Построение VPN туннеля между шлюзом безопасности «С-Терра Шлюз» и клиентом «С-Терра Клиент» с аутентификацией при помощи RADIUS сервера

Введение

Данный сценарий содержит пример настойки криптошлюза «С-Терра Шлюз» и ПО «С-Терра Клиент» для обеспечения безопасного взаимодействия между защищаемой подсетью центрального офиса и удаленным VPN-клиентом (компьютером пользователя).

Обеспечение безопасного взаимодействия достигается путем шифрования и туннелирования трафика с применением отечественных отраслевых стандартов ГОСТ и протокола IPsec.

В рамках данного сценария для аутентификации «С-Терра Клиент» помимо сертификата будет использоваться XAuth (расширенная аутентификация в рамках протокола IKE) совместно с RADIUS сервером. В качестве криптопровайдера будет использована криптографическая библиотека, разработанная компанией «С-Терра СиЭсПи». Шлюз безопасности (или криптошлюз) – «С-Терра Шлюз» версии 4.3. VPN-клиент – «С-Терра Клиент» версии 4.3.

Предварительные требования

Требования к материально-техническому обеспечению

Для переноса запросов и сертификатов между криптошлюзами и центром выпуска сертификатов требуется USB Flash накопитель.

Требования к квалификации администратора

Администратор должен обладать обширными знаниями в области сетевой информационной безопасности, иметь опыт работы с аналогичным оборудованием/программным обеспечением, знать и понимать следующие технологии и протоколы: PKI, IPsec, NAT, Firewall, routing, switching.

Требования к инфраструктуре

1. Требования к устройствам.

   1.1. С-Терра Шлюз.

      1.1.1 Устройство С-Терра Шлюз должно быть инициализировано (подробнее на http://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз 4.3 -> «Подключение ПАК и инициализация С-Терра Шлюз на вычислительных системах архитектуры Intel x86-64»).

   1.2. Центр выпуска сертификатов.

      1.2.1 Должен быть настроен центр выпуска сертификатов (удостоверяющий центр, далее УЦ) для IPsec. Устройство с именем Certification_authority на схеме взаимодействия (см. рисунок 1).

      1.2.2 Для выпуска цифровых сертификатов допускается использование встроенного в ОС Windows Server 2008R2 (или новее) удостоверяющего центра совместно с сертифицированным СКЗИ «КриптоПро» CSP 4.0 (или новее).

      Доставка нового списка отозванных сертификатов с удостоверяющего центра на HTTP-сервер должна происходить заблаговременно, до истечения срока действия предыдущего списка.

      1.2.3 Для тестовых целей можно использовать тестовый УЦ от «КриптоПро» (веб-интерфейс: https://www.cryptopro.ru/certsrv/certrqxt.asp).

      Категорически запрещено использование тестового УЦ от «КриптоПро» в производственной (боевой) эксплуатации, так как в данном случае отсутствует возможность контролировать процесс выпуска сертификатов и, соответственно, процедуру аутентификации.

   1.3. Устройство host-behind-hub1.

      1.3.1 На компьютере, устройство host-behind-hub1, расположенным в защищаемой сети центрального офиса, должна быть установлена ОС, поддерживающая стек протоколов TCP/IP.

   1.4. АРМ администратора.

      1.4.1 На АРМ администратора, устройство Admin_workstation, должна быть установлена ОС Windows (поддерживаемые версии 8/8.1/10).

   1.5. Устройство Radius.

      1.5.1 На устройстве Radius должен быть настроен RADIUS сервер, доступный внутри защищаемой сети центрального офиса.

   1.6. Устройство Client1.

1.6.1 На компьютере пользователя (устройство Client1) должна быть установлена ОС Windows (поддерживаемые версии 8/8.1/10).

1.7. HTTP сервер для распространения списка отозванных сертификатов.

1.7.1 Функционирующий HTTP сервер для распространения списка отозванных сертификатов (СОС). Устройство с именем CRL_distribution_point на схеме взаимодействия (см. рисунок 1). Если по объективным причинам использование СОС не представляется возможным или не требуется, то проверку СОС можно отключить в Cisco-like консоли.

Доставка нового списка отозванных сертификатов с удостоверяющего центра на HTTP сервер должна происходить заблаговременно, до истечения срока действия предыдущего списка.

2. Требования к сетевому взаимодействию.

2.1. Между устройствами стенда должна быть обеспечена IP связность.

Схема взаимодействия

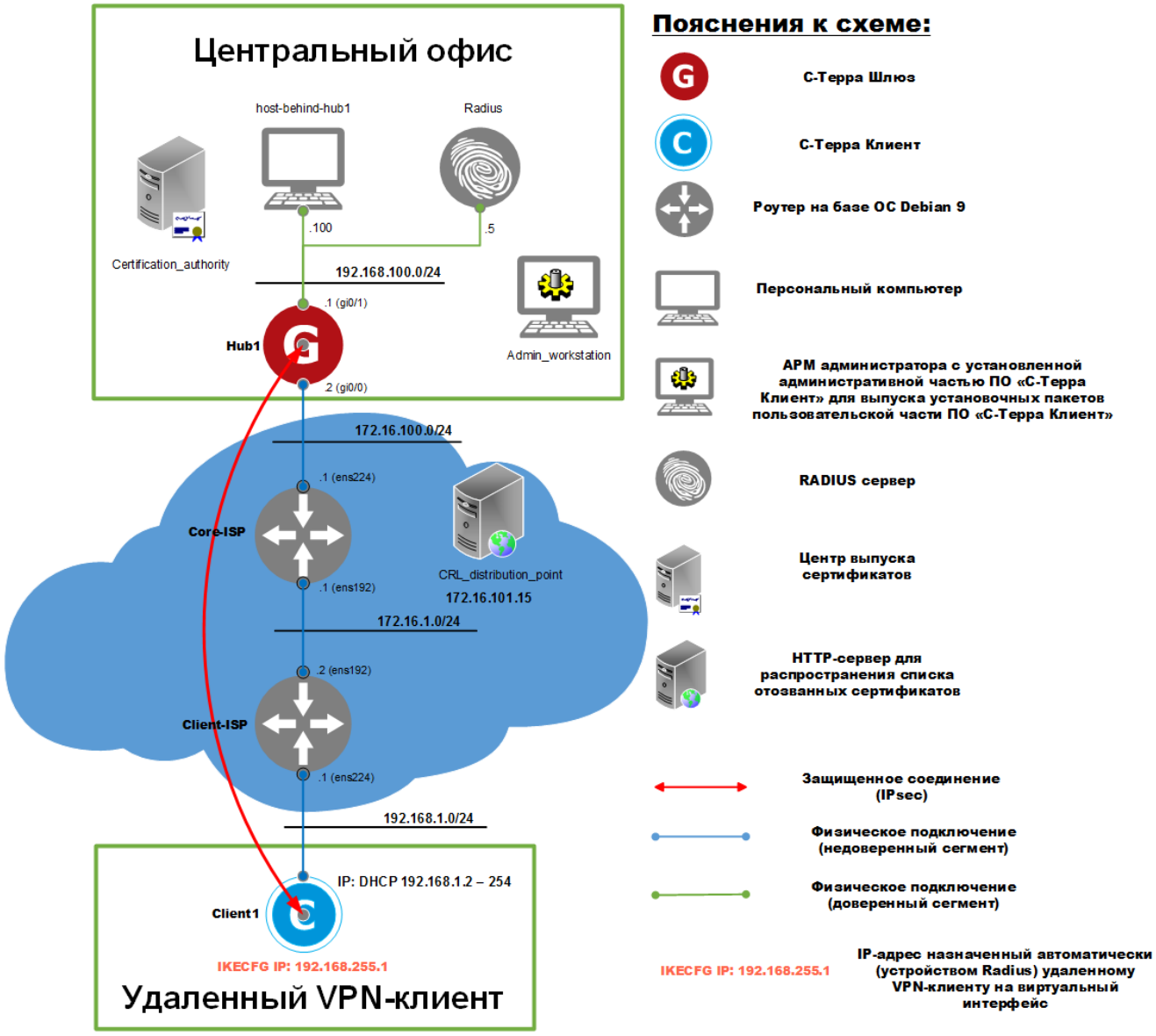

Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), АРМ администратора (Admin_workstation), RADIUS сервер (Radius), криптошлюз С-Терра Шлюз (Hub1) и персональный компьютер (host-behind-hub1).

   1.2. В неконтролируемом сегменте (синее облако на схеме взаимодействия (см. рисунок 1)) размещаются: HTTP сервер для распространения списка отозванных сертификатов (CRL_distribution_point), маршрутизаторы (Core-ISP, Client-ISP).

   1.3. За неконтролируемым сегментом размещается компьютер пользователя с ПО С-Терра Клиент (Client1).

2. Подключение к сети Интернет.
   В данном сценарии для эмуляции сети Интернет используются маршрутизаторы Core-ISP и Client-ISP.

2.1. Криптошлюз Hub1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Core-ISP).

2.2. Компьютер пользователя Client1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Client-ISP).

2.3. На маршрутизаторе Client-ISP происходит трансляция сетевых адресов (source NAT) в IP-адрес внешнего сетевого интерфейса (ens192).

В данном сценарии предполагается, что в центральном офисе не известно о том, в какой IP-адрес будут транслироваться запросы с компьютера пользователя Client1, так как устройство Client1 может находиться в любой части сети Интернет.

3. Параметры безопасного взаимодействия.

Весь IP трафик между подсетью центрального офиса и компьютером пользователя защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном режиме.

При построении IKE-сессии на компьютере пользователя выводится окно «XAuth request dialog». Введенные в окне данные передаются в защищенном виде сначала на криптошлюз Hub1, а далее эти данные криптошлюз пересылает RADIUS серверу для дополнительной аутентификации. При удачной аутентификации происходит построение IKE и IPsec туннелей между клиентом и криптошлюзом. При неудачной аутентификации на клиенте будет выведено окно «XAuth ERROR dialog» с сообщением «Extended authentication failed», а также окно для повторной аутентификации.

Компьютеру пользователя, на специальный виртуальный сетевой интерфейс, будет назначен IP-адрес, посредством механизма IKECFG. Данный IP-адрес, задается на RADIUS сервере (`Framed-IP-Address`). Все взаимодействия между компьютером пользователя и защищаемой подсетью центрального офиса будут осуществляться от этого IP-адреса, а не от IP-адреса, который пользователю был назначен по DHCP от маршрутизатора Client-ISP. Данная настройка используется для того, чтобы избежать совпадения IP-адресов у удаленных клиентов в случае отсутствия возможности осуществлять контроль над адресным пространством компьютеров удаленных клиентов.

