

ЗАО «С-Терра СиЭсПи»
124460, г. Москва, Зеленоград, проезд 4806, д.6, этаж 4-й
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: <http://www.s-terra.com>



Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1»

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

РЛКЕ.00005-01 90 03

12.05.2012

Содержание

Инструкция по подготовке к работе NME-RVPN модуля (MCM)	3
Комплект поставки	4
Подготовка модуля к работе	5
Установка модуля в маршрутизатор.....	6
Инициализация программного комплекса CSP VPN Gate	7
Подключение к локальной сети.....	8
Архитектура ПО CSP VPN	9
Пример топологии	11
Настройка политики безопасности шлюзов	12
Настройка модуля для работы с удаленными клиентами	17
Подготовка клиентского ПО	23
Установка клиентского ПО	28
Проверка клиентского соединения	28
Дополнительная информация.....	29

Инструкция по подготовке к работе NME-RVPN модуля (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)» 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 – версии 12.4(11)T и выше.

На модуль устанавливается продукт CSP VPN Gate 3.1, функционирующий под управлением ОС на базе свободно опубликованных исходных текстов Red Hat Enterprise Linux 5 (CentOS 5).

Модуль поддерживает IPsec VPN туннели с использованием российских алгоритмов шифрования по ГОСТ 28147-89 и проверки целостности данных по ГОСТ Р 34.11-94. Производительность на модуле достигает 95 Мбит/с при шифровании трафика с использованием алгоритма ГОСТ 28147-89.

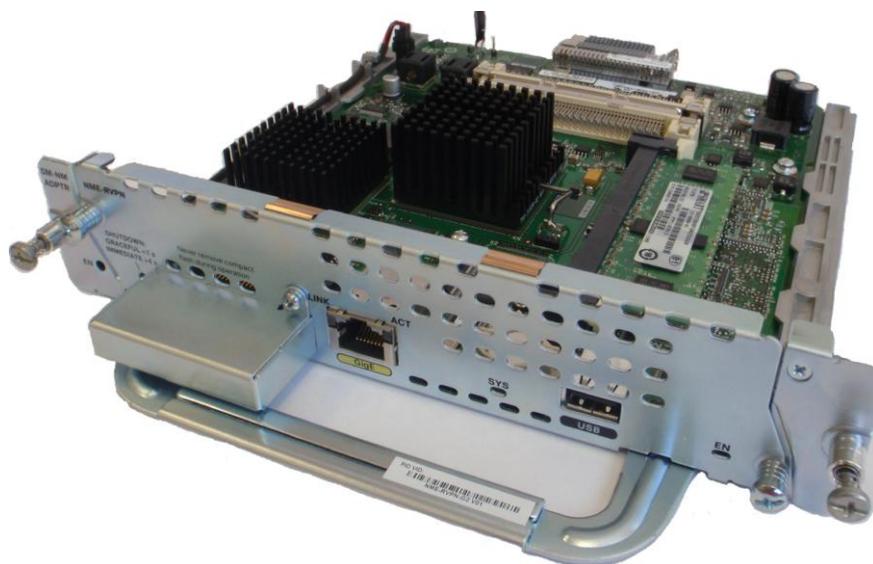


Рисунок 1

В этом документе описано как подготовить модуль NME-RVPN (MCM) к работе – установить модуль в маршрутизатор, инициализировать на нем программный комплекс CSP VPN Gate и создать локальную политику безопасности. Здесь даны только минимальные сведения, более детальную информацию по настройке модуля и его работе можно найти в документах:

1. [“Программный комплекс “Шлюз безопасности CSP VPN Gate. Версия 3.1. Руководство по установке и настройке NME-RVPN модуля \(MCM\)” \[1\].](#)
2. [”Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.1. Настройка шлюза” \[2\].](#)

Комплект поставки

В комплект поставки программного комплекса CSP VPN Gate входят:

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

- установлена ОС Red Hat Enterprise Linux 5 или ОС CentOS 5
- подготовлены к инициализации продукты CSP VPN Gate 3.1 и СКЗИ "КриптоПро CSP 3.6"

следующие документы в печатном виде:

- Копия сертификата соответствия ФСБ России
- Копия сертификата соответствия ФСТЭК России
- Голографический специальный защитный знак ФСТЭК России
- Лицензия на использование программного продукта компании ЗАО «С-Терра СиЭсПи»
- Лицензия на использование программного продукта КриптоПро CSP Driver версии 3.6
- Информационный купон к лицензии на использование программного продукта компании ЗАО «С-Терра СиЭсПи».

На сайте компании по адресу <http://www.s-terra.com/support/documents/ver31/> можно взять следующие материалы:

- в разделе «**CSP VPN Gate (CP и SC)**» - Пользовательскую документацию, Правила пользования (если используется СКЗИ "КриптоПро CSP 3.6"), Формуляр
- в разделе «**NME-RVPN (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) (для **МАРШ CF** этот диск не нужен).

Подготовка модуля к работе

Подготовка модуля NME-RVPN (MCM) к работе осуществляется в несколько этапов:

- Шаг 1:** Установка модуля NME-RVPN (MCM) в маршрутизатор
- Шаг 2:** Инициализация CSP VPN 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 NME-RVPN (MCM) в маршрутизатор ознакомьтесь с «Мерами безопасности и правилами эксплуатации», а также методом защиты от статического электричества, описанными в документе [1].



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

Сетевой модуль NME-RVPN (MCM) может быть установлен в single-wide слот на маршрутизаторах Cisco 2911, 2921, 2951, 3925, 3945, 2811, 2821, 2851, 3825, 3845. Более подробную информацию о количестве и расположении 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 CSP VPN Gate

Установленная в модуль компакт-флеш карта содержит:

- установленные продукты CSP VPN Gate 3.1 и СКЗИ “КриптоПро CSP 3.6”.

Для работы установленных продуктов необходимо провести процедуру начальной инициализации при первом старте модуля. Подробно процесс инициализации CSP VPN 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 CryptoPro CSP (СКЗИ “КриптоПро CSP 3.6”)
- ввести несколько символов с клавиатуры для инициализации начального значения ДСЧ
- ввести лицензионную информацию для CSP VPN Gate.

