

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 NME-RVPN (МСМ)

РЛКЕ.00009-01 90 03

02.09.2014

Содержание

Инструкция по подготовке к работе модуля NME-RVPN (MCM)	3
Комплект поставки	4
Подготовка модуля к работе	5
Установка модуля в маршрутизатор.....	6
Инициализация программного комплекса S-Terra Gate при первом старте	7
Подключение к локальной сети.....	8
Архитектура ПО С-Терра Шлюз	9
Пример топологии	11
Настройка политики безопасности шлюзов	12
Предварительные настройки	12
Настройка шлюза GW1	13
Настройка шлюза GW2	18
Проверка работоспособности стенда	19
Настройка модуля для работы с удаленными клиентами	20
Настройка маршрутизатора Router1	20
Настройка устройства Router2	21
Настройка устройства IPHost1	21
Регистрация сертификатов	22
Настройка шлюза безопасности MCM-1 (GW1)	22
Подготовка клиентского ПО	25
Проверка клиентского соединения	33
Дополнительная информация.....	34

Инструкция по подготовке к работе модуля NME-RVPN (MCM)

Модуль NME-RVPN (Network Module Enhanced Russian VPN) в исполнении MCM (Модуль Сетевой Модернизированный) производится в соответствии с технологическим процессом, согласованным с Центром ФСБ России «Порядком организации производства изделия «Модуль Сетевой Модернизированный (MCM)» в рамках подконтрольного технологического процесса на территории Российской Федерации».

Далее в документации этот модуль будем называть «Модуль NME-RVPN (MCM)», «модуль MCM», «MCM» или «модуль».

Модуль работает на маршрутизаторах Cisco ISR второго поколения (серии 2900, 3900) и первого (серии 2800, 3800).

Аппаратно модуль представляет собой вычислительную платформу на базе процессора Intel Celeron M, 1 ГГц, 512 Мб RAM и 1Гб постоянной памяти, размещенной на компакт-флеш карте.

Модуль работает независимо от ОС маршрутизатора, все обмены между ними производятся только по сети. Маршрутизаторы второго поколения работают под управлением ОС Cisco IOS, начиная с версии 15.x.x, а первого – под управлением ОС Cisco IOS версии 12.4(11)T и выше.

На модуль устанавливается ПО «Программный комплекс С-Терра Шлюз. Версия 4.1», функционирующее под управлением ОС Debian GNU/Linux 6.

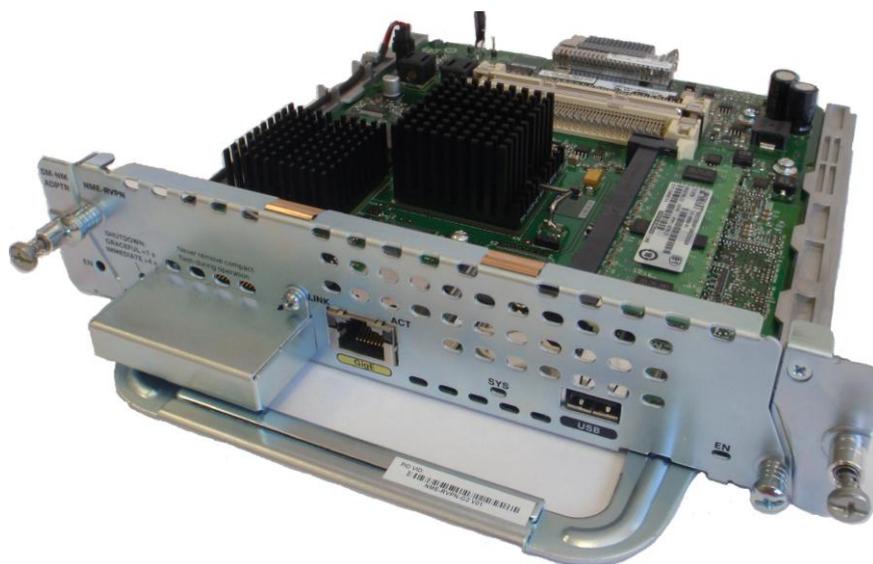


Рисунок 1

В этом документе описано как подготовить модуль MCM к работе – установить модуль в маршрутизатор, инициализировать на нем программный комплекс С-Терра Шлюз 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 NME-RVPN модуля \(MCM\)» \[1\]](#).

Комплект поставки

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

модуль NME-RVPN (MCM), установленный в сетевой модульный адаптер, с вставленной в него компакт-флеш картой (CF), на которой:

- инсталлирована 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:

- Руководство администратора, Правила пользования, Формуляр.
- в разделе «MCM – комплект материалов для восстановления» – образ компакт-диска NME-RVPN (MCM) Recovery CD (вспомогательное ПО для восстановления образа компакт-флеш карты, образ компакт-флеш карты (CF), скрипты.

Подготовка модуля к работе

Подготовка модуля MCM к работе осуществляется в несколько этапов:

- Шаг 1:** Установка модуля MCM в маршрутизатор.
- Шаг 2:** Инициализация C-Terra Шлюз 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 в маршрутизатор ознакомьтесь с «Мерами безопасности и правилами эксплуатации», а также методом защиты от статического электричества, описанными в документе [1].



Модуль MCM не поддерживает режим горячей замены, поэтому важно заранее выключить тумблер питания маршрутизатора и вытащить вилку шнура питания из розетки переменного тока.

Модуль MCM может быть установлен в single-wide NME слот на маршрутизаторах Cisco 2911, 2921, 2951, 3925, 3945, 2811, 2821, 2851, 3825, 3845. Более подробную информацию о количестве и расположении NME 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 NME-RVPN (MCM)
- Шаг 2:** соедините кабелем внешний сетевой интерфейс модуля Gigabit Ethernet с корпоративной сетью
- Шаг 3:** включите электропитание маршрутизатора
- Шаг 4:** проверьте, что на маршрутизаторе установлена правильная версия операционной системы Cisco IOS.

