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”

Руководство администратора

Web-based интерфейс управления: инструкция по установке и использованию

РЛКЕ.00005-01 90 03

23.03.2015

Содержание

Web-based интерфейс управления: инструкция по установке и использованию

Настроить шлюз безопасности CSP VPN Gate можно удаленно, используя Web-based графический интерфейс управления (GUI). Графический интерфейс является опциональной частью Продукта CSP VPN Gate и выделен в отдельный пакет, и инсталляция GUI производится отдельно. Для получения опционального пакета

`cspvpngui-3.1-xxxxx.noarch.rpm` – для ОС RHEL5

`VPNgui` – для ОС Solaris 10

обратитесь в службу поддержки по адресу support@s-terra.com.

Инсталляция

Установка пакета осуществляется стандартным для ОС менеджером пакетов.

В процессе установки создается файл `/opt/VPNagent/etc/httpd-add.conf`, используемый для настройки файла конфигурации Web-server Apache:

```
ServerName %имя хоста%
DocumentRoot /opt/VPNagent/cspmc
<Directory /opt/VPNagent/cspmc>
  Options Indexes Includes
  AllowOverride All
  Allow from all
  AddCharset koi8-r .htm
  DirectoryIndex index.html index.htm
</Directory>
```

Если настройка Apache завершится с ошибкой, то самостоятельно настройте файл конфигурации Apache `/etc/httpd/conf/httpd.conf`.

Инсталляция GUI в ОС Red Hat Enterprise Linux 5

Разместите опциональный пакет Web-based GUI в каталоге `/opt` и установите его командой:

```
rpm –i cspvpngui-3.1-xxxxx.noarch.rpm
```

Во время инсталляции проверяется наличие файла конфигурации Web-server Apache `/etc/httpd/conf/httpd.conf`:

- если файл существует, то формируется файл `/opt/VPNagent/etc/httpd-add.conf` с дополнением к конфигурации Apache, и в файл конфигурации добавляется инструкция о включении файла с дополнением

- если файл конфигурации отсутствует, то выводится сообщение: `WARNING: Could not find http daemon configuration file.` В этом случае, перед запуском графического интерфейса управления, необходимо самостоятельно настроить файл конфигурации apache `/etc/httpd/conf/httpd.conf`.

Включается автоматический запуск Apache при перезагрузке. Выполняется перезапуск Web-server Apache.

Инсталляция GUI в ОС Solaris 10

Разместите опциональный пакет VPNgui в каталоге `/opt/vpngui` и установите его командой:

```
pkgadd -d /opt/vpngui VPNgui
```

Во время инсталляции GUI проверяется наличие установленых пакетов SUNWapchr, SUNWapchu и VPNgate<суффикс, обозначающий криптопровайдера>. Если какой-либо из этих пакетов не установлен, то инсталляция пакета VPNgui будет прервана с соответствующим сообщением:

```
Apache package SUNWapchr required by CSP VPN Gate web-based GUI.
Apache package SUNWapchu required by CSP VPN Gate web-based GUI.
CSP VPN Gate must be installed before installation of web-based GUI.
```

При инсталляции выполняется настройка Web-server Apache в файле `/etc/apache/httpd.conf`.

Если настройка Apache завершилась с ошибкой, то выдается сообщение: `WARNING: Apache web server was not reconfigured.`

В этом случае перед запуском GUI самостоятельно настройте файл конфигурации Web-server Apache.

Деинсталляция

Удаление пакета осуществляется стандартным для ОС менеджером пакетов.

Деинсталляция в ОС Red Hat Enterprise Linux 5

Для деинсталляции GUI выполните команду:

```
rpm -e cspvpngui-3.1-xxxxx
```

При деинсталляции:

- из файла конфигурации Web-server Apache `/etc/httpd/conf/httpd.conf` удаляется инструкция включения файла `/opt/VPNagent/etc/httpd-add.conf`
- удаляется файл `/opt/VPNagent/etc/httpd-add.conf`
- останавливается Web-server Apache
- выключается автоматический запуск Web-server Apache при перезагрузке.

Деинсталляция в ОС Solaris 10

Для деинсталляции GUI выполните команду:

```
pkgrm VPNgui
```

При деинсталляции:

- удаляется файл `/etc/apache/httpd.conf`
- если существует файл `/etc/apache/httpd.conf.orig`, то он копируется в `/etc/apache/httpd.conf` (восстанавливается начальная конфигурация Web-server Apache).

Начальная конфигурация шлюза для удаленного управления

После инсталляции CSP VPN Gate и GUI рекомендуется загрузить начальную конфигурацию, которая позволит в дальнейшем создать защищенный канал для удаленного конфигурирования политики безопасности. Создание начальной конфигурации описано в разделе «Построение VPN туннеля между шлюзом безопасности CSP VPN Gate 3.1 и рабочим местом администратора для удаленной настройки шлюза» документа «Настройка шлюза».

Старт графического интерфейса управления

Для старта графического интерфейса Продукта CSP VPN Gate запустите интернет-браузер, например Microsoft Internet Explorer. В поле для ввода URL укажите с префиксом `http://` IP-адрес или DNS компьютера, на котором установлен CSP VPN Gate.

После этого происходит проверка наличия на компьютере установленного Продукта J2SE Java(TM) Runtime Environment версии не ниже 5.0 Update 4. Если этот Продукт не установлен или установлена версия ниже, то появляется окно (Рисунок 1) с предложением инсталлировать последнюю версию JRE:

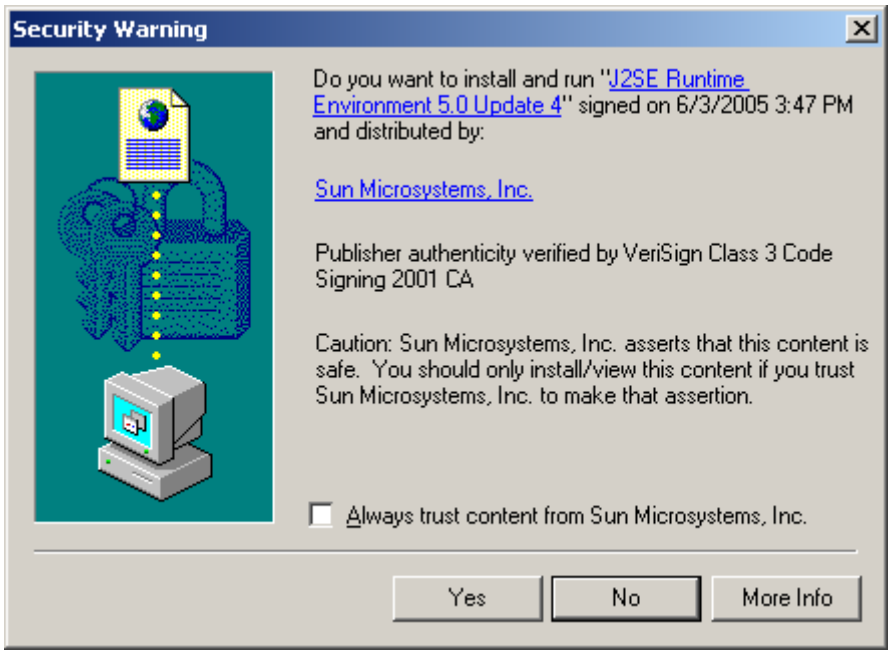

Рисунок 1

Если нажата кнопка Yes и с данного компьютера существует выход в интернет, то происходит загрузка страницы Web-site компании Sun Microsystems, Inc., с которой можно инсталлировать Продукт J2SE JRE последней версии.

Если выход в интернет отсутствует, то нужно установить JRE самостоятельно.

Замечание: если в качестве интернет-браузера используется Internet Explorer 7, то проверка наличия на компьютере установленного Продукта J2SE Java(TM) Runtime Environment не производится. В случае его отсутствия, установите этот продукт самостоятельно.

Во время загрузки Продукта появляются стандартные окна визарда для установки Продукта: Лицензионное соглашение, выбор типа установки (Typical), индикатор процесса инсталляции и перезагрузка системы.

После перезагрузки системы в окне браузера (Рисунок 2) появится заставка GUI for CSP VPN Gate 3.1 и текст, с предупреждением не закрывать это окно во время работы с Продуктом – `"Don't close this window until you logout CSP VPN Gate"`:

Рисунок 2

Примечание: повторный запуск Продукта из окна браузера, в котором уже появился графический интерфейс CSP VPN Gate, осуществлять нельзя. Нужно закрыть окно браузера и открыть его снова.

Одновременно будет запущен Java апплет, который откроет окно ввода имени пользователя и пароля (Рисунок 3). При установке Продукта создается специальный пользователь с именем `"cscons"` и паролем `"csp"`. После инсталляции рекомендовалось изменить этот пароль. В окне CSP VPN Login нужно ввести имя пользователя `"cscons"` и его новый пароль:

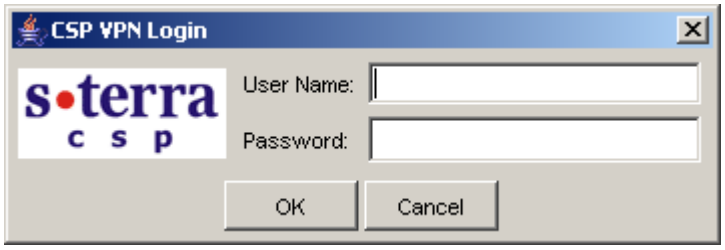

Рисунок 3

Если через некоторое время окно логина (Рисунок 3) не появляется, то нажмите на предложение Troubles and Solutions окна заставки CSP VPN Gate (Рисунок 2). В открывшемся окне (Рисунок 4) указаны возможные причины и пути устранения:

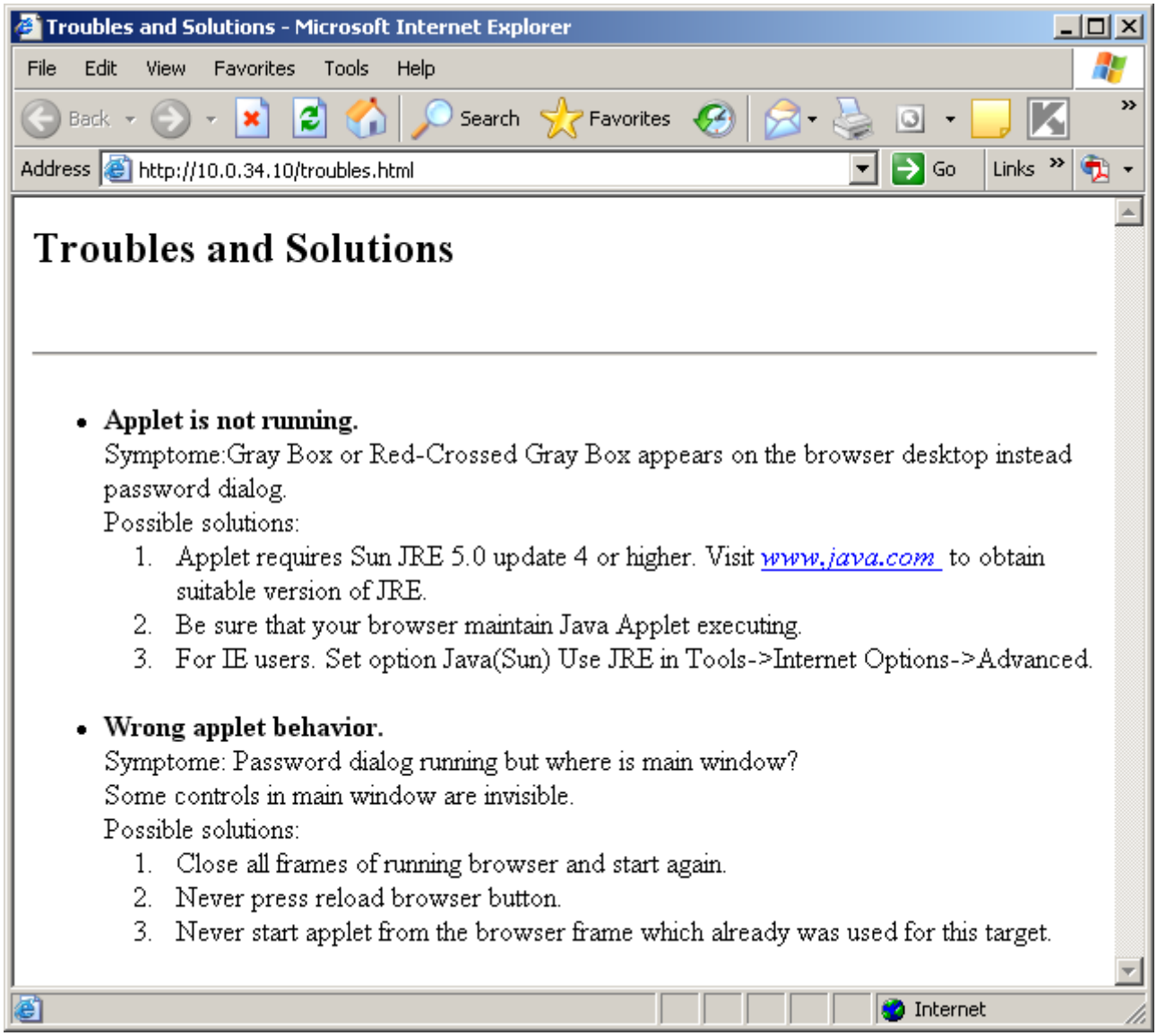

Рисунок 4

После ввода имени пользователя и пароля, и нажатия кнопки OK будет открыто окно (Рисунок 5), сообщающее о том, что Продукт CSP VPN Gate загружает конфигурацию со шлюза безопасности:

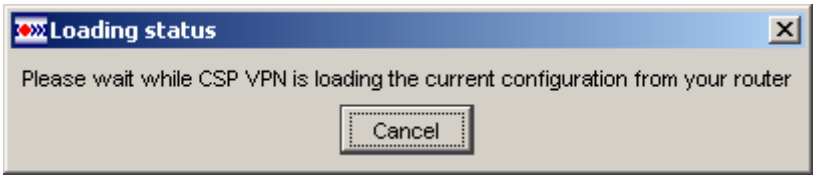

Рисунок 5

При нажатии кнопки Cancel загрузка конфигурации прерывается и выводится запрос на закрытие приложения. В случае утвердительного ответа приложение будет закрыто, при отрицательном ответе – загрузка конфигурации продолжится.

Главная форма

После успешной загрузки конфигурации открывается окно главной формы (Рисунок 6) на разделе Overview (Обзор).

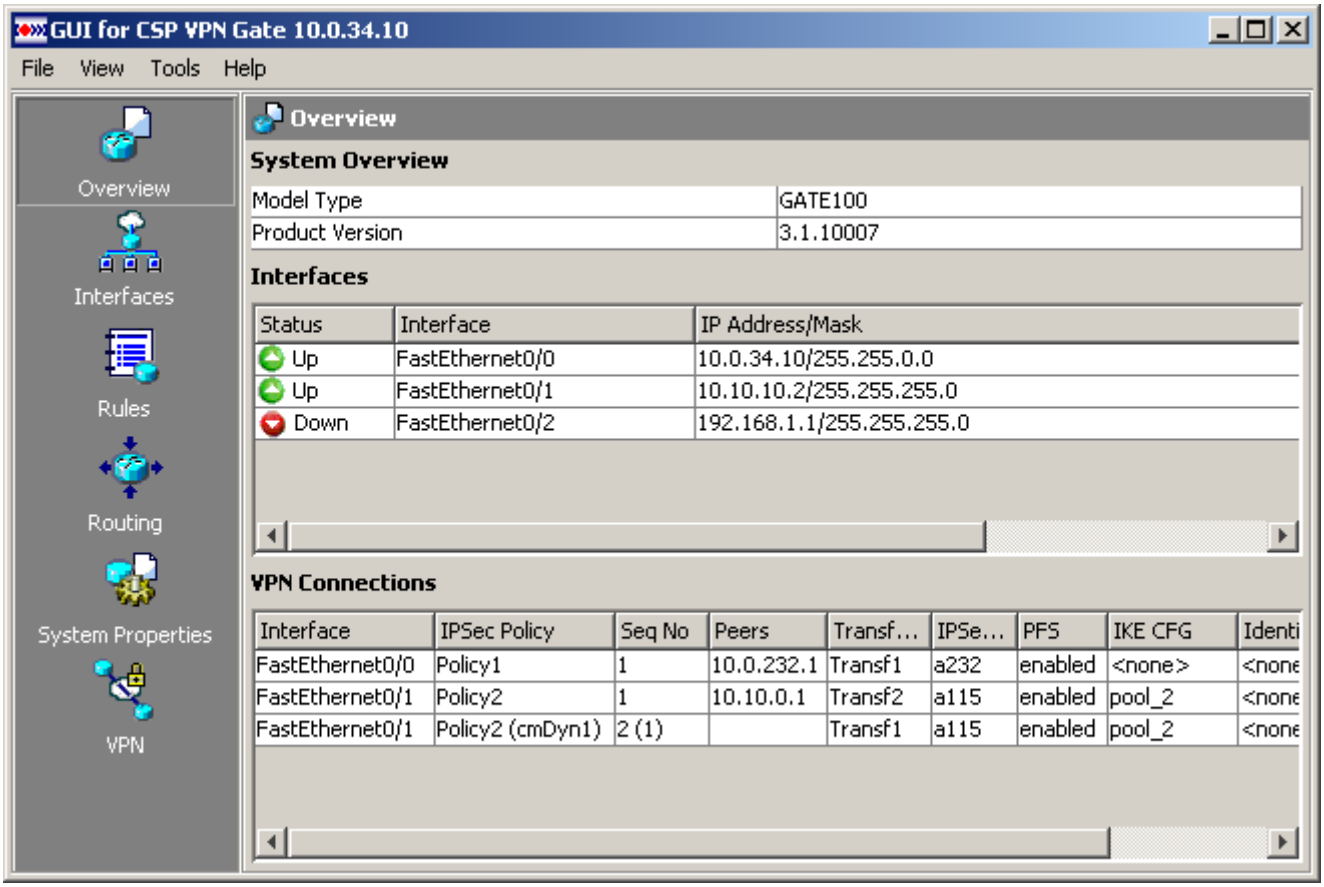

Рисунок 6

Главная форма содержит следующие элементы:

- Меню
- Панель инструментов
- Браузер.

Меню

Раздел File

- Backup Running Config to PC… – сохраняет на диск резервную копию действующей на шлюзе конфигурации. Открывает стандартный Save As диалог с предустановленным фильтром `*.txt`, после указания имени файла сохраняет в нем cisco-like конфигурацию.
- Backup Current Config to PC… – сохраняет на диск резервную копию текущей (отображаемой в GUI) конфигурации. Открывает стандартный Save As диалог с предустановленным фильтром `*.txt`, после указания имени файла сохраняет в нем cisco-like конфигурацию.

- Restore Current Config from PC… – восстанавливает (загружает) в GUI ранее сохраненную конфигурацию, созданную в GUI. Открывает стандартный диалог открытия файла с предустановленным фильтром `*.txt` и после выбора имени файла загружает cisco-like конфигурацию. При загрузке конфигурации из файла проверка содержащихся в ней команд не проводится, поэтому не рекомендуется загружать файлы, отредактированные вручную.
- Reload Running Config – запускает процедуру повторной загрузки действующей конфигурации со шлюза безопасности в GUI. Если никаких изменений в действующей конфигурации не производилось, то загрузка производится без предупреждений. Если было сделано хотя бы одно изменение, то будет открыто окно с предупреждением о необходимости сохранить сделанные изменения.
- Deliver to Router – открывает окно Deliver Configuration to Router для доставки конфигурации из GUI на шлюз безопасности.
- Don’t test config at delivering – проверка конфигурации перед ее доставкой на шлюз безопасности. Проверка производится в том случае, если флажок снят. По умолчанию тестирование запрещено.
- Exit – завершает сеанс работы с приложением. Если никаких изменений не производилось, то сеанс работы завершается без предупреждений. Если были произведены какие-либо изменения, то открывается окно с предупреждением, что все сделанные и не доставленные изменения в конфигурации будут утеряны.

Раздел View

- Overview – открывает одноименный раздел
- Interfaces – открывает одноименный раздел
- Rules – открывает одноименный раздел
- Routing – открывает одноименный раздел
- System – открывает одноименный раздел
- VPN – открывает одноименный раздел
- Running Config… – открывает окно Show Running Configuration с текстом действующей на шлюзе безопасности конфигурации
- Current Config… – открывает окно с текстом текущей (отображаемой в GUI) конфигурации.

Раздел Tools

- Ping – открывает окно Ping, из которого можно послать ping на заданный адрес.
- SA Manager – открывает окно SA Manager, в котором отображается статус существующих на шлюзе безопасности SA (Security Association).
- Adjust Timeout – открывает окно "Adjust Timeout", в котором устанавливается таймаут – время ожидания ответа при доставке конфигурации на агента. Отсутствие отклика в течение этого времени нужно рассматривать как неудачную доставку.

Раздел Help

- Help Topics – открывает файл помощи. Для появления окон помощи в браузере нужно выполнить следующую настройку – снять блокировку на всплывающие окна. Например, в Internet Explorer, это осуществляется следующим образом – Tools – Internet Options…– вкладка Privacy – снять флажок Block pop-ups.
- About GUI for CSP VPN Gate – открывает окно с названием Продукта, версии Продукта, номера сборки, копирайт и логотипа компании.

Панель инструментов

В панели инструментов расположены кнопки, которые дублируют соответствующие команды меню View и открывают одноименные разделы графического интерфейса.

Браузер

В браузере обычно располагаются таблицы. Поведение таблиц в главной форме:

- двойной клик на строке таблицы вызывает окно редактирования параметров этой строки, если подобная операция предусмотрена. Если же выделенная строка не подлежит редактированию, то никаких действий по двойному клику не производится
- клик на заголовке столбца осуществляет сортировку строк. При сортировке строк учитываются только значения в этом столбце. Сортировка имеет три этапа:
  - первый клик производит прямую сортировку (A-Z)
  - второй клик производит обратную сортировку
  - третий клик возвращает строки в положение, предшествующее сортировке
- выделять можно только одну строку, выделение нескольких строк в таблице не поддерживается
- операция drag&drop (перетащить и оставить) в таблицах не поддерживается.

