Построение VPN-каналов с шифрацией по ГОСТ на продуктах Check Point

Валерий Фраерман

Сертифицированный инструктор

Check Point и Juniper

Построение защищенных каналов, сертифицированных в России – задача, актуальная для многих организаций. Компания Check Point Software Technologies обеспечивает возможность решения этой задачи достаточно легко, быстро и на современном уровне. Достигается это путем интеграции программного обеспечения Check Point и сертифицированных криптомодулей компании КриптоПро.

«Боевое» построение туннеля с шифрацией по ГОСТу требует получения исходных последовательностей псевдослучайных данных и сертификатов из сертифицированных источников, хотя логика настройки межсетевого экрана при этом не меняется. В данной статье в основном рассматривается логика и порядок настройки, а также получение необходимых исходных материалов, пригодных для тестирования работы системы. Отличия настройки «боевой» системы приведены в последнем разделе.

1. Предварительные действия

Для построения VPN с шифрацией по ГОСТу нам потребуются следующие компоненты:

1. Обычное программное обеспечение Check Point версии R71.20 (будем считать, что оно уже установлено и настроено, описание этого процесса явно выходит за рамки данной статьи)
2. Лицензия **CPVP-VPG-GOST** на шифрацию ГОСТ. Эта лицензия не входит в 15-дневный пробный период, ее можно запросить у компаний – партнеров Check Point на территории России
3. Лицензия на работу сервера управления, шлюза и VPN – 15-дневный пробный период становится неактивным при установке лицензии на шифрацию ГОСТ. Если это тестовый стенд – можно заказать Evaluation License на 30 дней на сайте Check Point
4. Хотфикс **VPN_R71_20_HF_GOST_V2.0.tgz** – для шлюзов, серверов управления и Provider-1
5. Библиотека модулей шифрации КриптоПро – можно официально скачать с сайта КриптоПро вместе с лицензией на 30 дней
6. SmartConcole **SmartConsole_GOST_R71-20_976001001_1.exe**
7. Программа **csp-win32-kc1-eng.msi**, которую можно скачать с сайта КриптоПро – нужна для генерации файла с исходными псевдослучайными последовательностями – только для тестового развертывания.
8. Сертификаты внешнего удостоверяющего центра, поддерживающего алгоритм ГОСТ – мы получим их от тестового удостоверяющего центра КриптоПро

Предположим, что мы собрали все необходимые компоненты, можно начинать настройку.

2. Получение файла исходных материалов

!!!Это нужно делать только в тестовом варианте!!!

1. Инсталлируйте программу **CSP-Win32-KC1-Eng** на любой компьютер под управлением Windows. Потребуется перезагрузка.
2. Создайте каталоги для файлов исходного материала, например, C:\gamma\db1 и C:\gamma\db2
3. Из командной строки из каталога Program Files\CryptoPro\CSP запустите программу **genkpim <y> <n> <p>**

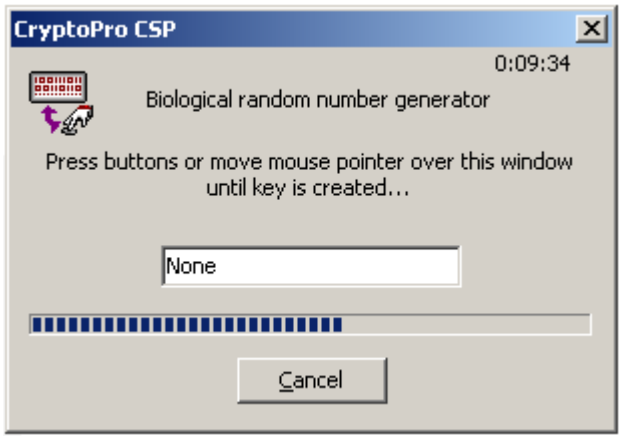
   где

   <y>- количество случайных последовательностей (например, 10)

   <n> - восемь шестнадцатеричных цифр (например, 11111111)

   <p> - путь к каталогам DB1 и DB2, например, C:\gamma

Параметр **<y>** – количество последовательностей – определяет, на какое количество действий хватит файла. После того как одна из последовательностей используется, она помечается как «потраченная» и больше не применяется.



