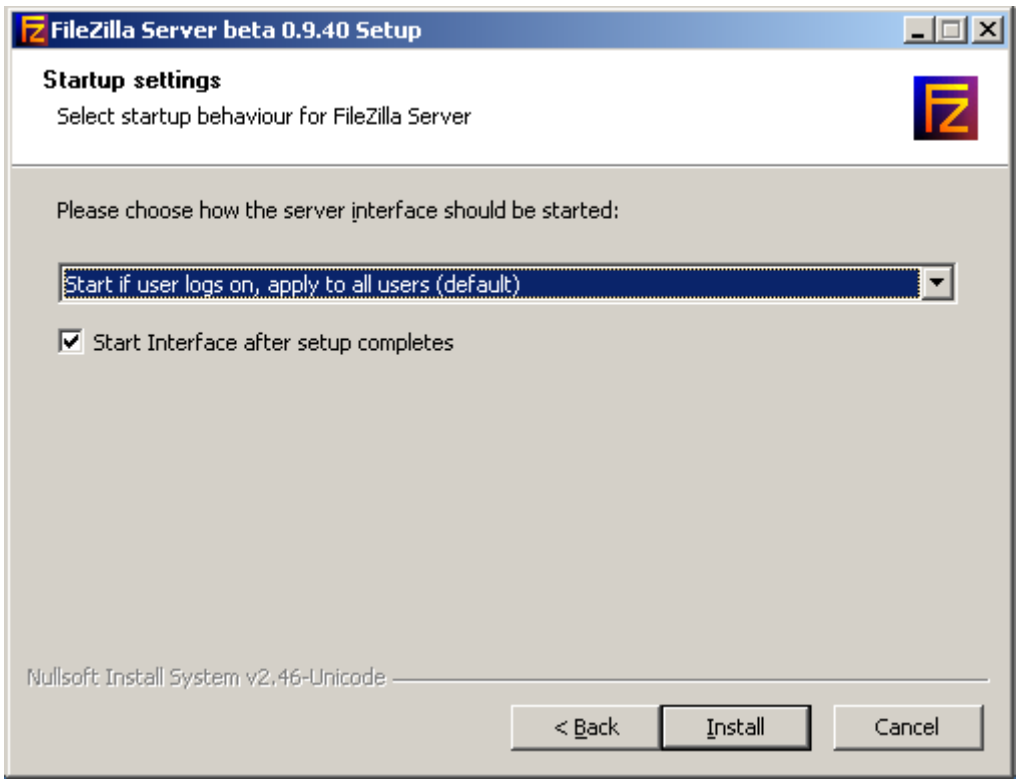


Рисунок 12

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

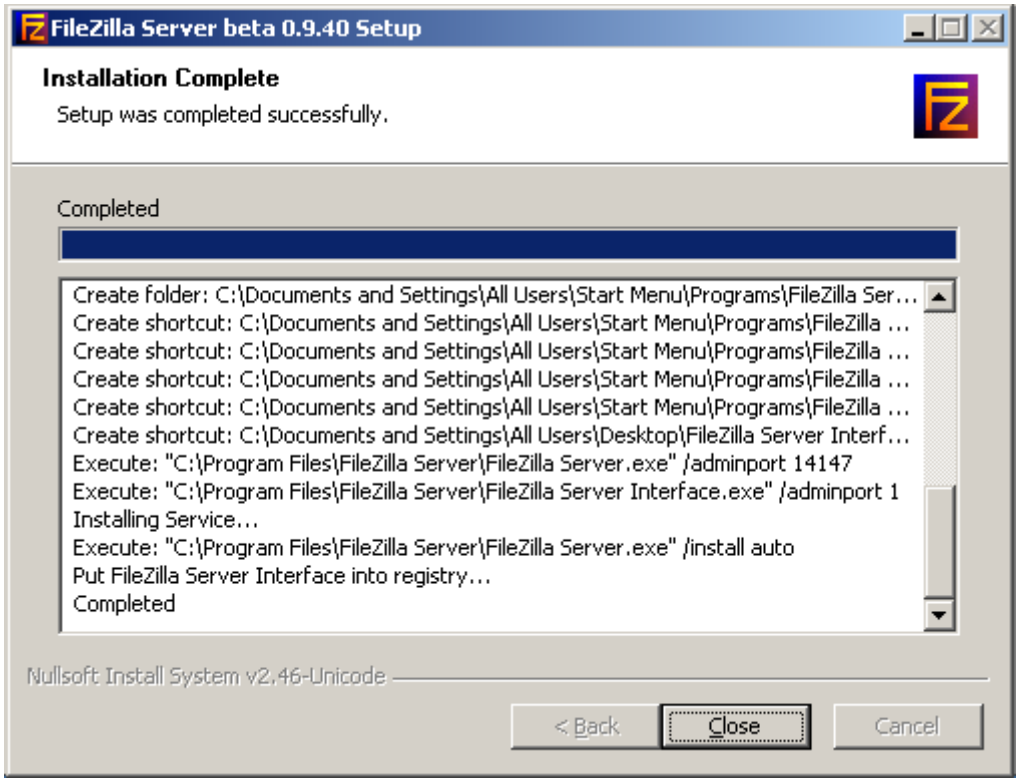


Рисунок 13

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

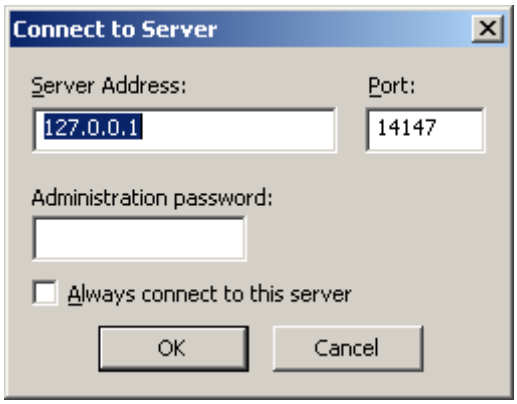


Рисунок 14

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

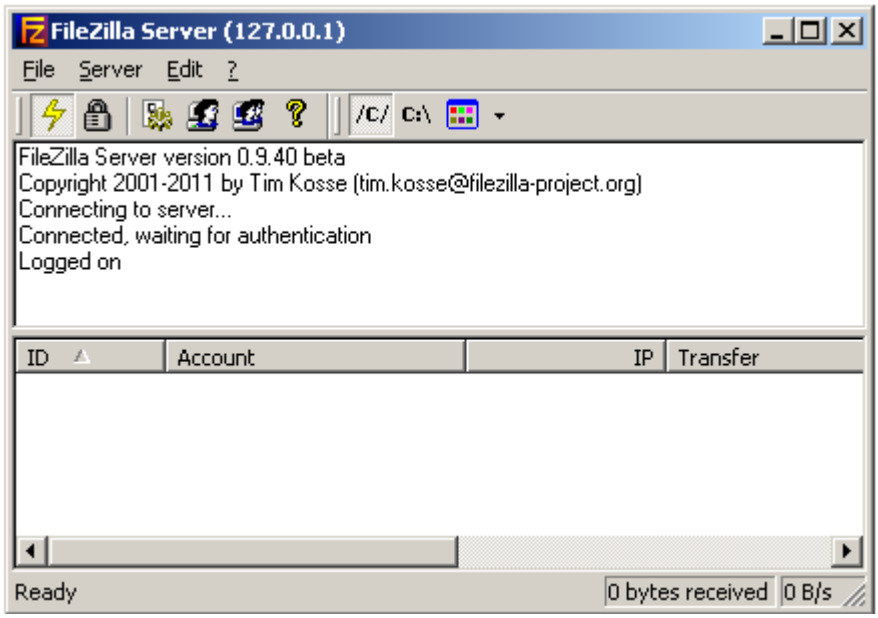


Рисунок 15

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. По окончании закончите установку продукта Сервер управления, нажав кнопку Finish (Рисунок 16).

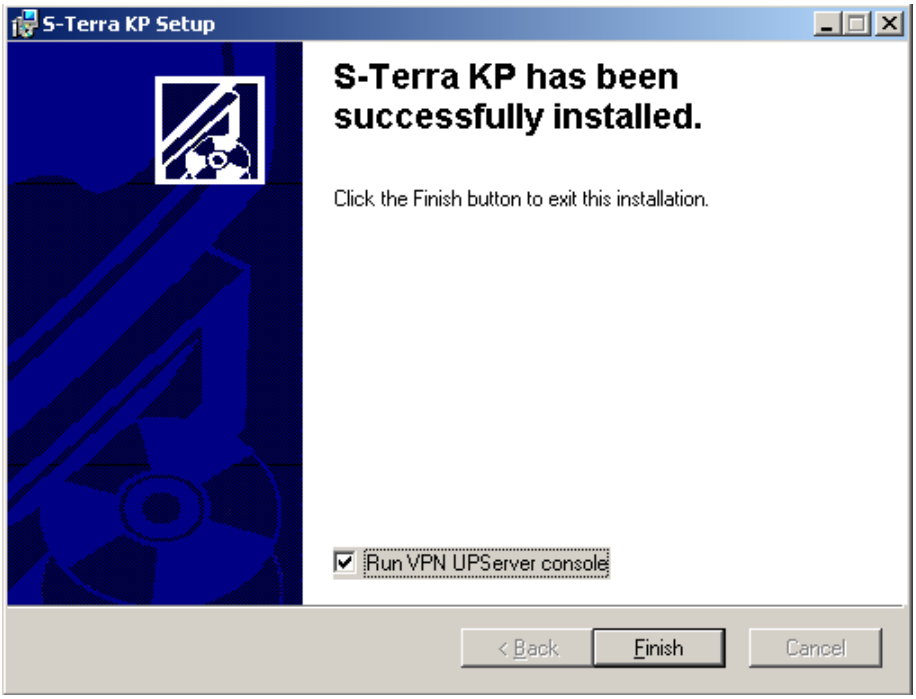


Рисунок 16

Настройка Сервера управления

Настройка и управление Сервером управления производится при помощи специального приложения **UPServer Console** (`Пуск-Программы-S-Terra-S-Terra KP-VPN UPServer Console`) (Рисунок 17).

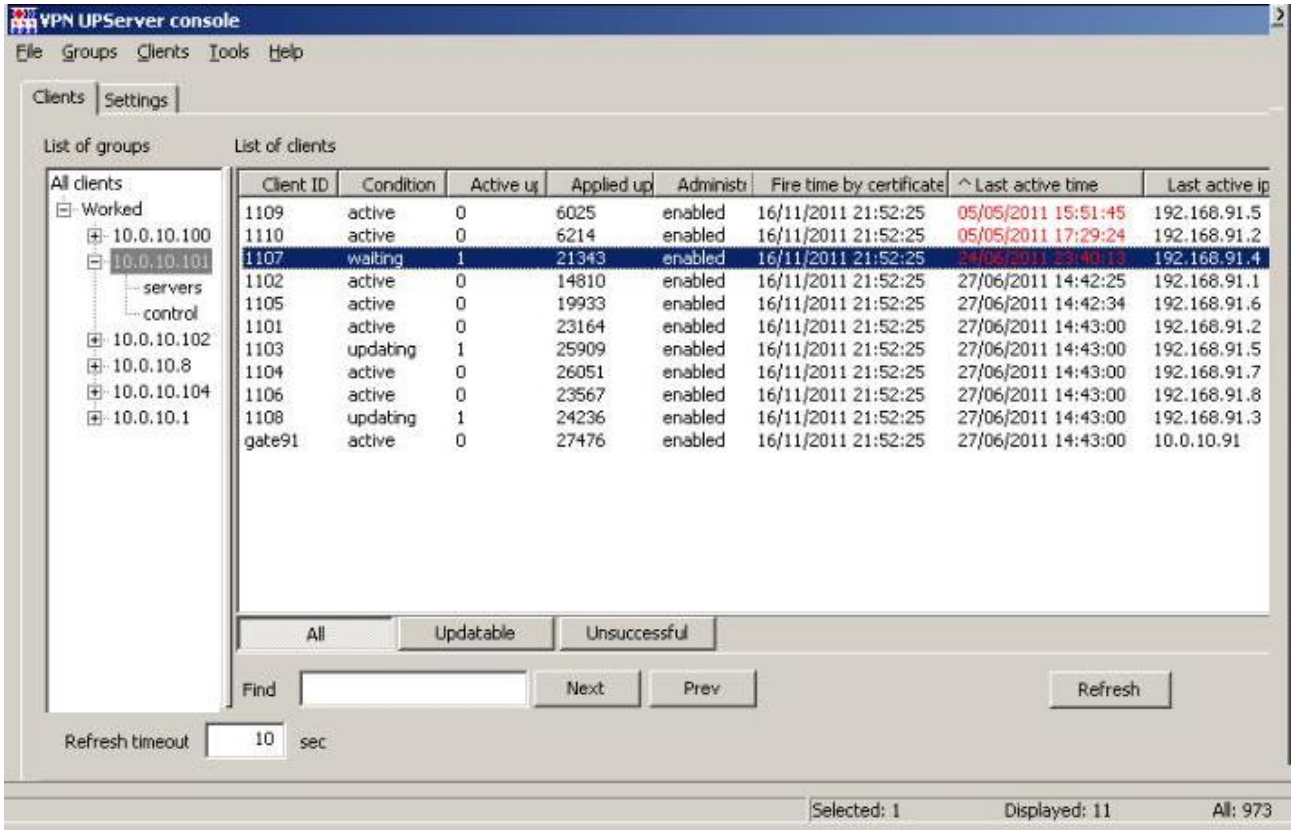


Рисунок 17

Создание и удаление учетных записей клиентов управляемых устройств, создание для них Клиентов управления, обновлений выполняются во вкладке **Clients** Сервера управления, интерфейс которой описан в главе «Описание интерфейса Сервера управления». Во вкладке **Clients** отражается информация обо всех управляемых устройствах.

Начальная настройка Сервера управления производится во вкладке **Settings.**

При первом запуске приложения **VPN UPServer Console** выводится предупреждение о необходимости задать настройки продукта ***Сервер управления*** (Рисунок 18).

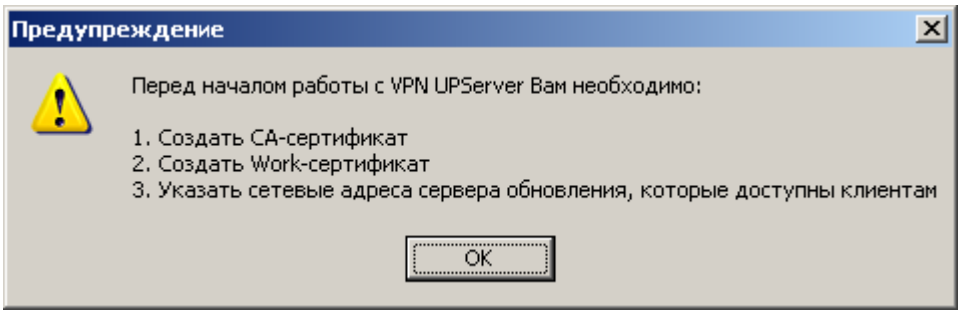


Рисунок 18

Нажмите кнопку OK, откроется окно настроек продукта Сервер управления (Рисунок 19). Во вкладке **Settings** введите данные лицензии, создайте CA-сертификат и рабочий сертификат (work certificate) Сервера управления, а также задайте сетевые адреса Сервера управления.

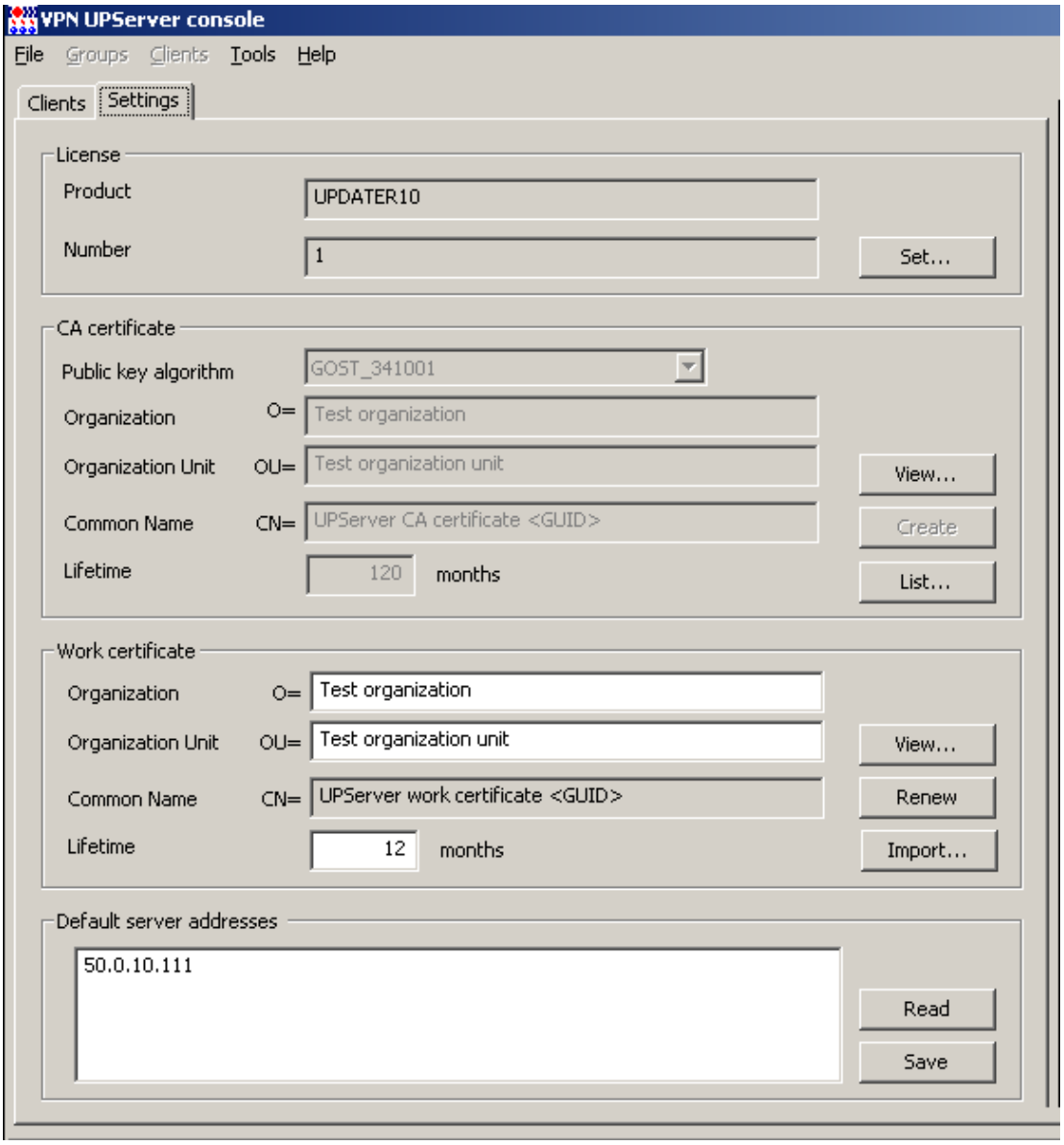


Рисунок 19

Ввод лицензии

Для ввода лицензии на продукт Сервер управления нажмите кнопку Set…(Рисунок 19).

В появившемся окне **Set license** (Рисунок 20):

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 обновления и не больше.

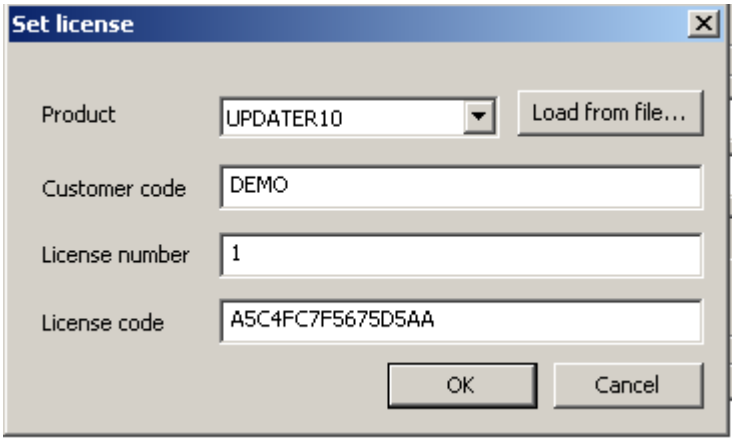


Рисунок 20

Создание CA сертификата

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. Опишем эту процедуру.

1. В группе **CA certificate** (Рисунок 19) нажмите кнопку Create и заполните поля в окне **Create new CA certificate**, например, следующими значениями (Рисунок 21):

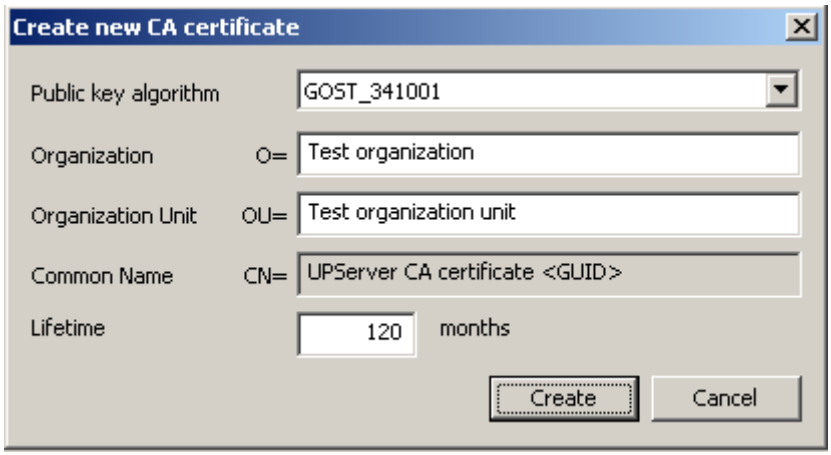


Рисунок 21

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 22), нажмите OK.

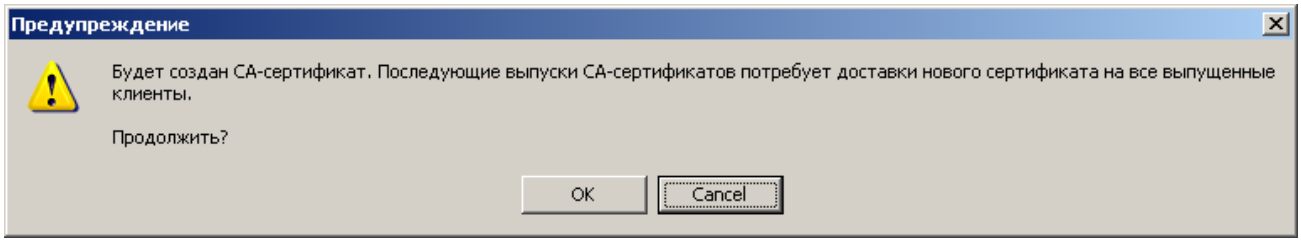


Рисунок 22

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

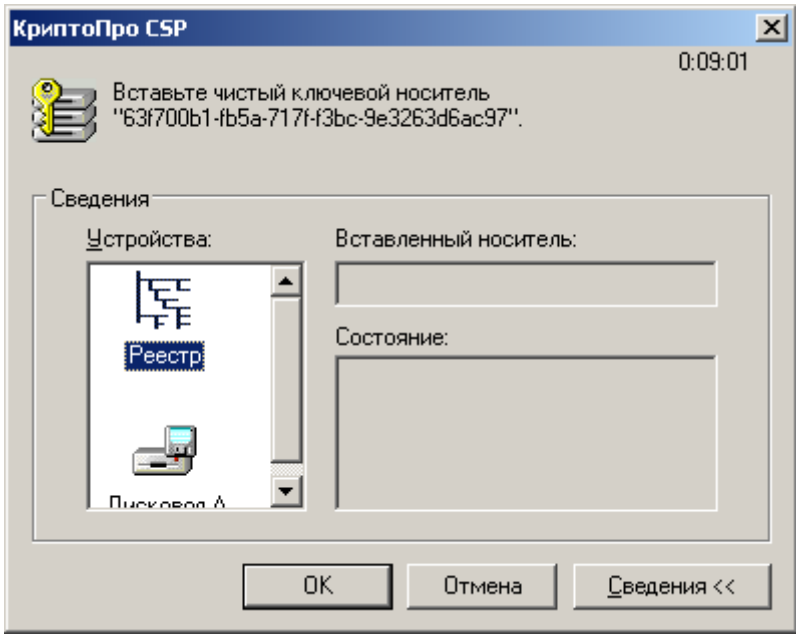


Рисунок 23

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.

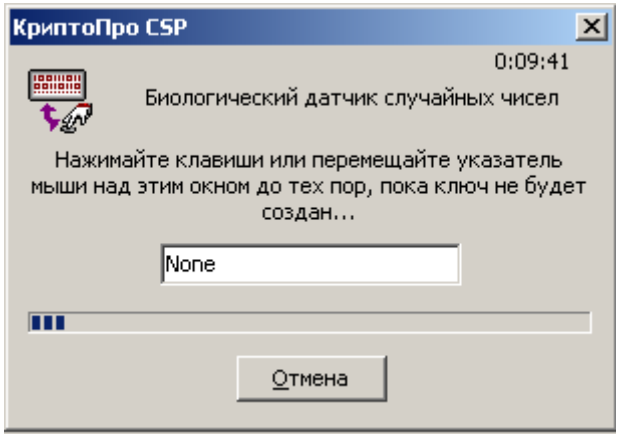


Рисунок 24

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

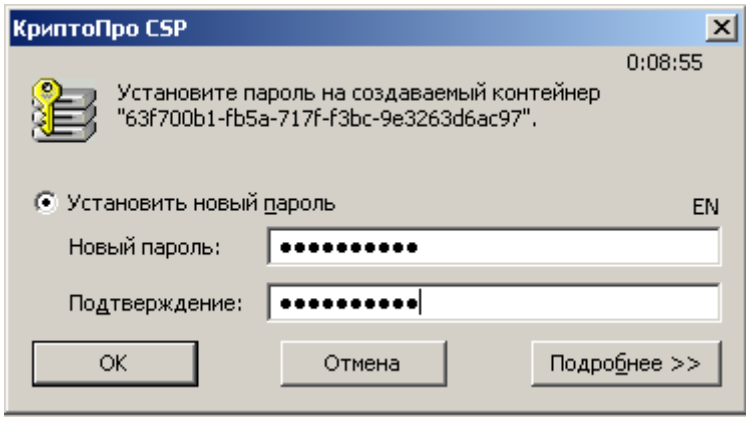


Рисунок 25

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

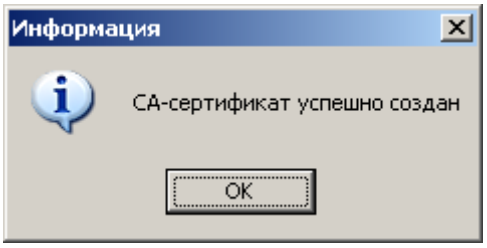


Рисунок 26

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 27), 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 (*).

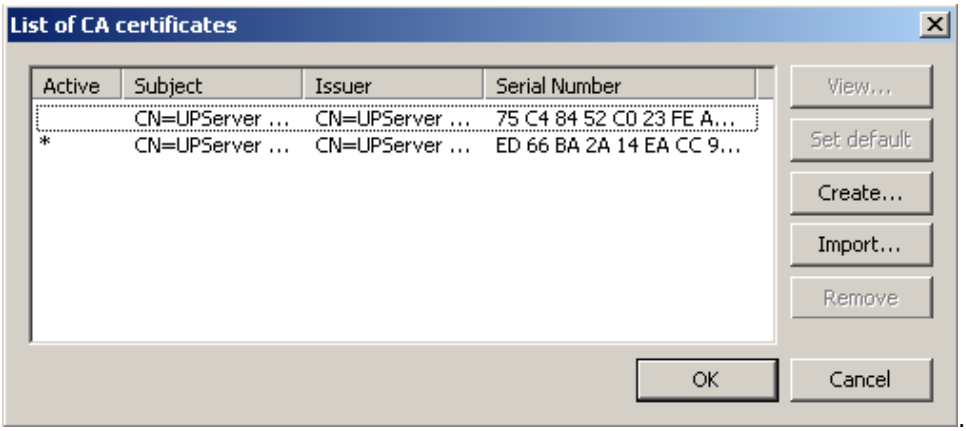


Рисунок 27

Создание рабочего сертификата

1. В группе **Work certificate** (Рисунок 19) заполните поля рабочего (локального) сертификата Сервера управления и нажмите кнопку Create. Перед созданием будет выдано **Предупреждение** (Рисунок 28):

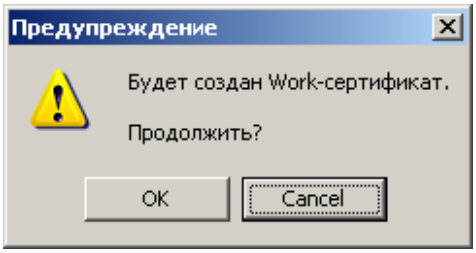


Рисунок 28

2. Если поля заполнены верно – нажмите кнопку OK. Возможен запрос ключевого носителя для размещения контейнера с секретным ключом рабочего сертификата (Рисунок 29). Выберите Реестр.

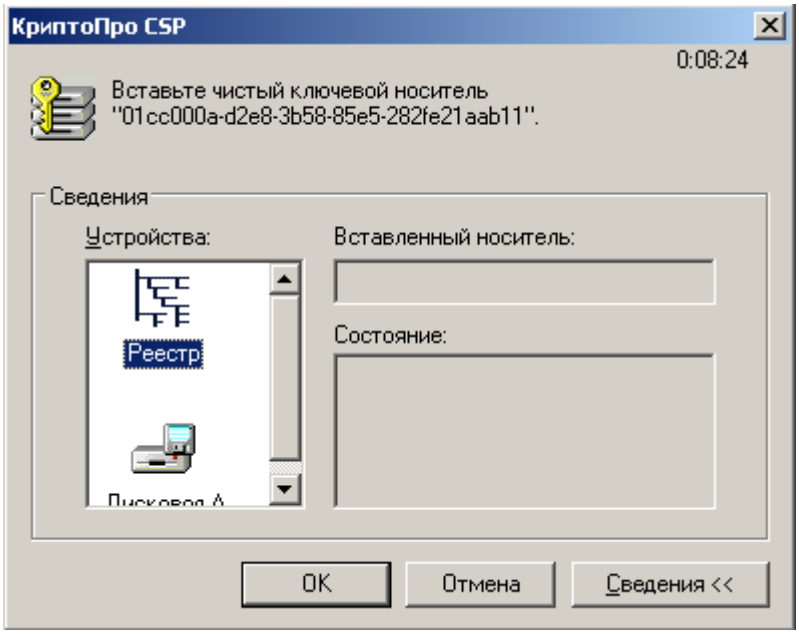


Рисунок 29

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.

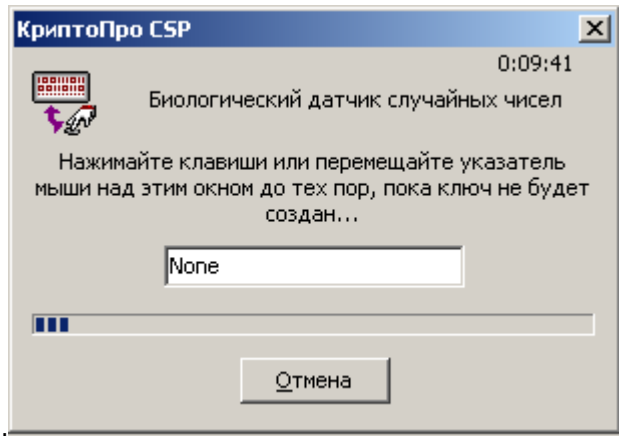


Рисунок 30

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

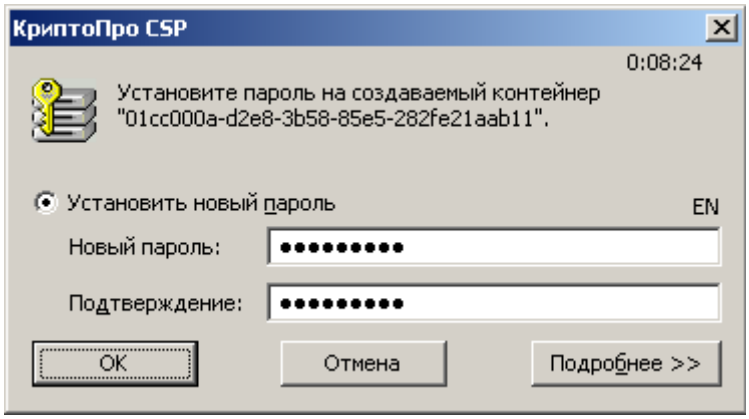


Рисунок 31

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

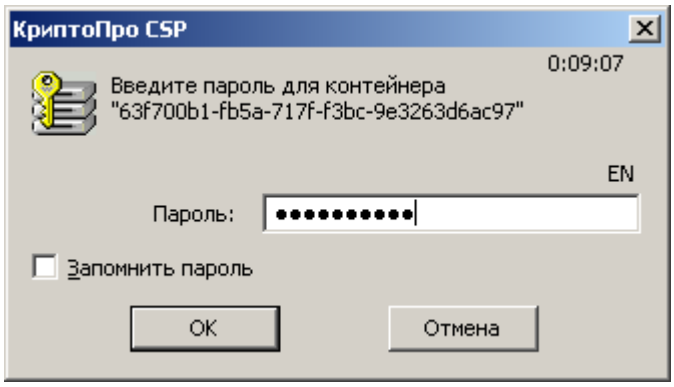


Рисунок 32

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 33).

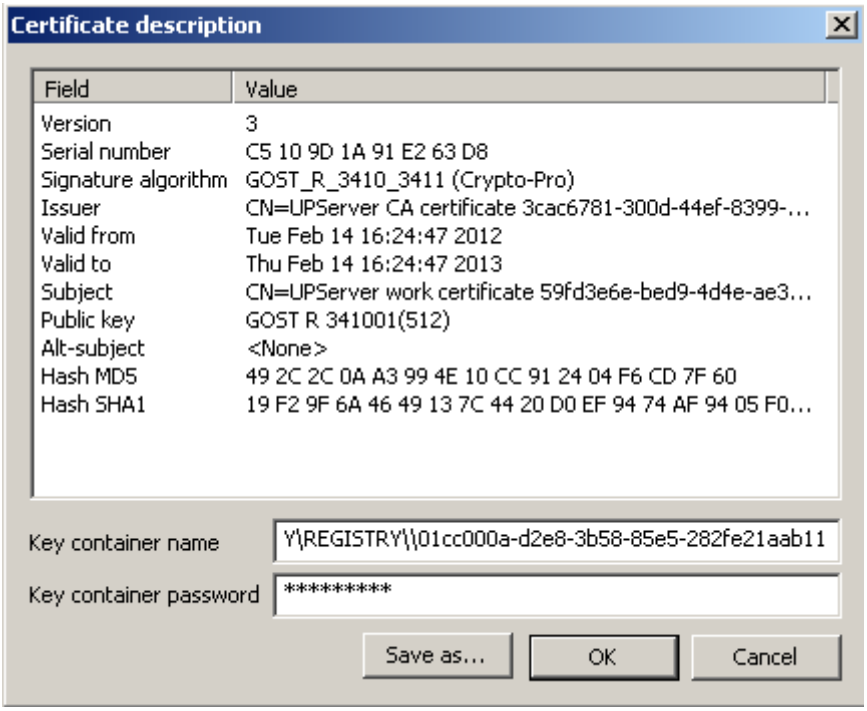


Рисунок 33

7. После успешного создания сертификата будет выдано подтверждение, нажмите кнопку OK (Рисунок 34).

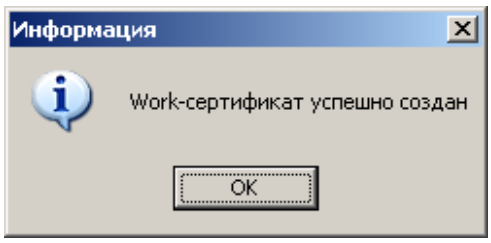


Рисунок 34

После этого кнопка Create в группе **Work certificate** изменится на Renew (Рисунок 19).

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

Задание адресов Сервера управления

1. В группе **Default server addresses** (Рисунок 19) 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 35).
3. Если адреса введены верно, то нажмите кнопку OK, при этом происходит проверка введенных данных и только после этого во все создаваемые скрипты для Клиентов управления по умолчанию будет вноситься список адресов Сервера управления.

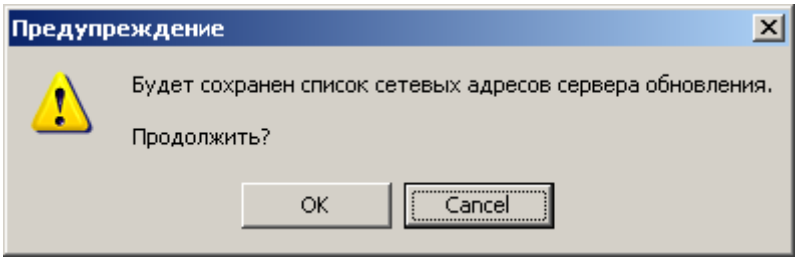


Рисунок 35

Note

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 центрального шлюза CSP VPN Gate.

Настройка и управление центральным шлюзом

Перед тем как настроить центральный шлюз, нужно создать локальный сертификат для центрального шлюза. А перед созданием ключевой пары для локального сертификата в режиме КС1/КС2/КС3 СКЗИ «КриптоПро CSP 3.6» изучите документ «Правила пользования», входящий в комплект поставки.

Далее описано как получить ключевую пару и локальный сертификат для центрального шлюза и СПДС «ПОСТ».

Создание локального сертификата

1. На Сервере управления в СКЗИ «КриптоПро CSP 3.6» инсталлируйте считыватель «Все считыватели смарт-карт» (Рисунок 36).

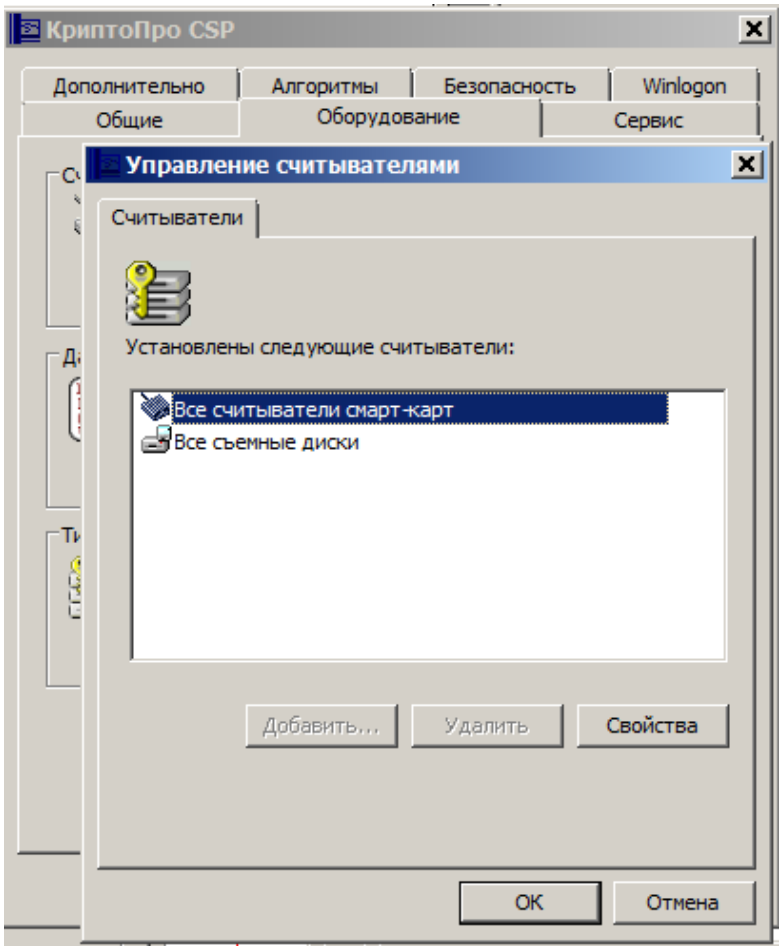


Рисунок 36

2. Для создания ключевой пары и запроса на сертификат можно использовать средства, например, Microsoft Windows CA. На Сервере управления запустите `Microsoft Internet Explorer`, в поле `Address` укажите адрес Удостоверяющего Центра (УЦ) и утилиту `certsrv (Certificate Service), например, http://10.10.10.10/certsrv`.

   На Сервере управления можно настроить свой Удостоверяющий Центр для целей тестирования (см. документ «Программный комплекс CSP VPN Gate. Приложение», раздел «Настройка Удостоверяющего Центра»). Далее будем вести описание для УЦ на Сервере управления.

3. В появившемся окне высвечивается имя УЦ. Выберите предложение `Request a certificate` (Рисунок 37).

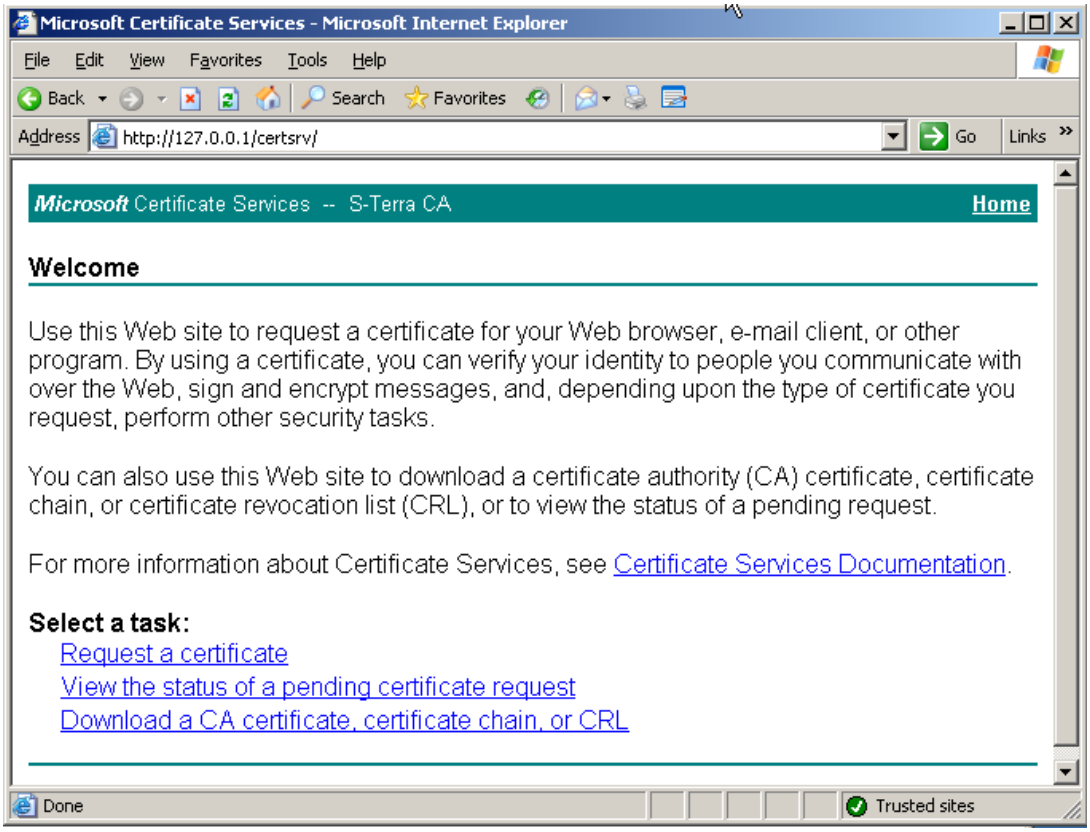


Рисунок 37

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

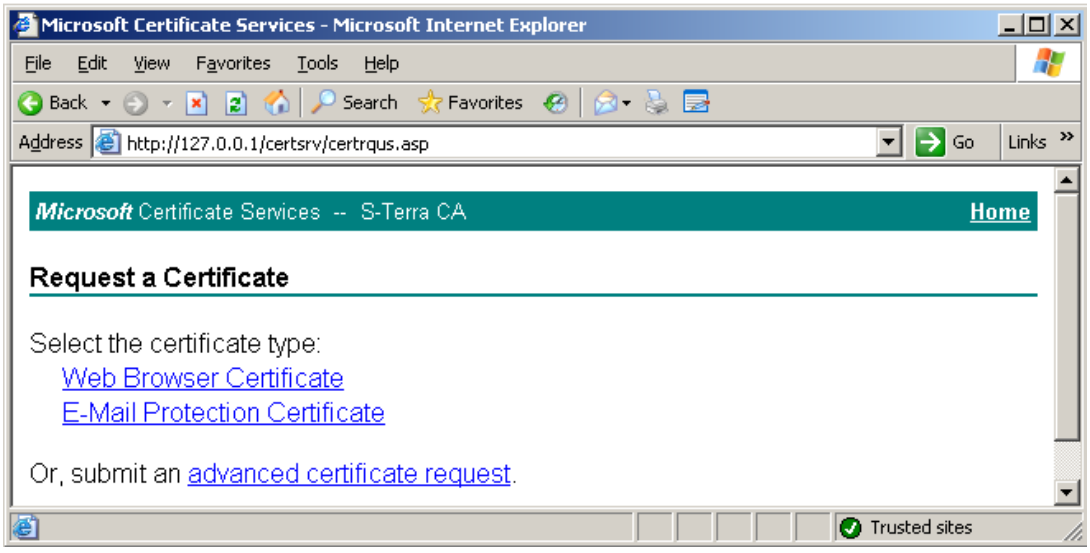


Рисунок 38

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

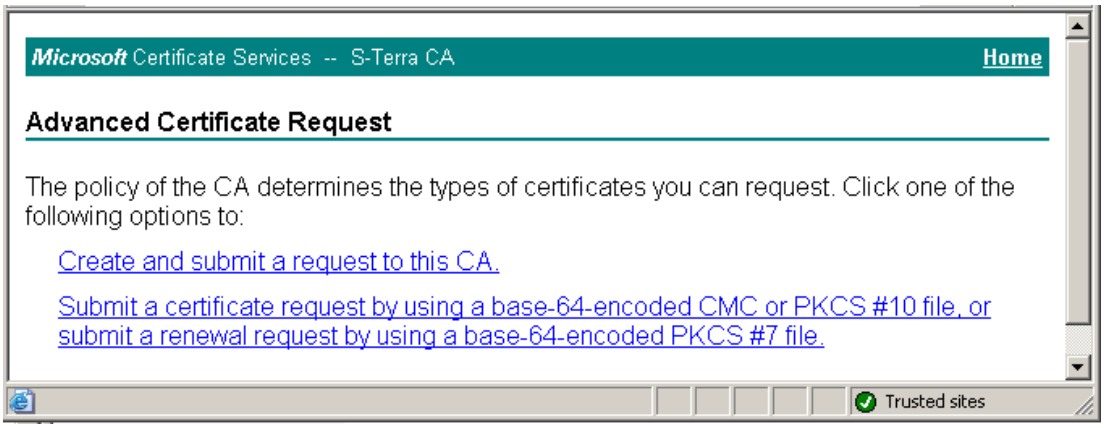


Рисунок 39

Заполните форму расширенного запроса (Рисунок 40). 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***
  - Далее можно поставить переключатель в положение:
    - Automatic key container name - имя контейнера с секретным ключом будет задаваться автоматически
    - ***User specified key container name*** – в этом случае имя контейнера надо задать в поле ***Container Name***
  - ***Mark keys as exportable*** – поставьте флажок, чтобы можно было скопировать контейнер с секретным ключом
  - ***Store certificate in the local computer certificate store*** – поставьте этот флажок
- в разделе **Additional Options** (Дополнительные опции):
  - request Format - ***CMC***
  - Hash Algorithm – выбрать ***GOST R 34.11-94***

По этому образцу заполните форму запроса и нажмите кнопку Submit.

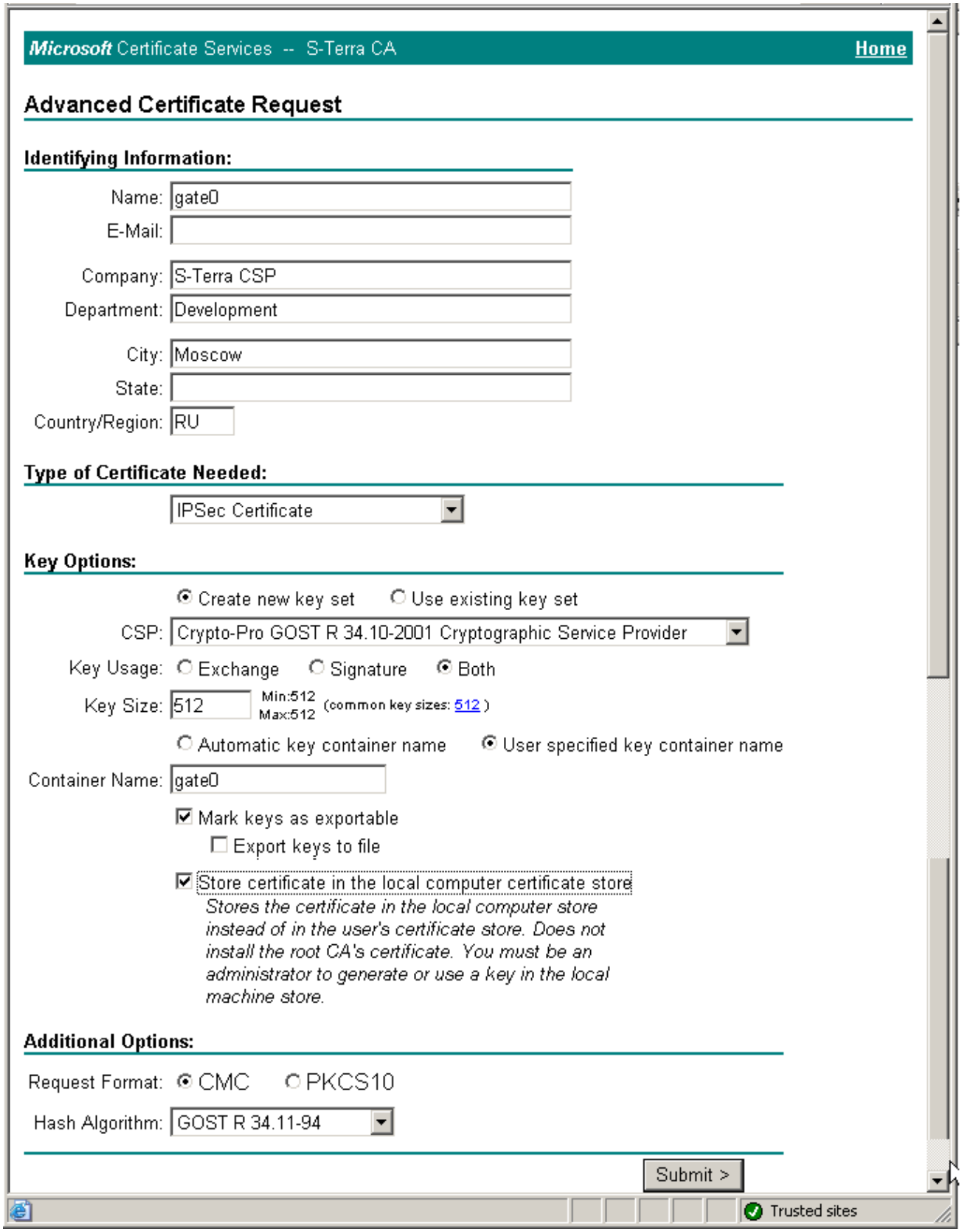

Microsoft Certificate Services -- S-Terra CA
Home
Advanced Certificate Request
Identifying Information:
Name: gate0
E-Mail:
Company: S-Terra CSP
Department: Development
City: Moscow
State:
Country/Region: RU
Type of Certificate Needed:
IPSec Certificate
Key Options:
Create new key set
Use existing key set
CSP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
Key Usage: Exchange Signature Both
Key Size: 512 Min:512 Max:512 (common key sizes: 512)
Automatic key container name
User specified key container name
Container Name: gate0
Mark keys as exportable
Export keys to file
Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.
Additional Options:
Request Format: CMC PKCS10
Hash Algorithm: GOST R 34.11-94
Submit >
Trusted sites

Рисунок 40

6. На следующем предупреждении нажмите кнопку Yes.

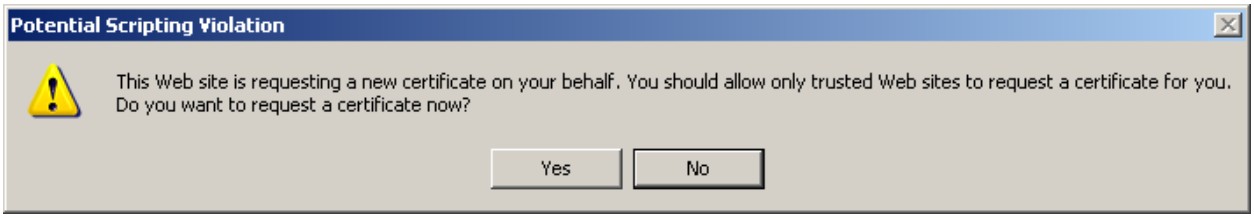


Рисунок 41

7. Вставьте USB-флеш и укажите ключевой носитель (Рисунок 42).

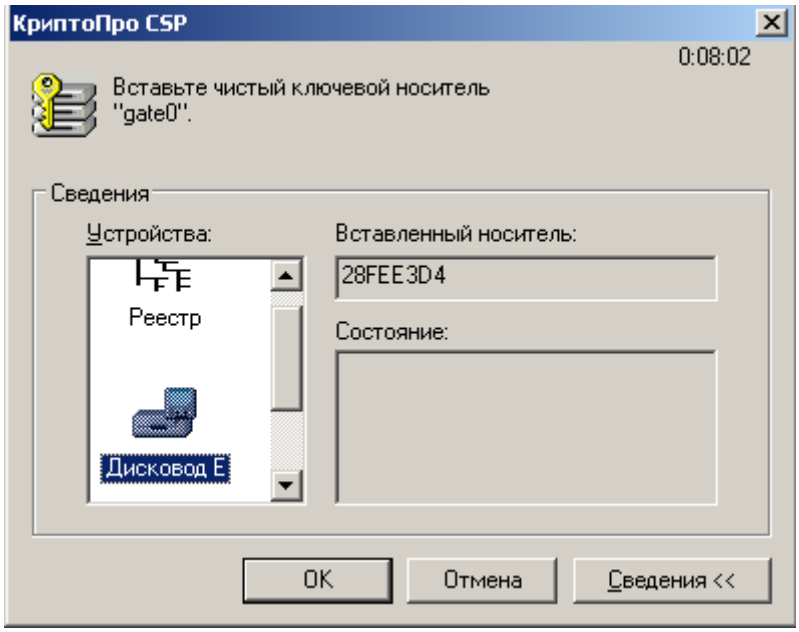


Рисунок 42

8. 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.

