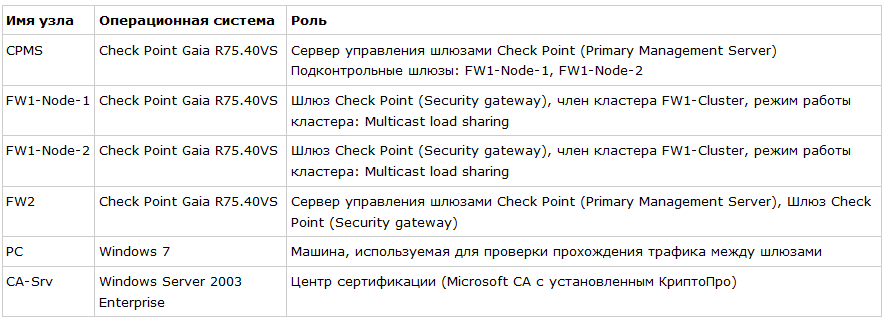
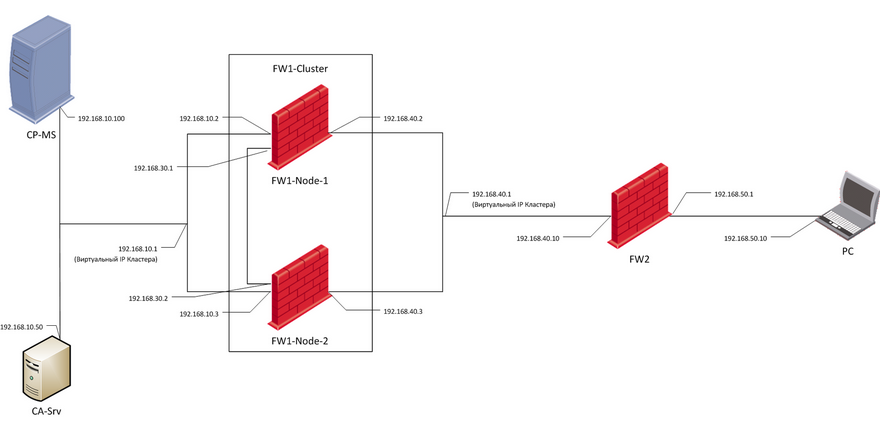
В данной статье мы расскажем вам о процессе настройки IPSec VPN на шлюзах Check Point R75.40VS с применением Российских криптоалгоритмов. Данная статья будет интересна в первую очередь инженерам, осуществляющим настройку и поддержку продуктов компании Check Point.  
  
Когда у меня возникла задача настроить на шлюзах Check Point IPSec VPN с использованием российской криптографии, я столкнулся с проблемой нехватки информации, описывающей данный процесс. По данной теме можно найти официальные гайды, описывающие процесс в общих чертах, и немного разрозненной информации в интернете. Лично у меня после их изучения осталось множество вопросов, которые мы постарались осветить в данной статье.  
  
  
  
Использование ГОСТового шифрования позволяет организациям выполнить требования по криптозащите каналов связи в случаях, когда это продиктовано требованиями Российского законодательства. Следует оговориться, что пока что шлюзы Check Point все еще проходят сертификацию в ФСБ как СКЗИ (средство криптозащиты информации), но производитель обещает, что получит сертификат в обозримом будущем. Хотя сами криптобиблиотеки имеют сертификат ФСБ, остается вопрос контроля их встраивания.  
  
Тема контроля встраивания криптосредств весьма неоднозначна и окончательный ответ на некоторые вопросы может дать лишь ФСБ.   
  
Интересный пост на эту тему можно почитать здесь:  
  
[www.cryptopro.ru/forum2/default.aspx?g=posts&t=1534](http://www.cryptopro.ru/forum2/default.aspx?g=posts&t=1534)  
  
В двух словах о данной теме можно прочитать в конце статьи.  
  
Поддержка ГОСТового шифрования на шлюзах Check Point существует уже довольно давно для сертифицированных и готовящихся к сертификации во ФСТЭК версий межсетевых экранов этого производителя. Возможность использовать ГОСТовое шифрование на шлюзах Check Point появляется благодаря установке специального патча (хотфикса в терминологии Check Point) и криптобиблиотек производства компании КриптоПро. Для всех версий кроме R65.50 доступно только построение IPSec Site-to-Site Domain Based VPN, для версии R65.50 так же доступна возможность построения IPSec Site-to-Site Route Based VPN. На данный момент хотфиксы для ГОСТового IPSec шифрования существуют для следующих версий Check Point:  
  
• R65.50 (используются криптобиблиотеки КриптоПро CSP 3.6);  
• R71.20 (используются криптобиблиотеки КриптоПро CSP 3.6 R2);  
• R75.30 (используются криптобиблиотеки КриптоПро CSP 3.6 R3);  
• R75.40VS (используются криптобиблиотеки КриптоПро CSP 3.6 R3).  
  
Версии R65.50 и R71.20 имеют сертификаты ФСТЭК России на межсетевой экран по третьему классу защищенности, а версия R71.20 дополнительно имеет сертификацию на систему обнаружения вторжений и сертификат на отсутствие не декларированных возможностей по четвертому уровню.  
  
Также следует отметить, что в версиях ГОСТ-пака для R75.30 и R75.40VS реализована поддержка многопоточности, что должно хорошо сказаться на производительности.  
  
В данной статье будет описан процесс настройки ГОСТового шифрования на последней из доступных версий (R75.40VS).  
  
Описание настройки ГОСТового шифрования для версии R71.20 довольно хорошо описано в этой статье:  
  
[www.masterlab.ru/CheckPoint/Knowledgebase/GOST-VPN-on-Check-Point/](http://www.masterlab.ru/CheckPoint/Knowledgebase/GOST-VPN-on-Check-Point/)  
  
Для того чтобы сделать описание более информативным, был выбран не самый простой вариант развёртывания. Описание включает в себя настройку Site-to-Site Domain Based VPN с аутентификацией партнеров по ГОСТовым сертификатам и по паролю (PSK). Для настройки аутентификации партнеров по ГОСТовым сертификатам необходим центр сертификации, позволяющий обеспечить их выпуск, в данном описании используется Microsoft Certification Authority c установленным КриптоПро CSP. Описание интеграции КриптоПро CSP с Microsoft Certification Authority заслуживает отдельного разговора и не будет приводиться в данной статье. Для тестовых целей, если у вас нет желания разворачивать центр сертификации для выпуска ГОСТовых сертификатов, можно использовать тестовый центр сертификации компании КриптоПро, он расположен по этому адресу:  
  
[www.cryptopro.ru/certsrv/](http://www.cryptopro.ru/certsrv/)  
  
Процесс настройки Microsoft Certification Authority c КриптоПро, например, неплохо описан ребятами из S-Terra в админ гайдах на CSP VPN Gate и CSP VPN Client, с которыми можно ознакомиться здесь:  
  
[www.s-terra.com/documents/R31/Gate/CSP\_VPN\_Appendix.pdf](http://www.s-terra.com/documents/R31/Gate/CSP_VPN_Appendix.pdf)  
[www.s-terra.com/documents/R311/Client/CSP\_VPN\_Client\_Admin\_Guide\_cp.pdf](http://www.s-terra.com/documents/R311/Client/CSP_VPN_Client_Admin_Guide_cp.pdf)  
  
В целом весь процесс можно разделить на следующие стадии:  
  
1. Предварительные действия, связанные с установкой и первоначальной настройкой Check Point и центра сертификации;  
2. Генерация файла внешней гаммы для датчиков псевдослучайных чисел, используемых на шлюзах;  
3. Установка хотфикса и криптобиблиотек;  
4. Создание и настройка датчика псевдослучайных чисел;  
5. Настройка VPN:  
5.1. Настройка VPN с использованием сертификатов;  
5.2. Настройка VPN с использованием пароля.  
  
Ниже по пунктам будут рассмотрены все приведенные стадии.  
  