Описанное поведение относится не только к таблицам главной формы, но и ко всем таблицам во вспомогательных окнах графического интерфейса.

Поведение деревьев в главной форме:

- поддерживаются операции по сворачиванию и раскрытию узлов дерева
- поддерживается память на состояние дерева (свернутые и раскрытые узлы) в рамках одной сессии редактирования
- после загрузки конфигурации все узлы деревьев раскрыты
- выделение нескольких узлов не поддерживается
- в дереве не поддерживается drag&drop.

Overview

Старт Продукта завершается открытием главной формы на разделе Overview (Обзор) (Рисунок 7).

В этом разделе можно посмотреть версию установленного Продукта CSP VPN Gate, зарегистрированные физические интерфейсы, их IP-адреса и созданные VPN соединения.

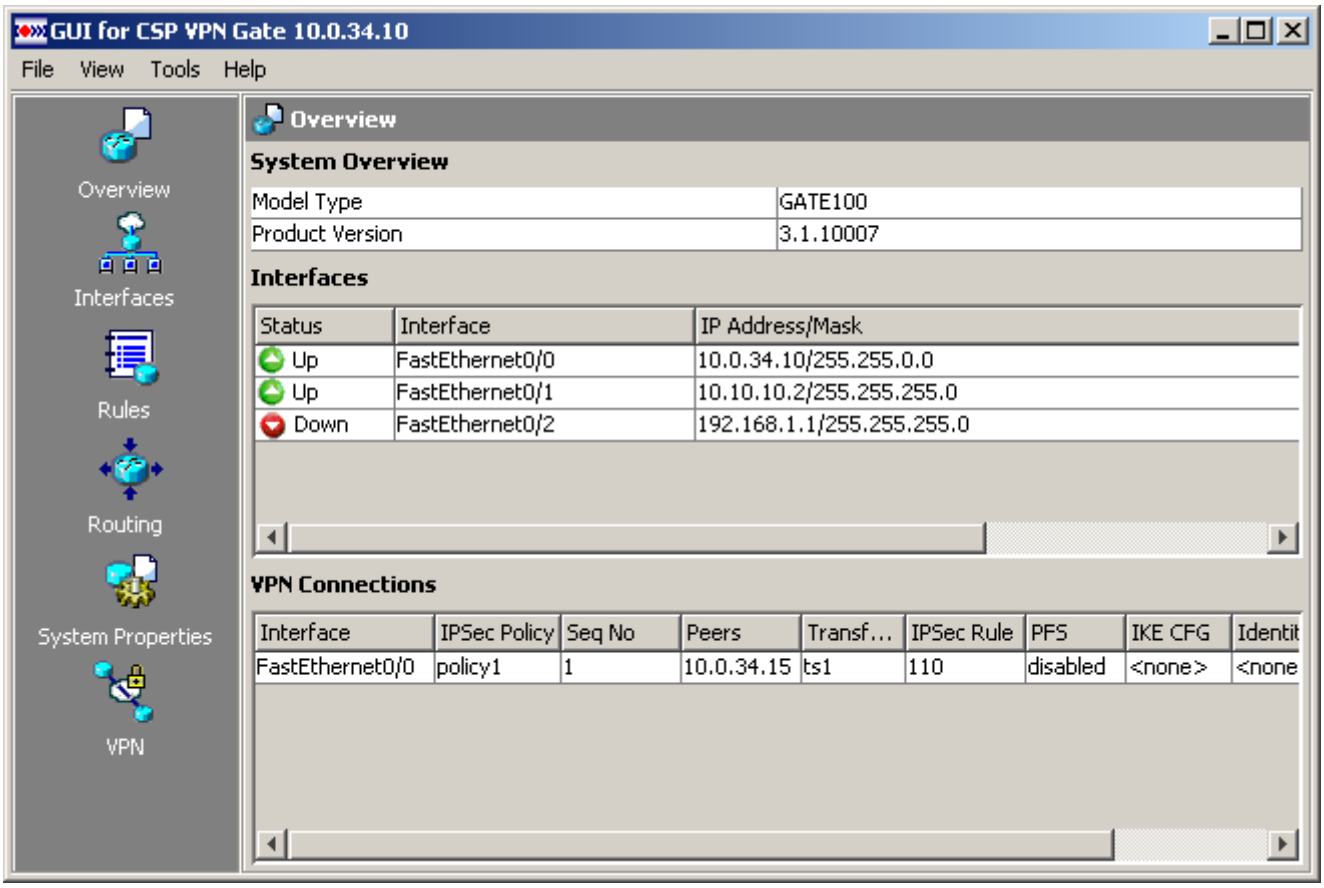

Рисунок 7

Браузер раздела Overview состоит из трех таблиц:

- System Overview – таблица со следующими параметрами Gate:
  - Model Type – тип программного обеспечения (Gate 100/Gate 100B/Gate 1000/Gate 3000/Gate 7000).
  - Product Version – версия программного обеспечения CSP VPN Gate
- Interfaces – таблица с параметрами зарегистрированных физических интерфейсов. Состав столбцов таблицы:
  - Status – статус интерфейса: Up – интерфейс включен, Down – выключен
  - Interface – имя интерфейса
  - IP Address/Mask – IP-адрес и маска интерфейса.
- VPN Connections – таблица со списком созданных VPN соединений. Состав столбцов таблицы такой же, как и в разделе VPN:
  - Interface – имя сетевого интерфейса

- IPSec Policy – имя политики IPsec
- Seq No. (Sequence Number) – порядковый номер криптографической карты в данной политике IPsec. Дальнейшие параметры относятся к конкретной криптографической карте
- Peers – список партнеров, описанных в криптографической карте
- Transform Sets – список наборов преобразований, установленных для криптографической карты
- IPSec Rule – номер или имя правила IPsec, привязанного к криптографической карте
- PFS – опция, включение которой усиливает защиту ключей
- IKE CFG Pool – имя пула адресов, используемого криптографической картой
- Identities – имя списка идентификаторов.

Interfaces

Физические интерфейсы не создаются, а считываются из конфигурации устройства. В разделе Interfaces (Рисунок 8) отображаются все сетевые интерфейсы, на которые установлен драйвер Продукта. Правила доступа, привязанные к интерфейсам, предназначены для фильтрации трафика, а политики IPsec, связанные с интерфейсами, задают параметры построения защищенного соединения.

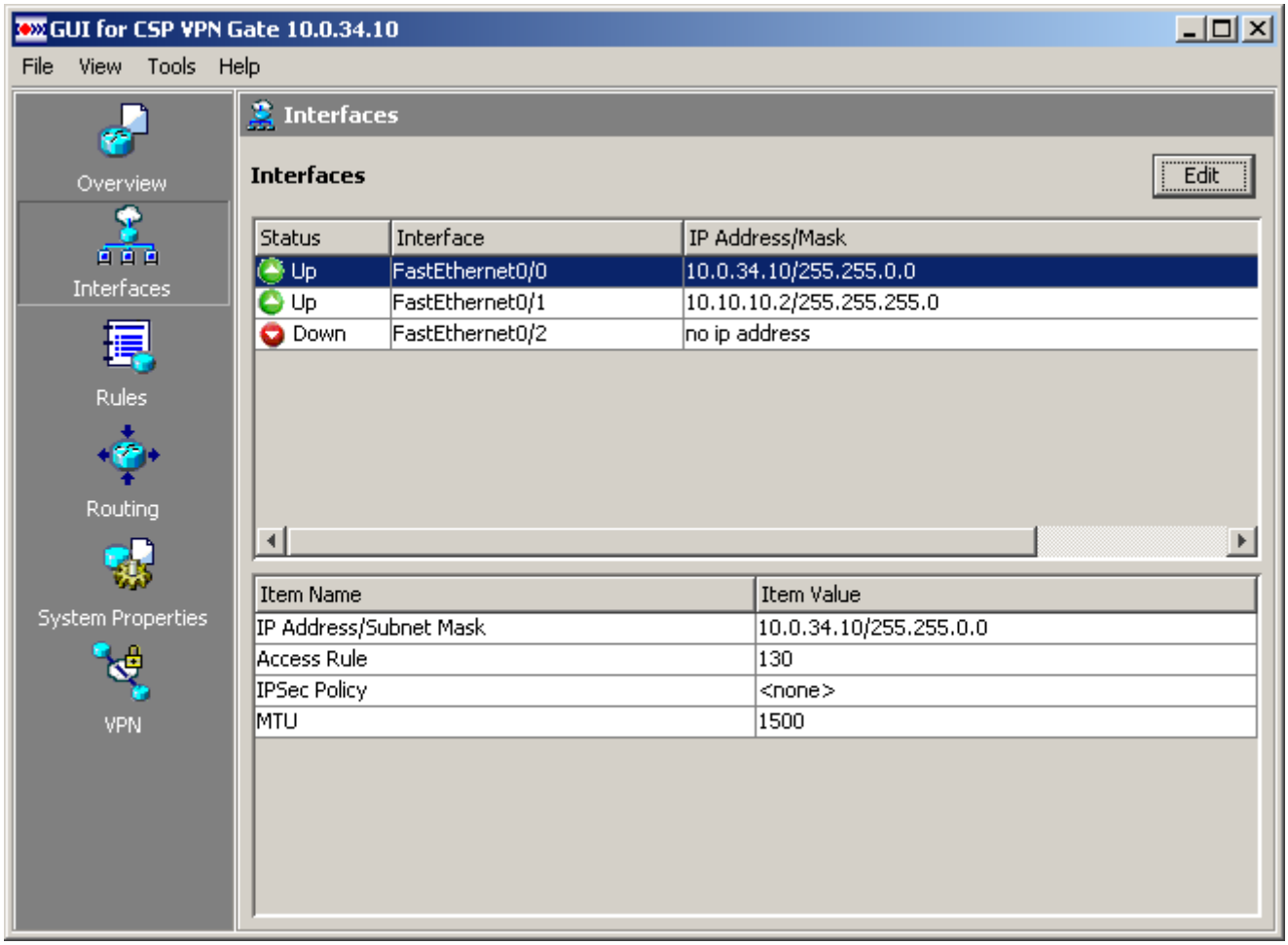

Рисунок 8

Состав элементов браузера раздела Interfaces:

- Кнопки управления:
  - Edit – кнопка вызова окна редактирования связи выделенного интерфейса с правилом доступа и политикой IPsec. Если в таблице не выделена ни одна строка – кнопка Edit блокируется.
- Таблица Interfaces состоит из столбцов:
  - Status – статус интерфейса: Up – интерфейс включен, Down – выключен
  - Interface – имя интерфейса
  - IP Address/Mask – IP-адрес и маска подсети физического интерфейса. В случае, когда адрес отсутствует, в столбце отображается значение "no ip address".