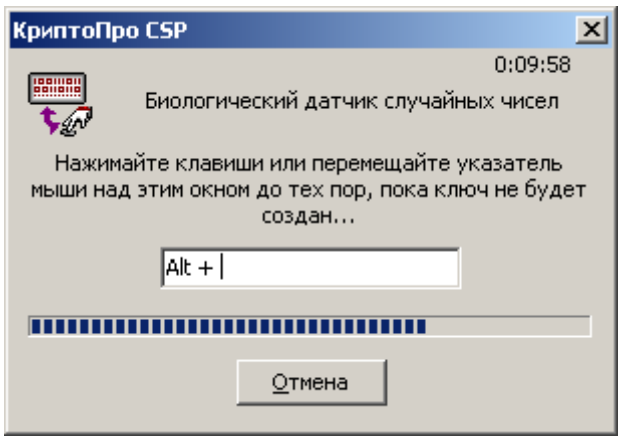


Рисунок 43

9. В окне запроса пароля на контейнер поля оставьте пустыми, чтобы его можно было открыть при создании сертификата (Рисунок 44).

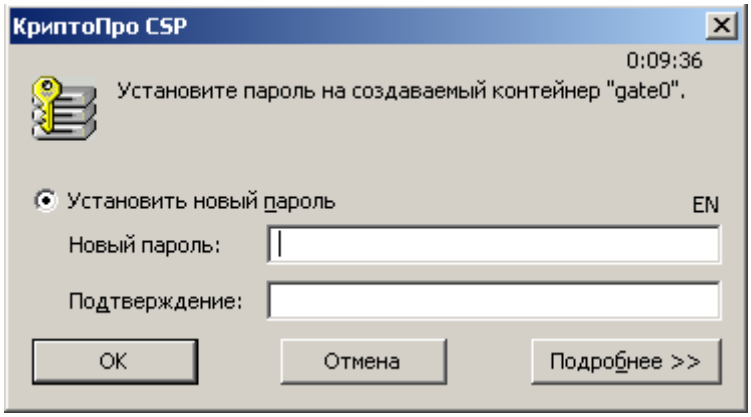


Рисунок 44

10. Если Удостоверяющий Центр настроен на автоматический выпуск сертификатов при получении запроса, то появляется окно с предложением получить (инсталлировать) сертификат (Рисунок 45). В этом случае выберите предложение Install this certificate.

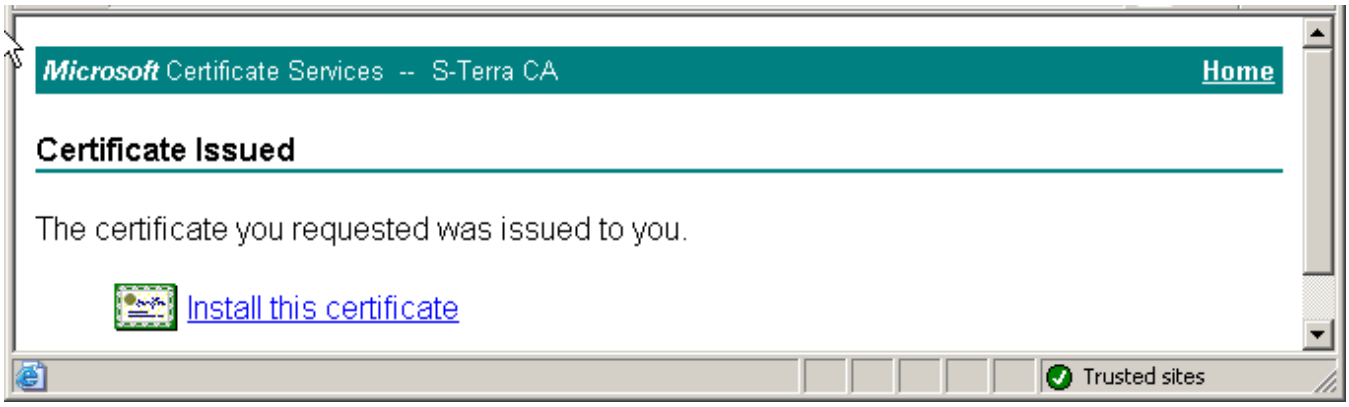


Рисунок 45

11. В результате сертификат будет записан в тот же контейнер на USB-флеш, что и ключевая пара, например, gate0.

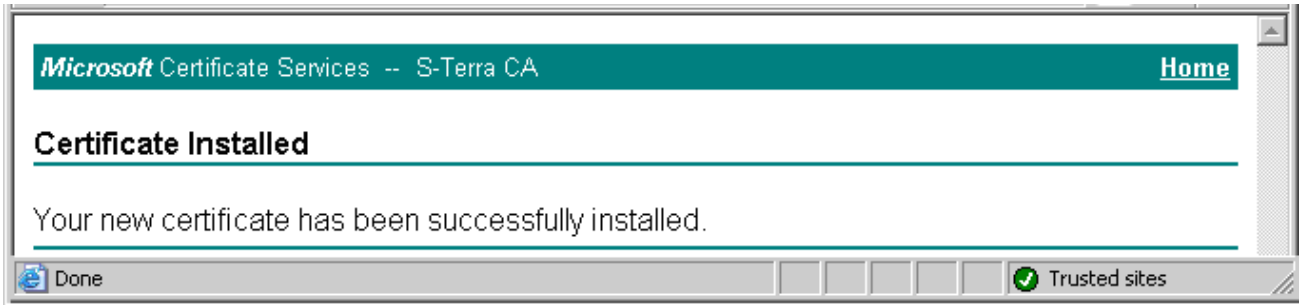


Рисунок 46

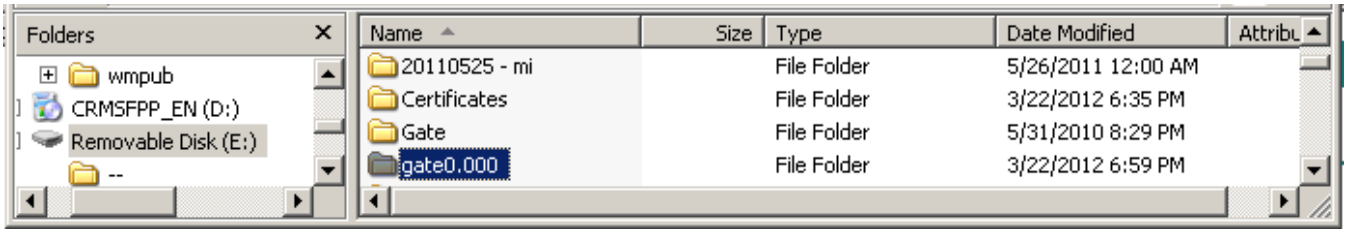


Рисунок 47

12. Экспортируйте локальный сертификат из контейнера в файл, так как он будет необходим на Сервере управления при настройке центрального шлюза. Для этого в «КриптоПро CSP» во вкладке Сервис нажмите кнопку Просмотреть сертификаты в контейнере.

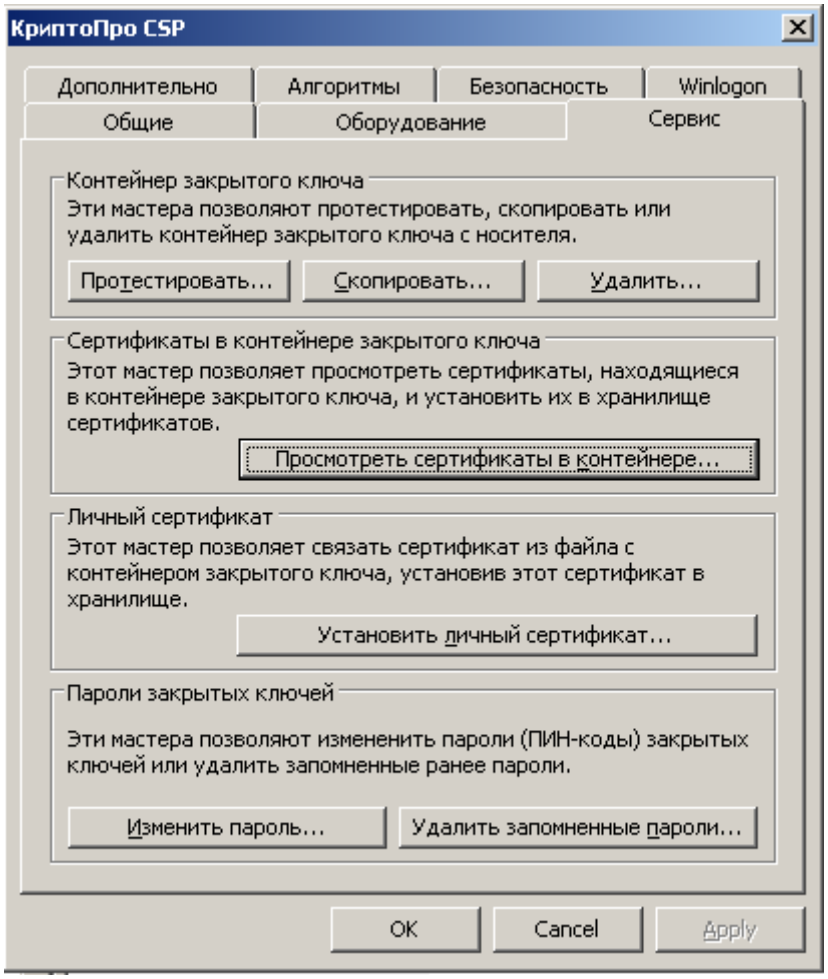


Рисунок 48

13. Далее нажмите кнопку По сертификату (Рисунок 49).

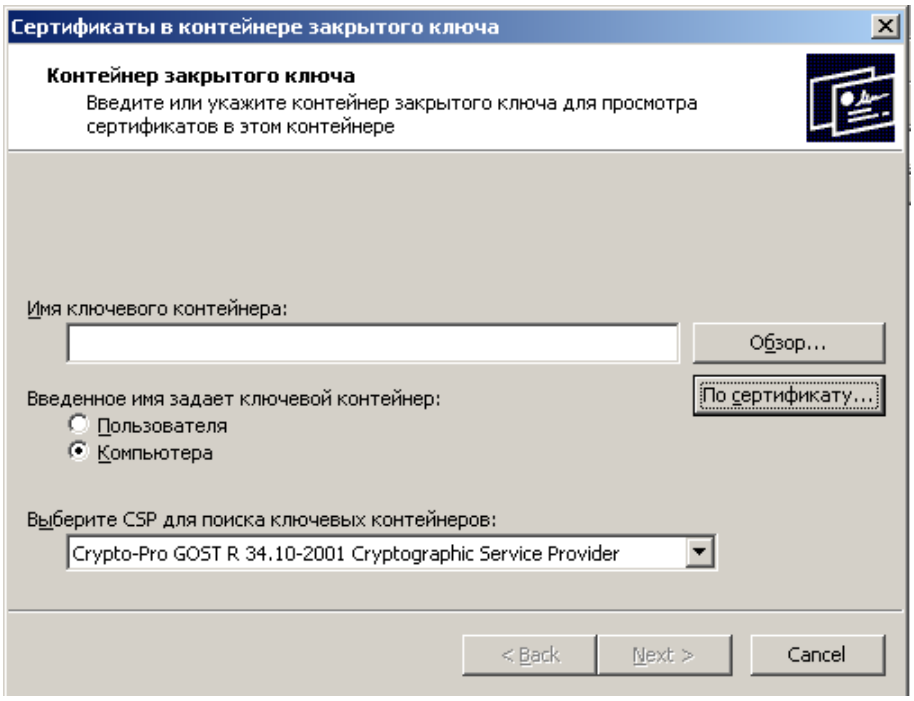


Рисунок 49

14. Выберите сертификат gate0 и нажмите кнопку View Certificate.

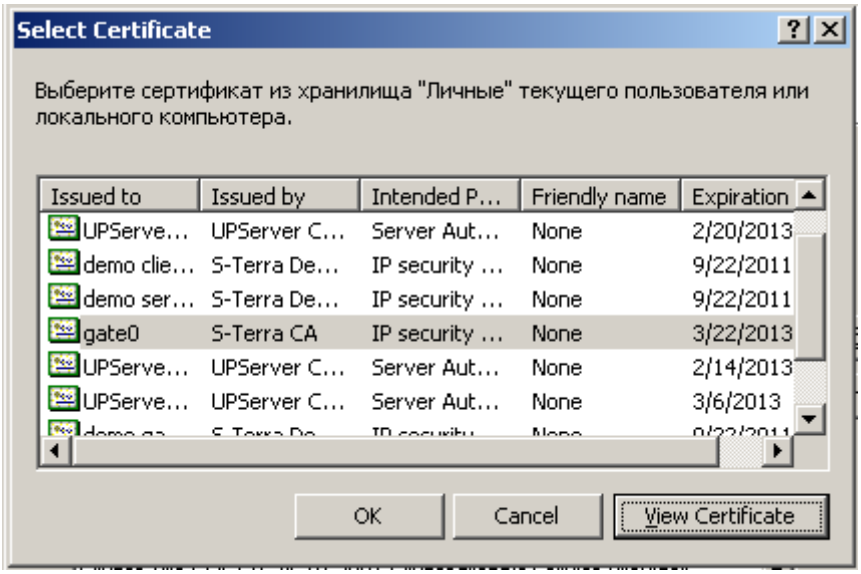


Рисунок 50

15. В следующем окне нажмите кнопку Copy to File….

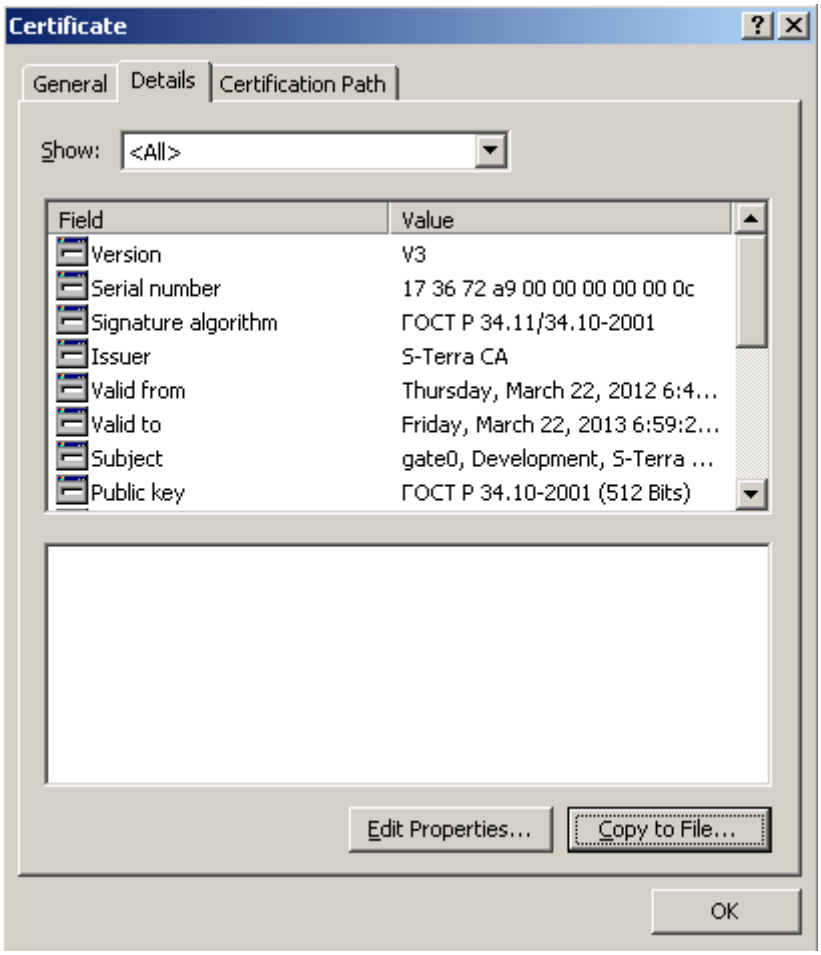


Рисунок 51

16. Экспортируйте только один сертификат, ключи не нужны.

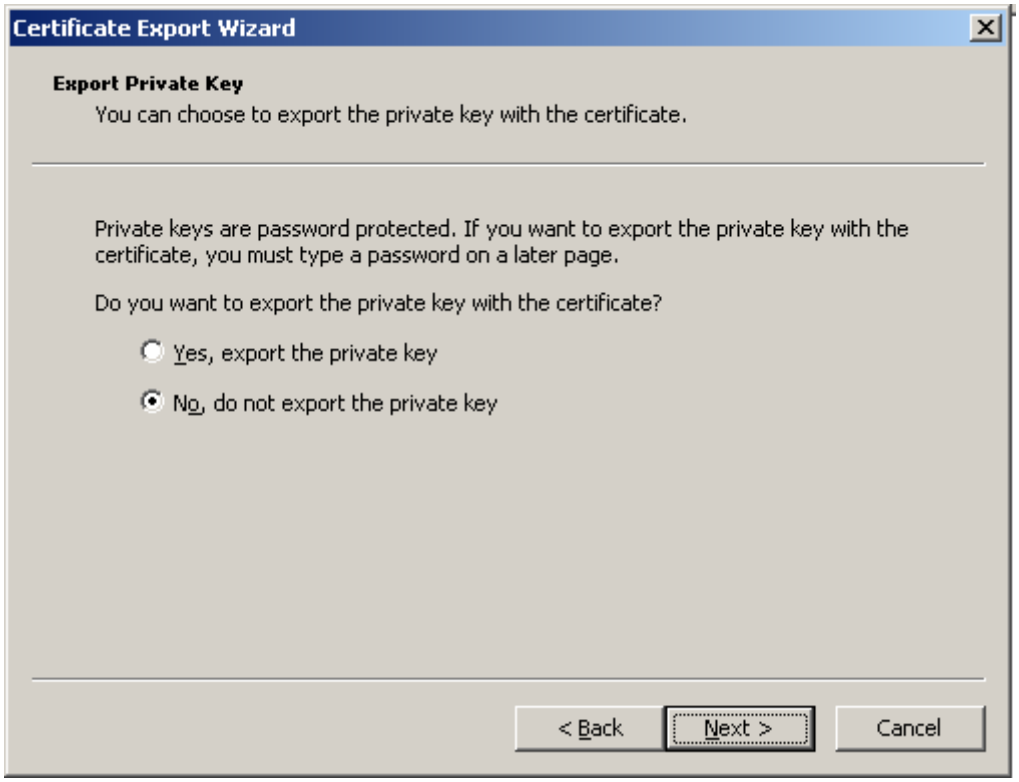


Рисунок 52

17. Укажите имя файла для локального сертификата на USB-флеш, например, в каталоге `C:\Certificates`.

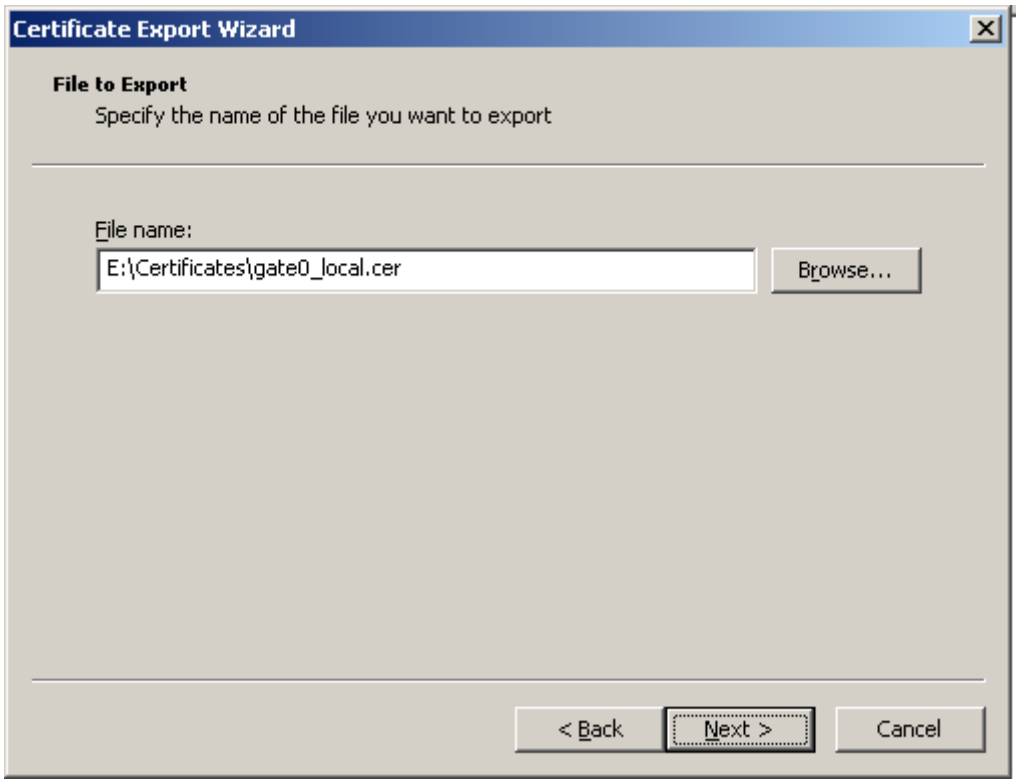


Рисунок 53

18. Также экспортируйте в файл CA сертификат УЦ (см. документ Приложение).

Таким образом, на USB-флеш записан контейнер с ключевой парой и в каталоге Certificates локальный и CA сертификаты для центрального шлюза (Рисунок 54).

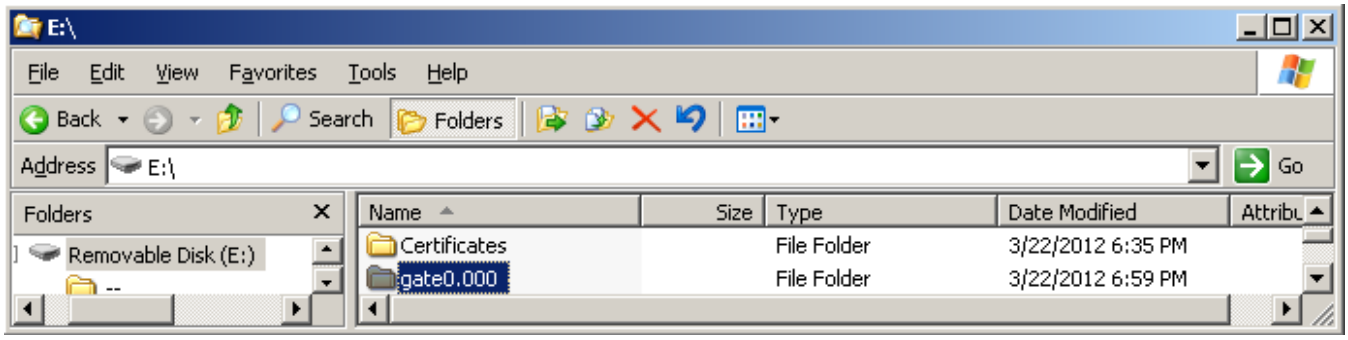


Рисунок 54

Создание учетной записи клиента для центрального шлюза

1. Запустите приложение **UPServer Console (**`Пуск-Программы-S-Terra-S-Terra КР-VPN UPServer Console`).
2. Во вкладке **Clients** в меню ***Group*** выберите предложение ***Create*** (Рисунок 57).

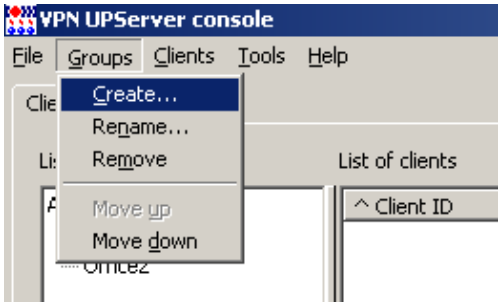


Рисунок 55

3. Внесите имя группы.

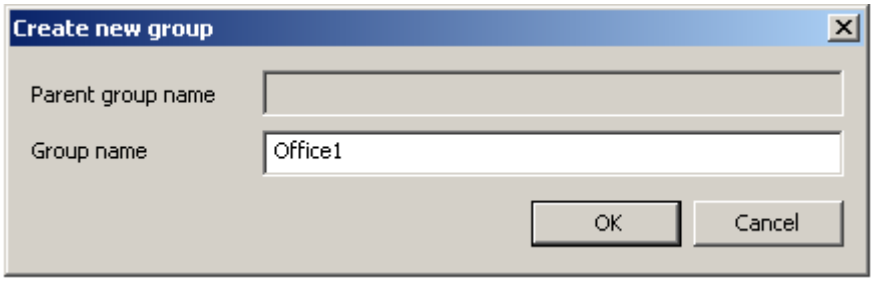


Рисунок 56

4. В контекстном меню выберите предложение ***Create***.

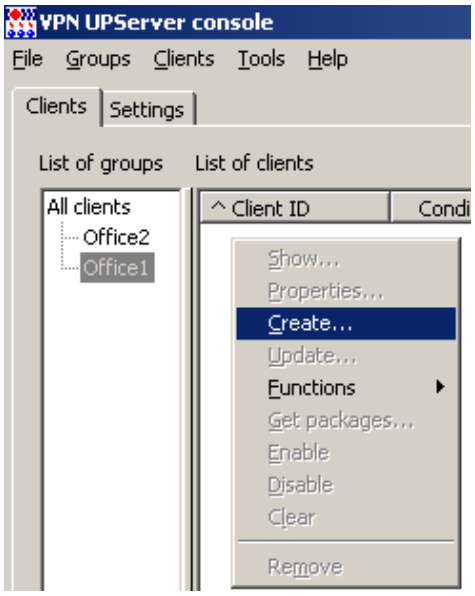


Рисунок 57

5. Появившееся окно (Рисунок 58) 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” или “LPTx”, где $x \in [1..9]$

   Product package – имя файла с настройками продукта CSP VPN Gate, созданного с помощью окна **VPN data maker**, вызываемого кнопкой E

   Кнопка E – вызывает окно **VPN data maker** (Рисунок 59) для задания политики безопасности и настроек продукта CSP VPN Gate.

   Device password – 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»).

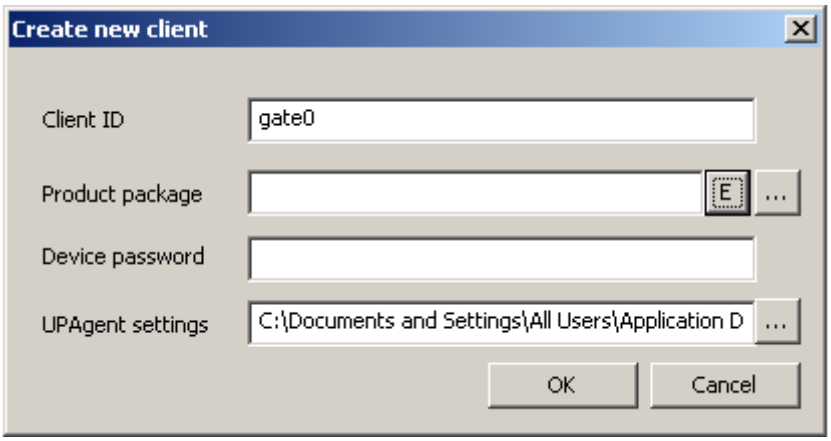


Рисунок 58

6. В поле **Client ID** введите идентификатор клиента, например, `gate0`.
7. Поле **UPAgent settings** оставьте без изменений, в нем указан файл с настройками Клиента управления.
8. В поле **Product package** нажмите кнопку E, появится окно **VPN data maker** (Рисунок 59).

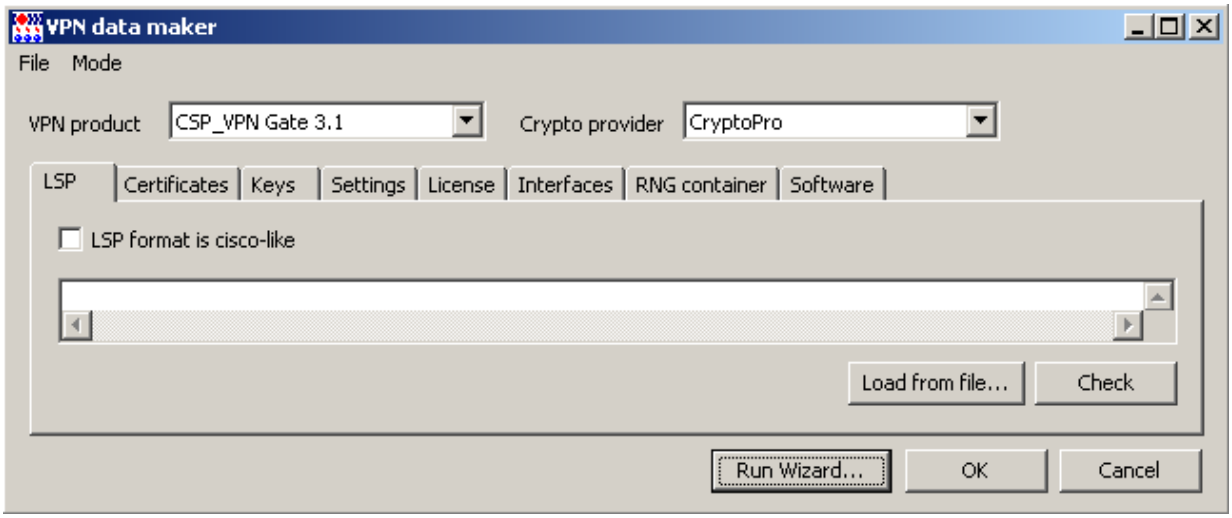


Рисунок 59

9. В окне **VPN data maker** выберите продукт CSP VPN Gate 3.1 и криптопровайдера CryptoPro (Рисунок 59).

10. Далее нужно задать политику безопасности для шлюза и другие настройки. Сложную политику можно задать во вкладке **LSP** (Рисунок 59) 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, покажем как это сделать. Нажмите кнопку Run Wizard в окне **VPN data maker**, появится окно для выбора метода аутентификации взаимодействующих сторон (Рисунок 60). Интерфейс этого окна описан в разделе «Задание политики и настроек с использованием мастера». Для получения сертифицированного решения для аутентификации сторон используйте сертификаты открытых ключей, а предопределенные ключи - только для целей тестирования.

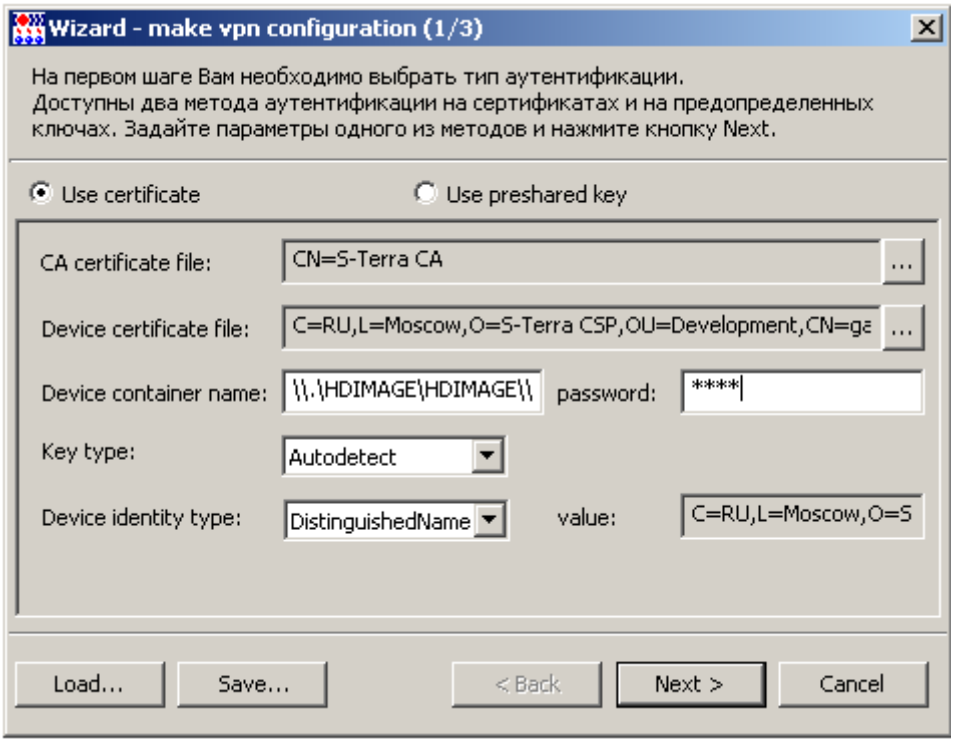


Рисунок 60

11. Выберите аутентификацию с использованием сертификатов:

В поле **CA certificate file** 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.

В поле **Device certificate file** отражается поле Subject локального сертификата управляемого устройства. Для этого в конце поля нажмите кнопку [...], в открывшемся окне выберите файл с локальным сертификатом. Обязательный параметр.

В поле **Device container name** отображается местоположение и имя ключевого контейнера на центральном шлюзе, в который он будет скопирован с USB-флеш при инициализации CSP VPN Gate.

В поле **Device container password** укажите пароль к контейнеру на центральном шлюзе.

В поле **Key type** установите значение ***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.

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 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.

12. 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. Для создания правила нажмите кнопку Add (Рисунок 61).

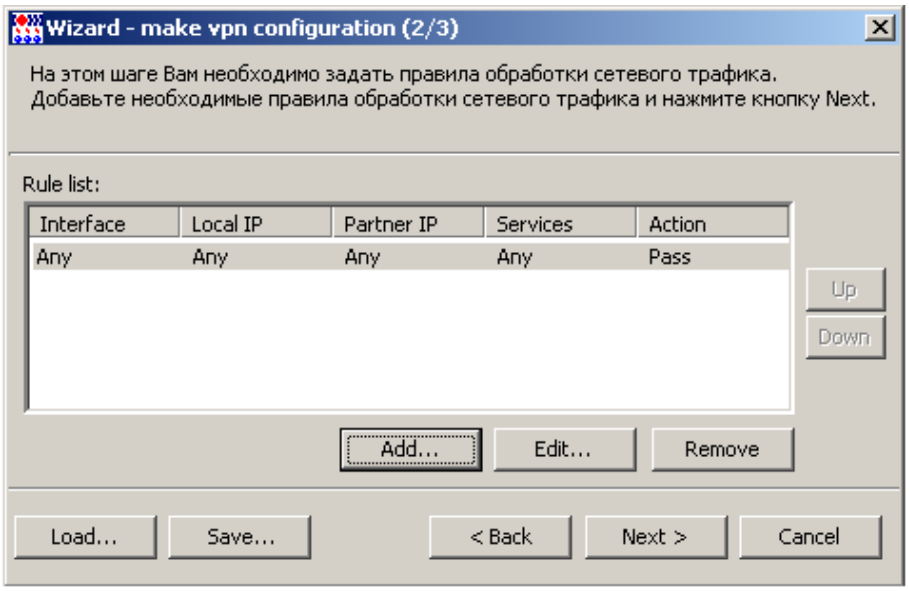


Рисунок 61

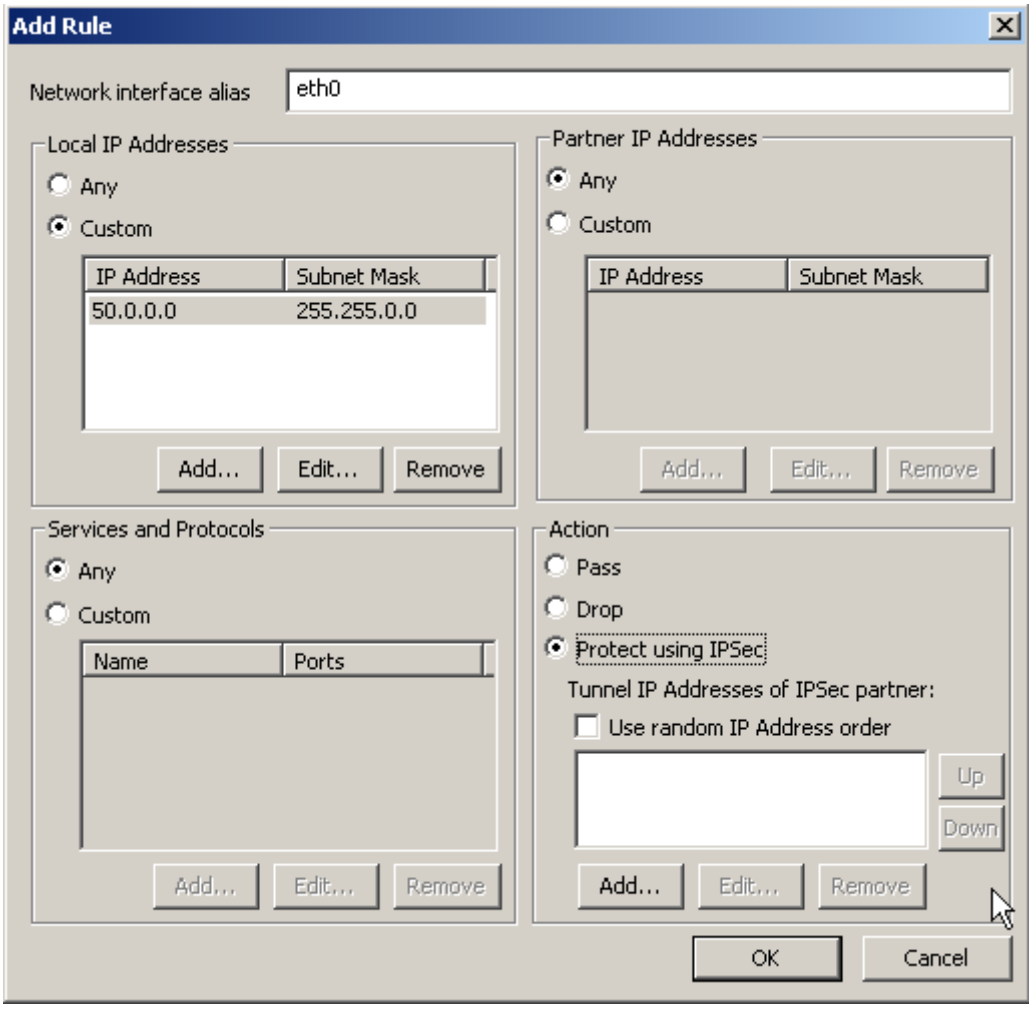


Рисунок 62

13. Создаваемое правило привяжите к интерфейсу шлюза с логическим именем, например, eth0, который смотрит во внешнюю сеть (Рисунок 2). В области **Local IP Addresses** (Рисунок 62) укажите адрес защищаемой подсети - 50.0.0.0/16, 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).
14. После нажатия кнопки OK появится предупреждение (Рисунок 63) о том, что не указан IP-адрес IPsec партнера, с которым центральный шлюз будет создавать IPsec-соединение. В этом случае шлюз будет работать только в качестве ответчика. Нажмите кнопку Yes.

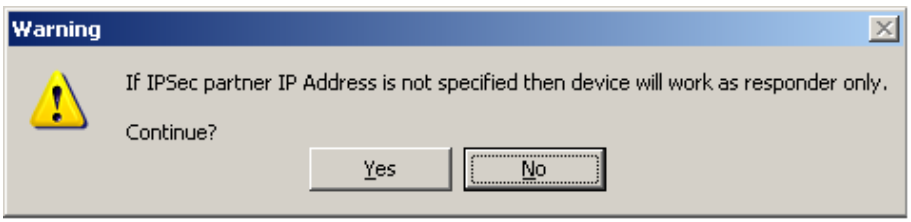


Рисунок 63

15. Увеличьте приоритет созданного правила (Рисунок 64), нажав кнопку Up.

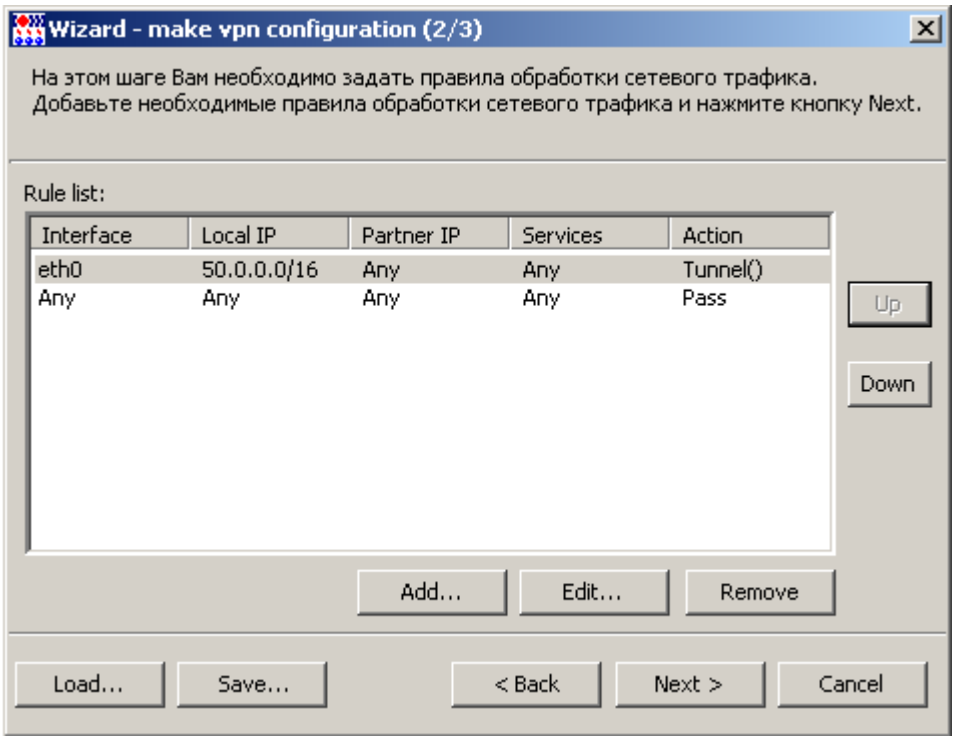


Рисунок 64

16. Нажмите кнопку Next.
17. Введите данные лицензии на продукт CSP VPN Gate и серийный номер лицензии на продукт криптопровайдера (КриптоПро CSP 3.6) (Рисунок 65). Эти данные можно взять с бланка лизензии, входящего в комплект поставки. Если на шлюзе лицензия на КриптоПро CSP 3.6 уже задана и не требуется ее замена, то поле **Serial number** оставьте пустым.

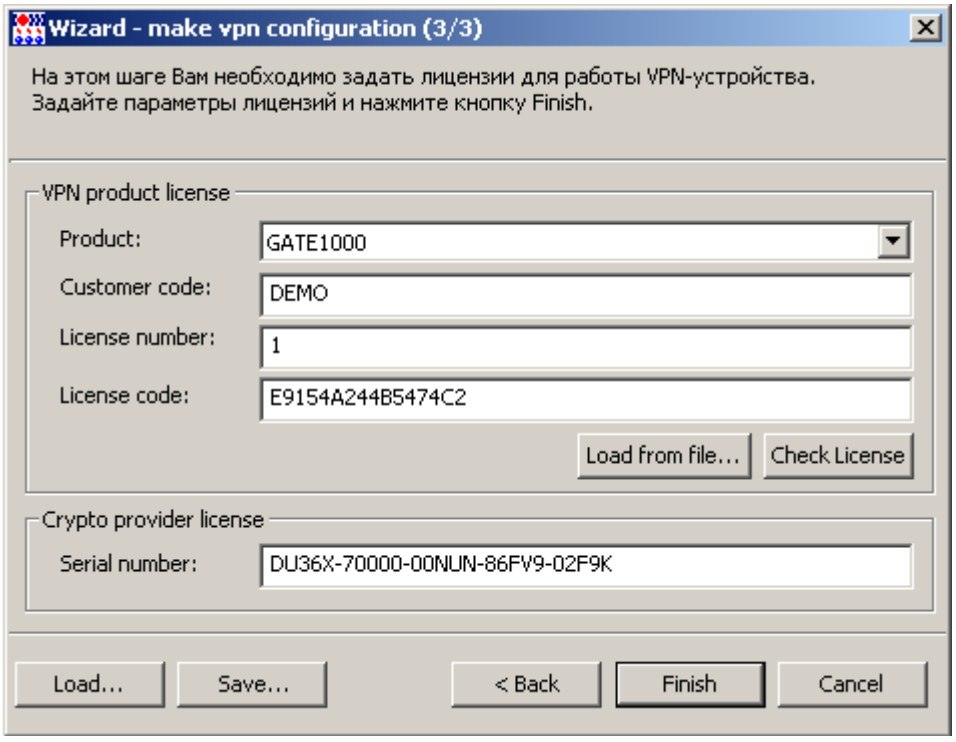


Рисунок 65

18. Сохраните введенные данные в окнах мастера, нажав кнопку Save…(Рисунок 65), и укажите имя файла-проекта в любом созданном вами каталоге (Рисунок 66).

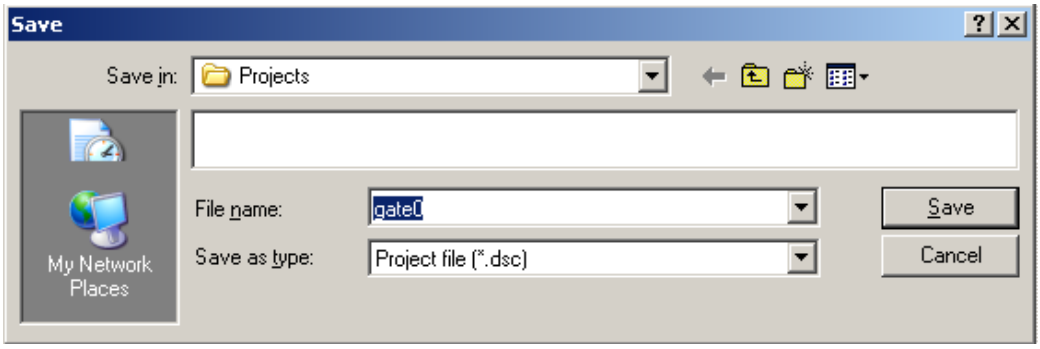


Рисунок 66

19. В окне мастера нажмите кнопку Finish (Рисунок 65). Все введенные данные будут отражены во вкладках проекта (Рисунок 67), за исключением вкладки **Interfaces**.

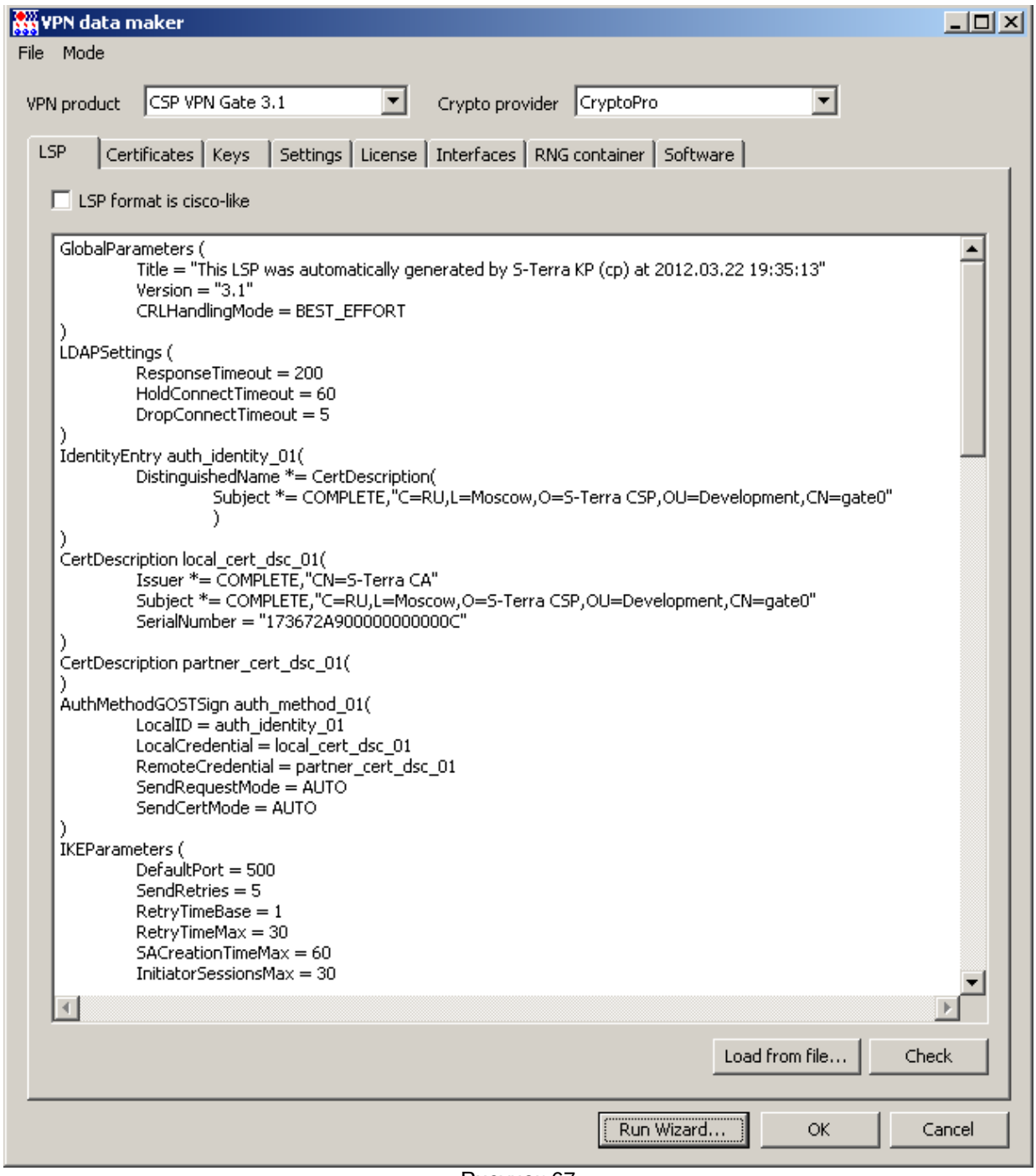


Рисунок 67

20. 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 68).

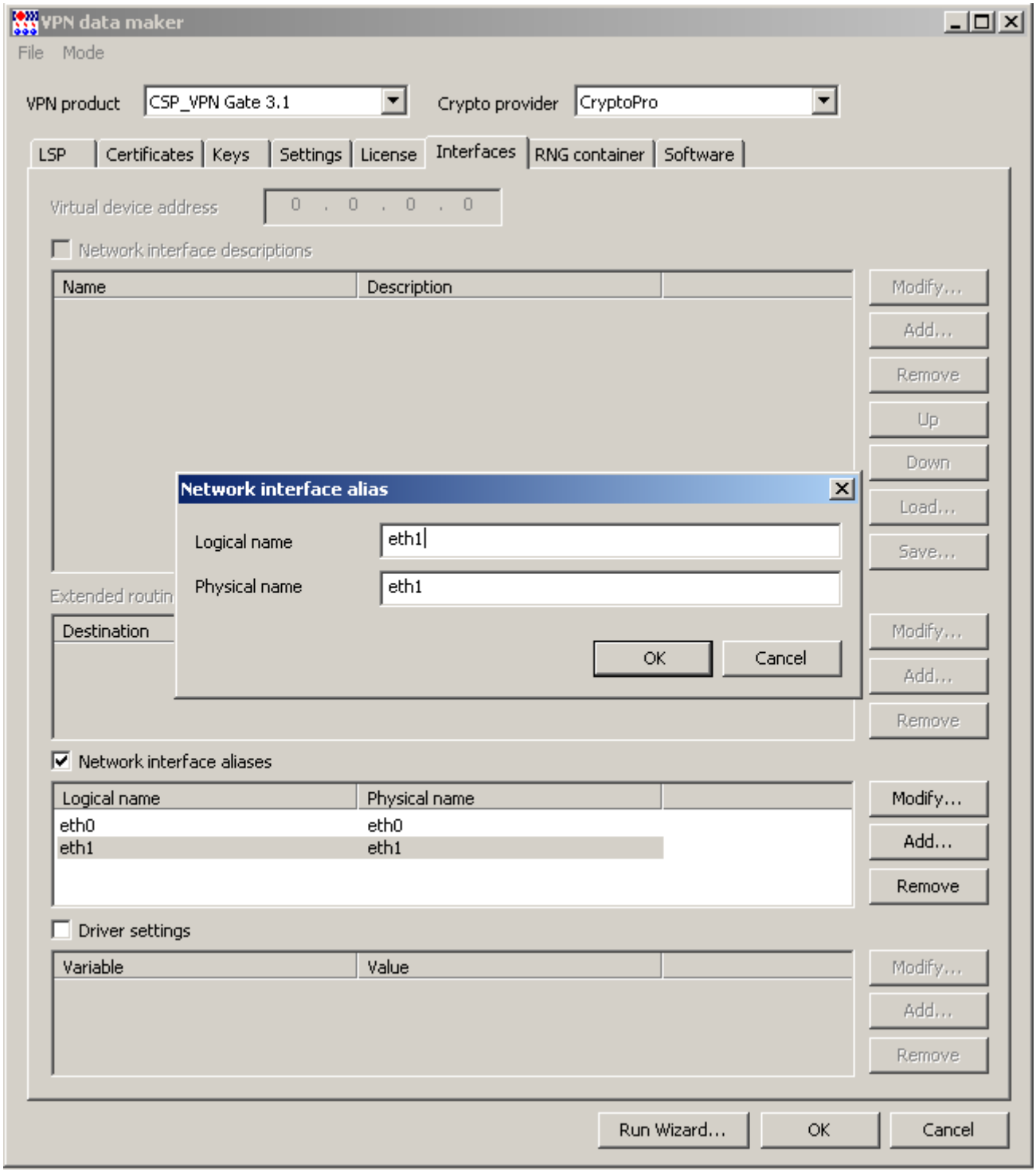


Рисунок 68

21. Во вкладке **Interfaces** нажмите кнопку OK, появится окно с настройками нового клиента (Рисунок 69), опять нажмите кнопку OK.