Схема стенда:



  
  
  
  
Для настройки ГОСТового шифрования на шлюзах Check Рoint понадобится следующее программное обеспечение:  
  
• Дистрибутив КриптоПро CSP 3.6 R3 для Windows (x86/x64), скачать можно здесь (необходима регистрация):  
  
[www.cryptopro.ru/sites/default/files/private/csp/36R3/7491/CSPSetup.exe](http://www.cryptopro.ru/sites/default/files/private/csp/36R3/7491/CSPSetup.exe)  
  
• Дистрибутив КриптоПро CSP 3.6 R3 для Check Point SPLAT/GAiA (x86/x64), скачать можно здесь (необходима регистрация):  
  
[www.cryptopro.ru/sites/default/files/private/csp/36R3/7491/splat-gaia.tgz](http://www.cryptopro.ru/sites/default/files/private/csp/36R3/7491/splat-gaia.tgz)  
  
• Дистрибутив Check Point R75.40VS Gaia, скачать можно здесь (необходима регистрация):  
  
[supportcenter.checkpoint.com/supportcenter/portal/user/anon/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit\_doGetdcdetails=&fileid=18503](https://supportcenter.checkpoint.com/supportcenter/portal/user/anon/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=18503)  
  
• Универсальный хотфикс (патч) для поддержки ГОСТ на шлюзах и серверах управления Check Point и специальную версию утилиты управления Check Point SmartConsole, c поддержкой элементов настройки ГОСТ, можно скачать здесь (Если необходим официальный источник, то можно запросить у дистрибьюторов или производителя):  
  
[ngfw.ru/2013/gost-ipsec-v4-r75-40vs](http://ngfw.ru/2013/gost-ipsec-v4-r75-40vs)  
  
В отличие от версий R65.50 и R71.20 настройка ГОСТового шифрования для версий R75.30 и R75.40VS не требует дополнительной лицензии от Check Point (бесплатная лицензия на функционал ГОСТового шифрования) и тестовая настройка может быть полностью произведена на триальных лицензиях.

**1. Предварительные действия**

• Произвести установку и инициализацию шлюзов и сервера управления Check Point;  
• Произвести настройку центра сертификации Microsoft Certification Authority c КриптоПро CSP.

**2. Генерация файла внешней гаммы**

В данном описании файл внешней гаммы создается на машине CA-Srv с помощью биологического датчика случайных чисел, входящего в состав КриптоПро CSP 3.6 для Windows, установленного на машине для создания центра сертификации. Для создания сертифицированного решения в реальных условиях файл внешней гаммы должен быть создан на машине, удовлетворяющей требованиям документа «АРМ выработки внешней гаммы» (ЖТЯИ.00050-03 90 05), который можно скачать здесь (необходима регистрация):  
  
[www.cryptopro.ru/sites/default/files/private/csp/36R3/7491/doc.zip](http://www.cryptopro.ru/sites/default/files/private/csp/36R3/7491/doc.zip)  
  
Данный файл содержит гамму для инициализации программного датчика псевдослучайных чисел, используемого для формирования закрытых ключей шифрования.  
  
Для генерации гаммы выполните следующую последовательность действий:  
  
1) Создайте каталоги для файлов исходного материала (В описываемом случае это отдельный каталог на каждый шлюз, так как использование одного и того же файла на разных шлюзах НЕ ДОПУСКАЕТСЯ, хотя технически это возможно);  
  
2) Из командной строки машины с установленным КриптоПро CSP 3.6 перейдите в директорию C:\Program Files\CryptoPro\CSP и выполните следующую команду:

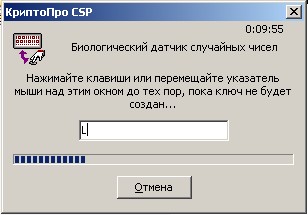
genkpim.exe y n <p>

, где:

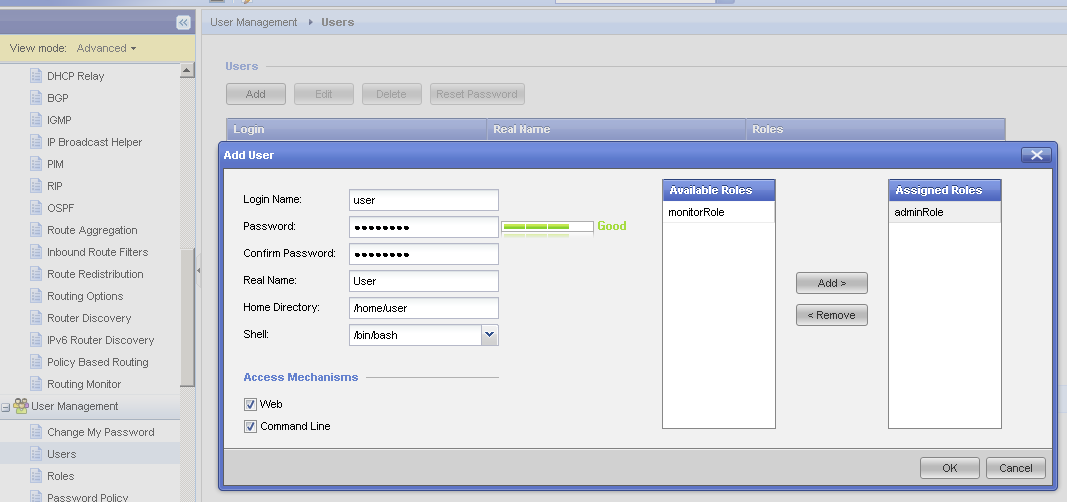
o y – необходимое количество отрезков гаммы (для создания закрытого ключа шифрования используется 2 отрезка, поэтому рекомендуем задавать число отрезков не ниже 10 в тестовом варианте и гораздо большее число, например 1000 в реальных условиях);

o n – номер комплекта внешней гаммы (8 символов в 16-ричном коде), в общем случае любое шестнадцатеричное восьмизначное число, например 11111111;

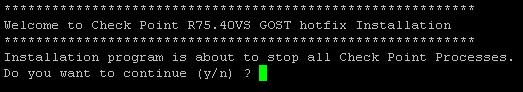
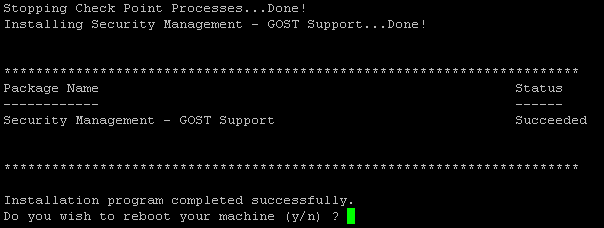
o <p> - путь для сохранения файлов гаммы (соответствующий каталог, созданный на этапе 1).

Пример ввода команды:  
  
image  
  
3) На «правильном» АРМ выработки внешней гаммы используется аппаратный датчик псевдослучайных чисел, входящий в состав электронного замка «Соболь», в тестовом случае используется биологический датчик псевдослучайных чисел и Вам будет предложено понажимать на клавиши или поводить мышью, выглядит это так:  
  
  
  
В случае успешного запуска утилиты genkpim.exe в командную строку будет выдано следующее сообщение:  
  
image  
  
По завершении работы биологического датчика случайных чисел будет создано заданное число отрезков гаммы длиною по 36 байт каждый (32 байта отрезка псевдослучайной последовательности и 4 байта CRC к отрезку). В каталоге, указанном в команде, будет создано два каталога с именами db1 и db2, содержащие по одному файлу c именем kis\_1, данные файлы идентичны и дублируются для надежности.

**3. Установка хотфикса и криптобиблиотек**

Криптобиблиотеки необходимо устанавливать только на шлюзах. На машине, выполняющей роль исключительно сервера управления Check Point, установка криптобибилиотек необязательна. Хотфикс необходимо устанавливать и на шлюзы, и на сервер управления.  
  
Для установки хотфикса на машину, выполняющую роль исключительно сервера управления Check Point, выполните следующую последовательность действий:  
  
1) Скопируйте файл хотфикса (архив с именем VPN\_R75.40VS\_HF\_GOST\_V4.0\_EA) во временную директорию на сервере;  
Для передачи/скачивания файлов с Check Point удобно использовать утилиту WinSCP. Для того чтобы с помощью утилиты WinSCP можно было подключиться с Check Point, необходимо при аутентификации указать пользователя использующего bash как стандартный шел. Для этого необходимо либо временно изменить в настройках шел, используемый пользователем, под которым вы логинитесь, либо создать пользователя, на которого Вы повесите этот шел на постоянной основе. В ОС Gaia это можно сделать через Web-интерфейс, вот пример того, как должно выглядеть окно с настройками для пользователя:  
  
  
  
2) Зайдите на сервер через SSH;  
  
3) Перейдите в экспертный режим;  
  
4) Распакуйте архив в текущий каталог;  
  
5) Запустите установочный скрипт, выполнив команду:

./UnixInstallScript

6) Установка хотфикса вызовет прерывание сервисов, предоставляемых сервером управления, согласитесь с предупреждением об этом:  
  
  
  
7) По завершении установки вам будет выдано следующее сообщение и предложено перезагрузить сервер, соглашайтесь:  
  
  
  