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.



После инициализации Продукта советуем изменить пароль пользователей “root” и “cscons”. Эта процедура описана в разделе “Изменение паролей” документа [2].



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 NME-RVPN модулем (MCM) в локальную сеть приведены на Рисунке 2.

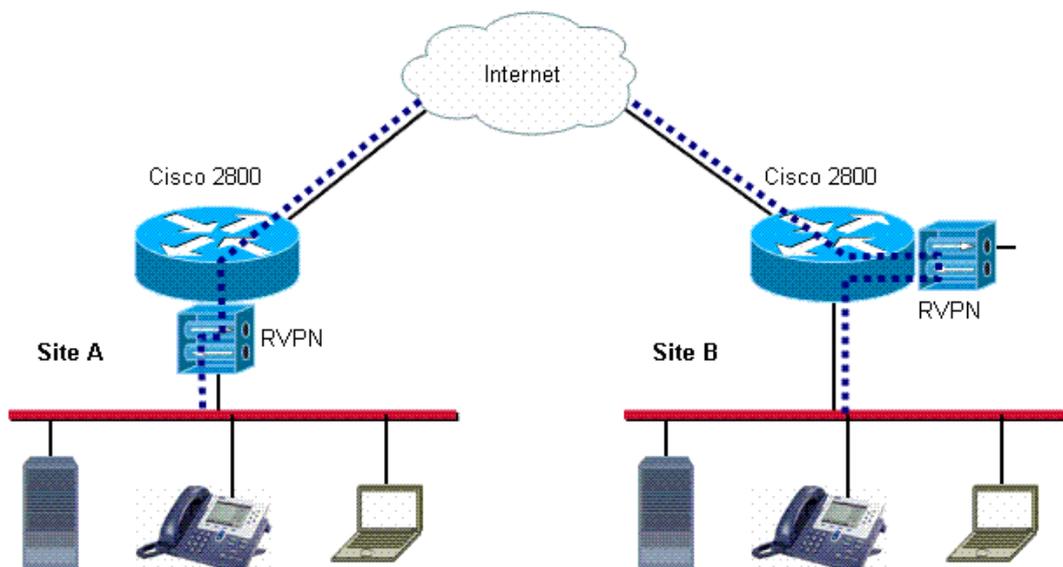


Рисунок 2

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 RVPN (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 CSP VPN

Функциональность NME-RVPN (MCM) обеспечивает программный продукт CSP VPN Gate, который состоит из следующих основных частей:

- VPN daemon (демон)
- VPN driver (драйвер)
- Cisco-like console (CLI консоль)
- Command Line Utilities (утилиты)
- Web-based Graphic User Interface (GUI).

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 в драйвер демоном 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 configuration” и загружается в vpnsvc.

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

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.

GUI является еще одним средством настройки шлюза безопасности. В состав ОС входит Web-сервер и SSH-сервер, а GUI представляет из себя Java-applet, который может быть загружен по протоколу HTTP администратором и запущен на его рабочем компьютере. После запуска GUI взаимодействует с консолью по протоколу SSH. Внешне GUI выполнен в стиле Cisco SDM с существенным сокращением функциональности. Он позволяет пользователю редактировать Cisco-like policy, представленную в виде набора связанных таблиц. После внесения

необходимых изменений они по специальной команде пользователя в виде набора команд конфигурационного режима передаются консоли.

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.

Перед созданием конфигурации с помощью графического Web-based интерфейса нужно зарегистрировать локальный сертификат в базе Продукта, используя утилиту. При запуске GUI вызывается Java-апплет, который использует консоль. В ней создается конфигурация, при доставке на шлюз безопасности она конвертируется и загружается, а также хранится в базе Продукта.

Пример топологии

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

Как видно на Рисунке 3, модуль NME RVPN (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.