- Нижняя таблица содержит параметры выделенного в верхней таблице интерфейса и состоит из двух столбцов:
  - Item Name. Этот столбец содержит параметры интерфейсов:
    - IP Address/Subnet Mask – IP-адрес/Маска подсети выделенного интерфейса
    - IP Address/Subnet Mask (Secondary) – в зависимости от количества IP-адресов на интерфейсе этот параметр может либо отсутствовать (когда у интерфейса только один IP-адрес), либо строк с этим параметром может быть несколько
    - Access Rule – правило доступа, привязанное к данному интерфейсу
    - IPSec Policy – политика IPsec, связанная с данным интерфейсом
    - MTU – максимальный размер пакета, передаваемый без фрагментации через интерфейс.
  - Item Value – столбец со значениями описанных параметров интерфейса, т.е. IP-адреса, приписанные данному интерфейсу, правила доступа и политики IPsec, связанные с данным интерфейсом. Если правила не установлены, то столбец будет содержать значение <none>.

Редактирование параметров физического интерфейса

Редактирование параметров выделенного физического интерфейса производится в окне Interface Feature Edit Dialog (Рисунок 9), которое вызывается кнопкой Edit.

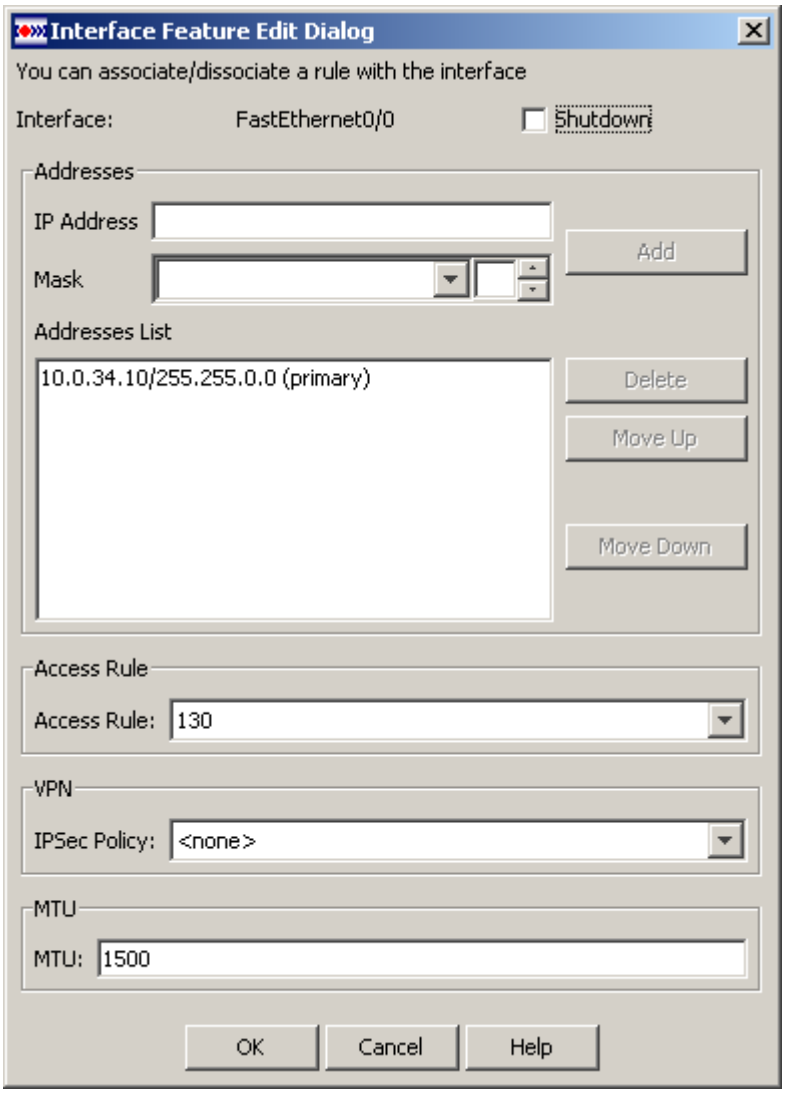

Рисунок 9

Состав элементов окна редактирования:

- Interface – имя редактируемого интерфейса
- Shutdown – флажок, управляющий состоянием интерфейса. Установленный флажок соответствует выключенному состоянию.
  Если состояние интерфейса «включен», но при этом у него нет ни одного назначенного адреса, то при нажатии кнопки OK будет выдан запрос «Interface will be shut down, because there is no any addresses assigned. Do you wish to continue?». В случае утвердительного ответа интерфейс будет выключен, и изменения будут приняты.
- Группа Addresses предназначена для управления IP-адресами, назначенными на интерфейс.
  - IP Address – IP-адрес
  - Mask – маска

- Addresses List – список адресов назначенных на интерфейс. Первый адрес в списке назначается в качестве primary (на это явно указывает соответствующая пометка), остальные как secondary. В случае отсутствия адресов в списке отображаеся текст «no ip address»
- Add – при нажатии на кнопку происходит добавление новой пары IP-адрес/маска в Addresses List, при этом добавление осуществляется в конец списка. Кнопка активна только когда в полях «IP Address» и «Mask» содержатся корректные значения. При попытке добавления уже назначенного на этот интерфейс адреса будет выдано предупреждение «This IP address/Mask pair alredy assigned to this interface» и адрес не будет добавлен. После успешного добавления поля «IP Address» и «Mask» очищаются
- Delete – кнопка предназначена для удаления выделенного адреса с интерфейса
- Move Up – управляет порядком адресов на интерфейсе, сдвигает выделенный адрес на одну позицию вверх
- Move Down – управляет порядком адресов на интерфейсе, сдвигает выделенный адрес на одну позицию вниз.

- Группа Access Rule – позволяет задать или выбрать правило доступа для привязки к данному интерфейсу. Правило предназначено для фильтрации входящего трафика. Поле выбора правила доступа содержит выпадающий список значений:
  - <none> – к интерфейсу правило доступа не привязано
  - Use Rule Pane for selection – при выборе этого предложения будет открыто окно Rule Pane (Рисунок 10) для выбора правила
  - Create new – открывает диалог создания правила доступа Add a Rule (Рисунок 14). В этом окне поле Associate with an Interface будет блокировано, так как создана связь с текущим интерфейсом. После создания правила и нажатия кнопки OK, имя или номер правила будут отображаться в поле выбора Access Rule, а правило доступа заносится в список Access Rules (Рисунок 13).
- Группа VPN – позволяет создать или выбрать политику IPsec для данного интерфейса. Политика IPsec задает параметры построения VPN туннеля между данным интерфейсом и интерфейсом с IP-адресом партнера. Поле выбора политики IPsec содержит выпадающий список значений:
  - <none> – политика IPsec не выбрана
  - Use IPSec Policy Pane for selection– при выборе этого значения будет открыто окно IPSec Policy Pane (Рисунок 11) для выбора политики IPsec
  - Create new – открывает диалог Add IPSec Policy (Рисунок 44) создания новой IPsec Policy. Создание новой политики IPsec описано в разделе "Создание IPsec Policy". Созданная политика IPsec заносится в список IPSec Policy.
- Группа MTU
  - MTU – максимальный размер пакета, передаваемого без фрагментации через интерфейс. Допустимые значения находятся в диапазоне 68–65535.

Окно выбора правила доступа

Окно выбора правила доступа Rule Pane (Рисунок 10) имеет следующие элементы:

- Rule Category – поле с выпадающим списком категорий правил – Access Rules и IPSec Rules. Правило может быть выбрано из любой категории и как стандартное, так и расширенное правило.
- Таблица со списком всех созданных правил доступа:
  - Name/Number – имя или номер правила доступа

- Used by – имя интерфейса, к которому привязано правило, или имя криптографической карты, которая ссылается на это правило. Статическая криптографическая карта идентифицируется по совокупности имени IPsec Policy и Sequence Number, а динамическая криптокарта – по имени набора динамических криптокарт (Dynamic Crypto Map Set) и Sequence Number. Для отображения интерфейса используется только имя интерфейса, а для статической криптокарты – префикс crypto map, имя IPsec Policy и Sequence Number, для динамической криптокарты – префикс dynamic crypto map, имя Dynamic Crypto Map Set и Sequence Number. В качестве разделителя используется запятая
- Type – тип правила.

- Уточняющая таблица со списком записей выделенного правила. Состав таблицы описан в разделе Access Rules.

При выделении правила в верхней таблице и нажатии кнопки Select – правило будет выбрано.

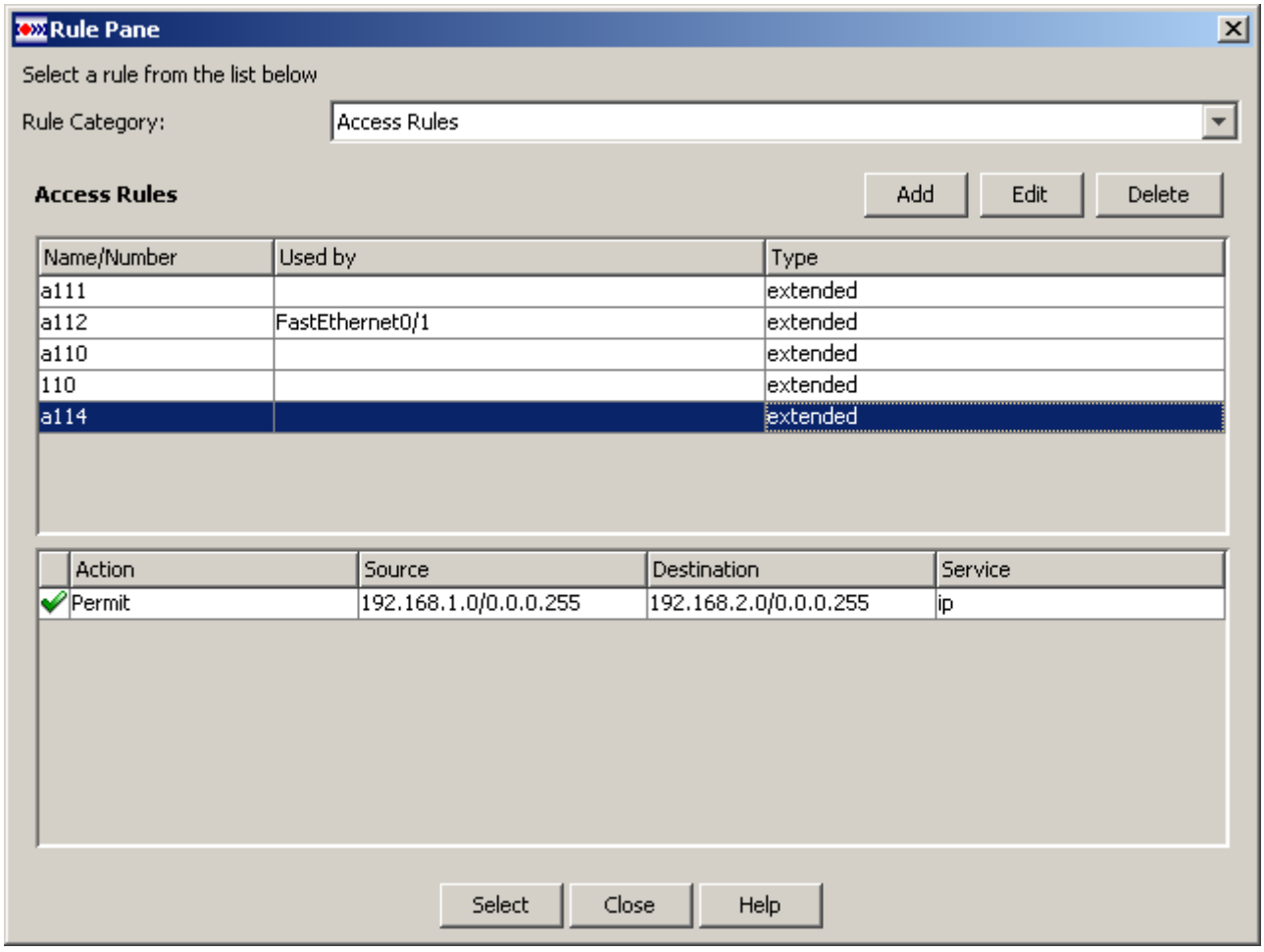

Рисунок 10

Окно выбора политики IPsec

В окне IPSec Policy Pane производится выбор политики IPsec.

