

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



Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Инструкция по подготовке к работе модуля МСМ-950

РЛКЕ.00009-01 90 03

21.09.2015

Содержание

Инструкция по подготовке к работе Модуля Сетевого Модернизированного MCM-950	3
Комплект поставки	5
Подготовка модуля к работе	6
Установка модуля в маршрутизатор.....	7
Инициализация «Программного комплекса С-Терра Шлюз» при первом старте	9
Подключение к локальной сети.....	10
Архитектура ПО С-Терра Шлюз	11
Пример топологии	13
Настройка политики безопасности шлюзов	14
Предварительные настройки	15
Регистрация СА сертификата (сертификата УЦ)	16
Регистрация локального сертификата	16
Настройка шлюза MCM950-1 (GW1)	17
Настройка шлюза MCM950-2 (GW2)	19
Проверка работоспособности стенда	20
Настройка модуля для работы с удаленными клиентами	21
Настройка маршрутизатора Router1	22
Настройка устройства Router2	22
Настройка устройства IPHost1	23
Регистрация сертификатов	23
Настройка шлюза безопасности MCM950-1 (GW1)	23
Подготовка клиентского ПО	26
Проверка клиентского соединения	35
Дополнительная информация.....	36

Инструкция по подготовке к работе Модуля Сетевого Модернизированного MCM-950

Модуль MCM-950 производится в соответствии с технологическим процессом, согласованным с Центром ФСБ России «Модуль сетевой модернизированный «MCM-950». Технические условия. РЛКЕ.466534.002 ТУ».

В рамках установленных Технических условий компания «С-Терра СиЭсПи» выступает в роли оператора контролируемого технологического процесса, цель которого – исключить вероятность внедрения в вычислительную среду эксплуатации средств криптографической защиты информации (СКЗИ) недокументированных вредоносных аппаратно-программных элементов.

Далее в документации модуль будем называть «Модуль MCM-950», «модуль» или «MCM-950».

Модуль работает на маршрутизаторах Cisco ISR второго поколения (серии 2900, 3900), а также на маршрутизаторах 4331, 4351 и 4451-X.

Аппаратно модуль представляет собой вычислительную платформу на базе процессора Sandy Bridge-Mobile, 1,2/1,6 ГГц, 4 Гб DRAM и 2 Гб постоянной памяти, размещенную на специальном загрузочном носителе (СЗН) «СПДС-USB-01», либо не менее 500 Гб постоянной памяти, размещенную на одном или двух (RAID-1) жестких дисках.

Возможен один из следующих вариантов исполнения модуля:

- MCM_950_KC1 (UCS-EN120SRU-SEC1=) – 1 жесткий диск (HDD0)
- MCM_950_KC1 (UCS-EN120SRU-S1H2=) – 2 жестких диска (HDD0, HDD1 в RAID-1)
- MCM_950_KC2 (UCS-EN120SRU-SEC2=) – СЗН «СПДС-USB-01»
- MCM_950_KC3 (UCS-EN120SRU-SEC3=) – СЗН «СПДС-USB-01».

Модуль работает независимо от ОС маршрутизатора, все обмены между ними производятся только по сети. Маршрутизаторы второго поколения работают под управлением ОС Cisco IOS версии 15.2(4)M и выше, маршрутизаторы 4331, 4351 и 4451 – под управлением ОС Cisco IOS XE 3.9S и выше.

На модуль устанавливается ПО «Программный комплекс С-Терра Шлюз. Версия 4.1» (далее может встречаться наименование «С-Терра Шлюз», «S-Terra Gate», «Продукт»), функционирующий под управлением ОС Debian GNU/Linux 6.

Для обеспечения доверенной загрузки «С-Терра Шлюз» по классам защиты KC2 и KC3 используется СЗН «СПДС-USB-01».

Применяться модуль может для защиты трафика среднего офиса – несколько сотен рабочих мест. В составе маршрутизаторов серий 3900, в которые можно установить от 2 до 4 модулей, может использоваться на узлах концентрации трафика множества региональных сетей, а также в крупных сетях удаленного доступа пользователей.

Модуль MCM-950 может поддерживать до 500 IPsec туннелей.

В этом документе описано как подготовить модуль MCM-950 к работе – установить модуль в маршрутизатор, инициализировать на нем программный комплекс S-Terra Gate и создать локальную политику безопасности. Здесь даны только минимальные сведения, более детальную информацию по настройке модуля и его работе можно найти в документе: [«Программный комплекс С-Терра Шлюз. Версия 4.1. Руководство по установке и настройке модуля MCM-950» \[1\]](#).



Рисунок 1

Комплект поставки

В комплект поставки «Программного комплекса С-Терра Шлюз. Версия 4.1» входят:

модуль МСМ-950 с одним или двумя жесткими дисками, либо (в случае исполнения КС2/КС3) с СЗН «СПДС-USB-01», на котором:

- установлена ОС Debian GNU/Linux 6
- подготовлены к инициализации «Программный комплекс С-Терра Шлюз. Версия 4.1» и СКЗИ «КриптоПро CSP 3.6R4/3.9»
- или подготовлен к инициализации «Программный комплекс С-Терра Шлюз. Версия 4.1» со встроенной криптобиблиотекой, разработанной компанией С-Терра СиЭсПи

документы в электронном виде:

- Копия сертификата соответствия ФСБ России
- Копия сертификата соответствия ФСТЭК России
- Лицензионное соглашение о праве пользования «Программным комплексом С-Терра Шлюз. Версия 4.1» производства ООО «С-Терра СиЭсПи»

документы в печатном виде:

- Голографический специальный защитный знак ФСТЭК России
- Лицензия на использование программного продукта «КриптоПро CSP Driver версии 3.6R4/3.9» (если используется СКЗИ «КриптоПро CSP»).
- Лицензия на использование «Программного комплекса С-Терра Шлюз. Версия 4.1».

На сайте компании по адресу <http://www.s-terra.com/support/documents/ver41/> можно взять следующие материалы:

- в разделе «С-Терра Шлюз» – Правила пользования, Формуляры, Руководство администратора,
- в разделе «Модули – комплект материалов для восстановления»:
 - S-Terra Gate Disk Image (образ жесткого диска и Приложение к Инструкции по восстановлению ПАК);
 - S-Terra Gate Recovery CD (ПО для восстановления образа диска и Инструкция по восстановлению ПАК. В случае исполнения КС2/КС3 не используется).

Подготовка модуля к работе

Подготовка модуля МСМ-950 к работе осуществляется в несколько этапов:

- Шаг 1:** Установка модуля в маршрутизатор.
- Шаг 2:** Инициализация S-Terra Gate на модуле.
- Шаг 3:** Подключение маршрутизатора с модулем к корпоративной сети.
- Шаг 4:** Настройка локальной политики безопасности.
- Шаг 5:** Проверка функционирования модуля.

Установка модуля в маршрутизатор

Перед установкой модуля MCM-950 в маршрутизатор ознакомьтесь с «Мерами безопасности и правилами эксплуатации», а также методом защиты от статического электричества, описанными в документе [1].



Note

Маршрутизаторы Cisco 3900 ISR G2 и Cisco ISR 4451-X поддерживают режим Горячей замены, т.е. установку/извлечение модуля во время работы маршрутизатора.

Следует иметь ввиду, что маршрутизаторы серии ISR G2 2900 и 4300 не поддерживают данного режима, а значит необходимо отключить электрическое питание и отсоединить сетевые кабели перед установкой/извлечением модуля во избежание поражения электрическим током.

Сетевой модуль MCM-950 может быть установлен в single-wide SM слот на маршрутизаторах Cisco 2911, 2921, 2951, 3925, 3945, 3925e, 3945e, 4331, 4351, 4451-X. Более подробную информацию о количестве и расположении SM слотов смотрите в документе [1].

Для установки модуля выполните все действия, описанные в главе 4 «Установка модуля в маршрутизатор» документа [1], а именно:

- Шаг 1:** трансформируйте слот большего размера в слот single-wide, если необходимо, и установите в него модуль MCM-950
- Шаг 2:** соедините кабелем внешний сетевой интерфейс модуля Gigabit Ethernet (GE2) с корпоративной сетью
- Шаг 3:** включите электропитание маршрутизатора (если не использовался режим Горячей замены модуля)
- Шаг 4:** проверьте, что на маршрутизаторе установлена правильная версия операционной системы Cisco IOS.
- Шаг 5:** убедитесь, что IOS распознала модуль MCM-950, для этого используйте одну из следующих команд:

для вывода на экран данных о всей системе используйте команду **show platform**:

```
Router# show platform
```

выводимая информация по этой команде должна содержать записи следующего вида:

```
Router# show platform
Chassis type: ISR4451/K9
Slot      Type                               State      Insert time (ago)
-----
0          ISR4451/K9                               ok         1d01h
0/0        ISR4400-4X1GE                             ok         1d01h
1          ISR4451/K9                               ok         1d01h
1/0        UCS-E160DP-M1/K9                         ok         1d01h
2          ISR4451/K9                               ok         1d01h
R0         ISR4451/K9                               ok, active 1d01h
F0         ISR4451/K9                               ok, active 1d01h
P0         XXX-XXXX-XX                              ok         1d01h
P1         Unknown                                  ps,        1d01h
P2         ACS-4450-FANASSY                         ok         1d01h

Slot      CPLD Version      Firmware Version
-----
0          12090323          12.2 (20120829:165313)
1          12090323          12.2 (20120829:165313)
```

2	12090323	12.2 (20120829:165313)
R0	12090323	12.2 (20120829:165313)
F0	12090323	12.2 (20120829:165313)