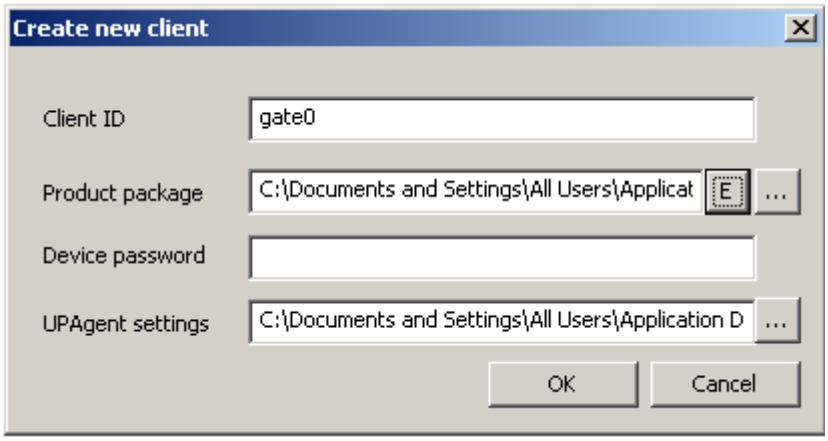


Рисунок 69

22. На Сервере управления в таблице клиентов появился новый клиент – gate0. Переведите его в активное состояние, выбрав в контекстном меню предложение ***Enable*** (Рисунок 70).

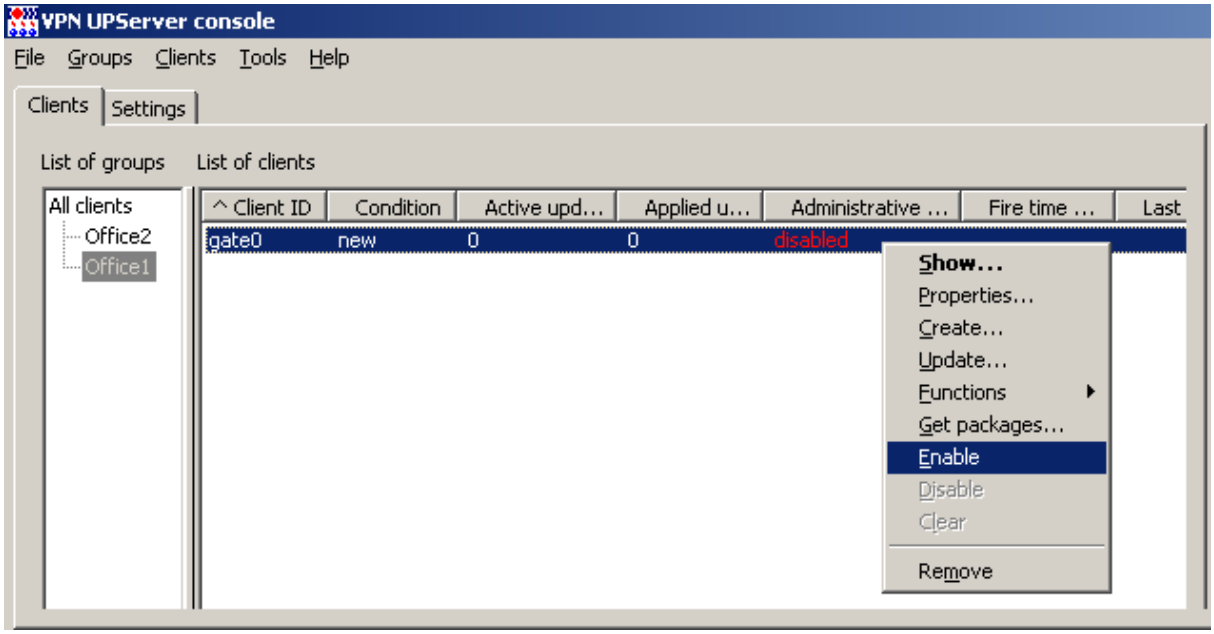


Рисунок 70

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. В таблице для клиента gate0 выберите предложение ***Get packages*** в контекстном меню (Рисунок 71).

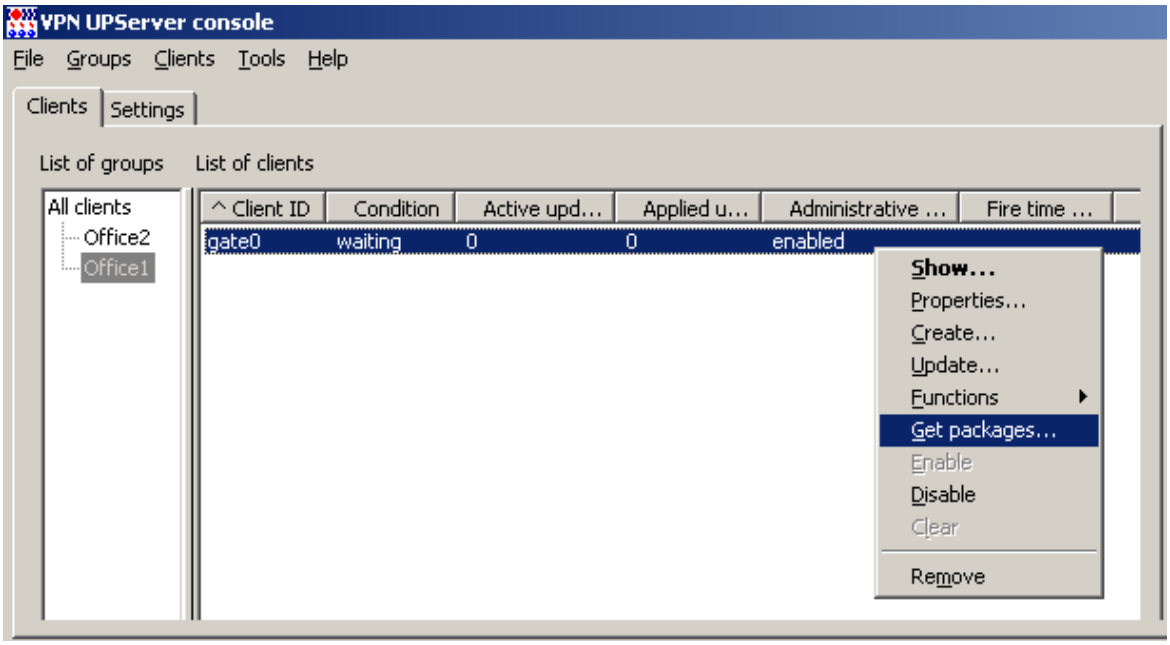


Рисунок 71

2. В открывшемся окне укажите каталог на USB-флеш для сохранения скриптов (Рисунок 72).

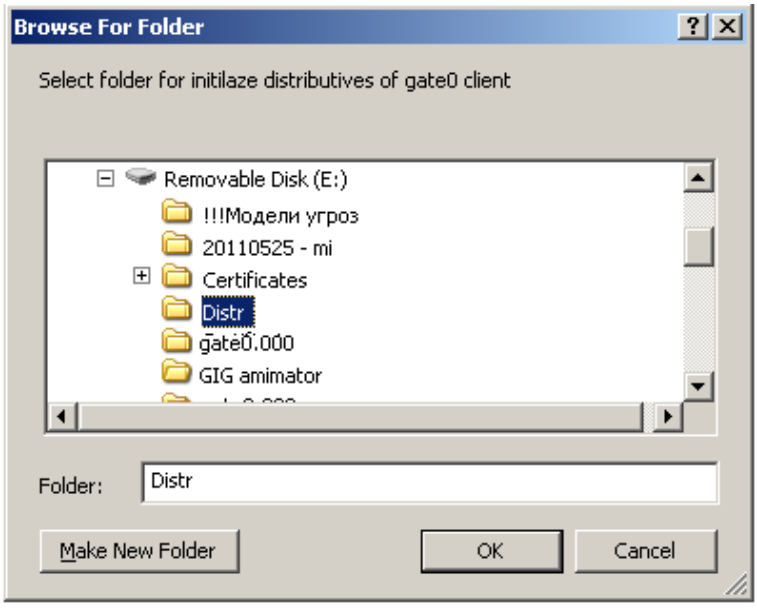


Рисунок 72

В указанный каталог будут сохранены два файла (Рисунок 73), (Рисунок 74):

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

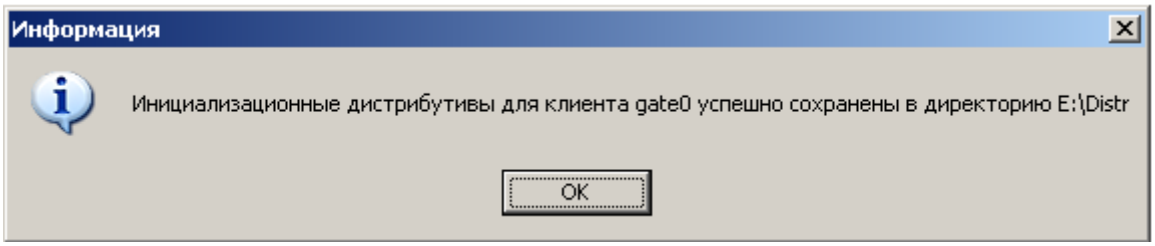


Рисунок 73

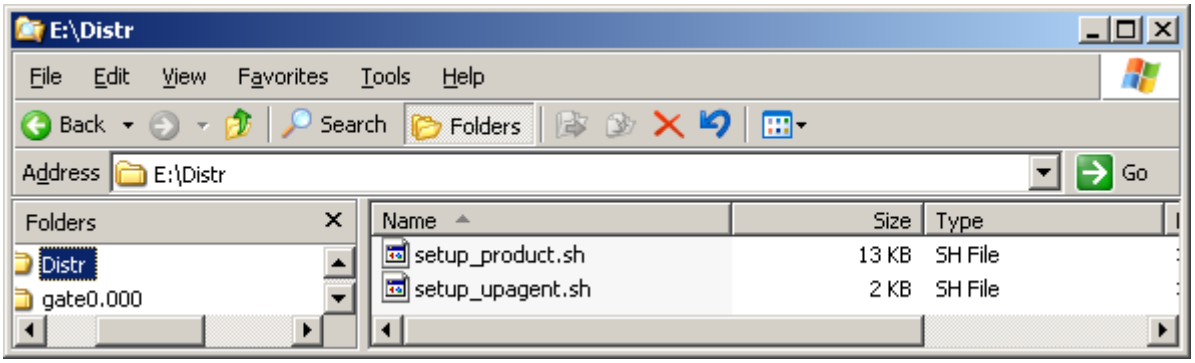


Рисунок 74

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 Клиент управления.

1. Вставьте USB-флеш с контейнером, CA и локальным сертификатом, двумя скриптами в ПАК CSP VPN Gate и выполните его монтирование, например, как устройство `sd1`:

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

2. Скопируйте с USB-флеш на ПАК CSP VPN Gate два подготовленных скрипта, например, в каталог `/tmp`:

```
mkdir /tmp
cp /mnt/Distr/setup_upagent.sh /tmp
cp /mnt/Distr/setup_product.sh /tmp
```

3. 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
```

4. 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.

Дистрибутивы продукта VPNUPAgent размещены на поставленном шлюзе в каталоге `/packages/VPNUPAgent`. Если это не так, то в каталоге установленного Сервера 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@50.0.10.110:/packages
```

И на шлюзе выполните команды:

```
cd /packages
tar xvf vpnupagent.tar
```

Запустите второй скрипт:

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

5. При успешном выполнении скриптов установится соединение с Сервером управления для проверки возможности скачивания обновлений. Состояние клиента изменится с **waiting** на **updating**, а затем на **active**. В **active** клиент готов к скачиванию обновлений (Рисунок 75).

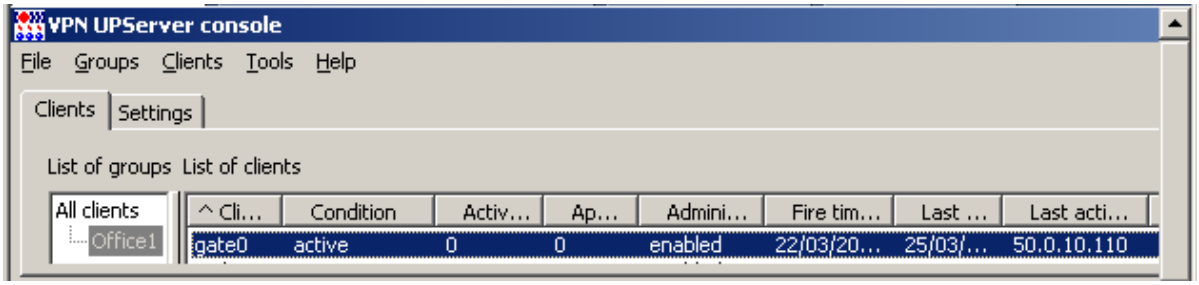


Рисунок 75

На этом настройка центрального шлюза закончена.

Настройка и управление СПДС «ПОСТ»

Для настройки СПДС “ПОСТ» нужно установить продукт SPDS Editor.

Установка SPDS Editor

1. На Сервере управления установите продукт SPDS Editor. Инсталляционный файл размещен в каталоге `Additional\SPDSEditor\setup.exe` дистрибутива продукта С-Терра КП. Запустите файл `setup.exe` и в появляющихся окнах нажимайте кнопку Next.

Рисунок 76

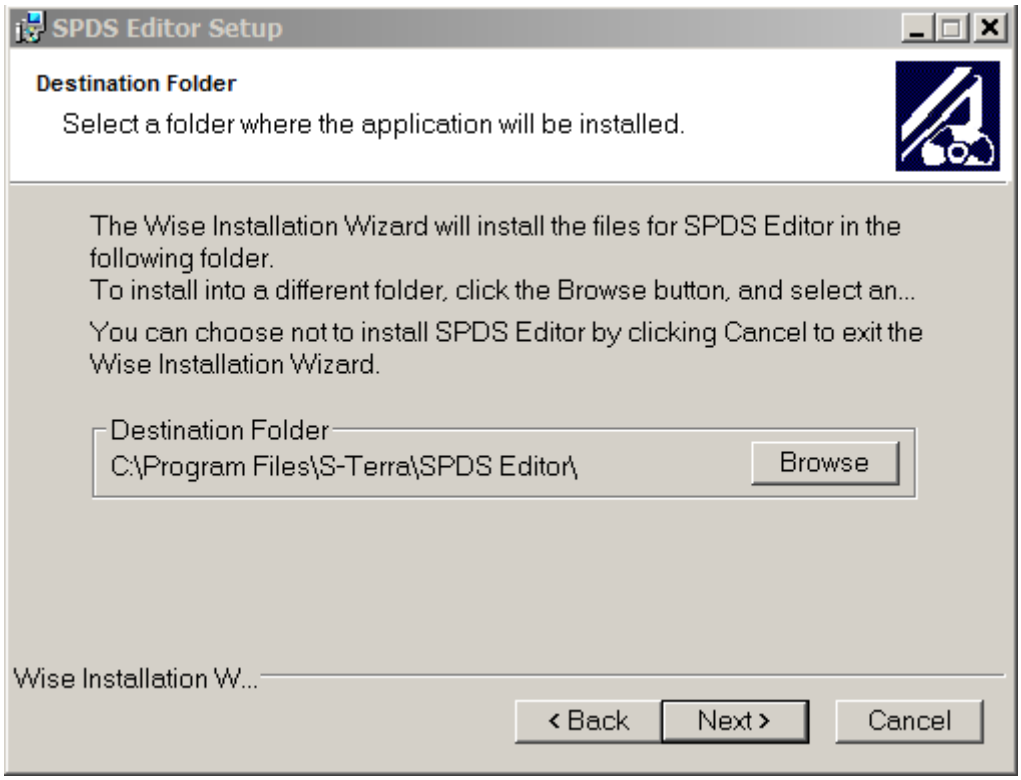


Рисунок 77

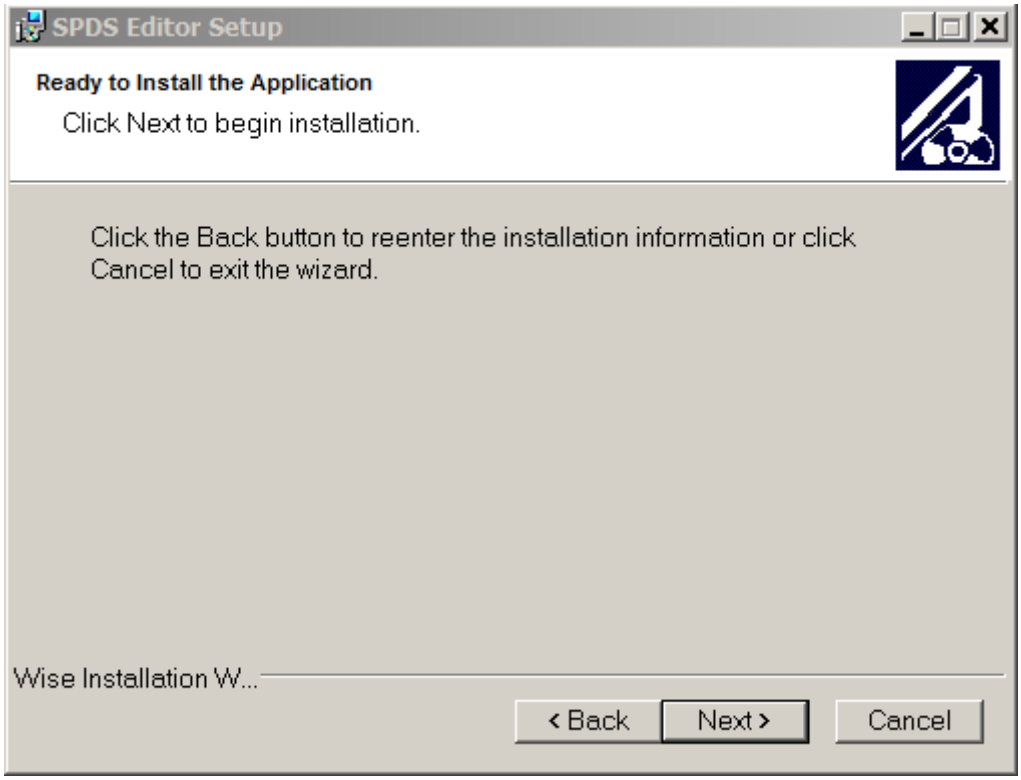


Рисунок 78

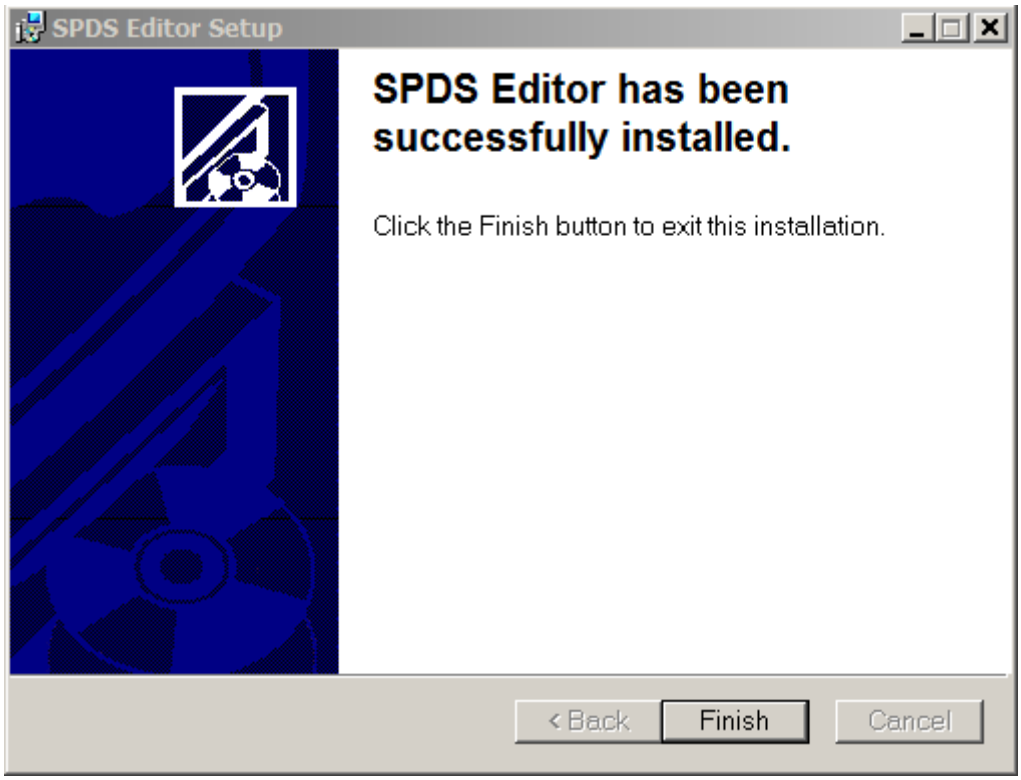


Рисунок 79

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

Создание ключевой пары и запроса на сертификат СПДС «ПОСТ»

1. Запустите установленный SPDS Editor – `Пуск-Программы-S-Terra-SPDS Editor-SPDS Editor` (Рисунок 80).

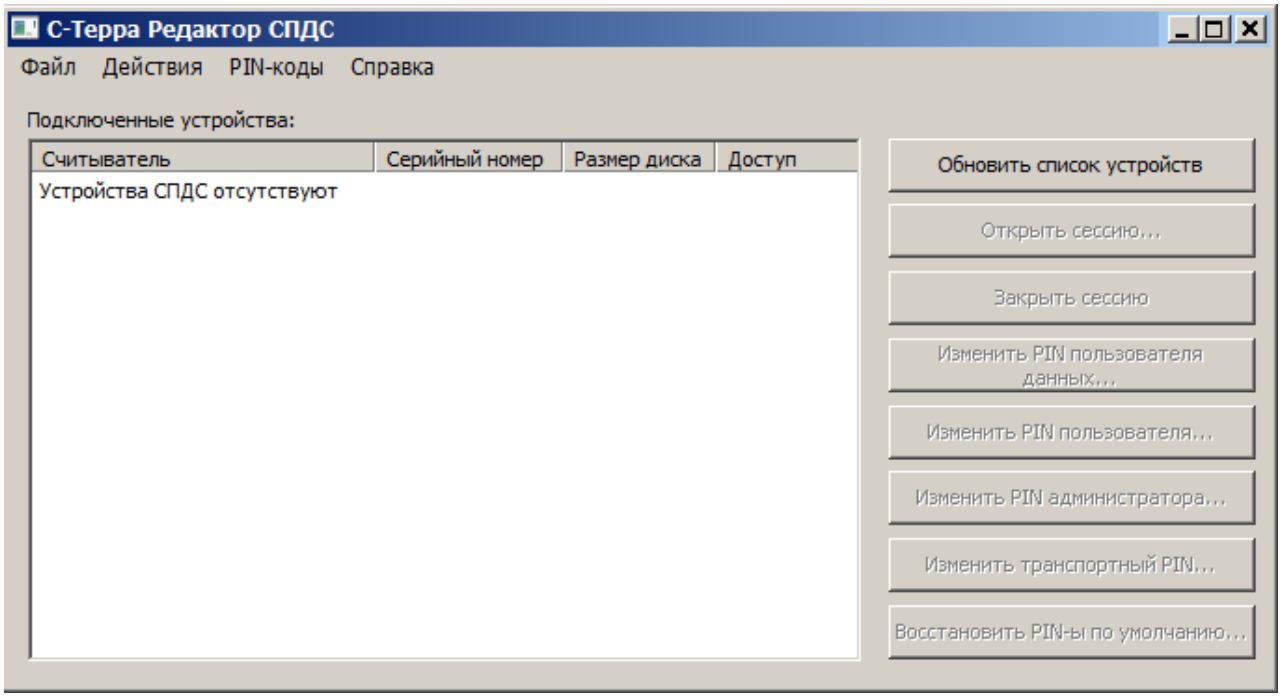


Рисунок 80

Меню ***Действия*** и ***PIN-коды*** дублируются кнопками на правой панели окна **С-Терра Редактор СПДС.** Единственное отличие – если не выделено никакого устройства, то доступно действие – ***Закрыть все сессии.***

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 низкоуровых 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 81).
5. Нажмите кнопку «Открыть сессию» для открытия Раздела данных на запись (Рисунок 82).
6. В окне **Авторизация** введите PIN пользователя данных и нажмите ОК.
7. Устройство СПДС «ПОСТ» готово для записи (Рисунок 83).

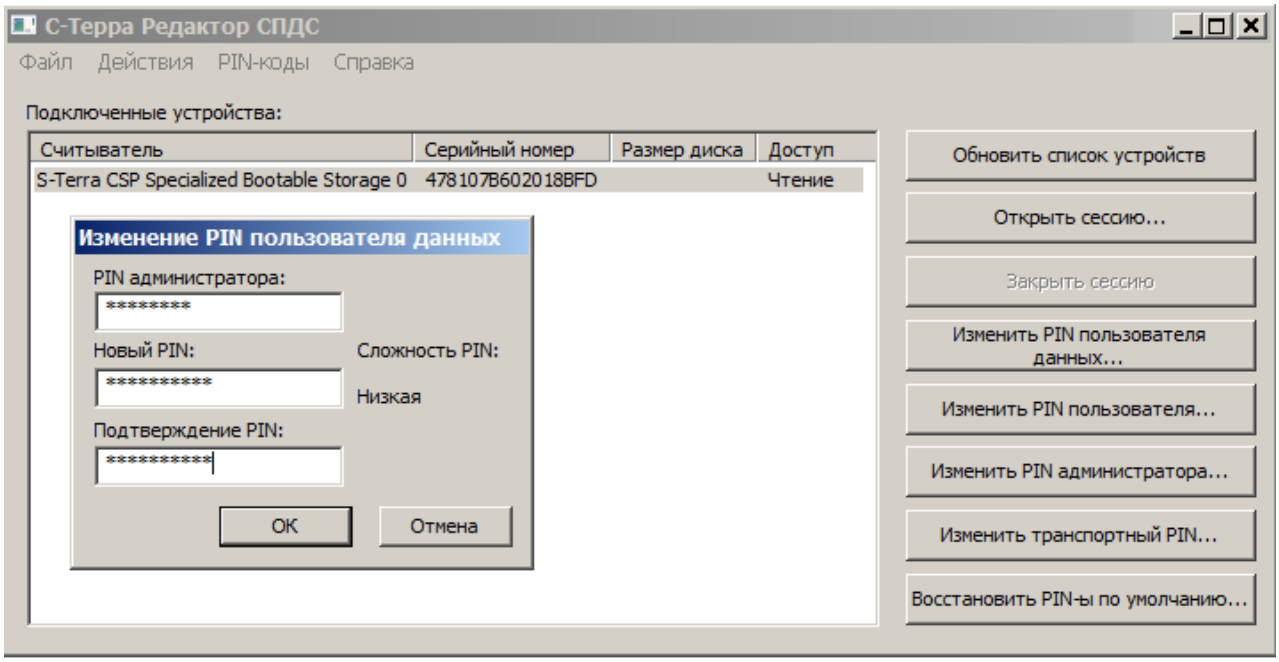


Рисунок 81

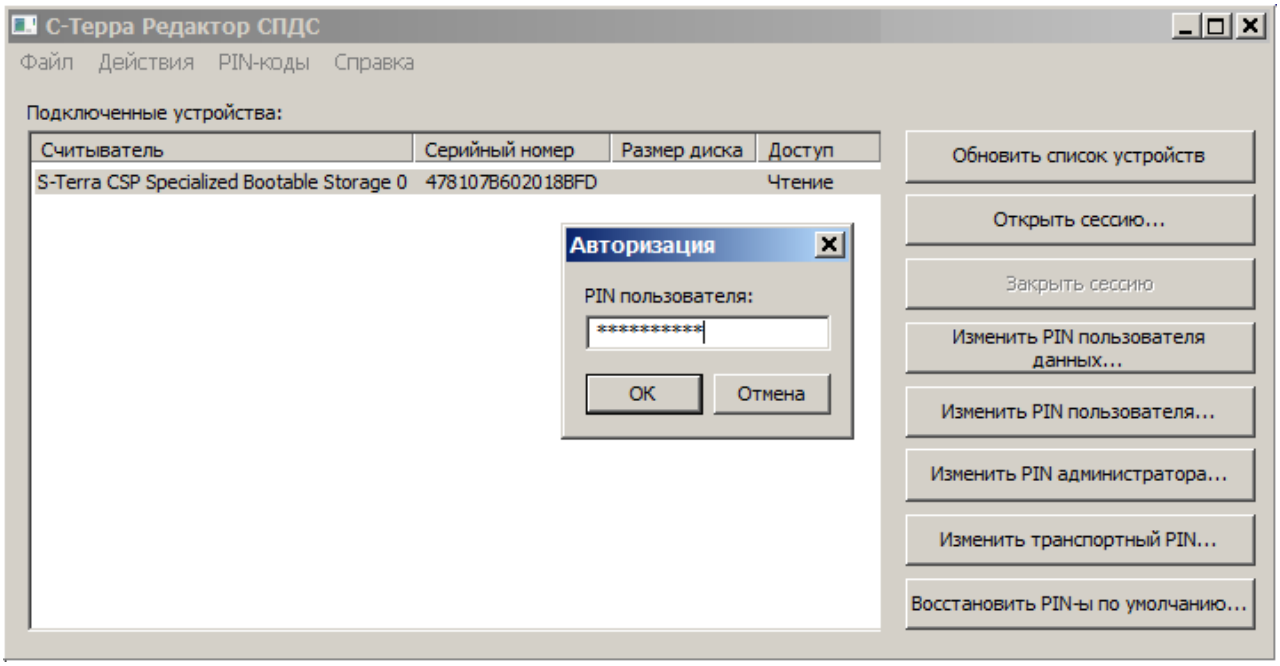


Рисунок 82

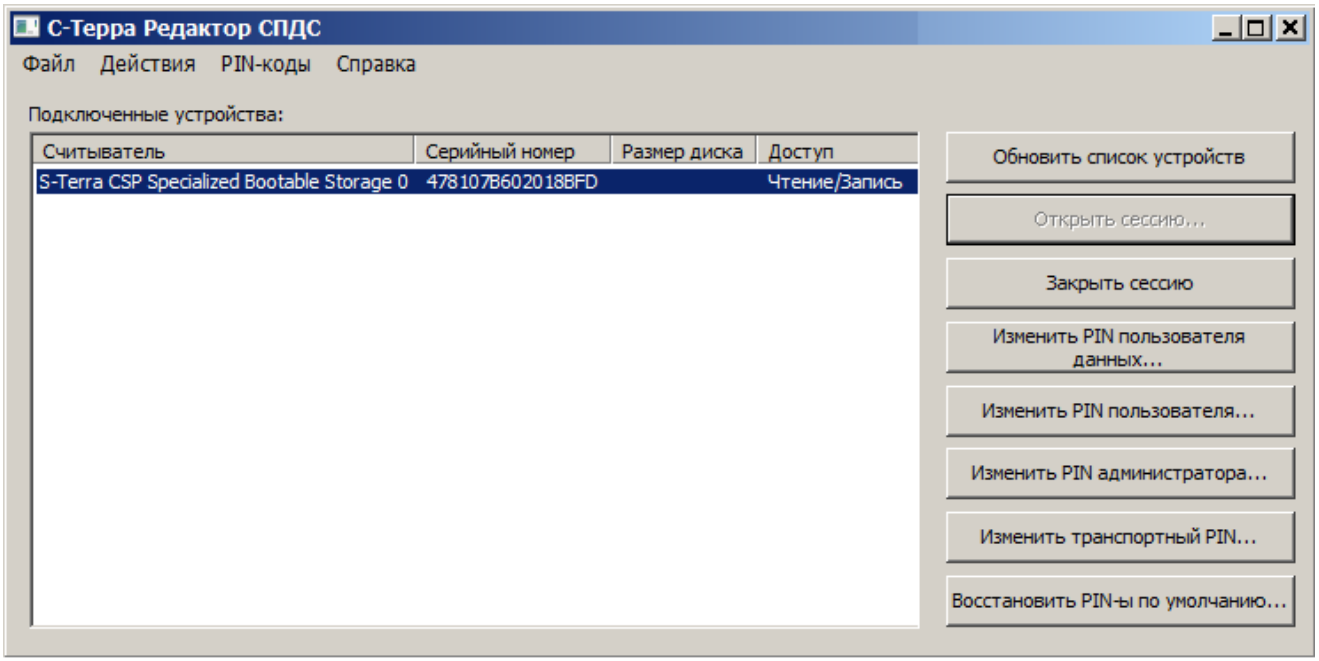


Рисунок 83

8. 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 УЦ и утилиту `certsrv (Certificate Service)`.

9. Следуйте рекомендациям, как было описано ранее для центрального шлюза. А форму расширенного запроса заполните по следующему образцу:

   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

По этому образцу заполните форму запроса и нажмите кнопку Submit.

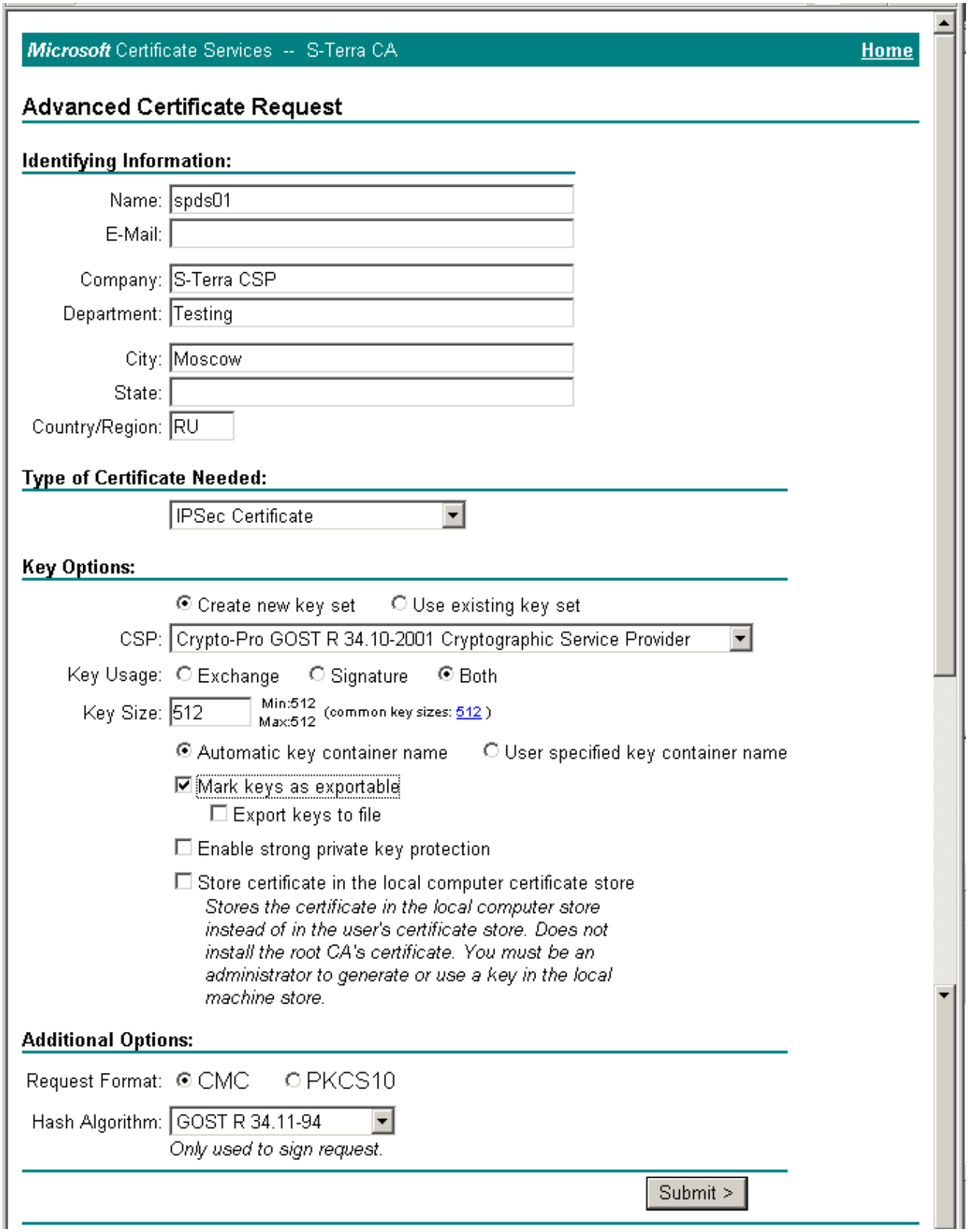


Рисунок 84

10. На следующем предупреждении нажмите кнопку Yes.

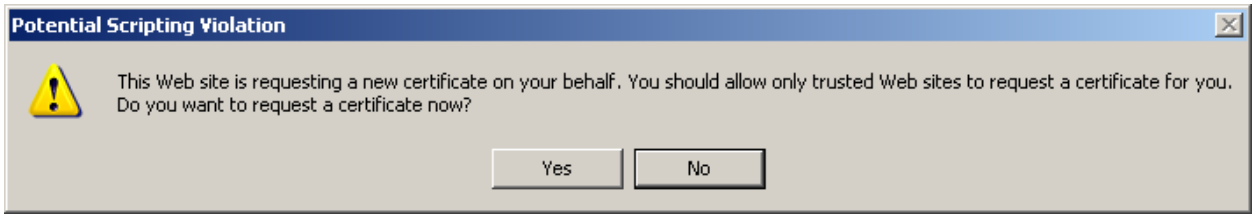


Рисунок 85

11. В следующем окне укажите ключевой носитель, соответствующий СПДС «ПОСТ» и нажмите ОК.

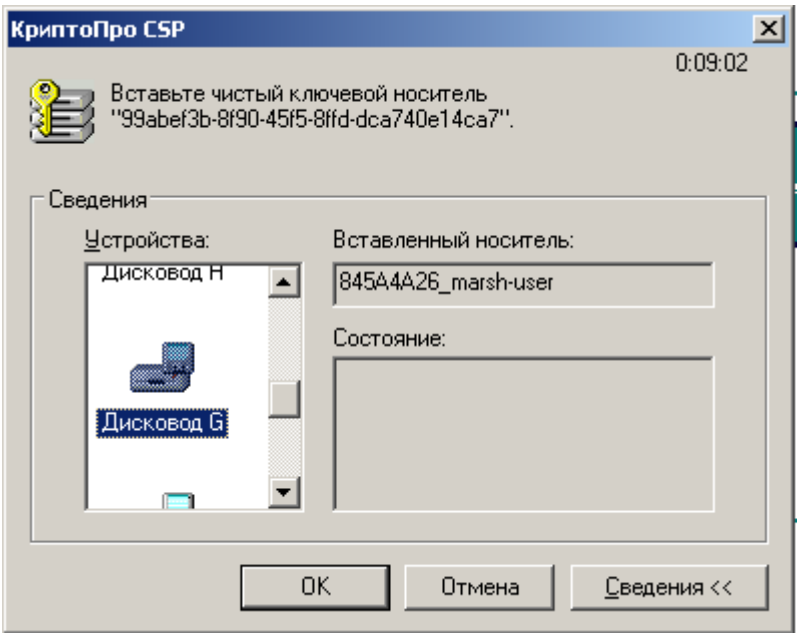


Рисунок 86

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

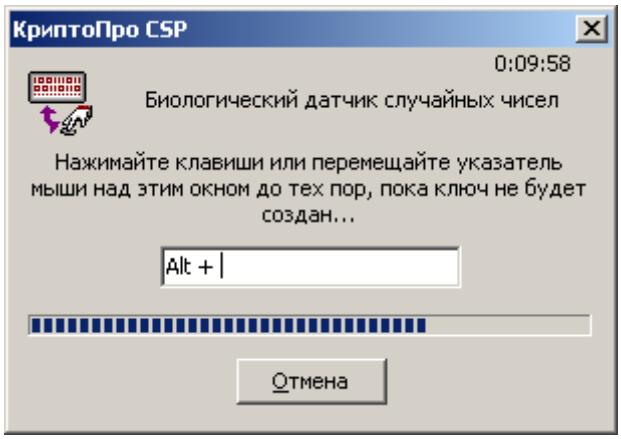


Рисунок 87

13. В окне запроса пароля поля оставьте пустыми, чтобы можно было скопировать контейнер при инициализации устройства СПДС.

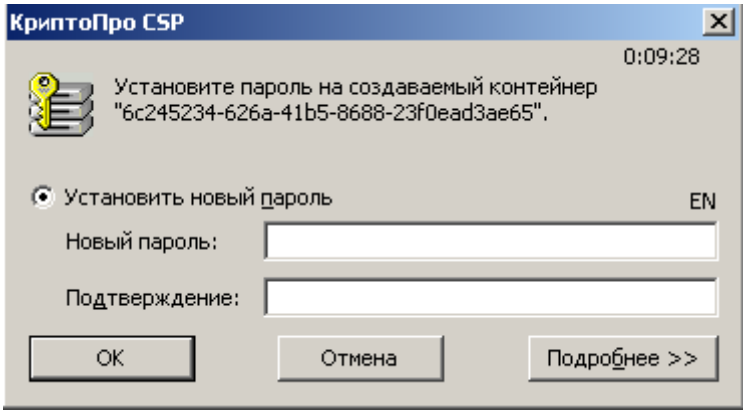


Рисунок 88

14. 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`.

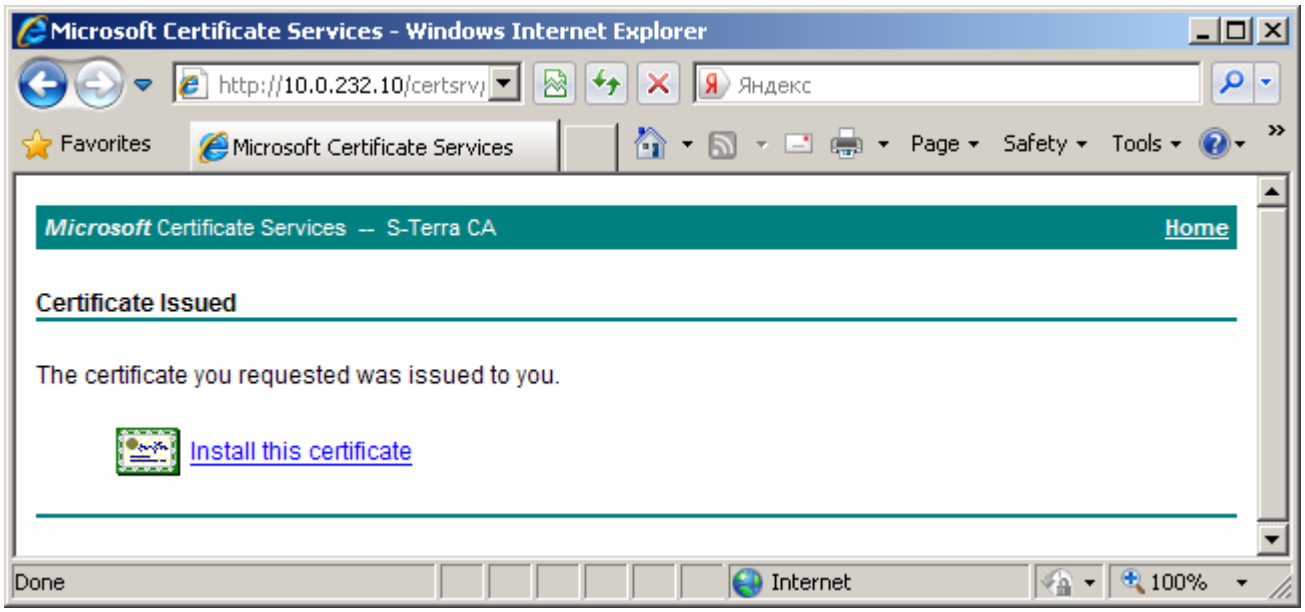


Рисунок 89

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

15. Экспортируйте локальный сертификат из контейнера в файл на Сервер управления, он будет необходим при настройке устройства СПДС «ПОСТ».
16. Также экспортируйте и CA сертификат в файл.

Создание настроек для СПДС «ПОСТ»

На устройстве СПДС «ПОСТ» установлена ОС и продукты CSP VPN Gate, КриптоПро CSP. Создание скриптов для инициализации CSP VPN Gate, создания политики безопасности и настроек осуществляется 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 90).

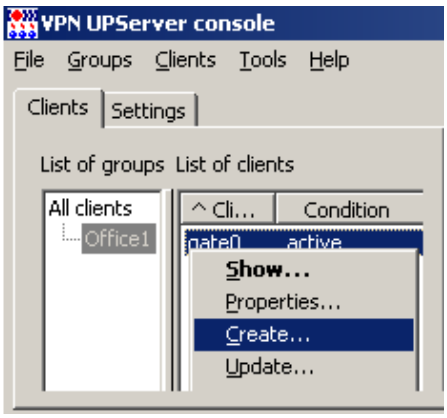


Рисунок 90

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

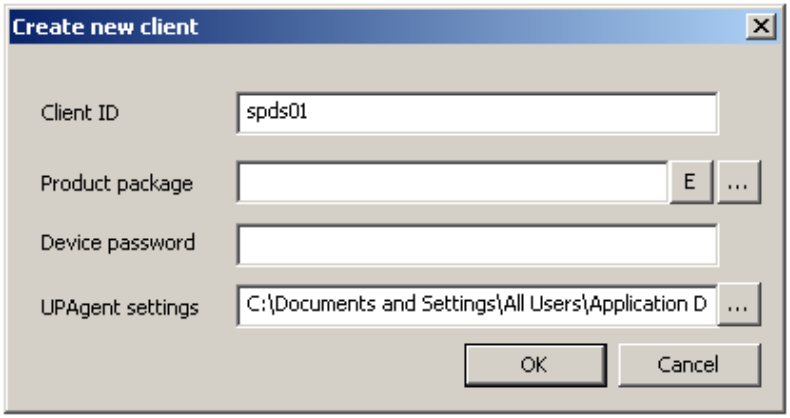


Рисунок 91

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.

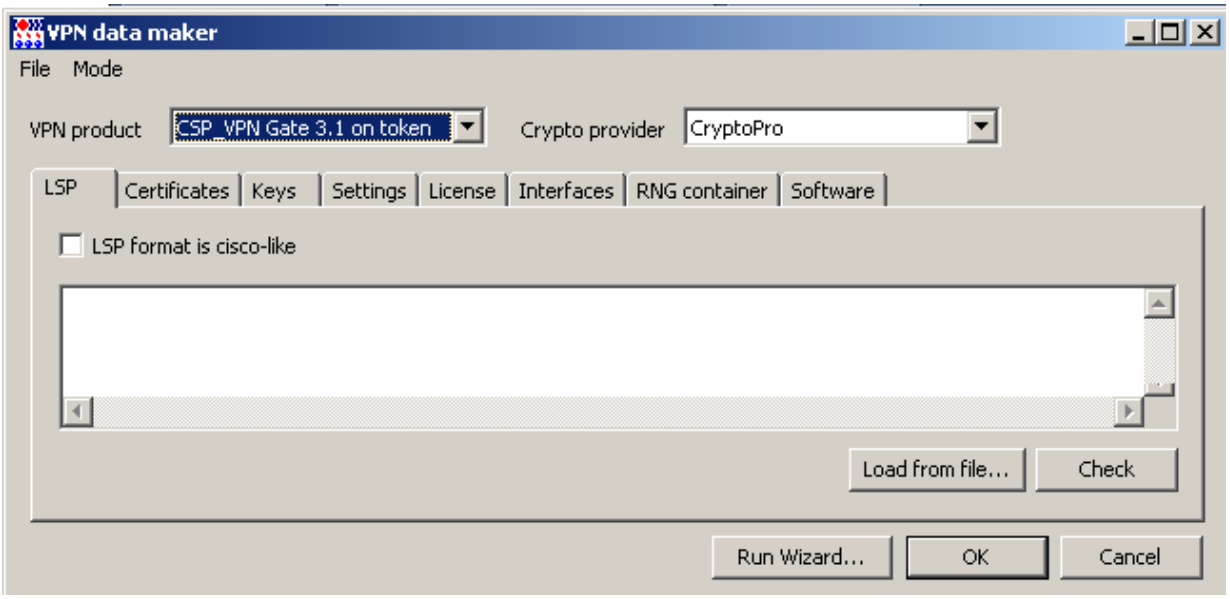


Рисунок 92

4. В первом окне мастера (Рисунок 93) выберите метод аутентификации сторон с использованием сертификатов:

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 уже на скопированный контейнер 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 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.

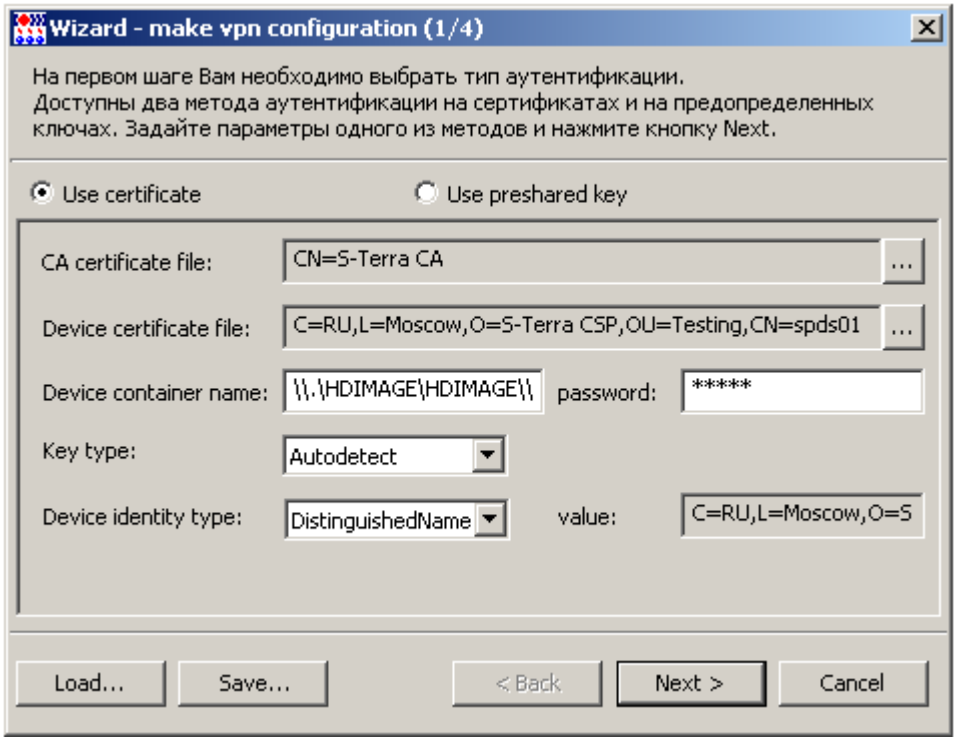


Рисунок 93

5. Во втором окне мастера (Рисунок 94) задайте правило, по которому будет пропускаться трафик от СПДС «ПОСТ» к Серверу управления и другим ресурсам в защищаемой подсети. Трафик между СПДС «ПОСТ» и центральным шлюзом должен защищаться по протоколу IPsec, для этого нажмите кнопку Add.

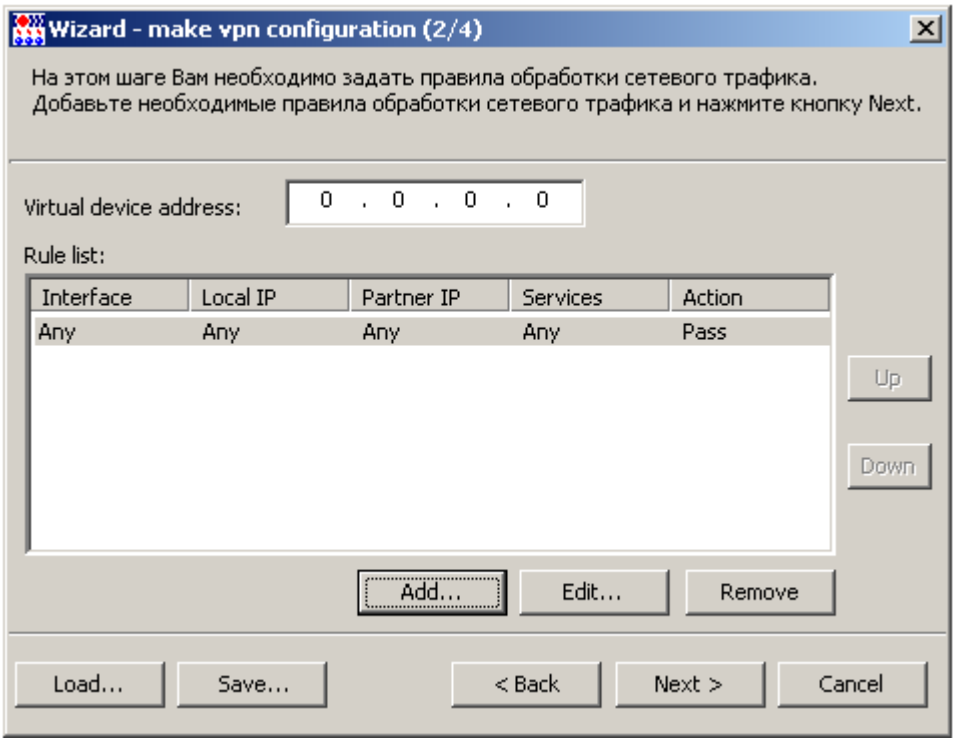


Рисунок 94

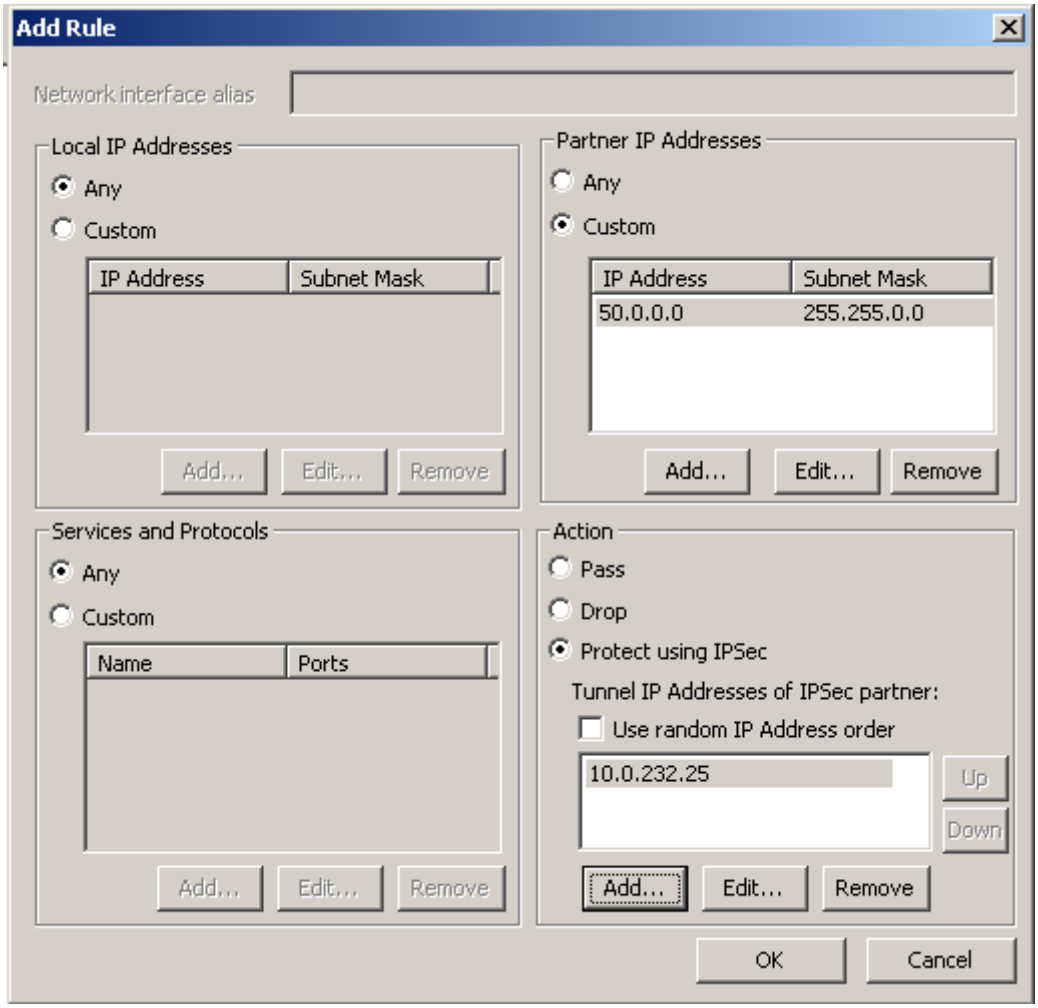


Рисунок 95

6. В окне **Add Rule** (Рисунок 95) укажите следующее:
   - в области **Local IP Addresses** поставьте переключатель в положение ***Any***.
   - в области **Partner IP Addresse**s поставьте переключатель в положение ***Custom*** и укажите адрес всей подсети Сервера управления, например, 50.0.0.0/16.
   - в области **Action** – укажите IPsec-партнера, с которым будет построено защищенное соединение. В нашем случае – это адрес интерфейса шлюза10.0.232.25, защищающего подсеть с Сервером управления.