Инициировать защищенное соединение в рамках данного сценария возможно только со стороны компьютера пользователя.

В случае если RADIUS сервер не поддерживает Framed-IP-Address, либо по той или иной причине нет возможности его настроить, можно задать IKECFG пул на криптоклюзе Hub1 как в пунктах 2.2 и 2.4.3 сценария Построение VPN туннеля между шлюзом безопасности "С-Терра Шлюз" и клиентом "С-Терра Клиент" на портале документации.
В данном сценарии эта настройка RADIUS сервера приведена в целях демонстрации.

3.1. Параметры протокола IKE:

- Аутентификация при помощи цифровых сертификатов, алгоритм подписи – ГОСТ Р 34.10-2012 (ключ 256 бит);
- Алгоритм шифрования – ГОСТ 28147-89 (ключ 256 бит);
- Алгоритм вычисления хеш-функции – ГОСТ Р 34.11-2012 ТК26 (ключ 256 бит);
- Алгоритм выработки общего ключа (аналог алгоритма Диффи-Хеллмана) – VKO_GOSTR3410_2012_256 (ключ 256 бит).

3.2. Параметры протокола ESP:

- Комбинированный алгоритм шифрования и имитозащиты (контроль целостности) – ESP_GOST-4M-IMIT (ключ 256 бит).

Настройка стенда

Настройка устройства host-behind-hub1

1. Настройте IP адрес – 192.168.100.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.100.1.
3. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Core-ISP

1. Настройте IP адрес – 172.16.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
2. Настройте IP адрес – 172.16.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
3. Разрешите прохождение IP трафика.

Настройка устройства Client-ISP

1. Настройте IP адрес – 172.16.1.2 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 192.168.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Настройте NAT (SNAT либо маскарадинг), транслирующий все адреса сети 192.168.1.0/24 в адрес внешнего интерфейса ens192.
4. Настройте на интерфейсе ens224 DHCP сервер, раздающий доступные IP адреса из подсети этого интерфейса (192.168.1.2 – 192.168.1.254) и требуемые сетевые настройки.
5. Разрешите прохождение IP трафика.

Настройка устройства Radius

1. Настройте IP адрес – 192.168.100.5 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.100.1.
3. Настройте RADIUS сервер для аутентификации и для отправки IP адресов аутентифицированным удаленным VPN-клиентам.

Пример настройки FreeRADIUS (версия ‘3.0.17+dfsg-1.1’ для Debian 10 x64) с краткими пояснениями представлен в Приложении.

Настройка криптошлюза Hub1

Настройка будет происходить локально при помощи консольного подключения.

Настройка может осуществляться и удаленно (по SSH), но исключительно по доверенному каналу связи. Доверенным каналом связи может считаться канал в пределах контролируемой зоны в случае отсутствия в нем нарушителя (в нашем примере это подсеть 192.168.100.0/24).

Начальные настройки

Дата и время на криптошлюзе и компьютере пользователя должны быть одинаковы, так как для аутентификации используются цифровые сертификаты, в которых зафиксированы дата и время начала их действия и окончания. Также одинаковые дата и время на всей инфраструктуре облегчают поиск неисправностей по лог-файлам.

1. Войдите в CLI разграничения доступа. Для этого, после появления сообщения:

   ```
   S-Terra administrative console
   ```

   введите логин и пароль для CLI разграничения доступа:

   Пользователь и пароль по умолчанию: `administrator`, `s-terra`. Обязательно смените пароль для пользователя `administrator` при помощи команды `change user password`.

   ```
   login as: administrator
   ```

   ```
   administrator's password:
   administrator@sterragate]
   ```

2. Установите правильный тип терминала (для `putty` тип терминала `xterm`) и требуемую ширину (для удобства работы), например:

   ```
   administrator@sterragate] terminal terminal-type xterm
   administrator@sterragate] terminal width 150
   ```

3. Установите нужную временную зону и правильные дату и время на криптошлюзе, используя консоль linux bash. Для этого выполните следующие команды.

   3.1. Войдите в linux bash.

   ```
   administrator@sterragate] system
   ```

   ```
   Entering system shell...
   ```

   3.2. Установите нужную временную зону:

   ```
   root@sterragate:~# dpkg-reconfigure tzdata
   ```

   3.3. Установите правильное время и дату (формат – месяц/день/год часы:минуты):

   ```
   root@sterragate:~# date -s "07/04/2019 12:32"
   ```

   ```
   Thu Jul  4 12:32:00 MSK 2019
   ```

4. Установите надежный пароль для пользователя root (под данным пользователем осуществляется доступ по SSH в linux bash):

   ```
   root@sterragate:~# passwd
   ```

   ```
   Enter new UNIX password:
   Retype new UNIX password:
   passwd: password updated successfully
   ```

5. Выйдите из linux bash обратно в CLI разграничения доступа:

   ```
   root@sterragate:~# exit
   ```

```
logout
Leaving system shell...
administrator@sterragate]
```

Начальные настройки завершены.

Настройки PKI (запросы и сертификаты)

Продукт не поддерживает разностные (delta) списки отзыва сертификатов, только базовые. Учитывайте это при выборе или развертывании УЦ.

Для аутентификации партнеров по IPsec можно использовать только цифровые сертификаты, выпущенные при помощи сертифицированного СКЗИ.

Аутентификация по предопределенным ключам запрещена и возможна только в тестовых целях.

Закрытый ключ для сертификата криптошлюза будет сгенерирован при помощи утилиты `cert_mgr` с использованием биологического датчика случайных чисел (БИО ДСЧ). Если на криптошлюзе установлен аппаратный датчик случайных чисел, то для выработки случайных чисел по умолчанию будет использоваться аппаратный датчик. Закрытый ключ может храниться либо на файловой системе устройства, либо на защищенном ключевом носителе (токен). В данном сценарии закрытый ключ будет располагаться в специальном контейнере на файловой системе устройства. Если требуется, чтобы контейнер располагался на токене, то смотрите описание параметра `create` утилиты `cert_mgr` на портале документации http://doc.s-terra.ru.

В момент генерации ключевой пары будет также сгенерирован запрос на локальный сертификат криптошлюза. Данный запрос для его последующей доставки на УЦ будет сохранен на USB Flash накопитель.

Настройка осуществляется в CLI разграничения доступа.

При выполнении сторонних команд в CLI разграничения доступа/консоли cisco-like перед командой нужно указывать ключевое слово `run`. Автодополнение для команд, указываемых после `run` не поддерживается.

1. **Генерация закрытого ключа и запроса на сертификат криптошлюза**.

   1.1. Вставьте USB Flash накопитель в свободный USB порт криптошлюза (накопитель будет автоматически примонтирован).

   1.2. Определите имя (идентификатор) USB Flash накопителя на криптошлюзе:

```
administrator@sterragate] dir media:
    1  dr-x          4096  Wed Mar  4 11:14:41 2020  C4349870349866E8
```

   Имя (идентификатор) USB Flash накопителя - **C4349870349866E8.**

   1.3. Запустите процесс генерации закрытого ключа и запроса на сертификат криптошлюза с сохранением файла запроса на USB Flash накопителе (закрытый ключ остается на криптошлюзе):

```
administrator@sterragate] run cert_mgr create -subj "C=RU,L=Zelenograd,O=S-Terra
CSP,OU=RnD,CN=Hub1" -GOST_R341012_256 -fb64 media:C4349870349866E8/hub1.request
```

   - ключ `-subj` задает отличительное имя сертификата (Distinguished Name, DN);

   Отличительное имя сертификата должно быть уникальным для каждого устройства.

   - ключ `-GOST_R341012_256` задает использование алгоритма подписи – ГОСТ Р 34.10-2012 (ключ 256 бит).

На УЦ для поддержки алгоритма ГОСТ Р 34.10-2012 (ключ 256 бит) должно быть установлено СКЗИ «КриптоПро CSP» версии 4.0 или новее.

- ключ `-fb64` задает месторасположение и формат представления запроса на сертификат; будет использован формат представления BASE64 с сохранением файла запроса в корень USB Flash накопителя под именем `hub1.request`.

Нажимайте предлагаемые клавиши на клавиатуре для инициализации БИО ДСЧ:

```
Progress: [********* ]
Press key: U
```

После завершения работы БИО ДСЧ файл запроса будет сохранен в корне USB Flash накопителя:

```
administrator@sterragate] dir media:C4349870349866E8/
```

```
 1 -rwx 473 Thu Jul  4 10:40:32 2019 hub1.request
```

Настоятельно рекомендуется сохранить контейнер закрытого ключа при помощи утилиты `cont_mgr`. Контейнер может понадобиться в случае восстановления криптошлюза при отказе HDD/SSD диска. Носитель с файлом контейнера нужно хранить в защищенном и недоступном для третьих лиц месте.

1.4. Отмонтируйте и извлеките USB Flash накопитель (посмотреть точки монтирования можно при помощи команды `run mount`):

```
administrator@sterragate] run umount /media/C4349870349866E8
```

2. **Выпуск сертификата криптошлюза на УЦ и импортирование сертификатов УЦ и криптошлюза в базу Продукта**.

2.1. Доставьте файл запроса на УЦ и выпустите по нему сертификат криптошлюза.

2.2. Скопируйте выпущенный сертификат для криптошлюза под именем `hub1.cer` и сертификат УЦ под именем `ca.cer` в корень USB Flash накопителя.

2.3. Вновь вставьте USB Flash накопитель, содержащий файлы сертификатов, в свободный порт USB на криптошлюзе.

2.4. Убедитесь в наличии сертификатов на USB Flash накопителе:

```
administrator@sterragate] dir media:C4349870349866E8/
```

```
 1 -rwx 592 Thu Jul  4 10:40:32 2019 ca.cer
 2 -rwx 804 Thu Jul  4 10:40:32 2019 hub1.cer
 3 -rwx 473 Thu Jul  4 10:40:32 2019 hub1.request
```

Сохраняйте сертификаты. Они могу понадобиться в случае восстановления криптошлюза при отказе HDD/SSD диска.

2.5. Импортируйте сертификат УЦ в базу Продукта:

```
administrator@sterragate] run cert_mgr import -f media:C4349870349866E8/ca.cer -t
```

- ключ `-f` задает месторасположение файла сертификата;
- ключ `-t` используется для импортирования доверенного (trusted) сертификата УЦ.