для подтверждения того, что IOS распознала модуль MCM-950, используйте команду **show hw-module subslot all oir**:

```
Router# show hw-module subslot all oir
Module Model Operational Status
-----
subslot 0/0 ISR4451-X-4X1GE ok
subslot 1/0 UCS-E140S-M1/K9 ok
subslot 2/0 UCS-E140S-M1/K9 ok
```

если IOS распознал модуль, то светодиод PWR на передней панели модуля загорится желтым, а в конфигурации маршрутизатора появится новый интерфейс:

```
interface ucse 1/0
 shutdown
 no keepalive
```

Шаг 6: перед настройкой модуля сделаем этот интерфейс активным и назначим ему адрес. Следующие команды выполняются при использовании маршрутизаторов Cisco 2900, 3900 ISR G2:

```
Router # configure terminal
Router(config)# interface ucse 1/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end
Router # show running-config
```

при использовании маршрутизаторов Cisco ISR 4451-X выполним команды:

```
Router # configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end
Router # show running-config
```

Шаг 7: для доступа к консоли введите команды (логин и пароль по умолчанию – admin и password):

```
Router# ucse 1 session imc

Trying 192.168.0.254, 2066 ... Open
...
Unknown login: admin
Password:
Unknown # connect host
CISCO Serial Over LAN:
Close Network Connection to Exit
```

На этом этапе можно начинать инициализацию.



Note

Для выхода из сессии нажмите "Ctrl-Shift-6" затем клавишу "x". В появившемся промте IOS наберите команду: **ucse 1 session host clear** и нажмите Enter.

Инициализация «Программного комплекса С-Терра Шлюз» при первом старте

СЗН «СПДС-USB-01» или один/два жестких диска содержат:

- установленную ОС Debian 6
- установленный и подготовленный к инициализации «Программный комплекс С-Терра Шлюз» и СКЗИ «КриптоПро CSP 3.6R4/3.9»
либо
- установленный и подготовленный к инициализации «Программный комплекс С-Терра Шлюз» со встроенным СКЗИ, разработанным компанией С-Терра СиЭсПи.

Для работы установленных продуктов необходимо провести процедуру начальной инициализации при первом старте модуля. Подробно процесс инициализации S-Terra Gate на модуле описан в документе [1]. Но если кратко, то процесс инициализации происходит следующим образом.

Инициализация запускается администратором при помощи скрипта при первом старте модуля. В диалоговом режиме предлагается:

- ввести лицензионную информацию для «КриптоПро CSP» (если используется СКЗИ «КриптоПро CSP»)
- инициализировать начальное значение ДСЧ для исполнений класса защиты КС1. Для исполнений класса защиты КС2 и КС3 инициализация начального значения ДСЧ выполняется без участия пользователя
- ввести лицензионную информацию для С-Терра Шлюз.

После этого, запускаются необходимые процессы. При этом о нормальном функционировании модуля говорит горящий зеленым индикатор PWR.

На этом инициализация заканчивается. В процессе инициализации создается пользователь с именем "cscons" и паролем "csp", которым можно войти в Cisco-like интерфейс командной строки (CLI), а в ОС – пользователем "root" (изначально без пароля).

Доступ в систему возможен также удаленно – по протоколу SSH.



Note

После инициализации Продукта, советуем изменить пароль пользователей "root" и "cscons". Эта процедура описана в документе [«Программный комплекс С-Терра Шлюз. Версия 4.1. Настройка шлюза»](#).



Note

Перед выключением маршрутизатора, желательно остановить работу ОС с помощью команды "poweroff", которую можно ввести в Linux shell, или из CLI – "run /sbin/poweroff". Такого же результата можно достигнуть, нажав кнопку "Shutdown" на передней панели модуля (и подождяв около 10 секунд). Перезапустить модуль можно повторным нажатием этой же кнопки.

Подключение к локальной сети

Две возможные схемы подключения маршрутизатора с модулем MCM-950 в локальную сеть приведены ниже (Рисунок 2).

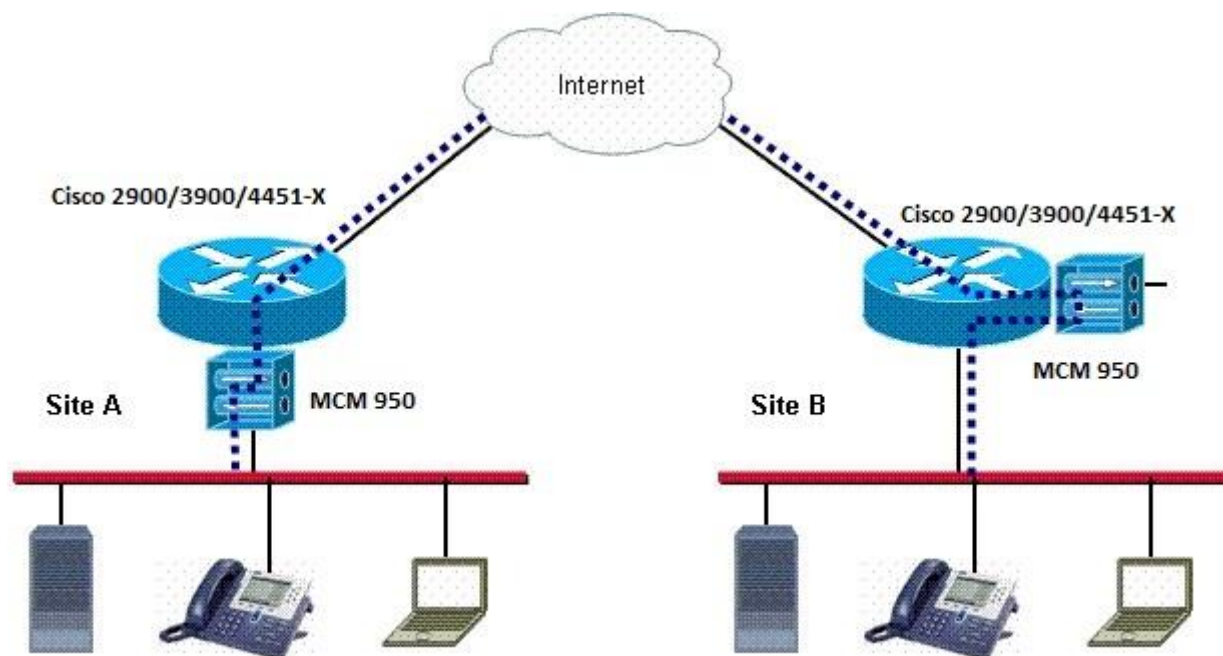


Рисунок 2

В простейшем случае, модуль (Site A), подключенный к локальной сети, используется как default gateway во внешний мир. В такой схеме модуль пропускает через себя весь трафик, при этом осуществляя шифрование/расшифрование только необходимых соединений. В настоящем документе мы будем рассматривать именно такой вариант.

В более сложном случае, когда необходимо подключить маршрутизатор непосредственно к локальной сети (например, для использования его в качестве DHCP сервера), роль default gateway может выполнять маршрутизатор, при этом перенаправляя трафик, подлежащий шифрованию/расшифрованию на модуль MCM-950. Как видно из рисунка (Site B), при этом можно использовать только один внутренний интерфейс модуля, внешний же оставить в резерве.

В любом случае, желательно использовать богатые возможности IOS маршрутизатора для подключения сети к Internet.

Для лучшего понимания способов настройки модуля рассмотрим архитектуру его программного обеспечения.

Архитектура ПО С-Терра Шлюз

Функциональность MCM-950 обеспечивает программный продукт С-Терра Шлюз, который состоит из следующих основных частей:

- VPN daemon (демон)
- VPN driver (драйвер)
- Cisco-like console (CLI консоль)
- Command Line Utilities (утилиты)
- Клиент управления КП
- База Продукта.

Рассмотрим каждый из них.

Демон (vpnsvc) – основная часть продукта, которая реализует протокол IKE, обеспечивает работу с базой IPsec SA, взаимодействует с драйвером, загружая в него конфигурационную информацию и обрабатывая его запросы на создание SA. Кроме этого, в демоне выполняется вся работа с сертификатами, событийное протоколирование, сбор статистики и реализована поддержка протоколов SNMP, LDAP, SYSLOG.

Работа **демона** управляется специальным описанием – Local Security Policy (LSP). LSP (или “native configuration”) имеет текстовое представление и может быть загружена в демон пользователем консоли или вызовом утилит. При загрузке новой LSP все существующие SA уничтожаются.

Основная задача **драйвера** – перехват, фильтрация и обработка пакетов. Перехватив пакет, драйвер сравнивает его со списком фильтров и, при совпадении параметров пакета (адреса, порты, протокол) с параметрами фильтра либо выполняет обработку пакета, либо пропускает его дальше без обработки, либо уничтожает пакет.

Параметры фильтров и описание действия, которое необходимо выполнить с пакетом, загружаются демоном в драйвер при загрузке LSP.

Консоль (CLI) предоставляет пользователю интерфейс в стиле командной строки Cisco IOS. Набор команд консоли является подмножеством команд IOS, с некоторыми ограничениями функциональности и небольшими дополнительными возможностями. Как и у IOS, у консоли есть привилегированный и конфигурационный режимы (configure terminal). Однако, следует отметить, что (в отличие от IOS) изменения настроек вступают в действие не сразу, а только после выхода из конфигурационного режима; в этот момент Cisco-like конфигурация автоматически конвертируется в native-конфигурацию и загружается в vpnsvc.