   Нажмите кнопку OK.
7. Увеличьте приоритет созданного правила, используя кнопку Up.

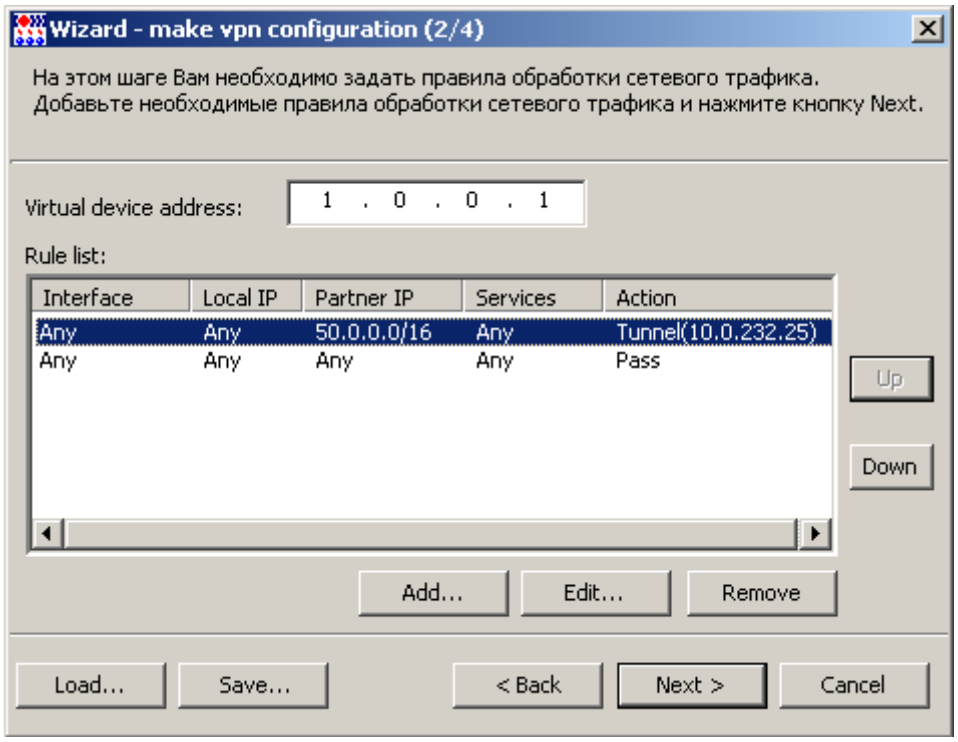


Рисунок 96

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.
9. В третьем окне мастера (Рисунок 97) укажите настройки целевого ПО, установленного на СПДС «ПОСТ», и сетевые настройки.
   - в поле **Software type** выберите клиента - Web-client, RDP-client, Other, в качестве которого будет выступать СПДС «ПОСТ».
   - в поле **Software server address** укажите адрес защищаемого сервера, к которому осуществляется удаленный доступ с СПДС «ПОСТ». Это может быть один IP-адрес (IPv4) либо список адресов, разделенных точкой с запятой. Для целевого ПО Firefox – указывается полный URL-адрес.
   - в поле **Software user name** введите имя пользователя, который будет иметь доступ к удаленному серверу. По умолчанию для RDP-клиента назначен пользователь с именем 'user'.
   - в поле **Software options** указываются дополнительные настройки для каждого целевого ПО. Для RDP-клиента по умолчанию заданы следующие настройки:

     ```
     -k en-us -D -g <размер_экрана> -a 16 -z -r disk:disk=/disk -r scard
     ```

     где

`-k en-us` – раскладка клавиатуры

`-D` – убрать декорацию окна

`-g <размер_экрана>` - отображаемый размер окна. Размер вычисляется автоматически в зависимости от разрешения экрана за вычетом места под управляющую панель СПДС

`-a 16` – палитра 16 цветов

`-z` – сжатие протокола при передаче

`-r disk:disk=/disk` – доступ с удаленного компьютера к локальному диску /disk как к сетевому устройству \\tsclient\disk

`-r scard` – доступ с удаленного компьютера на картридер локального компьютера.

Эти настройки могут быть переопределены. Можно указать и настройки с другими опциями, они не будут интерпретированы.СПДС и целевым ПО, а переданы в неизменном виде.

Если СПДС «ПОСТ» выступает в качестве RDP-клиента, то поставьте переключатель в это положение и укажите адрес RDP-сервера, например, 50.0.10.112 (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).

- Сетевые настройки можно подготовить заранее, записав в файлы, и указать каталог в поле **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`.

Сетевые настройки соединения можно будет задать позже в окне Edit connection во вкладке ***Interfaces***. Если сетевые настройки не указывать, то пользователю самому придется выполнять их.

Нажмите кнопку Next.

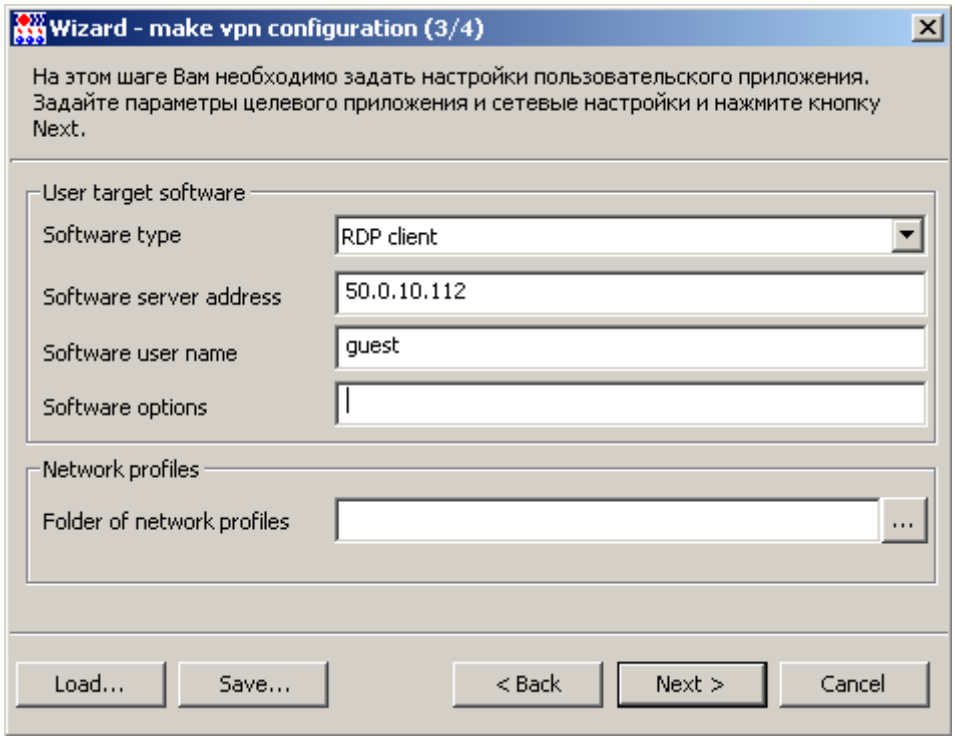


Рисунок 97

10. В следующем окне укажите лицензионные данные на продукт CSP VPN Gate и СКЗИ «КриптоПро CSP 3.6» (Рисунок 98).

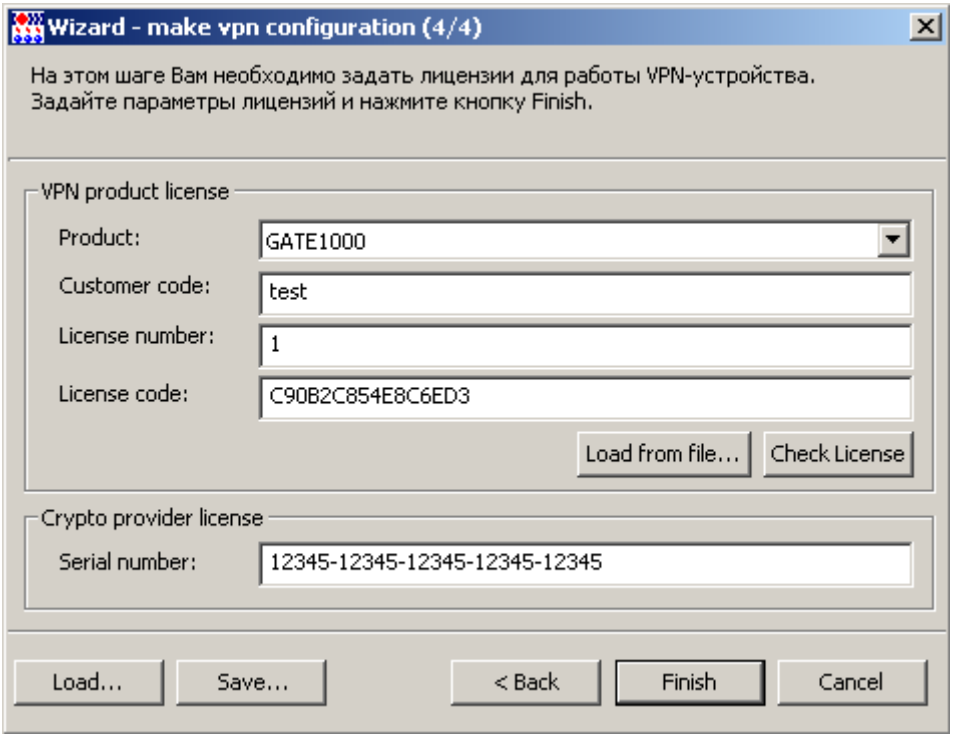


Рисунок 98

11. Далее нажмите кнопку Save для сохранения данных проекта (Рисунок 99).

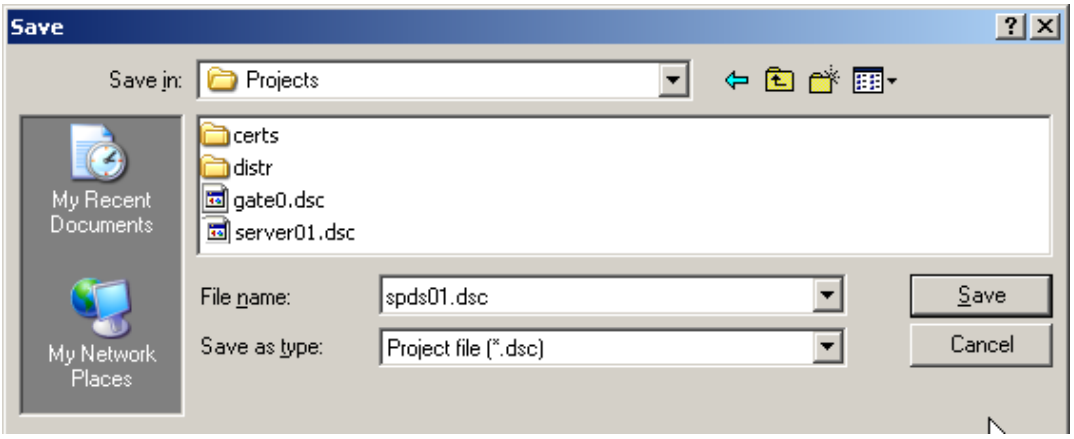


Рисунок 99

12. Затем нажмите кнопку Finish.

13. В окне **VPN data maker** перейдите во вкладку **Interfaces**. В разделе **Extended routing** прописались маршруты в результате заполнения окон мастера. В разделе **Network interface descriptions** можно установить флажок и задать сетевые настройки соединений, если они не были заданы ранее с использованием профайлов. Для задания настроек в данном разделе нажмите кнопку Add -. появится окно **Edit connection** (Рисунок 101).

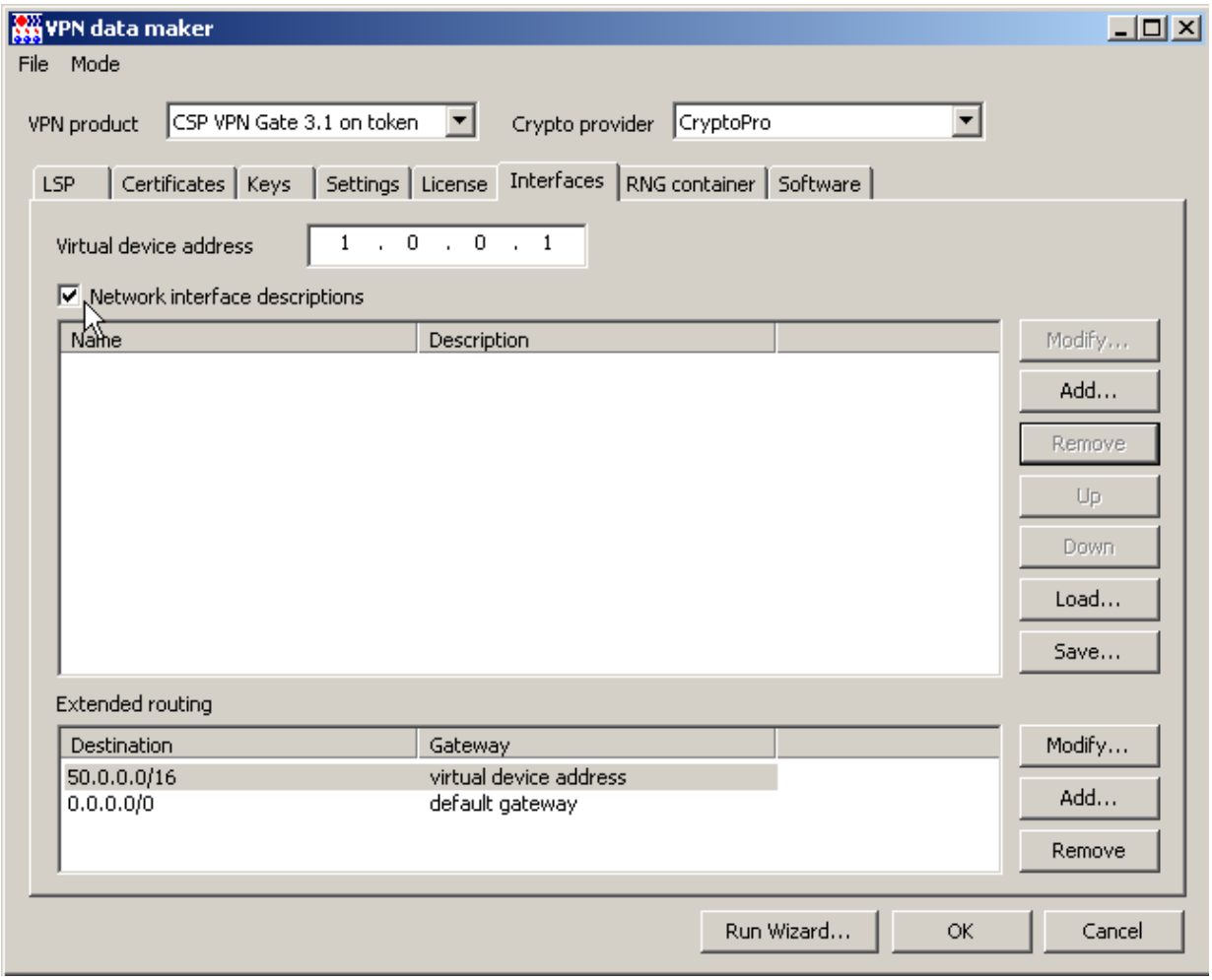


Рисунок 100

14. Окно **Edit connection** описано в аналогичном разделе главы «Описание интерфейса Сервера управления». Например, для проводного соединения для получения динамического адреса интерфейса по протоколу DHCP, в который будет вставлен СПДС «ПОСТ», установите следующие настройки и нажмите кнопку OK (Рисунок 101):

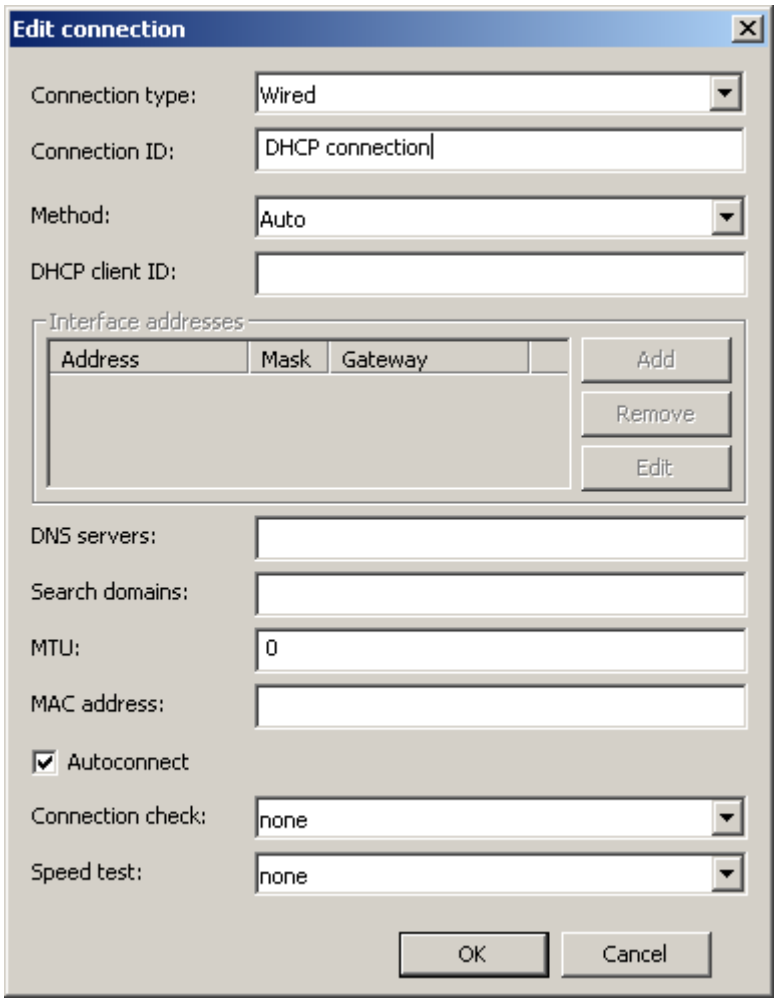


Рисунок 101

При назначении статического адреса интерфейсу СПДС «ПОСТ», например, для нашего стенда, установите следующие настройки и нажмите OK.

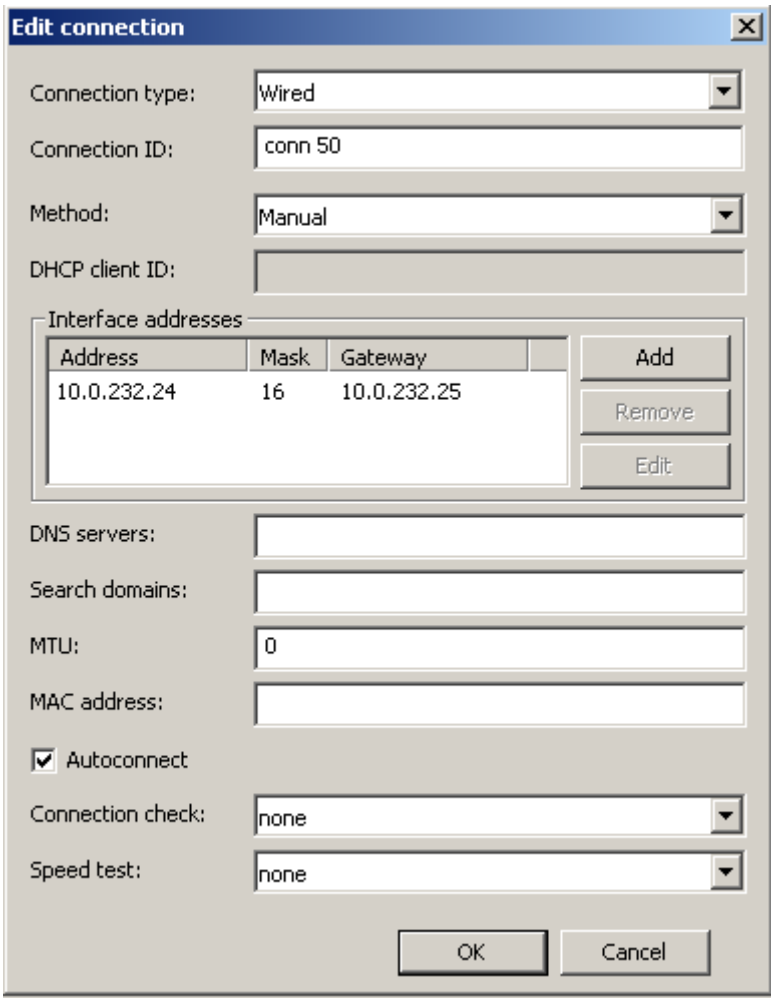


Рисунок 102

15. Опять нажмите кнопку OK.

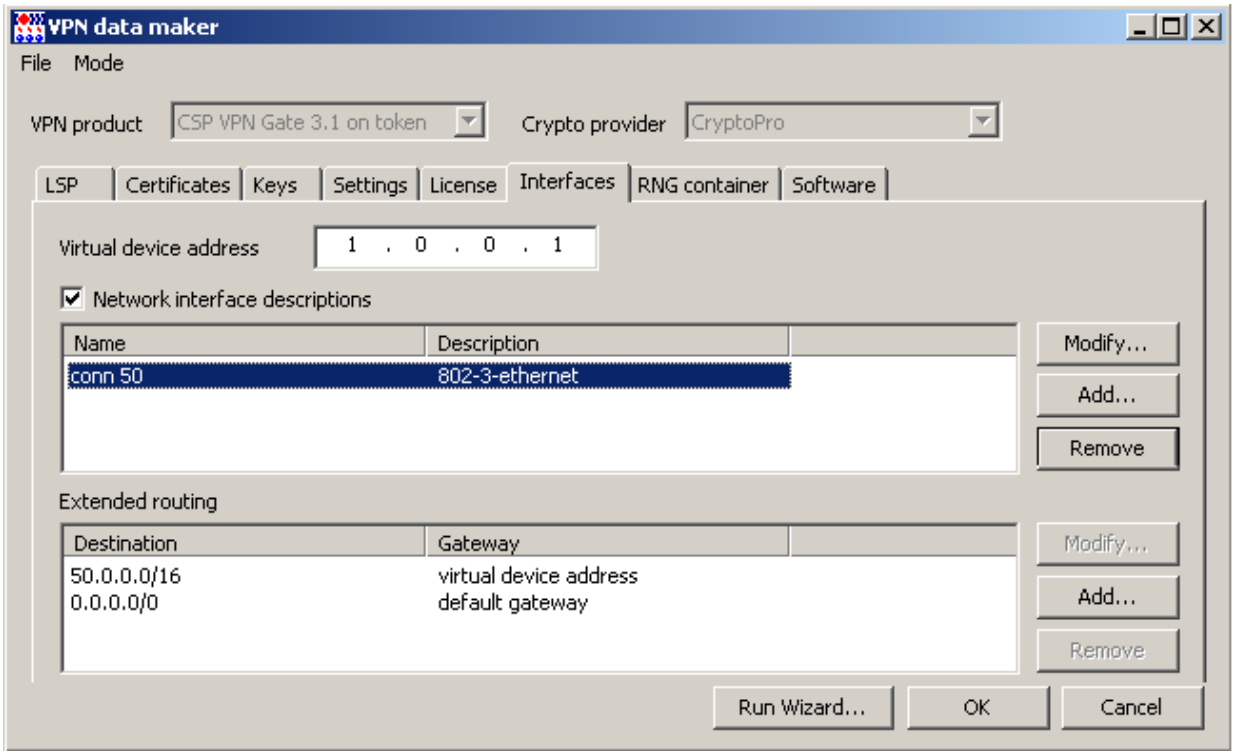


Рисунок 103

16. В окне создания нового клиента также нажмите кнопку OK (Рисунок 104).

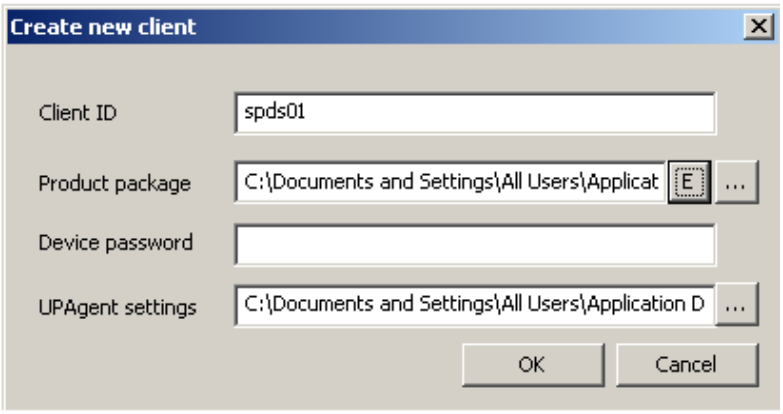


Рисунок 104

17. На Сервере управления выделите строку с новым клиентом и в контекстном меню выберите предложение ***Enable***, чтобы активировать клиента (Рисунок 105).

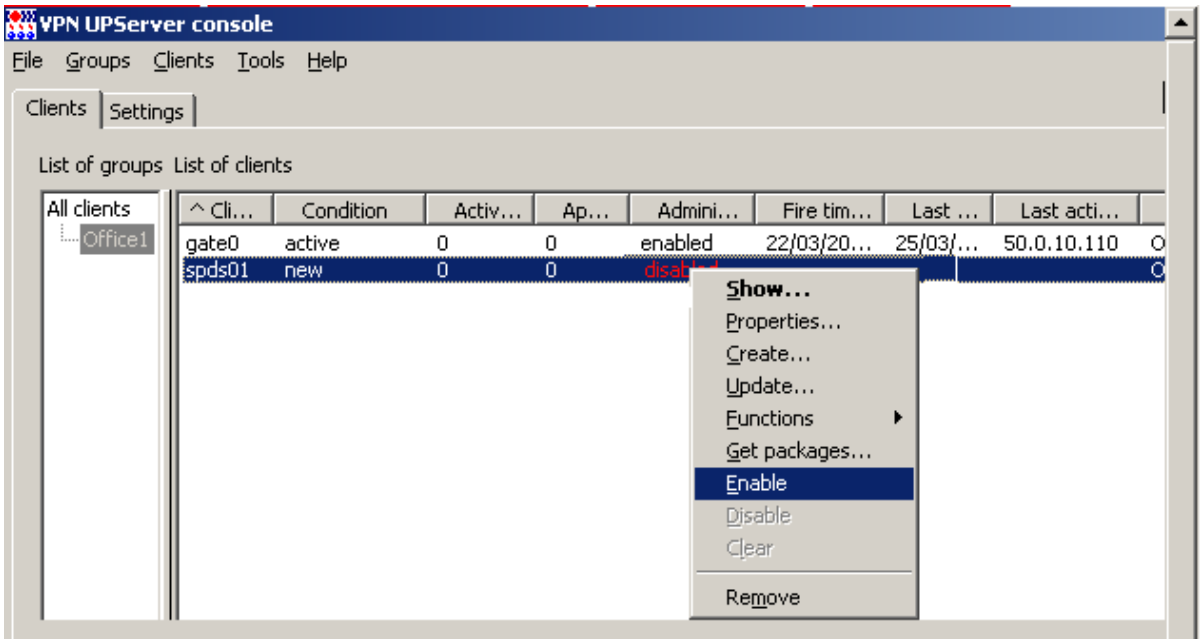


Рисунок 105

Note

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

18. На центральном шлюзе в таблицу маршрутизации внесите маршрут для доступа на адрес 1.0.0.1:

```
route add -host 1.0.0.1 gw 10.0.232.25
```

Подготовка скриптов для Клиента управления и CSP VPN Gate

1. Для установки 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 106).

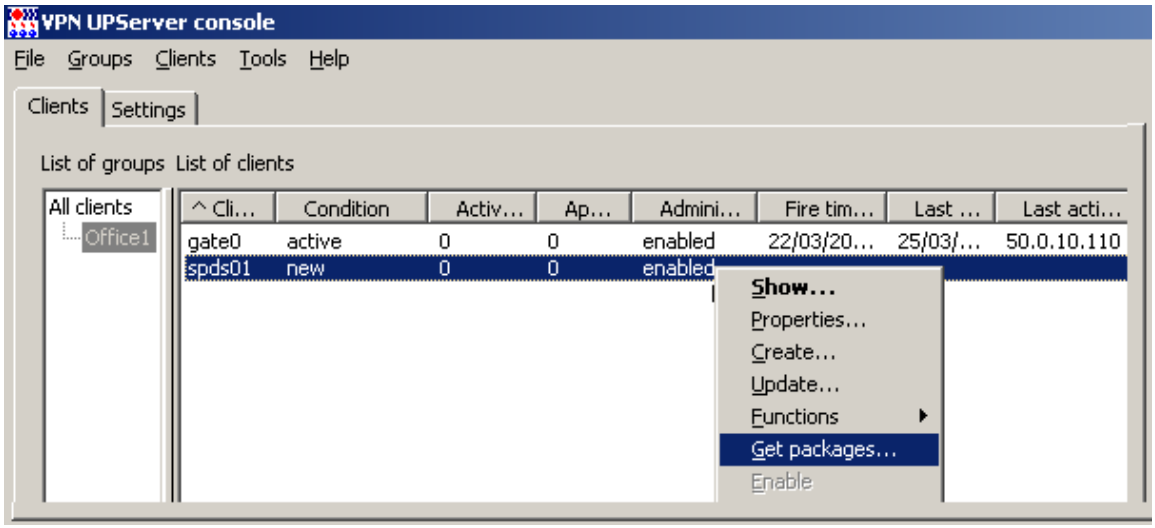


Рисунок 106

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

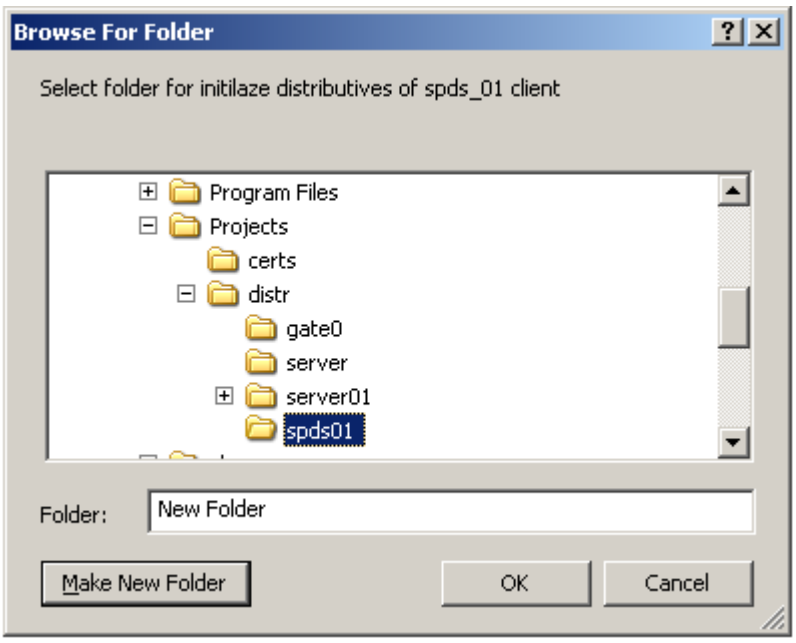


Рисунок 107

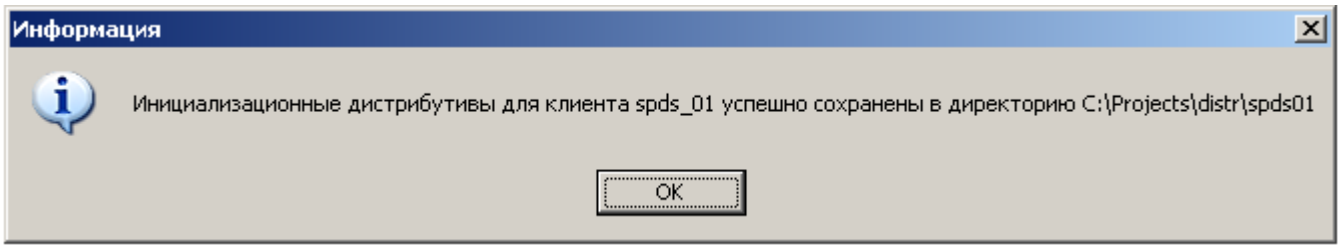


Рисунок 108

3. Два файла будут сохранены в указанный каталог (Рисунок 109):

   `setup_product.sh` – скрипт для инициализации продукта CSP VPN Gate

   `setup_upagent.sh` – скрипт, содержащий данные для Клиента управления.

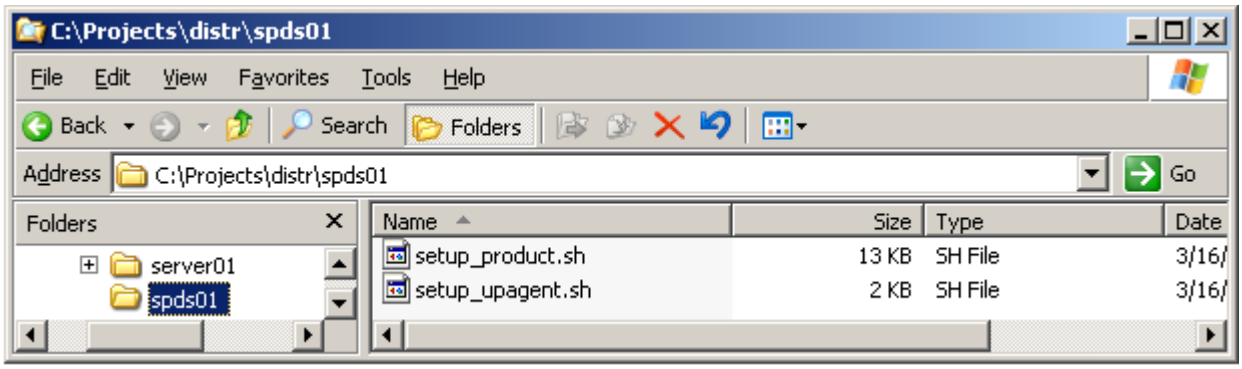


Рисунок 109

4. Созданные файлы скопируйте на СПДС «ПОСТ» в каталог `customization` (Рисунок 110). Можно было сразу сразу сохранить скрипты на СПДС «ПОСТ» (при запуске эти скрипты будут удалены из каталога `customization`).

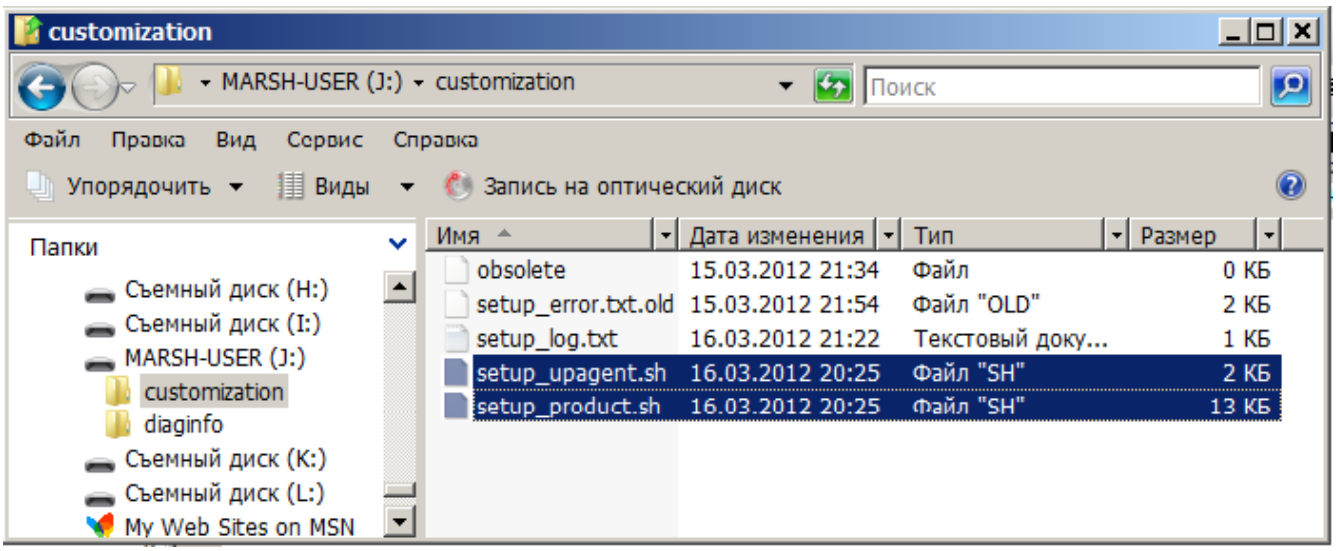


Рисунок 110

5. Закройте сессию с СПДС «ПОСТ», нажав кнопку «Закрыть сессию» в Редакторе СПДС.

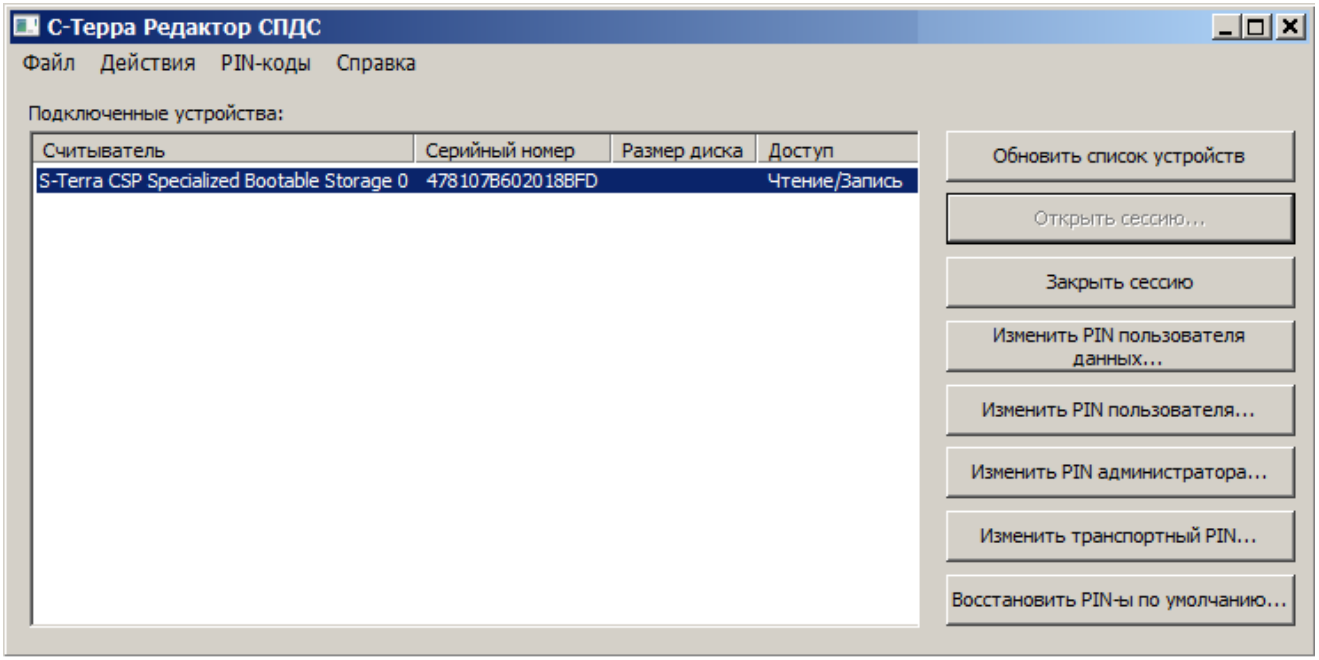


Рисунок 111

6. Закройте приложение и выньте СПДС «ПОСТ» из USB-разъема Сервера управления.

Note

Для СПДС «ПОСТ» администратор должен подготовить и положить на него контейнер с ключевой парой и два скрипта.

Инициализация СПДС «ПОСТ»

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. Затем осуществляется проверка целостности файлов на СПДС «ПОСТ».

```
Проверка целостности файлов:
```

6. Появляется заставка СПДС «ПОСТ».

Рисунок 112

7. Далее появляется окно **Choose application** (Рисунок 113) или (Рисунок 114) для выбора режима работы. Предлагается выбрать Режим клиента или Административный режим. При первом запуске выберите Административный режим.

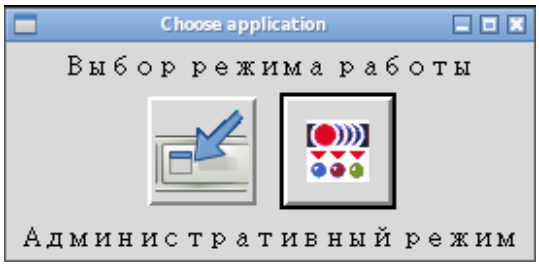


Рисунок 113

Рисунок 114

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 для него обновлений.
9. Получив нулевое обновление, Клиент управления загружает его и состояние клиента `spds01` на Сервере управления меняется на `active`, он готов для принятия обновлений.

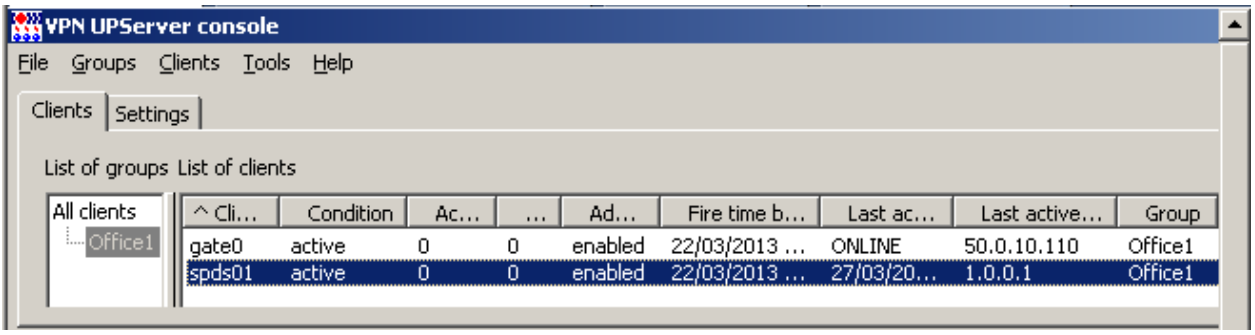


Рисунок 115

10. После работы СПДС «ПОСТ» в административном режиме компьютер всегда выключается и СПДС «ПОСТ» готов для эксплуатации пользователем.

Замечание

При первом запуске СПДС «ПОСТ» можно выбрать режим Клиента RDP, но в этом случае сразу устанавливается соединение с RDP-сервером. Клиент управления не устанавливает соединение с Сервером управления, не получает от него нулевое обновление и учетная запись на Сервере управления для данного СПДС «ПОСТ» остается в состоянии waiting.

Эксплуатация СПДС «ПОСТ» пользователем

1. Администратор передает устройство СПДС «ПОСТ» пользователю, который вставляет его в терминальное устройство или свой компьютер, который настроен для загрузки с СПДС «ПОСТ».
2. При загрузке с СПДС «ПОСТ» появятся следующие предложения:

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

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

```
Проверка целостности файлов:
```

5. После загрузки появляется большая заставка (Рисунок 112), а затем предлагается выбрать режим работы. Выберите Режим клиента, например, Клиент RDP.

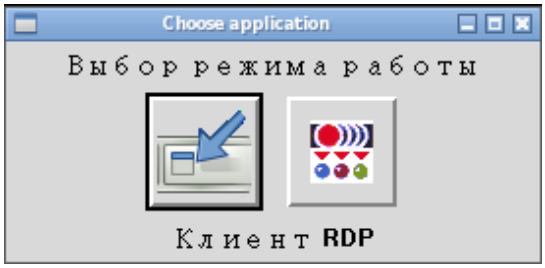


Рисунок 116

6. Далее осуществляется защищенный доступ к удаленному серверу в соответствии с заданными настройками, для нашего стенда - это RDP-сервер. Для аутентификации на RDP-сервере введите имя и пароль пользователя.
7. В соответствии с регламентом для работы данного пользователя на RDP-сервере будут доступны соответствующие папки и приложения (Рисунок 117).

Рисунок 117

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

Отображение текущего статуса СПДС «ПОСТ»

Текущий статус СПДС «ПОСТ» отображает иконка, расположенная в панели задач справа.

Если пользователь аутентифицировался, но СПДС «ПОСТ» не имеет защищенного соединения – иконка принимает вид:

Рисунок 118

Если пользователь аутентифицировался и СПДС «ПОСТ» имеет защищенное соединение, то на иконке изменяется цвет "монитора" с синего на бирюзовый.

Рисунок 119

При наведение курсора мыши на иконку всплывает информация о статусе СПДС «ПОСТ». Слева расположена иконка сетевого соединения. При наведении на нее курсора мыши всплывает информация о существующем сетевом соединении.

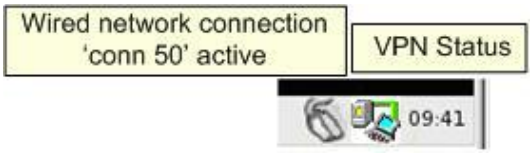


Рисунок 120

При отсутствии сетевого соединения иконки приобретают вид.

Рисунок 121

Нажатие правой кнопки мыши на иконке сетевого соединения вызывает меню для изменения сетевого соединения, получения информации о соединении или выборе сети.

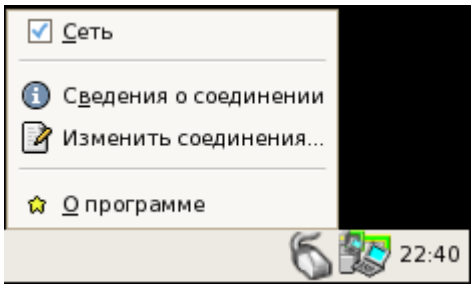


Рисунок 122

Завершение работы с СПДС «ПОСТ»

1. По окончании работы с СПДС «ПОСТ» в левом нижнем углу экрана наведите мышь на иконку с экраном дисплея.
2. В выпадающем меню выберите предложение «Завершение работы».

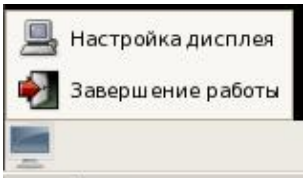


Рисунок 123

3. Появляется окно с запросом подтверждения на завершение работы с СПДС. При отрицательном ответе работу с СПДС «ПОСТ» можно продолжить. При утвердительном ответе защищенное соединение с RDP-сервером закрывается, компьютер выключается.
4. После этого выньте СПДС «ПОСТ» из USB-разъема компьютера.

Получение обновлений

Получение обновлений для СПДС «ПОСТ» с Сервера управления осуществляется только в Административном режиме.

1. Завершите работу в Режиме клиента.
2. Загрузите компьютер с СПДС «ПОСТ» и перейдите в Административный режим.
3. Клиент управления скачает обновление, применит его и выключит компьютер.
4. Снова загрузите компьютер с СПДС «ПОСТ» и перейдите в Режиме клиента для продолжения работы.

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).

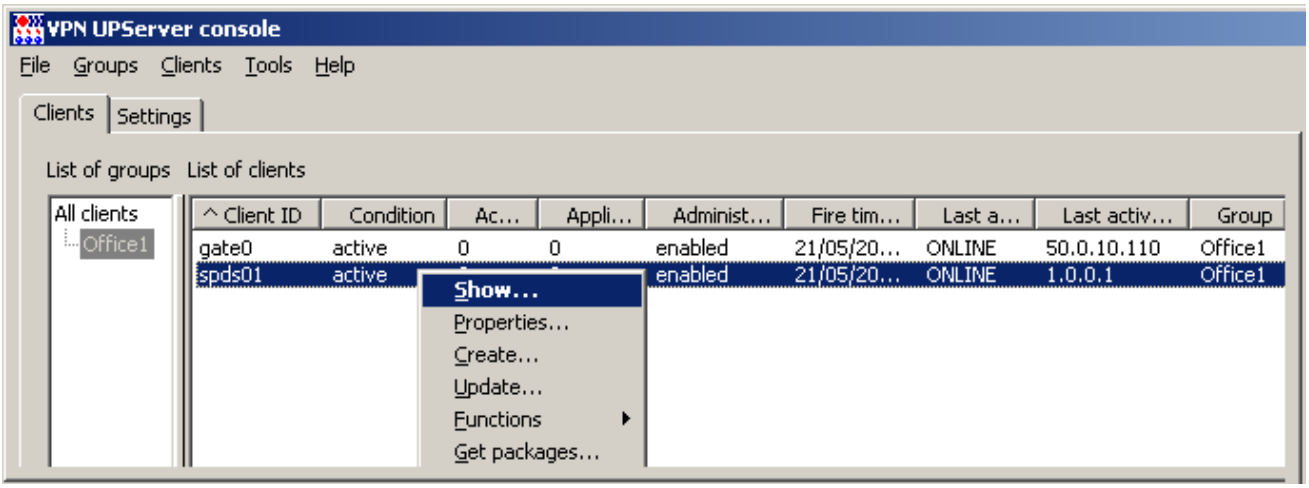


Рисунок 124

2. В результате будет выдано окно с разными вкладками (Рисунок 125), в которых отражена информация о проведенных обновлениях, настройках Клиента управления, действующей в данный момент политике безопасности на клиенте, используемых сертификатах, об интерфейсах клиента, таблице маршрутизации и т.п.
3. Во вкладке **UPLog** ведется лог событий по обновлению клиента.

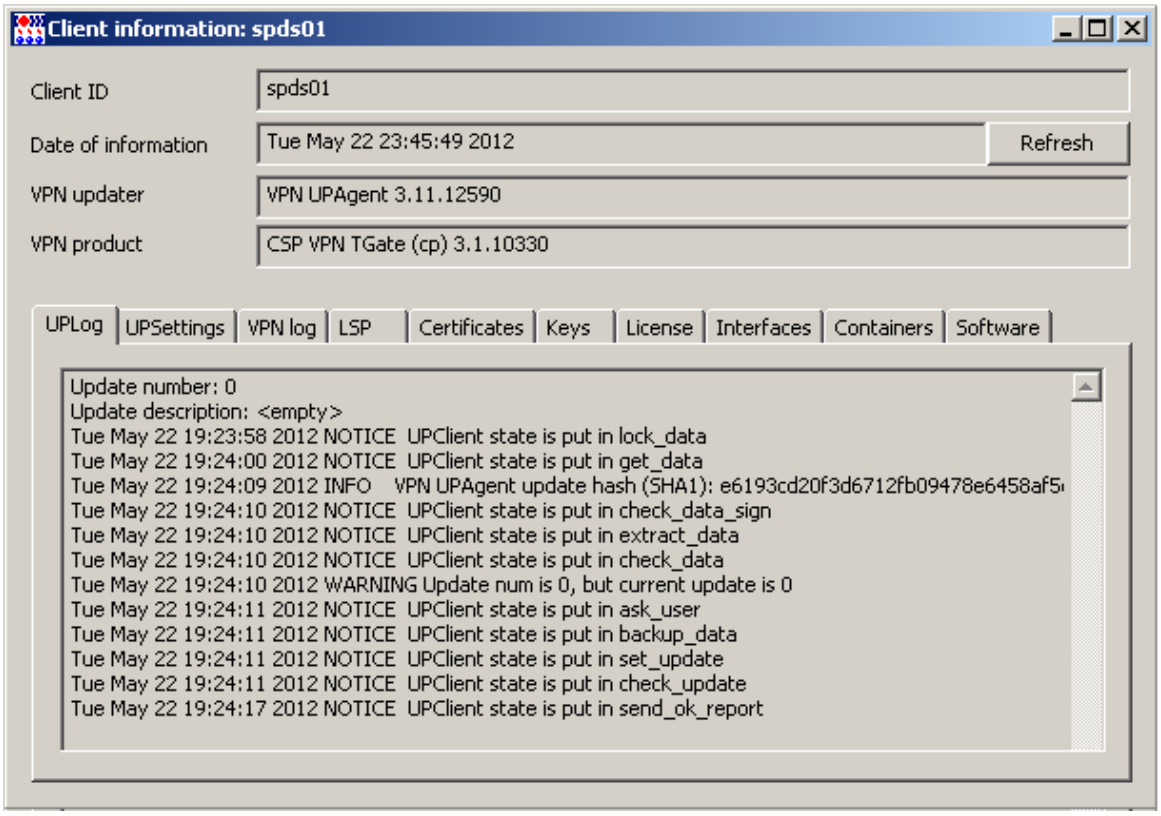


Рисунок 125

4. Во вкладке **UPSettings** (Рисунок 126) отражены настройки Клиента управления. Описание этих настроек дано в главе «Настройки Клиента управления».