Верхняя таблица содержит все созданные политики IPsec и имеет два столбца:

- Name – имя политики IPsec
- Interfaces – имена интерфейсов и криптографических карт, связанных с данной политикой IPsec

- Таблицы Crypto Maps и Dynamic Crypto Map Sets отображают детали криптографических карт, входящих в выделенную политику IPsec.

При выделении IPsec Policy в верхней таблице и нажатии кнопки Select – политика будет выбрана.

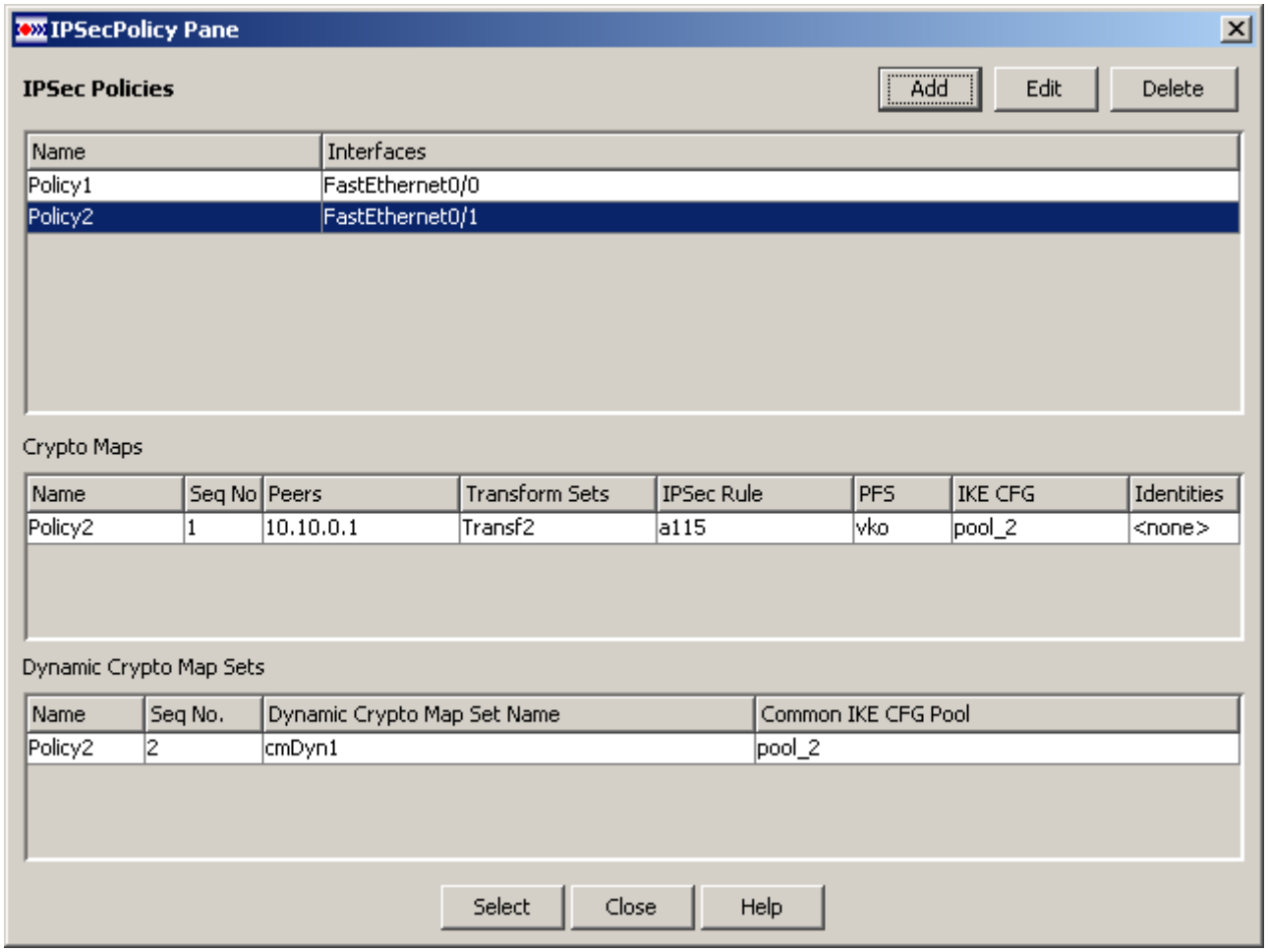

Рисунок 11

Rules

В разделе Rules создаются и редактируются правила доступа, которые привязываются к сетевым интерфейсам для пакетной фильтрации трафика и правила IPsec, которые привязываются к криптографическим картам для защиты трафика.

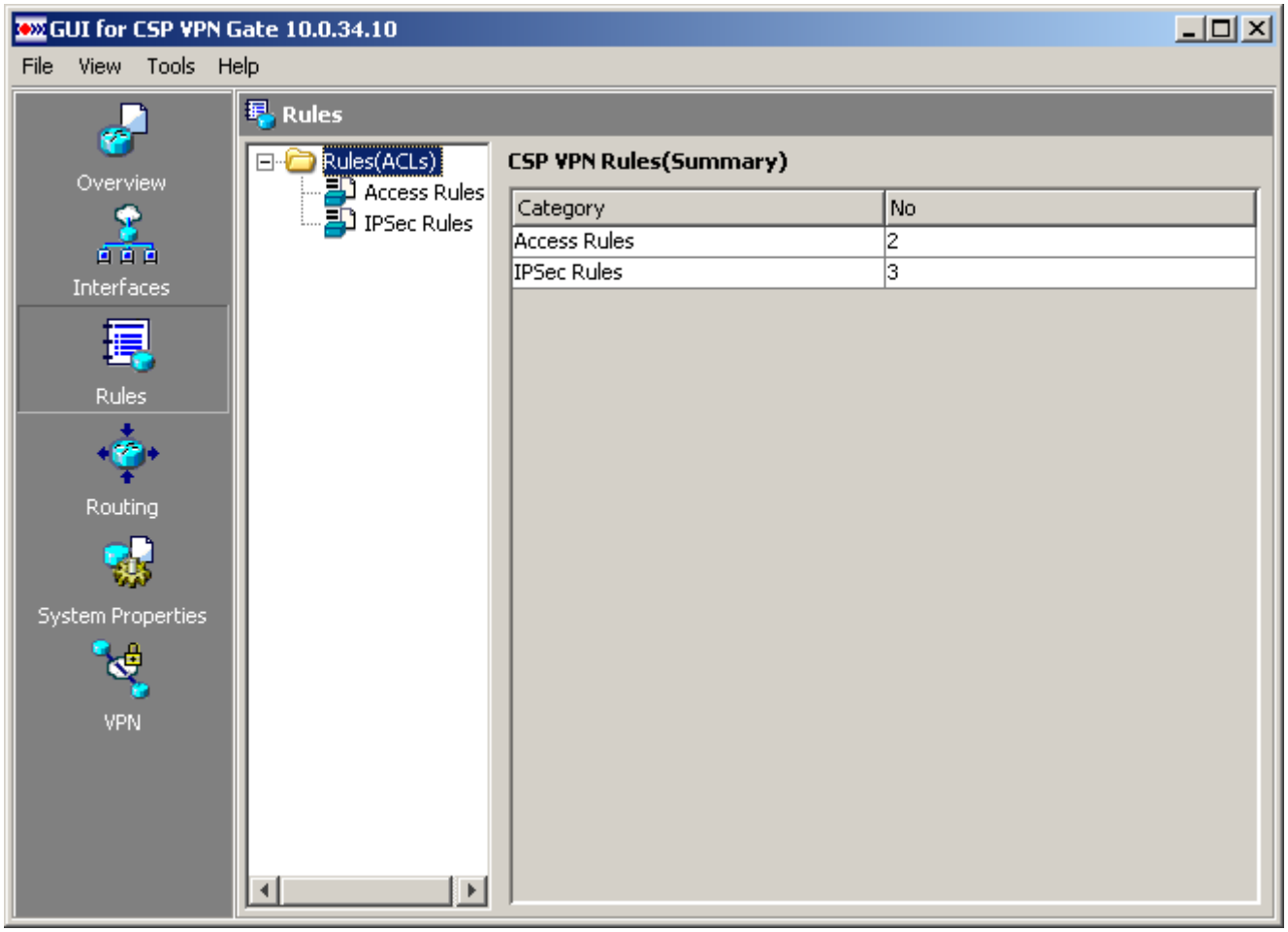

Рисунок 12

Корневой элемент Rules имеет два раздела:

- Access Rules (Правила доступа) – в этом разделе размещаются стандартные и расширенные правила доступа, которые предназначены для связи с интерфейсами для осуществления пакетной фильтрации трафика
- IPSec Rules (Правила IPsec) – в этом разделе размещаются только расширенные правила IPsec, которые предназначены для связи с криптографическими картами (Crypto Maps – криптографические карты) для защиты трафика.

При установке селектора на корневом элементе таблица детализации справа отображает статистику по каждому разделу. Таблица состоит из двух столбцов:

- Category – содержит названия правил
- No. – показывает количество правил в каждом разделе.

Логика размещения правил в Access Rules и IPsec Rules

В политике, которая загружается в CSP VPN Gate, правила Access Rule и IPsec Rule описываются абсолютно одинаковыми структурами. Создавая новое правило, пользователь обычно предполагает, будет оно привязано к интерфейсу или к криптографической карте. Поэтому, новое правило он сразу создает в соответствующем разделе:

- в разделе Access Rules отображаются правила, которые привязываются к интерфейсам
- в разделе IPSec Rules отображаются правила, которые привязываются к криптографической карте.

Использование одного и того же правила, для связи и с интерфейсом и с криптографической картой – экзотическая ситуация, но, тем не менее, это не запрещено. Существует ограничение:

- Standard Rule (Стандартное правило) – не может быть привязано к криптографической карте, следовательно, Standard Rule может отображаться только в Access Rules, и новое Standard Rule может быть создано только в разделе Access Rules.

Если правило привязано и к интерфейсу и к криптографической карте, то оно отображается в двух разделах. Заметим сразу, что это одно и то же правило, т.е. после редактирования его параметров в одном из разделов, произойдут те же изменения, если открыть правило в другом разделе.