CLI консоль на самом деле является специальным shell-ом по умолчанию для предопределенного пользователя “cscons” и всех пользователей, которые создаются в CLI конфигурации. Остальные пользователи, например “root”, при входе попадают в ОС Debian.

Утилиты служат для общего управления Продуктом. Они позволяют загружать и просматривать LSP, регистрировать в Продукте сертификаты и ключи, получать различную информацию о текущем состоянии Продукта.

Утилиты могут быть вызваны из CLI консоли с использованием специальной команды run.

Клиент управления КП – клиентская часть «Программного продукта С-Терра КП. Версия 4.1», устанавливается на управляемое устройство с установленным продуктом С-Терра Шлюз. В состав продукта С-Терра КП входит Сервер управления, устанавливаемый на выделенный компьютер, и предназначен для управления процессом обновления продуктов С-Терра Агент и их настроек, установленных на управляемых устройствах.

База Продукта – в ней хранятся сертификаты, предопределенные ключи, список интерфейсов, локальные настройки различных модулей, локальная политика безопасности и др.

Примеры взаимодействия описанных компонент

Перед созданием конфигурации с помощью интерфейса командной строки, нужно зарегистрировать локальный сертификат в базе Продукта, используя утилиту. Затем запустить консоль и создать в ней конфигурацию. При выходе из конфигурационного режима консоли конфигурация конвертируется, загружается на шлюз безопасности и хранится в базе Продукта. Используя утилиту, конфигурацию можно выгрузить из шлюза, и при этом загрузится политика DDP. Выгруженную конфигурацию можно опять загрузить на шлюз безопасности.

Пример топологии

В качестве примера рассмотрим вариант настройки LAN-to-LAN IPsec/VPN туннеля между двумя офисами, соединенными через сеть Internet (Рисунок 3).

Модуль MCM-950, подключенный внешним интерфейсом к локальной сети, будет выполнять роль шлюза безопасности, а маршрутизатор – функции подключения сети к Internet. Основной задачей модуля при этом будет шифрование трафика, а функции Firewall можно возложить либо на маршрутизатор, либо на модуль.

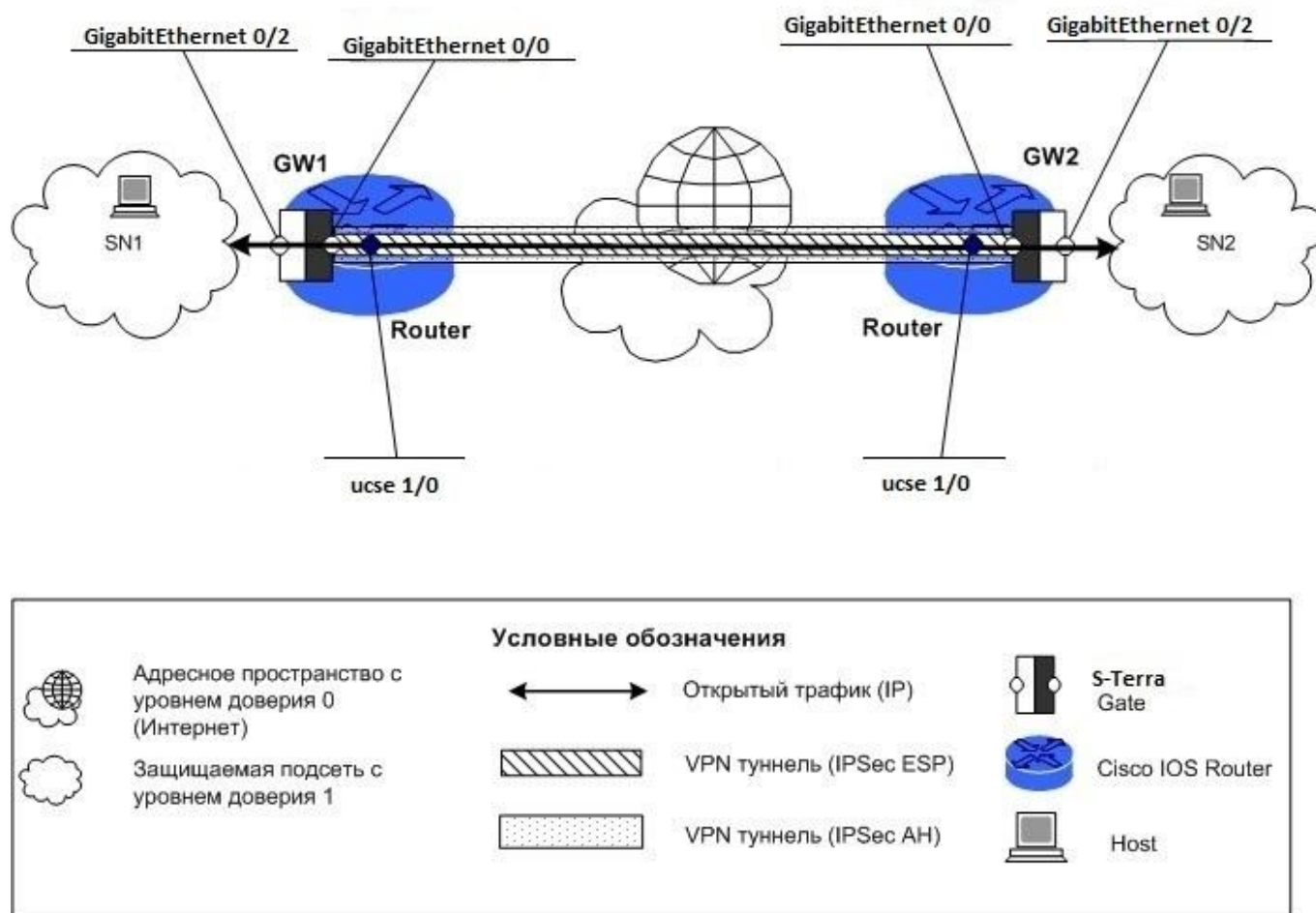


Рисунок 3

Настройка маршрутизаторов сложности не представляет и хорошо описана в многочисленных примерах на www.cisco.com. Приведем лишь несколько ссылок по настройке IOS Firewall и access-lists:

http://www.cisco.com/en/US/tech/tk648/tk361/tech_configuration_examples_list.html

Настройка политики безопасности шлюзов

Настройка IPsec туннелей на модуле мало отличается от настройки в IOS. В CLI модуля можно использовать те же команды и синтаксис, как и в IOS.

Будем предполагать, что инициализация программного обеспечения уже выполнена так, что модуль имеет нужные IP-адреса на интерфейсах.

Для примера настройки S-Terra Gate соберем стенд (Рисунок 4). Сценарий иллюстрирует построение защищенного соединения между двумя подсетями SN1 и SN2, которые защищаются шлюзами безопасности в исполнении MCM-950. Для защиты будет построен VPN туннель между устройствами MCM950-1 и MCM950-2. Устройства IPhost1 и IPhost2 смогут общаться между собой по защищенному каналу (VPN). Все остальные соединения разрешены, но защищаться не будут. Маршрутизаторы Cisco будут настроены статически NAT-ировать внутренние адреса MCM950 в свои внешние secondary-адреса.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6R4. Модуль «MCM-950» с ПО С-Терра Шлюз 4.1.

Параметры защищенного соединения:

- IKE параметры:
 - Аутентификация на сертификатах – GOST R 34.10-2001 Signature;
 - Алгоритм шифрования – GOST 28147-89 Encryption;
 - Алгоритм вычисления хеш-функции – GOST R 34.11-94 Hash;
 - Группа Диффи-Хеллмана – VKO GOST R 34.10-2001;
- IPsec параметры:
 - ESP алгоритм шифрования – ESP_GOST-4M-IMIT cipher.

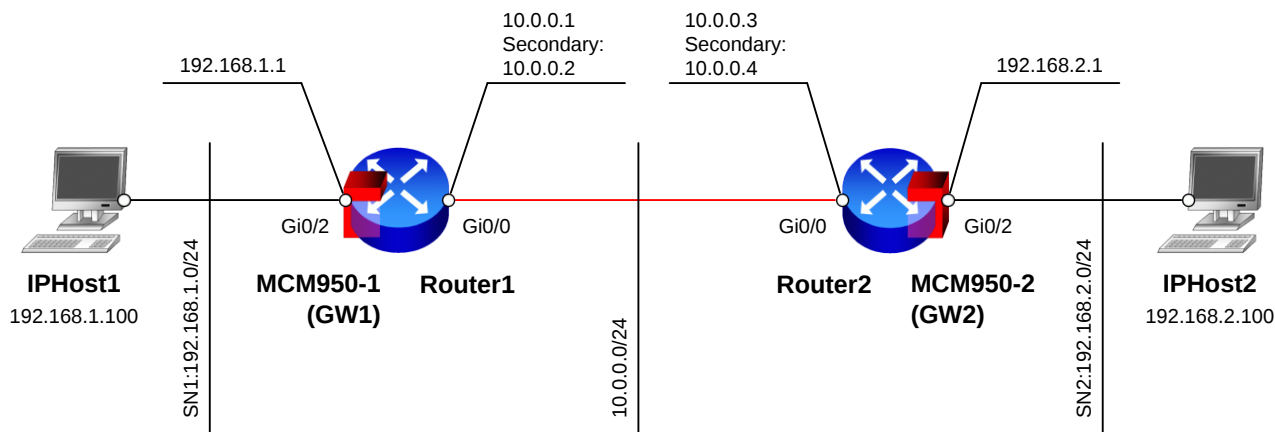


Рисунок 4

Предварительные настройки

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

На устройствах Host1 и Host2 зададим IP-адреса, а также адреса маршрутизаторов по умолчанию (default gateway):

- на Host1 в качестве шлюза по умолчанию назначим IP-адрес внутреннего интерфейса шлюза безопасности MCM950-1 (GW1) – 192.168.1.1.
- на Host2 в качестве шлюза по умолчанию назначим IP-адрес внутреннего интерфейса шлюза безопасности MCM950-2 (GW2) – 192.168.2.1.