Если IOS распознал модуль, то светодиод EN на передней панели модуля загорится, а в конфигурации маршрутизатора появится новый интерфейс:

```
interface Special-Services-Engine1/0
 shutdown
 no keepalive
```

Перед настройкой модуля сделаем этот интерфейс активным и назначим ему адрес:

```
Router(config)# interface Special-Services-Engine 1/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Если выполнить команду:

```
Router# service-module Special-Services-Engine 1/0 session
Trying 192.168.1.1, 2066 ... Open
Press ENTER to continue with initial setup...
```

то пользователь получает доступ к физической консоли модуля, работающей на скорости 9600 baud. На этом этапе можно начинать инсталляцию.



Для выхода из сессии нажмите "Ctrl-Shift-6" затем клавишу "x". В появившемся промте IOS наберите команду "disconnect" и нажмите Enter.

Инициализация программного комплекса S-Terra Gate при первом старте

Установленная в модуль компакт-флеш карта содержит:

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

Для работы установленных продуктов необходимо провести процедуру начальной инициализации при первом старте модуля. Подробно процесс инициализации С-Терра Шлюз 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 медленно мигающий (с периодом 4 сек) светодиод "SYS". А светодиод "CF" загорается, когда происходит чтение или запись на **компакт-флеш карту**.

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 подождав около 10 секунд). Перезапустить модуль можно повторным нажатием этой же кнопки.

Подключение к локальной сети

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

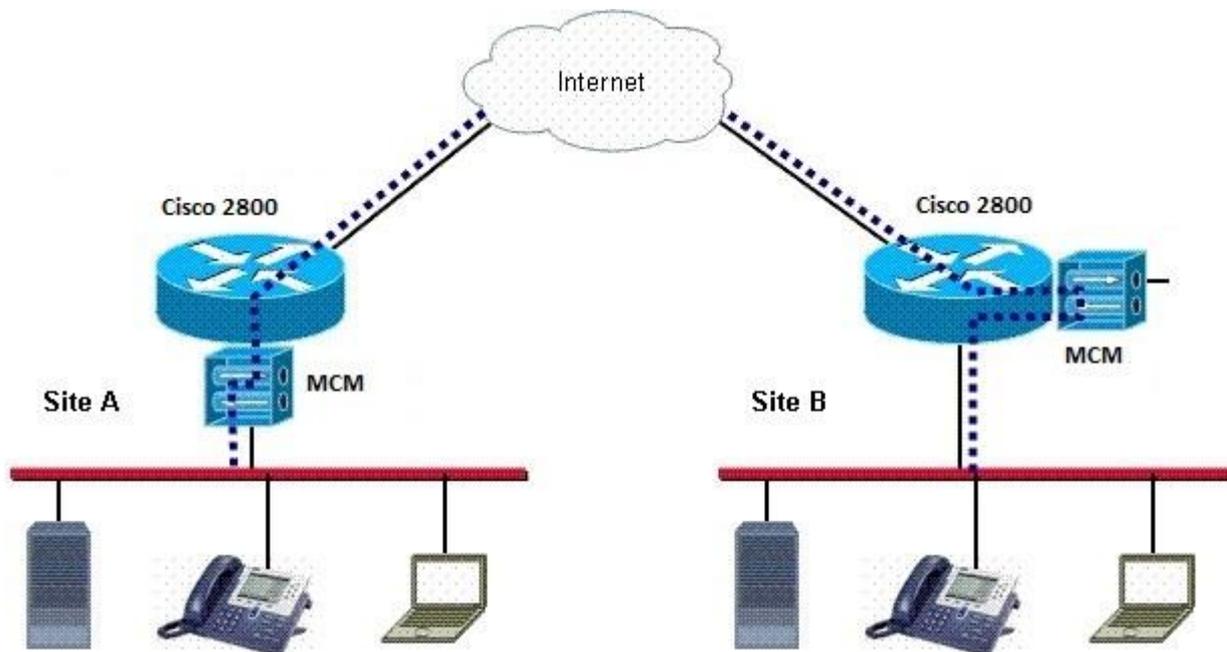


Рисунок 2

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. 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 модуля MCM 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 продукта «С-Терра КП» версии 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, 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.

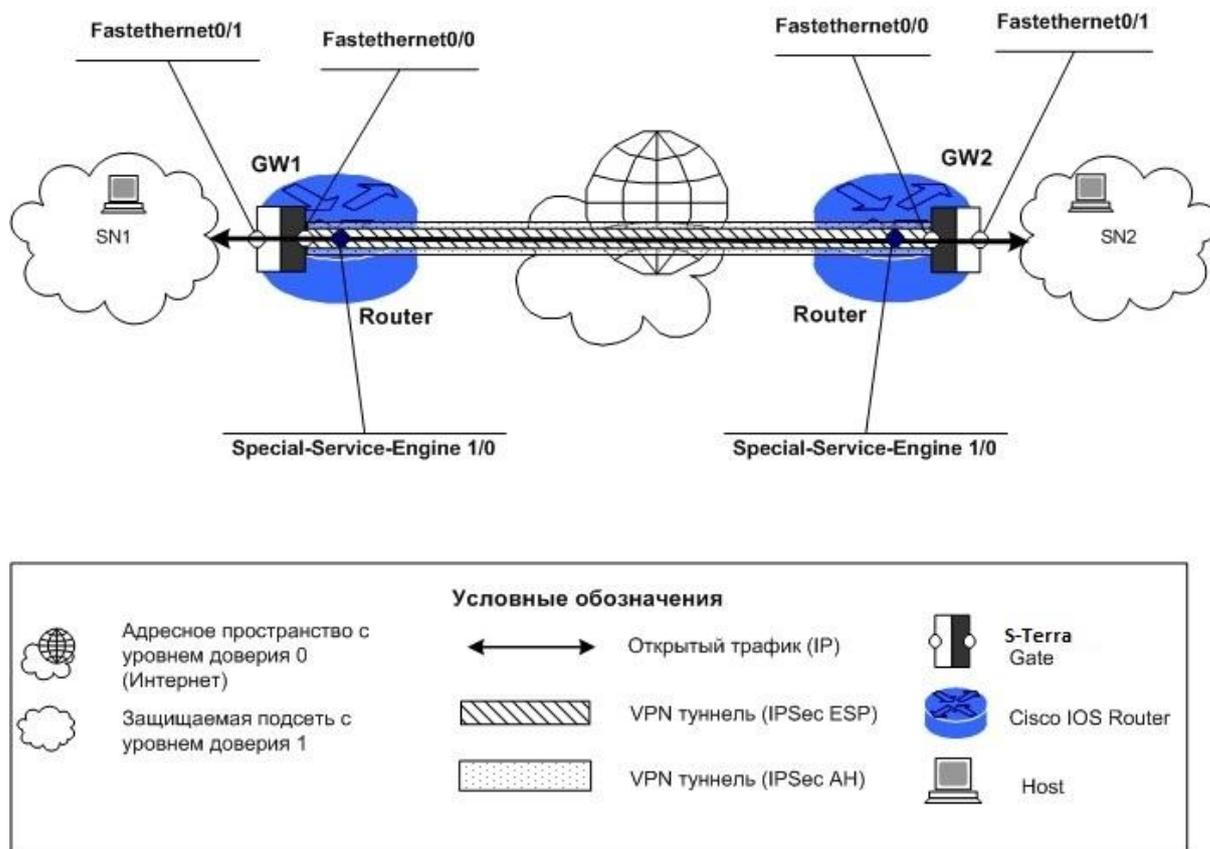


Рисунок 3

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/customer/products/sw/secursw/ps1018/prod_configuration_examples_list.html

http://www.cisco.com/en/US/customer/products/sw/secursw/ps1018/products_installation_and_configuration_guides_list.html

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

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml

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

Для примера настройки С-Терра Шлюз соберем стенд (Рисунок 4). Здесь два модуля MCM GW1 и GW2 обеспечивают передачу данных между локальными сетями SN1 и SN2 по защищенному IPsec VPN туннелю через Интернет.

Настроим политику безопасности, в которой подсети могут общаться только между собой и только по защищенному каналу.

Будем использовать следующие параметры для построения VPN туннеля:

- 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.

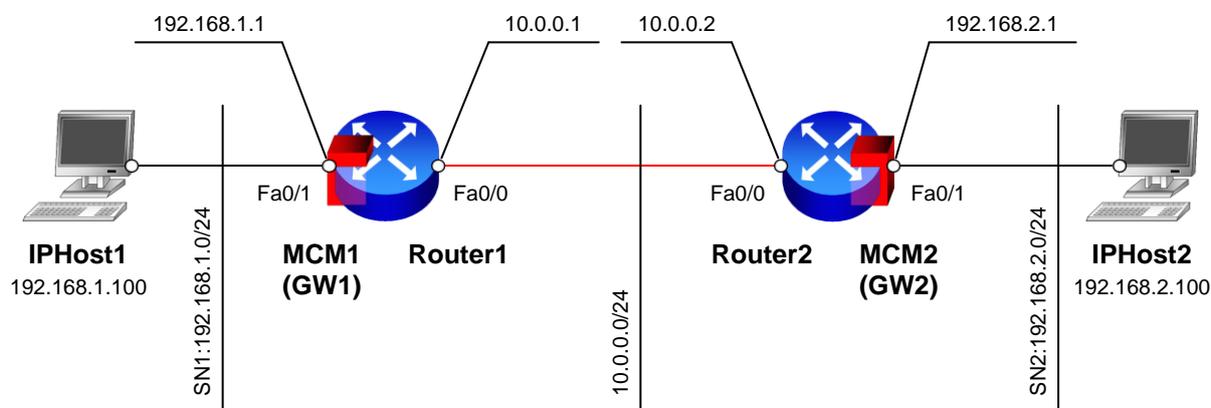


Рисунок 4

Предварительные настройки

Доступ к консоли MCM производится через маршрутизатор Cisco командой:

```
service-module special-Services-Engine 1/0 session
```

При этом интерфейс special-Services-Engine 1/0 в маршрутизаторе Cisco должен быть поднят и иметь IP-адрес. Логическое сетевое подключение маршрутизатора Cisco и MCM показано на рисунке 2.

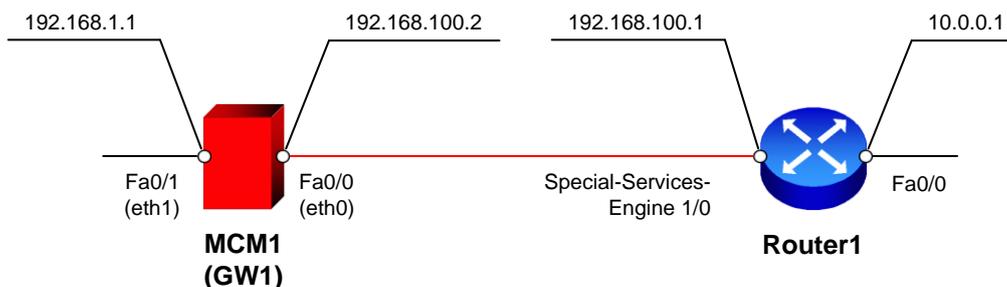


Рисунок 5

Возврат к консоли cisco можно осуществить, послав Brake-сигнал (нажать Ctrl+Shift+6, а после нажать x) и введя команду:

```
service-module special-Services-Engine 1/0 session clear
[confirm]
```

На маршрутизаторе Router1 необходимо настроить IP-адрес интерфейса special-Services-Engine 1/0 для связи с MCM, 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.

Необходимые настройки представлены ниже:

```
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
ip nat outside
!
!
interface special-Services-Engine 1/0
ip address 192.168.100.1 255.255.255.0
ip nat inside
!
ip nat inside source static 192.168.100.2 10.0.0.1
ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

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

Настройка шлюза GW1

Настройку начните со шлюза безопасности GW1. Все настройки производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Инициализация модуля описывается в документе «Руководство по установке и настройке NME-RVPN модуля (MCM)».