Псевдослучайные последовательности генерируются на основе работы датчика случайных чисел. Если у вас (случайно) нет аппаратного датчика, будет использован биологический – вам придется понажимать клавиши на клавиатуре или поводить мышкой над окошком, пока система не сообщит, что нужное количество данных получено. В результате в каталогах DB1 и DB2 появится файл kis_1, содержащий инициирующие последовательности. Два каталога нужны для надежности, файлы в них одинаковые.

3. Инсталляция хотфикса ГОСТ и библиотек КриптоПро.

1. Разверните архив с модулями шифрации КриптоПро, скачанный с их сайта. Получится каталог с модулями формата ***.rpm**
2. На всех шлюзах безопасности выполните команду **mkdir –p /var/gost_install/rpm** (из экспертного режима) и скопируйте в созданный каталог все модули ***.rpm**, разархивированные на предыдущем шаге. !!!Это нужно только для шлюзов безопасности, не для серверов управления!!!
3. На всех шлюзах безопасности выполните команду **mkdir –p /var/gost_install/kis** (из экспертного режима) и скопируйте в созданный каталог файл с исходными последовательностями **kis_1**
4. Скопируйте файл **VPN_R71_20_HF_GOST_V2.0.tgz** в каталог **/tmp** на всех модулях – и на шлюзах, и на серверах управления
5. Разверните архив командой **tar -zxvf VPN_R71_20_HF_GOST_V2.0.tgz**
6. Запустите скрипт **./UnixInstallScript** из каталога **/tmp**, по окончании его работы подтвердите перезагрузку
7. Установите для каждого модуля лицензию **CPVP-VPG-GOST** и, при необходимости, Evaluation License
8. Установите SmartConsole с поддержкой ГОСТ. Если на этом компьютере уже была установлена обычная SmartConsole версии R71.20, то инсталляцию придется запускать дважды, поскольку первый запуск приведет к деинсталляции установленной версии

4. Инициализация генератора случайных чисел

!!!Данное действие выполняется только на шлюзах, выполнять это на сервере управления не нужно!!!

1. Скопируйте файл **kis_1** в каталоги **/var/opt/cprocsp/dsrf/db1/** и **/var/opt/cprocsp/dsrf/db2/**
2. Последовательно подайте команды
   - **/opt/cprocsp/sbin/ia32/cpconfig -hardware rndm -add cpsd -name 'CPSDRNG' -level 0**
   - **/opt/cprocsp/sbin/ia32/cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1 /var/opt/cprocsp/dsrf/db1/kis_1**
   - **/opt/cprocsp/sbin/ia32/cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1 /var/opt/cprocsp/dsrf/db2/kis_1**

5. Генерация ключей шифрации модулей – Site Key

Данные ключи используются для шифрации передачи служебных данных внутри модуля и между модулями – например, в рамках одного кластера. Используются они только при работе с алгоритмом ГОСТ.

1. В командной строке шлюза из экспертного режима выполните команду **/opt/cprocsp/bin/ia32/cp-genpsk.sh <machine_name> <net_id> <expiry> <Site_ID>**