Доступ к консоли MCM950-1 производится через маршрутизатор Router1 командой: `ucse 1 session host`, при этом интерфейс `ucse1/0` на маршрутизаторе Router1 должен быть поднят и иметь IP-адрес. Логическое сетевое подключение маршрутизатора и модуля представлено на Рисунок 5.

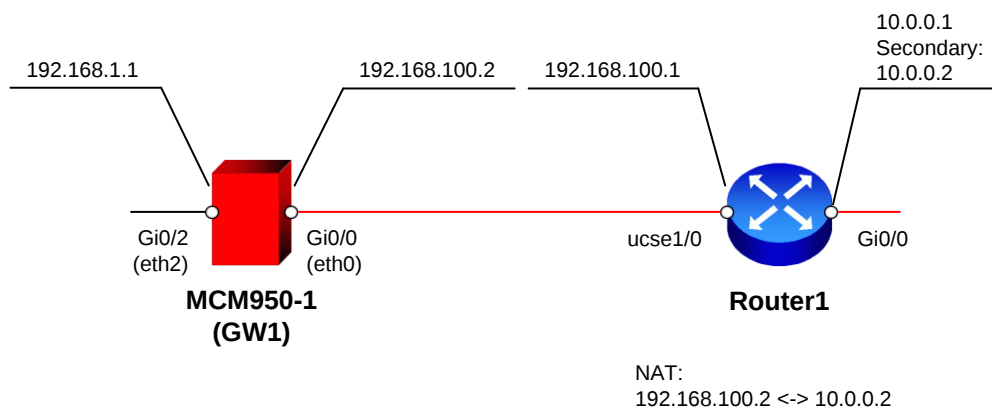


Рисунок 5

Возврат к консоли `cisco` можно осуществить, пошлав Brake-сигнал (нажать `Ctrl+Shift+6`, а после нажать `x`).

На маршрутизаторе Router1 необходимо настроить IP-адрес интерфейса `ucse 1/0` для связи с MCM950, а так же статический NAT, который будет преобразовывать внутренний адрес GW1 (192.168.100.2) во внешний secondary-адрес (10.0.0.1) и наоборот:

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 ip address 10.0.0.2 255.255.255.0 secondary
 ip nat outside
!
!
interface ucse 1/0
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
!
ip nat inside source static 192.168.100.2 10.0.0.2
ip route 0.0.0.0 0.0.0.0 10.0.0.3
```

Маршрутизатор Router2 настраивается аналогично Router1. Внутренняя сеть между MCM950 и маршрутизатором – 192.168.101.0/24.

Настроим интерфейсы Шлюза безопасности MCM950-1 (GW1) согласно схеме стенда, для этого перейдем в `cisco-like` консоль:

```
root@sterragate:~# cs_console
```

```
sterragate>en
Password: (по умолчанию - csp)
sterragate#conf t
sterragate(config)#interface GigabitEthernet 0/0
sterragate(config-if)#ip address 192.168.100.2 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
sterragate(config)#interface GigabitEthernet 0/2
sterragate(config-if)#ip address 192.168.1.1 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
sterragate(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.1
sterragate(config)#end
sterragate#exit
```

Настройка интерфейсов Шлюза безопасности МСМ950-2 (GW2) производится аналогичным образом.

Регистрация СА сертификата (сертификата УЦ)

Для регистрации СА сертификата (сертификата УЦ) необходимо выполнить следующие действия:

Шаг 1: установите правильное системное время. Например, 10 апреля 2013 года 13:15:

```
root@sterragate:~# date 041013152013
Wed Apr 10 13:15:00 UTC 2013
```

Шаг 2: создайте папку /certs:

```
root@sterragate:~# mkdir /certs
```

Шаг 3: доставьте файл СА сертификата на шлюз безопасности в предварительно созданный на нем каталог /certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, применив команду:

```
pscp <CA file path>/<CA file name> root@<gate address>:/<path>
```

Например:

```
pscp D:\ca.cer root@192.168.1.1:/certs
...
Store key in cache? (y/n)
root@192.168.1.1's password:
```

Важно: Среда передачи в этом случае должна быть доверенной.

Шаг 4: с помощью утилиты cert_mgr, входящей в состав продукта С-Терра Шлюз, зарегистрируйте сертификат в базе продукта:

```
root@sterragate:~# cert_mgr import -f /certs/ca.cer -t

1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-
X64-CA
```

Параметр -t в данной команде указывает на то, что импортируемый сертификат – корневой (сертификат УЦ).

Регистрация локального сертификата

Для регистрации локального сертификата в базе продукта выполните следующие действия:

Шаг 1: сформируйте запрос на сертификат с использованием утилиты cert_mgr, например:

```

root@sterragate:~# cert_mgr create -subj
"C=RU,OU=Research,CN=GW1" -GOST_R3410EL

Press keys...
[.....]
-----BEGIN CERTIFICATE REQUEST-----
MIIBCjCBuAIBADAuMQswCQYDVQQGEwJSVTERMA8GA1UECxMIUmVzZWFFyY2gx
DDAKBgNVBAMTA0dXMTBjMBwGBiqFAwICEzASBgqhQMCAiMBBgqhQMCAh4B
A0MABECTQeB5UoPsTbSs8obnrQ6KMJwpc/BFrUgfiI6AjQ195ccE4D5jEAq8m
BgNVHQ8EBAMCB4AwCgYGKoUDAgIDBQADQBAuCzk8bASJqbP5pYHAG5A3LKx
OPFjiF1m+2/WkxGkWJWEm5gjNNyWquslmxLq9nX2rff4X3E5xF40iudzHoZz
-----END CERTIFICATE REQUEST-----

```

Шаг 2: передайте полученный запрос на сертификат на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документации на [«Программный комплекс С-Терра Шлюз. Версия 4.1. Приложение»](#), раздел «Создание локального сертификата с использованием СКЗИ «КриптоПро CSP»).

Шаг 3: перенесите полученный файл на шлюз безопасности (параметры pscr описаны выше).

Шаг 4: зарегистрируйте локальный сертификат в базе продукта, применив утилиту cert_mgr:

```

root@sterragate:~# cert_mgr import -f /certs/gw1.cer

1 OK C=RU,OU=Research,CN=GW1

```

Шаг 5: убедитесь, что сертификаты импортированы успешно:

```

root@sterragate:~# cert_mgr show

Found 2 certificates. No CRLs found.
1 Status: trusted C=RU,L=Moscow,O=S-Terra
CSP,OU=Research,CN=CA-W2008SP1-X64-CA
2 Status: local C=RU,OU=Research,CN=GW1

```

Настройка шлюза MCM950-1 (GW1)

Настройку шлюза безопасности GW1 (путем задания политики безопасности) будем выполнять в интерфейсе командной строки.

Шаг 1: для входа в консоль перейдите в каталог /opt/VPNagent/bin/ и запустите cs_console:

```

root@sterragate:~# cs_console
sterragate>en
Password: (по умолчанию - csp)
sterragate#conf t - переходим в режим настройки
sterragate(config)#hostname GW1 - сменим название шлюза
GW1(config)#crypto isakmp identity dn - зададим тип
идентификации

```

Шаг 2: задайте параметры для протокола IKE:

```

GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)#hash gost
GW1(config-isakmp)#encryption gost
GW1(config-isakmp)#authentication gost-sig
GW1(config-isakmp)#group vko
GW1(config-isakmp)#exit

```

Шаг 3: создайте набор преобразований для IPsec:

```

GW1(config)#crypto ipsec transform-set TSET esp-gost28147-4m-
imit

```

```
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

- Шаг 4:** опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
GW1(config-ext-nacl)#exit
```

- Шаг 5:** создайте крипто-карту:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs vko
GW1(config-crypto-map)#set peer 10.0.0.2
GW1(config-crypto-map)#exit
```

- Шаг 6:** привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
GW1(config)#interface GigabitEthernet 0/0
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
```

- Шаг 7:** отключите обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-
terra_technological_trustpoint
GW1(ca-trustpoint)#revocation-check none
GW1(ca-trustpoint)#exit
```

- Шаг 8:** настройка устройства GW1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
GW1(config)#end
GW1#exit
```

Если в конфигурационном режиме запустить команду `show running-config`, то получим полный [текст cisco-like конфигурации](#).

Текст cisco-like конфигурации шлюза GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW1
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
encr gost
```

```

hash gost
authentication gost-sig
group vko
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extended LIST
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
match address LIST
set transform-set TSET
set pfs vko
set peer 10.0.0.4
!
interface GigabitEthernet0/0
ip address 192.168.100.2 255.255.255.0
crypto map CMAP
!
interface GigabitEthernet0/2
ip address 192.168.1.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
crypto pki trustpoint s-terra_technological_trustpoint
revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
...
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F

quit
!
end

```

Настройка шлюза МСМ950-2 (GW2)

Настройка шлюза безопасности МСМ950-2 (GW2) производится аналогично настройке шлюза МСМ950-1 (GW1) с заменой IP-адресов в необходимых разделах конфигурации.