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документе «Cisco-like команды», раздел «Команды для работы с сертификатами».

Настройка интерфейсов

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

1. Для входа в консоль запустите cs_console:

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

```
sterragate>en  
Password:
```

Пароль по умолчанию: csp.

2. Перейдите в режим настройки:

```
sterragate#conf t  
Enter configuration commands, one per line. End with CNTL/Z.
```

3. В настройках интерфейсов задайте IP-адреса, согласно рисунку 5:

```
sterragate(config)#interface FastEthernet 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 FastEthernet 0/1  
sterragate(config-if)#ip address 192.168.1.1 255.255.255.0  
sterragate(config-if)#no shutdown  
sterragate(config-if)#exit
```

4. Задайте адрес шлюза по умолчанию:

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

5. Выйдите из cisco-like интерфейса:

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

Регистрация CA сертификата (сертификата УЦ)

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

1. Установите правильное системное время.

Например:

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

Данная запись соответствует 10 апреля 2013 года 13:15.

2. Создайте папку /certs:

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

3. Доставьте файл CA 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.

Описание создания доверенной среды через недоверенные каналы связи смотрите в документации на ПК “С-Терра Шлюз 4.1” (“Настройка шлюза”, раздел “Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза”).

4. С помощью утилиты cert_mgr, входящей в состав продукта S-Terra Gate, 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:

1. Сформируйте запрос на сертификат при помощи утилиты `cert_mgr`:

```
root@sterragate:~# cert_mgr create -subj "C=RU,OU=Research,CN=GW1" -
GOST_R3410EL
Press keys...
[.....]
-----BEGIN CERTIFICATE REQUEST-----
MIIBCjCBuAIBADAuMQswCQYDVQQGEwJSVTERMA8GA1UECxmIUmVzZWYyY2g4
DDAKBgNVBAMTA0dXMTBjMBwGBlqFAwICEzASBgcqhQMCAiMBBgcqhQMCAh4B
A0MABECTQeB5UoPsTbSs8obnrQ6KMJwpc/BFrUgfl6AjQl95ccE4D5jEAq8m
BgNVHQ8EBAMCB4AwCgYGKouDAgIDBQADQQAuAuzk8bASJqbP5pYHAG5A3LKx
OPFjiF1m+2/WkxGkWJWEm5gjNNyWquslmxLq9nX2rff4X3E5xF40iudzHoZz
-----END CERTIFICATE REQUEST-----
```

2. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документации на ПК “С-Терра Шлюз 4.1” (“Приложение”, раздел “Создание локального сертификата с использованием СКЗИ “КриптоПро CSP”).
3. Перенесите полученный файл на шлюз безопасности (параметры `rsrp` описаны выше).
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
```

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
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для GW1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль запустите `cs_console`:

```
root@sterragate:~# cs_console
sterragate>en
Password:
```

Пароль по умолчанию: `csp`.

Важно: пароль по умолчанию необходимо сменить.

1. Перейдите в режим настройки:

```
sterragate#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

2. Смените пароль по умолчанию:

```
sterragate(config)#username cscons password <пароль>
```

3. Смените название шлюза:

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

4. Задайте тип идентификации:

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

5. 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
```

6. 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
```

7. 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
```

8. 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
```

9. Привяжите крипто-карту к интерфейсу, на котором будет туннель:

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

10. 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
```

11. Настройка устройства GW1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

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

Настройка устройства GW1 завершена. При выходе из конфигурационного режима произойдет загрузка конфигурации. Устройство готово к работе.

Если в конфигурационном режиме запустить команду `do 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 10.0.0.2
!
interface FastEthernet0/0
  ip address 192.168.100.2 255.255.255.0
  crypto map CMAP
!
interface FastEthernet0/1
  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 GW2

Настройка шлюза безопасности GW2 производится аналогично настройке шлюза 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 10.0.0.1
!
interface FastEthernet0/0
  ip address 192.168.101.2 255.255.255.0
  crypto map CMAP
!
interface FastEthernet0/1
  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 того, как настройка всех устройств завершена, иницируйте создание защищенного соединения.

На устройстве IPHost1 выполните команду ping:

```
ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_req=1 ttl=62 time=1359 ms
64 bytes from 192.168.2.100: icmp_req=2 ttl=62 time=356 ms
64 bytes from 192.168.2.100: icmp_req=3 ttl=62 time=4.37 ms
64 bytes from 192.168.2.100: icmp_req=4 ttl=62 time=5.52 ms
64 bytes from 192.168.2.100: icmp_req=5 ttl=62 time=7.11 ms
^C
--- 192.168.2.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 4.372/346.586/1359.566/524.385 ms, pipe 2
```

В результате выполнения этой команды между устройствами MCM1 и MCM2 будет установлен VPN туннель.

Убедиться в этом можно, выполнив на устройстве MCM2 команду:

```
root@GW1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 3 (192.168.100.2,4500)-(10.0.0.2,4500) active 1976 1904