При импорте текущей конфигурации правила распределяются по разделам по следующему алгоритму:

- Все Standard Rules отображаются в разделе Access Rules
- Если правило привязано к криптографической карте, оно обязательно отображается в IPSec Rules
- Если правило привязано к интерфейсу, оно обязательно отображается в Access Rules
- Если правило не привязано ни к интерфейсу, ни к криптографической карте, оно отображается в Access Rules. Из последнего следует, что если создать правила в разделе IPSec Rules, не привязать их к криптографической карте, и загрузить политику в CSP VPN Gate, то после импорта политики все эти правила окажутся в Access Rules. Но после привязки этих правил к криптографической карте и последующей загрузки-импорта, правила окажутся в разделе IPSec Rules, как изначально и планировалось.

Если правило, которое отображается в разделе Access Rules, привязывается к криптографической карте, или правило, которое отображается в IPSec Rules, привязывается к интерфейсу, то такое правило отображается в двух разделах.

Если правило было создано в разделе Access Rules, либо попало в этот раздел после импорта, оно отображается в этом разделе до следующего импорта конфигурации, либо до удаления этого правила. Если такое правило было привязано к криптографической карте, и стало отображаться в двух разделах, а в дальнейшем было отвязано от всех криптографических карт, то оно в итоге будет отображаться только в Access Rules.

Если правило было создано в разделе IPSec Rules, либо попало в этот раздел после импорта, оно отображается в этом разделе до следующего импорта конфигурации, либо до удаления этого правила. Если такое правило было привязано к интерфейсам, и стало отображаться в двух разделах, а в дальнейшем было отвязано от всех интерфейсов, то оно в итоге будет отображаться только в IPSec Rules.

Еще одна особенность – отображение Action (действие). Для одного и того же правила, отображающегося в двух разделах, будет следующее соответствие. Если в разделе Access Rules для некоторой записи задано действие Permit, то в разделе IPSec Rules для этой записи будет задано действие Protect the traffic, если же в Access Rules задано Deny, то в IPSec Rules будет Do not protect.

Access Rules

Правила доступа предназначены для фильтрации пакетов по разным признакам (Рисунок 13).

Пакеты можно фильтровать только по адресу отправителя либо по адресу отправителя пакета, адресу получателя пакета, типу протокола, порту отправителя и порту получателя.

Производится фильтрация только входящего трафика и все правила, создаваемые в разделе Access Rules, следует понимать только в этом смысле.

Правило доступа — это упорядоченный набор записей, каждая из которых разрешает или запрещает прохождение пакета через интерфейс в зависимости от информации, содержащейся в пакете. Записи правила доступа применяются к каждому пакету последовательно, начиная с первого, до тех пор, пока не будет найдена запись, параметры которой будут совпадать с параметрами заголовка пакета. И к пакету будет применяться то действие, которое предписано в этой записи. (В этом случае говорят, что пакет подпадает под правило.) При нахождении такой записи следующие записи в правиле уже не проверяются. Если такой записи не найдено – пакет уничтожается.

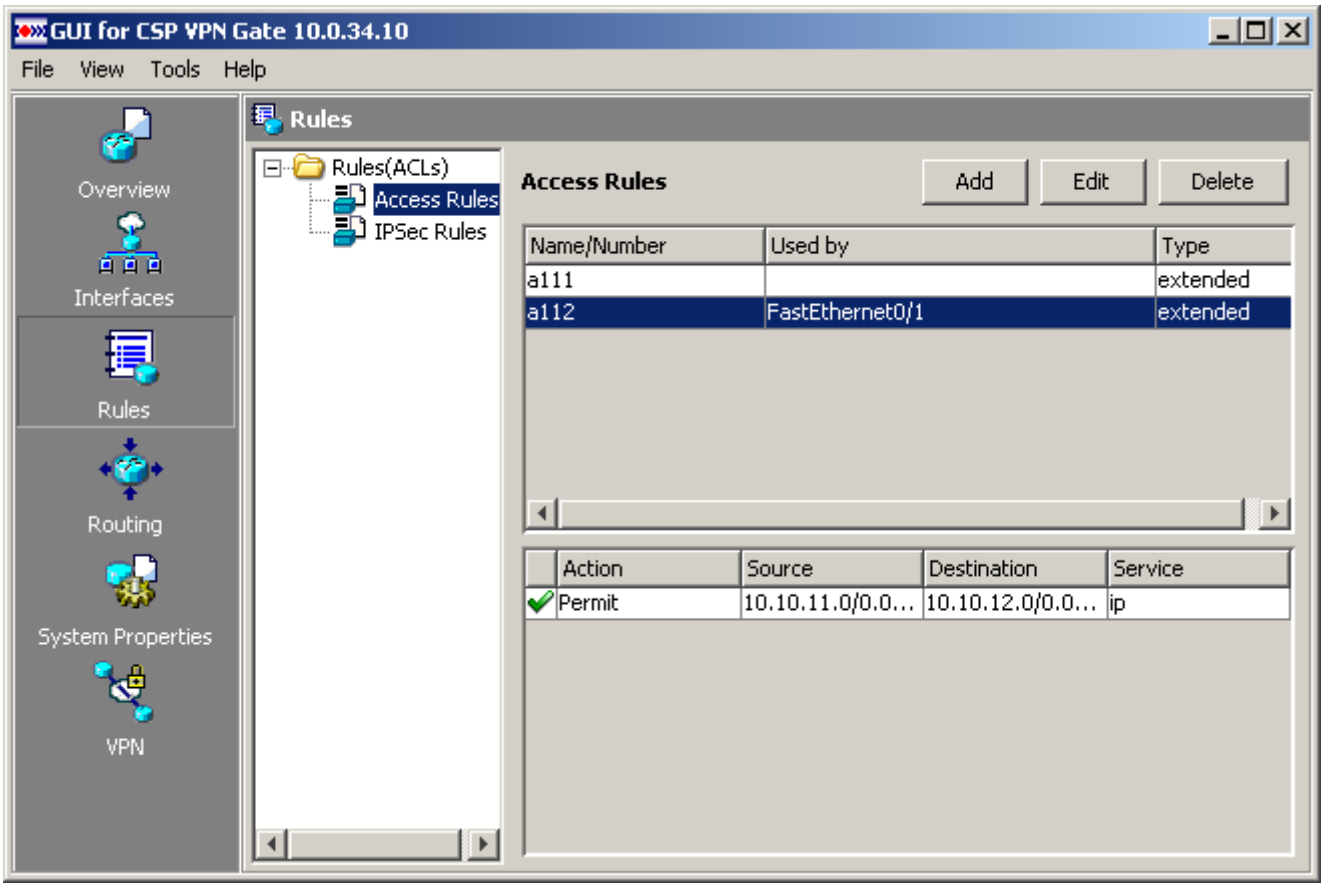

Рисунок 13

- Три кнопки управления:
  - Add – кнопка вызова окна для создания нового правила доступа
  - Edit – кнопка вызова окна для редактирования выделенного правила доступа
  - Delete – кнопка удаления выделенного правила доступа
- В верхней таблице размещаются правила доступа. В ней можно выделять только одну строку. Состав столбцов таблицы:
  - Name/Number – имя или номер правила доступа

- Used by – имена интерфейсов и политик IPsec, к которым привязано правило доступа
- Type – тип правила доступа (standard/extended – стандартное/расширенное)

- В нижней таблице детализируется содержание выделенного правила доступа. В зависимости от типа выделенного правила доступа состав столбцов таблицы будет разным. Для правила доступа типа Extended состав столбцов таблицы будет следующий:
  - столбец без названия, в котором содержится иконка, соответствующая типу выбранного действия ("галочка" – Permit (Пропускать), "крестик" – Deny (Не пропускать))
  - Action – действие, которое будет применяться к пакету (Permit/Deny) в случае подпадания его под правило
  - Source – IP-адрес отправителя пакета. Возможно значение any
  - Destination – IP-адрес получателя пакета. Возможно значение any
  - Service – сетевой сервис

Информация в столбце Service выводится в соответствии со следующей логикой:

- Если в качестве сетевого сервиса установлен протокол IP или протоколы семейства IP (которые установлены выбором из списка предопределенных протоколов в окне на Рисунок 19), то в столбце Service должно отображаться только имя протокола.
  Пример:
  Permit – 192.0.2.2 – any – ip
- Если в рамках протоколов TCP или UDP установлены порты, отличные от Any, то структура строки формируется следующим образом:
  <Protocol Name>, src: <Port Name | Port Number>, dst: <Port Name | Port Number>
  Если в качестве значения порта введено численное значение, которому соответствует имя порта в списке предопределенных портов, то численное значение будет заменено на имя порта. Замена производится после нажатия кнопки ОК в окне редактирования. При открытии следующей сессии редактирования, в соответствующем поле окна будет отображаться не численное значение, а соответствующее ему имя.
  Если у источника или получателя значение порта установлено равным Any, то такой блок данных не показывается.
  Пример, в котором у порта получателя установлено значение Any:
  Permit – 192.0.2.2 – any – udp, src: 124
  Пример, в котором значение Any установлено у источника:
  Permit – 192.0.2.2 – any – udp, dst: ntp
- Если в качестве значений портов используются диапазоны, то они отображаются в скобках с дефисом в качестве разделителя.
  Пример:
  Permit – 192.0.2.2 – any – udp, src: (123-345)

  При выводе значений диапазонов используются только численные значения даже в случаях, когда численному значению можно поставить в соответствие имя из списка предопределенных портов.

Состав столбцов таблицы для правила доступа типа Standard:

- столбец без названия с иконками возможных действий
- Action – действие, которое будет применяться к пакету
- Source – имя или IP-адрес отправителя пакета. Возможно значение any.

Создание нового правила доступа

Создание нового правила доступа осуществляется в окне Add a Rule (Рисунок 14), которое вызывается кнопкой Add в окне Rules.

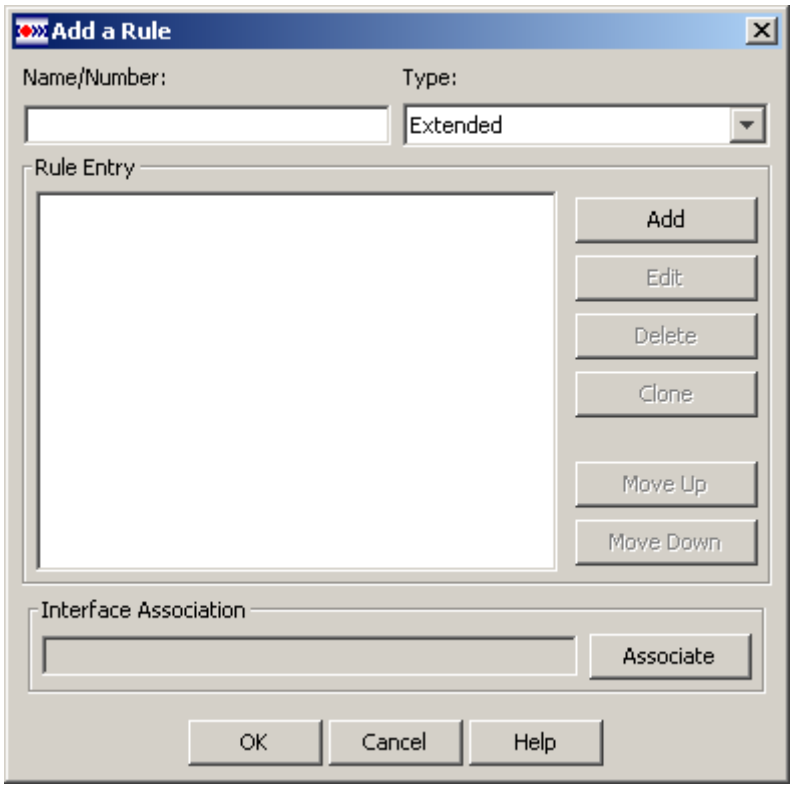

Рисунок 14

Окно содержит следующие элементы:

- Name/Number – поле ввода имени или номера правила, которые должны удовлетворять следующим условиям:
  - номера для стандартных правил должны лежать в диапазонах от 1 до 99 и от 1300 до 1999
  - номера для расширенных правил должны лежать в диапазонах от 100 до 199 и от 2000 до 2699
  - имя или номер создаваемого (редактируемого) правила должны быть уникальными
  - в имени должны использоваться только латинские буквы, цифры и символы !"#$%&'()*+,-./;:<=>@[\]^_`{|}~? и не допускаются пробелы
  - название правила обязательно должно начинаться с буквы.
- Type – тип правила – Standard Rule или Extended Rule.
  Стандартные правила используются тогда, когда нужно фильтровать пакеты только по адресу отправителя пакета.
  Расширенные правила используются для более гибкой фильтрации пакетов - по адресу отправителя пакета, адресу получателя пакета, по типу протокола, порту отправителя пакета и порту получателя.
  Выбор типа правила определяет окно, которое будет открыто по нажатию кнопки Add для создания записи. После того как в Rule Entry (список записей в правиле) будет помещена первая запись, элемент Type блокируется. Если список записей очистить, то элемент Type будет разблокирован. Логика основана на том, что правило не может содержать разнородных записей.