Текст cisco-like конфигурации GW2

```

!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW2
enable password csp
!
!
!

```

```
logging trap debugging
!
!
crypto isakmp policy 1
  encr gost
  hash gost
  authentication gost-sig
  group vko
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extended LIST
  permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
  match address LIST
  set transform-set TSET
  set pfs vko
  set peer 10.0.0.2
!
interface GigabitEthernet0/0
  ip address 192.168.101.2 255.255.255.0
  crypto map CMAP
!
interface GigabitEthernet0/2
  ip address 192.168.2.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 192.168.101.1
!
crypto pki trustpoint s-terra_technological_trustpoint
  revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530
...
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F

quit
!
end
```

Проверка работоспособности стенда

После загрузки конфигурации на GW1 и GW2 и настройки маршрутизации, проверим работу VPN. Для этого инициируем трафик между Host1 и Host2 с помощью команды `Ping`. В работоспособности туннеля при этом можно убедиться по наличию IPsec SA в выводе команды `sa_mgr show`. Ping также должен работать без потери пакетов.

Настройка модуля для работы с удаленными клиентами

Следующий сценарий иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности в исполнении модуля «MCM-950», и мобильным клиентом С-Терра Клиент (Рисунок 6). Для защиты будет построен VPN туннель между устройствами MCM950-1 и Client1. Устройство Client1 сможет общаться по защищенному каналу (VPN) с устройствами из подсети SN1 (в частности с IPHost1). Адрес мобильного клиента неизвестен заранее – клиент находится за динамическим NAT-ом. Маршрутизатор Router1 будет настроен статически NAT-ировать внутренний адрес MCM950 в свой внешний secondary-адрес.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6R4. На MCM950 инициализировано ПО С-Терра Шлюз 4.1. На устройстве Client1 – установлен С-Терра Клиент 4.1.

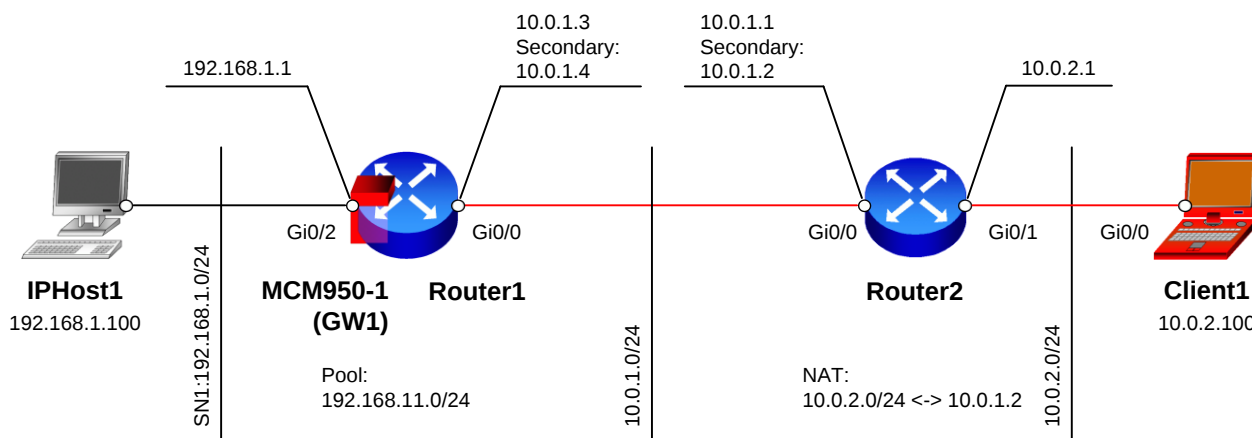


Рисунок 6

Параметры защищенного соединения:

- IKE параметры:
 - Аутентификация на сертификатах – GOST R 34.10-2001 Signature;
 - Алгоритм шифрования – GOST 28147-89 Encryption;
 - Алгоритм вычисления хеш-функции – GOST R 34.11-94 Hash;
 - Группа Диффи-Хеллмана – VKO GOST R 34.10-2001;
- IPsec параметры:
 - ESP алгоритм шифрования – ESP_GOST-4M-IMIT cipher.

Настройка маршрутизатора Router1

Доступ к консоли MCM950-1 производится через маршрутизатор Router1 командой: `ucse 1 session host`, при этом интерфейс `ucse1/0` на маршрутизаторе Router1 должен быть поднят и иметь IP-адрес. Логическое сетевое подключение маршрутизатора и модуля представлено на Рисунок 7.

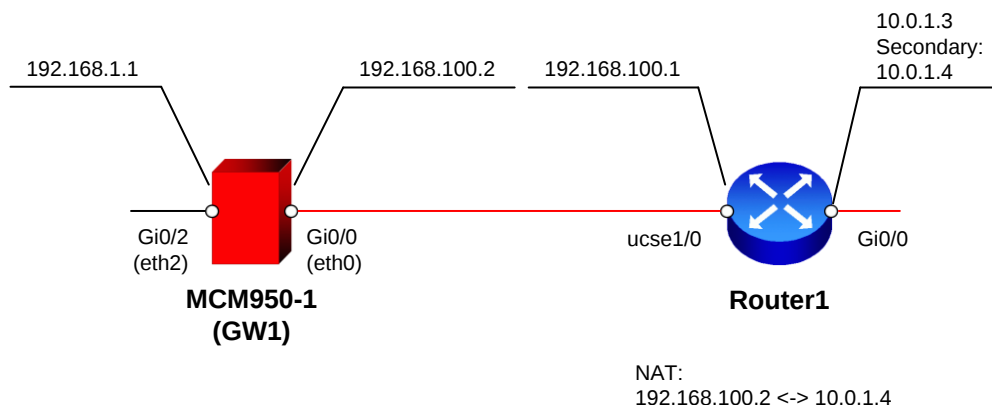


Рисунок 7

Возврат к консоли `cisco` можно осуществить, послав Brake-сигнал (нажать `Ctrl+Shift+6`, а после нажать `x`).

На маршрутизаторе Router1 необходимо настроить IP-адрес интерфейса `ucse 1/0` для связи с MCM950, а так же статический NAT, который будет преобразовывать внутренний адрес GW1 (192.168.100.2) во внешний secondary-адрес (10.0.1.4) и наоборот.

Интерфейс `Gi0/0` устройства Router1 в реальной схеме должен быть подключен к сети Интернет и иметь 2 “белых” IP-адреса. Адреса из подсети 10.0.1.0.24 даны для примера.

Необходимые настройки представлены ниже:

```
interface GigabitEthernet 0/0
 ip address 10.0.1.3 255.255.255.0
 ip address 10.0.1.4 255.255.255.0 secondary
 ip nat outside
!
!
interface ucse 1/0
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
!
ip nat inside source static 192.168.100.2 10.0.1.4
ip route 0.0.0.0 0.0.0.0 10.0.1.1
```

Настройка устройства Router2

На устройстве Router2 необходимо настроить динамический NAT, который будет преобразовывать адреса из подсети 10.0.2.0/24 во внешний secondary-адрес 10.0.1.2 и наоборот.

Настройка устройства IPHost1

На устройстве IPHost1 задайте IP-адрес, а в качестве шлюза по умолчанию укажите IP-адрес внутреннего интерфейса шлюза безопасности MCM950-1 (GW1) – 192.168.1.1.

Регистрация сертификатов

Процесс регистрации сертификатов CA и локального аналогичен описанному в соответствующих разделах в предыдущем примере.

Настройка шлюза безопасности MCM950-1 (GW1)

IP-адреса для интерфейсов рекомендуется настроить через cisco-like консоль.

Шаг 1: для входа в консоль запустите cs_console:

```
root@sterragate:~# cs_console
sterragate>en
Password: (по умолчанию - csp)
```

Шаг 2: перейдите в режим настройки:

```
sterragate#conf t
```

Шаг 3: в настройках интерфейсов задайте IP-адреса:

```
sterragate(config)#interface GigabitEthernet 0/0
sterragate(config-if)#ip address 192.168.100.2 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
sterragate(config)#interface GigabitEthernet 0/2
sterragate(config-if)#ip address 192.168.1.1 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
```

Шаг 4: задайте адрес шлюза по умолчанию:

```
sterragate(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.1
```

Шаг 5: выйдите из cisco-like интерфейса:

```
sterragate(config)#end
sterragate#exit
```

Шаг 6: далее сменим название шлюза:

```
sterragate(config)#hostname GW1
```

Шаг 7: задайте тип идентификации:

```
GW1(config)#crypto isakmp identity dn
```

Шаг 8: задайте параметры для IKE:

```
GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)#hash gost
GW1(config-isakmp)#encryption gost
GW1(config-isakmp)#authentication gost-sig
GW1(config-isakmp)#group vko
GW1(config-isakmp)#exit
```

Шаг 9: создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-gost28147-4m-
imit
```

```
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

Шаг 10: задайте пул, из которого будет выдан адрес клиенту:

```
GW1(config)#ip local pool POOL 192.168.11.1 192.168.11.254
```

Шаг 11: опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255
192.168.11.0 0.0.0.255
GW1(config-ext-nacl)#exit
```

Шаг 12: создайте динамическую крипто-карту:

```
GW1(config)#crypto dynamic-map DMAP 1
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs vko
GW1(config-crypto-map)#set pool POOL
GW1(config-crypto-map)#reverse-route
GW1(config-crypto-map)#exit
```

Шаг 13: привяжите динамическую карту к статической:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp dynamic DMAP
```