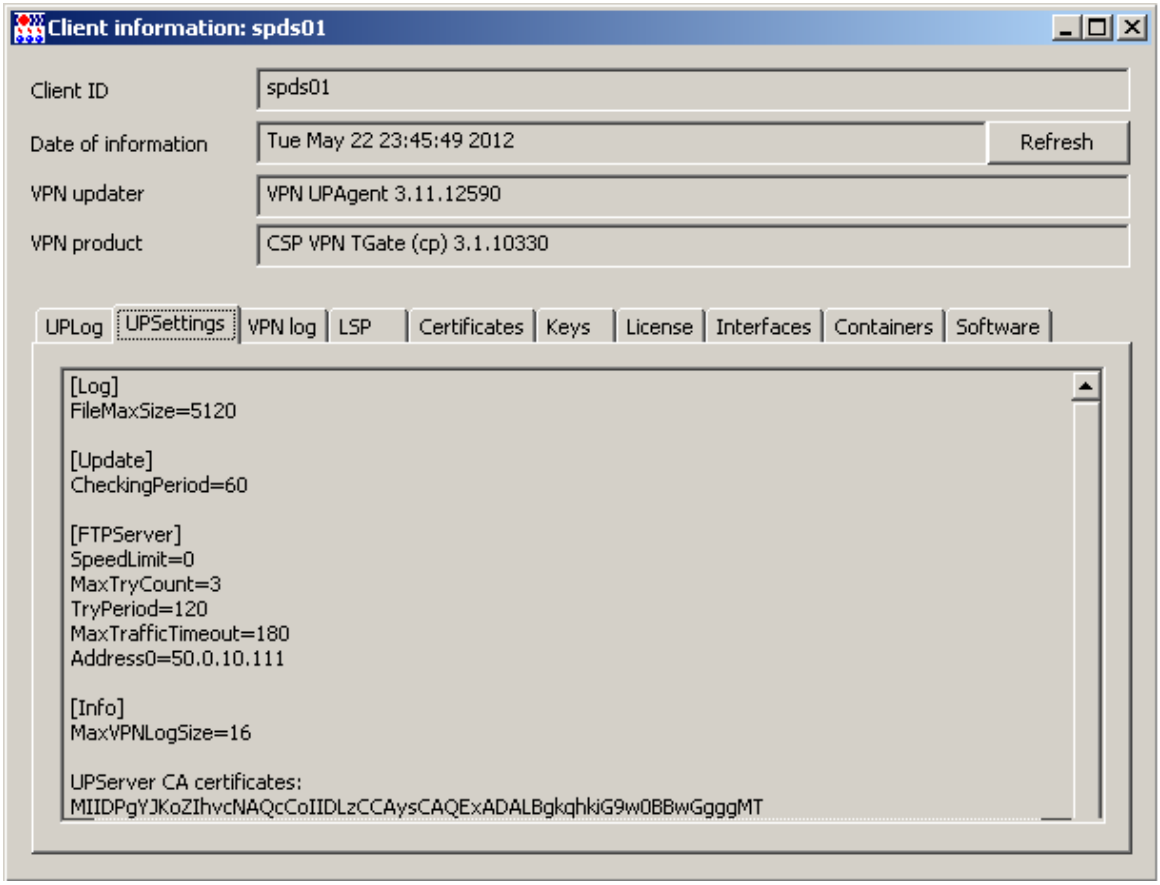


Рисунок 126

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

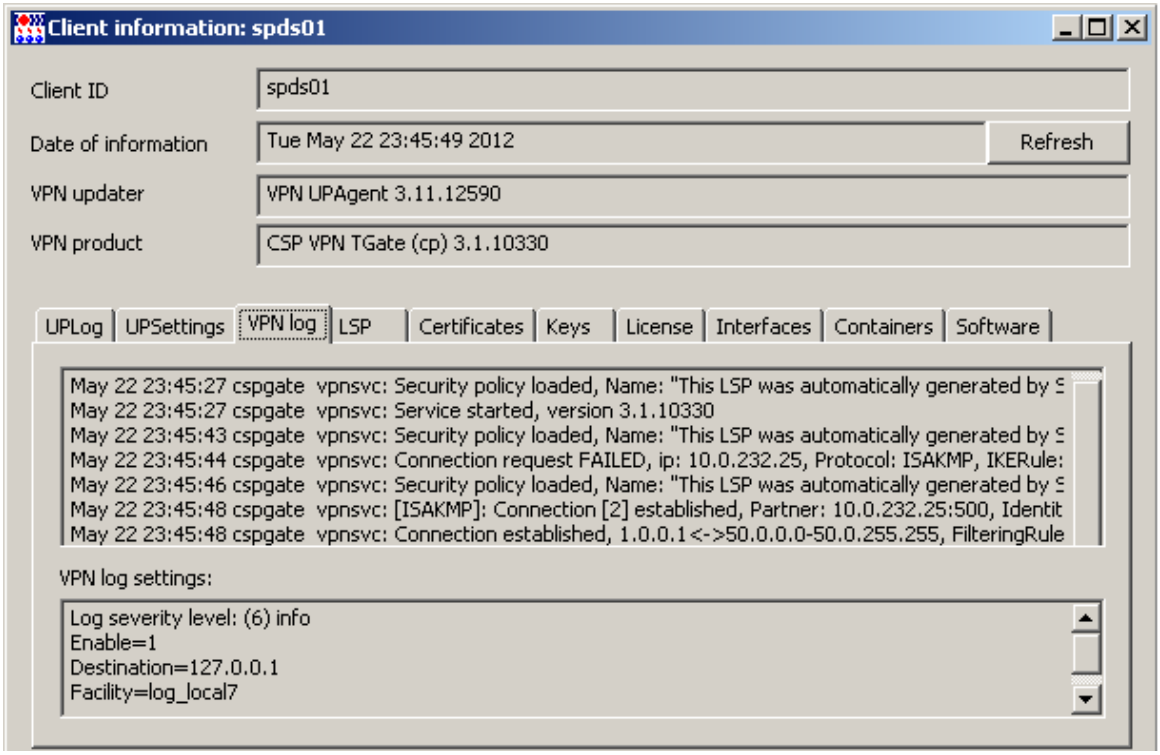


Рисунок 127

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 128).

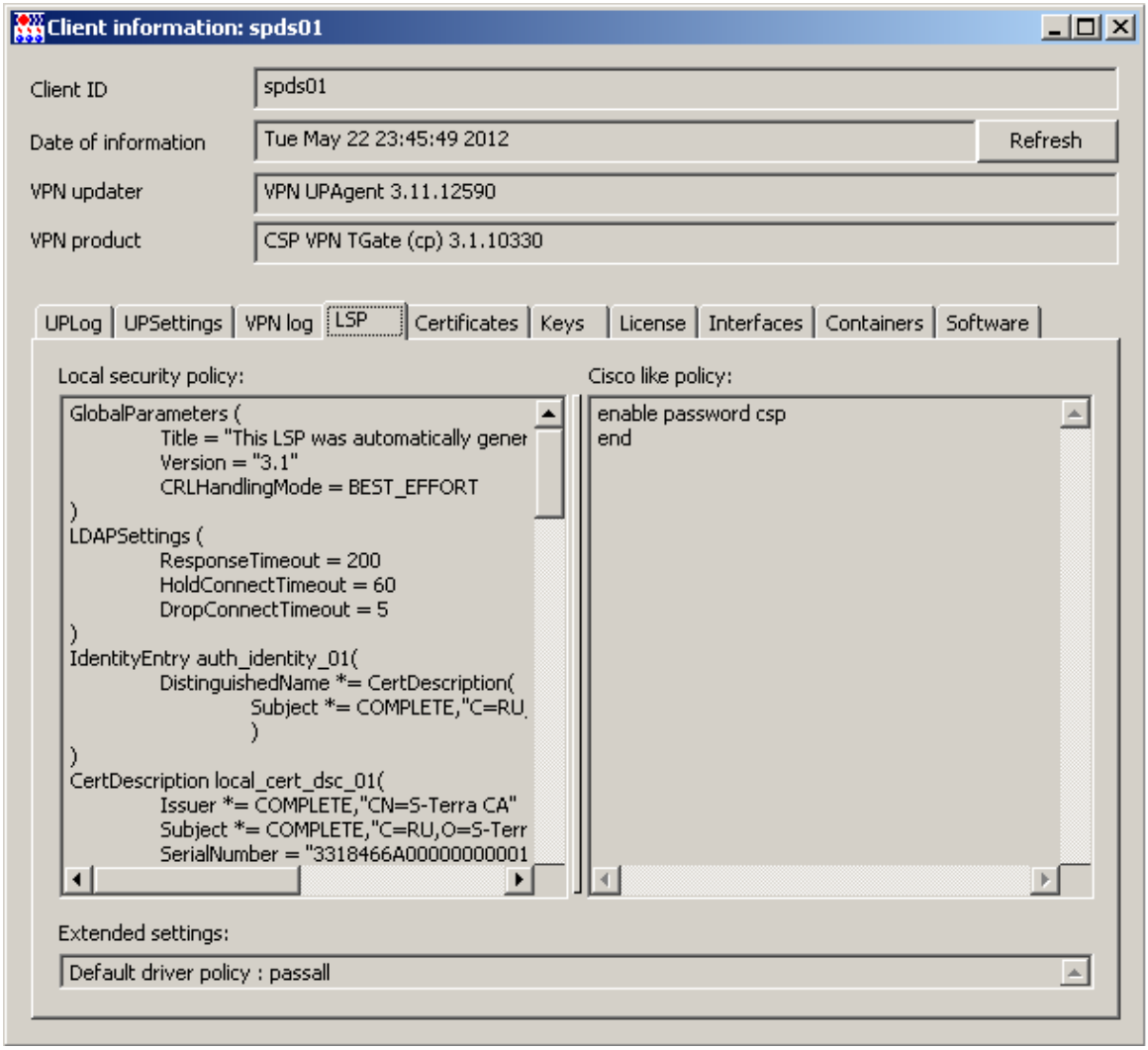


Рисунок 128

7. Вкладка **Keys** показывает только имена предопределенных ключей, не выдавая их значений. При работе с СПДС «ПОСТ» ключи не используются.

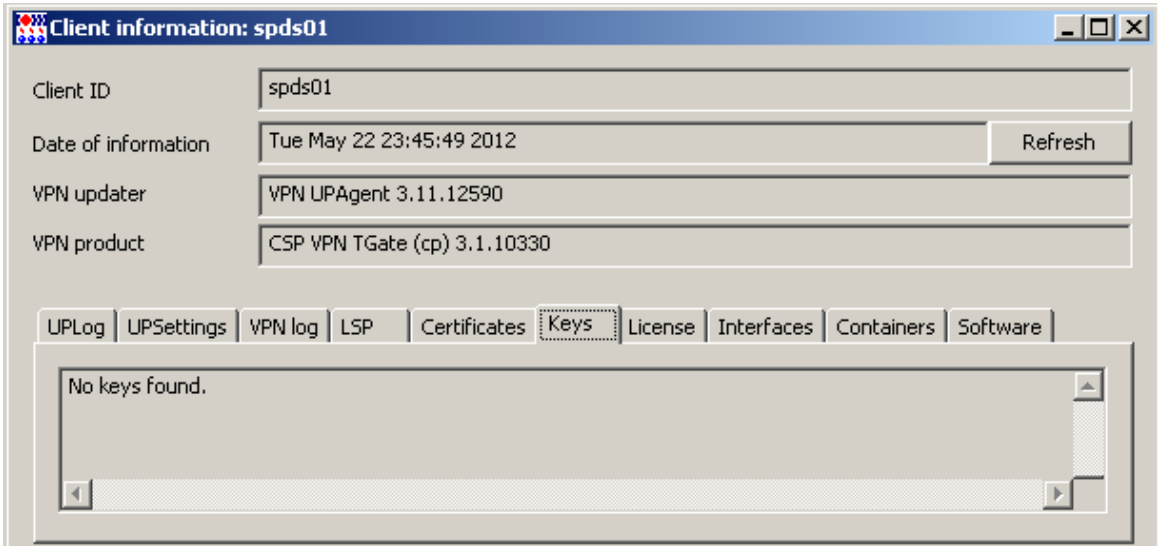


Рисунок 129

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

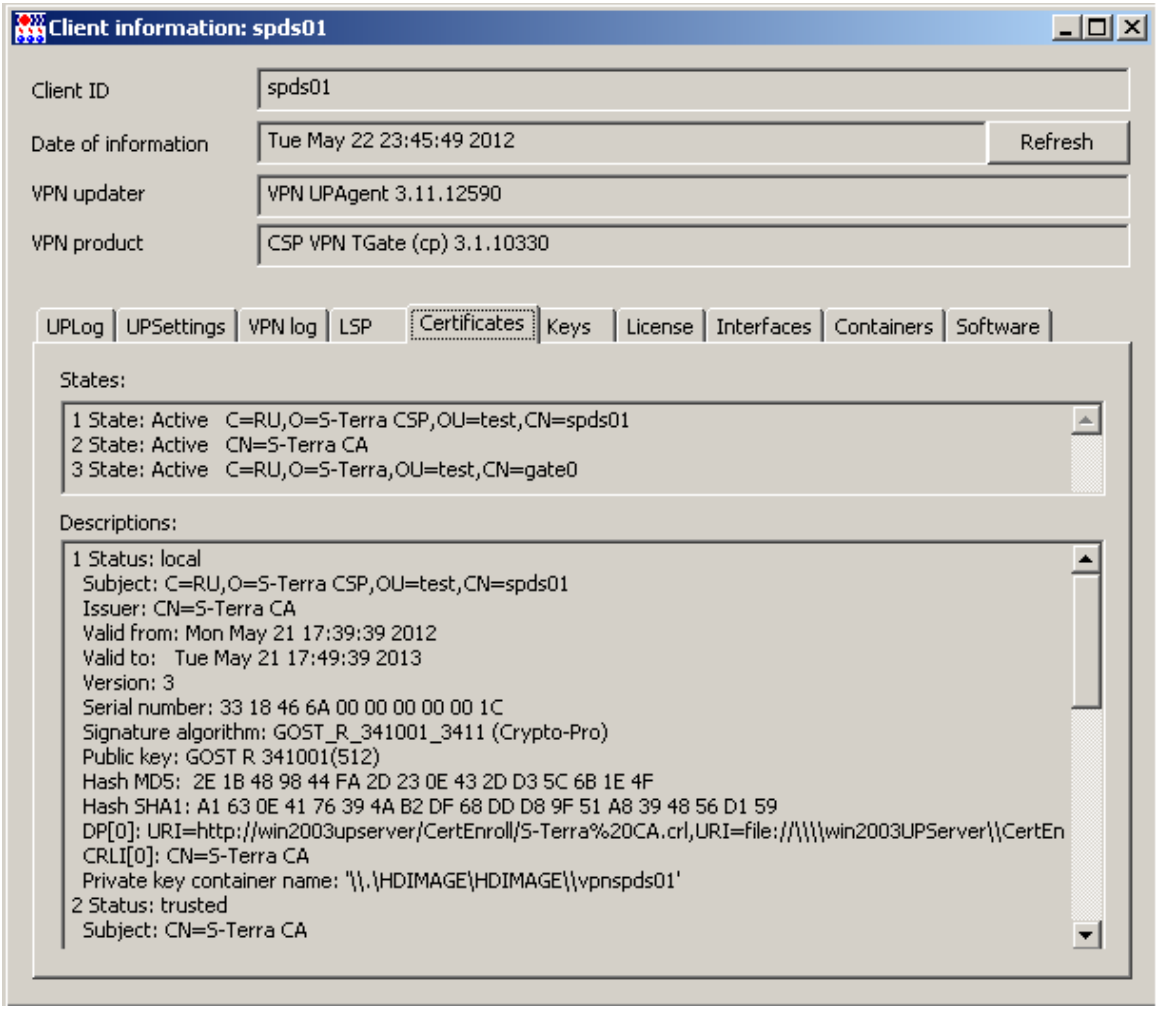


Рисунок 130

9. Во вкладке **License** отражена информация о Лицензии на продукт CSP VPN Gate и КриптоПро CSP.

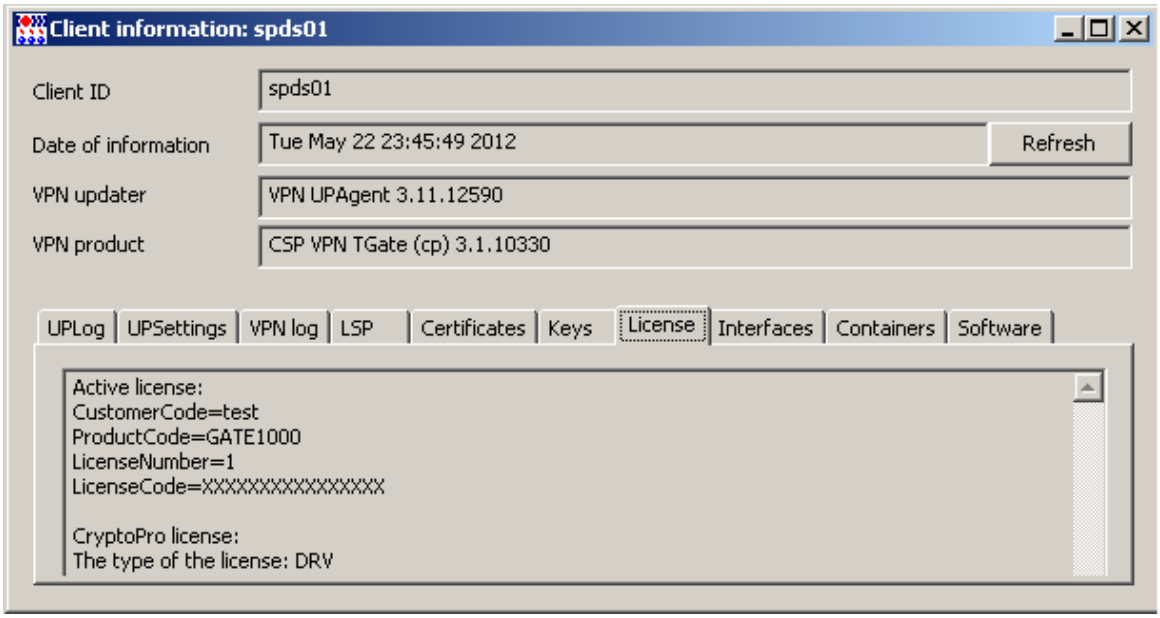


Рисунок 131

10. Вкладка **Interfaces** содержит информацию обо всех сетевых интерфейсах управляемого устройства, таблицу маршрутизации, а раздел ***Driver settings*** показывает настройки IPsec-драйвера.

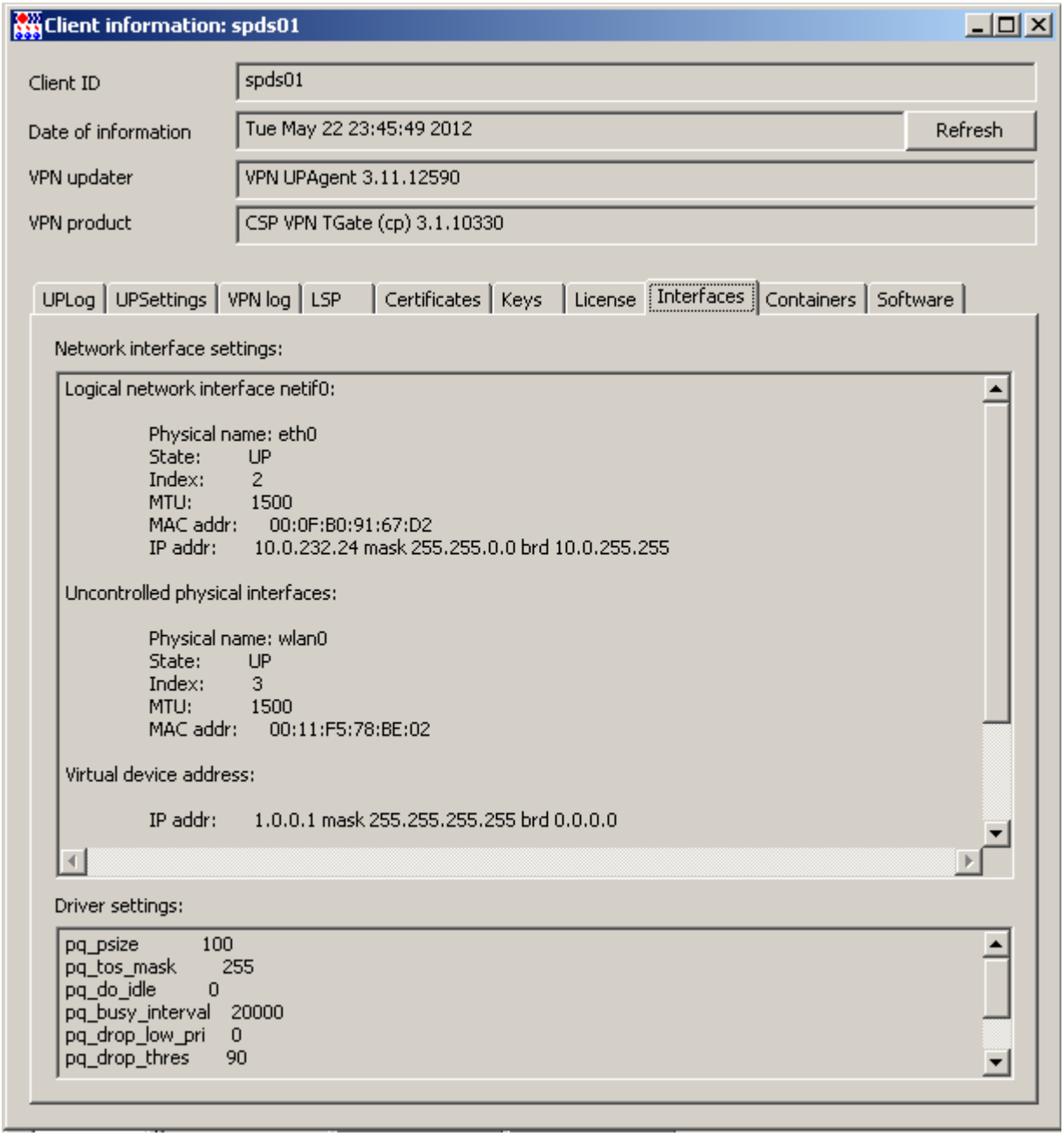


Рисунок 132

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

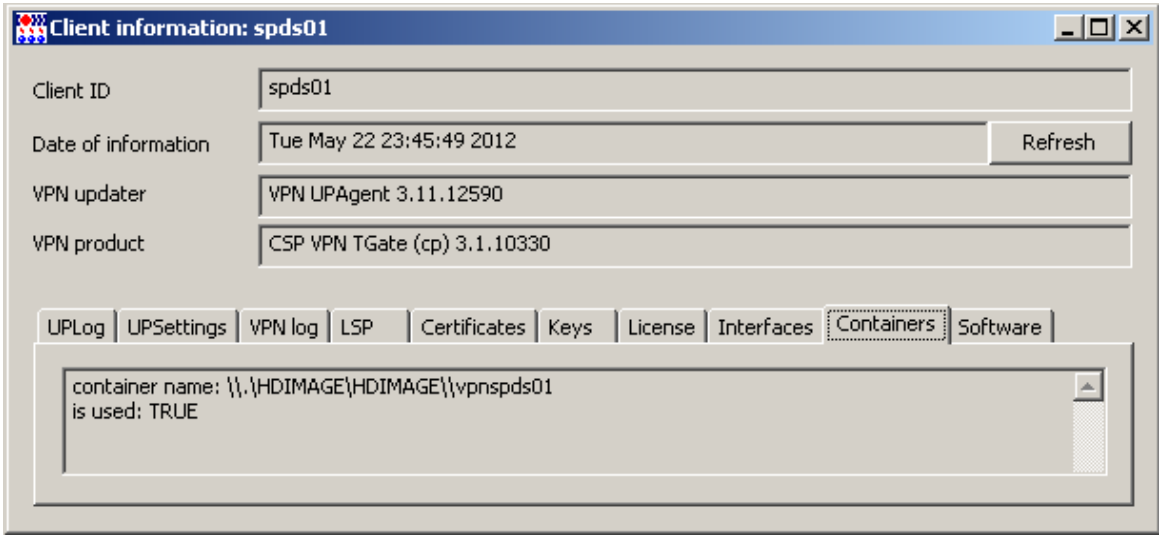


Рисунок 133

12. Вкладка **Software** показывает данные, введенные администратором для доступа к удаленному серверу.

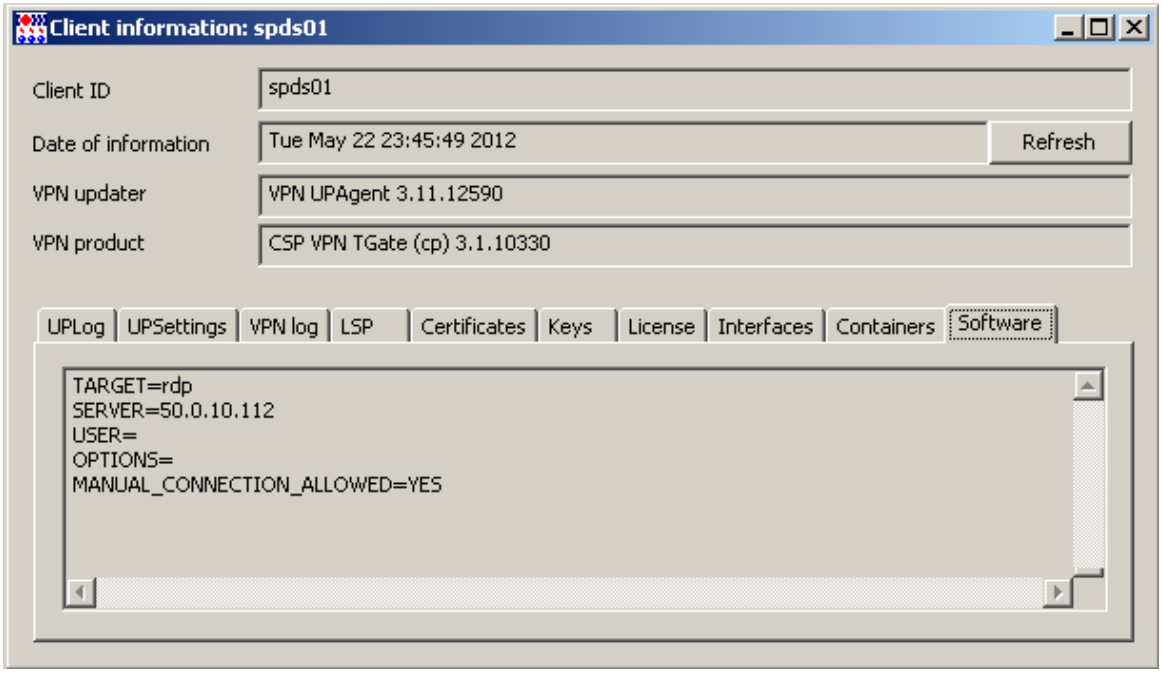


Рисунок 134

Сценарий неудачного обновления клиента

1. Для проверки неудачного обновления клиента укажите неверный адрес Сервера управления в настройках Клиента управления. Для этого во вкладе **Settings** измените, например, адрес 50.0.10.111 на адрес 50.0.10.112 и нажмите кнопку Save (Рисунок 135).

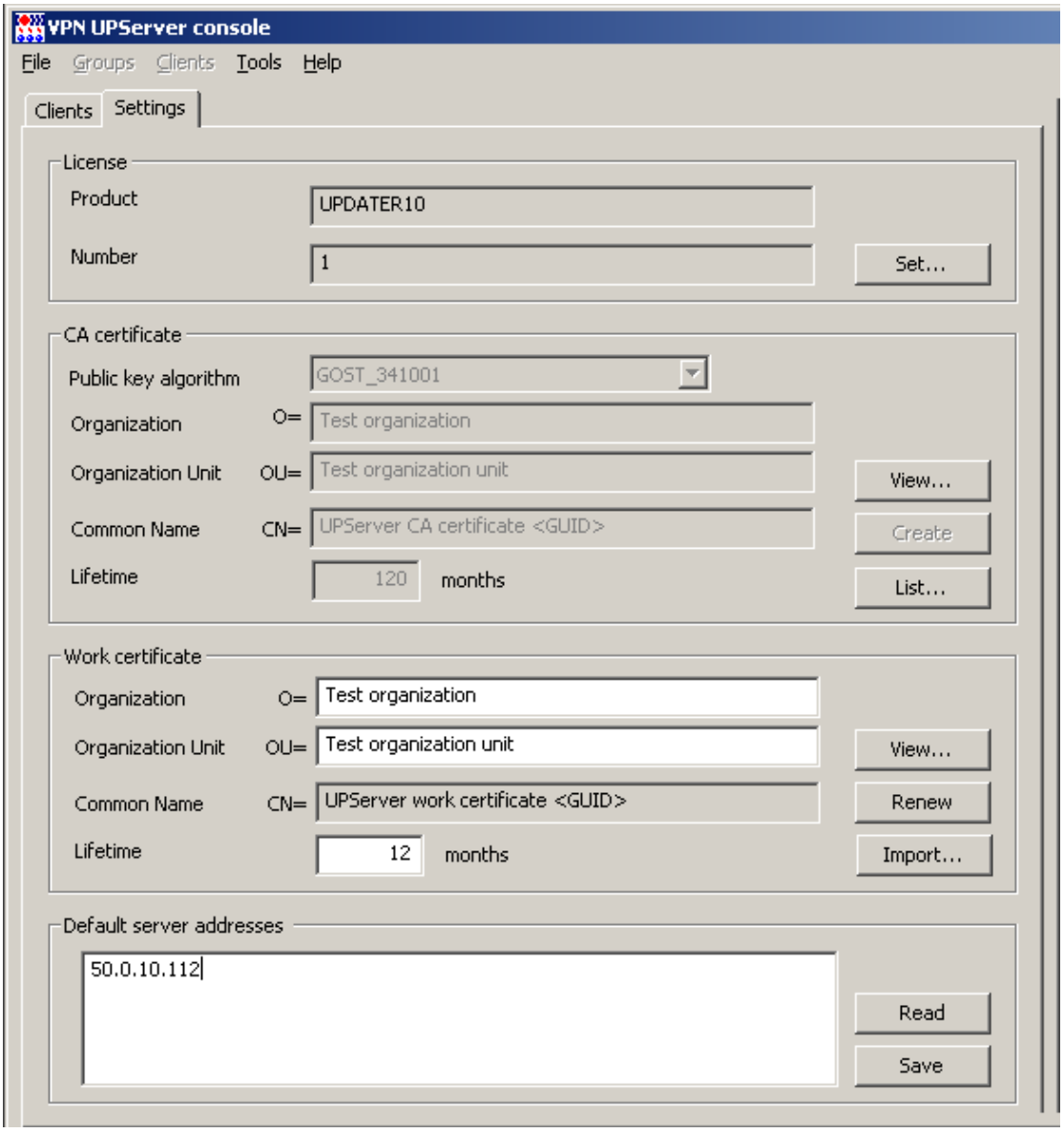


Рисунок 135

2. В окне **Предупреждение** нажмите кнопку OK (Рисунок 136).

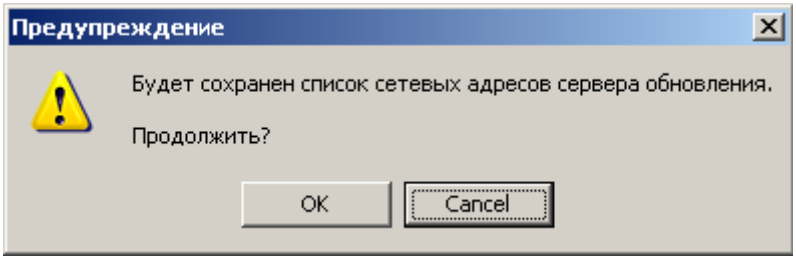


Рисунок 136

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

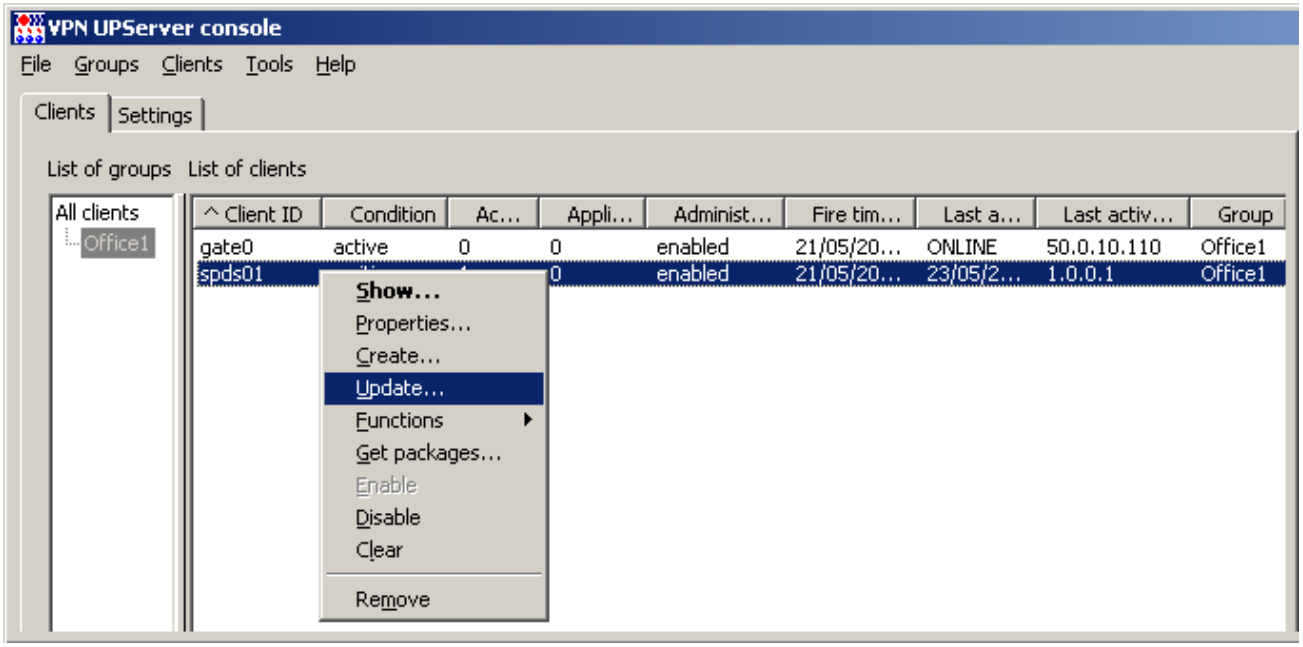


Рисунок 137

4. В открывшемся окне **Update client** (Рисунок 138) задайте файл настроек Клиента управления, 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".`

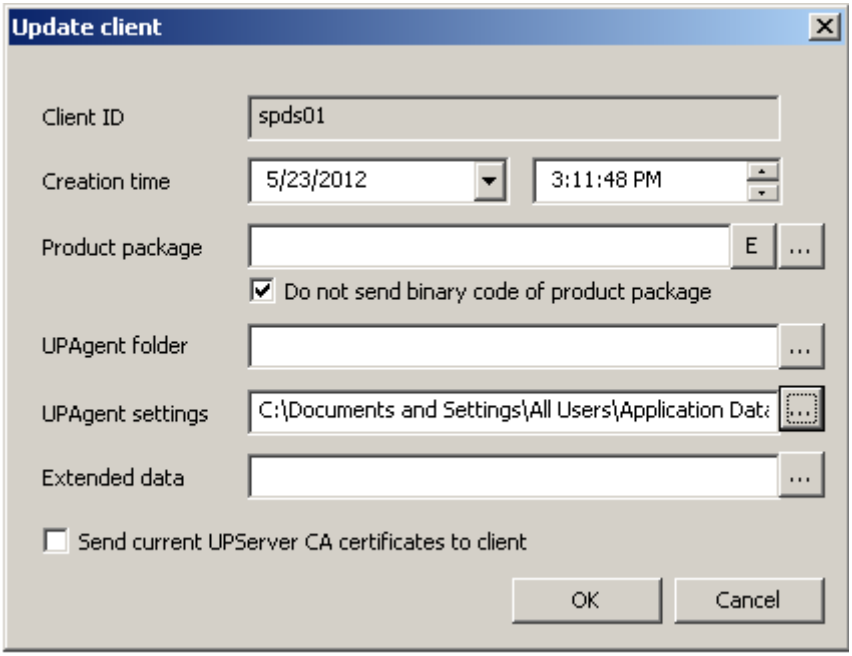


Рисунок 138

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

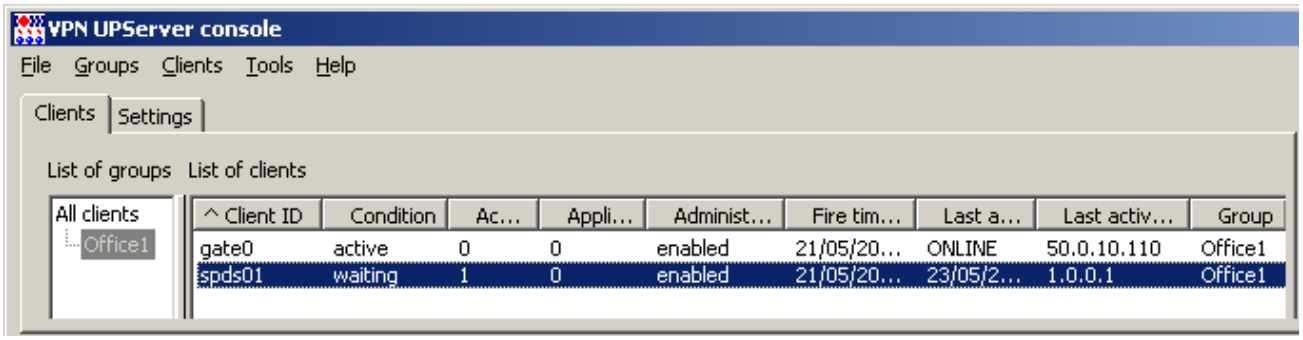


Рисунок 139

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

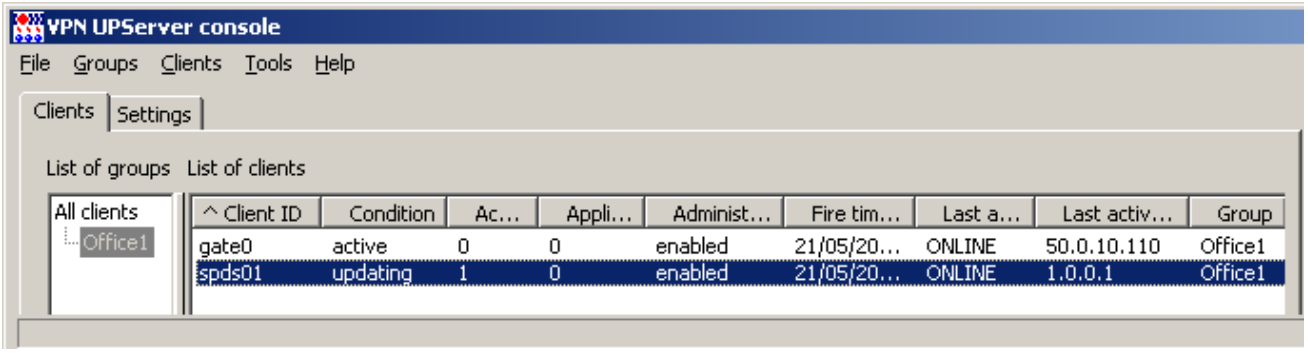


Рисунок 140

7. По истечении некоторого времени (если настройки по умолчанию не менялись, то примерно через 6 минут) состояние изменится с **updating** на **failed** （Рисунок 141）.

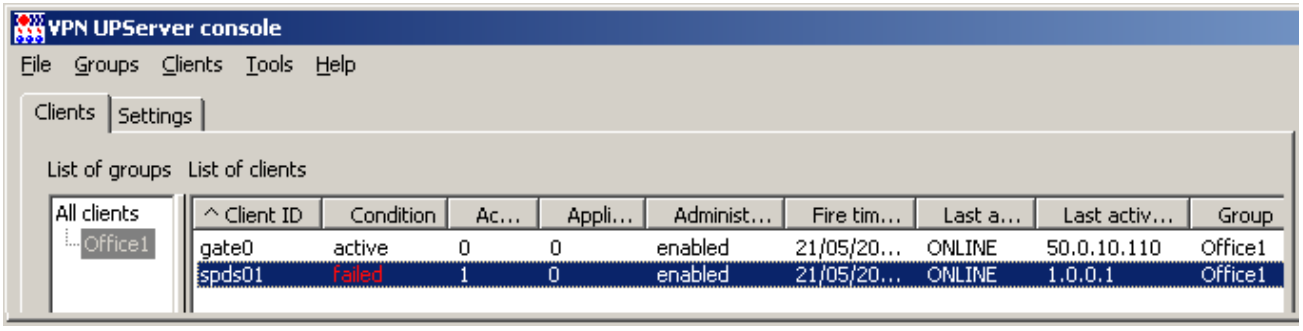


Рисунок 141

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 – (Рисунок 142)), и во вкладке **UPLog** - лог операции обновления (Рисунок 143).

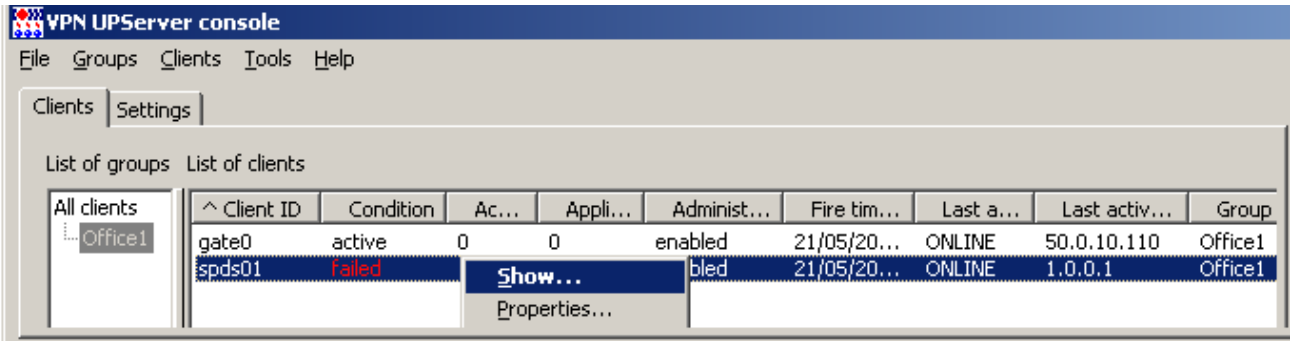


Рисунок 142

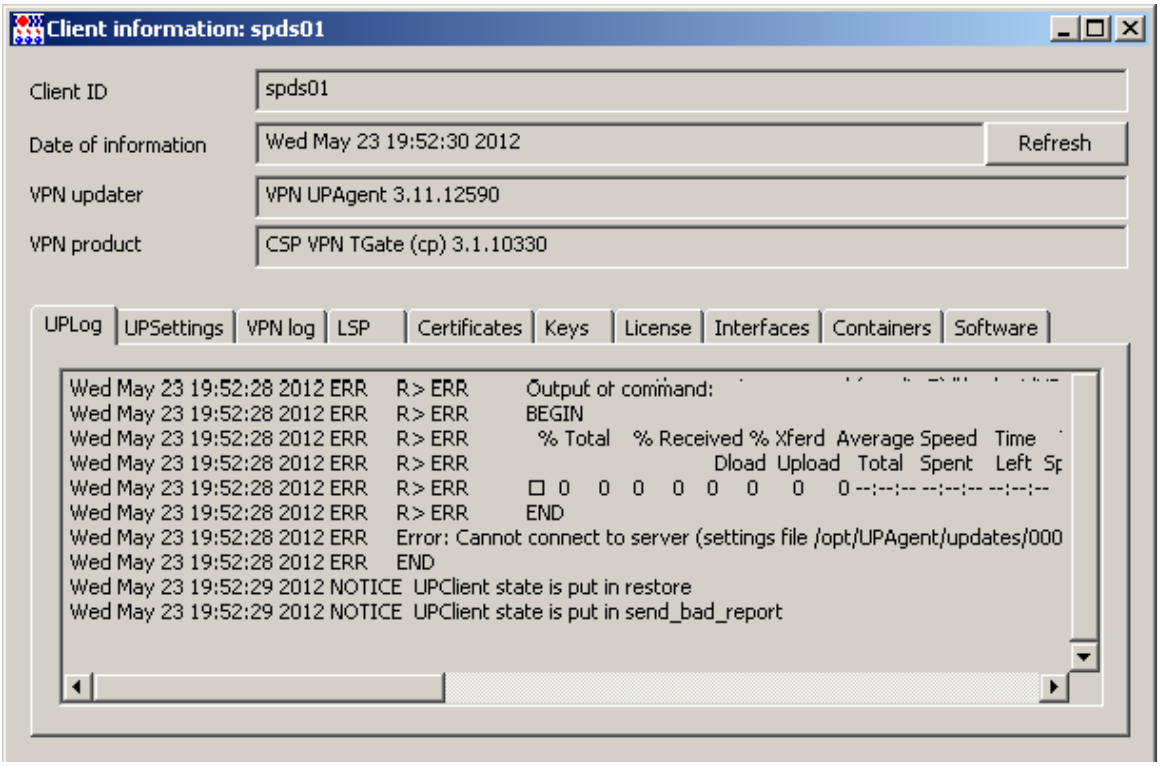


Рисунок 143

9. Для отмены неудачного обновления для данного клиента в контекстном меню выберите предложение ***Clear*** (Рисунок 144).

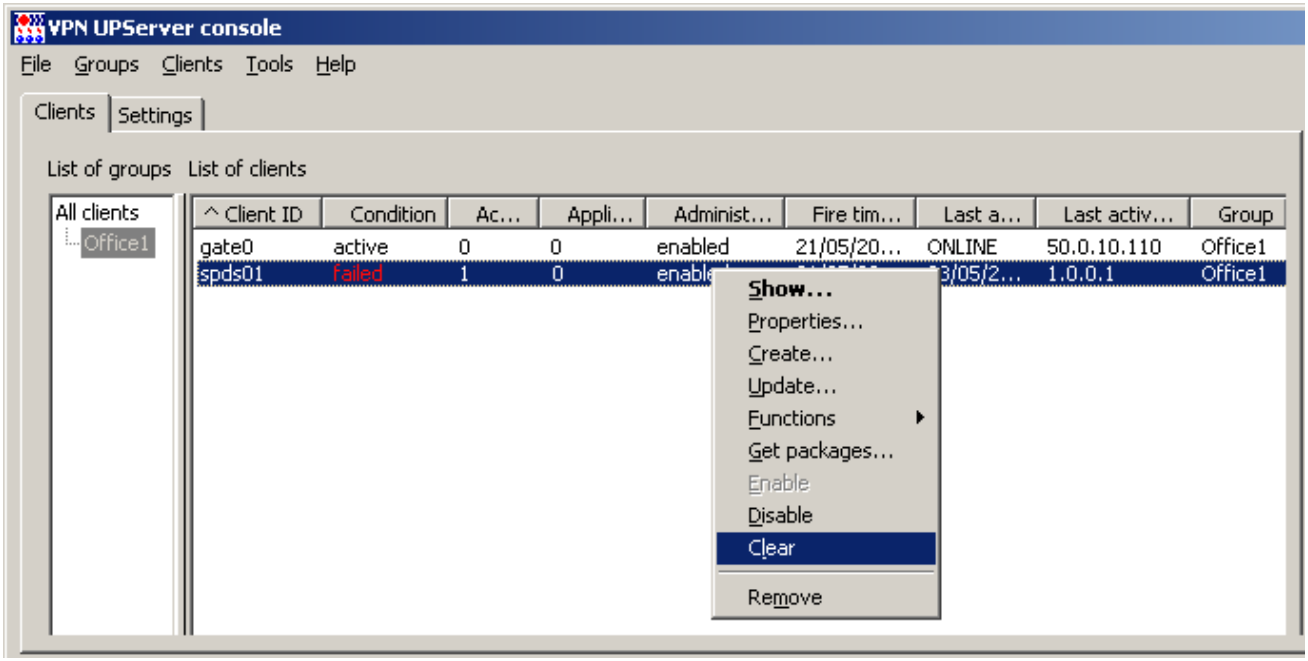


Рисунок 144

10. Выдается предупреждение с просьбой подтвердить удаление всех не примененных обновлений. Нажмите кнопку OK (Рисунок 145).

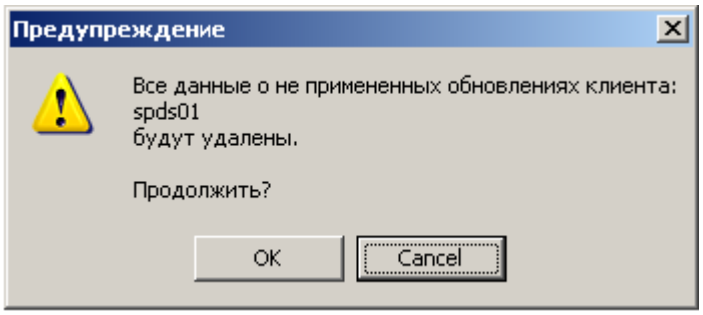


Рисунок 145

11. После этого количество активных обновлений станет равным нулю и через некоторое время состояние изменится с **failed** на **active** (Рисунок 146). В этом состоянии клиент готов для последующих обновлений.

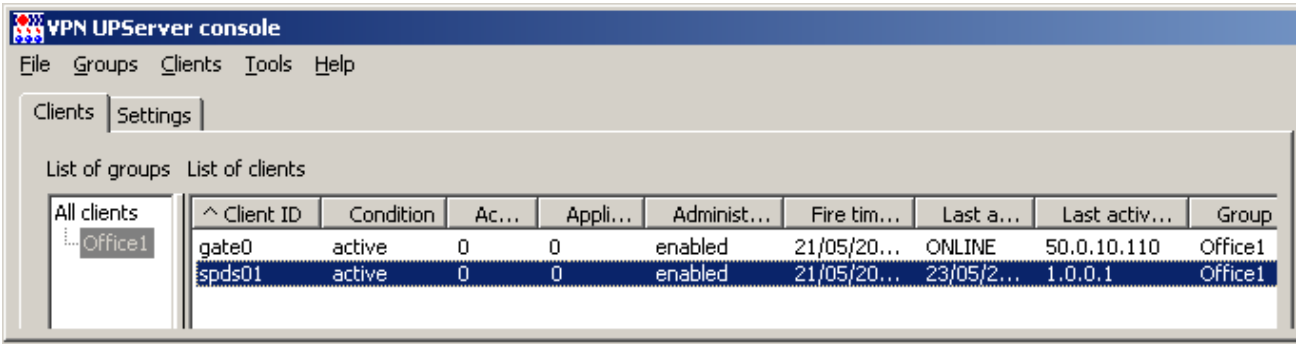


Рисунок 146

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

Сценарий обновления сертификатов на устройствах

Сценарий перехода на новый локальный сертификат на управляемом устройстве 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 этот контейнер
2. Клиент управления скачает подготовленное обновление и на управляемом устройстве будет создана ключевая пара и запрос на сертификат
3. на Сервере управления появится новая информация о клиенте - создан контейнер с ключевой парой и запрос на сертификат. Скопируйте запрос с Сервера управления и отправьте в Удостоверяющий Центр, а затем получите локальный сертификат для клиента
4. на Сервере управления подготовьте обновление, включающее новый локальный сертификат, СА сертификат и подкорректированную политику безопасности для данного клиента, если необходимо
5. Клиент управления скачает новое обновление и применит его.

В данном сценарии все действия по обновлению сертификатов на устройствах осуществляются удаленно.

Создание обновления с параметрами ключевой пары и запроса на сертификат

1. На Сервере управления сразу для двух устройств создайте обновления - создание ключевой пары и запроса на сертификат на этих устройствах. Поэтому выделите в таблице строки с клиентами и выберите предложение ***Functions – Key pairs – Generate*** (Рисунок 147).

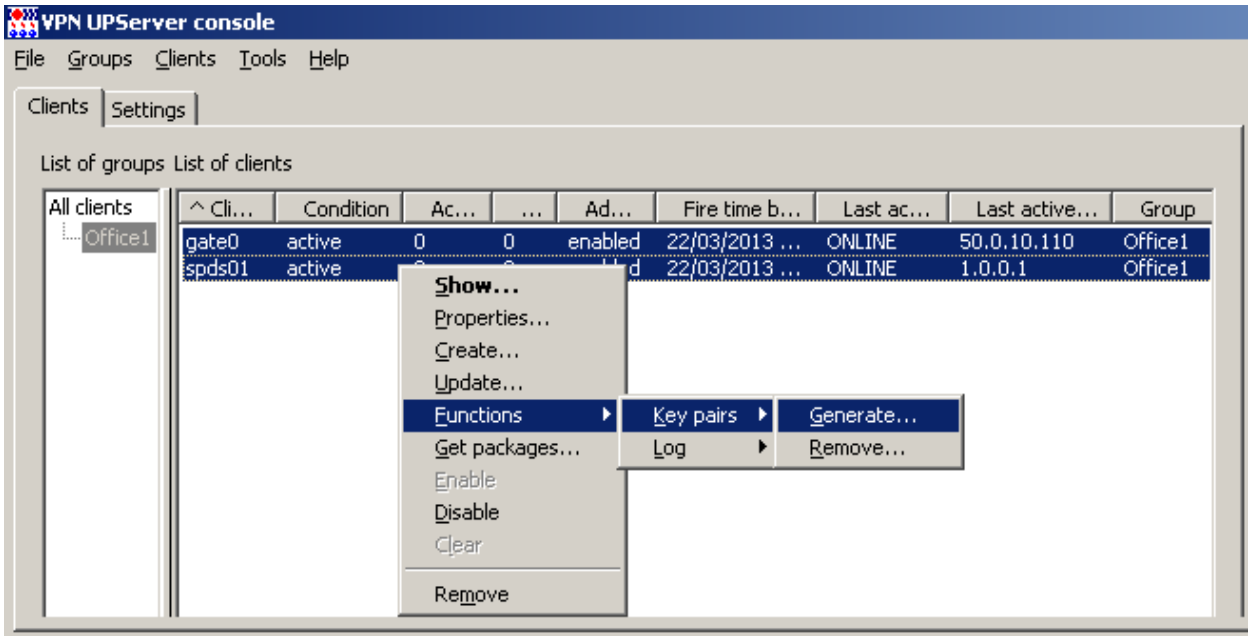


Рисунок 147

2. В открывшемся окне (Рисунок 148) заполните только два поля – задайте пароль на контейнер и его подтверждение, в который будет размещена ключевая пара для локального сертификата.