2.6. Импортируйте сертификат криптошлюза в базу Продукта:

```
administrator@sterragate] run cert_mgr import -f media:C4349870349866E8/hub1.cer
```

2.7. Убедитесь, что сертификаты успешно импортированы в базу Продукта:

```
administrator@sterragate] run cert_mgr show
```

```
Found 2 certificates. No CRLs found.
```

```
1 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
```

Видно, что сертификат УЦ импортирован как **trusted**, а сертификат криптошлюза как **local** (local означает, что для данного сертификата есть соответствующий ключевой контейнер).

2.8. Выполните проверку статуса сертификатов в базе Продукта:

```
administrator@sterragate] run cert_mgr check
```

```
1 State: Inactive C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
                  Certificate can not be verified.
2 State: Inactive C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
                  Certificate can not be verified.
```

Видно, что все сертификаты имеют статус Inactive (неактивный) с пометкой: «Certificate can not be verified» (сертификат не может быть проверен). Причиной этому является включенный по умолчанию в консоли cisco-like механизм проверки списка отозванных сертификатов (далее COC или CRL). Так как в базе Продукта COC отсутствует, поэтому проверка не может быть осуществлена. Далее будет описан процесс настройки автоматической загрузки COC и импортирование его в базу Продукта. Загрузка COC осуществляется по протоколу HTTP с заданной периодичностью.

Настройка паролей доступа к консоли cisco-like

1. Войдите в cisco-like консоль из CLI разграничения доступа:

Пользователь и пароль по умолчанию `cscons`, `csp`. Обязательно смените пароль для пользователя `cscons`, так как под этим пользователем осуществляется доступ по SSH в cisco-like консоль. Также не забудьте сменить `enable` пароль.

```
administrator@sterragate] configure
sterragate login: cscons
```

```
Password:
S-Terra Gate 4.3.XXXXX (amd64)
sterragate#
```

2. Смените пароль для пользователя `cscons` и на `enable`:

```
sterragate#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
sterragate(config)#username cscons secret 0 ПАРОЛЬ
sterragate(config)#enable secret 0 ПАРОЛЬ
```

Настройка сетевых параметров

Изменение состояния интерфейсов и назначение IP адресов применяются сразу после ввода соответствующих команд. Политика безопасности применяются после выхода из режима конфигурирования.

1. Задайте имя устройства:

```
sterragate(config)#hostname Hub1
```

2. Включите внешний `GigabitEthernet0/0` и внутренний `GigabitEthernet0/1` интерфейсы:

```
Hub1(config)#interface range GigabitEthernet 0/0 - 1
Hub1(config-if-range)#no shutdown
Hub1(config-if-range)#exit
```

3. Убедитесь, что интерфейсы административно включены и line protocol (способность интерфейса передавать пакеты в данный момент) находится в состоянии up:

```
Hub1(config)# do show interfaces
```

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware address is 0050.569e.b06d
  MTU 1500 bytes
GigabitEthernet0/1 is up, line protocol is up
  Hardware address is 0050.569e.d3c3
  MTU 1500 bytes
...
```

Если line protocol находится в состоянии down, то проверьте подключение сетевого интерфейса криптошлюза к коммутационному или прочему оборудованию.

4. Задайте IP адреса в соответствии со схемой стенда (см. рисунок 1) на внешнем `GigabitEthernet0/0` и внутреннем `GigabitEthernet0/1` интерфейсах:

```
Hub1(config)#interface GigabitEthernet 0/0
Hub1(config-if)#ip address 172.16.100.2 255.255.255.0
Hub1(config-if)#exit
Hub1(config)#interface GigabitEthernet 0/1
Hub1(config-if)#ip address 192.168.100.1 255.255.255.0
Hub1(config-if)#exit
```

5. Задайте маршрут по умолчанию через устройство Core-ISP:

```
Hub1(config)#ip route 0.0.0.0 0.0.0.0 172.16.100.1
```

6. Проверьте доступность устройства Core-ISP:

```
Hub1(config)#do ping 172.16.100.1
```

```
PING 172.16.100.1 (172.16.100.1) 100(128) bytes of data.
108 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=1.13 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.237 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.192 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.200 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=0.299 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.192/0.411/1.131/0.362 ms
```

Настройка шифрования

1. Параметры IKE.

   1.1. Укажите в качестве типа идентификатора, используемого в рамках протокола IKE, отличительное имя (Distinguished Name, DN):

```
Hub1(config)#crypto isakmp identity dn
```

   По умолчанию отличительное имя будет взято из сертификата устройства, например, для Hub1 это «`C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1`».

   1.2. Настройте параметры DPD (dead peer detection):

```
Hub1(config)#crypto isakmp keepalive 3 2
Hub1(config)#crypto isakmp keepalive retry-count 5
```

   Пояснение:

   Если в течение 3 секунд отсутствует входящий трафик в IPsec туннеле, то с интервалом в 2 секунды посылается 5 keepalive пакетов в рамках IKE туннеля, чтобы удостовериться в работоспособности туннеля. Если партнер не отвечает на keepalive пакеты, то соответствующий

IKE туннель и связанные с ним IPsec туннели уничтожаются. В случае наличия исходящего защищаемого трафика происходит попытка создания новых IKE/IPsec туннелей.

1.3. Включите фрагментацию IKE пакетов:

```
Hub1(config)#crypto isakmp fragmentation
```

1.4. Включите случайный разброс времени жизни IKE и IPsec SA, чтобы снизить нагрузку на шлюз (позволяет избежать единовременное массовое пересоздания SA):

```
Hub1(config)#crypto isakmp security-association lifetime delta 50
```

1.5. Увеличьте допустимое количество одновременно инициируемых IKE сессий (не путать с общим количеством IKE сессий) для всех партнёров (значение по умолчанию 30):

```
Hub1(config)#crypto isakmp initiator-sessions-max 100
```

1.6. Увеличьте допустимое количество одновременных IKE обменов, проводимых шлюзом со всеми партнерами в качестве ответчика (не путать с общим количеством IKE сессий; значение по умолчанию 20):

```
Hub1(config)#crypto isakmp responder-sessions-max 100
```

1.7. Создайте политику, описывающую параметры IKE туннеля:

```
Hub1(config)#crypto isakmp policy 1
Hub1(config-isakmp)#encryption gost
Hub1(config-isakmp)#hash gost341112-256-tc26
Hub1(config-isakmp)#authentication gost-sig
Hub1(config-isakmp)#group vko2
Hub1(config-isakmp)#exit
```

Рекомендуется использовать одну политику для IKE туннелей. Несколько политик может потребоваться в том случае, если необходимо обеспечить совместимость со старыми версиями Продуктов, в которых нет поддержки новых алгоритмов.

2. Настройте взаимодействие с RADIUS сервером:

```
Hub1(config)#aaa new-model
Hub1(config)#aaa authentication login RADIUS1 group radius
Hub1(config)#radius-server host 192.168.100.5 auth-port 1812 acct-port 1813
Hub1(config)#radius-server key secret1
```

Пояснение:

- `RADIUS1` – наименование списка методов аутентификации для использования в криптокарте;
- `192.168.100.5` – IP-адрес RADIUS сервера, `1812` – порт для аутентификации и авторизации (по умолчанию - 1645), `1813` – UDP порт, используемый внешним RADIUS сервером для учёта активности IPsec соединений (по умолчанию – 1646);
- `secret1` – пароль для аутентификации шлюза на RADIUS сервере.

В случае необходимости можно задать сообщение, которое будет выводиться в окне аутентификации XAuth, которое впоследствии появится на компьютере пользователя (см. рисунок 10):

```
Hub1(config)#aaa authentication banner "Put your message here"
```

Вместо «Put your message here» введите требуемое сообщение.

3. Параметры IPsec.

3.1. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика:

```
Hub1(config)#crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-
imit
Hub1(cfg-crypto-trans)#exit
```

3.2. Создайте список доступа (ACL) для трафика, который нужно защищать между центральным офисом и клиентами:

```
Hub1(config)#ip access-list extended IPSEC_ACL_HUB1_AND_CLIENTS
Hub1(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.255.0 0.0.0.255
Hub1(config-ext-nacl)#exit
Hub1(config)#
```

Пояснение:

Диапазон `192.168.255.0 0.0.0.255` соответствует общему диапазону IP адресов, выдаваемых RADIUS сервером (устройство Radius).

3.3. Создайте динамическую криптокарту (имя DMAP, раздел 1):

```
Hub1(config)#crypto dynamic-map DMAP 1
```

3.3.1 Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_AND_CLIENTS
```

3.3.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

```
Hub1(config-crypto-map)#set transform-set GOST_ENCRYPT_AND_INTEGRITY
```

3.3.3 Привяжите список методов аутентификации к криптокарте:

```
Hub1(config-crypto-map)#set client authentication list RADIUS1
```

3.3.4 Включите поддержку XAuth:

```
Hub1(config-crypto-map)#set client authentication xauth
```

При наличии настроенной связки RADIUS + OTP к команде можно добавить опцию «`otp`» (`set client authentication xauth otp`). В таком случае при аутентификации XAuth в том же окне будет запрашиваться одноразовый пароль.
Если связка настроена с использованием механизма Access-Challenge опцию использовать не следует. В таком случае одноразовый пароль будет запрошен в отдельном окне после аутентификации RADIUS. На Hub1 тогда рекомендуется в LSP в «IKEParameters» добавить значение «SessionTimeMax = 130». В противном случае на заполнение полей в двух окнах будет в общей сложности даваться 60 секунд.

3.3.5 Если в сети центрального офиса есть локальный DNS сервер, укажите его адрес в динамической криптокарте, чтобы у удаленного клиента была возможность им воспользоваться:

```
Hub1(config-crypto-map)#set dns <IP_адрес_DNS_сервера>
```

3.3.6 Включите механизм RRI:

```
Hub1(config-crypto-map)#reverse-route
```

3.3.7 Обязательно отключите историю удаленных туннелей (если не отключить, то могут быть проблемы с построением IPsec туннелей с устройствами, которые находятся за NAT):

```
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#exit
```

3.4. Создайте статическую криптокарту и привяжите к ней динамическую:

```
Hub1(config)#crypto map VPN 1 ipsec-isakmp dynamic DMAP
```

3.5. Прикрепите созданную криптокарту `VPN` к внешнему интерфейсу `GigabitEthernet0/0`:

```
Hub1(config)#interface GigabitEthernet0/0
Hub1(config-if)#crypto map VPN
```

3.6. Примените настройки:

```
Hub1(config-if)#end
```

Настройка политики обработки COC (CRL)

В целях безопасности настоятельно рекомендуется включать проверку списков отзыва сертификатов. Разностные списки отозванных сертификатов (delta CRL) не поддерживаются.