Шаг 14: привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
GW1(config)#interface GigabitEthernet 0/0
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
```

Шаг 15: отключите обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-
terra_technological_trustpoint
GW1(ca-trustpoint)#revocation-check none
GW1(ca-trustpoint)#exit
```

Шаг 16: настройка устройства GW1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
GW1(config)#end
GW1#exit
```

Текст cisco-like конфигурации шлюза GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW1
enable password csp
!
!
!
logging trap debugging
!
!
```

```
crypto isakmp policy 1
  encr gost
  hash gost
  authentication gost-sig
  group vko
!
ip local pool POOL 192.168.11.1 192.168.11.254
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extended LIST
  permit ip 192.168.1.0 0.0.0.255 192.168.11.0 0.0.0.255
!
!
crypto dynamic-map DMAP 1
  match address LIST
  set transform-set TSET
  set pfs vko
  set pool POOL
  reverse-route
!
crypto map CMAP 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
  ip address 192.168.100.2 255.255.255.0
  crypto map CMAP
!
interface GigabitEthernet0/1
  no ip address
  shutdown
!
interface GigabitEthernet0/2
  ip address 192.168.1.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
crypto pki trustpoint s-terra_technological_trustpoint
  revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530
...
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F

quit
!
end
```

Подготовка клиентского ПО

Программное обеспечение для клиента разработано с идеей обеспечения корпоративной безопасности. Как результат – все настройки политики безопасности прописываются администратором в процессе создания инсталляционного пакета для клиента. Пользователю остается лишь установить пакет на своей машине и проверить как работает VPN туннель. Процесс подготовки клиентского ПО выглядит следующим образом:

- Шаг 1:** Администратор устанавливает S-Terra Client AdminTool.
- Шаг 2:** Администратор настраивает параметры туннелей и создает клиентский инсталляционный пакет.
- Шаг 3:** Пользователь устанавливает этот пакет на своей машине и проверяет его работоспособность.

Давайте проделаем эти шаги.

На машине администратора установим и запустим “S-Terra Client AdminTool”. Во вкладке *License* введем параметры лицензии на C-Terra Клиент 4.1 (Рисунок 8):

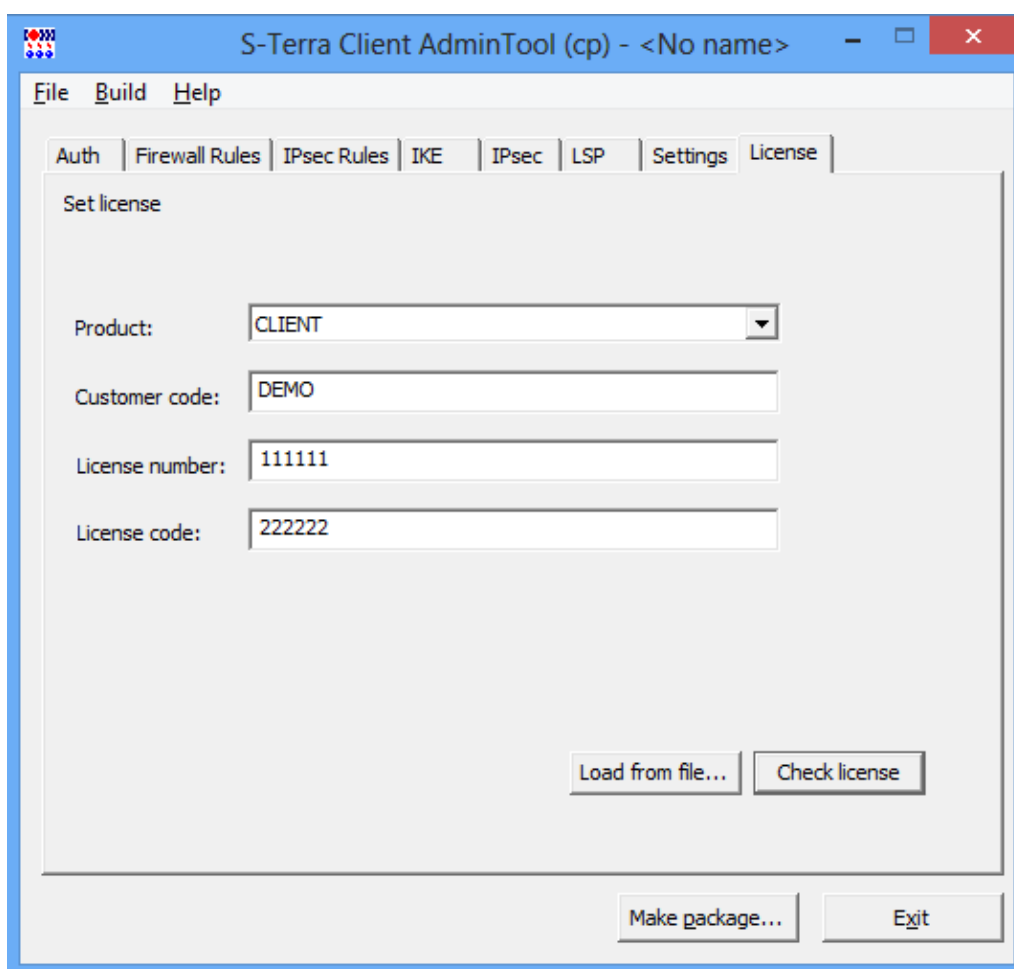


Рисунок 8

На вкладке “Auth” выполните следующие действия (Рисунок 9):

- в данном сценарии используется метод аутентификации на сертификатах - пункт “Use certificate” выбран по умолчанию;
- в поле “CA certificate” и “User certificate” укажите путь к сертификату УЦ и пользовательскому сертификату, размещенных на машине администратора;
- в поле “User container name” укажите уникальное имя контейнера, размещенного на компьютере пользователя, на который будет установлен С-Терра Клиент, в данном случае \\.\REGISTRY\Client1.
- в поле “User identity type” выберите в качестве идентификатора, пересылаемого партнеру, “DistinguishedName”. Поле “Value” заполняется автоматически..
- установите флажок “Check consistency now”, если нужно выполнить проверку соответствия сертификата пользователя и секретного ключа в контейнере, который нужно разместить на машине администратора. Для этого нажмите кнопку “[...]” и выберите нужный контейнер, и укажите пароль к нему. Такая проверка будет выполнена при создании инсталляционного пакета.
- установите флажок “Copy container”, если нужно во время инсталляции С-Терра Клиент на компьютере пользователя, выполнить копирование контейнера с секретным ключом, указанного в поле Source container name, в другой контейнер с именем, указанным в поле User container name. Если имеются пароли к контейнерам, то укажите их (в данном примере происходит копирование контейнера с дискеты в реестр с контейнером Client1).

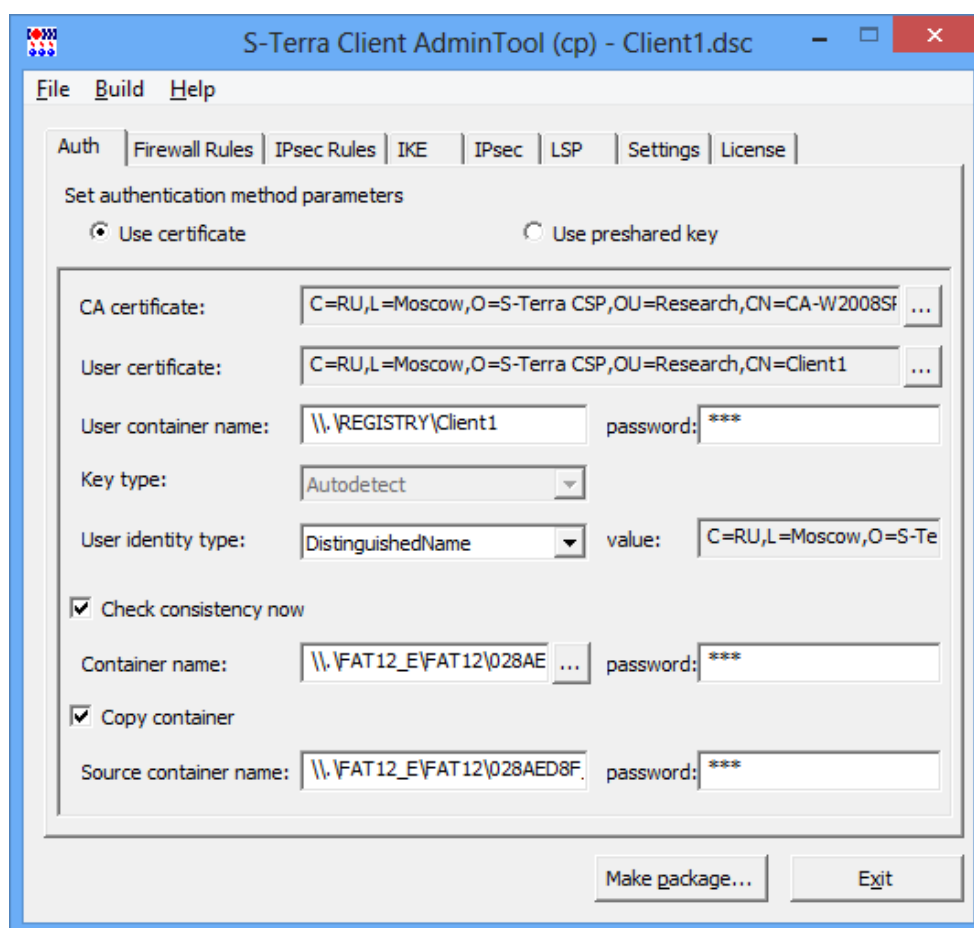


Рисунок 9

На вкладке “Firewall Rules” (Рисунок 10) можно настроить правила фильтрации трафика. В данном случае оставим настройки по умолчанию – пропускать весь трафик.