   где

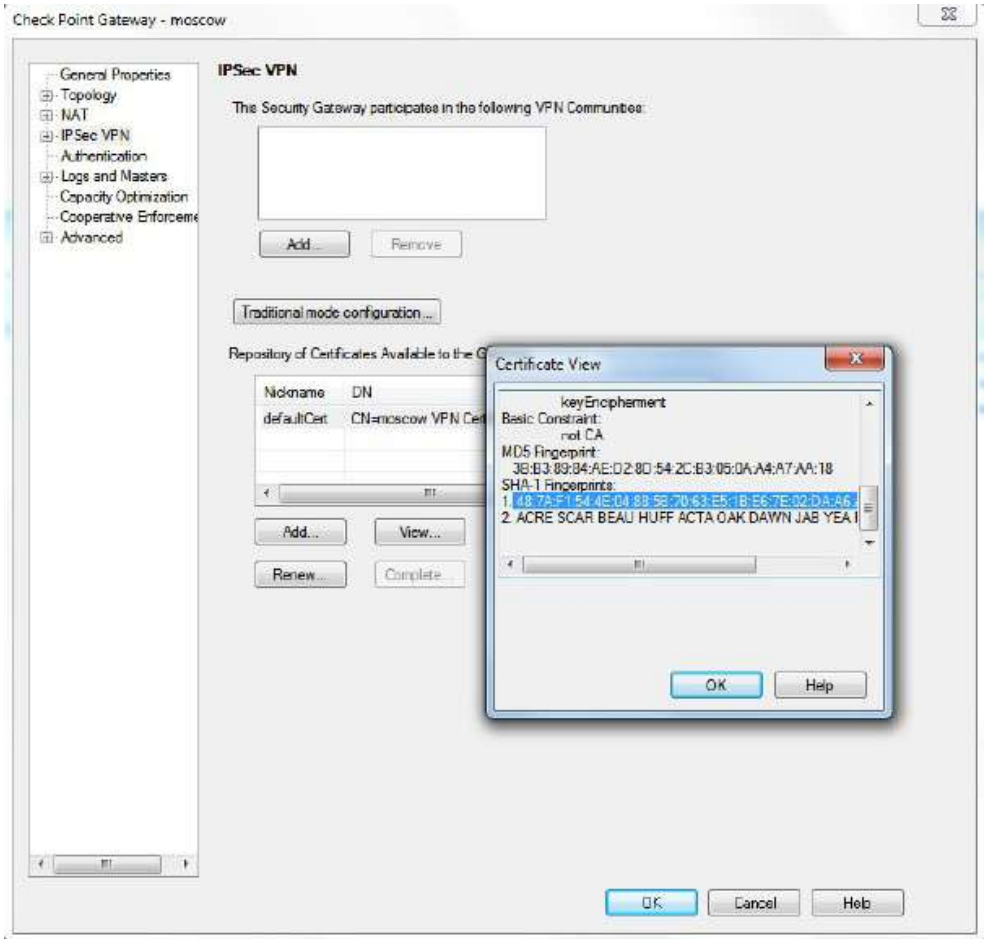
   <machine_name> - произвольное имя

   <net_id> - Net

   <expiry> - срок действия ключа в месяцах (например, 6)

   <Site_ID> - контрольная сумма сертификата данного модуля

Параметр Site_ID представляет собой SHA-1 хэш от SIC-сертификата данного модуля. На скриншоте ниже можно увидеть, где в свойствах модуля можно найти Site_ID.