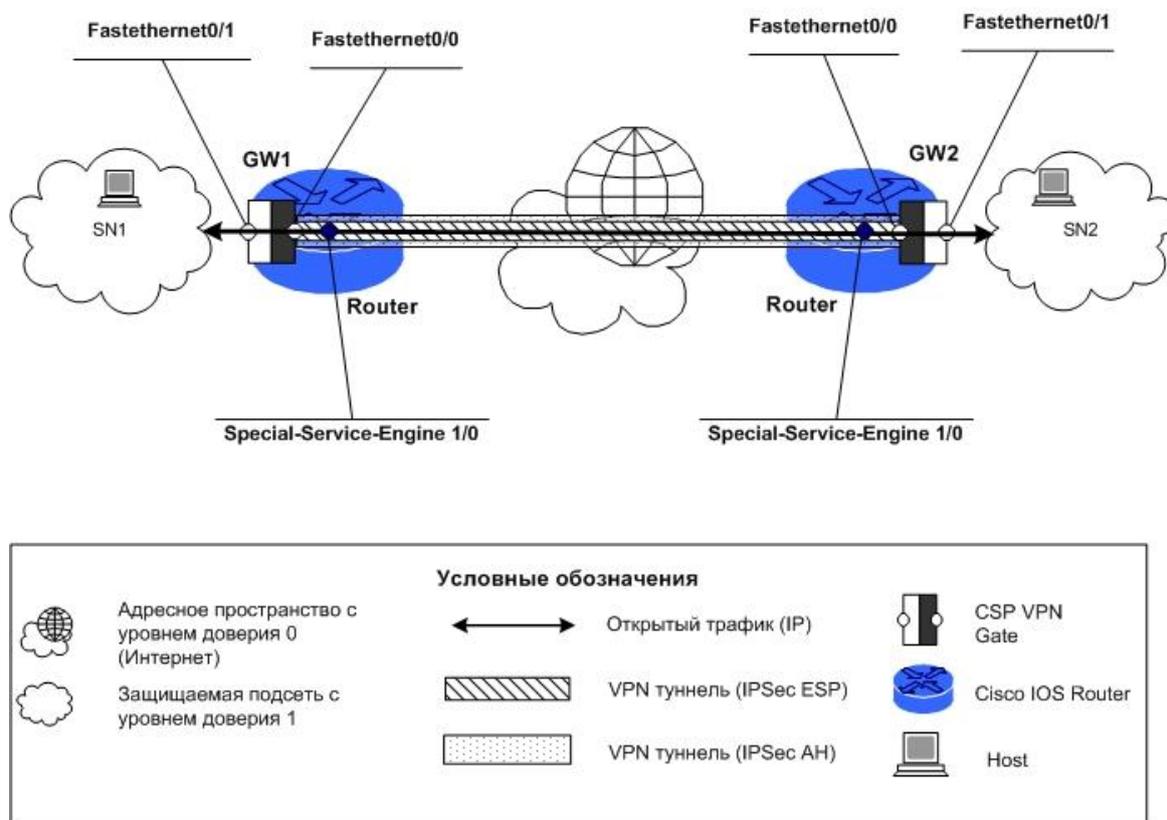


Рисунок 3

Настройка маршрутизаторов сложностей 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 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 шлюзов безопасности соберем стенд, представленный на Рисунок 4. Здесь два модуля NME-RVPN (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:

- Аутентификация на Preshared Key
- IKE parameters:
 - Encryption algorithm – GOST
 - Hash algorithm – GOST
 - DH-group – group2 (1024)
- IPsec parameters:
 - ESP encryption algorithm – GOST
 - AH integrity algorithm – GOST.

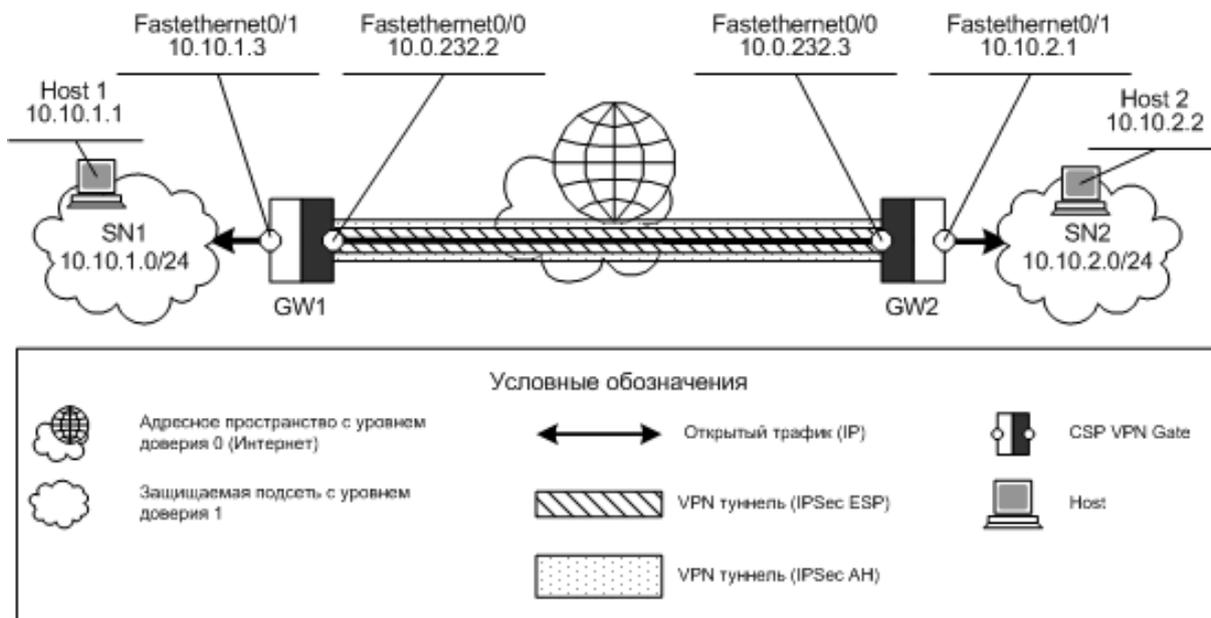


Рисунок 4

Предварительные настройки

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

1. на устройствах Host1 и Host2 зададим адреса маршрутизаторов по умолчанию (default gateway):

на Host1 в качестве шлюза по умолчанию назначим адрес 10.10.1.3

на Host2 назначим адрес 10.10.2.1

2. на шлюзе GW1 укажем маршруты в подсети, которые защищаются шлюзами-партнерами. Для этого в глобальном конфигурационном режиме cs_console зададим команды:

```
ip route 10.10.2.0 255.255.255.0 10.0.232.3 1
```

3. на шлюзе GW2 выполним аналогичные действия:

```
ip route 10.10.1.0 255.255.255.0 10.0.232.2 1
```

4. После выполнения настроек убедимся, что пакеты маршрутизируются верно. Для этого:

на устройстве Host1 зададим команду: ping 10.10.2.2 и убедимся, что на echo request приходят echo reply с этого адреса:

```
ping 10.10.2.2
```

```
Pinging 10.10.2.2 with 32 bytes of data:
```

```
Reply from 10.10.2.2: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.10.2.2:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

на устройстве Host1 зададим команду tracer 10.10.2.2 (или ей аналогичную) и убедимся, что вывод совпадает с приведенным ниже в примере:

```
tracert 10.10.2.2
```

```
Tracing route to 10.10.2.2 over a maximum of 30 hops
```

```
  0  <1 ms    <1 ms    <1 ms    10.10.1.3
  1  <1 ms    <1 ms    <1 ms    10.0.232.3
  2  <1 ms    <1 ms    <1 ms    10.10.2.2
```

```
Trace complete.
```

Настройка шлюза GW1

Настройку шлюза безопасности GW1 будем выполнять в интерфейсе командной строки. Для входа в консоль перейдем в директорию `/opt/VPNagent/bin/` и запустим `cs_console`. В глобальном конфигурационном режиме выполним следующее:

1. зададим параметры для IKE:

```
gw1(config)#crypto isakmp policy 1
gw1(config-isakmp)#hash md5
gw1(config-isakmp)#encryption des
gw1(config-isakmp)#authentication pre-share
gw1(config-isakmp)#group 2
gw1(config-isakmp)#exit
```

2. создадим предопределенный ключ для соединения со шлюзом GW2:

```
gw1(config)#crypto isakmp key 12345 address 10.0.232.3
```

3. создадим набор преобразований для IPsec:

```
gw1(config)#crypto ipsec transform-set gost ah-md5-hmac esp-des
gw1(cfg-crypto-trans)#mode tunnel
gw1(cfg-crypto-trans)#exit
```

4. опишем трафик, который планируется защищать:

```
gw1(config)#ip access-list extended SN1toSN2
gw1(config-ext-nacl)#permit ip 10.10.1.0 0.0.0.255 10.10.2.0
0.0.0.255
gw1(config-ext-nacl)#exit
```

5. создадим криптокарту:

```
gw1(config)#crypto map CMAP 1 ipsec-isakmp
gw1(config-crypto-map)#match address SN1toSN2
gw1(config-crypto-map)#set transform-set gost
gw1(config-crypto-map)#set peer 10.0.232.3
```

6. привяжем криптокарту к интерфейсу, на котором будет терминироваться туннель:

```
gw1(config)#interface FastEthernet0/0
gw1(config-if)# crypto map CMAP
gw1(config-if)#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

```
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons password csp
hostname cspgate
enable password csp

logging trap debugging

crypto isakmp policy 1
  hash md5
  encryption des
  authentication pre-share
  group 2

crypto isakmp key 12345 address 10.0.232.3

crypto ipsec transform-set gost ah-md5-hmac esp-des
mode tunnel

ip access-list extended SN1toSN2
permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255

crypto map CMAP 1 ipsec-isakmp
match address SN1toSN2
set transform-set gost
set peer 10.0.232.3

interface FastEthernet0/0
ip address 10.0.232.2 255.255.0.0
crypto map CMAP

ip route 10.10.2.0 255.255.255.0 10.0.232.3 1
```

Настройка шлюза GW2

Аналогично пишется политика безопасности для шлюза GW2.

Текст cisco-like конфигурации GW2

```
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons password csp
hostname cspgate
enable password csp

logging trap debugging

crypto isakmp policy 1
  hash md5
  encryption des
  authentication pre-share
  group 2

crypto isakmp key 12345 address 10.0.232.2

crypto ipsec transform-set gost ah-md5-hmac esp-des
mode tunnel

ip access-list extended SN2toSN1
  permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255

crypto map CMAP 1 ipsec-isakmp
  match address SN2toSN1
  set transform-set gost
  set peer 10.0.232.2

interface FastEthernet0/0
  ip address 10.0.232.3 255.255.0.0
  crypto map CMAP

ip route 10.10.1.0 255.255.255.0 10.0.232.2 1
```

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 "run sa_mgr show". Ping также должен работать без потери пакетов.

Настройка модуля для работы с удаленными клиентами

Давайте несколько усложним нашу схему: настроим туннель через Internet и дадим возможность удаленным VPN клиентам подключаться к модулю RVPN1 для доступа в локальную сеть главного офиса SN1 и сеть филиала SN2.

Топология сети и адресация предлагается следующая:

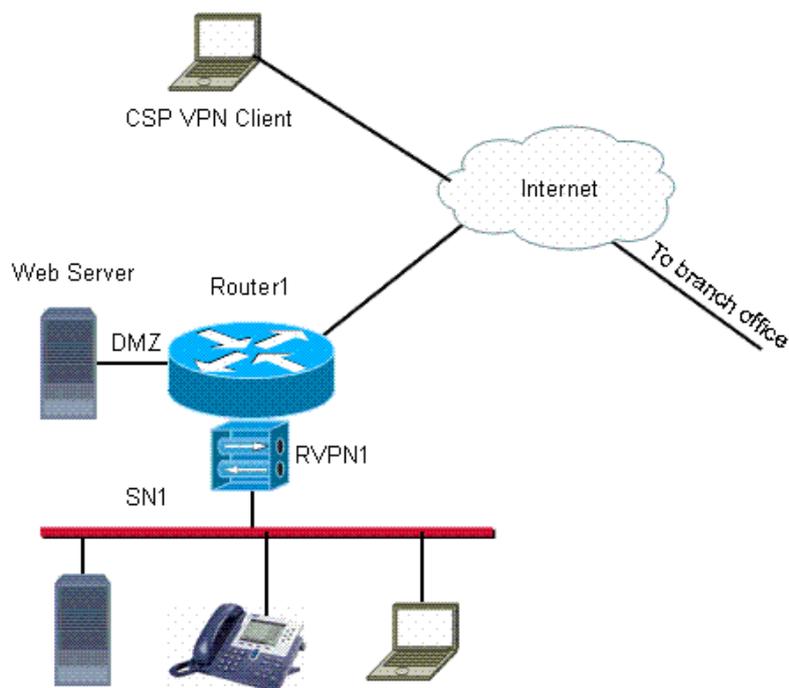


Рисунок 5

Router1:

```
interface Serial 0/0/0 (линк в Internet) - 123.45.67.1
interface FastEthernet0/0 (сеть DMZ) - 10.3.3.1
interface Special-Services-Engine 1/0 (интерфейс к модулю) - 10.0.232.1
```

RVPN1:

```
interface fastethenet0/0 (внутренний интерфейс модуля) - 10.0.232.2
interface fastethenet0/1 (к локальной сети) - 10.10.1.3
```