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent
Rcvd
1 2 (192.168.1.0-192.168.1.255,*)-(192.168.2.0-192.168.2.255,*) * ESP nat-t-
tunn 440 440
```

Согласно созданной политике безопасности весь трафик между сетями SN1 и SN2 будет зашифрован. Прохождение остального трафика будет разрешено, но не будет защищаться шифрованием.

Настройка модуля для работы с удаленными клиентами

Следующий сценарий иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности в исполнении модуля MCM, и мобильным клиентом С-Терра Клиент (Рисунок 6). Для защиты будет построен VPN туннель между устройствами MCM-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 MCM в свой внешний secondary-адрес.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6 (R4). На MCM установлен «Программный комплекс С-Терра Шлюз. Версия 4.1», на мобильном клиенте установлен «Программный комплекс С-Терра Клиент. Версия 4.1».

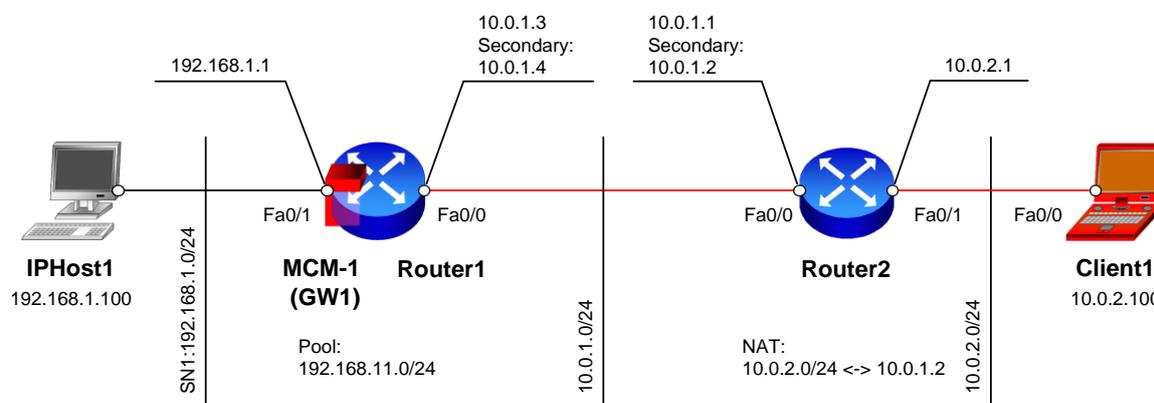


Рисунок 6

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 MCM-1 производится через маршрутизатор Router1 командой:

```
service-module special-Services-Engine 1/0 session
```

При этом интерфейс special-Services-Engine 1/0 на маршрутизаторе Router1 должен быть поднят и иметь IP-адрес. Логическое сетевое подключение маршрутизатора и модуля представлено на Рисунок 7 **Ошибка! Источник ссылки не найден..**

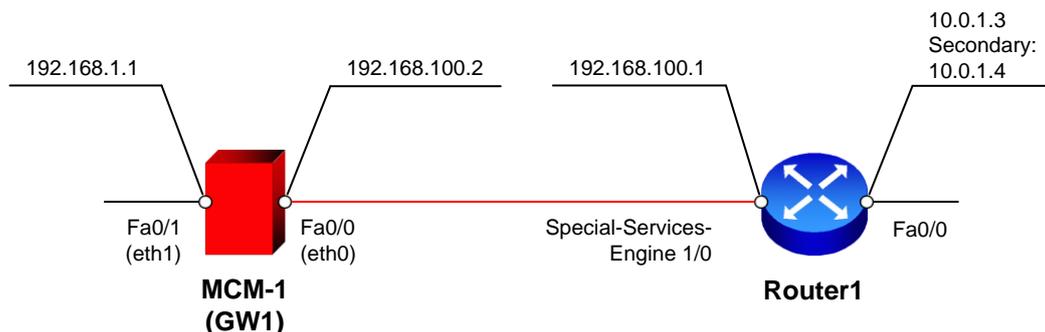


Рисунок 7

Возврат к консоли cisco можно осуществить, послав Brake-сигнал (нажать Ctrl+Shift+6, а после нажать x) и введя команду:

```
service-module special-Services-Engine 1/0 session clear
[confirm]
```

На маршрутизаторе Router1 необходимо настроить IP-адрес интерфейса special-Services-Engine 1/0 для связи с MCM, 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.

Необходимые настройки представлены ниже:

```
interface FastEthernet0/0
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 special-Services-Engine 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 MCM-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 MCM-1 (GW1)

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

1. Для входа в консоль запустите cs_console:

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

2. Перейдите в режим настройки:

```
sterragate#conf t
```

3. В настройках интерфейсов задайте IP-адреса:

```
sterragate(config)#interface FastEthernet 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 FastEthernet 0/1
sterragate(config-if)#ip address 192.168.1.1 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
```

4. Задайте адрес шлюза по умолчанию:

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

5. Выйдите из cisco-like интерфейса:

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

6. Далее сменим название шлюза:

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

7. Задайте тип идентификации:

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

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
```

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
```

10. Задайте пул, из которого будет выдан адрес клиенту:

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

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
```

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
```

13.Привяжите динамическую карту к статической:

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

14.Привяжите крипто-карту к интерфейсу, на котором будет туннель:

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

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
```

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 FastEthernet0/0  
  ip address 192.168.100.2 255.255.255.0  
  crypto map CMAP  
!  
interface FastEthernet0/1  
  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. Изменить настройки клиента после инсталляции нельзя. 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 сделаем эти шаги.

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

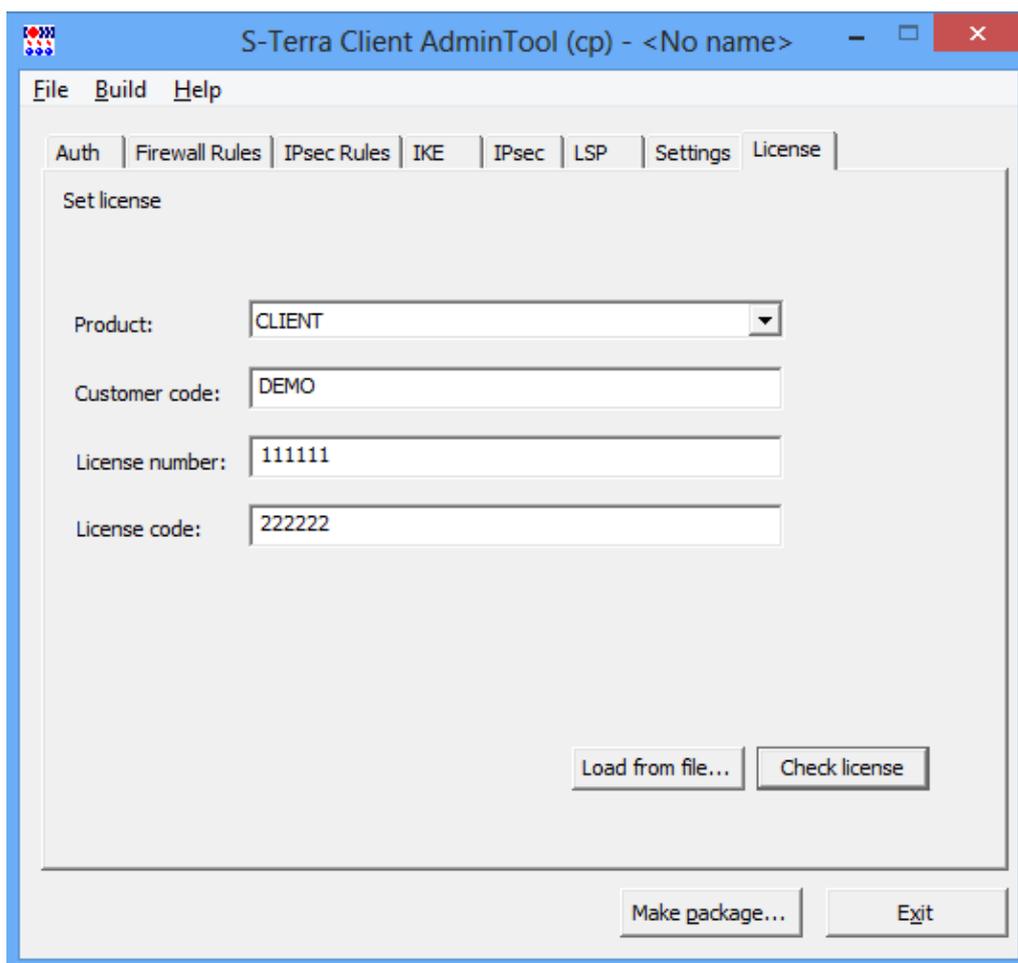


Рисунок 8

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

- в данном сценарии используется метод аутентификации на сертификатах – пункт “Use certificate” выбран по умолчанию;
- укажите путь к сертификату УЦ и пользовательскому сертификату;