8) После перезагрузки установку хотфикса на сервер управления можно будет считать завершенной, необходимо установить хотфикс и криптобибилиотеки на шлюзы;  
  
9) Для установки хотфикса и криптобибилиотек на машину, выполняющую роль шлюза или шлюза совмещённого с сервером управления, выполните следующую последовательность действий:  
  
• Зайдите на шлюз через SSH;  
  
• Перейдите в экспертный режим;  
  
• Создайте на шлюзе следующие каталоги:

/var/gost\_install/rpm

/var/gost\_install/kis

• Скопируйте на шлюз файлы rmp, входящие в состав дистрибутива КриптоПро CSP 3.6 R3 для Check Point SPLAT/GAiA (x86/x64), в каталог /var/gost\_install/rpm;  
  
• Скопируйте на шлюз соответствующий файл внешней гаммы kis\_1 в каталог /var/gost\_install/kis, это может быть любой файл и советующего каталога db1 или db2 директории, указанной в команде genkpim.exe y n p, так как файлы идентичны;  
  
• Скопируйте хотфикс (архив с именем VPN\_R75.40VS\_HF\_GOST\_V4.0\_EA) во временную директорию на шлюзе;  
  
• Распакуйте архив в текущий каталог;  
  
• Запустите установочный скрипт, выполнив команду:

./UnixInstallScript

• Установка хотфикса вызовет прерывание сервисов, предоставляемых шлюзом (в том числе передачу трафика через шлюз), согласитесь с предупреждением об этом;  
  
• По завершении установки вам будет выдано следующие сообщение и предложено перезагрузить шлюз, соглашайтесь.  
  
Для машины, выполняющей роль шлюза, сообщение будет иметь следующий вид:  
  
  
  
Для машины, выполняющей роль шлюза, совмещённого с сервером управления, – следующий:  
  
  
  
10) По завершении установки вам будет необходимо ввести лицензионный ключ на КриптоПро. Сделать это можно следующей командой:

/opt/cprocsp/sbin/ia32/cpconfig -license -set <лицензионный ключ>

Для просмотра статуса лицензии используется следующая команда:

/opt/cprocsp/sbin/ia32/cpconfig -license -view

В тестовой среде данный пункт можно пропустить и использовать триальную лицензию на КриптоПро.  
  
11) Если вы используете 64 разрядную версию ОС Gaia, вам необходимо отключить технологию SecureXL с помощью утилиты cpconfig, запускаемой из командой строки.

**4. Создание и настройка датчика псевдослучайных чисел**

Данные действия выполняются на шлюзах, в том числе шлюзах, совмещённых с сервером управления.  
  
1) Зайдите на шлюз через SSH;  
  
2) Перейдите в экспертный режим;  
  
3) Скопируйте файл kis\_1 из каталога /var/gost\_install/kis в каталоги /var/opt/cprocsp/dsrf/db1/ и /var/opt/cprocsp/dsrf/db2/;  
  
4) Создайте датчик псевдослучайных чисел, выполнив следующею команду:

/opt/cprocsp/sbin/ia32/cpconfig -hardware rndm -add cpsd -name 'CPSDRNG' -level 0

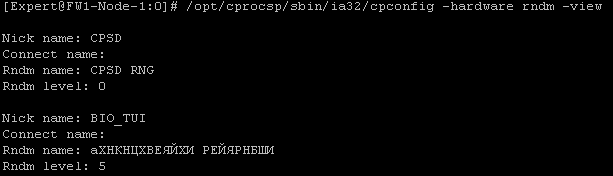
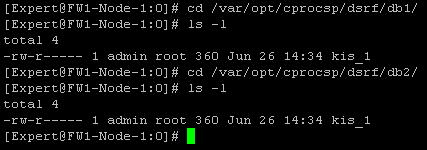
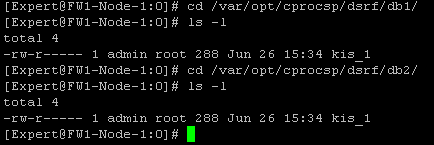
5) Настройте созданный датчик псевдослучайных чисел на использование файла внешней гаммы, выполнив следующие команды:

/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

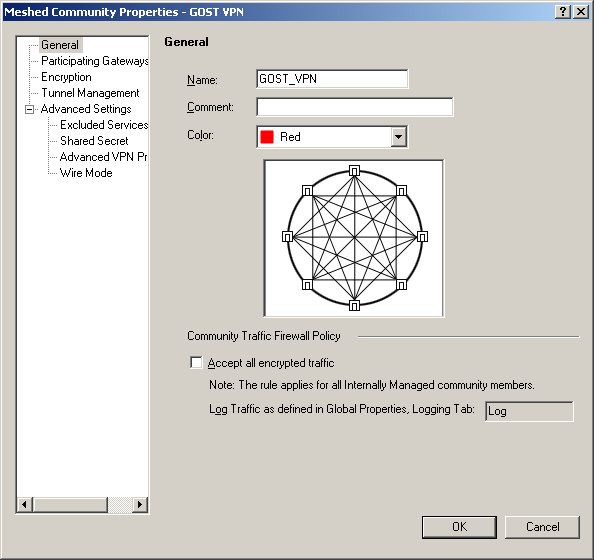
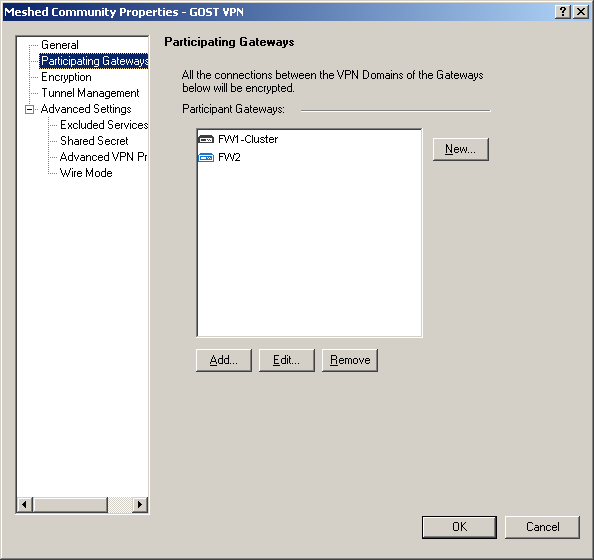
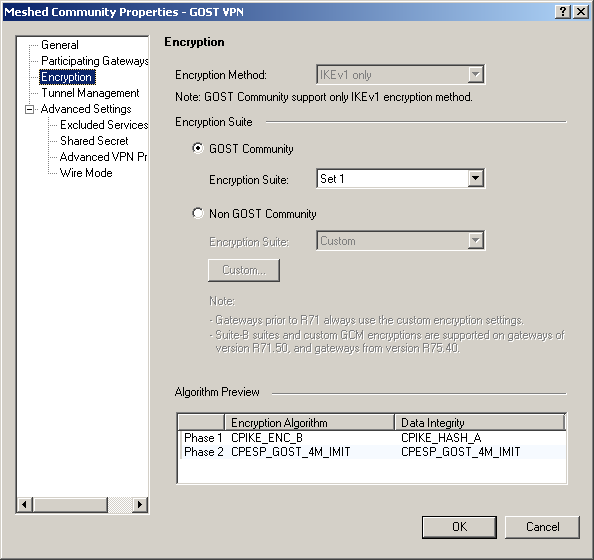
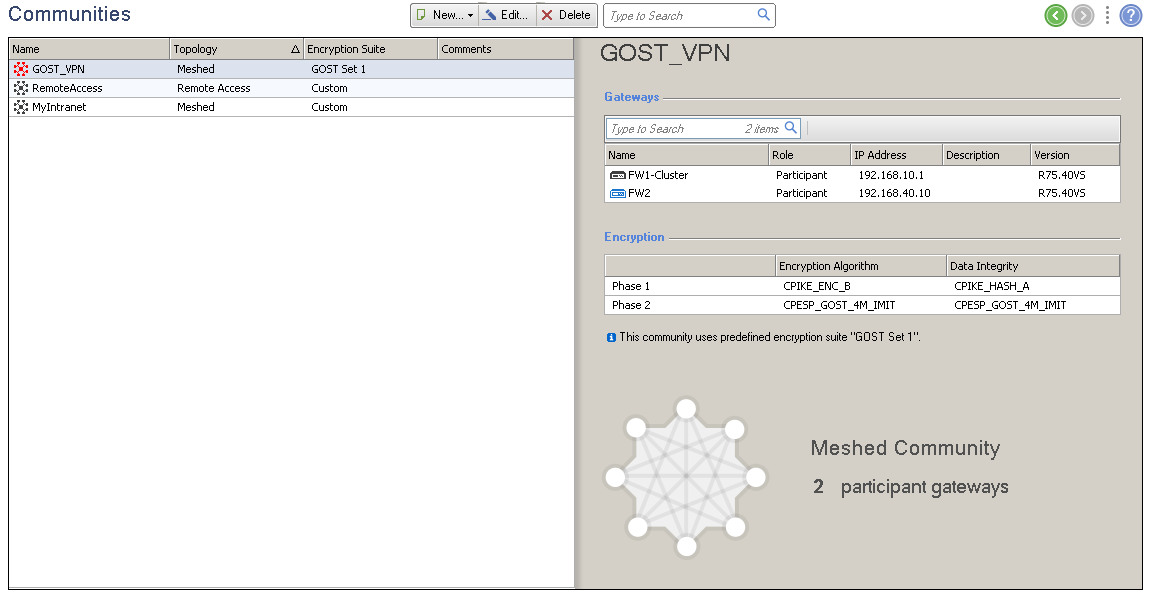
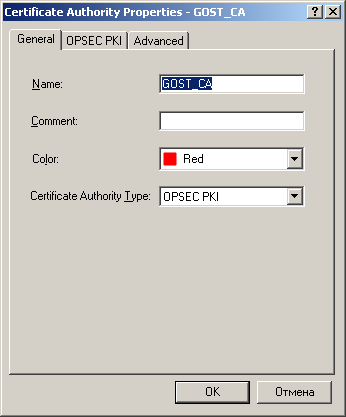
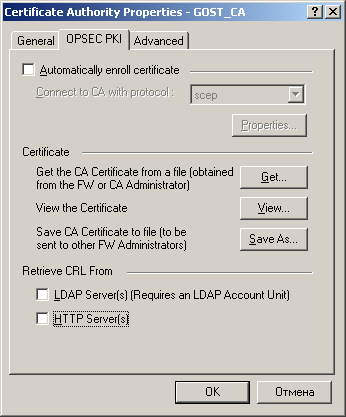
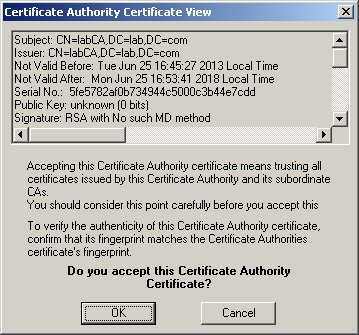
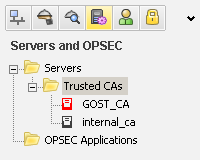
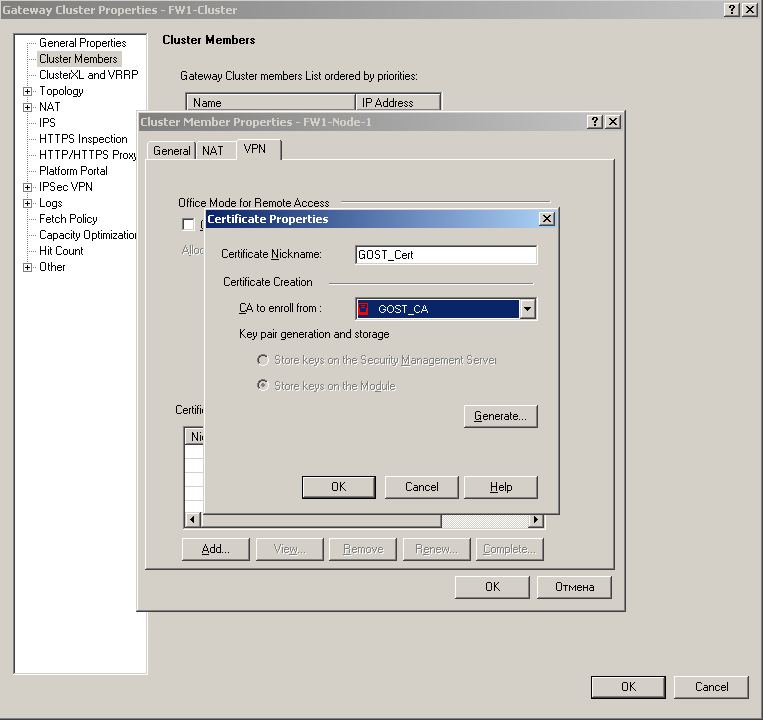
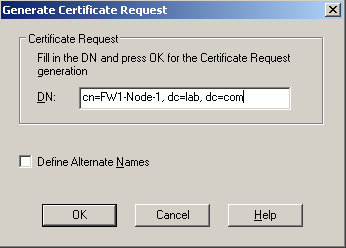
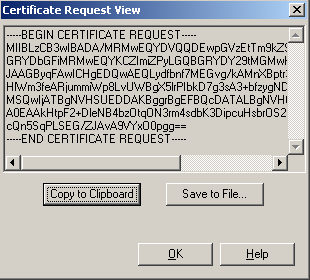
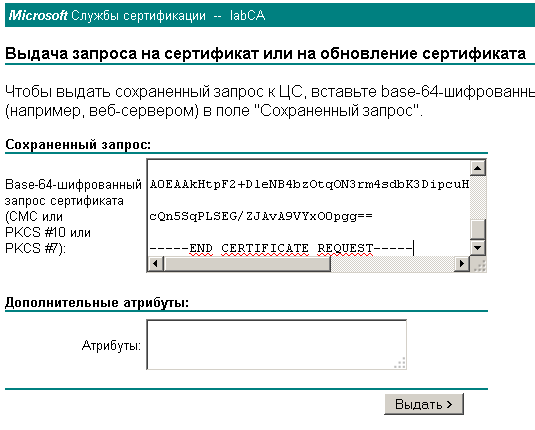
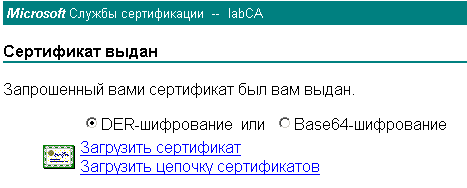
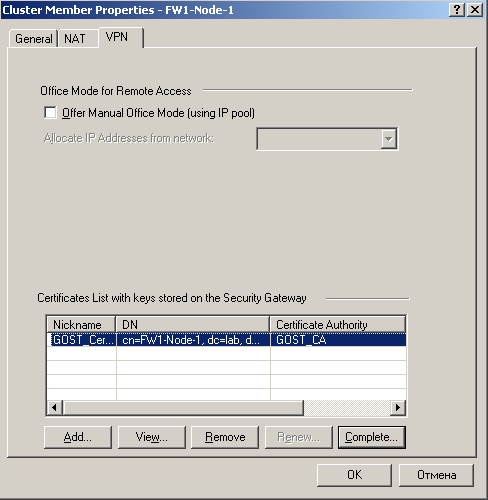
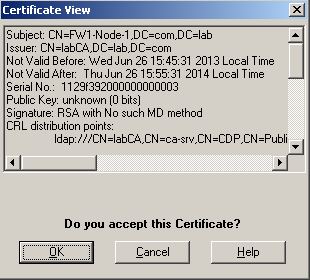
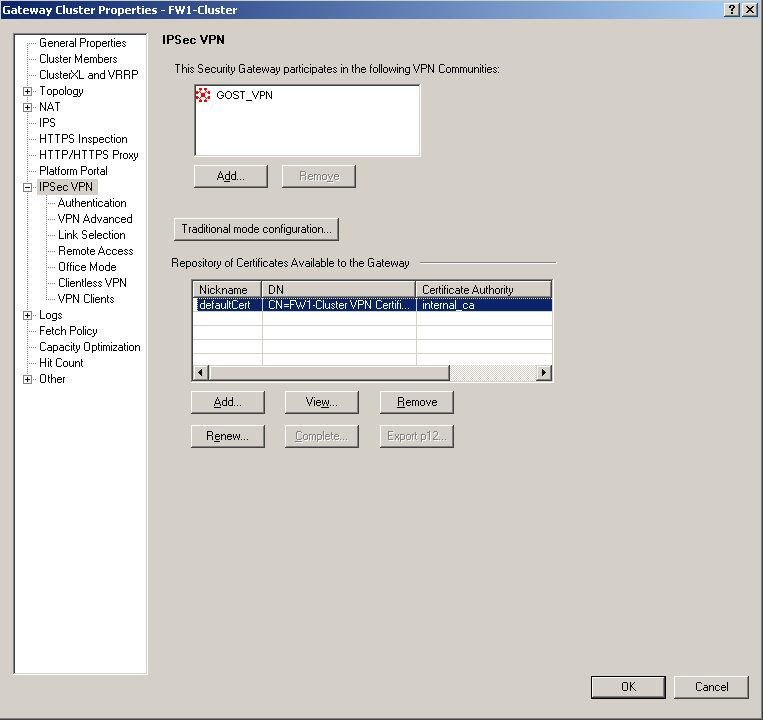
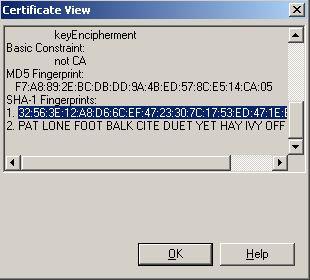
Убедиться в том, что новый датчик псевдослучайных чисел был создан, можно следующей командой:

/opt/cprocsp/sbin/ia32/cpconfig -hardware rndm -view

Вывод команды будет иметь вот такой вид и должен содержать информацию о датчике с именем CPSDRNG и максимальным уровнем приоритета, равным нулю:  
  
  
  
Файл kis\_1 будет расходоваться при инициализации датчика, например, на создание контейнера закрытого ключа, при добавлении сертификата уходит 2 отрезка последовательности. Отрезки последовательности берутся из конца файла, использованные отрезки удаляются.  
  