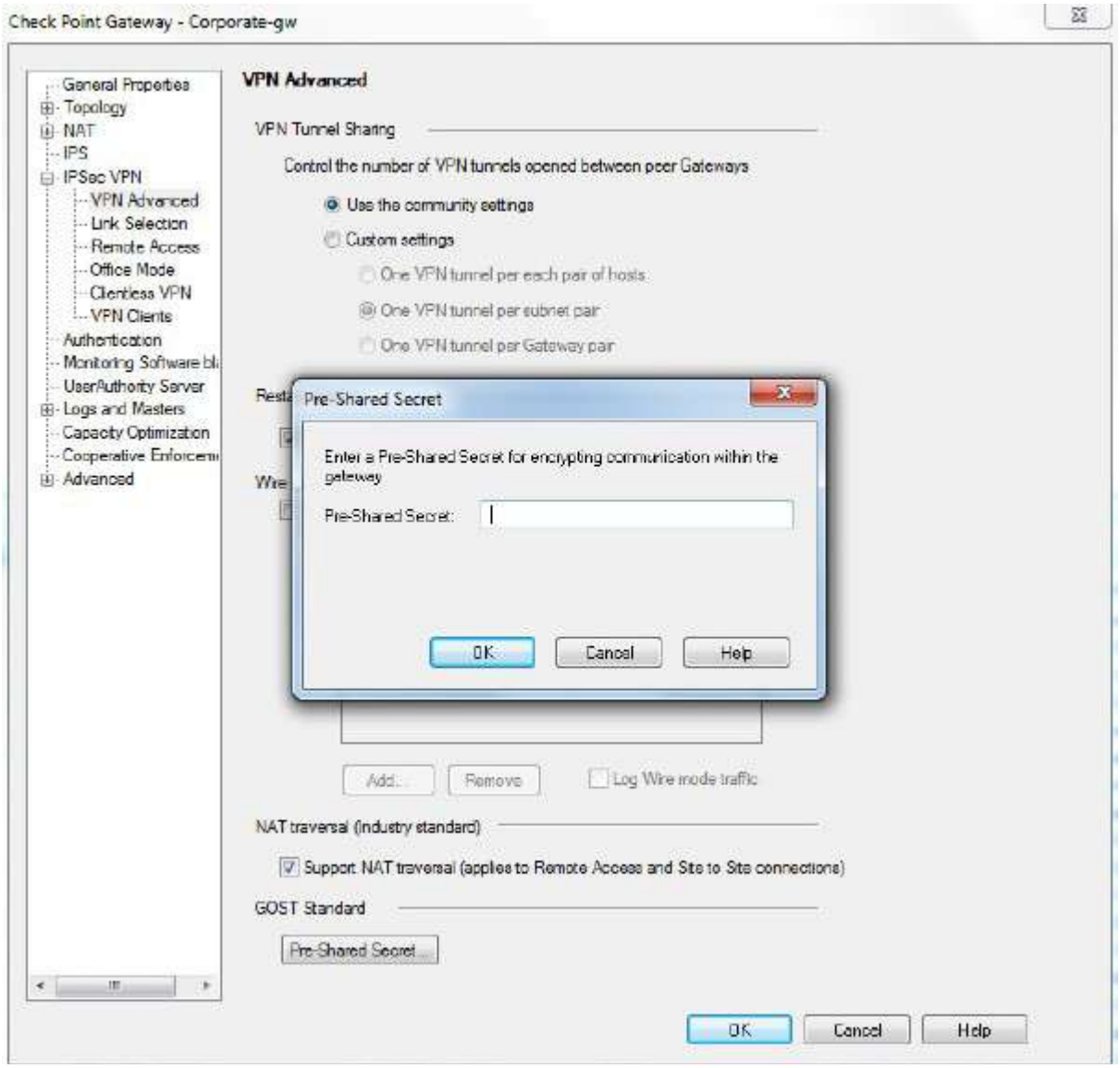
Результатом выполнения такой команды будут две группы из трех одинаковых последовательностей каждая

```
bash /opt/cprocsp/bin/ia32/cp-genpsk.sh GOST_lab_CP Net 6
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3
Convert to integer
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3 =
0x71b4a787
genpsk
   UTC Tue Jan 29 18:30:41 2008

        GOST_lab_CP.  Number of stations 1.
        Stations:
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3
Part 0.     Valid for (months) 6.

  GOST_lab_CP   UTC  Tue Jan 29 18:30:41 2008
   EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3   part 0
valid for (months) 6
893D5WNKNW1AP4
893D5WNKNW1AP4
893D5WNKNW1AP4

genpsk
   UTC Tue Jan 29 18:30:41 2008

        GOST_lab_CP.  Number of stations 1.
        Stations:
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3
Part 1.     Valid for (months) 6.

  GOST_lab_CP   UTC  Tue Jan 29 18:30:41 2008
   EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3   part 1
valid for (months) 6
T2PYY6A49E50U5
T2PYY6A49E50U5
T2PYY6A49E50U5
```

Ключ является конкатенацией частей 0 и 1, в данном примере ключ получится равным

893D5WNKNW1AP4T2PYY6A49E50U5

2. Полученный ключ введите в Gateway properties →IPSec VPN →VPN Advanced → Pre-Shared Secret



Данную последовательность действий нужно повторить для всех шлюзов, работающих с алгоритмами ГОСТ.