- отметьте пункт “Check consistency now” и нажмите кнопку “...”, где выберите нужный контейнер; если при генерации сертификатов указывался пароль на контейнер, введите его в графе “password”;
- отметьте пункт “Copy container” и скопируйте имя контейнера из графы “Container name” в графу “Source container name”; если при генерации сертификатов указывался пароль на контейнер, введите его в графе “password”;
- задайте имя контейнера в графе “User container name”; в данном случае указано - \\.\REGISTRY\Client1. Данная запись означает, что контейнер с переносного устройства (токен или USB Flash) будет скопирован в реестр с именем Client1.
- в графе “User identity type” выберите “DistinguishedName” (выбрано по умолчанию).

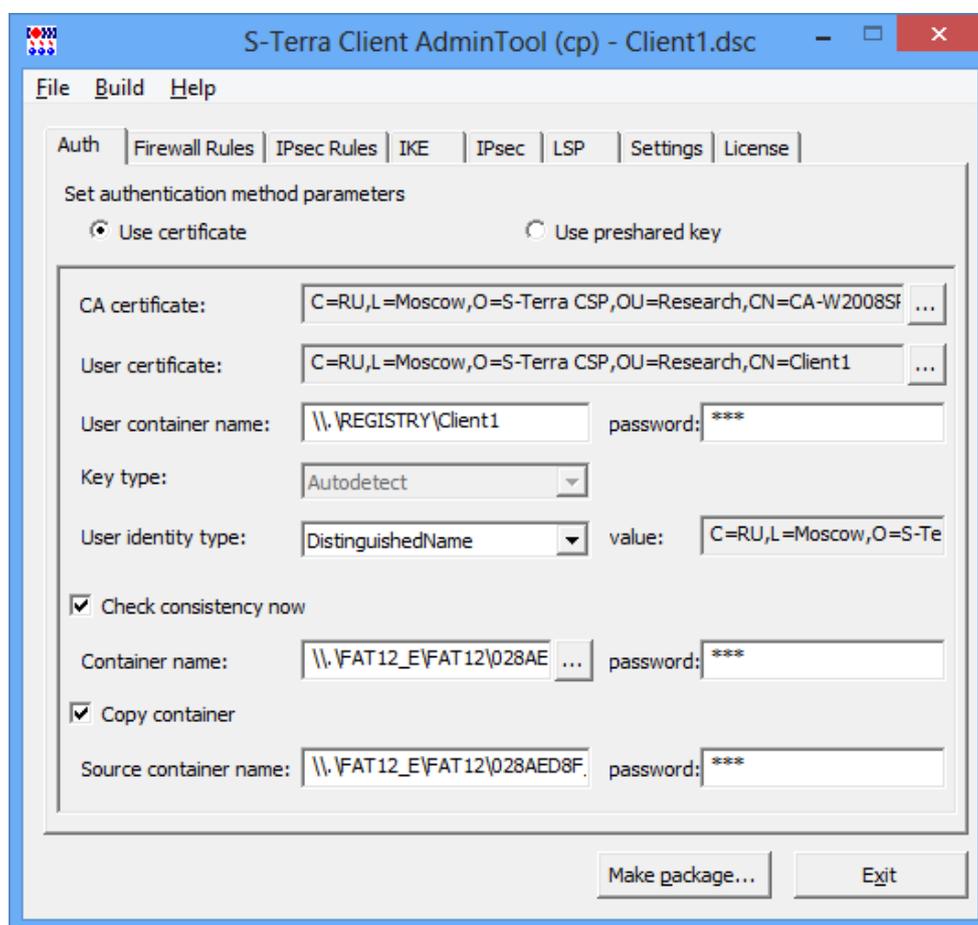


Рисунок 9

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

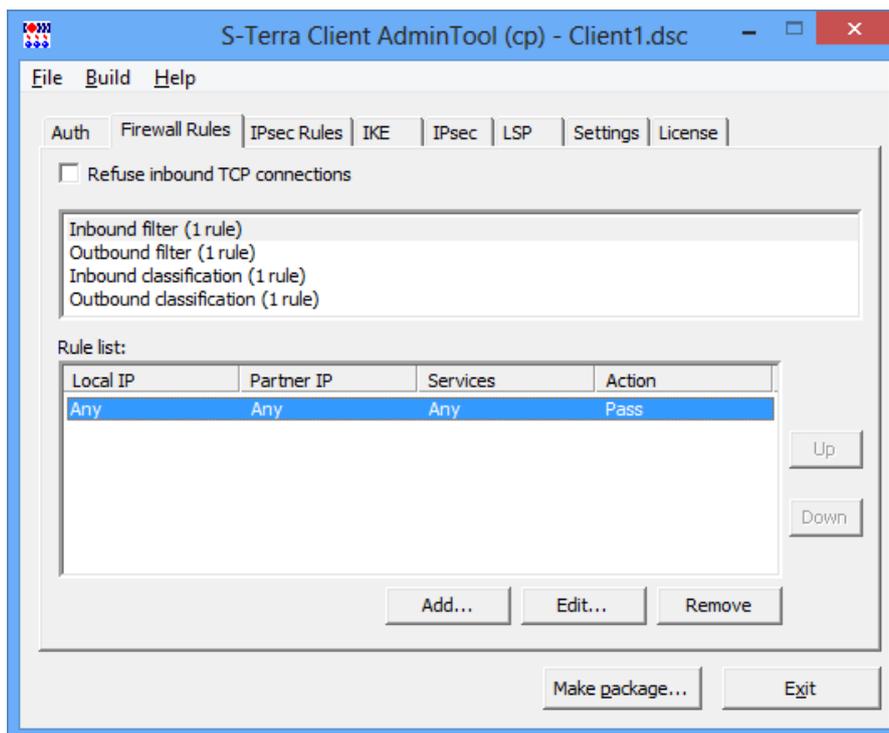


Рисунок 10