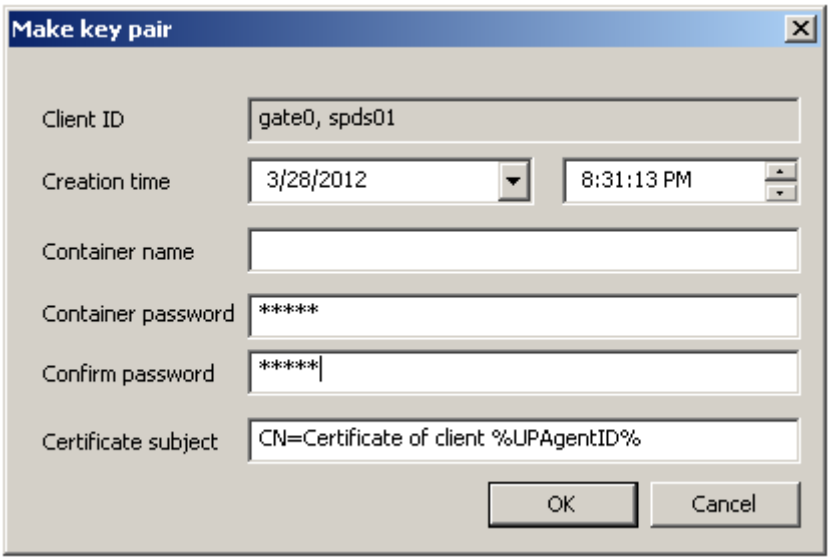


Рисунок 148

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

- **Creation time** – время, когда Сервер управления сделает доступным для клиента 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
- **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. Должен совпадать со значением Container password
- **Certificate subject** – строка, используемая в качестве поля Subject при создании запроса на сертификат. В этой строке можно использовать макросы, такие как %UPAgentID%, %UPAgentGroup% и т.п, которые будут заменены на их значения (список макросов, которые можно использовать, совпадает с переменными, передаваемыми в файл cook.bat при его запуске).

3. При нажатии кнопки OK предлагается выполнить «биологическую» инициализацию ДСЧ – понажимайте клавиши или перемещайте указатель мыши (Рисунок 149). Если на Сервере управления установлен аппаратный ДСЧ, то данное окно не выводится.

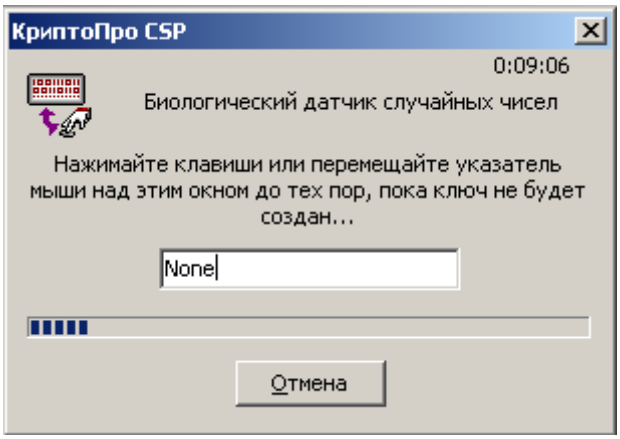


Рисунок 149

4. После этого в таблице появятся новые обновления с параметрами ключевых пар и контейнеров для данных клиентов (Рисунок 150). Количество активных обновлений (столбец Active updates) увеличится на единицу. На рисунке видно, что Клиент управления с

центрального шлюза скачал обновление и применил его – количество примененных обновлений увеличилось на единицу.

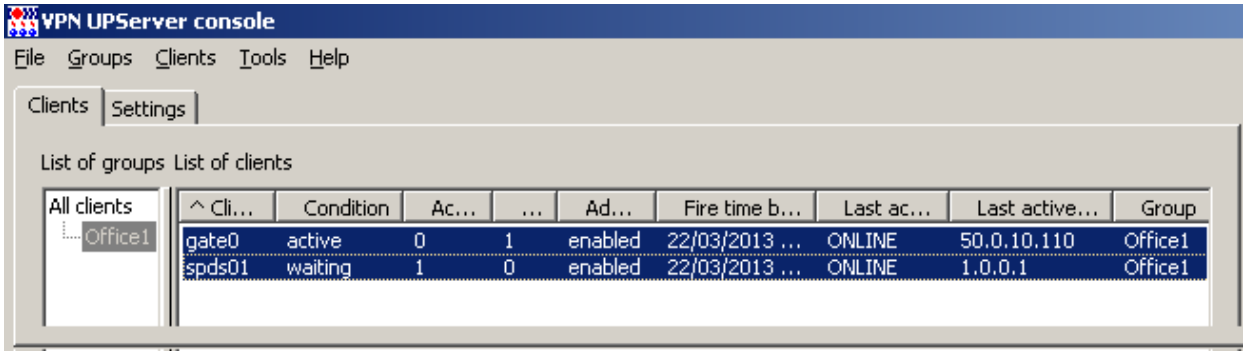


Рисунок 150

5. На СПДС «ПОСТ» для получения обновления перейдите в Административный режим.
6. Через некоторое время обновление на СПДС «ПОСТ» будет применено, что отразится в таблице на Сервере управления (Рисунок 151).

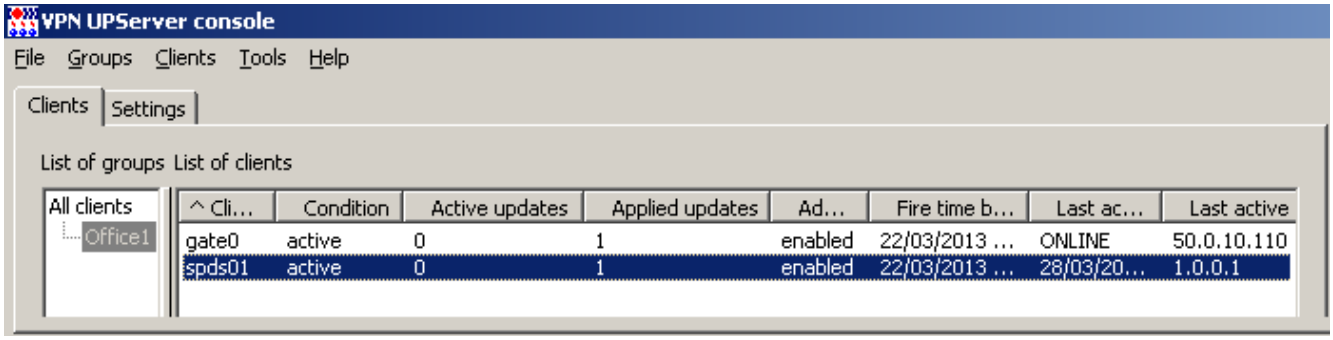


Рисунок 151

Создание на клиенте ключевой пары и запроса на сертификат

В результате обновлений на каждом устройстве будет создан контейнер с ключевой парой и запрос на локальный сертификат, которые можно увидеть на Сервере управления.

1. Для выделенного клиента в контекстном меню выберите предложение ***Show***.

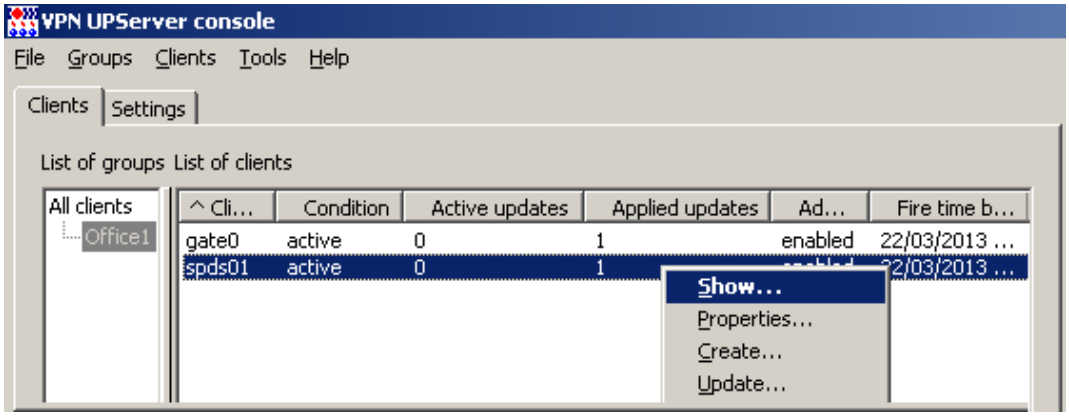


Рисунок 152

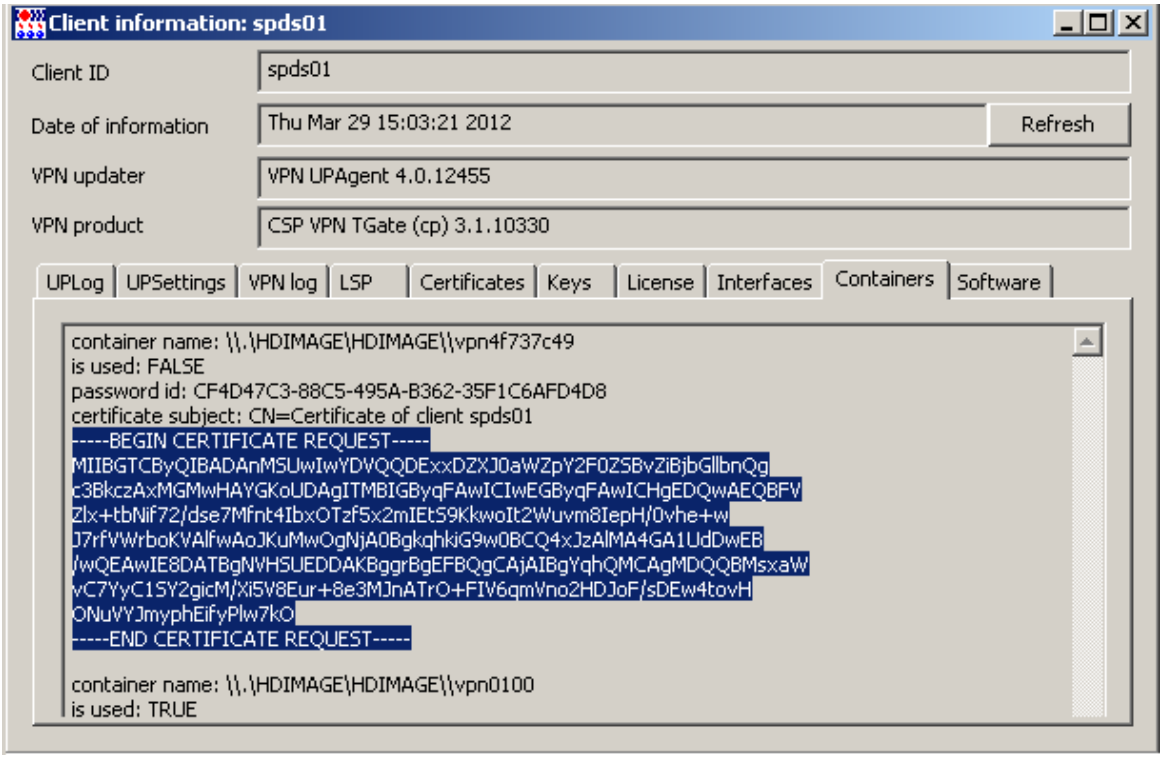


Рисунок 153

2. Во вкладке **Containers** для выделенного клиента появилась запись о созданном контейнере:
   - **container name** – имя созданного контейнера на СПДС «ПОСТ»
   - **is used: FALSE** – признак того, что контейнер еще не используется продуктом CSP VPN Gate
   - **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.

Создание сертификата

1. Скопируйте из вкладки **Containers** запрос на сертификат и передайте его в УЦ, используя, например, средства Microsoft Windows CA, как было описано ранее (Рисунок 37). Выберите отправку запроса в формате PKCS#7 или PKCS#10 и вставьте в него запрос (Рисунок 154).

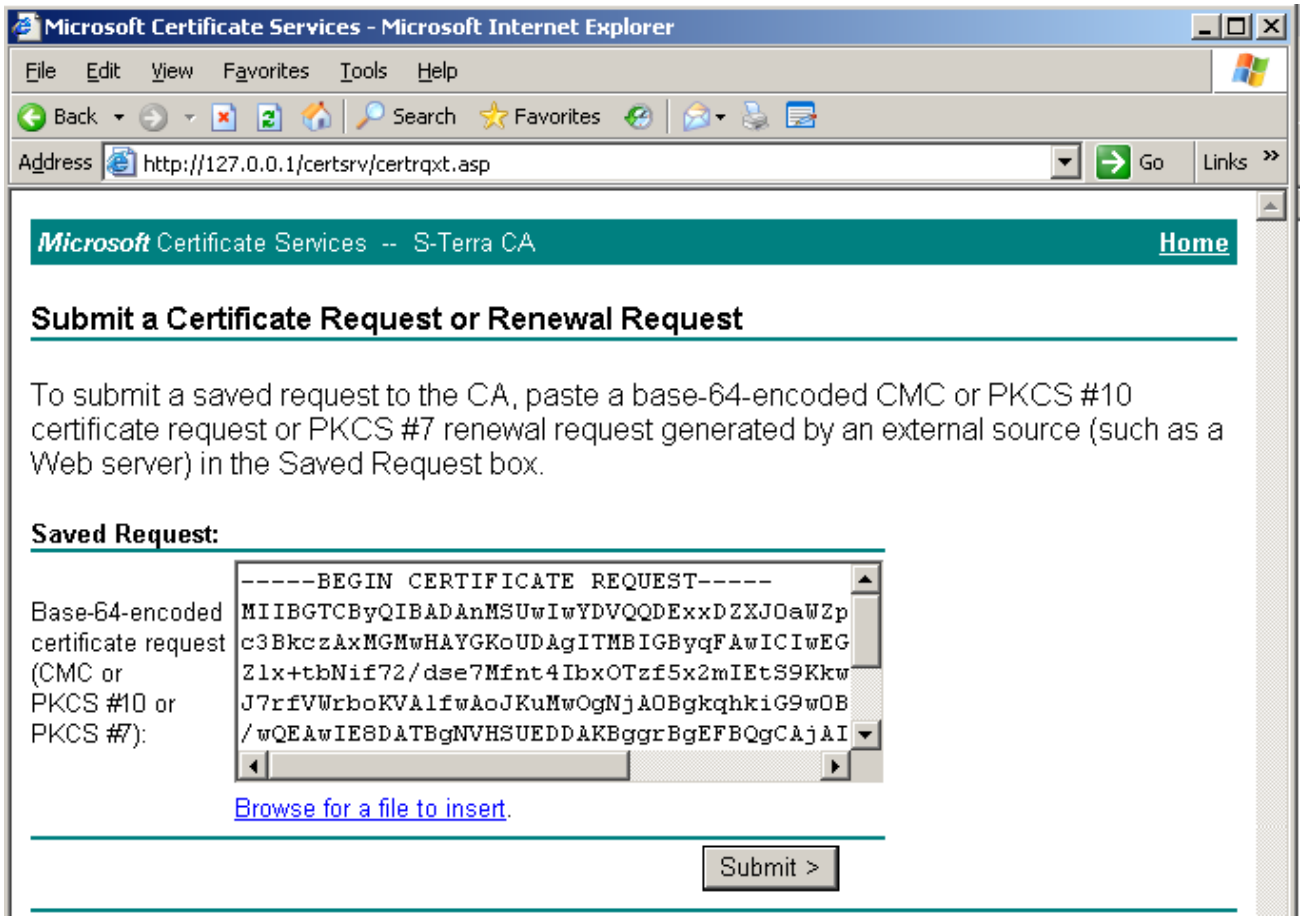


Рисунок 154

2. Созданный локальный сертификат для `spds01` сохраните на Сервере управления, выбрав ***Download certificate*** (Рисунок 155).

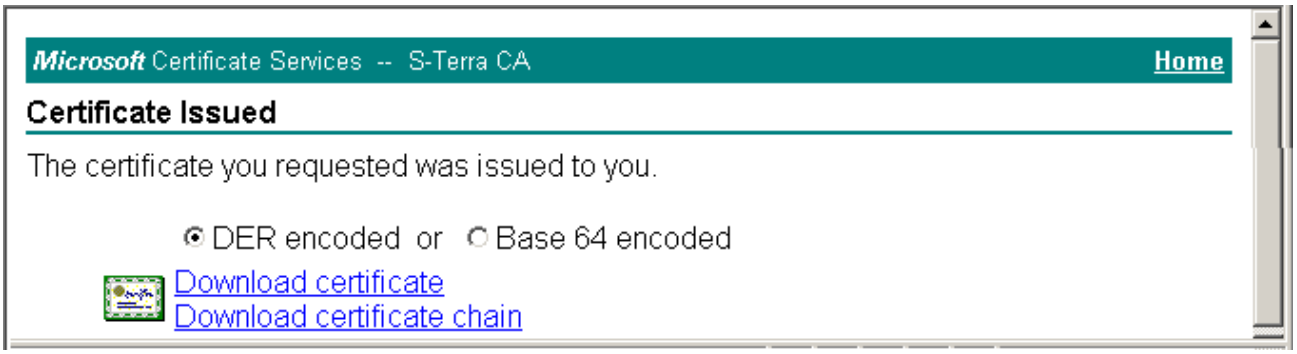


Рисунок 155

3. Выполните описанные операции также для клиента gate0 и создайте для него новый локальный сертификат, сохранив его на Сервере управления.

Создание обновления с новым сертификатом

1. На Сервере управления выделите одного клиента и в контекстном меню выберите предложение ***Update*** (Рисунок 156).

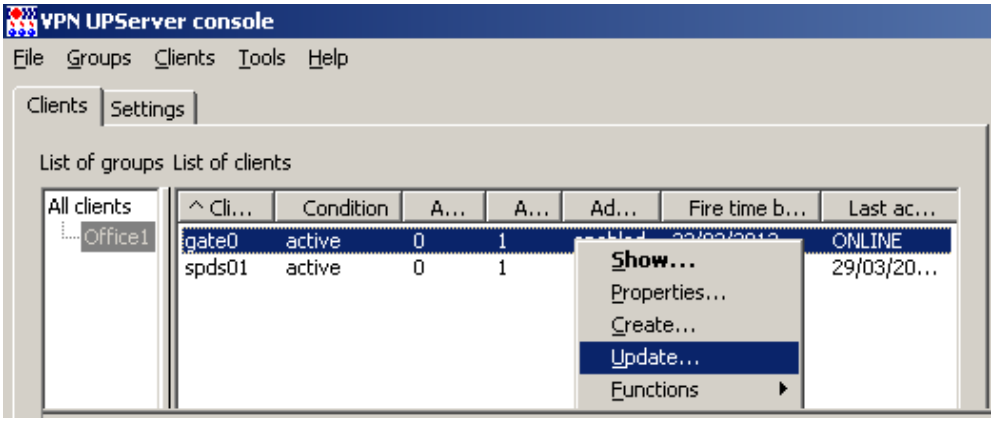


Рисунок 156

2. В открывшемся окне **Update client** нажмите кнопку E.

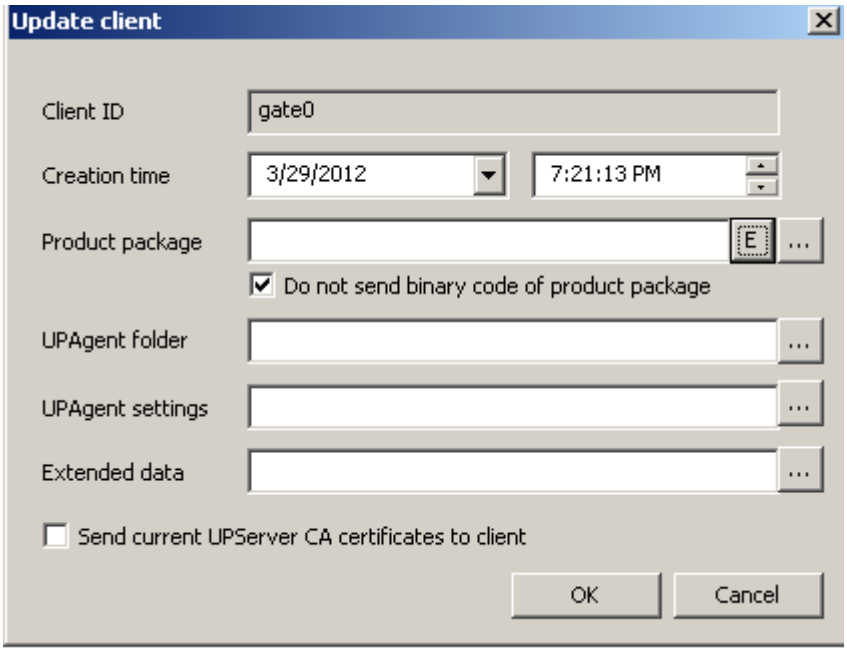


Рисунок 157

3. Войдите во вкладку **Certificates**, укажите новый CA сертификат, если он изменился, и добавьте новый локальный сертификат для центрального шлюза.

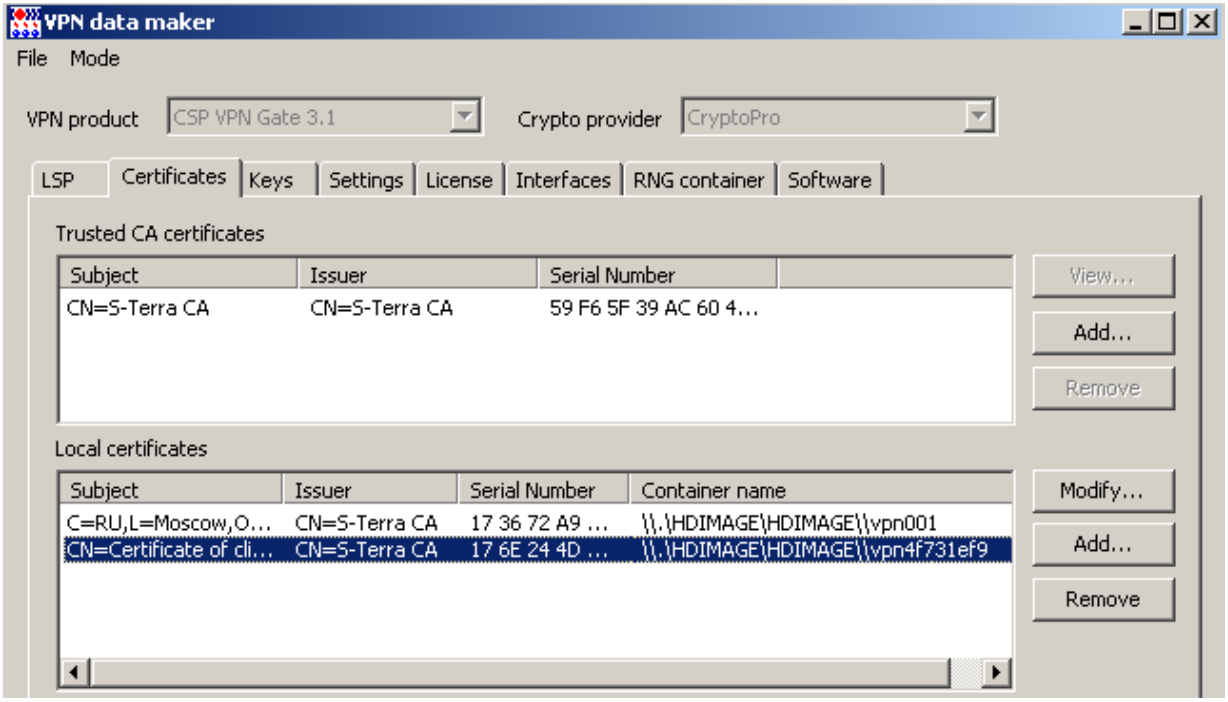


Рисунок 158

4. Старый локальный сертификат удалите.

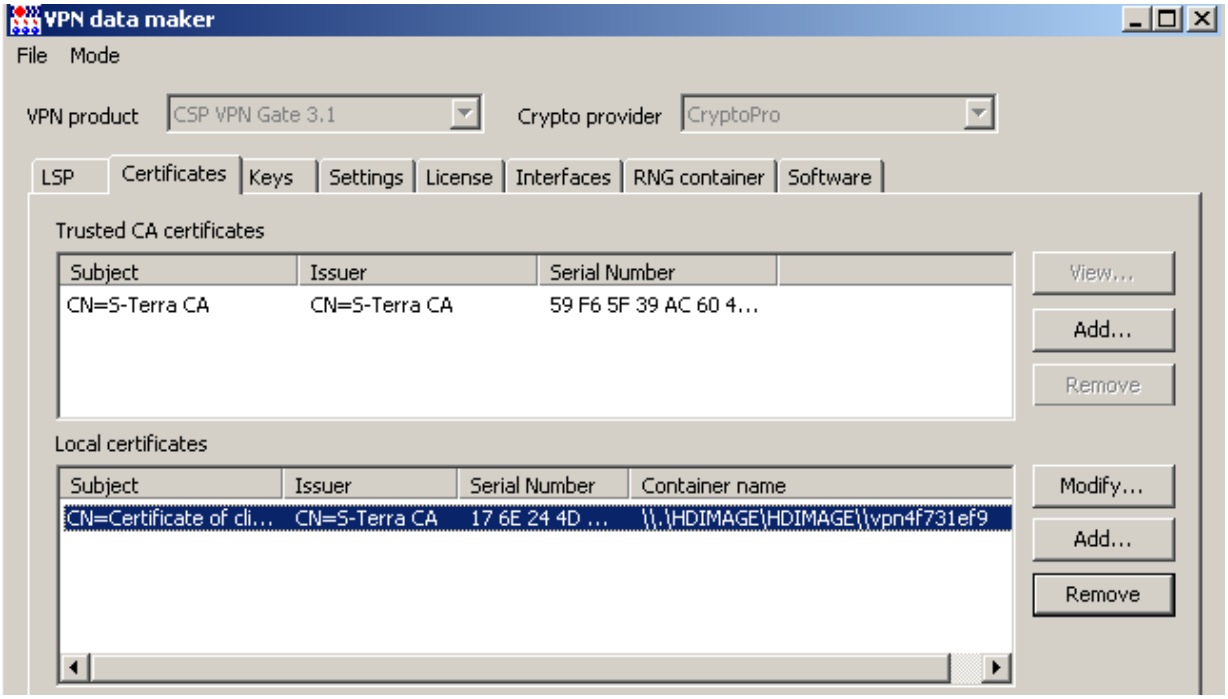


Рисунок 159

5. Во вкладке **LSP** следует внести изменения в структуры CertDescription local_cert_dsc_01 и `IdentityEntry`, связанные с локальным сертификатом. Внесите новое значение поля Subject, если оно изменилось, и новый серийный номер сертификата (Рисунок 160).

   Структура `CertDescription local_cert_dsc_01` описывает поля локального сертификата и только при наличии такого сертификата в базе продукта, будут строиться защищенные соединения с партнерами, заданные данной политикой безопасности. В структуре `IdentityEntry` задается значение идентификатора, которое должно быть передано партнеру. Нажмите кнопку OK.

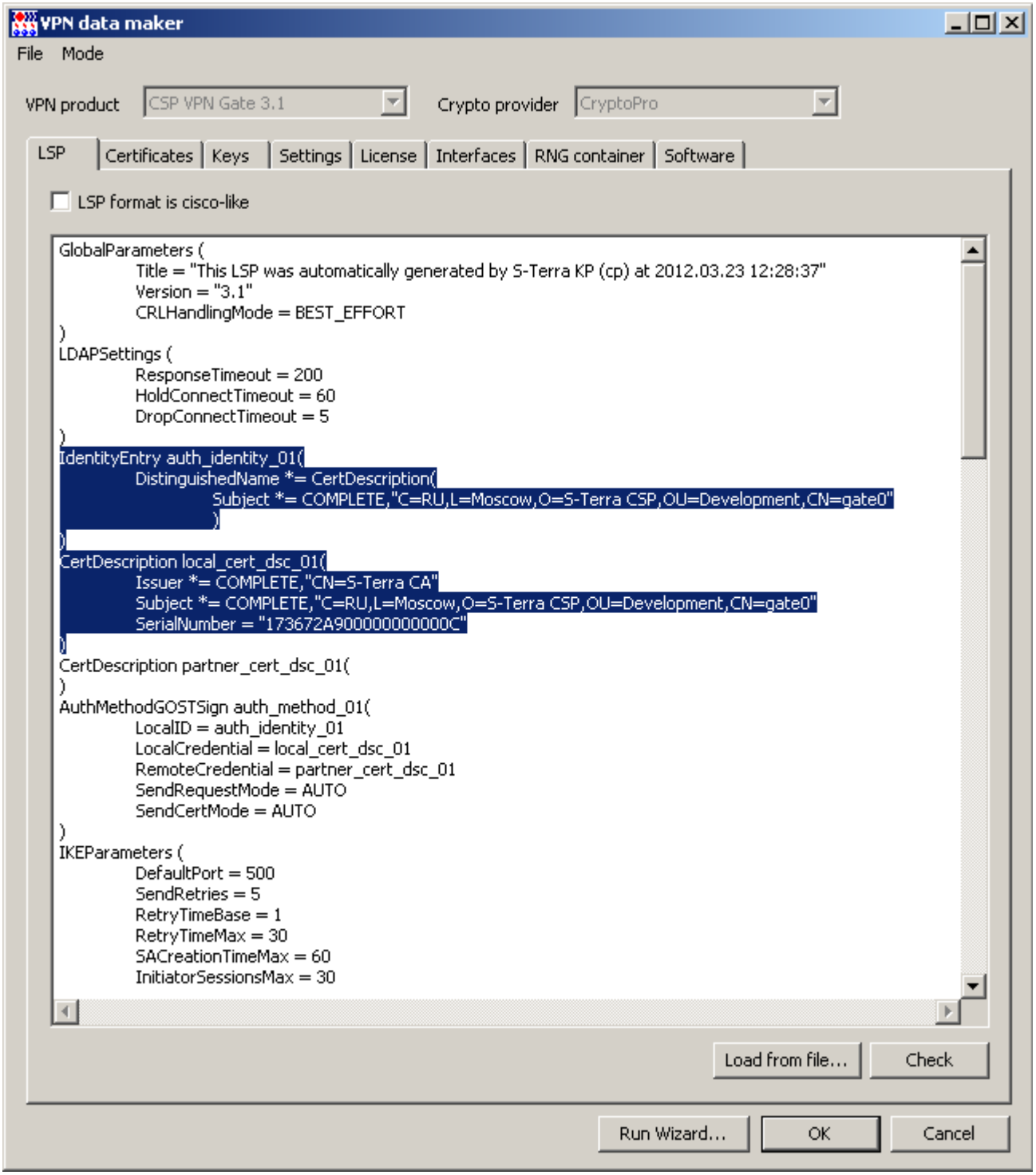


Рисунок 160

Замечание: Если выделить в таблице учетные записи сразу обеих устройств и применить к ним операцию ***Update***, то отредактировать LSP для каждого устройства не будет возможности, LSP для всех будет одна и та же. В целях тестирования обновления сертификатов для большого количества устройств, в **LSP** можно убрать зависимость от конкретного сертификата - будет использоваться поле `Subject` того сертификата, который лежит в базе продукта, но в этом случае безопасность доступа к удаленным серверам будет снижена. Для этого вместо двух структур надо внести следующую одну структуру:

```
IdentityEntry auth_identity_01(
    DistinguishedName *= USER_SPECIFIC_DATA
)
```

6. Файл с данными для обновления сертификатов в продукте CSP VPN Gate создан, нажмите OK.

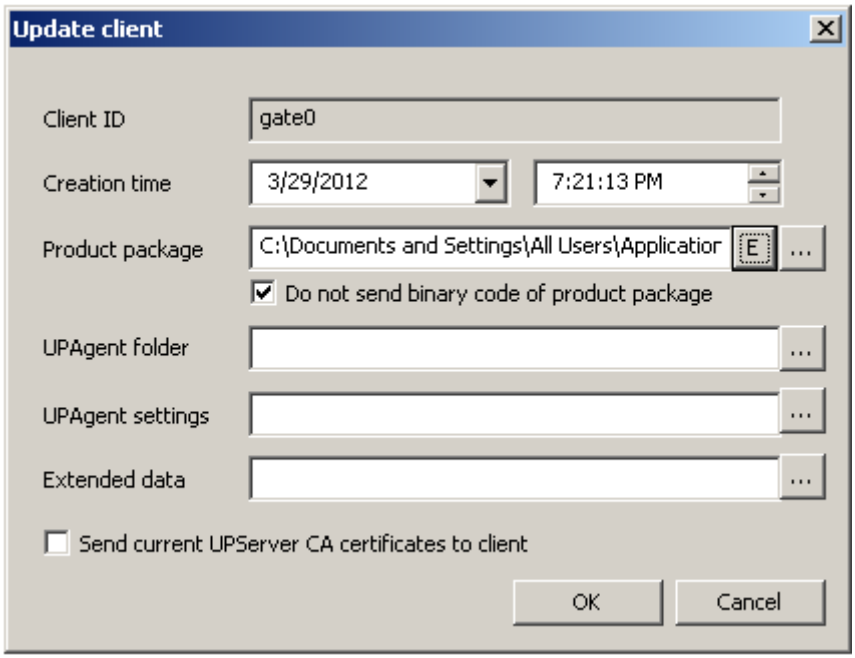


Рисунок 161

7. Обновление подготовлено для скачивания. После обновления сертификатов на центральном шлюзе учетная запись будет иметь вид (Рисунок 162).

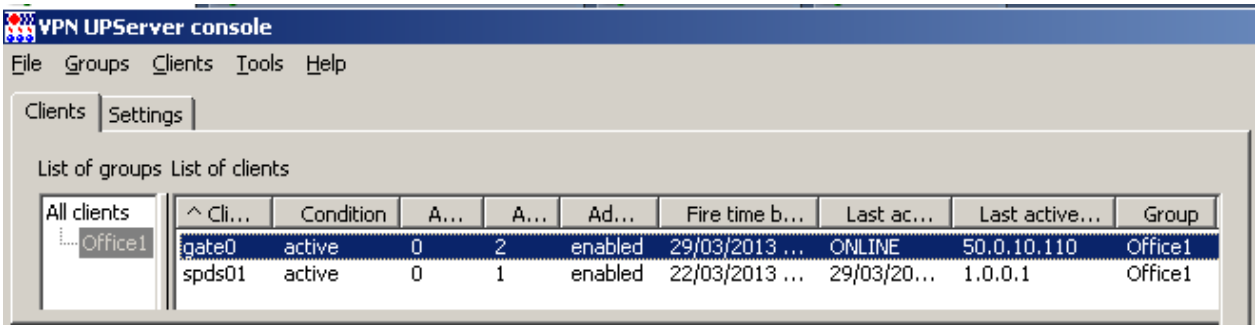


Рисунок 162

8. Выбрав в контекстном меню операцию ***Show***, можно проконтролировать, что новые сертификаты зарегистрированы в продукте CSP VPN Gate и используются, просматривая вкладки **Certificates (**Рисунок 163**) и Containers (**Рисунок 164**).**

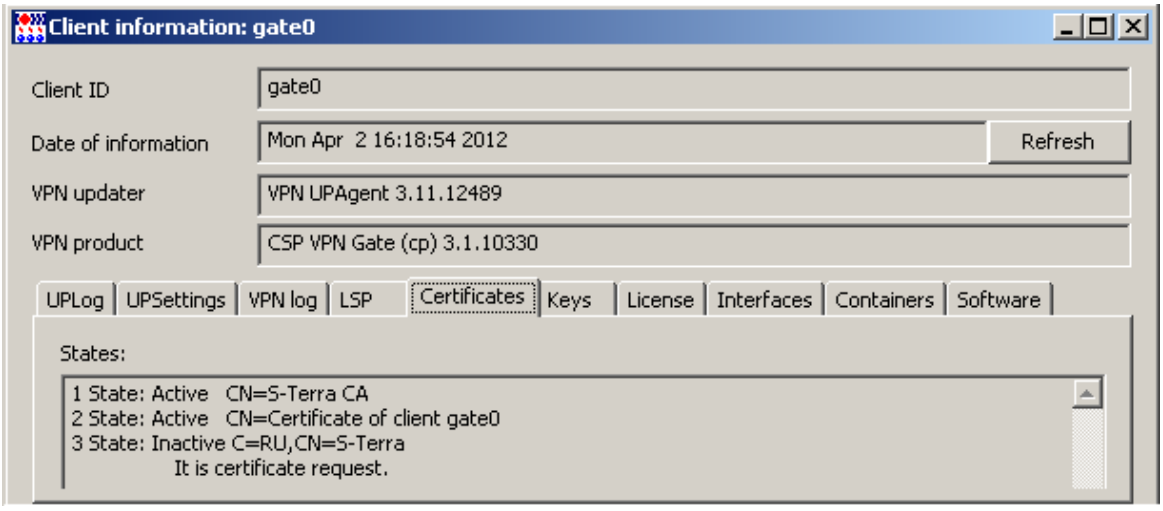


Рисунок 163

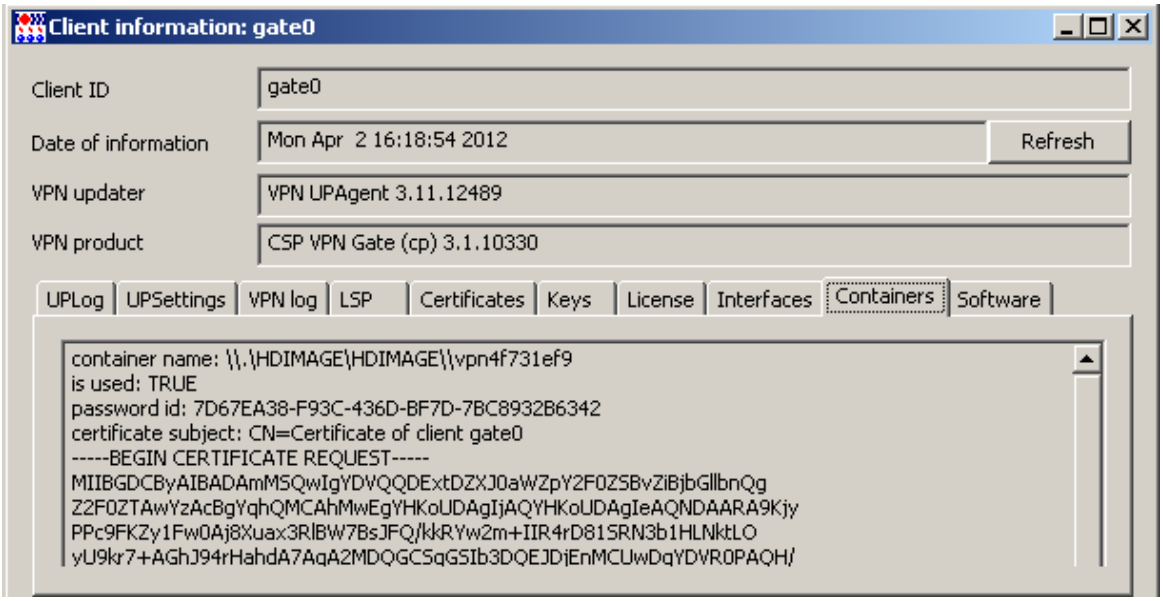


Рисунок 164

9. Подготовьте обновление с новым локальным сертификатом для клиента `spds01` по аналогичному сценарию.
10. На этом процедура обновления сертификатов завершена.

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 package*** (Рисунок 165).

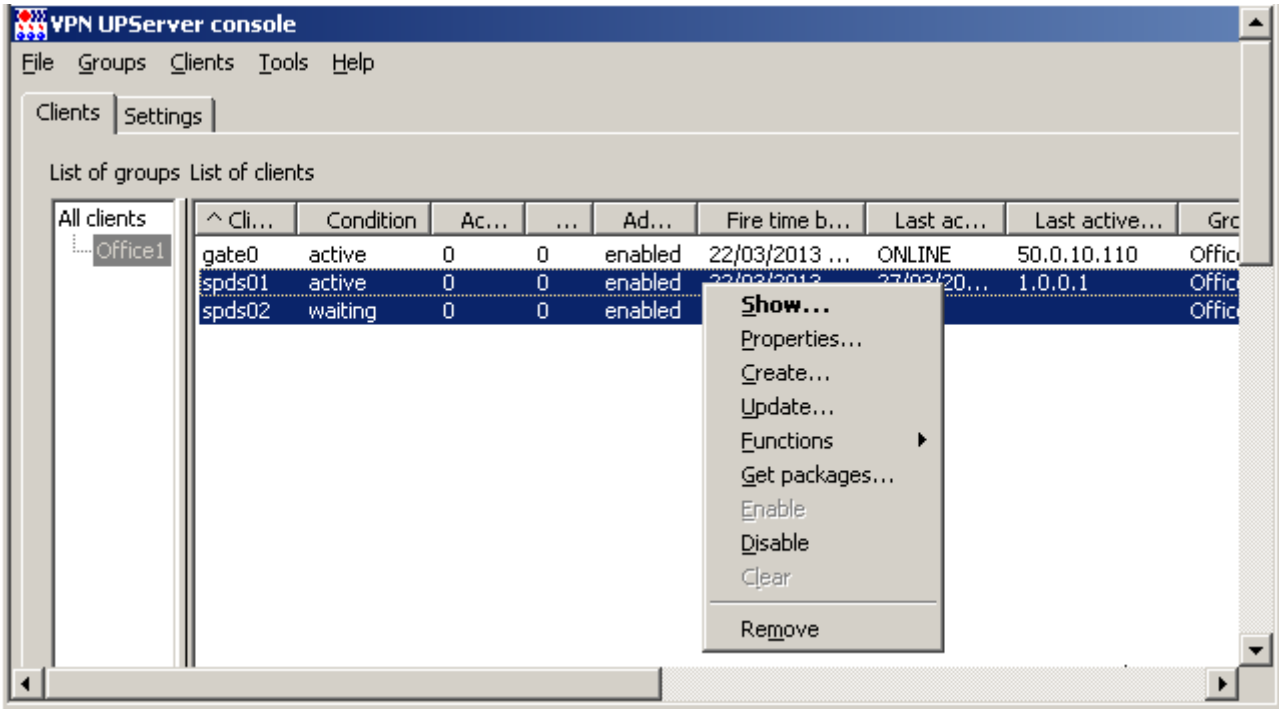


Рисунок 165

Каждый клиент на Сервере управления создается отдельно и для каждого клиента скрипты для инсталляции и инициализации 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 и локальных сертификатов. 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.

Создание шаблона проекта

1. Не выделяя в таблице клиентов, в меню ***Tools*** выберите предложение ***VPN data maker*** (Рисунок 166).

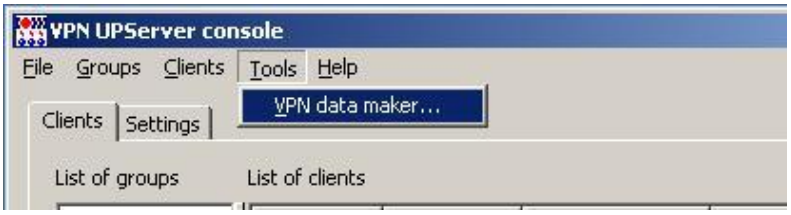


Рисунок 166

2. В открывшемся окне **VPN data maker** заполните необходимые вкладки (или используйте Run Wizard) для настройки продукта CSP VPN Gate (Рисунок 167).

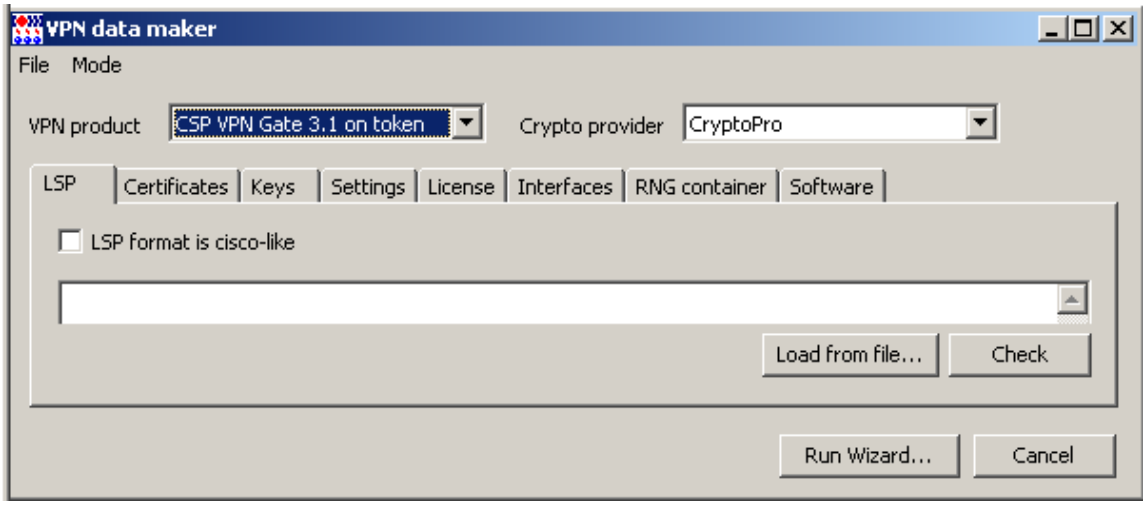


Рисунок 167

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

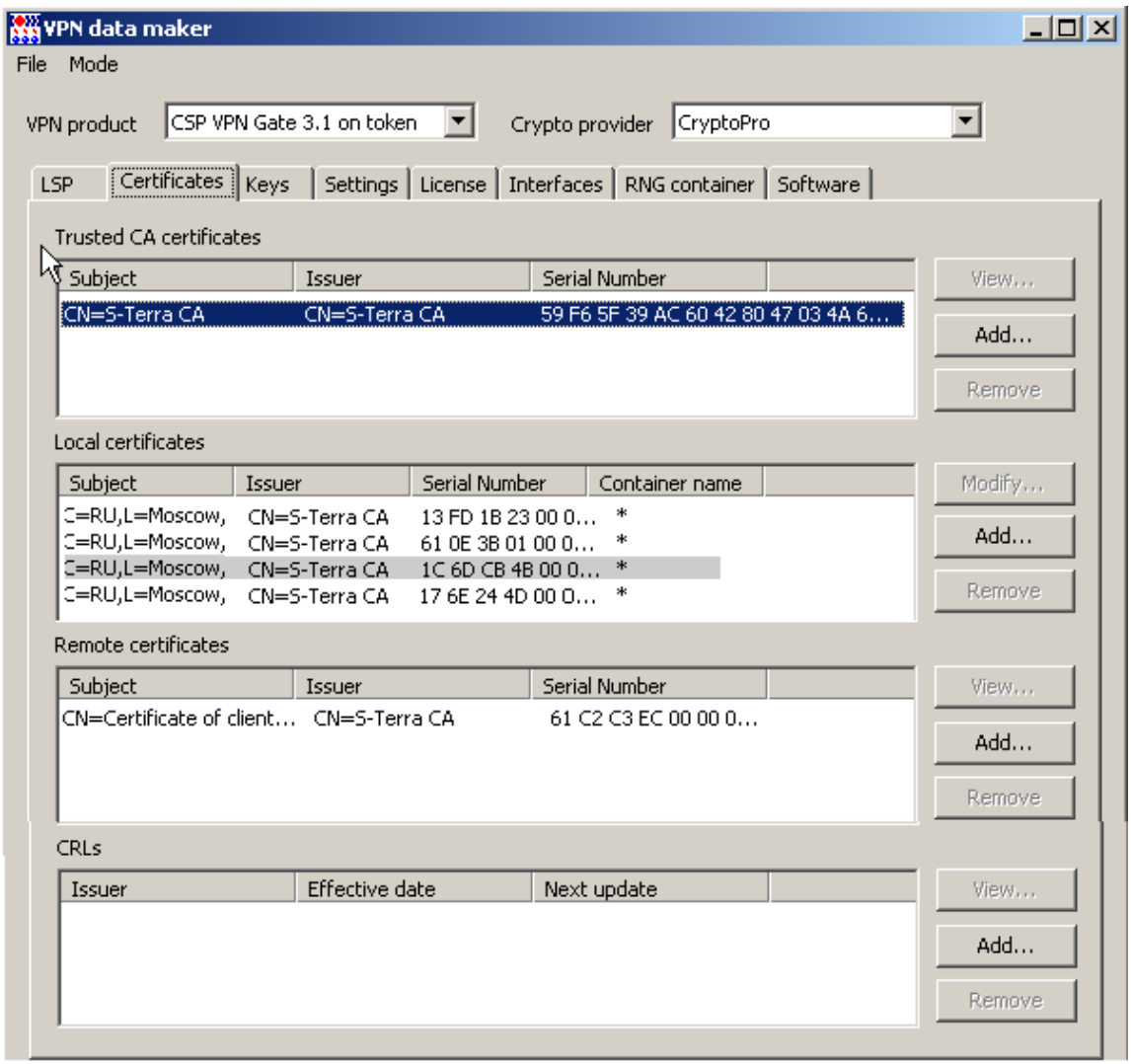


Рисунок 168

При задании локальных сертификатов появляется окно **Certificate description (**Рисунок 169**)**, 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 действительное значение.

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.

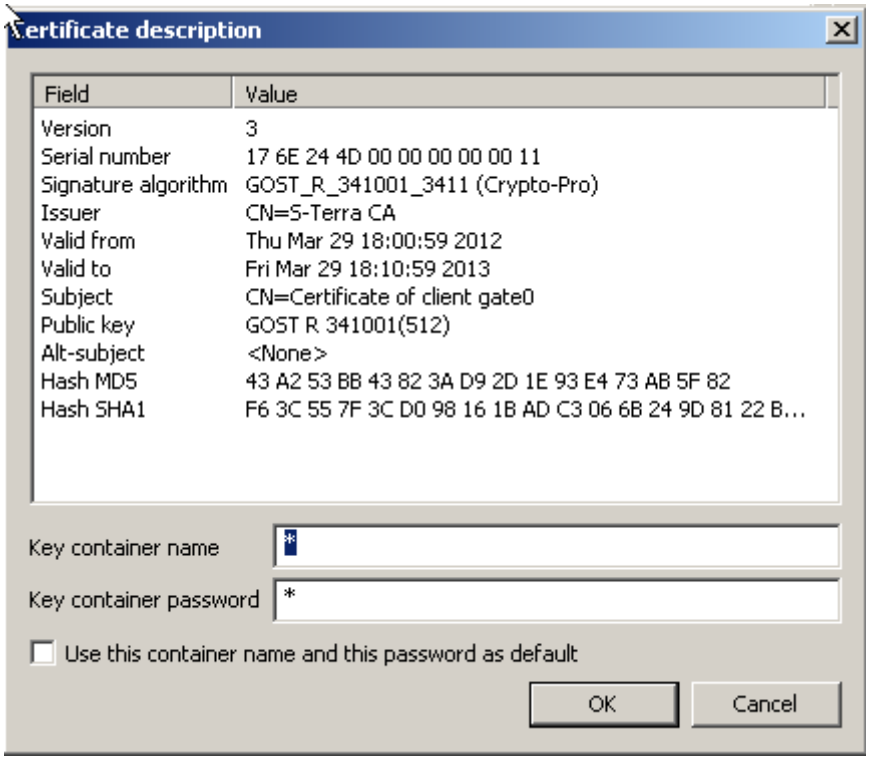


Рисунок 169

4. Заполнив необходимые вкладки, перейдите в режим шаблона проекта, выбрав в меню ***Mode*** предложение ***Enable template mode*** （Рисунок 170）.

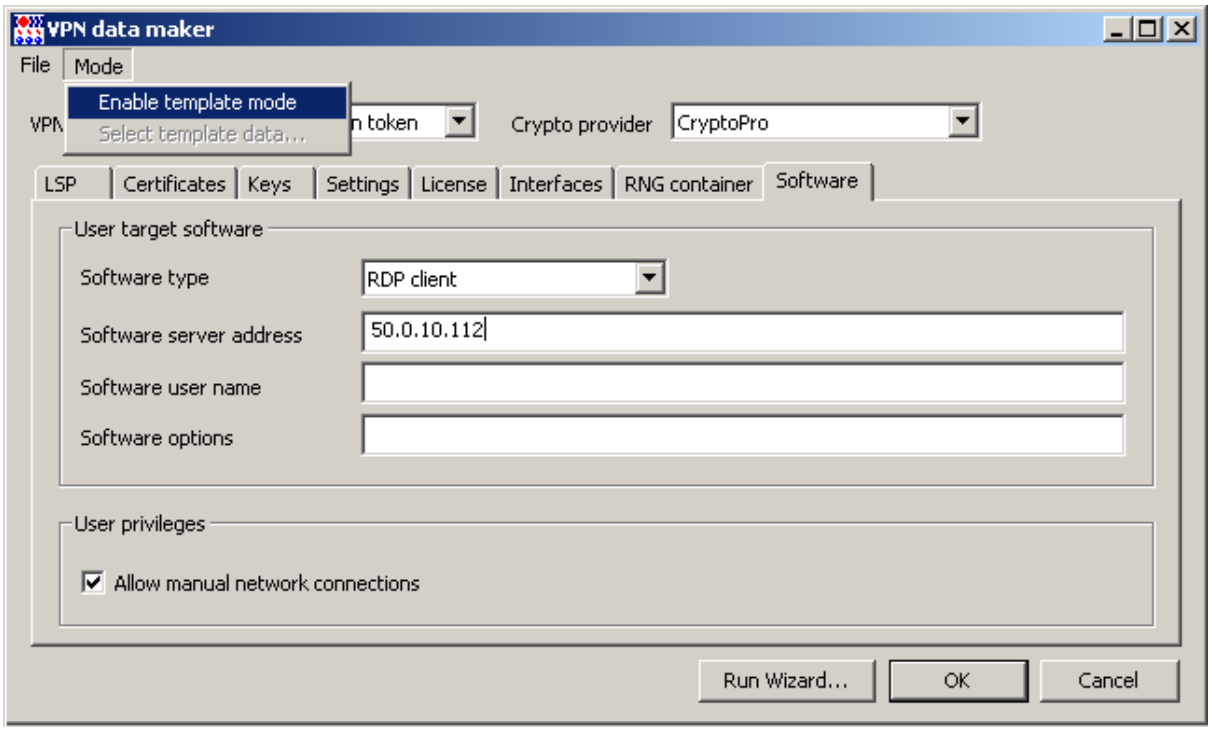


Рисунок 170

5. Затем в меню ***Mode*** выберите предложение ***Select template data*** (это предложение доступно только в режиме шаблона проекта)（Рисунок 171）.