1. Включите проверку COC:

```
Hub1#configure terminal
Hub1(config)#crypto pki trustpoint s-terra_technological_trustpoint
Hub1(ca-trustpoint)#revocation-check crl
```

   Если по обоснованным причинам использование COC невозможно, то выключите проверку COC и **не включайте автоматическую загрузку COC**:

```
Hub1(ca-trustpoint)#revocation-check none
```

2. Включите автоматическую загрузку и импортирование в базу Продукта списка отозванных сертификатов с HTTP сервера CRL_distribution_point:

```
Hub1(ca-trustpoint)#crl download group ROOTCA http://172.16.101.15/certcrl.crl
```

3. Настройте периодичность загрузки COC в 60 минут (по умолчанию 24 часа):

```
Hub1(ca-trustpoint)#crl download time 60
```

4. Примените настройки:

```
Hub1(ca-trustpoint)#end
```

5. Проверьте загружен ли COC в базу Продукта:

```
Hub1#run cert_mgr show
```

```
Found 2 certificates. Found 1 CRL.
1 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
3 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

   Если COC не загрузился, то проверьте файл журнала, например:

```
Hub1#run grep getcrls_daemon /var/log/cspvpngate.log
```

   Примечание: чтобы не ждать следующего периода загрузки COC можно перезапустить сервис getcrls вручную:

```
Hub1#run systemctl restart getcrls.service
```

6. Выполните проверку статуса сертификатов в базе Продукта:

```
Hub1#run cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
```

   Настройка криптошлюза Hub1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст консоли cisco-like;
- текст LSP.

Создание установочного пакета «С-Терра Клиент» и настройка компьютера пользователя Client1

Для того чтобы сконфигурировать компьютер пользователя, нужно выполнить следующие действия:

- установить приложение AdminTool на компьютере администратора;
- получить запрос на сертификат (на основе нового контейнера с ключами) на компьютере администратора;
- перенести запрос на УЦ, получить сертификат из запроса и перенести сертификат на компьютер администратора;
- сформировать установочный пакет для целевого клиентского компьютера с помощью AdminTool;
- перенести пакет и установить его на компьютер пользователя.

Предполагается, что формирование установочного пакета будет происходить на компьютере администратора. Контейнеры с ключами будут генерироваться также на компьютере администратора. На базе сгенерированных ключей будут выпускаться запросы на сертификаты. Запросы на сертификаты будут переданы на УЦ и на их основе будут получены сертификаты.

Настройка АРМ администратора Admin_workstation

Установка С-Терра AdminTool

1. Вставьте носитель с дистрибутивом ПО «С-Терра Клиент» (должен быть в комплекте поставки) в дисковод.
2. Создайте директорию с именем S-Terra_Client_ST_KC1_KC2 на диске C:\.
3. Перейдите в директорию S-Terra_Client_ST_KC1_KC2, расположенную в корне носителя с дистрибутивом, и разархивируйте архив S-Terra_Client_ST_KC1_KC2.zip в созданную ранее директорию C:\S-Terra_Client_ST_KC1_KC2.
4. Прейдите в директорию C:\S-Terra_Client_ST_KC1_KC2 и запустите `setup.exe`.
5. В появившемся окне нажмите кнопку **Next**.
6. В окне **License Agreement** установите переключатель в положение в **I accept the license agreement** и нажмите кнопку **Next**.
7. В окне **Destination Folder** нажмите кнопку **Next**.
8. В окне **Ready to install the Application** нажмите кнопку **Next**.
9. В окне **Random Number Generation** вводите предлагаемые символы.
10. Дождитесь завершения установки и нажмите кнопку **Finish**.

Установка С-Терра AdminTool на АРМ администратора завершена.

Генерация ключевой пары и запроса на сертификат

1. Создайте запрос на сертификат с помощью утилиты `excont_mgr`, входящей в состав AdminTool

   1.1. Запустите командую строку от имени Администратора

   1.2. Перейдите в директорию, где установлен AdminTool:

   ```
   cd "C:\Program Files (x86)\S-Terra Client AdminTool st"
   ```

   1.3. Создайте запрос на сертификат. При этом будет создан новый контейнер с ключами.

   ```
   C:\Program Files (x86)\S-Terra Client AdminTool st> .\excont_mgr.exe create_req -subj
   "C=RU,O=S-Terra CSP,OU=Research,CN=Client1" -GOST_R341012_256 -kc file_p15://Client1
   -kcp 1234 -fo C:\Client1.req
   ```

   - ключ `create_req` – создает запрос на сертификат;
   - ключ `–subj` задает отличительное имя сертификата (Distinguished Name, DN);

- ключ `-GOST_R341012_256` задает использование алгоритма подписи – ГОСТ Р 34.10-2012 (ключ 256 бит);
- `-kc <имя контейнера>` – задает имя контейнера;
- `-kcp <PIN>` – задает пароль на контейнер;
- `-fo <путь до файла>` – указывает путь, по которому будет сохранен запрос на сертификат.

Ключ `-GOST_R341012_256` предполагает использование ГОСТ 2012. На УЦ для его поддержки должно быть установлено СКЗИ «КриптоПро CSP» версии 4.0 или новее. При необходимости, можно воспользоваться более старым ключом `-GOST_R3410EL`.

Получение сертификатов

Созданный запрос перенесите на УЦ и получите на его основе пользовательский сертификат. Также получите сертификат данного УЦ. Перенесите сертификат УЦ и пользовательский сертификат на компьютер администратора.

Сертификат УЦ должен доставляться доверенным способом.

Создание установочного пакета для Client1

1. Запустите установленное приложение Package Maker из пакета AdminTool.
2. Во вкладке Auth выполните следующие действия (см. рисунок 2):

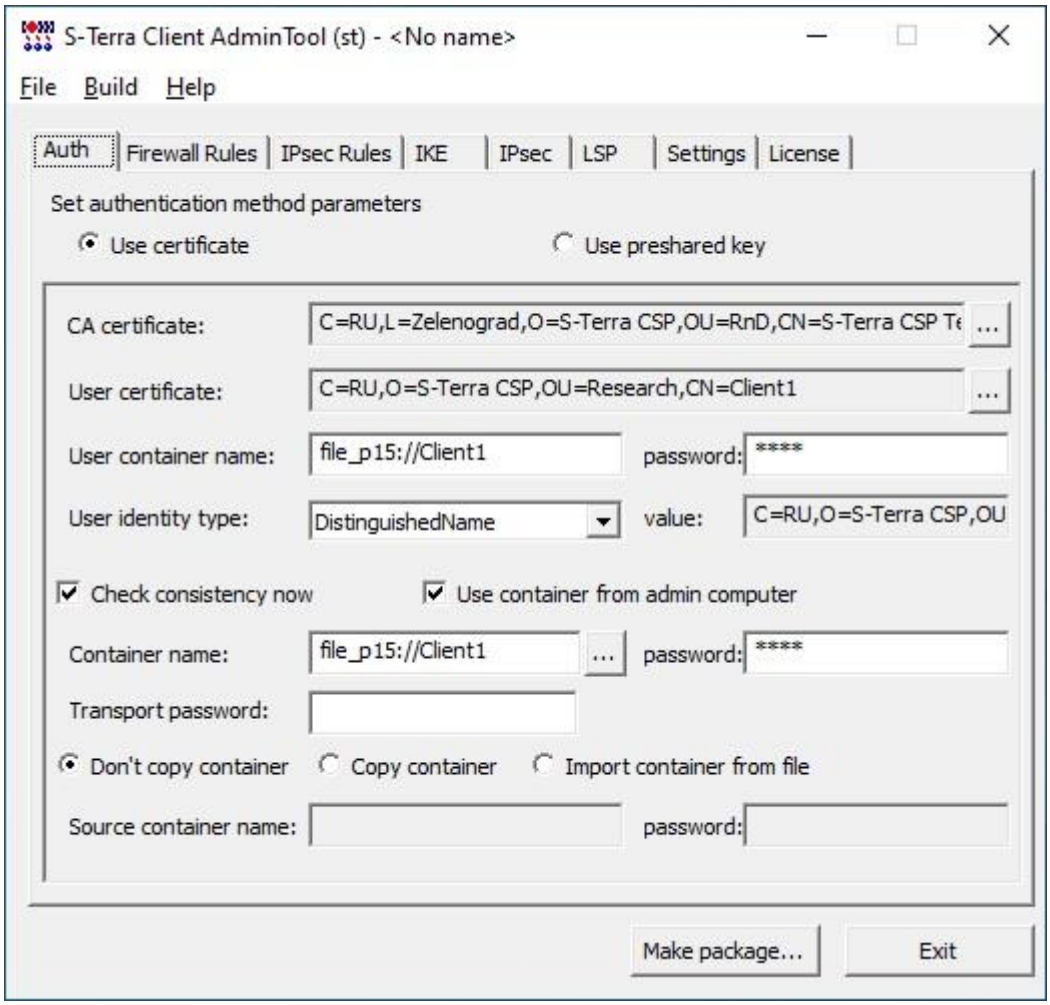

Рисунок 2. Вкладка Auth утилиты AdminTool

2.1. В данном сценарии используется метод аутентификации на сертификатах – переключатель установлен на **Use certificate** по умолчанию.