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 отметьте пункт “Request IKECFG address”. Добавленное правило поднимите вверх.

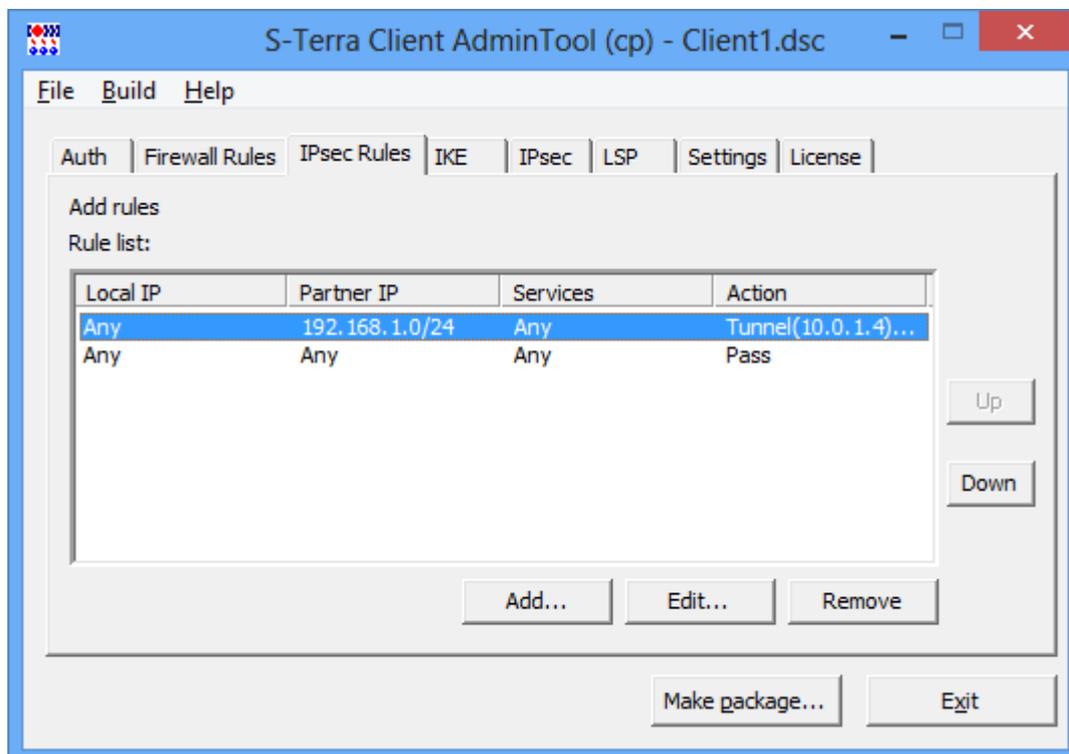


Рисунок 11

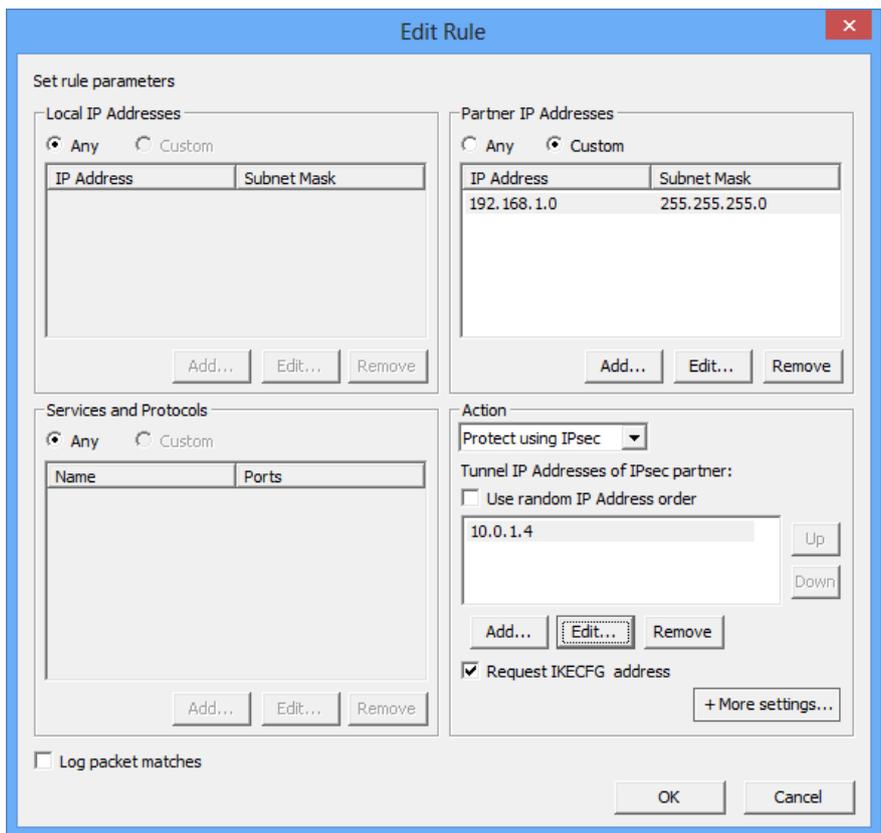


Рисунок 12

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

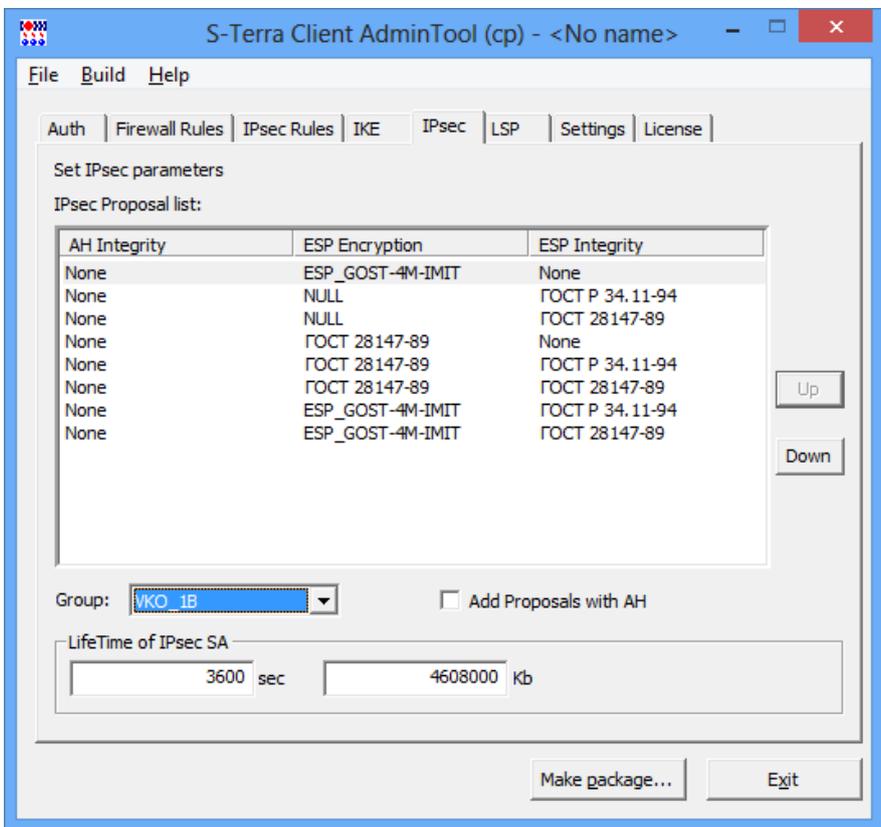


Рисунок 13

Во вкладке LSP загружаем [конфигурацию](#) для устройства Client1.

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.

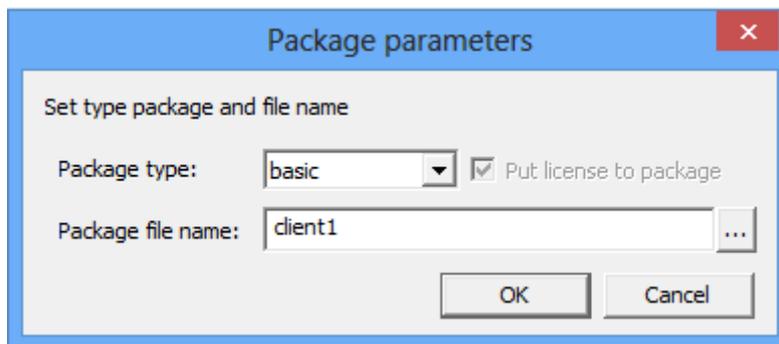


Рисунок 14

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

На панели задач появится иконка S-Terra Client (Рисунок 15). Для начала работы указатель на иконку, нажмите правую кнопку мыши и выполните вход в продукт (Login) (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 = "6118B135000000000002"
  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/>.