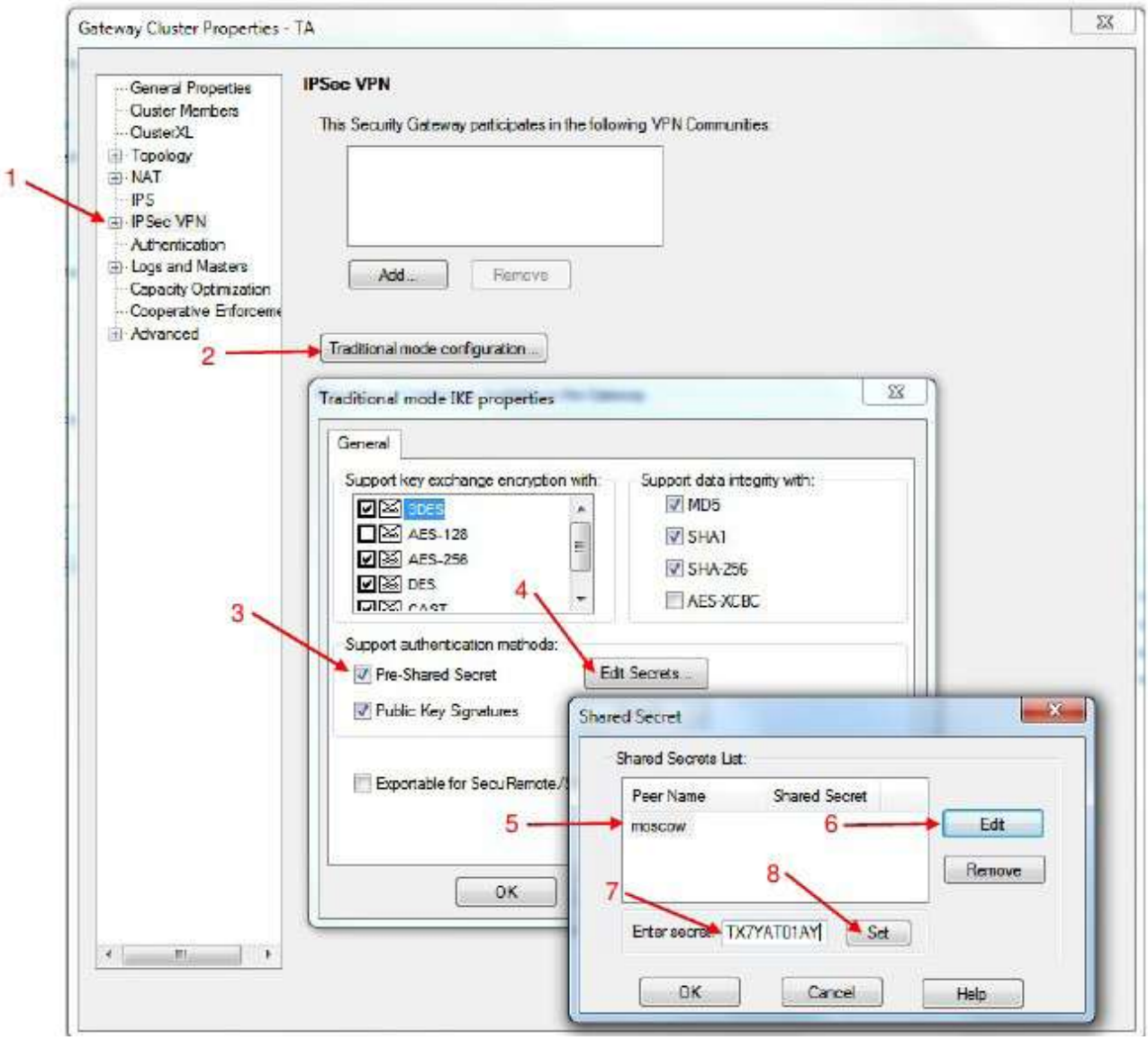
Все вышеперечисленное является предварительными настройками, одинаковыми для аутентификации паролем и сертификатами.

Теперь настроим по очереди оба варианта.

6. Настройка VPN с аутентификацией паролем (PreShared Secret)

1. В настройках VPN Community → Advanced Settings → Shared Secret поставьте галочку “Use Pre-Shared Secret for Authentication in GOST community”

2. Создайте ключ для каждой пары модулей. В случае использования ГОСТ ключ нельзя задавать произвольно, его нужно генерировать. Для этого в свойствах каждого модуля в IPSec VPN → Traditional mode configuration поставьте галочку Pre-Shared Secret (действия 1-3) и нажмите OK



3. Сгенерируйте ключ аутентификации, для этого из командной строки одного из модулей, из экспертного режима выполните команду **/opt/cprocsp/bin/ia32/cp-genpsk.sh <pair_name> <net_id> <expiry><GW_1_Site_ID><GW_2_Site_ID>**

   где <GW_1_Site_ID> и <GW_2_Site_ID> - SHA-1 контрольные суммы сертификатов обоих модулей