Например:  
  
Размер файлов до добавления сертификата:  
  
  
  
Размер файлов после добавления сертификата:  
  


**5. Настройка VPN**

**5.1. Настройка VPN с использованием сертификатов**

Для настройки ГОСТового шифрования с аутентификацией партнеров по сертификатам необходимо выполнить следующую последовательность действий:  
  
1) Установить специальную версию Check Point SmartConsole (файл с именем: SmartConsole\_GOST\_R75.40VS\_EA);  
  
2) Зайти на сервер управления с помощью данной утилиты;  
  
3) Создать новое VPN Community:  
  
  
  
4) Поместить в создаваемое VPN Community шлюзы, между которыми будет строиться VPN соединение:  
  
  
  
5) Настроить VPN Community на использование ГОСТового шифрования:  
  
  
  
Предлагается 3 варианта:  
  
Set 1 и Set 2- отличающихся используемыми режимами шифрования, можно использовать любой (поддерживаются всеми версиями, для которых есть ГОСТ, кроме R65.50);  
  
Legacy – режим совместимости с ГОСТ на Check Point R65.50, если есть необходимость построения VPN туннелей со шлюзами, функционирующими на данной версии Check Point.  
  
6) Нажать кнопку «ОК», тем самым создав новое VPN Community;  
  
Список VPN Community будет выглядеть примерно вот так:  
  
  
  
7) После создания VPN Community и добавления в него шлюзов, необходимо внести в конфигурацию сервера управления сведения о ГОСТовом центре сертификации, который будет выпускать сертификаты для наших шлюзов. Добавьте в конфигурацию новый доверенный центр сертификации:  
  
  
  
8) В случае если CRL Distribution Point (в примере это сервер центра сертификации) находится за одним из шлюзов и другие шлюзы будут соединяться с ним через VPN-соединение, эти шлюзы не смогут загрузить CRL, потому что не смогут построить VPN из-за невозможности проверки сертификата первого шлюза. Получиться замкнутый круг. В этом случае необходимо отключить проверку CRL для этого центра сертификации. Для этого необходимо снять все флажки в разделе «Retrieve CRL From» во вкладке OPSEC PKI:  
  
  
  
Или можно вынести CRL Distribution Point за пределы VPN домена защищающего его шлюза, что бы другие шлюзы обращались к нему не через VPN соединение.  
  
9) Выгрузите корневой сертификат центра сертификации в формате DER и добавьте его в конфигурацию Check Point:  
  
  
  
  
10) После добавления нового центра сертификации необходимо выпустить сертификаты для шлюзов. Порядок выпуска и добавления сертификатов для кластера и некластеризованных шлюзов немного отличается.  
  
В случае кластера шлюзов сертификаты выпускаются на КАЖДЫЙ член кластера. Для выпуска сертификата выполните следующую последовательность действий:  
  
• Откройте окно свойств объекта кластера шлюзов;  
  
• Перейдите во вкладку «Cluster Members»;  
  
• Щелкните два раза по объекту члена кластера;  
  
• В открывшемся окне «Cluster Member Properties» перейдите во вкладку «VPN» и в поле «Certificates List with keys stored on Security Gateway» нажмите кнопку «Add»:  
  
  
  
• Введите имя сертификата;  
  
• В поле «CA to enroll from» выберете добавленный ГОСТовый центр сертификации и нажмите кнопку Generate;  
  
• Заполните Distinguished Name для запроса, например:  
  
  
  
• Будет сгенерирован запрос на сертификат, нажмите «Copy to Clipboard»:  
  
  
  
• Вставьте запрос на сертификат в поле «Сохраненный запрос» на портале центра сертификации и нажмите выдать:  
  
  
  
• Сохраните файл сертификата в формате DER:  
  
  
  
• В поле «Certificates List with keys stored on Security Gateway» нажмите кнопку «Complete», в открывшемся окне выберете сохраненный файл сертификата:  
  
  
  
• Примите сертификат:  
  
  
  
• Повторите данную последовательность действий для каждого члена кластера.  
  
В случае выпуска сертификата для некластерированного шлюза запрос на сертификат создается в окне свойств шлюза, раздел «IPSec VPN», графа «Repository of Certificates Available to the Gateway». Также нажмите клавишу «Add», только в случае некластерированного шлюза будет выбор, где будут храниться ключи шифрования. В таком случае необходимо выбрать графу «Store keys on the Module», в остальном процедура полностью аналогична вышеописанной.  
  
  
  
После добавления сертификатов некластерированный шлюз уже готов к построению ГОСТового VPN после установки политики, но в случае кластера это еще не все. КриптоПро шифрует трафик, передаваемый между членами кластера и между библиотеками на шлюзе, используя для этого Site Key или Site Certificate. В случае некластеризованного шлюза, в качестве Site Certificate используется тот сертификат, который был выпущен и добавлен на шлюз. В случае кластера для этих целей может быть использован только Site Key и его необходимо сгенерировать и внести в конфигурацию;  
  
11) Для генерации Site Key необходимо выполнить следующую последовательность действий:  
  
• Открыть окно свойств объекта шлюза, в разделе «IPSec VPN» в графе «Repository of Certificates Available to the Gateway» выбрать сертификат, выданный шлюзу внутренним центром сертификации (Check Point internal\_ca), и нажать кнопку «View»;  
  
  
  
• В открывшемся окне свойств сертификата необходимо найти первую строчку с SHA-1 хешем сертификата, она понадобится для генерации Site Key;  
  
  
  
• На любом шлюзе с установленным КриптоПро из экспертного режима необходимо выполнить команду:

bash /opt/cprocsp/bin/ia32/cp-genpsk.sh <machine\_name> <net\_id> <expiry> <Site\_ID>

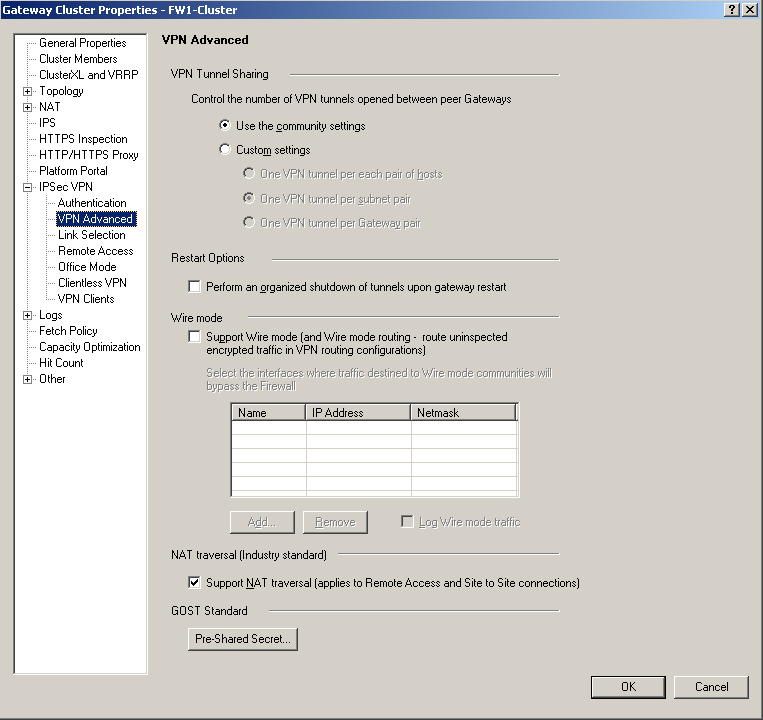
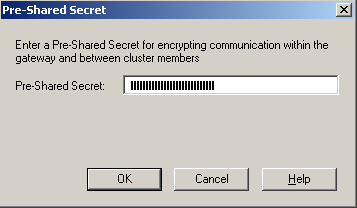
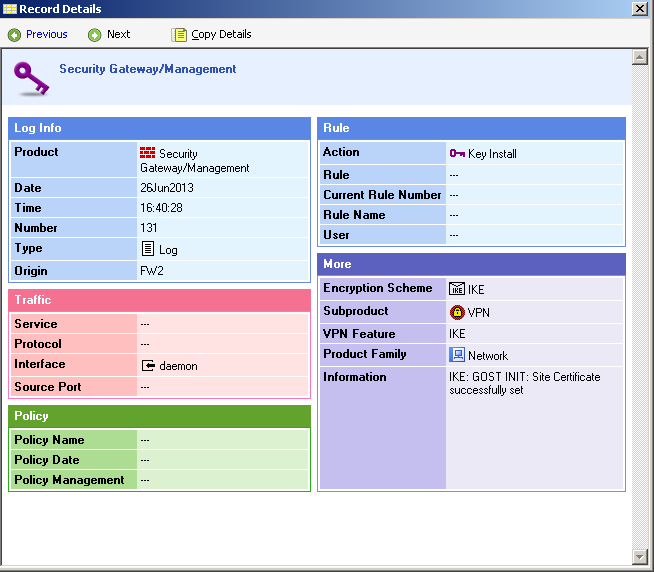
, где:

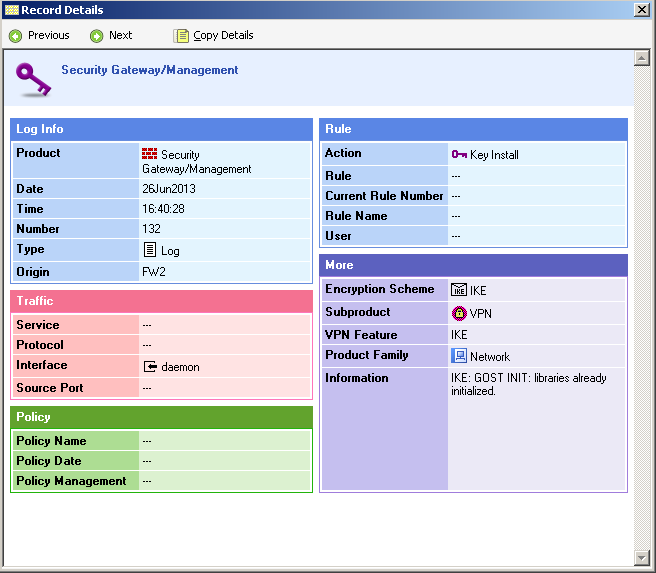
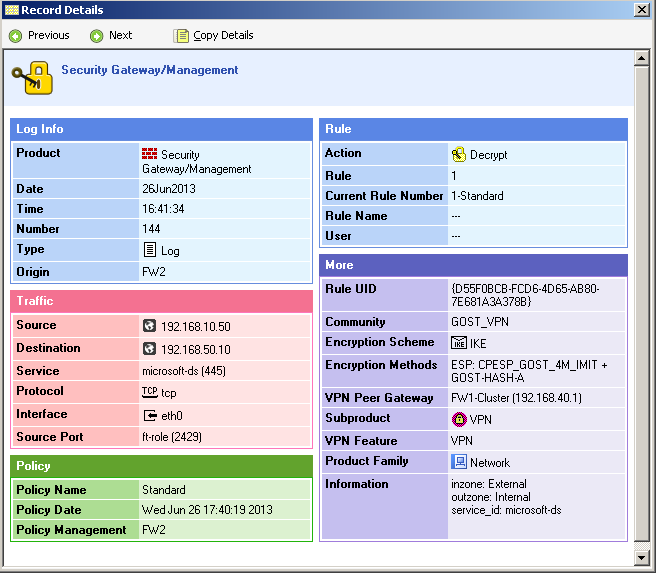
o <machine\_name> - имя шлюза;

o <net\_id> - неописанный, но обязательный параметр, должно стоять Net, причем, если вставить параметр Net с прописной буквы, вывод команды будет корректным, но сгенерированный Site Key работать НЕ БУДЕТ;

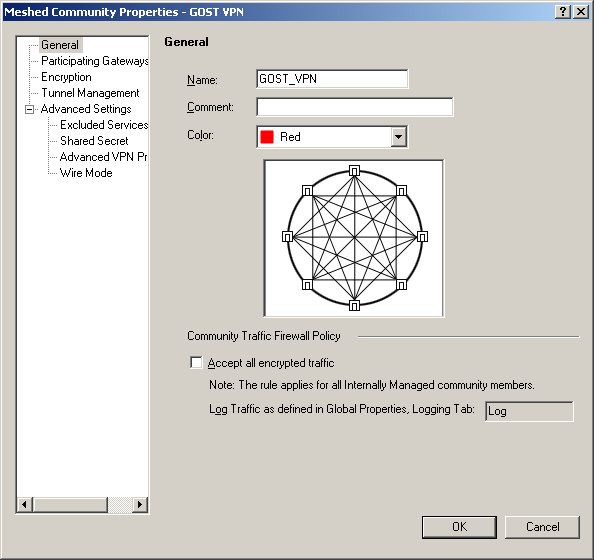
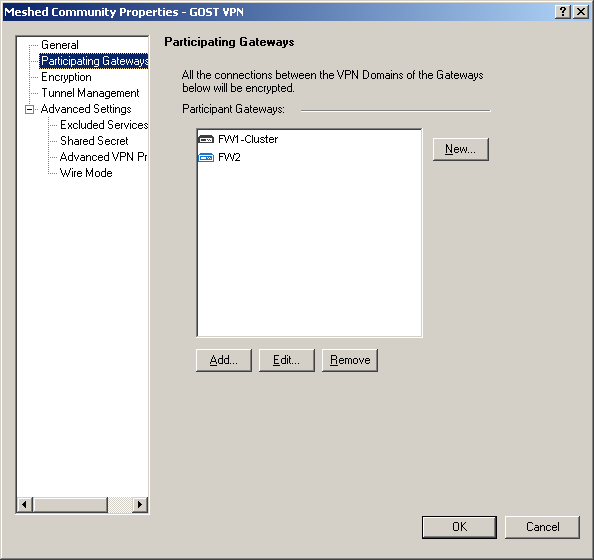
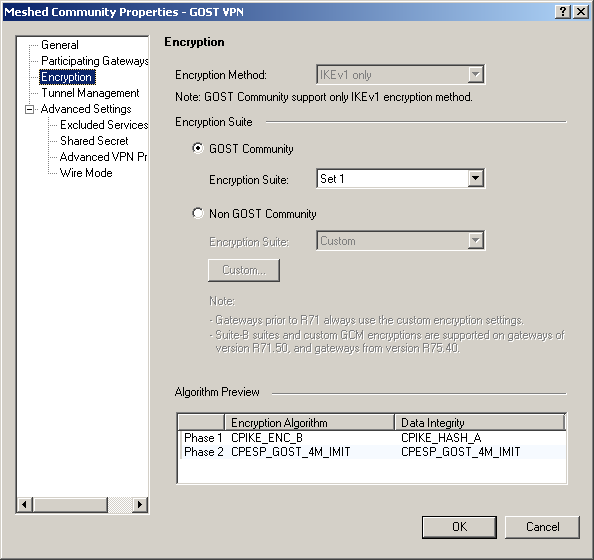
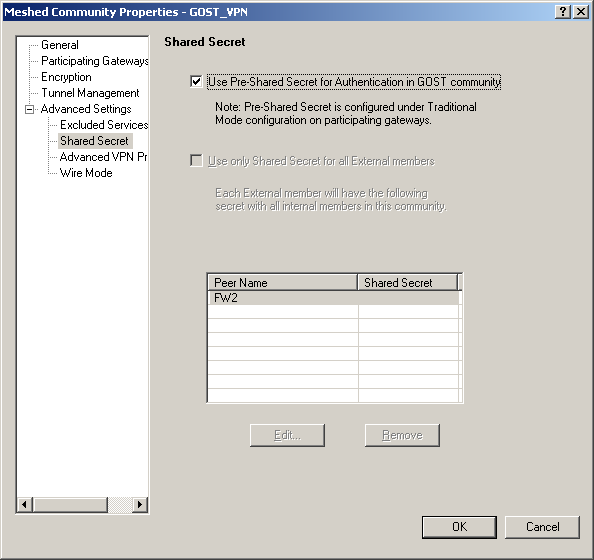
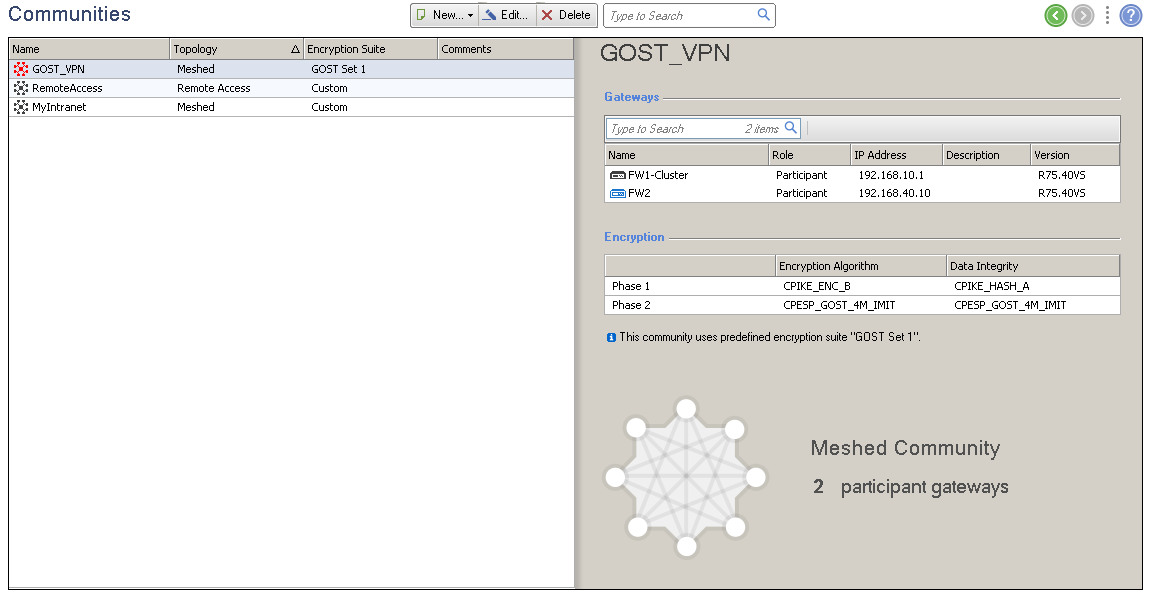
o <expiry> - срок действия ключа в месяцах, максимальное значение 6;