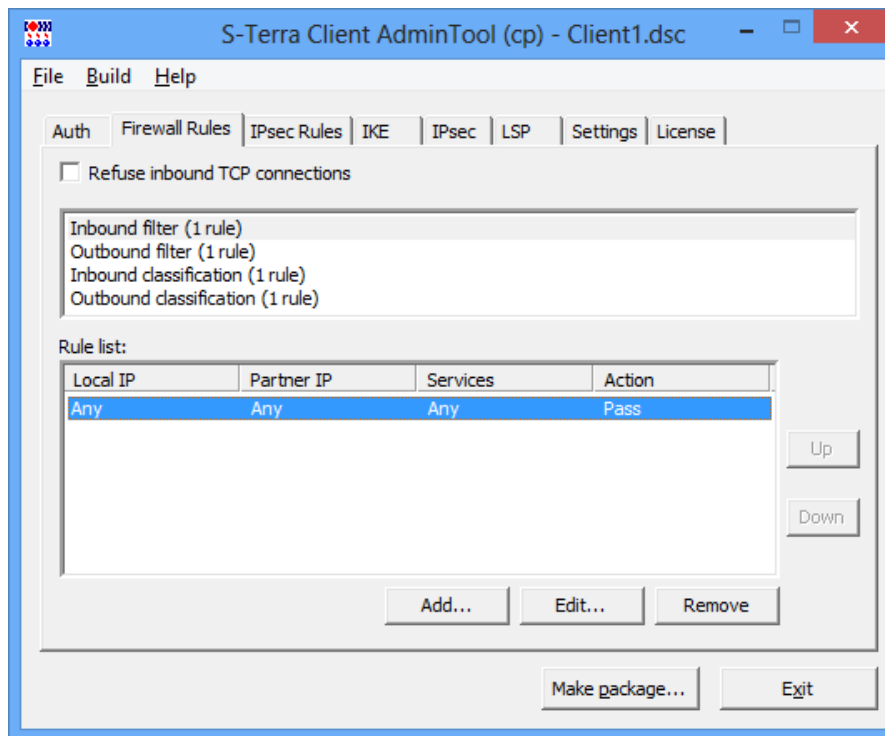


Рисунок 10

На вкладке “IPsec Rules” (Рисунок 11) добавьте правило для трафика, подлежащего шифрованию, IP-адрес шлюза, с которым будет построено защищенное соединение (Рисунок 12). Так же установите флажок “Request IKECFG address”. Добавленному правилу увеличьте приоритет.

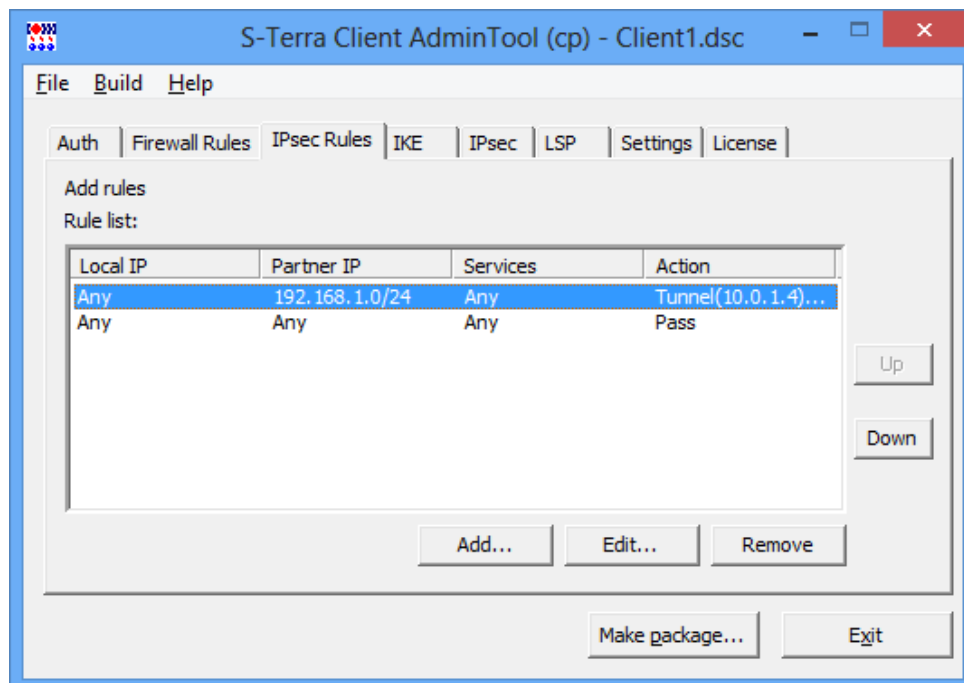


Рисунок 11

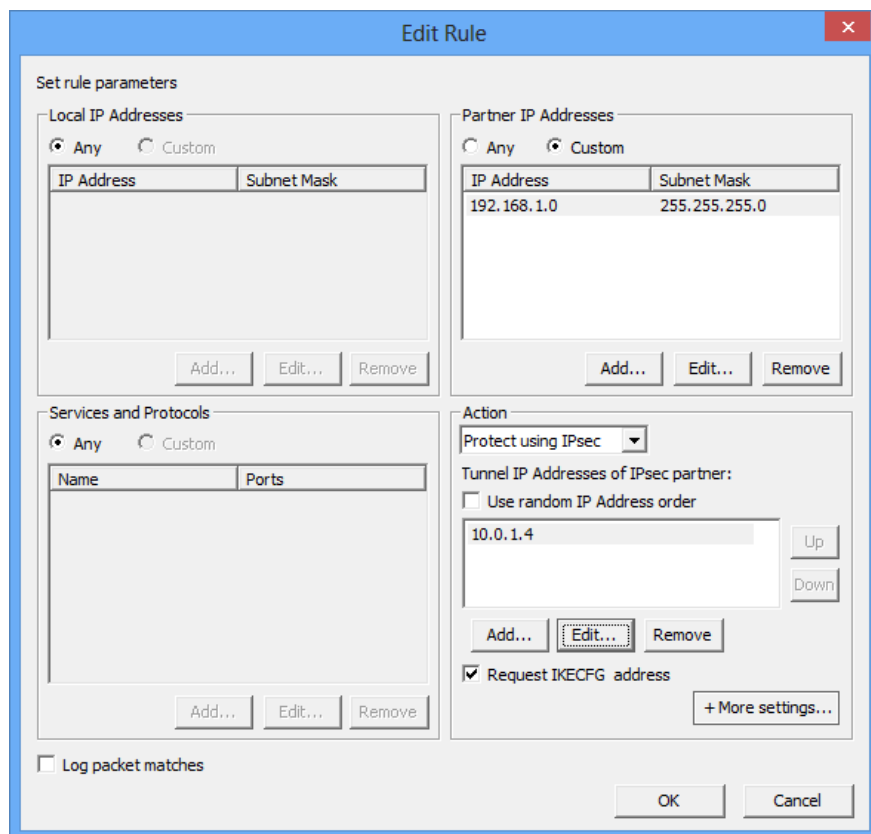


Рисунок 12

На вкладке “IPsec” поднимите вверх правило, соответствующее настроенному на шлюзе IPsec Transform Set и выберите “Group” – “VKO_1B” (Рисунок 13).

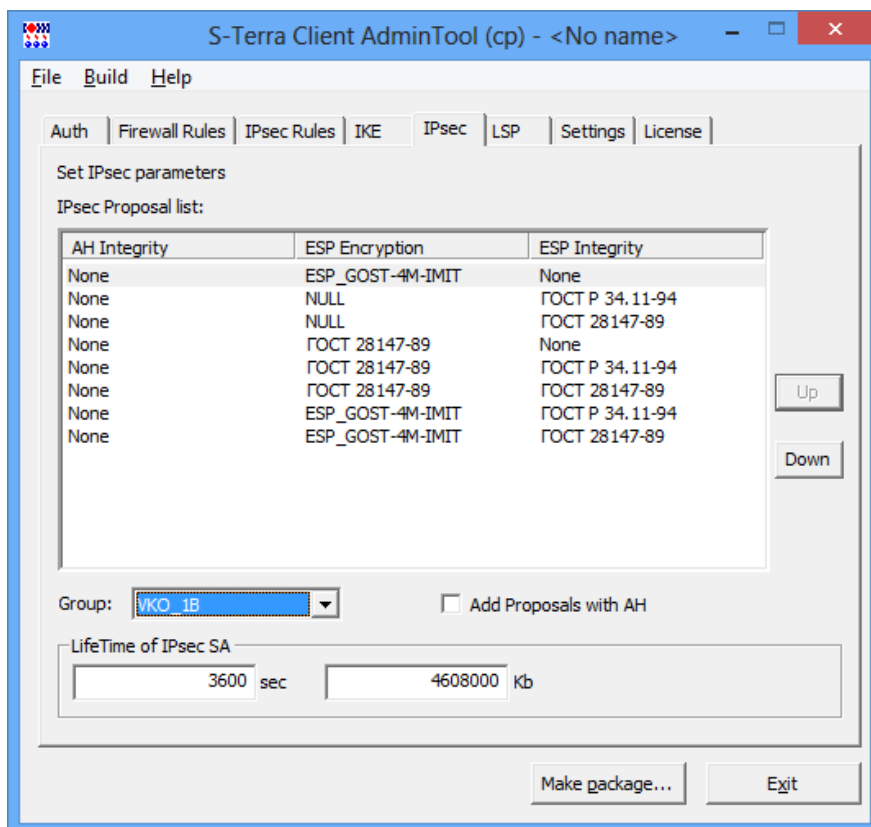


Рисунок 13

Остальные настройки можно оставить без изменений. Главное мы сделали: указали, что шифровать, как шифровать и с кем устанавливать соединение.