Результатом будут четыре последовательности

```
bash /opt/cprocsp/bin/ia32/cp-genpsk.sh GOST_lab_CP Net 6
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3
05:9C:C9:2C:85:6E:65:7F:30:1C:E4:14:95:20:D3:A5:90:E1:6E:15
Convert to integer
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3 =
0x71b4a787
Convert to integer
05:9C:C9:2C:85:6E:65:7F:30:1C:E4:14:95:20:D3:A5:90:E1:6E:15 =
0xe217fbe0
genpsk
   UTC Mon Feb 25 16:49:15 2008

        GOST_lab_CP.  Number of stations 2.
        Stations:
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3
05:9C:C9:2C:85:6E:65:7F:30:1C:E4:14:95:20:D3:A5:90:E1:6E:15
Part 0.     Valid for (months) 6.

  GOST_lab_CP   UTC  Mon Feb 25 16:49:15 2008
   EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3   part 0
valid for (months) 6
948AZ65V617GZ6
948AZ65V617GZ6
948AZ65V617GZ6


  GOST_lab_CP   UTC  Mon Feb 25 16:49:15 2008
   05:9C:C9:2C:85:6E:65:7F:30:1C:E4:14:95:20:D3:A5:90:E1:6E:15   part 0
valid for (months) 6
UDQE383VR2UNF7
UDQE383VR2UNF7
UDQE383VR2UNF7
```

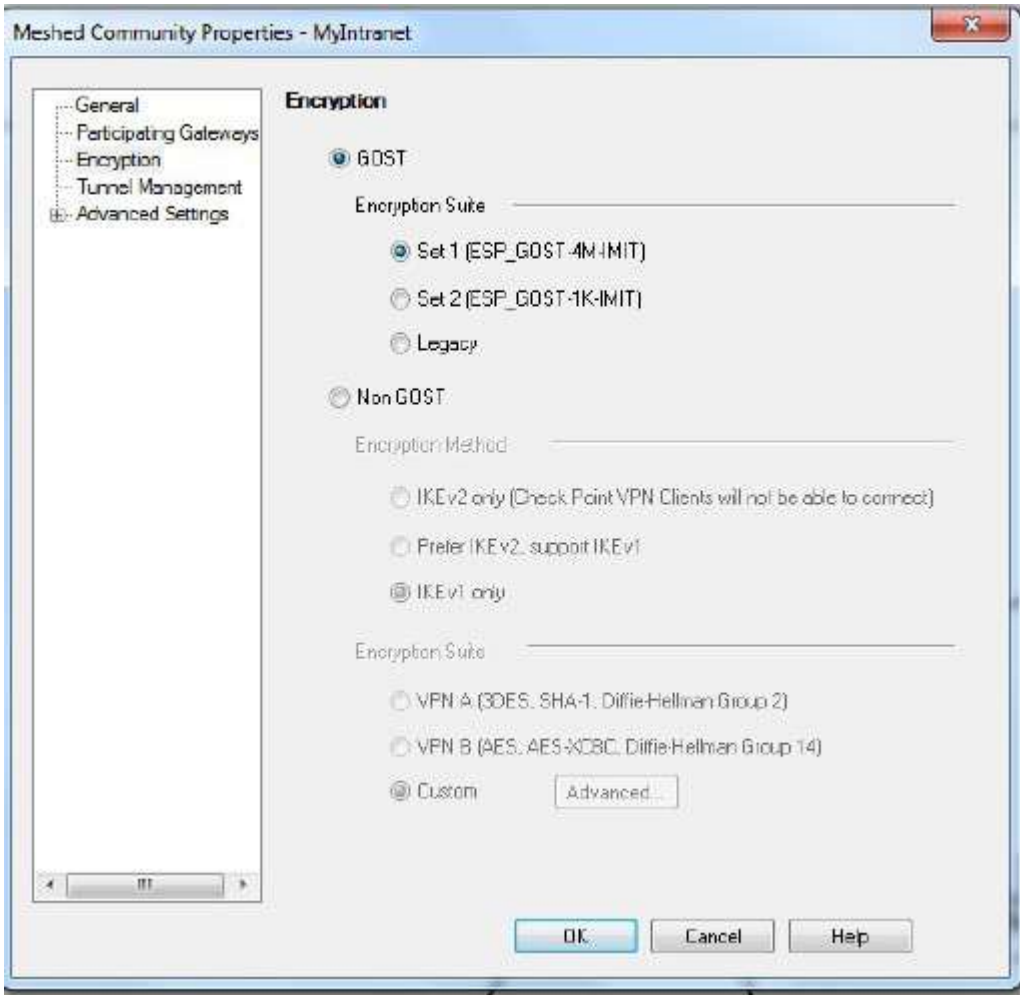
```
genpsk
   UTC Mon Feb 25 16:49:15 2008

        GOST_lab_CP.  Number of stations 2.
        Stations:
EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3
05:9C:C9:2C:85:6E:65:7F:30:1C:E4:14:95:20:D3:A5:90:E1:6E:15
Part 1.     Valid for (months) 6.

  GOST_lab_CP   UTC  Mon Feb 25 16:49:15 2008
   EF:50:3F:90:0E:B1:1C:01:D4:B1:01:1B:38:37:59:62:81:DE:A6:D3   part 1
valid for (months) 6
8M5V1TTUURACU6
8M5V1TTUURACU6
8M5V1TTUURACU6


  GOST_lab_CP   UTC  Mon Feb 25 16:49:15 2008
   05:9C:C9:2C:85:6E:65:7F:30:1C:E4:14:95:20:D3:A5:90:E1:6E:15   part 1
valid for (months) 6
F6TXXUNLF29291
F6TXXUNLF29291
F6TXXUNLF29291
```