Первая проблема при создании VPN туннеля через Internet – это необходимость на VPN шлюзе использовать IP-адрес, доступный из Internet. Так как часто количество реальных IP-адресов бывает ограничено, например, одним адресом, настроенным на интерфейсе к провайдеру, то давайте применим трансляцию адресов в IOS для разрешения этой проблемы. Примерная конфигурация Router1 будет такая:

```
hostname Router1
!
interface Serial0/0/0
 ip address 123.45.67.1 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface FastEthernet0/0
 ip address 10.3.3.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Special-Services-Engine1/0
 ip address 10.0.232.1 255.255.255.252
 ip nat inside
 no keepalive
!
! /// PAT для обычного доступа в интернет:
ip nat inside source list 101 Serial0/0/0 overload
!
! /// Port static для Web сервера с адресом 10.3.3.3
ip nat inside source static tcp 10.3.3.3 80 interface Serial0/0/0 80
!
! /// Port static к RVPN модулю для IPsec в режиме NAT Transparency
ip nat inside source static udp 10.0.232.2 500 interface Serial0/0/0 500
ip nat inside source static udp 10.0.232.2 4500 interface Serial0/0/0 4500
!
ip route 0.0.0.0 0.0.0.0 123.45.67.2
ip route 10.10.1.0 255.255.255.0 10.0.232.2
!
access-list 101 permit ip 10.10.1.0 0.0.0.255 any
```

Как видно из конфигурации, единственный реальный IP-адрес используется здесь в режиме трансляции по портам: для терминации IPsec, доступа к Web серверу и для выхода в Internet из локальной сети.

Далее, усовершенствуем конфигурацию крипто модуля для возможности работы с удаленными клиентами с помощью интерфейса командной строки. Для этого установите SSH соединение с модулем (как пользователь "cscons") и перейдите в конфигурационный режим. Затем скопируйте (copy/paste) следующие команды:

```
! /// изменить адрес удаленного филиала - тоже публичный адрес:
no crypto isakmp key 1234567890 address 10.0.232.3
```

```
crypto isakmp key 1234567890 address 212.34.56.1
!
! /// перейти на использование hostname для идентификации шлюзов
crypto isakmp identity hostname
ip host rvpn2 212.34.56.1
!
! /// pre-shared key для клиентов
crypto isakmp key 0987654321 address 0.0.0.0 0.0.0.0
!
! /// пул адресов для клиентов
ip local pool p1 10.30.30.1 10.30.30.200
crypto isakmp client configuration address-pool local p1
!
ip access-list extended 110
! /// направлять трафик, пришедший от клиента, но направленный
! /// к сети SN2 в Lan-to-Lan
 permit ip 10.30.30.0 0.0.0.255 10.10.2.0 0.0.0.255
exit
!
! /// создавать туннели между клиентом и сетями SN1 и SN2
ip access-list extended clients
 permit ip 10.10.1.0 0.0.0.255 10.30.30.0 0.0.0.255
 permit ip 10.10.2.0 0.0.0.255 10.30.30.0 0.0.0.255
exit
!
! /// через NAT работает полько ESP:
crypto ipsec transform-set ts esp-des esp-md5-hmac
 mode tunnel
exit
!
! /// это шаблон для клиентов
crypto dynamic-map dyn 10
 match address clients
 set transform-set ts
!
! /// две записи в crypto map: для Lan-to-Lan и для клиентов
crypto map cm 10 ipsec-isakmp
 match address 110
 set transform-set ts
 set peer 212.34.56.1
crypto map cm 20 ipsec-isakmp dynamic dyn
crypto map cm client configuration address respond
!
interface FastEthernet0/0
```

```
crypto map cm
exit
!
no crypto map site_to_site 1
no crypto ipsec transform-set TS1
no ip route 0.0.0.0 0.0.0.0 10.0.232.3
ip route 0.0.0.0 0.0.0.0 10.0.232.1
!
end
```

В результате должна получиться готовая конфигурация RVPN1 модуля в виде:

```
crypto ipsec df-bit clear
crypto isakmp identity hostname
username cscons password csp
hostname s1
enable password csp
!
ip host rvpn2 212.34.56.1
!
crypto isakmp policy 1
  hash md5
  encryption des
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp client configuration address-pool local p1
!
crypto isakmp key 1234567890 address 212.34.56.1
crypto isakmp key 0987654321 address 0.0.0.0 0.0.0.0
!
ip local pool p1 10.30.30.1 10.30.30.200
!
crypto ipsec transform-set ts esp-des esp-md5-hmac
  mode tunnel
!
ip access-list extended 110
  permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
  permit ip 10.30.30.0 0.0.0.255 10.10.2.0 0.0.0.255
!
ip access-list extended clients
  permit ip 10.10.1.0 0.0.0.255 10.30.30.0 0.0.0.255
  permit ip 10.10.2.0 0.0.0.255 10.30.30.0 0.0.0.255
exit
!
```

```
crypto dynamic-map dyn 10
  match address clients
  set transform-set ts
!
crypto map cm client configuration address respond
crypto map cm 10 ipsec-isakmp
  match address 110
  set transform-set ts
  set peer 212.34.56.1
crypto map cm 20 ipsec-isakmp dynamic dyn
!
interface FastEthernet0/0
  ip address 10.0.232.2 255.255.0.0
  crypto map cm
interface FastEthernet0/1
  ip address 10.10.1.3 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.0.232.1 1
end
```



Здесь предполагается, что на маршрутизаторе филиала также настроен NAT для трансляции адреса RVPN2 в адрес 212.34.56.1.

Конфигурация сети филиала (SN2) производится аналогично, она даже будет несколько проще из-за отсутствия необходимости терминировать удаленных клиентов:

```
crypto ipsec df-bit clear
crypto isakmp identity hostname
username cscons password csp
hostname s2
enable password csp
!
ip host rvpn1 123.45.67.1
!
crypto isakmp policy 1
  hash md5
  encryption des
  authentication pre-share
  group 2
  lifetime 3600
!
crypto isakmp key 1234567890 address 123.45.67.1
```

```
!  
crypto ipsec transform-set ts esp-des esp-md5-hmac  
  mode tunnel  
!  
ip access-list extended 110  
  permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255  
  permit ip 10.10.2.0 0.0.0.255 10.30.30.0 0.0.0.255  
!  
crypto map cm 10 ipsec-isakmp  
  match address 110  
  set transform-set ts  
  set peer 123.45.67.1  
!  
interface FastEthernet0/0  
  ip address 10.0.232.3 255.255.0.0  
  crypto map cm  
interface FastEthernet0/1  
  ip address 10.10.2.1 255.255.255.0  
!  
ip route 0.0.0.0 0.0.0.0 10.0.232.1 1  
end
```

На этом конфигурация модулей завершена и можно проверить работоспособность LAN-to-LAN туннеля.