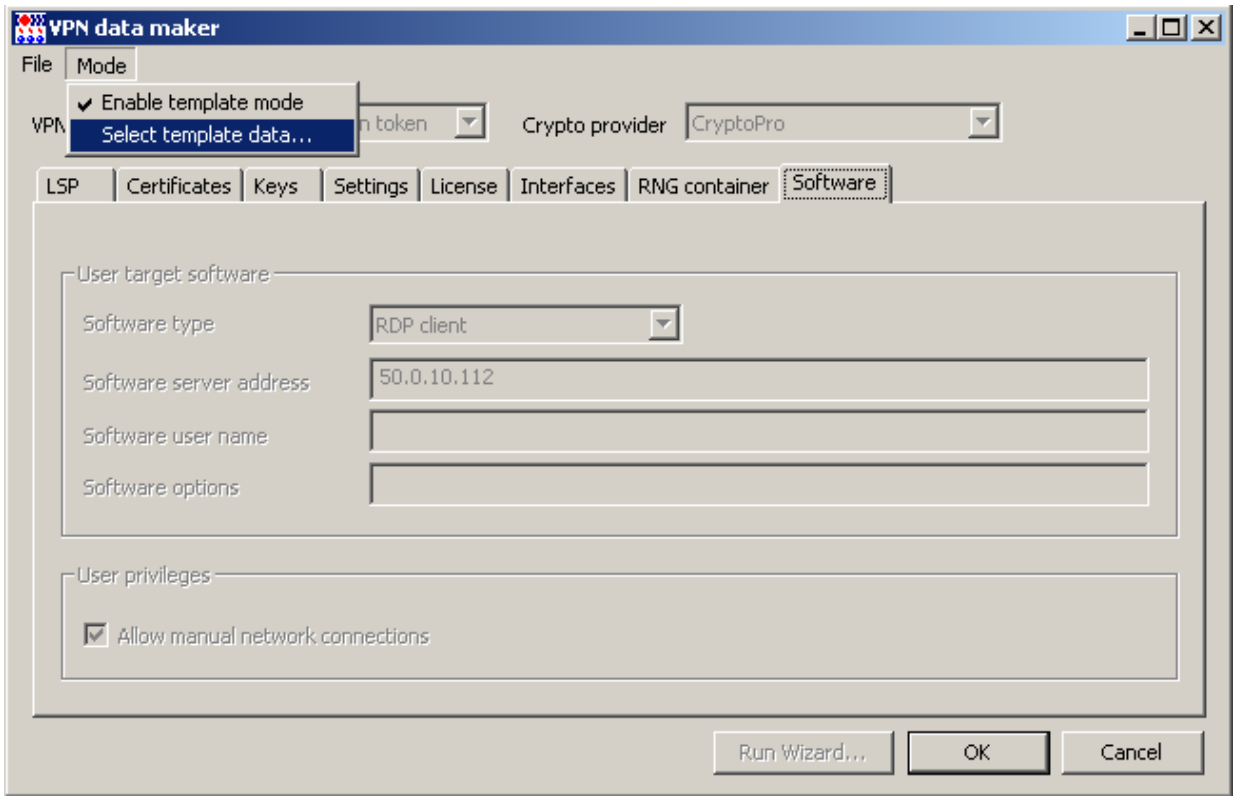


Рисунок 171

6. Появилось окно **Update data types** со списком данных, которые могут входить в шаблон проекта (Рисунок 172). Пометьте флажком данные, которые будут входить в шаблон. При применении обновления, созданного с использованием шаблона, только входящие в него данные будут изменяться на клиенте.

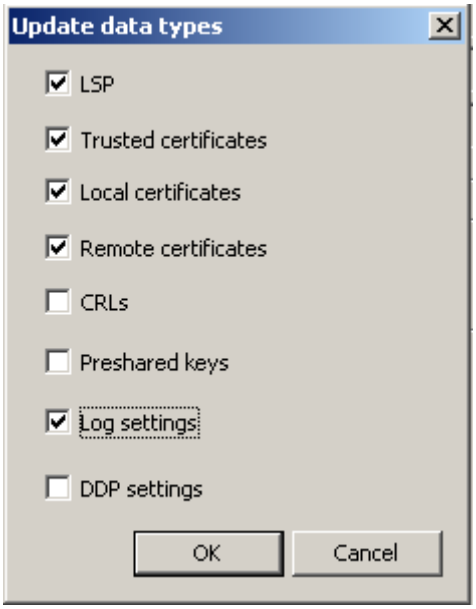


Рисунок 172

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 выбранных данных, сохраните созданный шаблон в файл, используя предложение ***Save as*** меню ***File*** (Рисунок 173), (Рисунок 174).

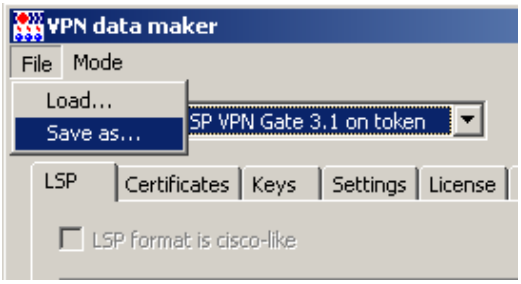


Рисунок 173

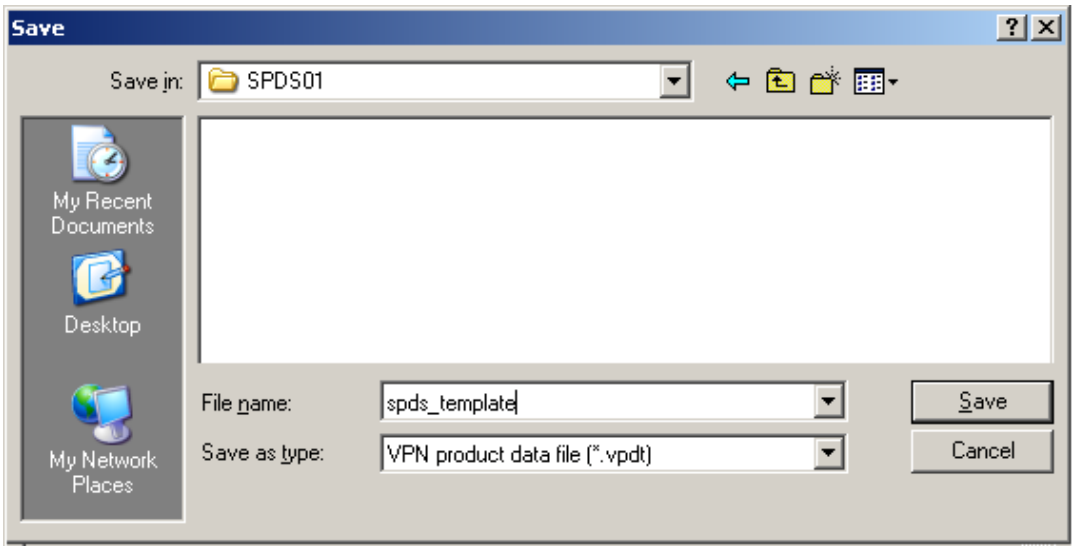


Рисунок 174

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 175).

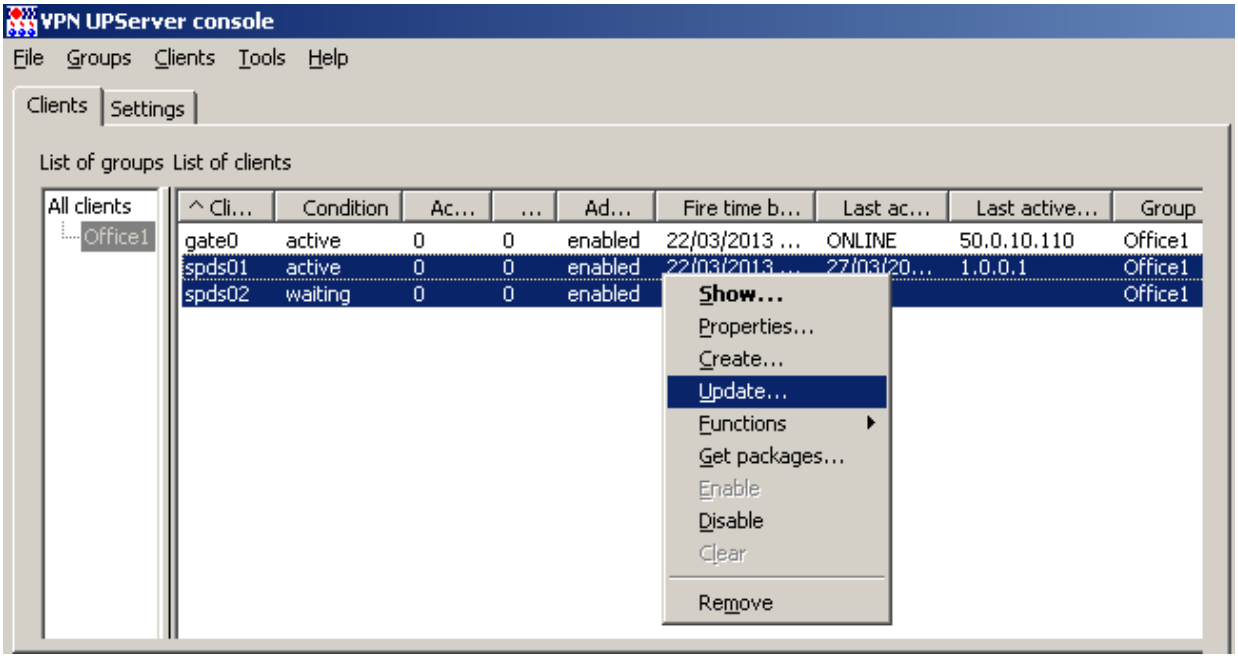
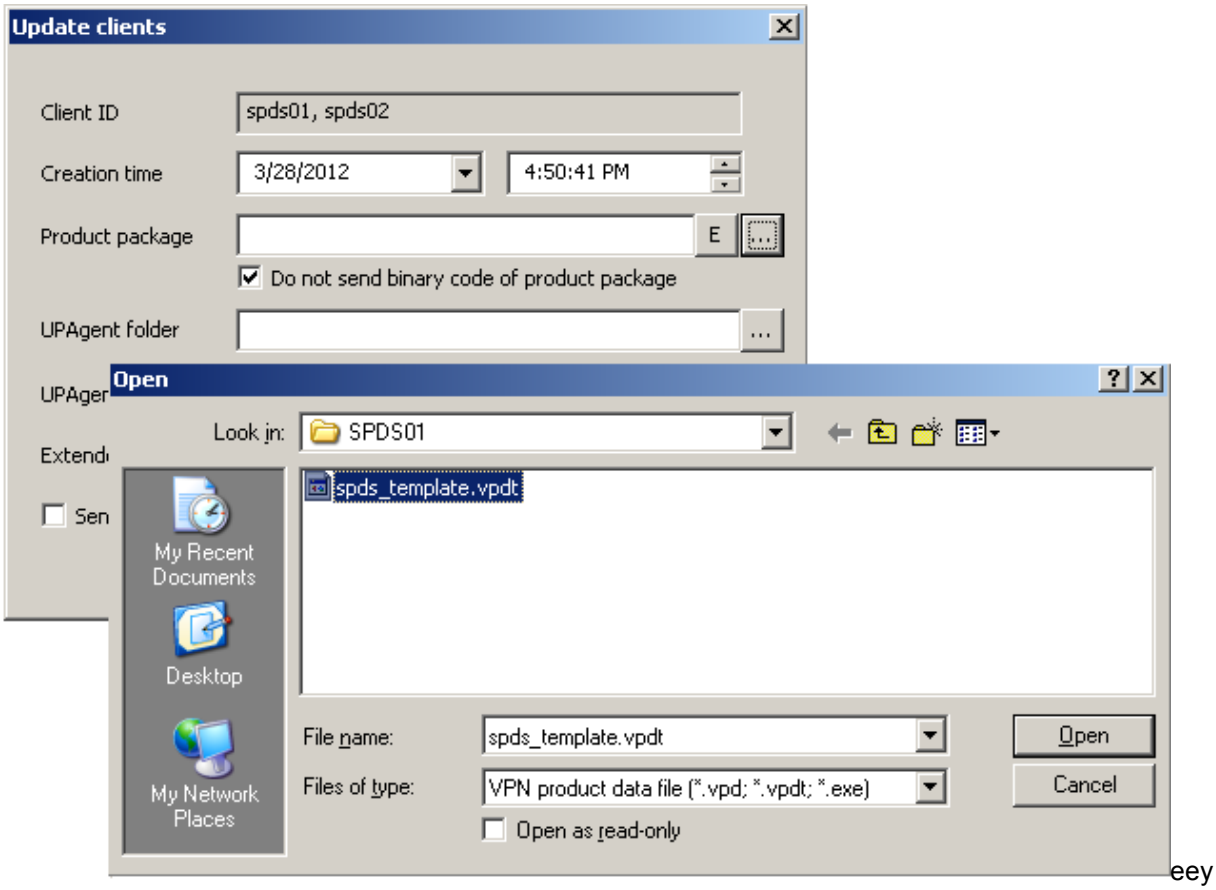


Рисунок 175

2. В открывшемся окне **Update clients** в поле **Product package** нажмите кнопку [...] и в стандартном окне открытия файла укажите файл с шаблоном проекта, например, `spds_template.vpdt` (Рисунок 176).



eey

Рисунок 176

3. Если в шаблон входит список локальных сертификатов, то при применении обновления для каждого клиента будет отбираться локальный сертификат из списка с использованием 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.

Сценарий создания клонов 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.

Создание базового проекта

1. Зададим настройки (конфигурацию) продукта CSP VPN Gate для базового проекта `gate_base.pvd`, который будет использоваться для клонирования. В меню Tools выберите предложение ***VPN data maker*** (Рисунок 177).

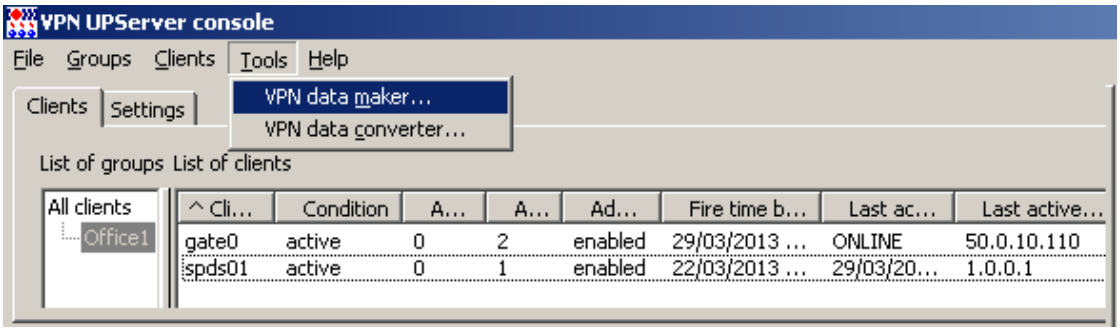


Рисунок 177

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

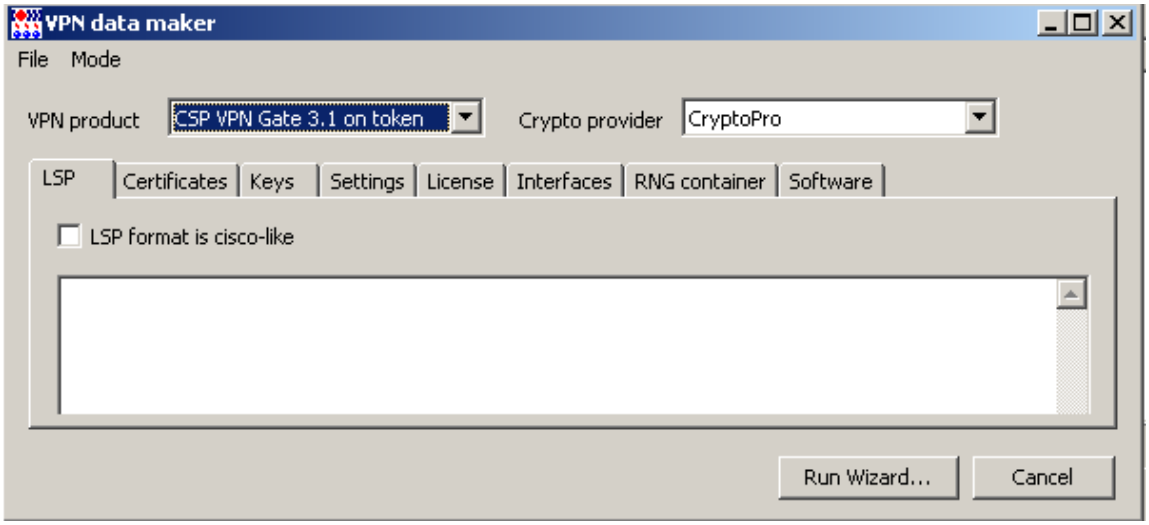


Рисунок 178

3. В следующем окне укажите CA и локальный сертификат, который у вас есть или создайте новый с полем **Subject**, например, `spds_base`.

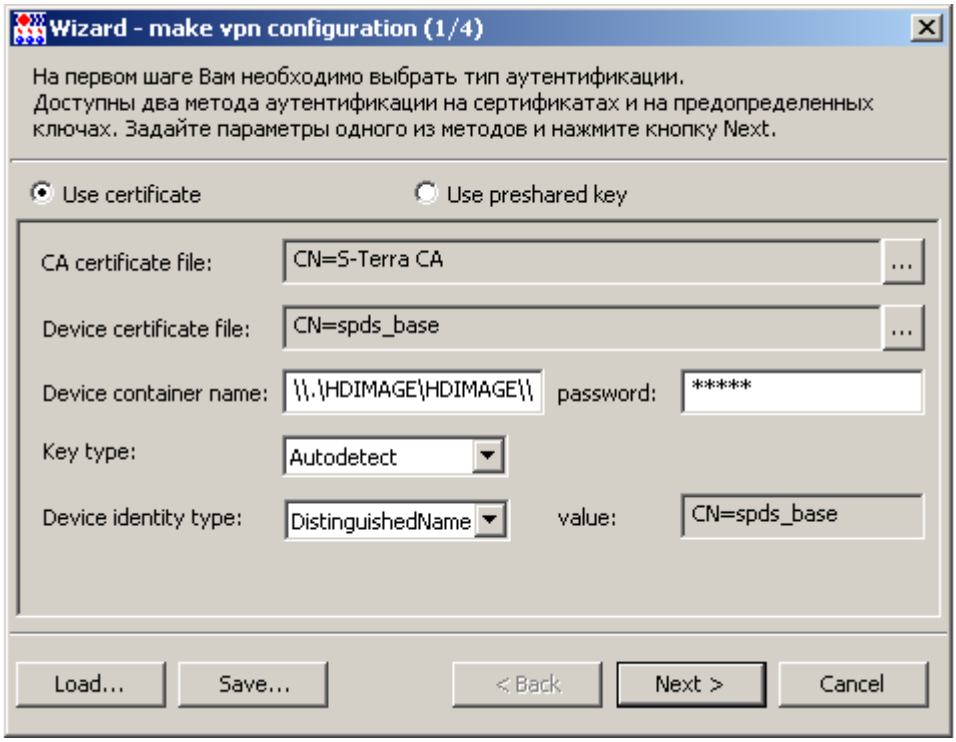


Рисунок 179

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

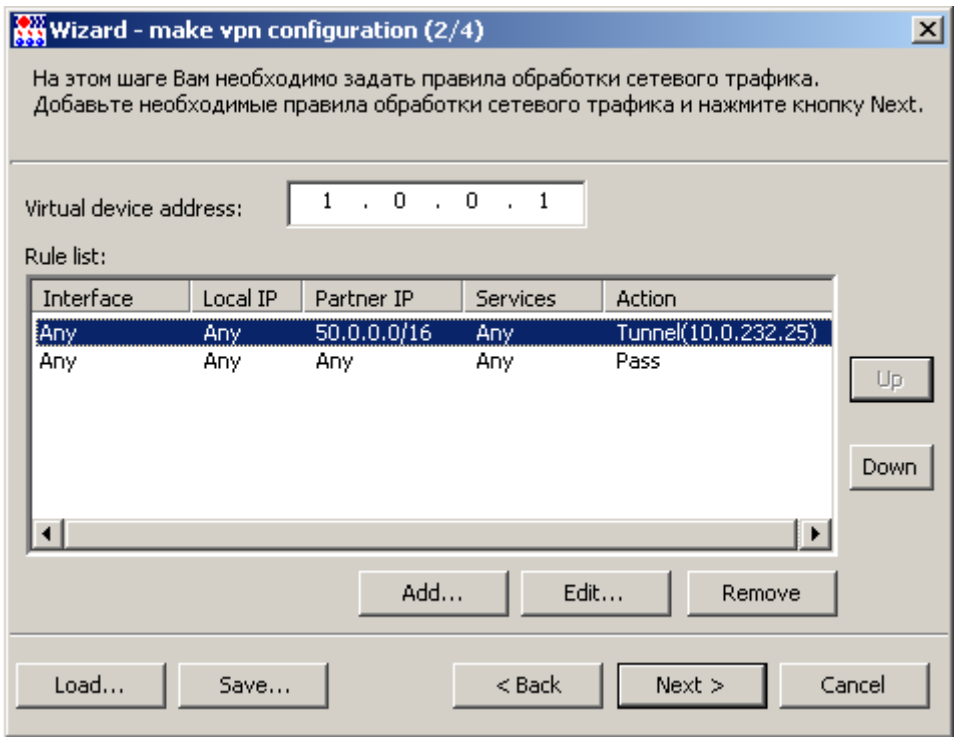


Рисунок 180

5. Укажите в каком качестве будет выступать управляемое устройство и адрес сервера для удаленного доступа.

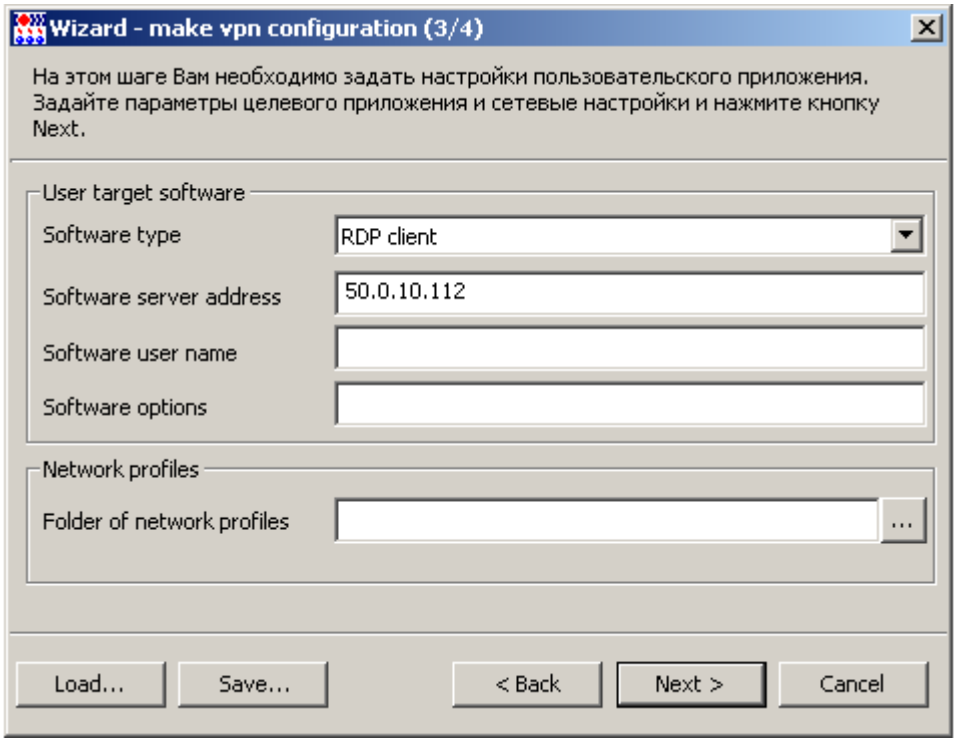


Рисунок 181

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

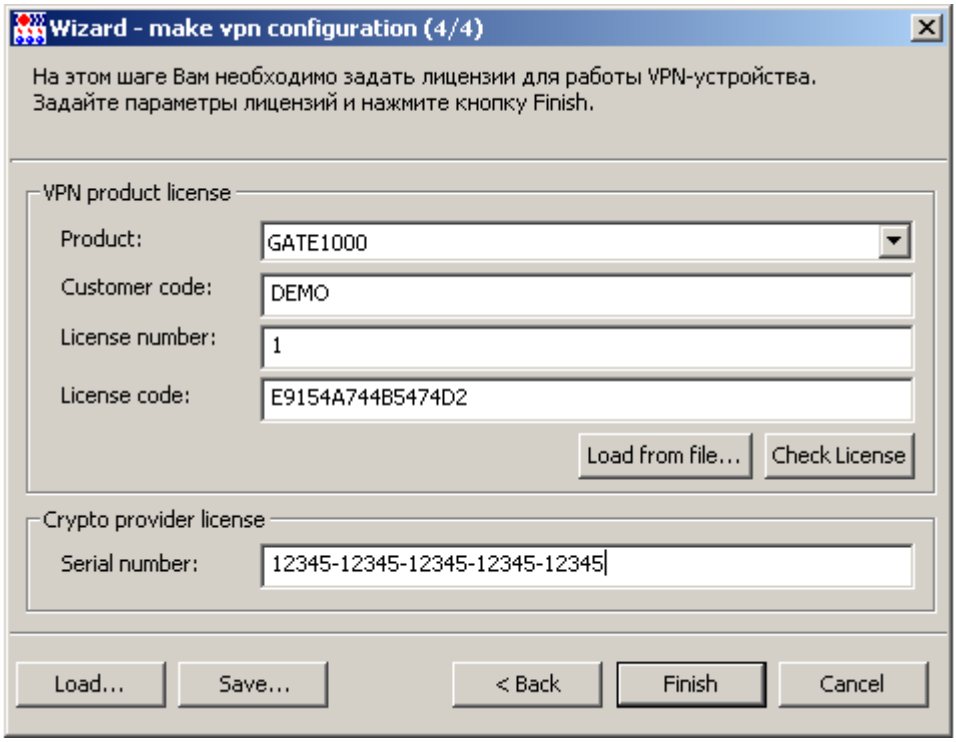


Рисунок 182

7. Таким образом, все выставленные настройки отражены во вкладках. Для того, чтобы в базовом проекте конфигурация не зависела от полей локального сертификата, во вкладке ***LSP*** следующие структуры (Рисунок 183):

```
IdentityEntry auth_identity_01(
    DistinguishedName *= CertDescription(
          Subject *= COMPLETE,"CN=spds_base"
          )
)
```

```
CertDescription local_cert_dsc_01(
    Issuer *= COMPLETE,"CN=S-Terra CA"
    Subject *= COMPLETE,"CN=spds_base"
    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
)
```

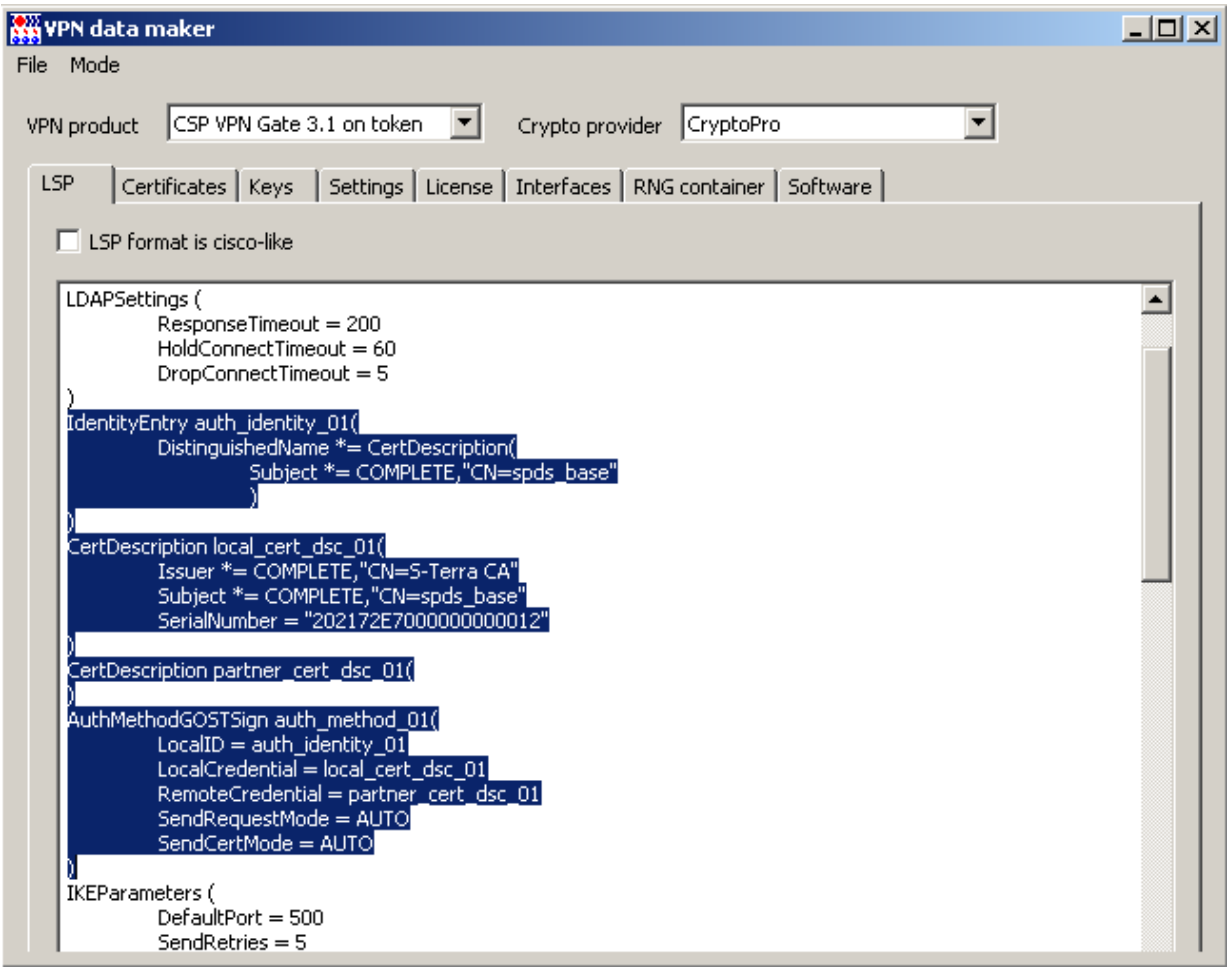


Рисунок 183

замените 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 был только один локальный сертификат.

8. Далее во вкладке ***Interfaces*** можно задать сетевые настройки соединений, если они будут одинаковыми у клонов. Воспользуйтесь окном **Edit connection**, как было описано ранее, например (Рисунок 184). Нажмите кнопку OK.

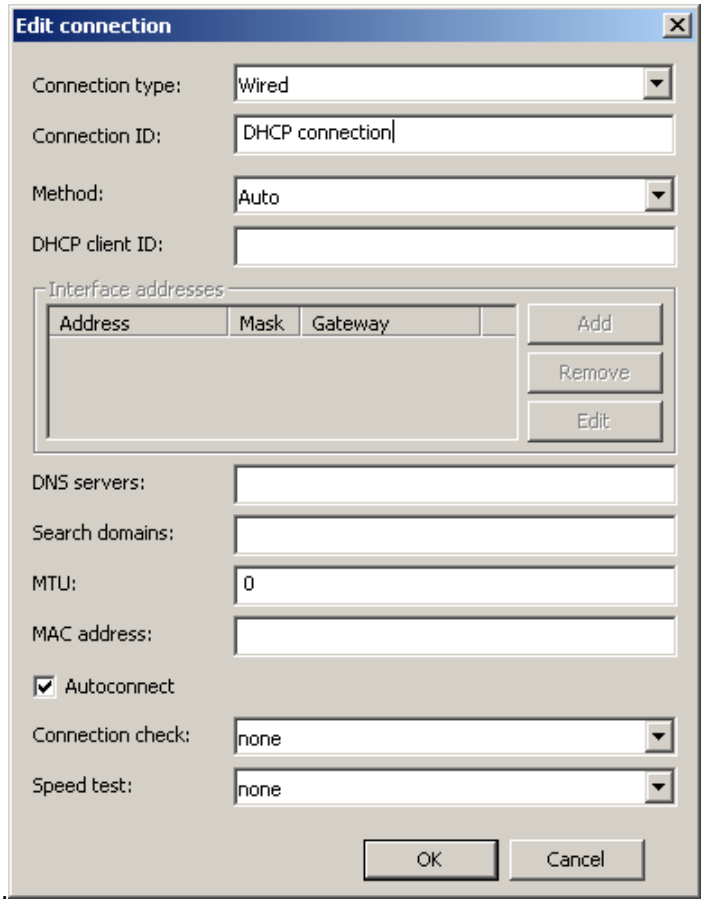


Рисунок 184

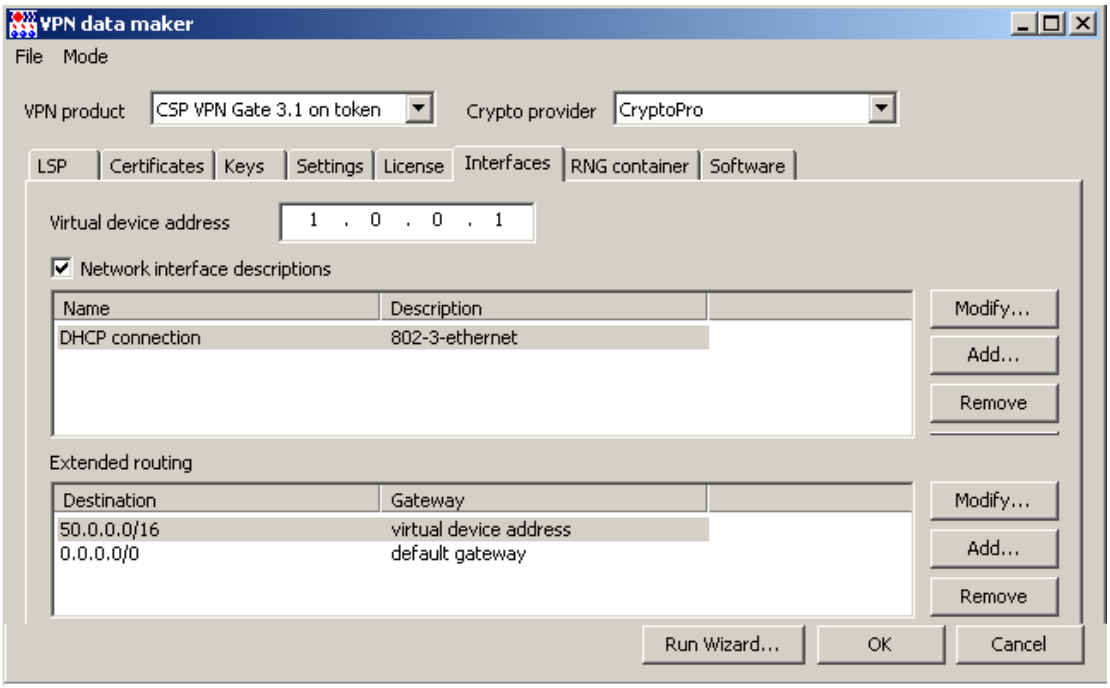


Рисунок 185

9. Получен базовый проект (Рисунок 185), сохраните его на Сервере управления, выбрав предложение ***Save as*** в меню ***File***.

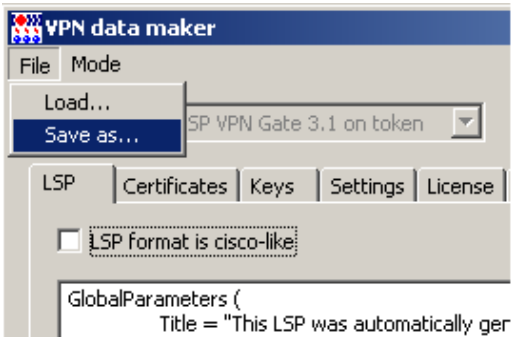


Рисунок 186

10. Сохраните в каталоге Clone под именем, например, `spds_base.vpd`.

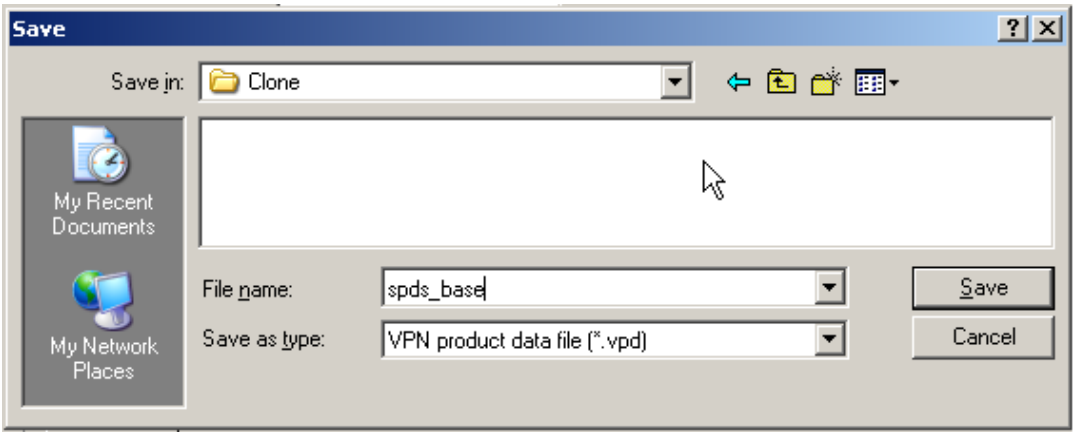


Рисунок 187

Подготовка материалов для клонов

Далее следует подготовить материал для создания клонов базового проекта – для каждого управляемого устройства СПДС «ПОСТ» создадим локальный сертификат, политику безопасности (LSP), файлы с лицензиями на CSP VPN Gate и КриптоПро CSP. Выполним это.

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 на Сервере управления и зарегистрируйте лицензию:

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

2. Подключите к Серверу управления СПДС «ПОСТ».
3. Запустите С-Терра Редактор СПДС, откройте сессию, разрешив запись на устройство.
4. Узнайте имя СПДС «ПОСТ», на который 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         Дисковод G
    0x0102  FAT12_A         Дисковод A
```

5. Создайте ключевую пару, запрос на локальный сертификат клиента, например, spds03, 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 СПДС «ПОСТ», например, `FAT12_G\spds03`. Для выполнения всех этих действий запустите команду:

```
"C:\Program Files\Crypto Pro\CSP\cryptcp.exe" -creatcert -dn "CN=spds03" -both
-km -cont "\\.\FAT12_G\spds03" -exprt -CA "http://50.0.10.111/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 188). Обязательно задайте пустой пароль.

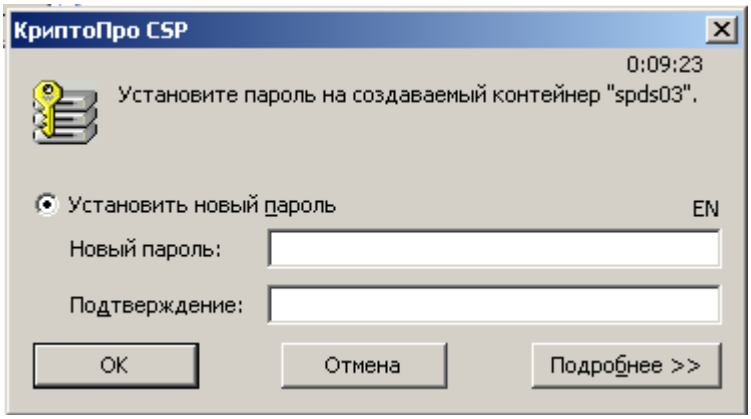


Рисунок 188

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=spds03" -both -km -cont
'\\.\FLASH\spds03' -exprt -pin "" -CA "http://50.0.10.111/certsrv" -dm -enable-
install-root
```

6. На Сервере управления в каталог `C:\Clone` скопируйте созданный локальный сертификат в кодировке DER из контейнера в файл `C:\Clone\spds03.cer`:

```
"C:\Program Files\Crypto Pro\CSP\cryptcp.exe" -CSPcert -cont \\.\FAT12_G\spds03
-df C:\Clone\spds03.cer -der
```

7. Создайте файл `C:\Clone\st_spds03.lic` с лицензией на продукт CSP VPN Gate, например::

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

8. Создайте файл `C:\Clone\cp_spds03.lic` с лицензией на продукт КриптоПро CSP, например:

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

9. Создайте файл `C:\Clone\rv_spds03.txt` с описанием виртуального адреса СПДС «ПОСТ» и роутинга, например:

```
VirtualDeviceAddress=1.1.0.1

[ExtendedDeviceRoutes]
Route_0=0.0.0.0/16 DGA
Route_1=50.0.0.0/16 VDA
```


где

DGA – default gateway address

VDA – virtual device address

Аналогичные данные для базового проекта можно посмотреть во вкладке `Interfaces` (Рисунок 185).

Создание проекта-клона

1. Создайте файл нового проекта `C:\Clone\spds03.pvd` на основе базового проекта, выполнив команду:

```
"C:\Program Files\S-Terra\S-Terra KP\vpnmaker.exe" replace -fi
C:\Clone\spds_base.vpd -fo C:\Clone\spds03.vpd -lic C:\Clone\st_spds03.lic -
cryptolic C:\Clone\cp_spds03.lic -cert C:\Clone\spds03.cer -certkey
\\.\HDIMAGE\HDIMAGE\\vpnspds03 -certkeypwd 12345 -ifdesc C:\Clone\rv_spds03.txt
```

где

`\\.\HDIMAGE\HDIMAGE\\vpnspds03` – имя контейнера на жестком диске в защищенной области, в который будет скопирован контейнер spds03. Контейнер на СПДС «ПОСТ» будет найден по локальному сертификату.

`certkeypwd` - пароль на новый скопированный контейнер.

2. Создайте на Сервере управления учетную запись клиента `spds03` для нового проекта, а потом переведите его в состояние ***Enable***, выполнив команды:

```
"C:\Program Files\S-Terra\S-Terra KP\upmgr.exe" create -i spds03 -p
C:\Clone\spds03.vpd
"C:\Program Files\S-Terra\S-Terra KP\upmgr.exe" enable -i spds03
```

3. Создайте два скрипта для настройки CSP VPN Gate и инсталляции Клиента управления на управляемом устройстве, сохранив их на СПДС «ПОСТ» в каталоге `customization`:

```
"C:\Program Files\S-Terra\S-Terra KP\upmgr.exe" get -i spds03 -d
G:\customization
```

В каталоге `customization` будут сохранены два скрипта:

`setup_product.sh` – скрипт, содержащий данные для настройки продукта CSP VPN Gate

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

Таким образом, на СПДС «ПОСТ» записаны два скрипта и контейнер с ключевой парой.

Управление с использованием командной строки – утилита upmgr

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

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

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 VPN данные, который был создан с помощью окна консоли управления VPN data maker
`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.

Команда ***show*** выводит информацию, аналогичную таблице клиентов. Если не указывать ключ `-i` – выводится краткая информация обо всех клиентах, при указании ключа `-i` – 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
```


Изменение готового проекта с данными VPN агента – утилита vpnmaker

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

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

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

Параметры утилиты:

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


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

You can enter many keys and many certificates.
```

В режиме работы replace некоторые старые данные проекта заменяются новыми.

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 гейтов. 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 у гейта на токене. Пример файла:

```
VirtualDeviceAddress=23.24.24.24

[ExtendedDeviceRoutes]
Route_0=10.0.2.0/24 192.168.5.1
Route_1=23.45.55.67/24 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 на токене. 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 устройстве.

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).

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`.