Ключ аутентификации является результатом конкатенации ключей из всех четырех последовательностей. Соединять их надо в порядке 1-3-2-4, то есть для данного примера ключ окажется равным

948AZ65V617GZ68*M5V1TTUURACU6*UDQE383VR2UNF7*F6TXXUNLF29291*

4. Полученный ключ скопируйте в настройки Traditional Mode одного из шлюзов (действия 4-8 на изображении выше). В настройках второго модуля ключ появится автоматически

5. Настройте VPN Community с выбором шифрации ГОСТ. Вариант Legacy — для старой версии 1.5, в данной версии уже не поддерживается



!!!После этого надо инсталлировать политику и перезагрузить модули!!!

Перезагрузка будет требоваться каждый раз при переключении между использованием алгоритмов ГОСТ и строенных алгоритмов.

7. Настройка VPN с аутентификацией сертификатами

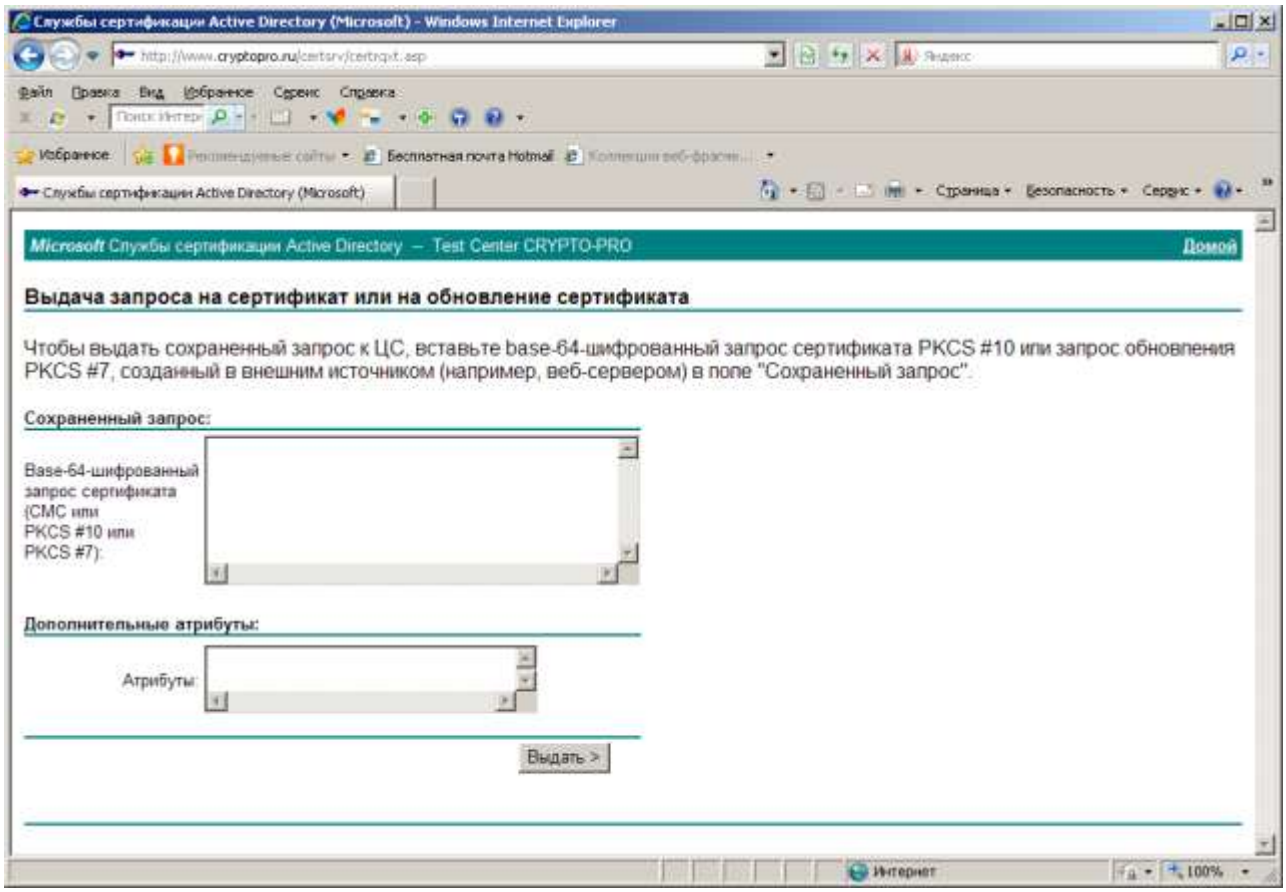
!!!Внимание! В статье используется тестовый удостоверяющий центр, который не может быть использован для построения сертифицированного туннеля!!!