2.2. Укажите путь к сертификату УЦ (**CA certificate**) и пользовательскому сертификату (**User certificate**).

2.3. Отметьте флаг **Check consistency now** и нажмите кнопку **"..."** рядом с полем **Container name**, где выберите созданный ранее контейнер. Если при создании запроса на сертификат указывался пароль на контейнер, введите его в поле **password**.

2.4. Отметьте флаг **Use container from admin computer**. Указанный в запросе на сертификат контейнер (п.1.3) будет помещен в установочный пакет.

2.5. Задайте имя контейнера в поле **User container name.** В данном случае указано – `file_p15://Client1`. Данное поле указывает по какому пути искать контейнер при работе. Контейнер, указанный в поле **Container name** будет скопирован по указанному пути. Пароль в поле **password** можно указать отличный от указанного рядом с **Container name**.

2.6. В поле **User identity type** необходимо использовать **DistiguishedName** (выбрано по умолчанию).

3. Во вкладке **Firewall Rules** (см. рисунок 3) можно настроить правила фильтрации трафика. В данном сценарии оставьте настройки по умолчанию - разрешать весь трафик.

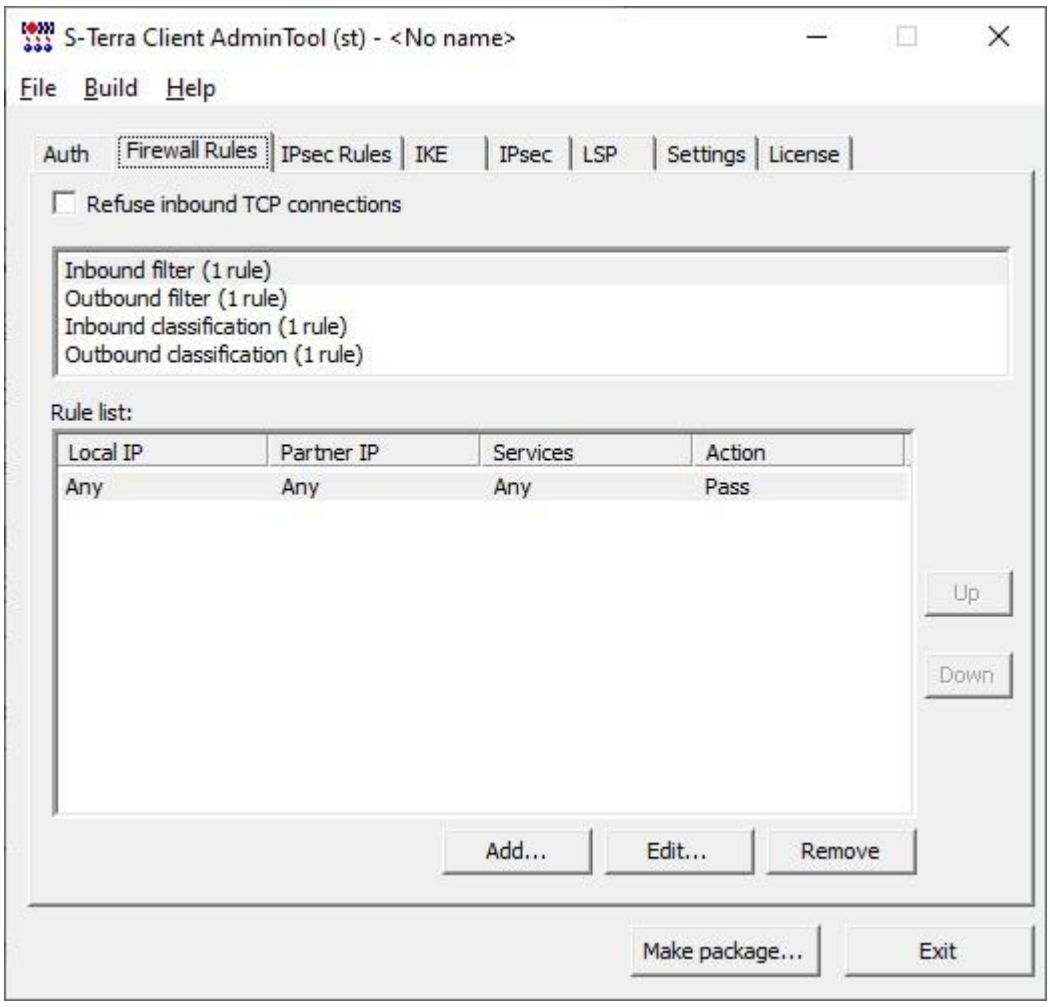

Рисунок 3. Вкладка Firewall Rules утилиты AdminTool

4. Вкладка **IPsec Rules**:

4.1. Добавьте правило для трафика, подлежащего шифрованию. Нажмите кнопку **Add…** и в открывшемся окне **Add Rule** проведите следующие настройки (см. рисунок 4):

4.1.1 В разделе **Partner IP Address** укажите адрес 192.168.100.0 и маску – 255.255.255.0 (выбрав **Custom**).

4.1.2 В разделе **Action** выберите из списка **Protect using IPsec**, нажмите кнопку **Add…** и укажите адрес шлюза Hub1 – 172.16.100.2 и отметьте флаг **Request IKECFG address**.

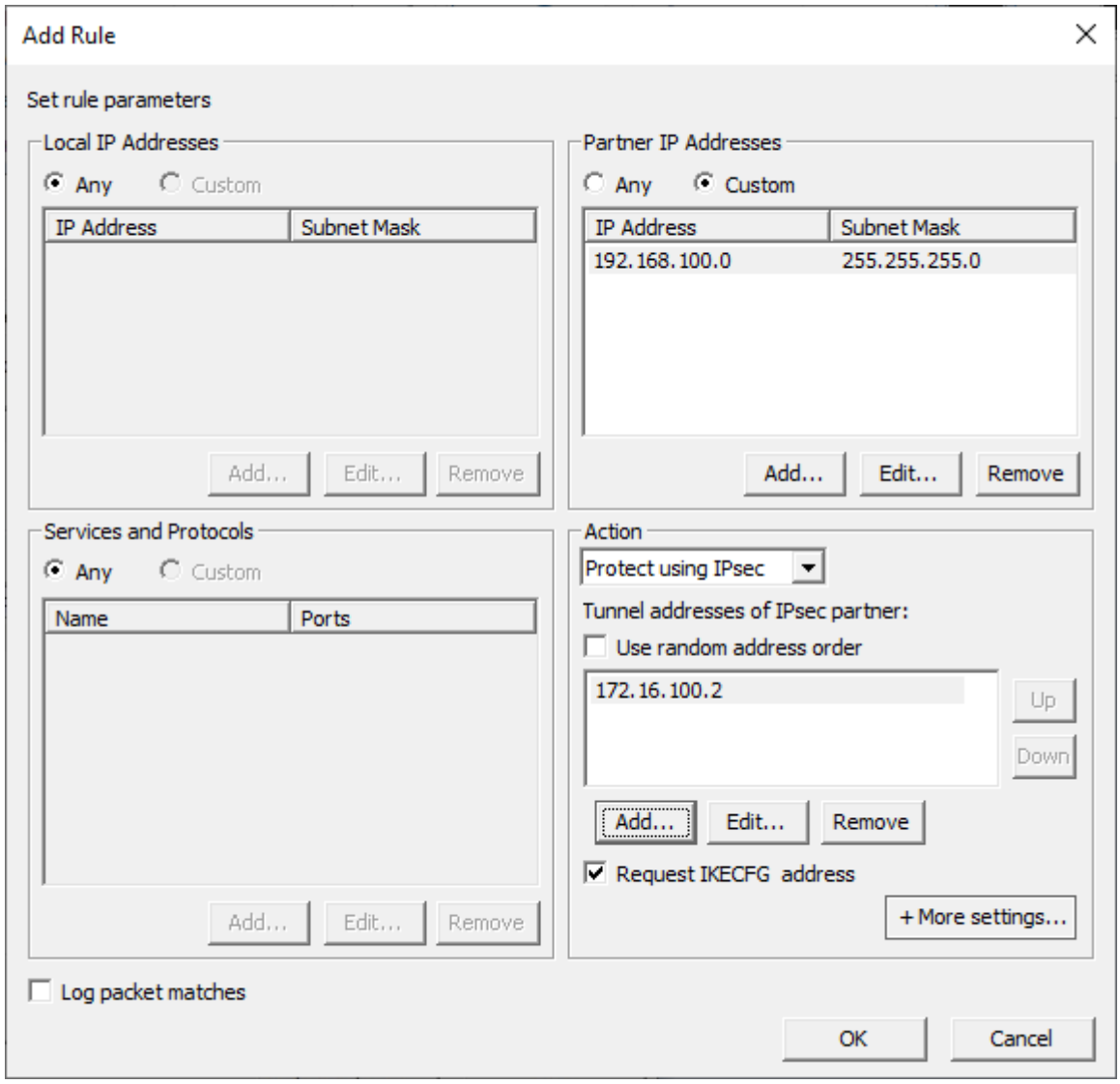

Рисунок 4. Окно Add Rule вкладки Firewall Rules утилиты AdminTool

4.1.3 Добавленное правило поднимите вверх (см. рисунок 5).

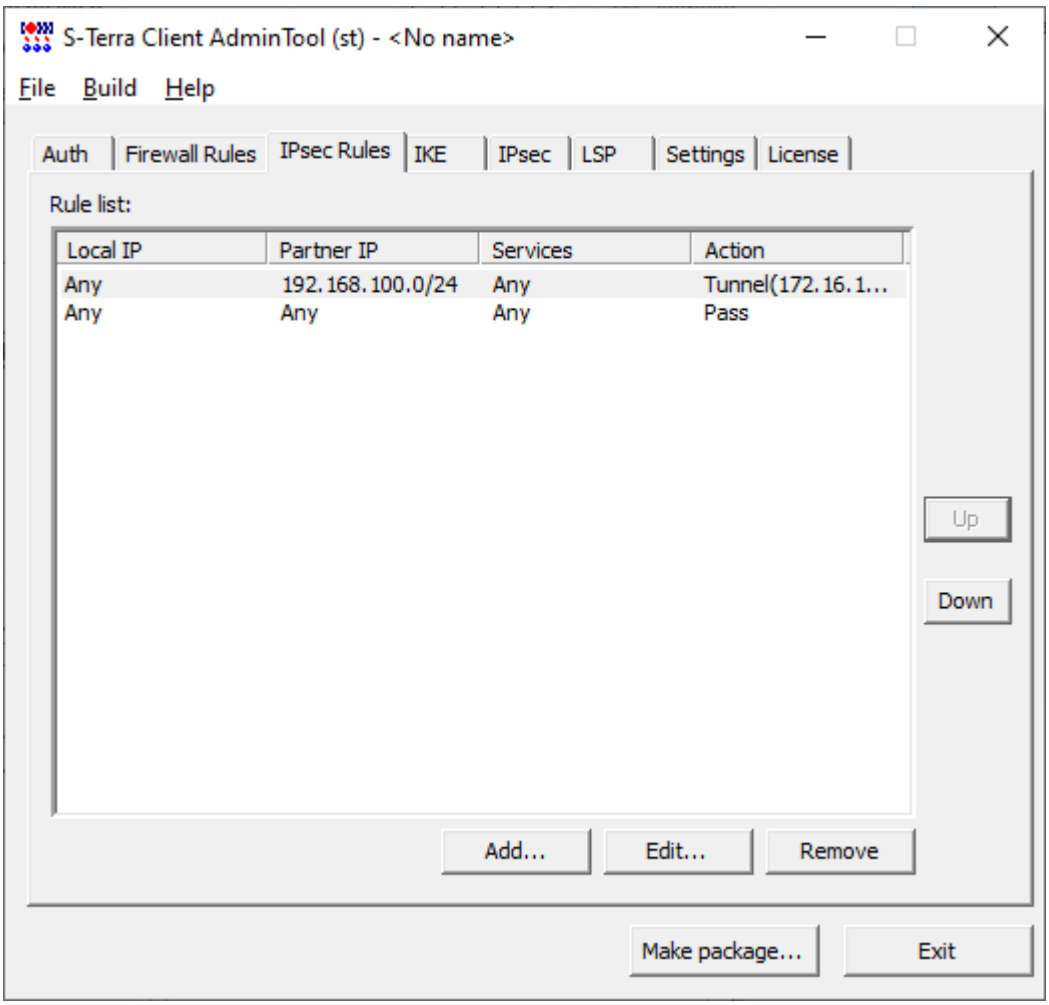

Рисунок 5. Вкладка IPsec Rules утилиты AdminTool

5. Во вкладке **IKE** по умолчанию установлены нужные настройки (см. рисунок 6). При необходимости можно поднять в приоритете используемое правило.

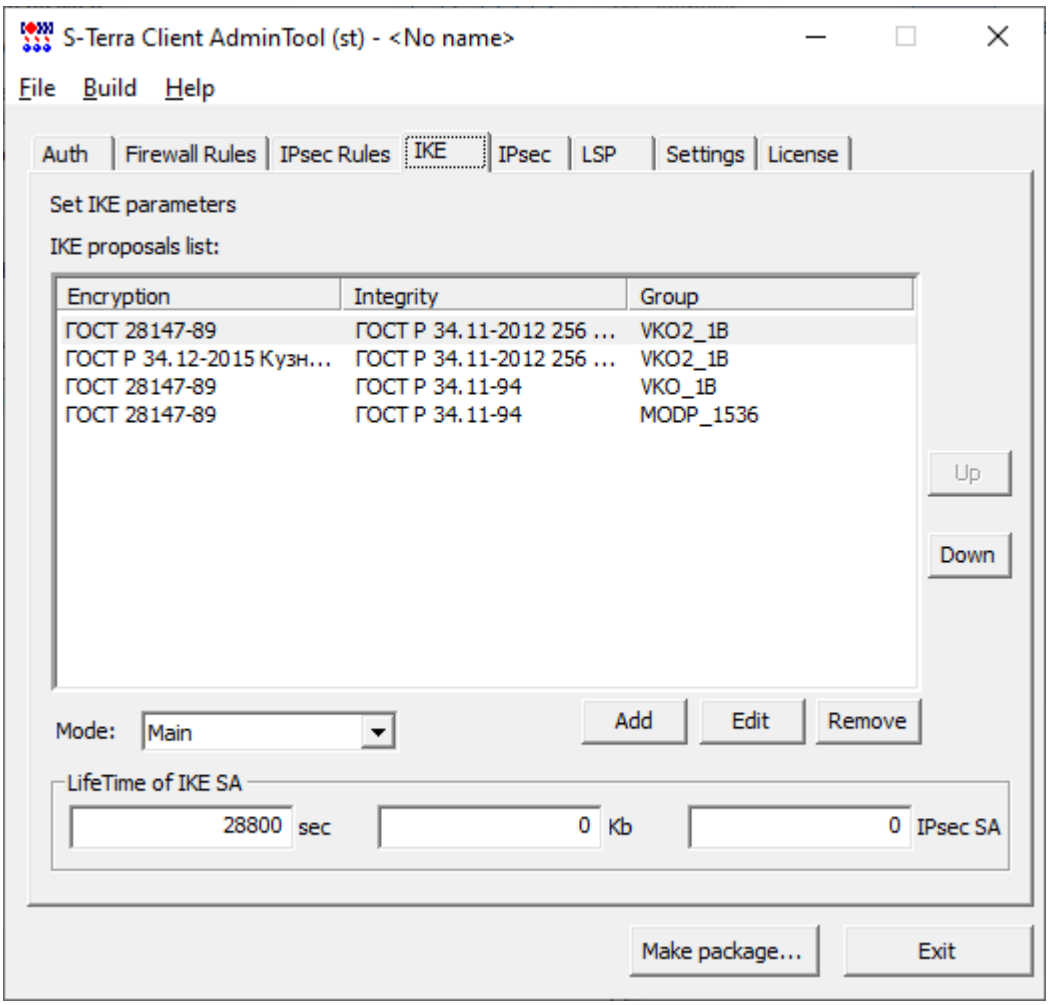

Рисунок 6. Вкладка IKE утилиты AdminTool

6. Во вкладке **IPsec** по умолчанию установлены нужные настройки (см. рисунок 7). При необходимости можно поднять в приоритете используемое правило.

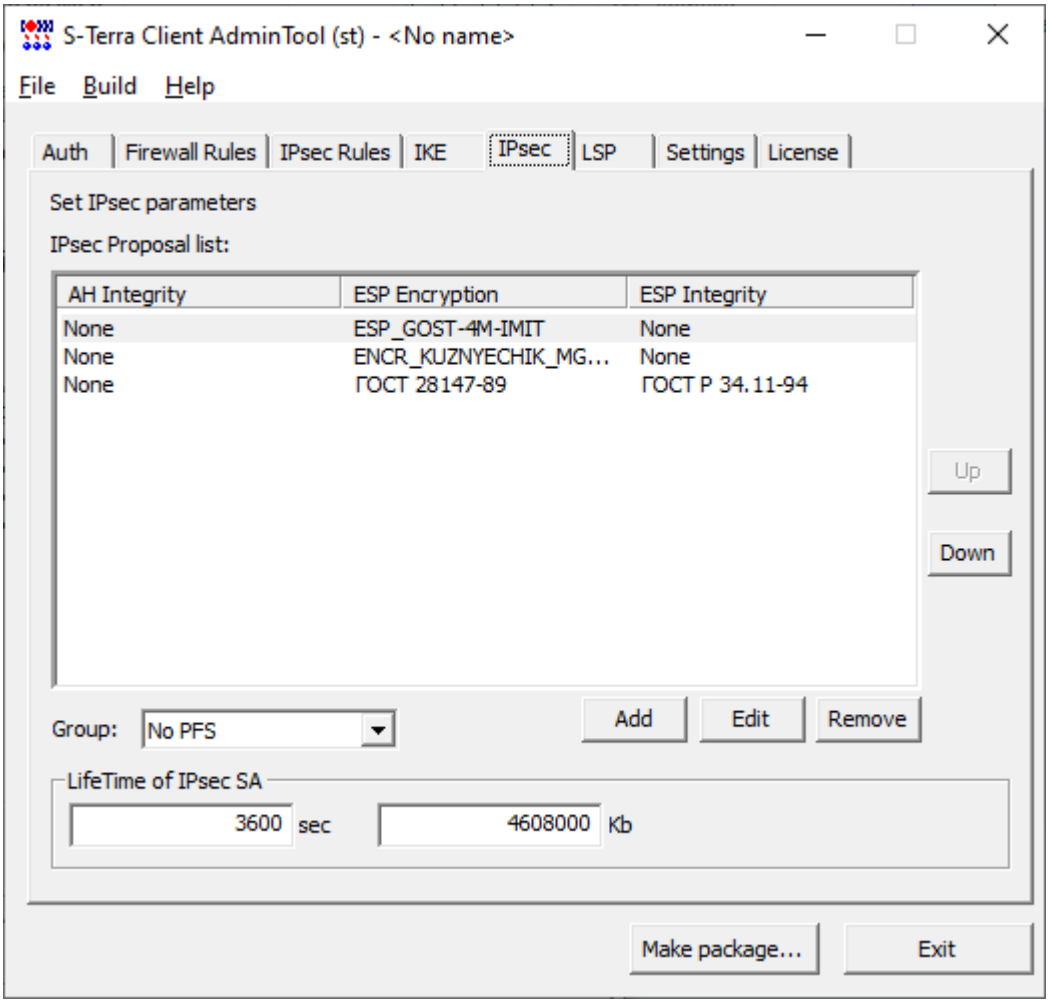

Рисунок 7. Вкладка IPsec утилиты AdminTool

7. Во вкладке **LSP** можно просмотреть получившуюся политику безопасности. Нажмите «**Refresh LSP**» для того, чтобы получить текущую версию.
8. Во вкладке **License** введите лицензию на продукт «С-Терра Клиент» версии 4.3.
9. Сохраните файл созданного проекта, на тот случай, если захотите в будущем сделать похожий клиентский пакет. Для этого в меню **File** выберите **Save project**.
10. Создайте установочный exe-файл для «С-Терра Клиент», нажав кнопку **Make package...**.

Установка на компьютер пользователя

1. Установите на клиентском компьютере полученный exe-файл.
2. В области уведомлений появится иконка «С-Терра Клиент» (см. рисунок 8). Для начала работы необходимо пройти процедуру аутентификации (см. рисунок 9). Имя пользователя по умолчанию – `user`. Пароль по умолчанию отсутствует, в дальнейшем его нужно установить.

Рисунок 8. Иконка «С-Терра Клиент»

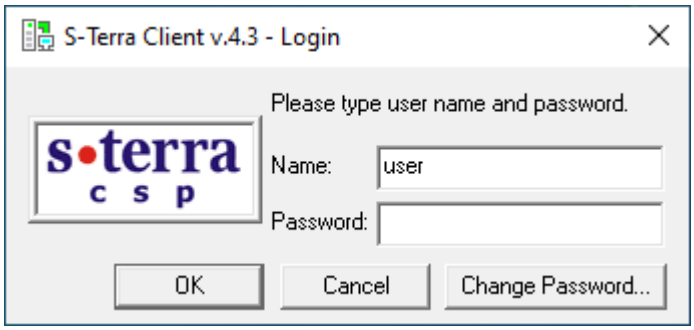

Рисунок 9. Окно аутентификации ПО «С-Терра Клиент»

В приложении представлен текст LSP конфигурации для Client1.

Проверка работоспособности стенда

После того, как настройка всех устройств завершена, аутентифицируйтесь в «С-Терра Клиент». После прохождения аутентификации (см. рисунок 9) при правильных настройках также должно появиться окно XAuth (см. Рисунок 10).

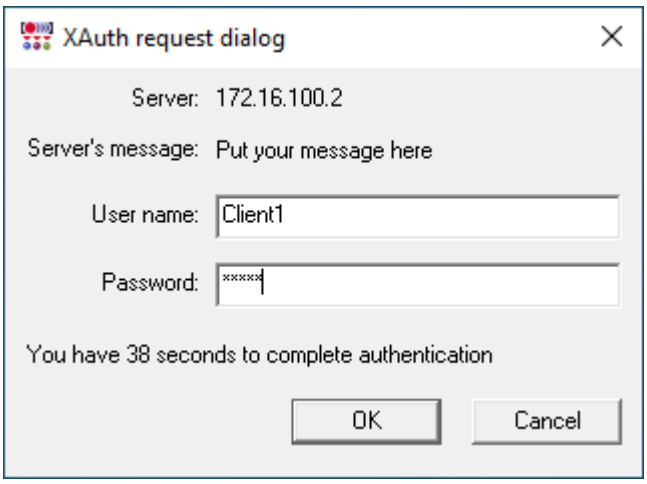

Рисунок 10. Окно аутентификации XAuth

В случае успешной аутентификации должно появиться соответствующее сообщение (см. рисунок 11).

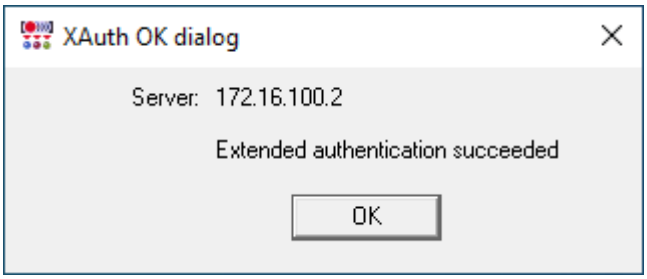

Рисунок 11. Успешная аутентификация XAuth

При правильных настройках на этот момент туннель уже должен быть построен.

Для проверки соединения на устройстве Client1 выполните команду ping:

```
C:\Users\Administrator> ping 192.168.100.100

Обмен пакетами с 192.168.100.100 по с 32 байтами данных:
Ответ от 192.168.100.100: число байт=32 время=33мс TTL=62
Ответ от 192.168.100.100: число байт=32 время=1мс TTL=62
Ответ от 192.168.100.100: число байт=32 время=1мс TTL=62
Ответ от 192.168.100.100: число байт=32 время=1мс TTL=62

Статистика Ping для 192.168.100.100:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 33 мсек, Среднее = 9 мсек
```

Узнать информацию о соединениях можно на устройстве Client1 в окне VPN SA Monitor ПО «С-Терра Клиент» (см. рисунок 12 и рисунок 13):

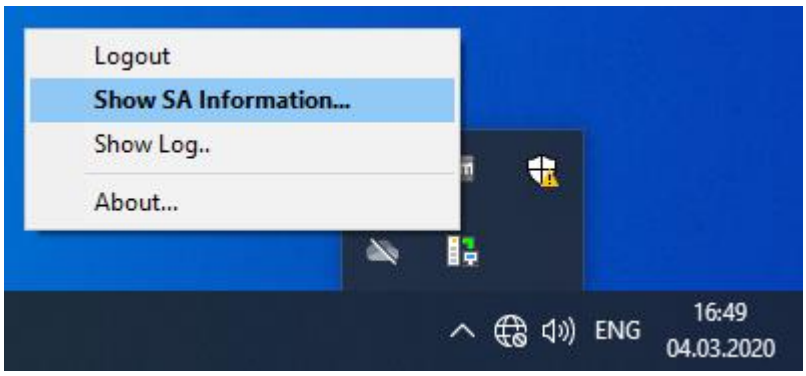

Рисунок 12. Запуск окна VPN SA Monitor ПО «С-Терра Клиент»

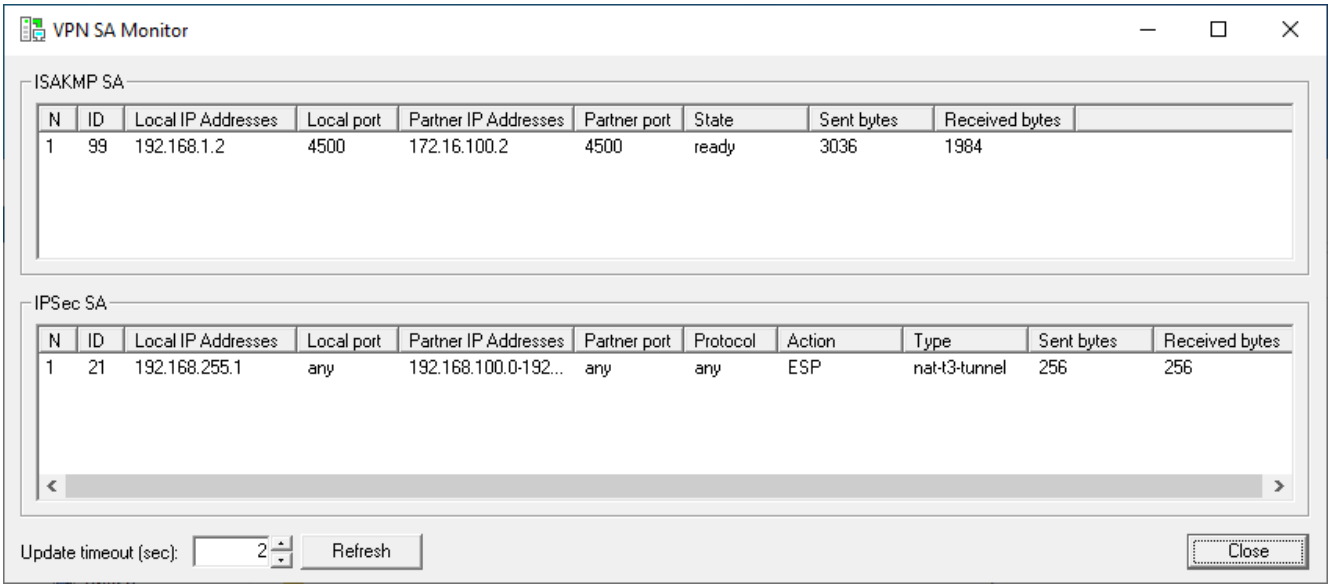

Рисунок 13. Окно VPN SA Monitor ПО «С-Терра Клиент»

Также в этом можно убедиться на устройстве Hub1, выполнив команду:

```
root@Hub1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 2 (172.16.100.2,4500)-(172.16.1.2,4500) active 1984 3036

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 2 (192.168.100.0-192.168.100.255,*)-(192.168.255.1,*) * ESP nat-t3-tunn 256 256
```

Логирование на компьютере пользователя

Для дополнительной диагностики на компьютере пользователя можно воспользоваться средствами логирования.

Для того чтобы включить логирование на компьютере пользователя нужно выполнить следующую последовательность команд:

1. Перейти в директорию установленного ПО «С-Терра Клиент»:

```
cd "C:\Program Files (x86)\S-Terra Client"
```

2. Выполнить следующую команду:

```
C:\Program Files (x86)\S-Terra Client> .\log_mgr.exe set-filelog -y enable
```

```
Filelog parameters are set successfully
```

Теперь можно просматривать логи в окне **Show Log..** ПО «С-Терра Клиент» (см. рисунок 14 и рисунок 15)

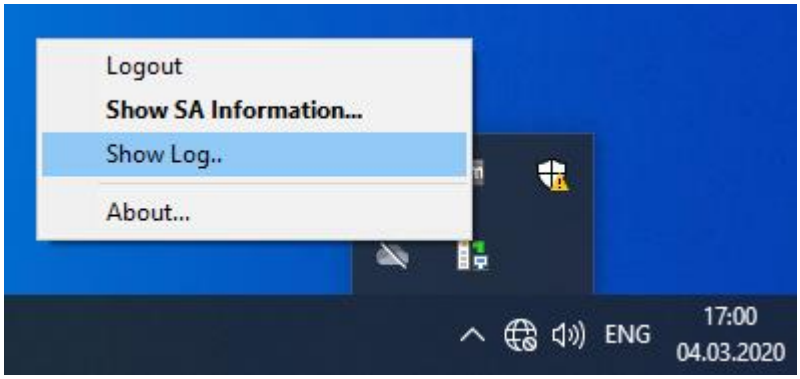

Рисунок 14. Запуск окна просмотра логов ПО «С-Терра Клиент»

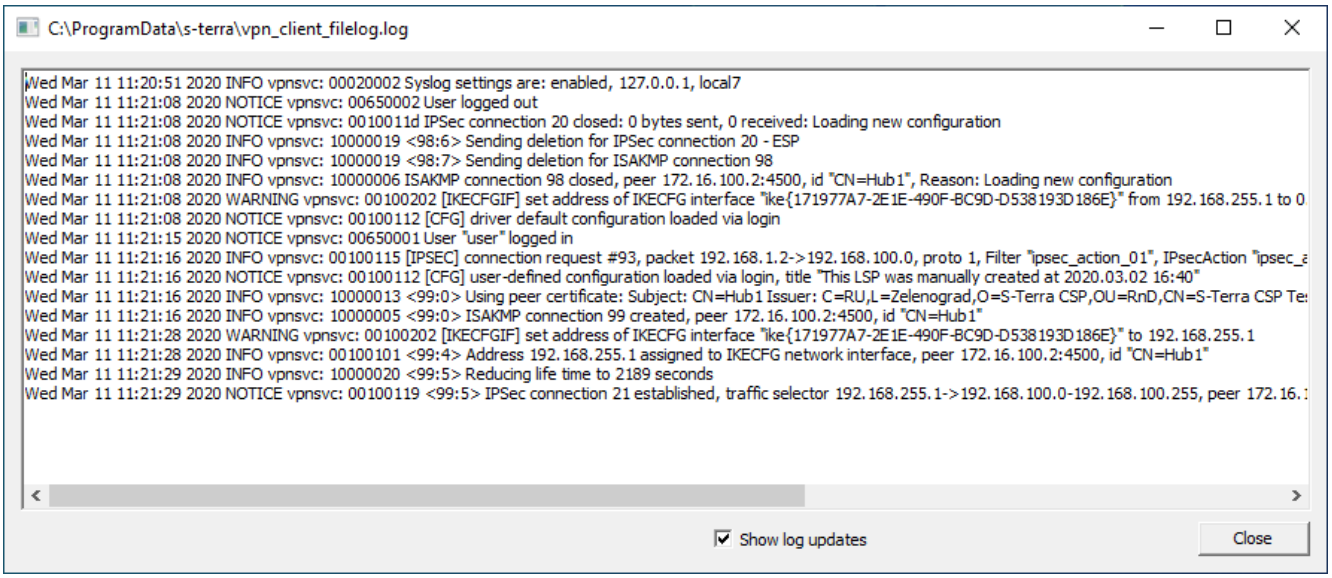

Рисунок 15. Окно просмотра лога ПО «С-Терра Клиент»

Приложение

Конфигурации криптошлюза Hub1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$tHtq8SR6$t3CWE6udI6L/ARr9jQowUYR7wEbOW
Zlx61OvLi7goonOFUYhNSGV49BA.RDGEZ7oKXBA1aTRi20E1R4wtMXTl0
aaa new-model
aaa authentication banner "Put your message here"
aaa authentication login RADIUS1 group radius
!
radius-server host 192.168.100.5 auth-port 1812 acct-port 1813
radius-server key secret1
!
hostname Hub1
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
!
!
!
!
!
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-imit
!
ip access-list extended IPSEC_ACL_HUB1_AND_CLIENTS
 permit ip 192.168.100.0 0.0.0.255 192.168.255.0 0.0.0.255
!
!
crypto dynamic-map DMAP 1
 match address IPSEC_ACL_HUB1_AND_CLIENTS
 set transform-set GOST_ENCRYPT_AND_INTEGRITY
 reverse-route
 set client authentication list RADIUS1
 set client authentication xauth
 set dead-connection history off
!
crypto map VPN 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 172.16.100.2 255.255.255.0
 crypto map VPN
!
interface GigabitEthernet0/1
 ip address 192.168.100.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
```

```
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
ADE9BB6B223814A76CEC9E9BD24ECA72A6AE472E96144F5AAA08F9CDC3DA5457
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Tue Mar 10 21:38:58 2020

GlobalParameters(
    Title                              = "This LSP was automatically generated by CSP
Converter at Tue Mar 10 21:38:58 2020 (user: cscons)"
    Version                    = LSP_4_3
    CRLHandlingMode            = ENABLE
    PreserveIPsecSA            = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.100.1
        )
)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
)

RADIUSServer RADIUSServer
(
    IPAddress = 192.168.100.5
    SecretId = "cs_radius_server_key__"
    AuthenticationPort = 1812
    AccountingPort = 1813
    Retries = 4
    ResponseTimeout = 5
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "G2814789CPRO1-K256-CBC-65534"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)
```

```
ESPProposal GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO2-K288-CNTMAC-253"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4608000
    )
)

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

AAARule AAA:VPN:1:DMAP:1
(
    ClientDialogType = PAP
    ClientDialogMessage = "Put your message here"
    AuthenticationServer = RADIUSServer
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID        =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    SendRequestMode    =  ALWAYS
    SendCertMode       =  ALWAYS
)

IKERule IKERule:VPN:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    AAA                 = AAA:VPN:1:DMAP:1
    Priority            = 100
)

IPsecAction IPsecAction:VPN:1:DMAP:1
(
    TunnelingParameters = TunnelEntry(
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( GOST_ENCRYPT_AND_INTEGRITY:ESP )
    ReverseRoute = TRUE
    NoDeadConnectionHistory = TRUE
    IKERule = IKERule:VPN:1:DMAP:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.255.0/24
```

```
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_ACL_HUB1_AND_CLIENTS"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    IPsecPolicy = IPsecPolicy:VPN
)
```