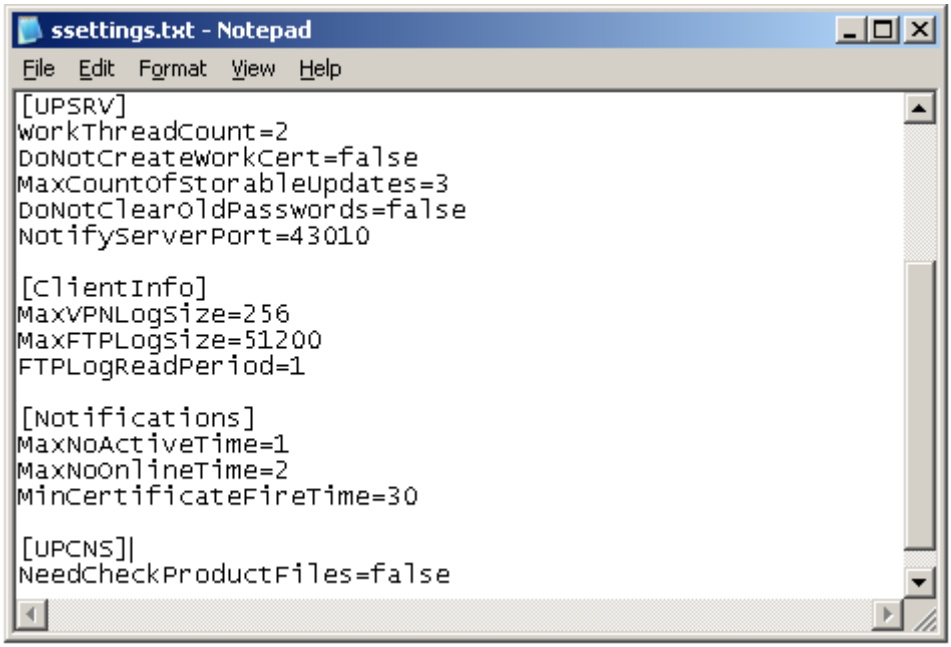


Рисунок 189

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_LifetimeKB` 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.
	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
```


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`

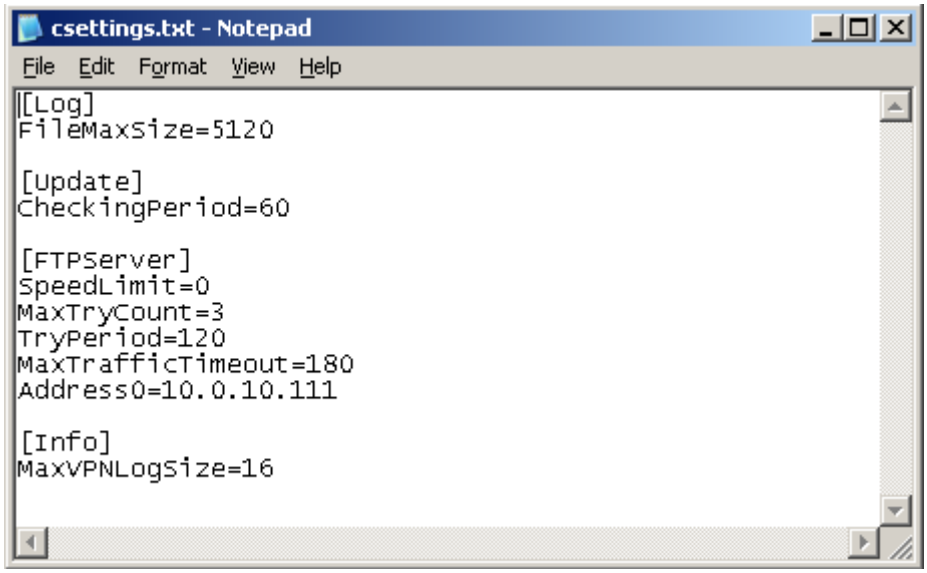


Рисунок 190

Для каждого клиента настройки Клиента управления можно изменить и сохранить в другом файле, а затем указать его в поле **UPAgent settings** (Рисунок 58) 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 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 1 до 300 секунд (значение по умолчанию 20).
	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.

Описание интерфейса Сервера управления

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

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.

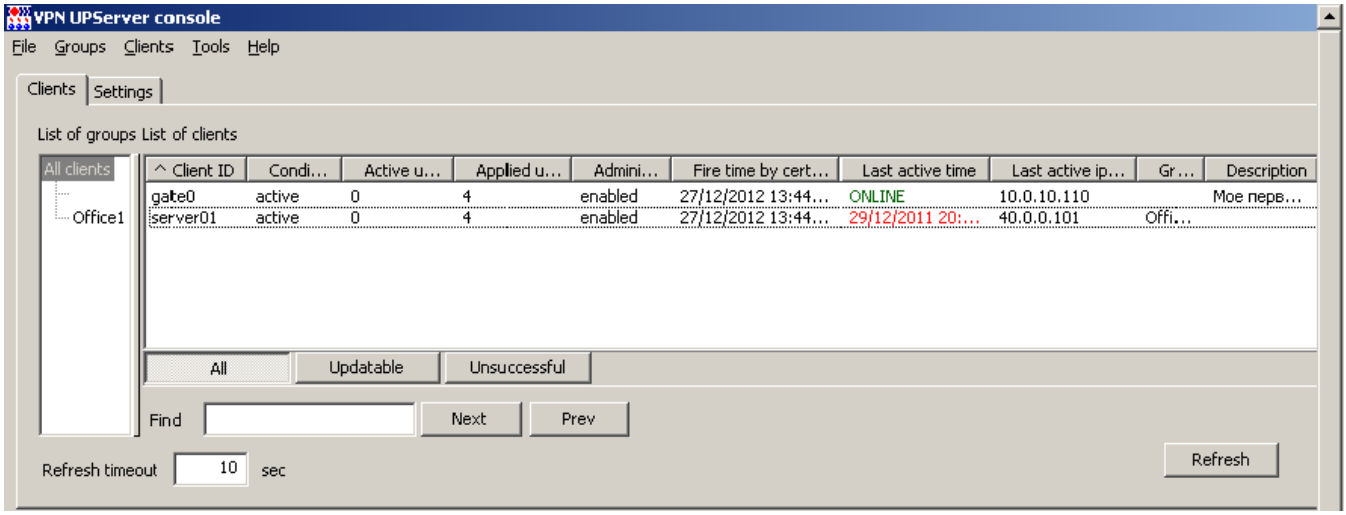


Рисунок 191

Описание вкладки **Clients**.

Параметр	Описание
List of groups	дерево групп клиентов, объединенных администратором по территориальному или организационному признаку расположения управляемых компьютеров
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 Gate/S-Terra Gate
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.

Меню File

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

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

Меню Groups

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

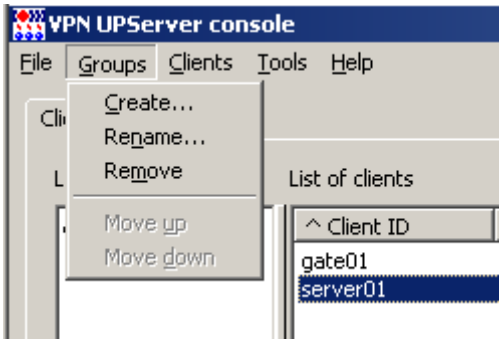


Рисунок 192

Create… - вызывает окно создания новой группы (группа создается как подгруппа выделенной группы), в котором надо задать имя группы (Рисунок 193).

Parent group name – имя группы, в которой создается подгруппа

Group name – имя создаваемой подгруппы.

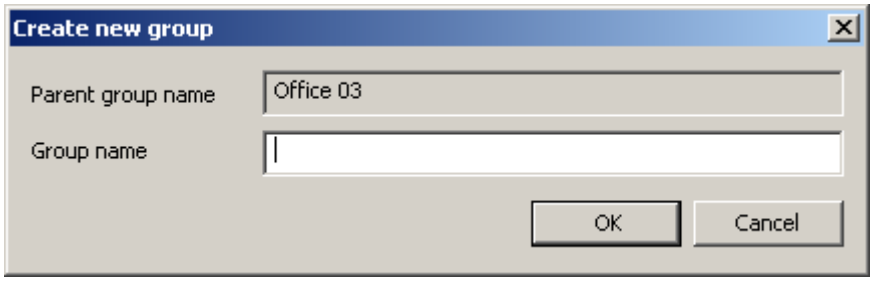


Рисунок 193

Rename… - вызывает окно переименования выделенной группы, в котором задается новое имя группы (Рисунок 194).

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.

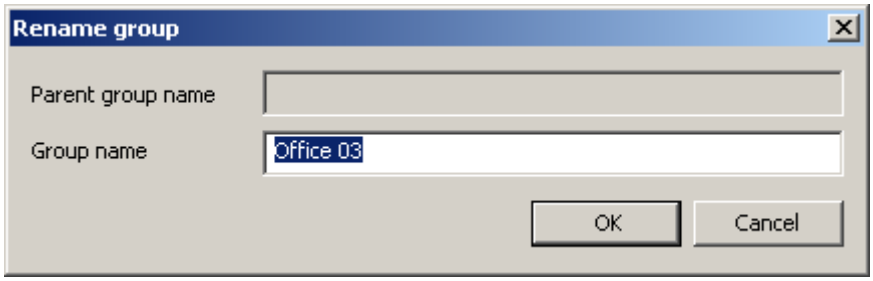


Рисунок 194

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.

Меню Clients

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

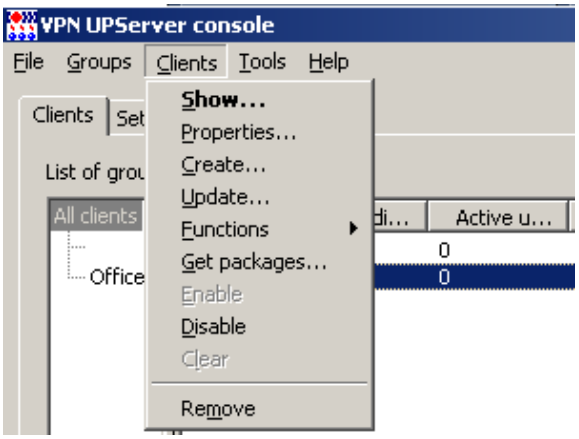


Рисунок 195

Show… – вызывает окно отображения параметров существующего клиента (Рисунок 125)

Properties… - вызывает окно **Client properties** с информацией об управляемом устройстве (Рисунок 196) и следующими полями:

Client ID - идентификатор клиента

Client description – введенная администратором в это поле информация будет отображена в поле Description вкладки **Clients** (Рисунок 191)

Device password – в данной версии это поле не используется

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

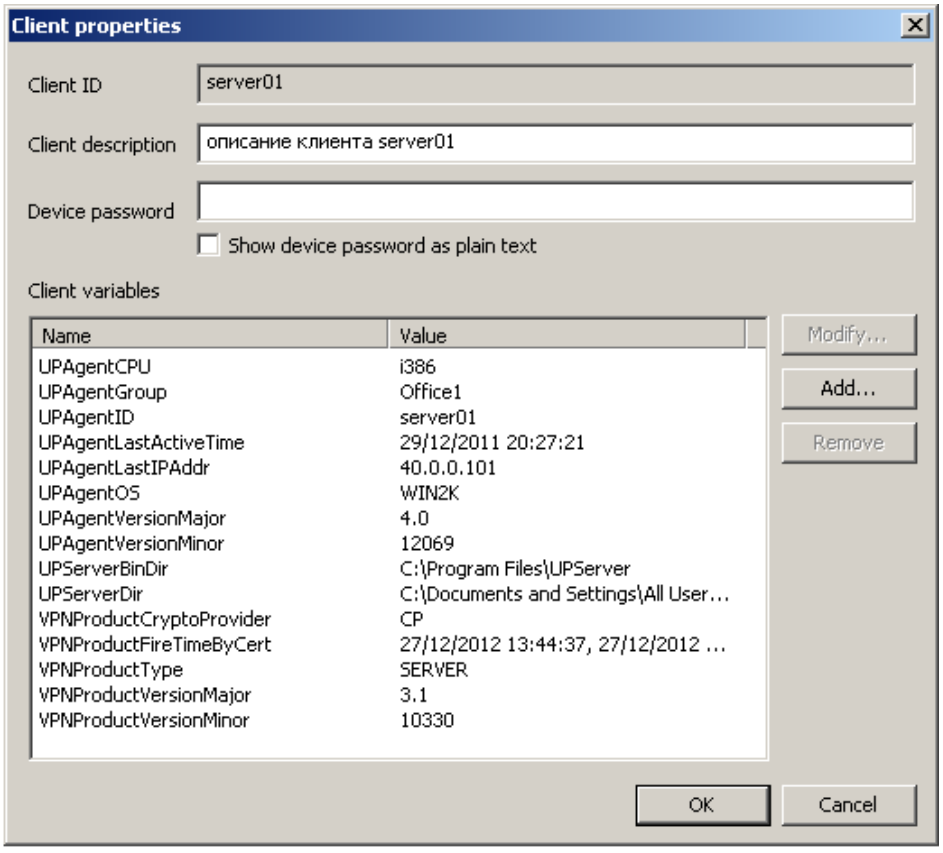


Рисунок 196

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 58)

Update… – вызывает окно **Update client** создания обновления для существующего клиента (Рисунок 197) 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 с данными продукта CSP VPN Gate, созданного с помощью окна **VPN data maker**, вызываемого кнопкой E

Кнопка E – вызывает окно **VPN data maker** (Рисунок 59) для задания политики безопасности и настроек продукта CSP VPN Gate

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.

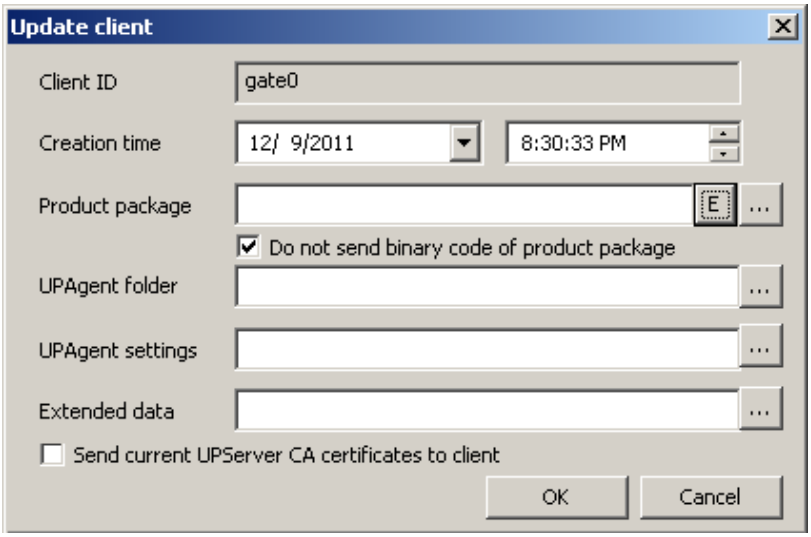


Рисунок 197

Functions – вызывает подменю (Рисунок 198):

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

Remove… -удалить ключевую пару с управляемого устройства, при этом появляется окно **Remove container** (Рисунок 199) 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.

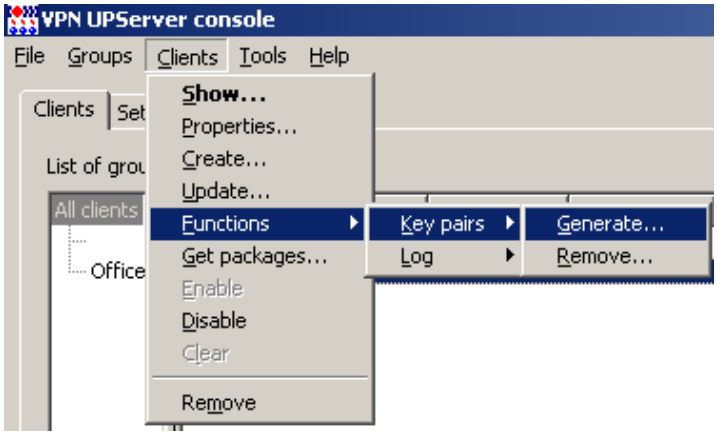


Рисунок 198

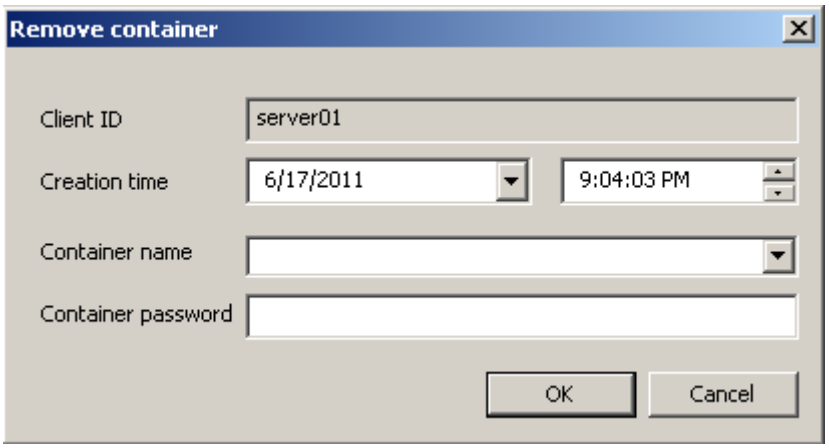


Рисунок 199

Log – позволяет задать настройки протоколирования событий на управляемом устройстве, при этом возможны два действия (Рисунок 200):

Setup… - задать параметры протоколирования в окне **Setup log** (Рисунок 201):

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 ОС Windows

`OFF` – выключить пересылку syslog сообщений в стандартную систему протоколирования ОС 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.

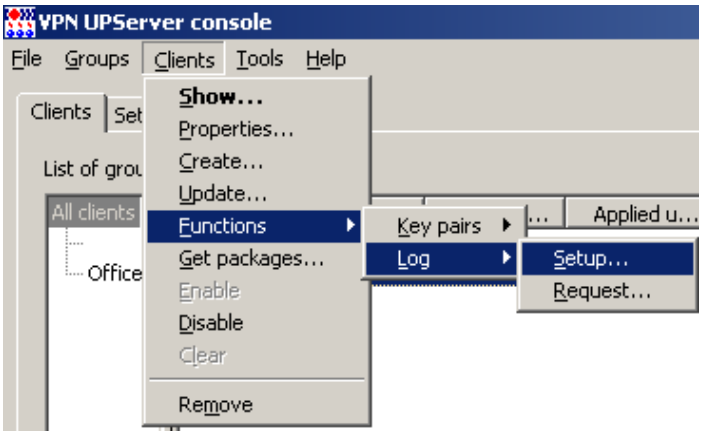


Рисунок 200

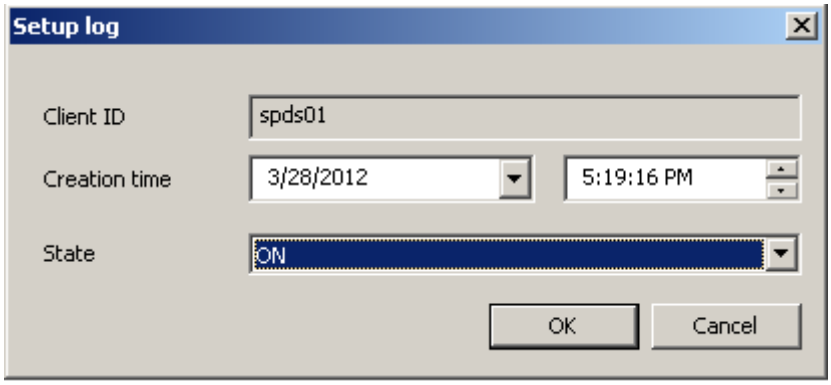


Рисунок 201

Request… - запросить данные из системы протоколирования на управляемом устройстве, заполнив в окне **Request log** (Рисунок 202) 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.

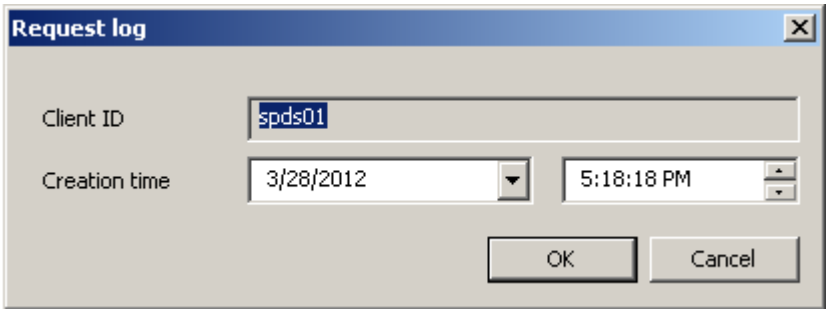


Рисунок 202

Меню Tools

Меню ***Tools*** содержит два предложения VPN data maker и VPN data converter (Рисунок 203):

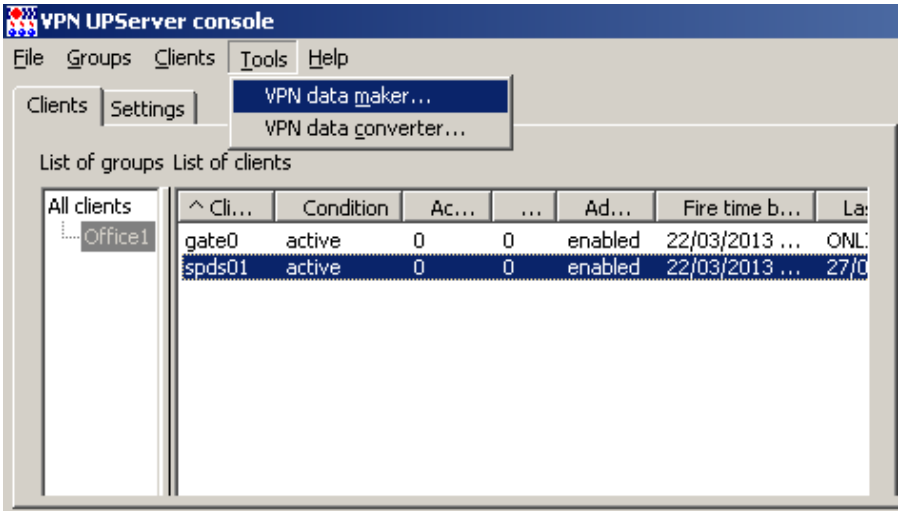


Рисунок 203

Предложение ***VPN data maker*** вызывает одноименное окно **VPN data maker** для задания настроек продукта CSP VPN Gate для нового проекта (Рисунок 204). 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**).

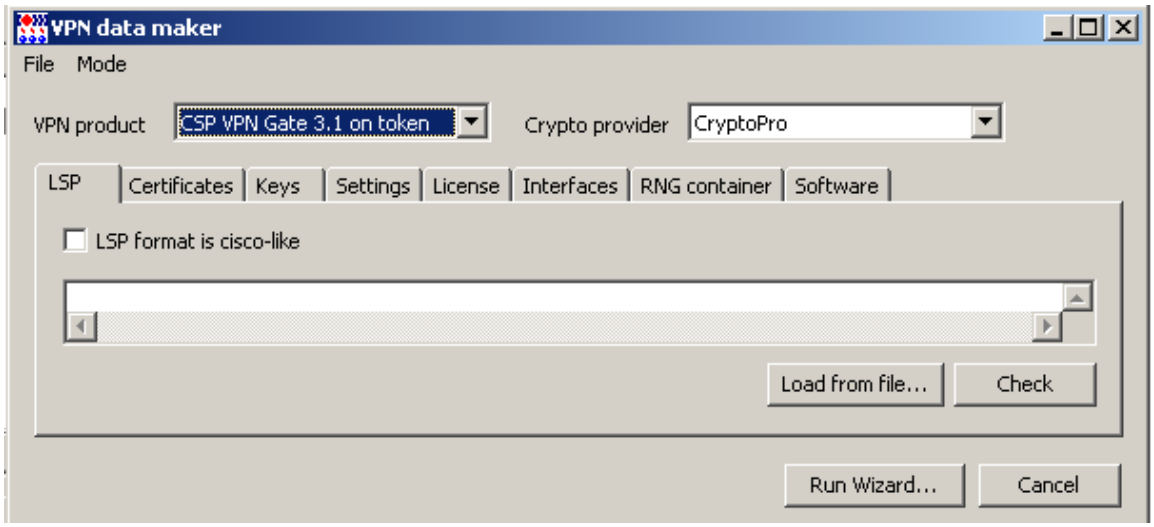


Рисунок 204

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 Gate, предписанной управляемому устройству (Рисунок 204):

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.

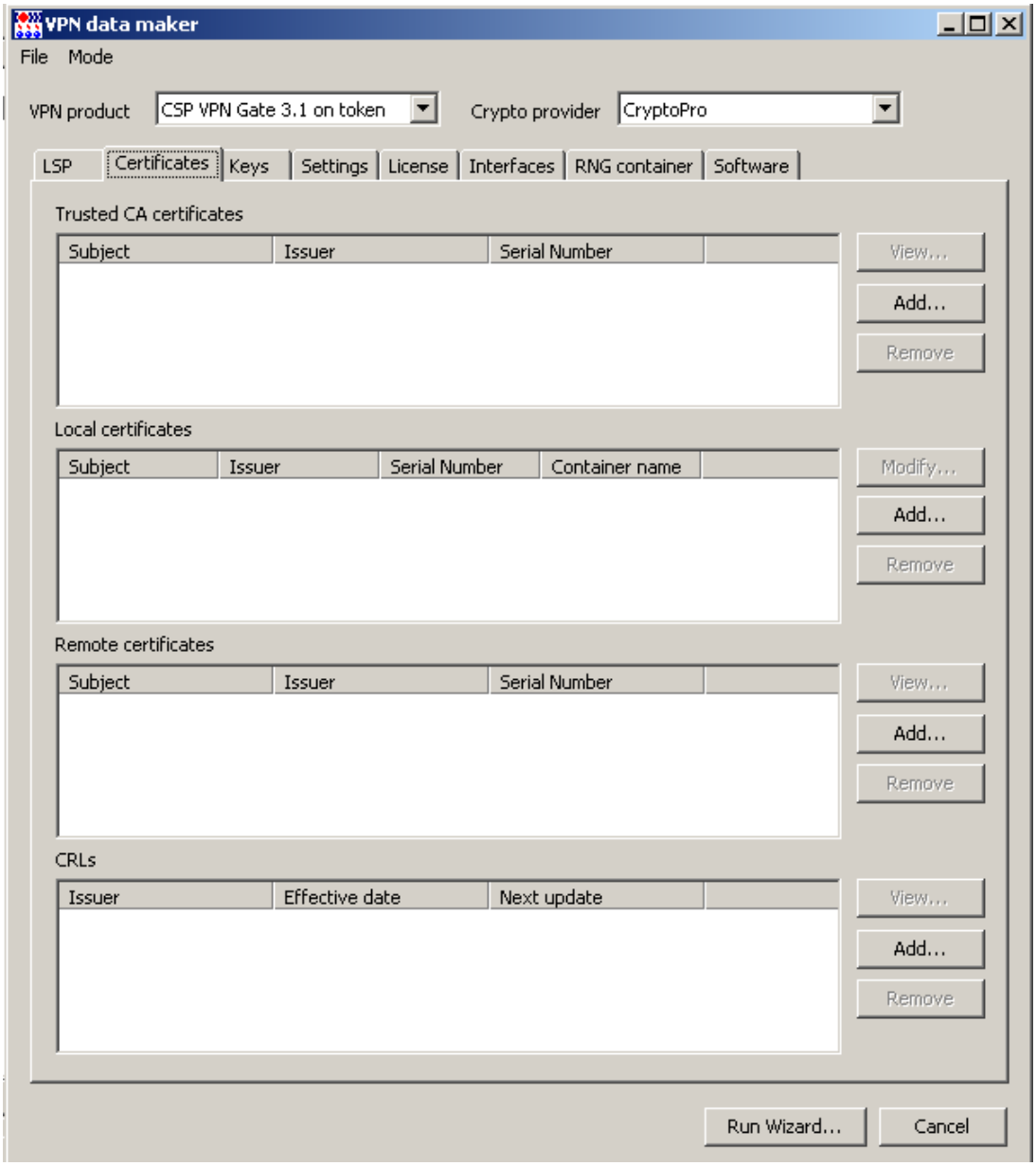


Рисунок 205

Certificates – вкладка для задания CA, локальных, партнерских и списков отозванных сертификатов для продукта CSP VPN Gate (Рисунок 205).

Keys – вкладка для задания предопределенных ключей для работы продукта CSP VPN Gate с партнерами (Рисунок 206).

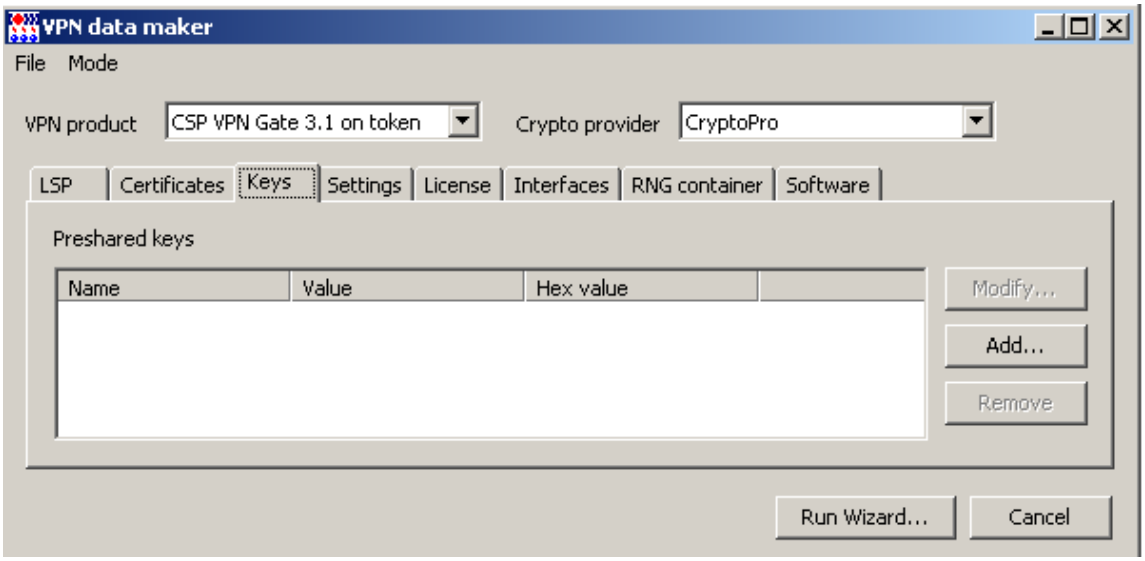


Рисунок 206

Settings – вкладка для задания локальных настроек продукта CSP VPN Gate.

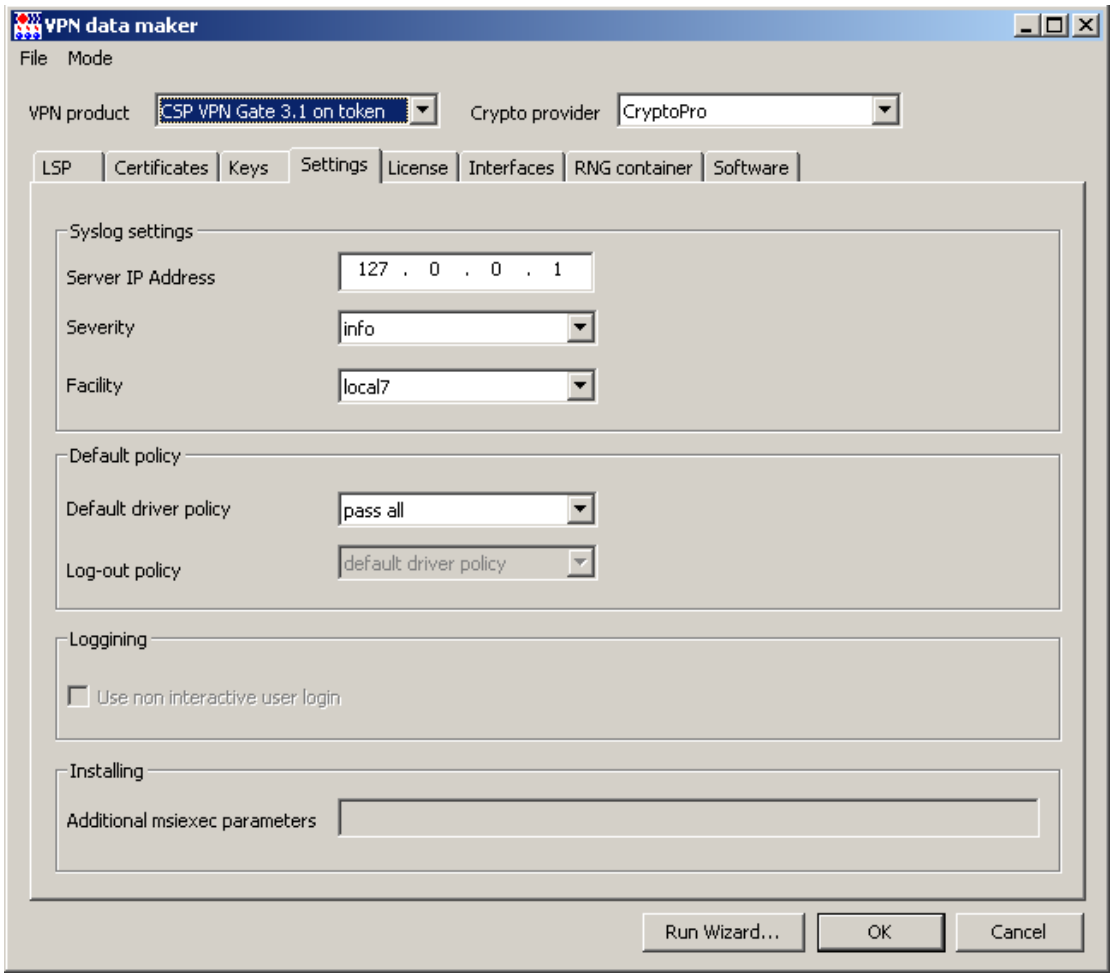


Рисунок 207

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

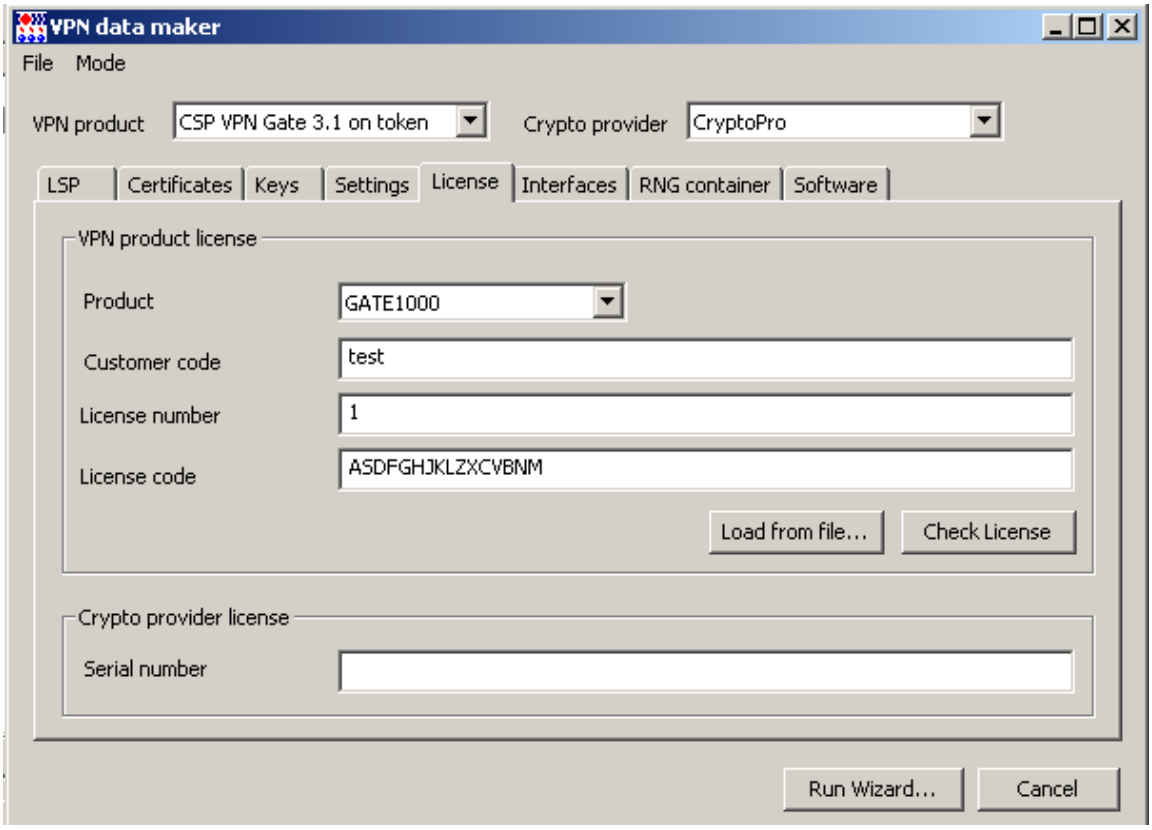


Рисунок 208

Interfaces – вкладка для задания настроек сетевых интерфейсов управляемого устройства (Рисунок 209).

Virtual device address – в это поле вносится адрес, с которым будут проходить пакеты от СПДС «ПОСТ» к партнерам.

Network interface descriptions – при нажатии кнопки Add в этой области появляется окно **Edit connection** для настройки сетевых параметров (Рисунок 211). Эти же настройки можно задать в профайлах, подготавливаемых администратором, и загрузить по кнопке Load. 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`.

Extended routing – в этой области можно прописать маршруты для СПДС «ПОСТ», при задании правил в окнах мастера эти маршруты прописываются автоматически.

Network interface aliases – для СПДС эта область недоступна для заполнения.

Driver settings – установка этого флажка позволяет изменить настройки IPsec драйвера, установленные по умолчанию (Рисунок 210**Ошибка! Источник ссылки не найден.**). Эти настройки имеются только у продукта CSP VPN Gate и описаны в утилите drv_mgr в документе «Специализированные команды», входящем в состав «Программный комплекс CSP VPN Gate. Руководство администратора».

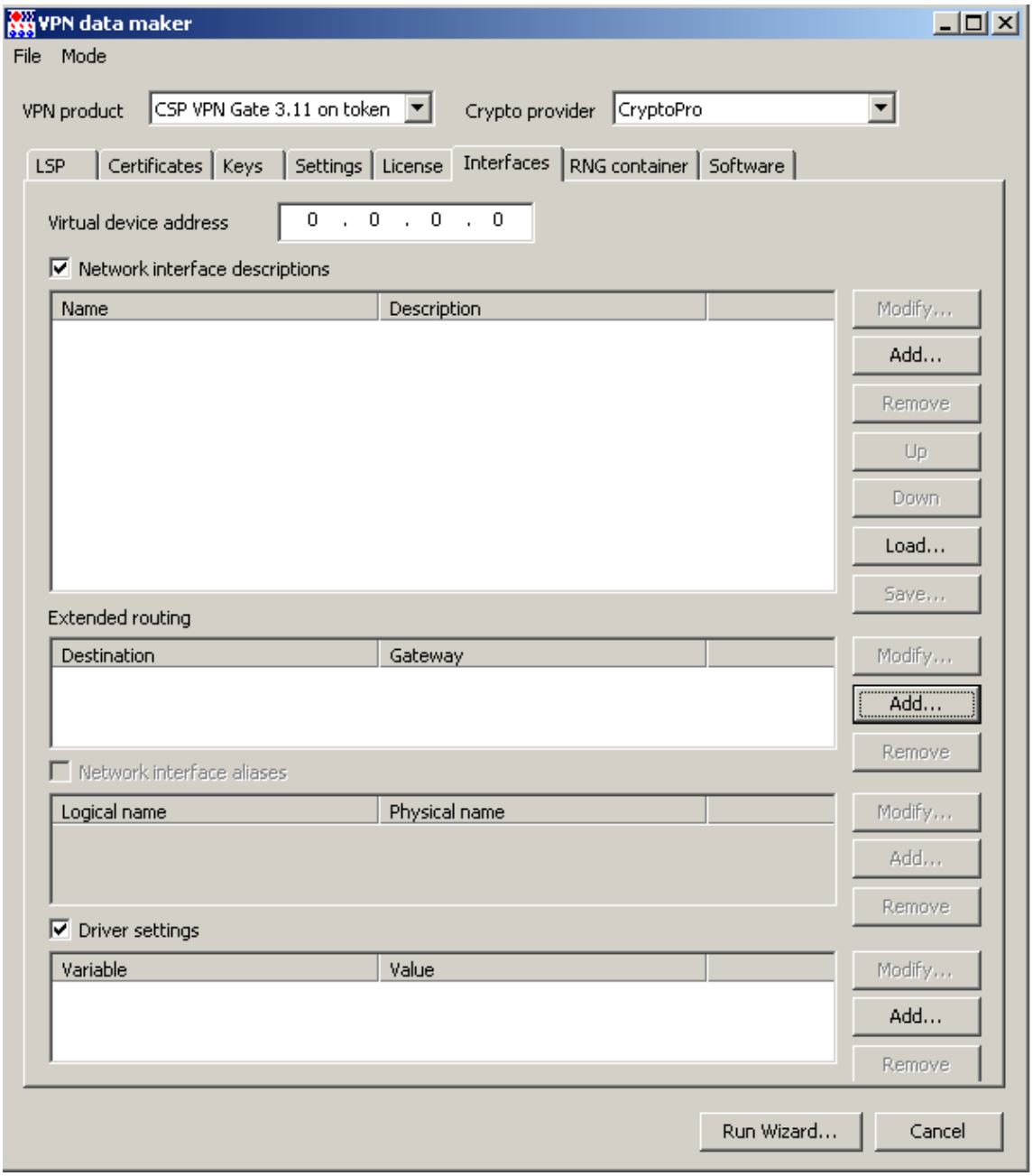


Рисунок 209

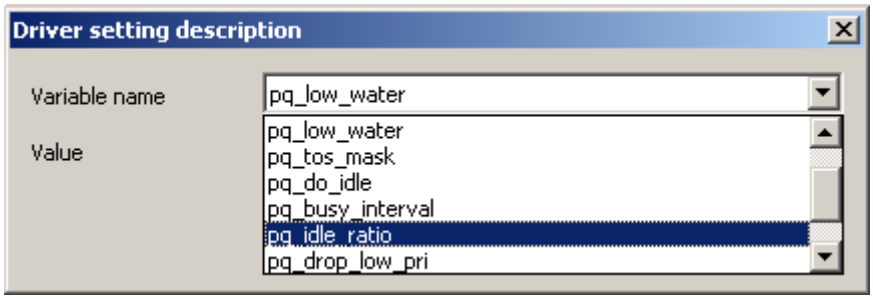


Рисунок 210

Окно Edit connection

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

Проводное соединение (Ethernet)

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

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

Connection ID – идентификатор соединения, свободное текстовое поле.

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

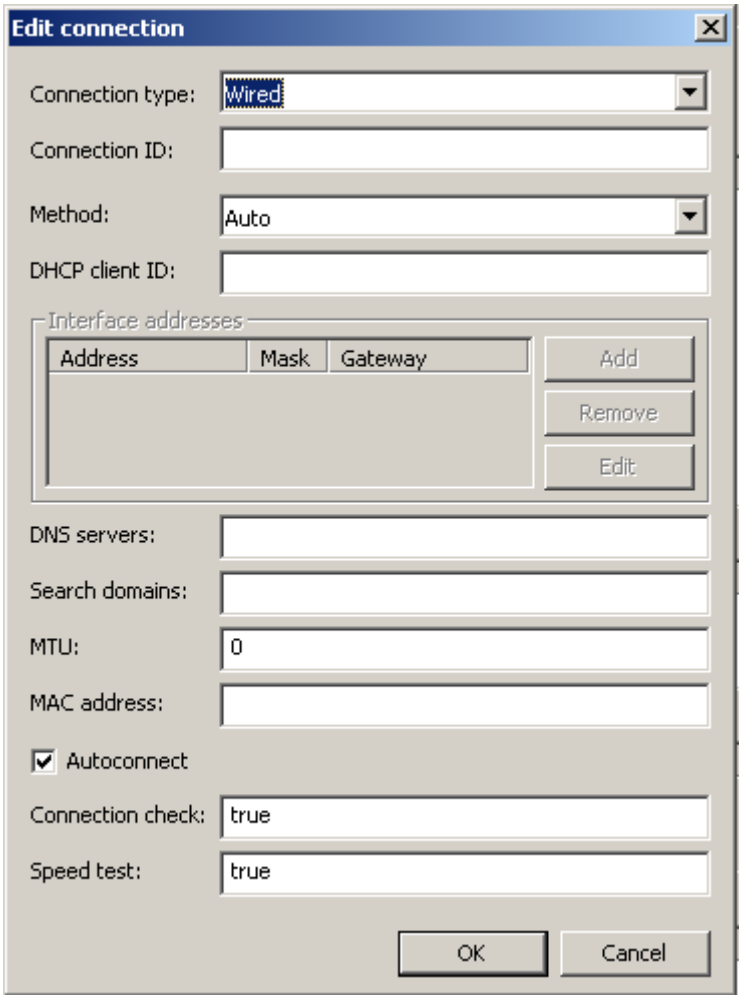


Рисунок 211

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

Interface addresses – область для задания IP-адреса интерфейса СПДС «ПОСТ». 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).

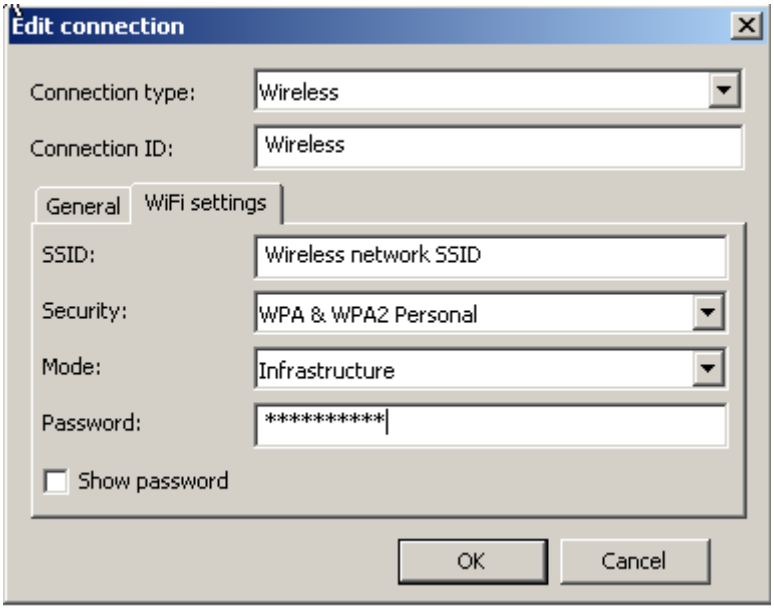


Рисунок 212

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.

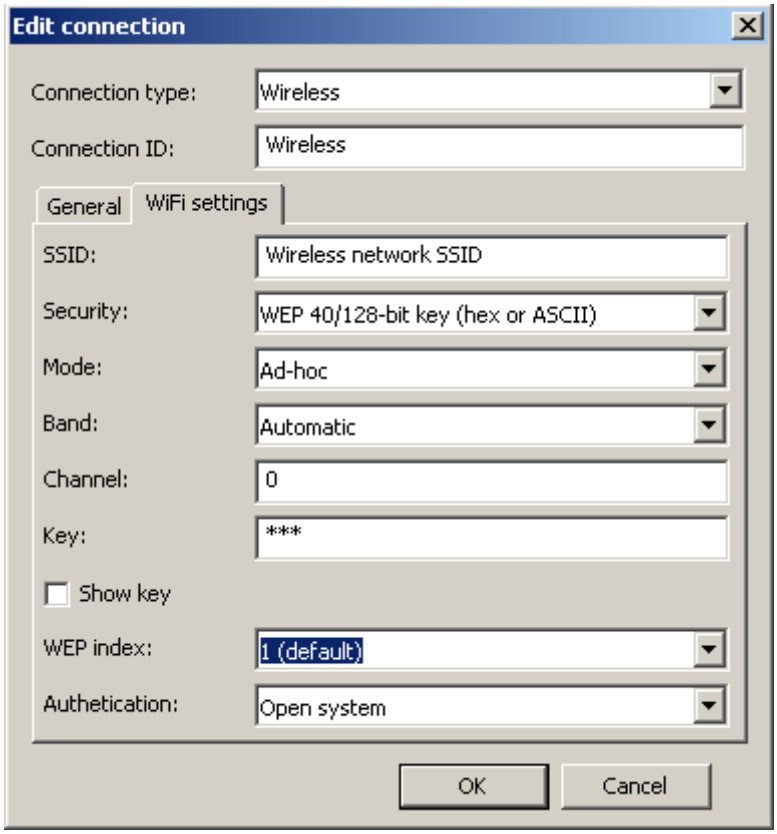


Рисунок 213

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».

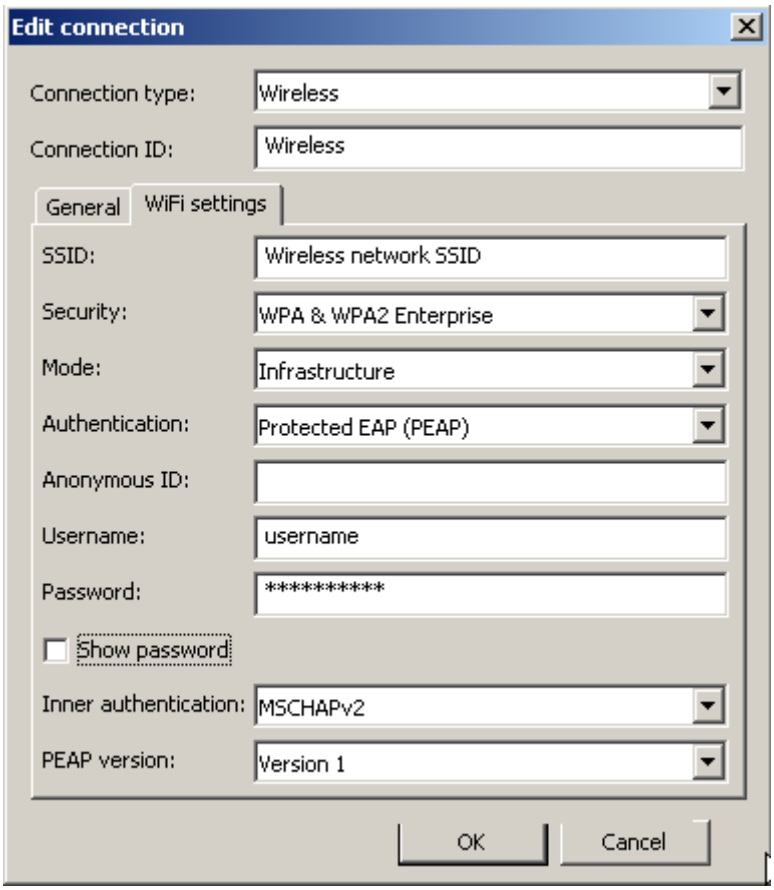


Рисунок 214

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».

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 215). Используется только для криптопровайдера SignalCOM.

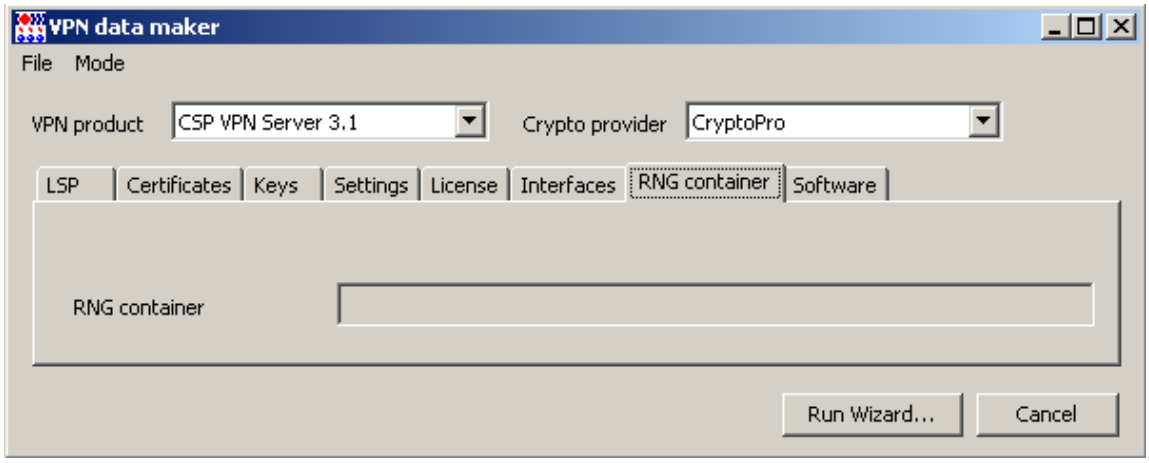


Рисунок 215

Software – вкладка настроек для удаленного доступа к серверам, где СПДС ПОСТ» может выступатьт в качестве RDR, Web или другого клиента (Рисунок 216).

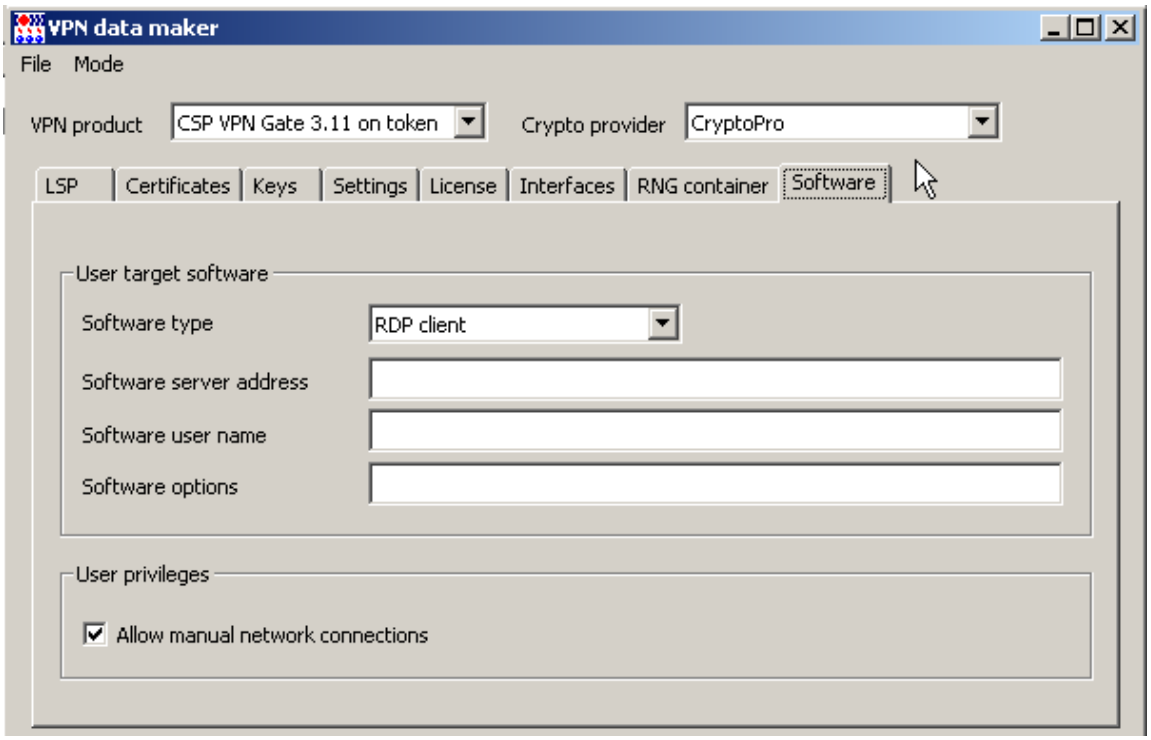


Рисунок 216

Сохранение и загрузка настроек продукта

Меню ***File*** окна **VPN data maker** содержит два предложения (Рисунок 217):

Load – загружает настройки из файла данных продукта CSP VPN Gate, созданные ранее

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

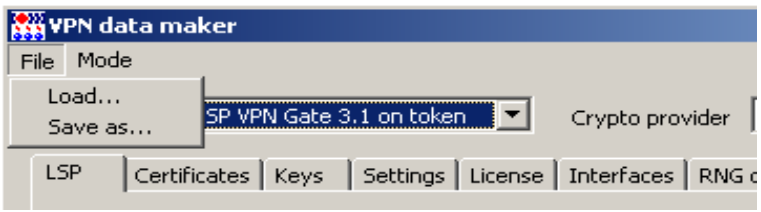


Рисунок 217

Задание политики и настроек с использованием окон мастера

При нажатии кнопки Run Wizard в окне **VPN data maker** появляется окно мастера создания несложной политики безопасности и настроек для управляемого устройства (Рисунок 218).

При выборе аутентификации с использованием сертификатов доступны следующие поля:

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, под которым контейнер будет скопирован на СПДС «ПОСТ». При указании локального сертификата это поле заполняется автоматически.

Device container password – пароль к новому скопированному контейнеру.

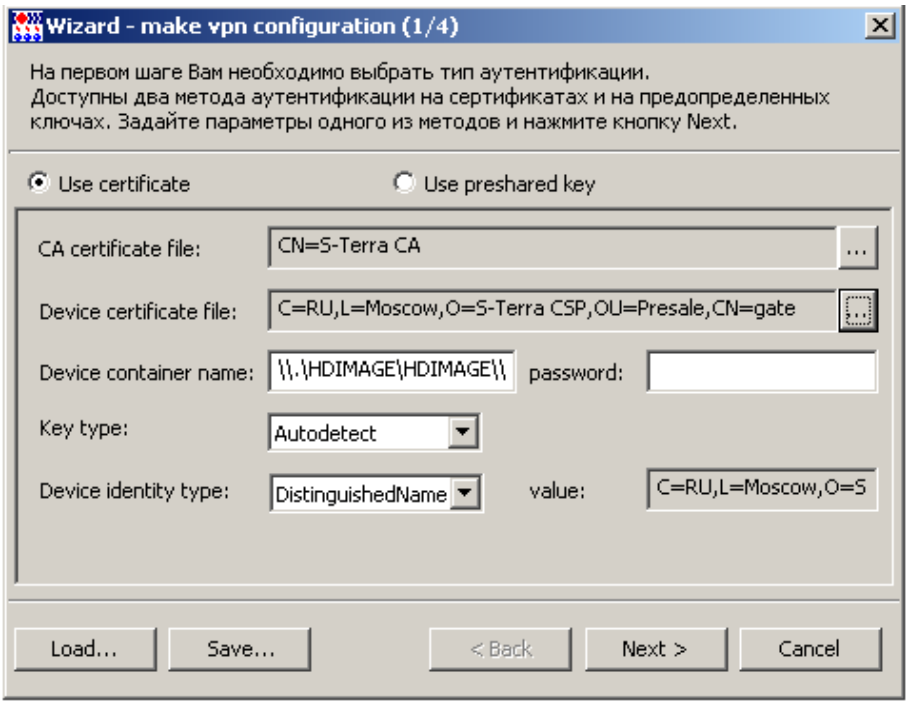


Рисунок 218

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 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.

При выборе аутентификации с использованием предопределенного ключа доступны следующие поля (Рисунок 219):

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.

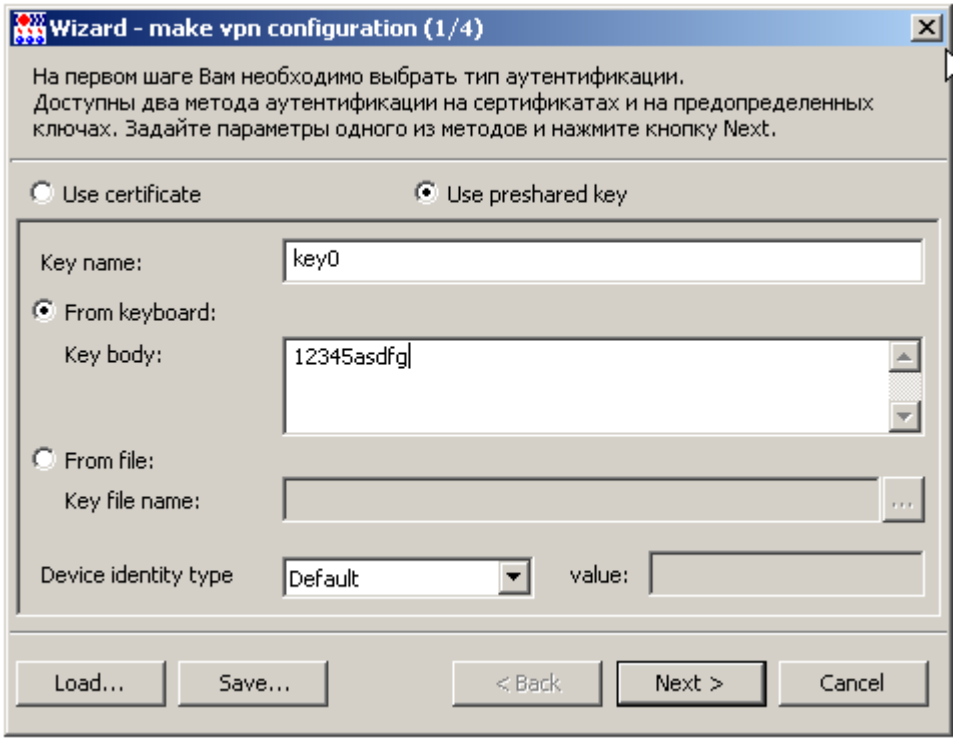


Рисунок 219

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

Задание правил фильтрации и защиты трафика, ввода лицензионной информации были описаны в разделе «Сценарий управления центральным шлюзом».

Конвертирование политики

При выборе предложения ***vpn data converter*** (Рисунок 203) 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.

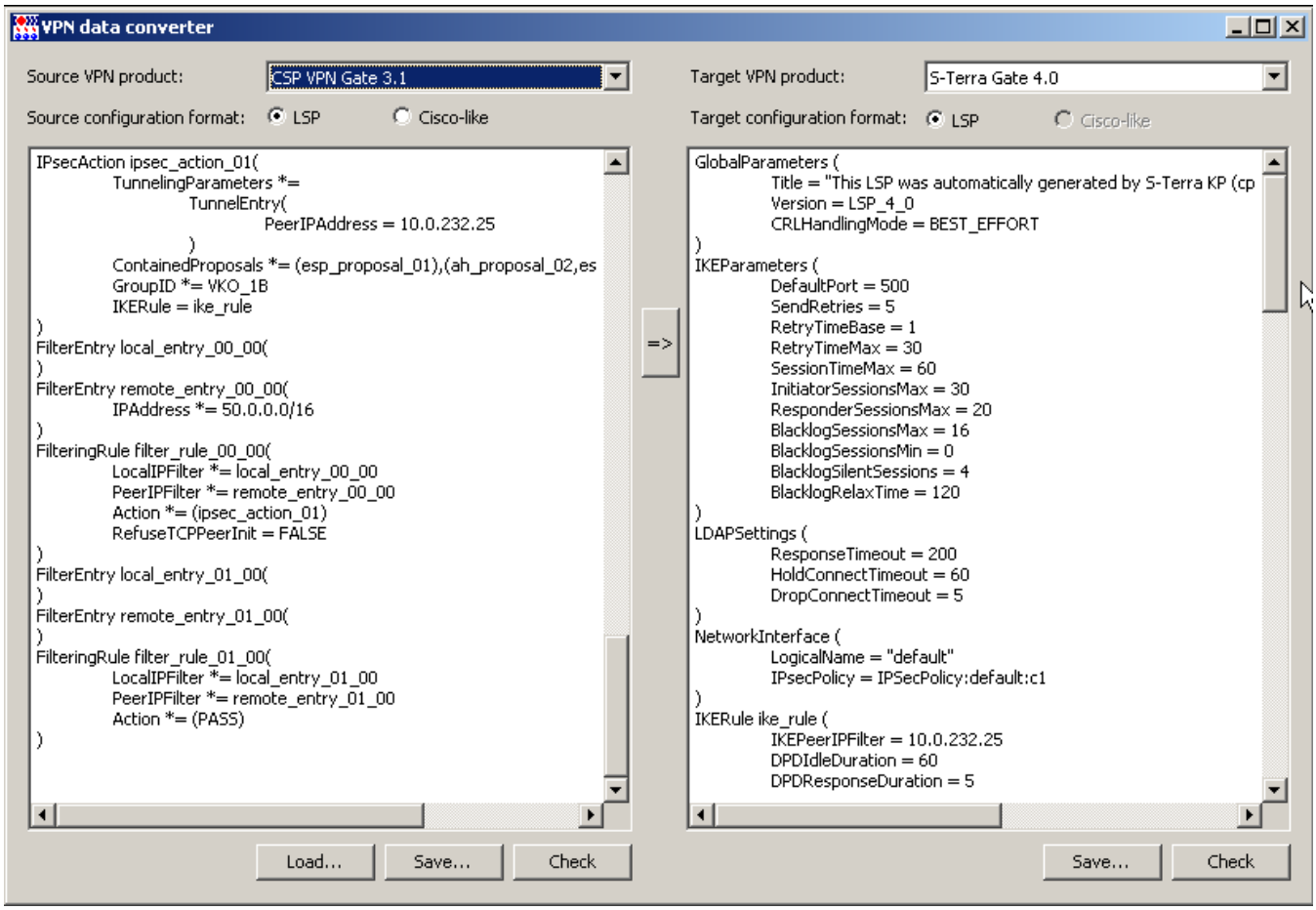


Рисунок 220

Меню Help

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

Рисунок 221

Протоколирование событий

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.`

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.

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».