1. Получите сертификат тестового удостоверяющего центра по адресу http://www.cryptopro.ru/certsrv и сохраните его в файл
2. Создайте в SmartDashboard объект Trusted Certificate Authority и загрузите в него полученный сертификат. В случае, если ваши модули не имеют выхода в Интернет, снимите галочку Check CRL и подтвердите при получении предупреждения, иначе система постоянно будет сообщать о невозможности проверки сертификатов, и никакого туннеля вы не получите…
3. Для каждого модуля выполните генерацию запроса на получение внешнего сертификата, нажав кнопку Add в закладке IPSec VPN свойств модуля

Выберите в поле CA to enroll from вновь созданный объект Trusted CA. После нажатия кнопки Generate укажите полное имя модуля, например CN=gost_1,O=gost_1.diona.cp

Сгенерируйте запрос

4. Выберите в списке сертификатов появившуюся строку запроса на сертификат, нажмите кнопку View и скопируйте текст целиком
5. Вставьте текст в окно запроса на получение сертификата на сайте удостоверяющего центра и нажмите кнопку Выдать. Сохраните полученный файл.



6. В списке сертификатов модуля выберите строчку запроса на сертификат, нажмите кнопку, завершающую добавление сертификата, и выберите сохраненный файл

7. После того, как сертификаты будут созданы и загружены во все модули, отмените использование Shared Secret в свойствах VPN Community и инсталлируйте политику. В случае работы с кластером сертификаты должны быть созданы для каждого из модулей — членов кластера

После выполнения настроек разделов 5 или 6 можно убедиться в том, что канал действительно построен, просмотрев лог-файл. В записях о выполнении фазы 1 IKE можно убедиться, что аутентификация произошла паролем или сертификатами соответственно. В записях о шифрованных сессиях можно увидеть, что шифрация происходит с применением алгоритмов ГОСТ, выбранных на этапе настройки VPN Community (раздел 6 пункт 5).

8. Построение сертифицированных туннелей

Технически, с точки зрения настройки, построение сертифицированных туннелей не отличается от того тестового примера, который мы рассмотрели выше, однако все материалы, содержащие шифры, пароли или инициирующие случайные последовательности, должны быть получены из официальных источников.

Ниже перечислены основные отличия построения «боевой» сертифицированной системы от тестовой:

1. Лицензия на работу программного обеспечения, упомянутая в разделе 1, пункт 3, должна быть настоящей, а не Evaluation
2. Набор библиотек КриптоПро, упомянутый в разделе 1, пункт 5, должен быть куплен вместе с лицензией
3. Файл, упомянутый в разделе 1, пункт 7, не требуется
4. Весь раздел 2 выполнять не требуется, вместо этого надо получить официальный файл исходных материалов, сгенерированный на основе работы аппаратного датчика случайных чисел
5. В разделе 7 необходимо использовать сертификаты, полученные от сертифицированного центра выдачи сертификатов

В остальном построение сертифицированного туннеля технически не отличается от описанного в статье. Помимо чисто технических аспектов построение сертифицированных каналов также связано и с рядом организационных мер, но это выходит за рамки рассмотрения данной статьи.