Конфигурации Client1

1. Конфигурация LSP:

```
GlobalParameters (
       Title = "This LSP was automatically generated by S-Terra Client AdminTool (st)
at 2020.03.04 22:54:14"
       Version = LSP_4_3
       CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
       ResponseTimeout = 200
       HoldConnectTimeout = 60
       DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
       DistinguishedName *= CertDescription(
              Subject *= COMPLETE,"C=RU,O=S-Terra CSP,OU=Research,CN=Client1"
              )
)
CertDescription local_cert_dsc_01(
       Subject *= COMPLETE,"C=RU,O=S-Terra CSP,OU=Research,CN=Client1"
       Issuer *= COMPLETE,"C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test
Root CA"
       SerialNumber = "2F0000022BF3A10917A4346AEA00000000022B"
       FingerprintMD5 = "BD995EF7E23A83AC1EECA352DFBF743E"
)
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
)
IKEParameters (
       DefaultPort = 500
       SendRetries = 5
       RetryTimeBase = 1
       RetryTimeMax = 30
       SessionTimeMax = 60
       InitiatorSessionsMax = 30
       ResponderSessionsMax = 20
       BlacklogSessionsMax = 16
       BlacklogSessionsMin = 0
       BlacklogSilentSessions = 4
       BlacklogRelaxTime = 120
       IKECFGPreferDefaultAddress = FALSE
)
IKETransform ike_trf_01(
       LifetimeSeconds = 28800
       CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
       HashAlg *= "GR341112_256TC26-65128"
       GroupID *= VKO2_1B
```

```
)
IKETransform ike_trf_02(
	LifetimeSeconds = 28800
	CipherAlg  *= "GR341215K-K256-CFB-65528"
	HashAlg *= "GR341112_256TC26-65128"
	GroupID *= VKO2_1B
)
IKETransform ike_trf_03(
	LifetimeSeconds = 28800
	CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
	HashAlg *= "GR341194CPRO1-65534"
	GroupID *= VKO_1B
)
IKETransform ike_trf_04(
	LifetimeSeconds = 28800
	CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
	HashAlg *= "GR341194CPRO1-65534"
	GroupID *= MODP_1536
)
ESPTransform esp_trf_01(
	CipherAlg *= "G2814789CPRO2-K288-CNTMAC-253"
	LifetimeSeconds = 3600
	LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_01(
	Transform *=esp_trf_01
)
ESPTransform esp_trf_02(
	CipherAlg *= "GR341215K-K352-MGM-251"
	LifetimeSeconds = 3600
	LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_02(
	Transform *=esp_trf_02
)
ESPTransform esp_trf_03(
	CipherAlg *= "G2814789CPRO1-K256-CBC-254"
	IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
	LifetimeSeconds = 3600
	LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_03(
	Transform *=esp_trf_03
)
IKERule ike_rule_with_ikecfg_01(
	DoNotUseDPD = FALSE
	DPDIdleDuration = 60
	DPDResponseDuration = 5
	DPDRetries = 3
	MainModeAuthMethod *= auth_method_01
	Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
	IKECFGRequestAddress = TRUE
)
IPsecAction ipsec_action_01(
	PersistentConnection = TRUE
	TunnelingParameters *=
		TunnelEntry(
			PeerAddress = 172.16.100.2
			Assemble = TRUE
			ReRoute = FALSE
			TCPEncapsulation = FALSE
		)
	ContainedProposals *= (esp_proposal_01),(esp_proposal_02),(esp_proposal_03)
	IKERule = ike_rule_with_ikecfg_01
)
FilterChain filter_chain_input(
```

```
	Filters *= Filter(
		ProtocolID *= 17
		DestinationPort *= 500
		Action = PASS
		LogEventID = "pass_action_02_01"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		ProtocolID *= 17
		DestinationPort *= 4500
		Action = PASS
		LogEventID = "pass_action_02_02"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		SourceIP *= 172.16.100.2
		ProtocolID *= 50
		Action = PASS
		LogEventID = "pass_action_03_01"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		SourceIP *= 172.16.100.2
		ProtocolID *= 51
		Action = PASS
		LogEventID = "pass_action_03_02"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		Action = PASS
		LogEventID = "pass_action_04"
	)
)
FilterChain filter_chain_output(
	Filters *= Filter(
		ProtocolID *= 17
		SourcePort *= 500
		Action = PASS
		LogEventID = "pass_action_05_01"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		ProtocolID *= 17
		SourcePort *= 4500
		Action = PASS
		LogEventID = "pass_action_05_02"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		DestinationIP *= 172.16.100.2
		ProtocolID *= 50
		Action = PASS
		LogEventID = "pass_action_06_01"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		DestinationIP *= 172.16.100.2
		ProtocolID *= 51
		Action = PASS
		LogEventID = "pass_action_06_02"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		Action = PASS
		LogEventID = "pass_action_07"
	)
)
FilterChain filter_chain_classification_input(
	Filters *= Filter(
		Action = PASS
		LogEventID = "pass_action_08"
	)
)
FilterChain filter_chain_classification_output(
```

```
	Filters *= Filter(
		Action = PASS
		LogEventID = "pass_action_09"
	)
)
FilterChain filter_chain_ipsec(
	Filters *= Filter(
		ProtocolID *= 17
		SourcePort *= 500
		Action = PASS
		LogEventID = "pass_action_10_01"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		ProtocolID *= 17
		SourcePort *= 4500
		Action = PASS
		LogEventID = "pass_action_10_02"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		DestinationIP *= 172.16.100.2
		ProtocolID *= 50
		Action = PASS
		LogEventID = "pass_action_11_01"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		DestinationIP *= 172.16.100.2
		ProtocolID *= 51
		Action = PASS
		LogEventID = "pass_action_11_02"
		PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
	),Filter(
		DestinationIP *= 192.168.100.0/24
		Action = PASS
		ExtendedAction *= ipsec<sa=ipsec_action_01>
		LogEventID = "ipsec_action_01"
	),Filter(
		Action = PASS
		LogEventID = "pass_action_12"
	)
)
NetworkInterface(
	InputFilter = filter_chain_input
	OutputFilter = filter_chain_output
	InputClassification = filter_chain_classification_input
	OutputClassification = filter_chain_classification_output
	IPsecPolicy = filter_chain_ipsec
)
```

Пример настроек FreeRADIUS

В конце файла настроек /etc/freeradius/3.0/clients.conf:

```
client Hub1 {
        ipaddr = 192.168.100.1
        secret = secret1
}
```

где

- **Hub1** – имя настройки (можно задать любое допустимое);
- **192.168.100.1** – адрес RADIUS клиента (в данном случае в качестве него выступает шлюз Hub1);
- **secret1** – пароль доступа. Пароль должен совпадать с заданным в пункте 2 («Настройте взаимодействие с RADIUS сервером») раздела «Настройка шифрования» из настроек криптошлюза Hub1.

В начале файла настроек `/etc/freeradius/3.0/mods-config/files/authorize`:

```
Client1 Cleartext-Password := "Pass1"
        Framed-IP-Address = 192.168.255.1,
        Framed-IP-Netmask = 255.255.255.255
```

где

- **Client1** – имя пользователя XAuth;
- **Pass1** – пароль пользователя XAuth Client1;
- **192.168.255.1** – адрес IKECFG, который будет выдаваться данному пользователю;
- **255.255.255.255** – маска, которая будет передаваться с указанным адресом.

Маска всегда должна быть равна /32 (255.255.255.255). Менять ее значение не следует.