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 CSP VPN 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 “CSP VPN Client AdminTool”. Во вкладке “License” введем лицензионный номер, как показано на Рисунке 6:

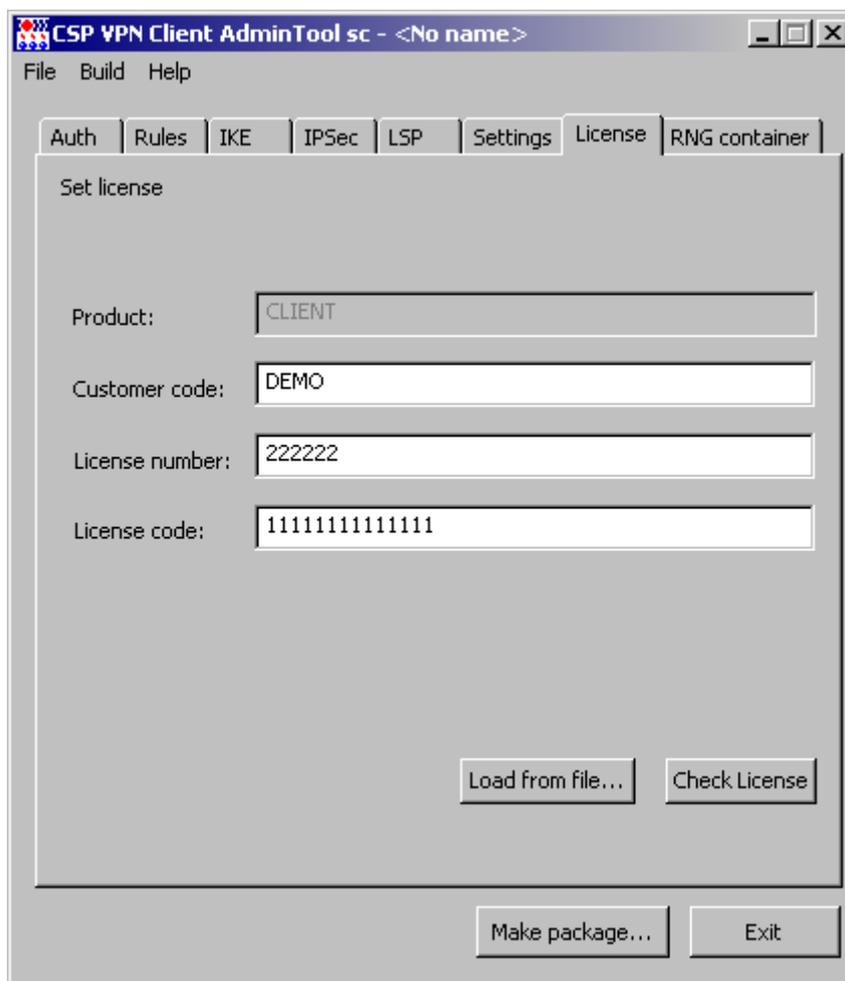


Рисунок 6

Затем перейдем к настройке параметров IPsec в соответствии с нашей схемой.

Во вкладке "Auth" введем значение Preshared key:

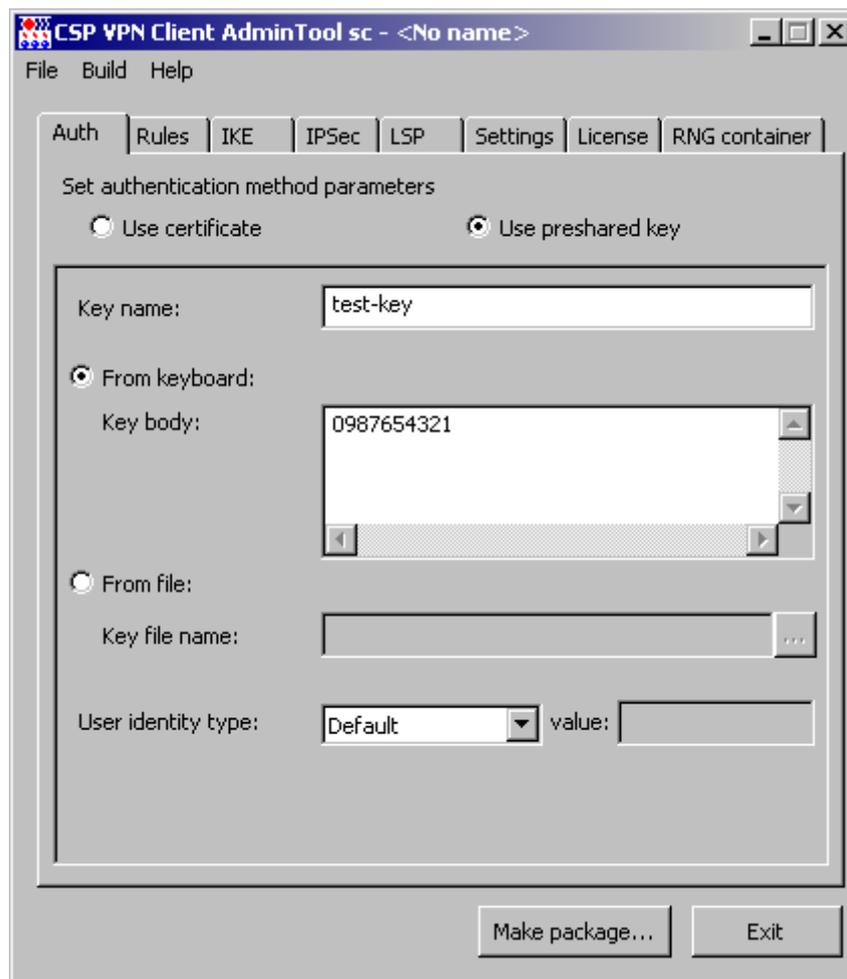


Рисунок 7

В настройках “Rules” опишем правила обработки пакетов, в частности, какой трафик подлежит шифрованию. Нажмем “Add...” для описания нового правила:

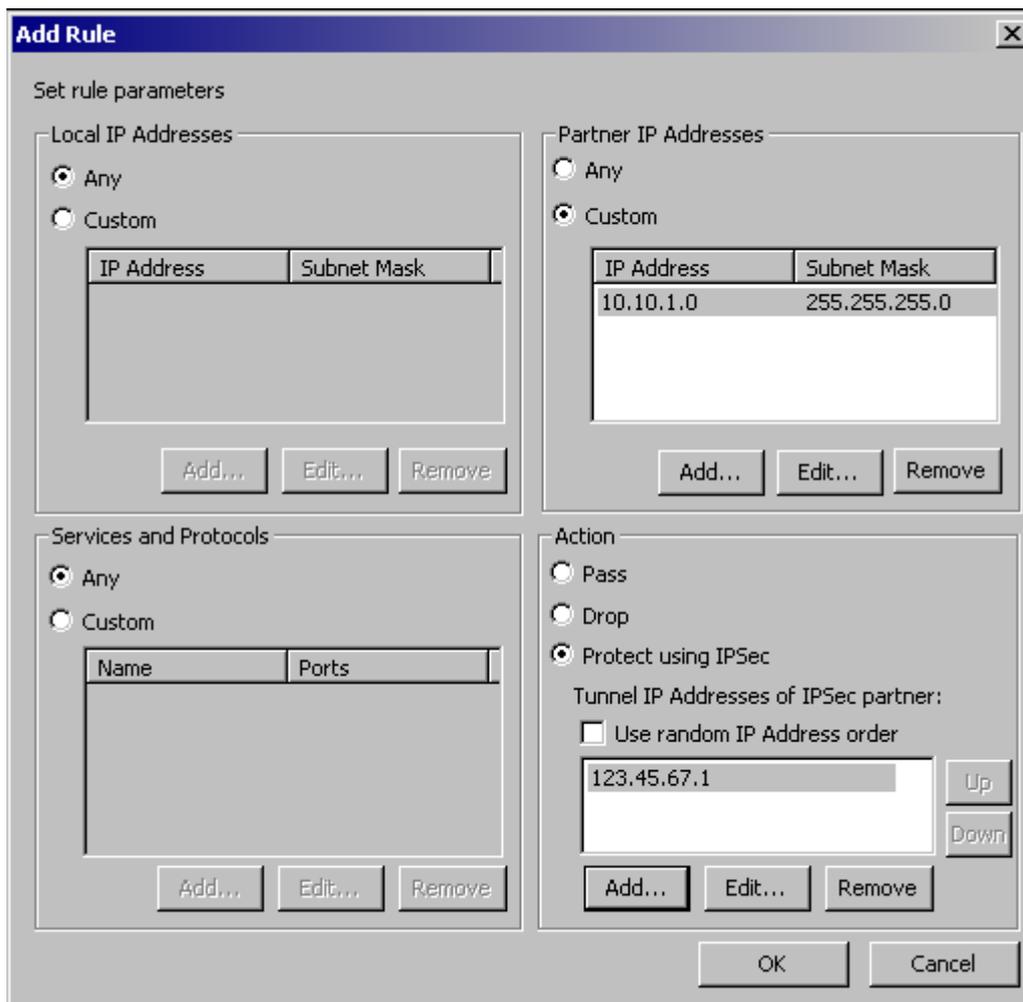


Рисунок 8

Выберем: “Local IP address” – Any; “Partner IP address” – Custom и здесь добавим подсеть 10.10.1.0 с маской 255.255.255.0. Для трафика в эту подсеть выберем Action – “Protect using IPSec” и добавим IP-адрес этого партнера – 123.45.67.1

Аналогичные действия выполним для указания правила к подсети филиала. В результате получим список правил, как изображено на Рисунок 9:

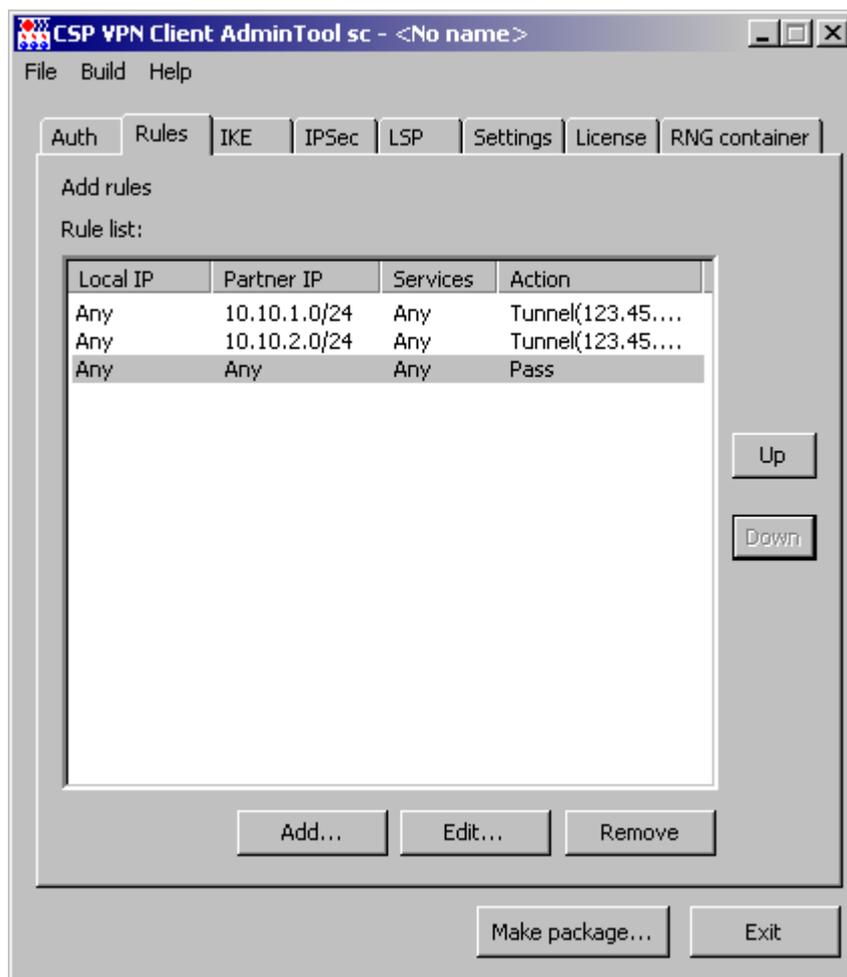


Рисунок 9

Наконец, во вкладке “IPSec” изменим порядок правил преобразования, как показано на Рисунок 10:

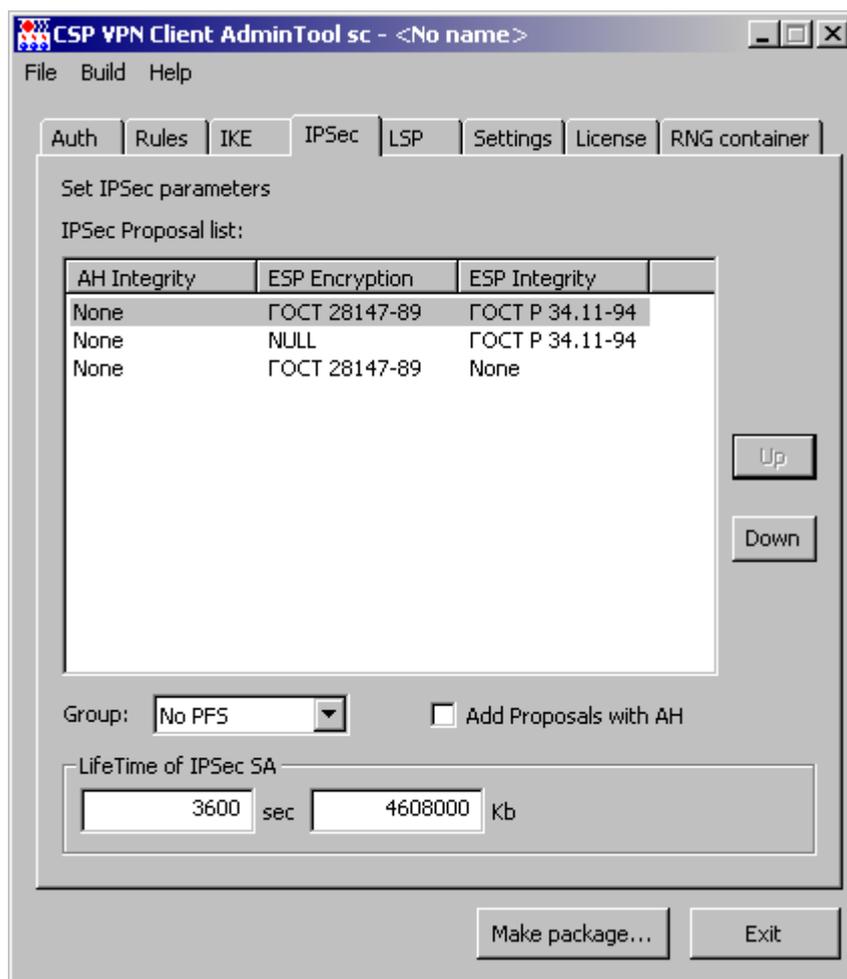


Рисунок 10

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

Теперь можно нажать кнопку “Make package...”

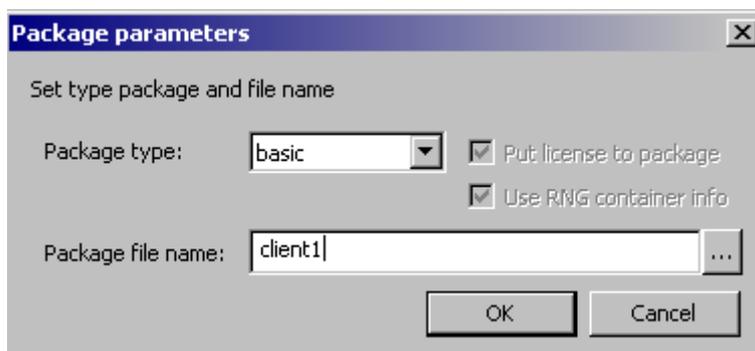


Рисунок 11

Укажем имя и выберем каталог, куда положить инсталляционный пакет. После нажатия кнопки “OK” за несколько секунд будет создан инсталляционный файл, который можно смело ставить на машину пользователя.

Установка клиентского ПО

Его инсталляция не должна вызывать сложностей, нужно только иметь в виду, что несколько VPN клиентов от разных производителей не могут сосуществовать на одной машине. Как и в случае инсталляции ПО модуля, пользователю будет предложено пройти интерактивную инициализацию генератора случайных чисел. Завершается инсталляция приглашением перезапустить компьютер, после этого стартует VPN сервис, который берет на себя задачи установления связи с VPN модулем и шифрования трафика.

Пользователь имеет возможность активизировать/удалить VPN соединение путем выполнения операций Login/Logout в сервис клиента. При этом Login промпт доступен даже до входа в Windows, что позволяет заранее устанавливать соединение с корпоративной сетью и Windows доменом.



Рисунок 12

Мониторинг ISAKMP SA и IPsec SA доступен через выбор предложения Show SA Information в окне, вызываемом при нажатии правой кнопкой мыши на иконке в панели задач Windows.



Рисунок 13

Более подробно подготовка программного обеспечения клиента описана в документации на сайте компании "С-Терра СиЭсПи":

<http://www.s-terra.com/support/documents/ver31/>

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 и модуле.

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/ver31/>

Информацию по технической поддержке, типовых сценариях и часто задаваемых вопросах можно посмотреть по адресу:

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