o <Site\_ID> - первая срока с SHA-1 хешем сертификата.

Пример выполнения и вывода команды:  
  
[Expert@FW1-Node-1:0]# bash /opt/cprocsp/bin/ia32/cp-genpsk.sh FW1-Cluster Net 6 32:56:3E:12:A8:D6:6C:EF:47:23:30:7C:17:53:ED:47:1E:BD:7F:7D  
genpsk  
UTC Wed Jun 26 12:15:53 2013  
  
FW1-Cluster. Net. Number of stations 1.  
Stations: 32563E12A8D66CEF4723307C1753ED471EBD7F7D  
Part 0. Valid for (months) 6.  
  
FW1-Cluster UTC Wed Jun 26 12:15:53 2013  
32563E12A8D66CEF4723307C1753ED471EBD7F7D part 0 valid for (months) 6  
W6426WLHP3C8TM  
W6426WLHP3C8TM  
W6426WLHP3C8TM  
  
genpsk  
UTC Wed Jun 26 12:15:53 2013  
  
FW1-Cluster. Net. Number of stations 1.  
Stations: 32563E12A8D66CEF4723307C1753ED471EBD7F7D  
Part 1. Valid for (months) 6.  
  
FW1-Cluster UTC Wed Jun 26 12:15:53 2013  
32563E12A8D66CEF4723307C1753ED471EBD7F7D part 1 valid for (months) 6  
41NKET2QC6B3NW  
41NKET2QC6B3NW  
41NKET2QC6B3NW  
  
• Вывод команды содержит две части сгенерированного Site Key, которые нужно совместить и внести в конфигурацию кластера. Первая часть помечена зеленым, вторая часть помечена красным. Совмещать их нужно так:  
  
W6426WLHP3C8TM41NKET2QC6B3NW  
  
Site Key должен быть повторно сгенирирован в следующих случаях:  
  
• Истек срок действия Site Key;  
• VPN был включен и выключен;  
• Сертификат выданный внутренним центром сертификации (internal\_ca) был обновлен.  
  
• После того как у вас появился Site Key, его необходимо внести в конфигурацию кластера. Откройте окно свойств объекта кластера, раздел «IPSec VPN», графа «VPN Advanced» и нажмите кнопку «Pre-Shared Secret» в разделе «GOST Standard»:  
  
  
  
• В открывшемся окне введите Site Key и нажмите ОК:  
  
  
  
12) Теперь можно установить политики на шлюзы и проверить логи на предмет того, что VPN успешно собрался. В логах должны присутствовать сообщения об успешной установке Site Key или Site Certificate и инициализации криптобиблиотек и сообщения типов Encrypt/Decrypt для трафика, передаваемого через VPN соединение. Примеры сообщений:  
  


  
  
  
13) Если политика установилась без ошибок и данные сообщения в логах присутствуют, то поздравляю вас, вам успешно удалось настроить VPN с использованием ГОСТового шифрования.

**5.2. Настройка VPN с использованием пароля**

Если в силу стечения обстоятельств у вас нет желания или возможности заморачиваться с сертификатами, можно настроить аутентификацию партнеров с использованием парольной фразы. Крайне не рекомендуется использование данного варианта при большом количестве шлюзов в силу сложности работы с большим количеством паролей, а так как пароль необходимо указывать для каждой пары шлюзов, их количество может быть поистине колоссальным. Итак, чтобы настроить ГОСТовый VPN с использованием пароля, необходимо выполнить следующую последовательность действий:  
  
1) Установить специальную версию Check Point SmartConsole (файл с именем: SmartConsole\_GOST\_R75.40VS\_EA);  
  
2) Зайти на сервер управления с помощью данной утилиты;  
  
3) Создать новое VPN Community:  
  
  
  
4) Поместить в создаваемое VPN Community шлюзы, между которыми будет строиться VPN соединение:  
  
  
  
5) Настроить VPN Community на использование ГОСТового шифрования:  
  
  
  
Предлагается 3 варианта:  
  
Set 1 и Set 2- отличающихся используемыми режимами шифрования, можно использовать любой (поддерживаются всеми версиями, для которых есть ГОСТ, кроме R65.50);  
  
Legacy – режим совместимости с ГОСТ на Check Point R65.50, если есть необходимость построения VPN туннелей со шлюзами, функционирующими на данной версии Check Point.  
  
6) Установить в настройках VPN Community использование пароля для аутентификации. Делается это в свойствах VPN Community в разделе «Advanced Settings», пункт «Shared Secret»:  
  
  
  
7) Нажать кнопку «ОК», тем самым создав новое VPN Community;  
  
Список VPN Community будет выглядеть примерно вот так:  
  
  
  
8) Сгенерировать Site Key для КАЖДОГО шлюза, как это прописано в разделе 5.1 пункт 11. В случае кластера шлюзов генерируется один Site Key на кластер. Если у вас на некластеризованном шлюзе есть установленный ГОСТовый сертификат, то Site Key для этого шлюза можно не генерировать. Для некластеризованных шлюзов может использоваться как Site Key, так и Site Certificate. Site Certificate предпочтительнее и, если есть сертификат, будет использован именно он;  
  
9) После генерации и установки Site Key, необходимо сгенерировать пароль для пары шлюзов. В отличие от «традиционной» настройки VPN на Check Point при настройке ГОСТового VPN нельзя использовать произвольный пароль, его нужно сгенерировать по аналогии с Site Key. Чтобы сгенерировать пароль для пары шлюзов, выполните следующую последовательность действий:  
  
• На любом шлюзе с установленным КриптоПро из экспертного режима необходимо выполнить команду:

bash /opt/cprocsp/bin/ia32/cp-genpsk.sh <pair\_name> <net\_id> <expiry> <GW\_1\_Site\_ID> <GW\_2\_Site\_ID>

, где:

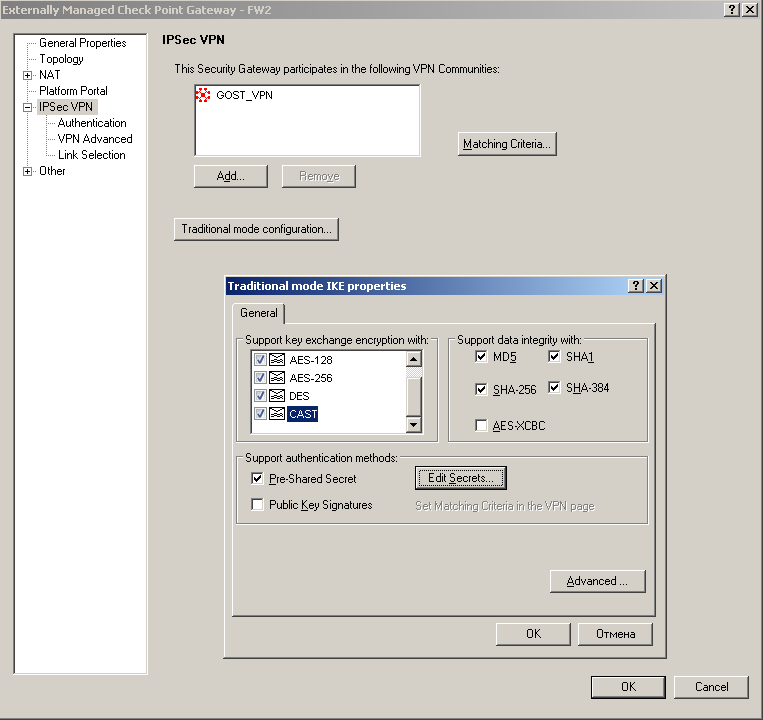
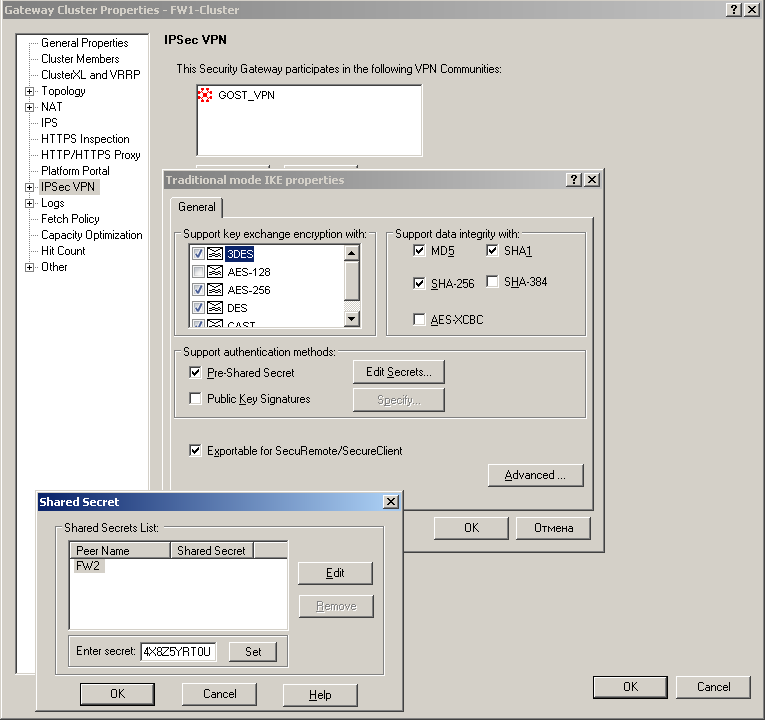
o <pair\_name> - имя пары шлюзов;

o <net\_id> - неописанный но обязательный параметр, должно стоять Net, причем если вставить параметр Net с прописной буквы вывод команды будет корректным, но сгенерированный пароль работать НЕ БУДЕТ;

o <expiry> - срок действия ключа в месяцах, максимальное значение 6;

o <GW\_1\_Site\_ID> - первая срока с SHA-1 хешем сертификата первого шлюза пары;

o <GW\_2\_Site\_ID> - первая срока с SHA-1 хешем сертификата второго шлюза пары.

Какой-либо принципиальной разницы в том, какой шлюз первый, а какой второй –нет, поле <pair\_name> можно заполнить произвольно.  
  
Пример выполнения и вывода команды:  
  
Expert@FW1-Node-1:0]# bash /opt/cprocsp/bin/ia32/cp-genpsk.sh FW1-FW2 Net 6 32:56:3E:12:A8:D6:6C:EF:47:23:30:7C:17:53:ED:47:1E:BD:7F:7D A6:F0:24:9A:16:AA:7F:42:9A:3A:A2:83:66:FA:67:E9:75:08:46:1B  
genpsk  
UTC Sat Jun 29 11:17:26 2013  
  
FW1-FW2. Net. Number of stations 2.  
Stations: 32563E12A8D66CEF4723307C1753ED471EBD7F7D A6F0249A16AA7F429A3AA28366FA67E97508461B  
Part 0. Valid for (months) 6.  
  
FW1-FW2 UTC Sat Jun 29 11:17:26 2013  
32563E12A8D66CEF4723307C1753ED471EBD7F7D part 0 valid for (months) 6  
BC1HGFATY4N6QM  
BC1HGFATY4N6QM  
BC1HGFATY4N6QM  
  
FW1-FW2 UTC Sat Jun 29 11:17:26 2013  
A6F0249A16AA7F429A3AA28366FA67E97508461B part 0 valid for (months) 6  
ZPYLCHU36QNZNM  
ZPYLCHU36QNZNM  
ZPYLCHU36QNZNM  
  
genpsk  
UTC Sat Jun 29 11:17:26 2013  
  
FW1-FW2. Net. Number of stations 2.  
Stations: 32563E12A8D66CEF4723307C1753ED471EBD7F7D A6F0249A16AA7F429A3AA28366FA67E97508461B  
Part 1. Valid for (months) 6.  
  
FW1-FW2 UTC Sat Jun 29 11:17:26 2013  
32563E12A8D66CEF4723307C1753ED471EBD7F7D part 1 valid for (months) 6  
WKDHN8MRYD599U  
WKDHN8MRYD599U  
WKDHN8MRYD599U  
  
FW1-FW2 UTC Sat Jun 29 11:17:26 2013  
A6F0249A16AA7F429A3AA28366FA67E97508461B part 1 valid for (months) 6  
FN4T4X8Z5YRT0U  
FN4T4X8Z5YRT0U  
FN4T4X8Z5YRT0U  
  
• Вывод команды содержит четыре части сгенерированного пароля, которые нужно совместить и внести в конфигурацию. Первая часть помечена зеленым, вторая часть помечена красным, третья честь помечена синим, четвертая – оранжевым, но совмещаются они, в отличие от Site Key, не по порядку, а так: часть 1 + часть 3 + часть 2 + часть 4, пример совмещения частей:  
  
BC1HGFATY4N6QMWKDHN8MRYD599UZPYLCHU36QNZNMFN4T4X8Z5YRT0U  
  
Пароль должен быть повторно сгенирирован в следующих случаях:  
  
• Истек срок действия пароля;  
• VPN был включен и выключен;  
• Сертификат выданный внутренним центром сертификации (internal\_ca) был обновлен.  
  
10) После того как у вас появился пароль, его необходимо внести в конфигурацию. Откройте окно свойств шлюза, раздел «IPSec VPN», нажмите кнопку «Traditional mode configuration», установите флажок «Pre- Shared Secret»:  
  
  
  
11) Нажмите кнопку «Edit Secrets», введите сгенерированный ключ для другого члена пары шлюзов и нажмите «ОК»:  
  
  
  
12) Если у вас есть шлюзы, находящиеся под управлением других серверов управления, как в примере, повторите операцию добавления ключа на них;  
  
13) Теперь можно установить политики на шлюзы и проверить логи на предмет того, что VPN успешно собрался. В логах должны присутствовать сообщения об успешной установке Site Key или Site Certificate и инициализации криптобиблиотек и сообщения типов Encrypt/Decrypt для трафика, передаваемого через VPN соединение.  
  
14) Если политика установилась без ошибок и данные сообщения в логах присутствуют, то поздравляю вас, вам успешно удалось настроить VPN с использованием ГОСТового шифрования.

**P.S. Необходимо ли проводить контроль встраивания криптосредств?**

Вопрос «Необходимо ли проводить контроль встраивания криптосредств?» возникает при организации защиты персональных данных. Документ «Положение ПКЗ-2005» обязывает нас производить контроль встраивания криптосредств в случае использования криптосредств для защиты информации, если обязательность защиты обусловлена законодательством Российской Федерации. Однако, существует документ «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», где в разделе 5 приведены требования по контролю встраивания криптосредств при их использовании для защиты персональных данных. Исходя из требований, следует, что при правильно составленной модели угроз выполнять контроль встраивания криптосредств необязательно.