Теперь можно нажимать кнопку `Make package...` (Рисунок 14) Укажем имя и выберем каталог, куда положить инсталляционный пакет. После нажатия кнопки `OK` за несколько секунд будет создан инсталляционный файл.

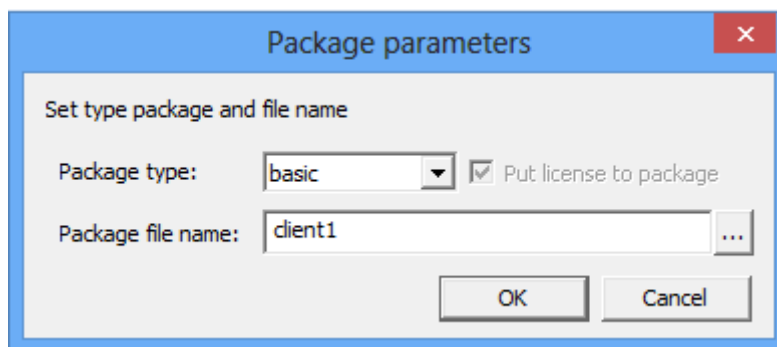


Рисунок 14

Установите на клиентском компьютере полученный ехе-файл и перезагрузите компьютер (на операционных системах Windows 7 и Windows 8 перезагрузка не требуется).

В трее появится иконка S-Terra Client (Рисунок 15). Для начала работы необходимо залогиниться (Рисунок 16). По умолчанию пароль отсутствует, в дальнейшем его можно установить.



Рисунок 15

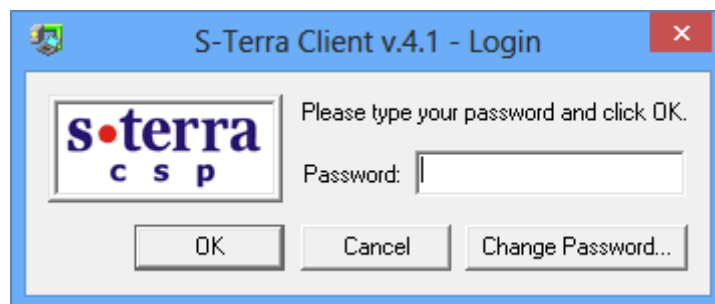


Рисунок 16

Текст LSP конфигурации для устройства Client1

```
GlobalParameters (
    Title = "This LSP was automatically generated by S-Terra Client
AdminTool (cp) at 2014.06.20 14:32:18"
    Version = LSP_4_1
    CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
    ResponseTimeout = 200
    HoldConnectTimeout = 60
    DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
```

```

DistinguishedName *= CertDescription(
    Subject *= COMPLETE, "C=RU, L=Moscow, O=S-Terra
CSP, OU=Research, CN=Client1"
)
)
CertDescription local_cert_dsc_01(
    Subject *= COMPLETE, "C=RU, L=Moscow, O=S-Terra
CSP, OU=Research, CN=Client1"
    Issuer *= COMPLETE, "C=RU, L=Moscow, O=S-Terra CSP, OU=Research, CN=CA-
W2008SP1-X64-CA"
    SerialNumber = "6118B13500000000000002"
    FingerprintMD5 = "5063E6A36023E8D35258E054A09CA586"
)
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_02(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= VKO_1B
)
IKETransform ike_trf_03(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= MODP_1536
)
IKETransform ike_trf_04(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= MODP_1024
)
IKETransform ike_trf_05(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= MODP_768
)
ESPTransform esp_trf_01(
    CipherAlg *= "G2814789CPR01-K288-CNTMAC-253"
    LifetimeSeconds = 3600

```

```
        LifetimeKilobytes = 4608000
    )
    ESPProposal esp_proposal_01(
        Transform *=esp_trf_01
    )
    ESPTransform esp_trf_02(
        IntegrityAlg *= "GR341194CPR01-H96-HMAC-65534"
        CipherAlg *= "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
    ESPProposal esp_proposal_02(
        Transform *=esp_trf_02
    )
    ESPTransform esp_trf_03(
        IntegrityAlg *= "GR341194CPR01-H96-HMAC-65534"
        CipherAlg *= "NULL"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
    ESPProposal esp_proposal_03(
        Transform *=esp_trf_03
    )
    ESPTransform esp_trf_04(
        IntegrityAlg *= "G2814789CPR01-K256-MAC-65535"
        CipherAlg *= "NULL"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
    ESPProposal esp_proposal_04(
        Transform *=esp_trf_04
    )
    ESPTransform esp_trf_05(
        CipherAlg *= "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
    ESPProposal esp_proposal_05(
        Transform *=esp_trf_05
    )
    ESPTransform esp_trf_06(
        IntegrityAlg *= "G2814789CPR01-K256-MAC-65535"
        CipherAlg *= "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
    ESPProposal esp_proposal_06(
        Transform *=esp_trf_06
    )
    ESPTransform esp_trf_07(
        IntegrityAlg *= "GR341194CPR01-H96-HMAC-65534"
        CipherAlg *= "G2814789CPR01-K288-CNTMAC-253"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
    ESPProposal esp_proposal_07(
        Transform *=esp_trf_07
    )
    ESPTransform esp_trf_08(
        IntegrityAlg *= "G2814789CPR01-K256-MAC-65535"
        CipherAlg *= "G2814789CPR01-K288-CNTMAC-253"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
```

```

)
ESPProposal esp_proposal_08(
    Transform *=esp_trf_08
)
IKERule ike_rule_with_ikecfg(
    DoNotUseDPD = FALSE
    DPDIIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_02,ike_trf_03,ike_trf_04,ike_trf_05
    IKECFGRequestAddress = TRUE
)
IPsecAction ipsec_action_01(
    PersistentConnection = TRUE
    TunnelingParameters *=
        TunnelEntry(
            PeerIPAddress = 10.0.1.4
            Assemble = TRUE
            ReRoute = FALSE
        )
    ContainedProposals *=
(esp_proposal_01),(esp_proposal_02),(esp_proposal_03),(esp_proposal_04
), (esp_proposal_05),(esp_proposal_06),(esp_proposal_07),(esp_proposal_
08)
    GroupID *= VKO_1B,MODP_1536,MODP_1024,MODP_768
    IKERule = ike_rule_with_ikecfg
)
FilterChain filter_chain_input(
    Filters *= Filter(
        ProtocolID *= 17
        DestinationPort *= 500
        Action = PASS
        LogEventID = "pass_action_02_01"
    ),Filter(
        ProtocolID *= 17
        DestinationPort *= 4500
        Action = PASS
        LogEventID = "pass_action_02_02"
    ),Filter(
        SourceIP *= 10.0.1.4
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_03_01"
    ),Filter(
        SourceIP *= 10.0.1.4
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_03_02"
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_04"
    )
)
FilterChain filter_chain_output(
    Filters *= Filter(
        ProtocolID *= 17
        SourcePort *= 500
        Action = PASS
        LogEventID = "pass_action_05_01"
    ),Filter(
        ProtocolID *= 17
        SourcePort *= 4500

```

```

        Action = PASS
        LogEventID = "pass_action_05_02"
    ),Filter(
        DestinationIP *= 10.0.1.4
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_06_01"
    ),Filter(
        DestinationIP *= 10.0.1.4
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_06_02"
    ),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"
    ),Filter(
        ProtocolID *= 17
        SourcePort *= 4500
        Action = PASS
        LogEventID = "pass_action_10_02"
    ),Filter(
        DestinationIP *= 192.168.1.0/24
        Action = PASS
        ExtendedAction *= ipsec<sa=ipsec_action_01>
        LogEventID = "ipsec_action_01"
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_11"
    )
)
NetworkInterface(
    InputFilter = filter_chain_input
    OutputFilter = filter_chain_output
    InputClassification = filter_chain_classification_input
    OutputClassification = filter_chain_classification_output
    IPsecPolicy = filter_chain_ipsec
)

```

Проверка клиентского соединения

Туннель между клиентом и модулем устанавливается автоматически, как только клиент отправит пакет в сеть SN1 или SN2. Ping должен заработать сразу – с небольшой задержкой в отклике на первый пакет. Убедиться, что трафик действительно шифруется, можно по наличию IPsec SA на клиенте, запустив VPN SA Monitor, и модуле, выполнив команду `sa_mgr show`.

Дополнительная информация

Cisco.com

Для получения документации по продуктам компании Cisco Systems и дополнительной информации можно обратиться на сайт www.cisco.com.

Информация на русском языке доступна на Российском сайте компании Cisco Systems по адресу:

<http://www.cisco.com/global/RU/index.shtml>

S-Terra.com

Получить информацию по продуктам компании «С-Терра СиЭсПи» можно по адресу:

<http://www.s-terra.com/products/productline/>

С документацией по работе с продуктами компании можно ознакомиться по адресу:

<http://www.s-terra.com/support/documents/>

Информацию по технической поддержке можно посмотреть по адресу:

<http://www.s-terra.com/support/support/>