- Rule Entry – список записей в данном правиле. Записи в списке нужно расположить в порядке убывания приоритета
- Interface Association – группа, в которой производится связывание создаваемого правила с сетевым интерфейсом. Группа состоит из блокированного поля ввода и кнопки Associate.
- Кнопки управления:
  - Add – кнопка вызова окна для создания новой записи в правиле
  - Clone – кнопка вызова окна для создания новой записи на базе существующей выделенной записи
  - Edit – кнопка вызова окна для редактирования выделенной записи
  - Delete – кнопка удаления выделенной записи
  - Move Up – кнопка перемещения выделенной записи правила на одну позицию вверх для увеличения приоритета
  - Move Down – кнопка перемещения выделенной записи на одну позицию вниз для снижения приоритета
  - Associate – кнопка, вызывающая окно для связывания правила с интерфейсом
  - OK – кнопка закрытия окна с сохранением сделанных изменений
  - Cancel – кнопка закрытия окна без сохранения сделанных изменений.

Разрешается создавать "пустые" правила, которые имеют только номер/имя и тип правила, но не содержат записей.

Создание записи в стандартном правиле

Для создания записи в стандартном правиле используется окно Add a Standard Rule Entry (Рисунок 15), которое вызывается кнопкой Add в окне Add a Rule.

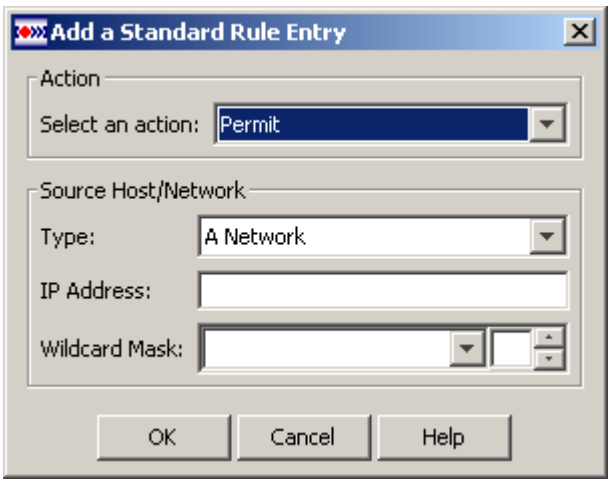

Рисунок 15

Это окно содержит следующие элементы:

- Action – действие, которое будет применяться к пакету, если он подпадает под правило. Содержит выпадающий список с двумя возможными действиями – Permit (пропускать пакет) и Deny (не пропускать пакет). По умолчанию установлено значение Permit.

- Source Host/Network – так как производится фильтрация только входящего трафика, в этой группе указывается IP-адрес или диапазон IP-адресов отправителя пакетов, приходящих извне на интерфейс, к которому должно быть привязано правило.
  - Type – тип отправителя
    - A Network – подсеть
    - A Host – хост
    - Any IP Address – любой IP-адрес. Значение по умолчанию.
  - IP Address – IP-адрес отправителя пакетов
  - Wildcard Mask используется в правилах доступа и правилах IPsec для того, чтобы определить соответствует ли пакет какой-либо записи в правиле.
    Wildcard Mask – это шаблон маски, который указывает какая часть IP-адреса пакета должна совпадать с IP-адресом в записи правила. Wildcard Mask содержит 32 бита, такое же количество бит и в IP-адресе.

    Если в шаблоне маски какой-либо бит равен 0, то тот же самый бит в IP-адресе пакета должен точно совпадать по значению с тем же битом в IP-адресе записи правила.

    Если в шаблоне маски какой-либо бит равен 1, то соответствующий бит в IP-адресе пакета проверять не нужно, он может принимать значение либо 0, либо 1, т.е. он является несущественным битом.

    Например, если Wildcard Mask равна 0.0.0.0, то все значения битов в IP-адресе пакета должны точно совпадать с соответствующими битами в IP-адресе записи правила. При Wilcard Mask равной 0.0.255.255 значения первых 16 битов в IP-адресе пакета должны точно совпадать со значениями этих же битов в IP-адресе записи правила.

    Важно, чтобы в Wildcard Mask в двоичном представлении не чередовались 0 и 1. Например, можно использовать шаблон 0.0.31.255, который можно записать в двоичном представлении как 00000000.00000000.00011111.11111111 и нельзя использовать шаблон 0.0.255.0 (00000000.00000000.11111111.00000000).

    Шаблон маски можно задать с помощью выбора одного из предустановленных значений из выпадающего списка или вводом с клавиатуры, или использовать поле спинбокса. В поле спинбокса будет выставляться не битовая маска, а инвертированная битовая маска.
    Выпадающий список содержит пять предустановленных значений:
    0.0.0.0, 0.0.0.255, 0.0.255.255, 0.255.255.255, 255.255.255.255
    Установка значения шаблона маски, которое равно 255.255.255.255 для любого IP Address, будет интерпретироваться, как установка значения Type равного Any IP Address. При установке такого значения и закрытии окна редактирования кнопкой ОК строка созданной записи в окне Add a Rule (Рисунок 14) будет вместо адреса и маски содержать значение any. При вызове окна редактирования этой строки выпадающий список Type будет выставлен в положение Any IP Address, а поля IP Address и Wildcard Mask – заблокированы.

В зависимости от установленного значения Type элементы группы Source Host/Network будут менять свое поведение:

- если установлено значение A Network, то будут доступны и обязательны к заполнению все поля группы (Рисунок 15)
- при установке значения A Host блокируется элемент Wildcard Mask (Рисунок 16)

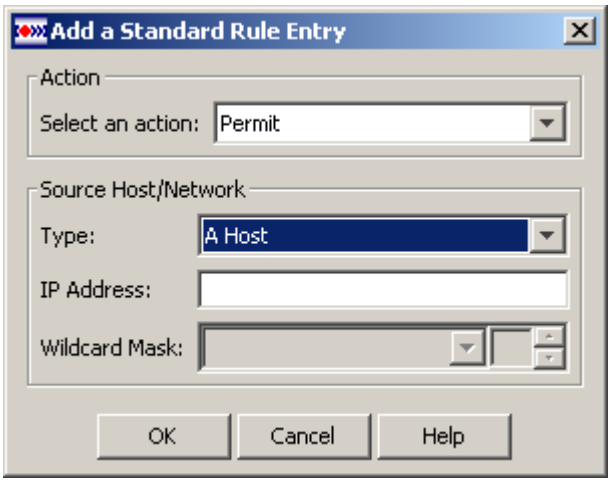

Рисунок 16

- при установке значения Any IP Address будут блокированы элементы IP Address и Wildcard Mask (Рисунок 17).

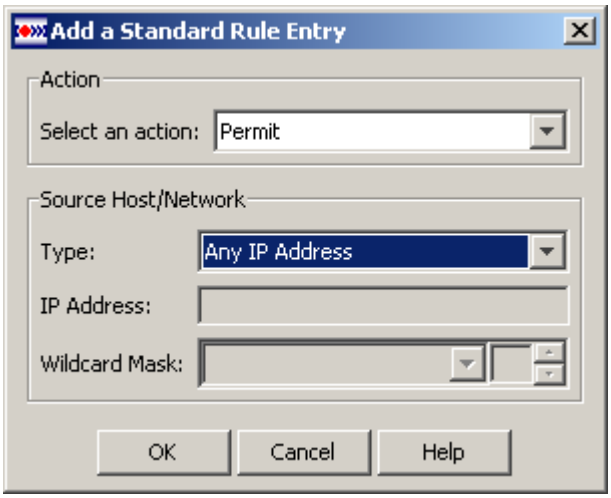

Рисунок 17

Создание записи в расширенном правиле доступа

Нажатие кнопки Add в окне создания расширенного правила Add a Rule открывает окно Add an Extended Rule Entry для создания записи в правиле (Рисунок 18):

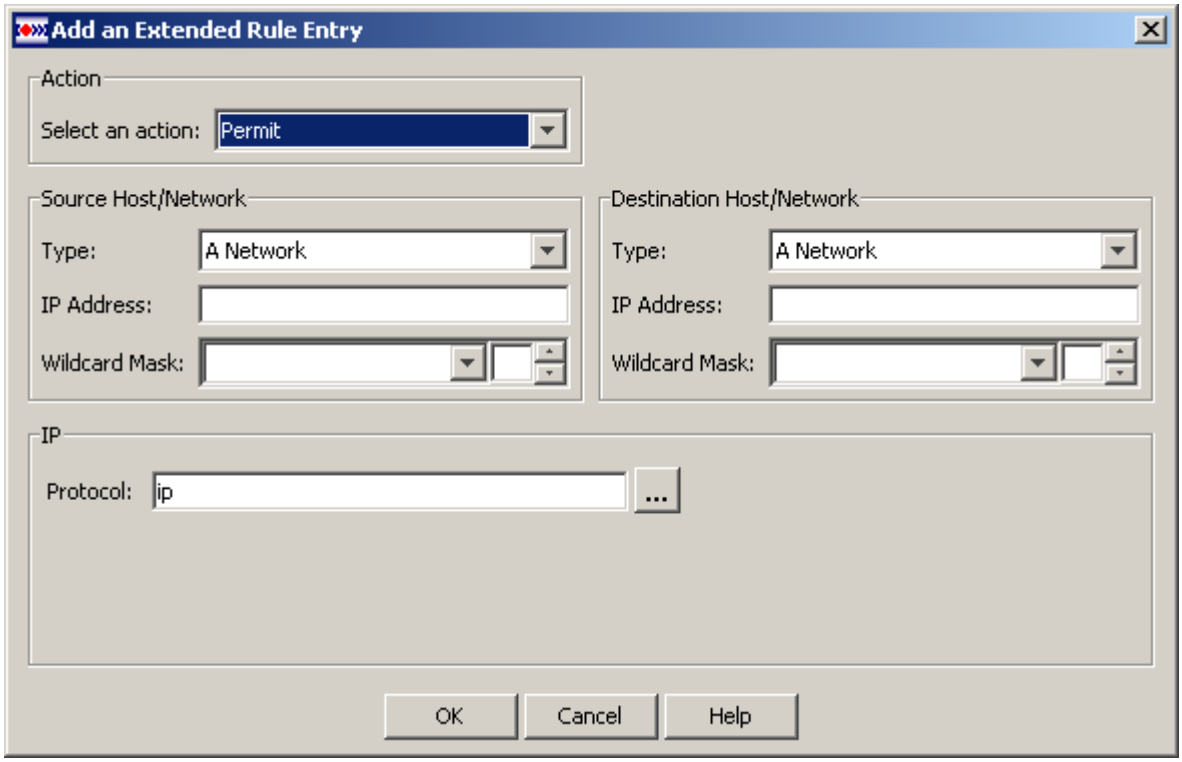

Рисунок 18

Окно содержит следующие элементы:

- Группа Action – выбрать действие, которое будет применяться к пакету, подпадающему под данную запись правила: пропускать или не пропускать пакет
- Группа Source Host/Network – так как производится фильтрация только входящего трафика, в этой группе указывается IP-адрес или диапазон IP-адресов отправителя пакетов, приходящих извне на интерфейс, к которому должно быть привязано правило.
- Группа Destination Host/Network – в этой группе указывается IP-адрес или диапазон IP-адресов получателя пакетов, приходящих извне на интерфейс, к которому должно быть привязано правило.

Поведение элементов в группах Source Host/Network и Destination Host/Network аналогично поведению подобных элементов, описанных в разделе "Создание записи в стандартном правиле"

- Группа IP содержит как общие, так и специфические части, в зависимости от выбранного IP-протокола.
  - Protocol – поле для ввода имени протокола. Протокол можно ввести вручную, указав имя протокола или номер протокола в диапазоне от 0 до 255, либо выбрать из списка предопределенных протоколов в окне IP Protocols, которое открывается по нажатию кнопки «...» (Рисунок 19). Номер введенного протокола будет проверяться по нажатию кнопки OK. Если номер протокола выходит за пределы зарезервированного пространства – будет выдано сообщение об ошибке. Если введенному номеру соответствует имя протокола в предопределенном списке, то это имя и будет подставлено в поле ввода.

Окно со списком предопределенных протоколов:

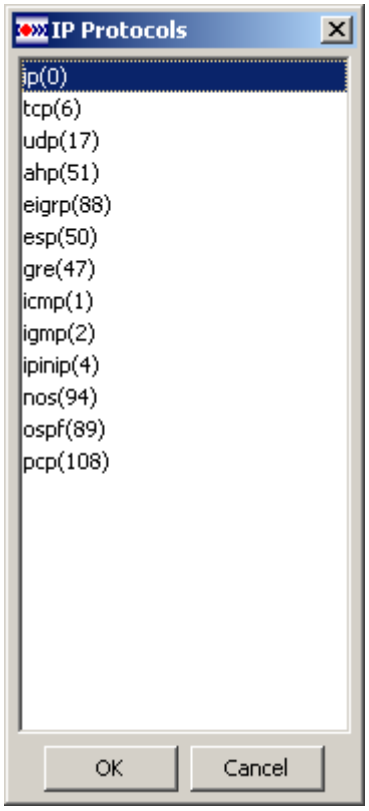

Рисунок 19

При выборе протокола TCP из списка предопределенных протоколов (Рисунок 19), в окне Add an Extended Rule Entry появится два новых поля – Source Port TCP (range) и Destination Port TCP (range) (Рисунок 20):

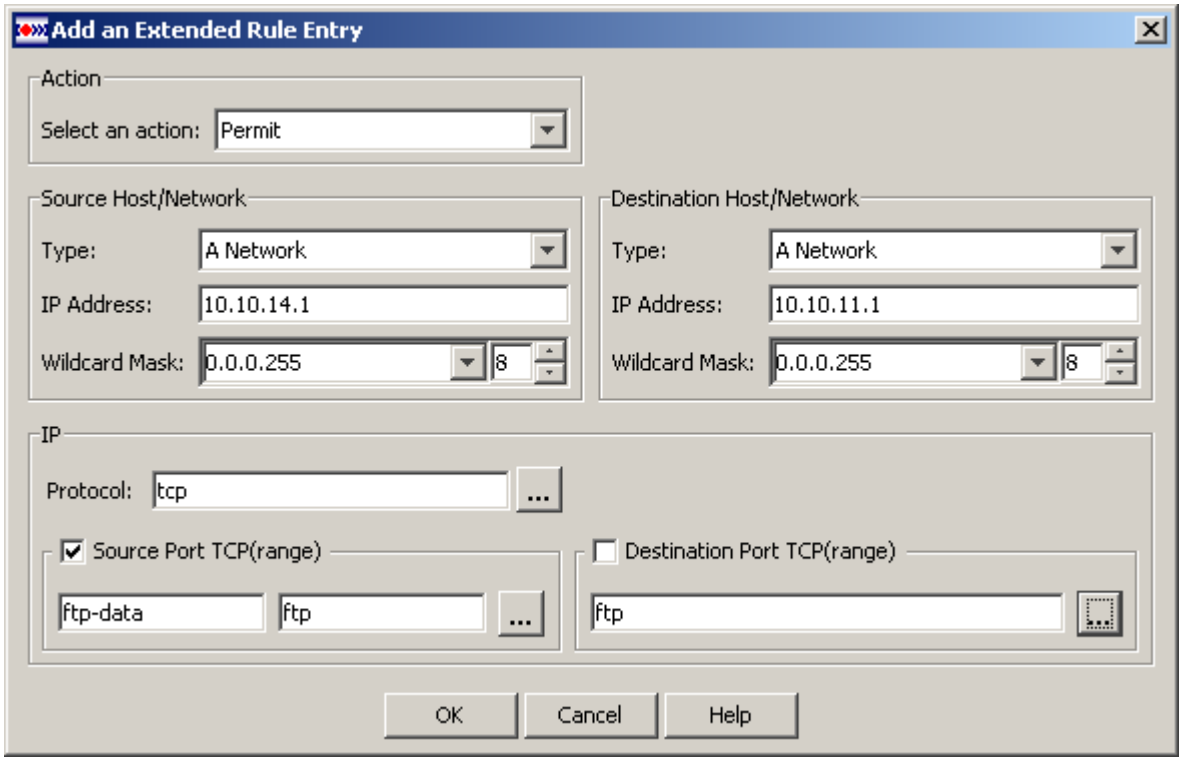

Рисунок 20

- Группа Source Port TCP (range) – в ней указывается порт или диапазон портов отправителя пакета
- Группа Destination Port TCP (range) – в ней указывается порт или диапазон портов получателя пакета
  При установке флажка (range) происходит переключение в режим ввода диапазонов портов. При этом появляется дополнительное поле ввода.

  Указать порт можно либо вручную, либо нажать кнопку «...» и выбрать значение из предопределенного списка. При вводе вручную возможен ввод как цифровых значений от 0 до 65535, так и названий портов. Если задается одиночный порт и вручную вводится численное значение порта, который присутствует в предопределенном списке, то после нажатия кнопки OK вместо номера порта будет подставлено его имя.
  Если задается диапазон портов и вручную или из списка в поле вводится имя порта, то после нажатия кнопки OK вместо имени порта будет подставлено его численное значение. Если первое значение при вводе диапазона портов больше второго, то после нажатия кнопки OK эти значения поменяются местами.

При выборе протокола UDP из списка предопределенных протоколов (Рисунок 19), в окне Add an Extended Rule Entry появятся две новые группы Source Port UDP(range) и Destination Port UDP(range), аналогичные описанным выше группам для TCP протокола.

Редактирование выделенной записи в правиле

Редактирование записи производится в окне Edit a Standard/Extended Rule Entry, которое вызывается с помощью кнопки Edit в окне Add a Rule или Edit a Rule. Редактируется выделенная строка. Окно редактирования совпадает с окном Add a Standard Rule Entry или Add an Extended Rule Entry. Окно будет заполнено параметрами выделенной записи (теми, которые были установлены при создании записи или последнем сеансе редактирования).

Клонирование выделенной записи в правиле

Нажатие кнопки Clone в окне Add a Rule открывает окно создания новой записи в правиле на основе существующей записи. В зависимости от типа правила будет открыто либо окно Add a Standard Rule Entry, либо окно Add an Extended Rule Entry. В открытом окне поля будут заполнены параметрами записи, которая была выбрана для клонирования.

Удаление выделенной записи в правиле

Удаление выделенной записи производится кнопкой Delete в окне Add a Rule. Нажатие этой кнопки вызывает окно с предупреждением о необходимости подтвердить удаление записи. После получения подтверждения запись удаляется.

Привязка правила к интерфейсу

При нажатии кнопки Associate в окне Add a Rule появляется окно Associate with an Interface (Рисунок 21):

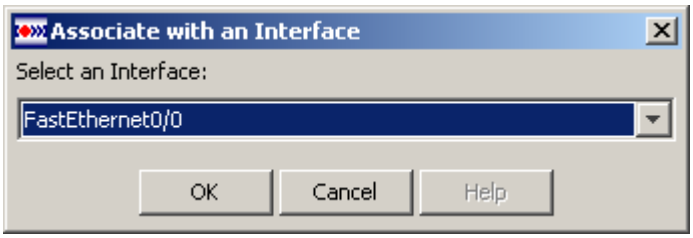

Рисунок 21

Ассоциация правила с интерфейсом означает, что правило начинает работать как фильтрующее для входящего трафика на интерфейс.

Это окно содержит следующие элементы:

- Select an Interface – поле для выбора интерфейса, к которому будет привязываться данное правило. Содержит выпадающий список интерфейсов:
  - none – значение по умолчанию. При выборе этого значения правило не будет привязано к интерфейсу.

Если выбранный интерфейс уже имеет связанное с ним правило, то при нажатии кнопки ОК будет открыто окно с предупреждением, что выбранный интерфейс уже связан с правилом (номер/имя правила) и вопросом, желает ли пользователь изменить у этого интерфейса связанное правило. При утвердительном ответе на этот вопрос связь выбранного интерфейса и привязанного правила разрывается, к интерфейсу привязывается создаваемое правило. При отрицательном ответе – процедура создания правила продолжается. При выборе значения none правило будет создано без привязки к интерфейсу.

Редактирование выделенного правила доступа

Кнопка Edit в окне Rules вызывает окно редактирования правила Edit a Rule (Рисунок 22), которое по составу элементов совпадает с окном создания нового правила Add a Rule за исключением кнопки Associate. Редактирование правила имеет следующие особенности:

- запрещено редактирование поля Name/Number
- запрещено редактирование поля Type
- запрещено редактирование поля Interface Association (блокирован список интерфейсов).

Редактирование правила производится теми же управляющими кнопками, что и при создании нового правила доступа.

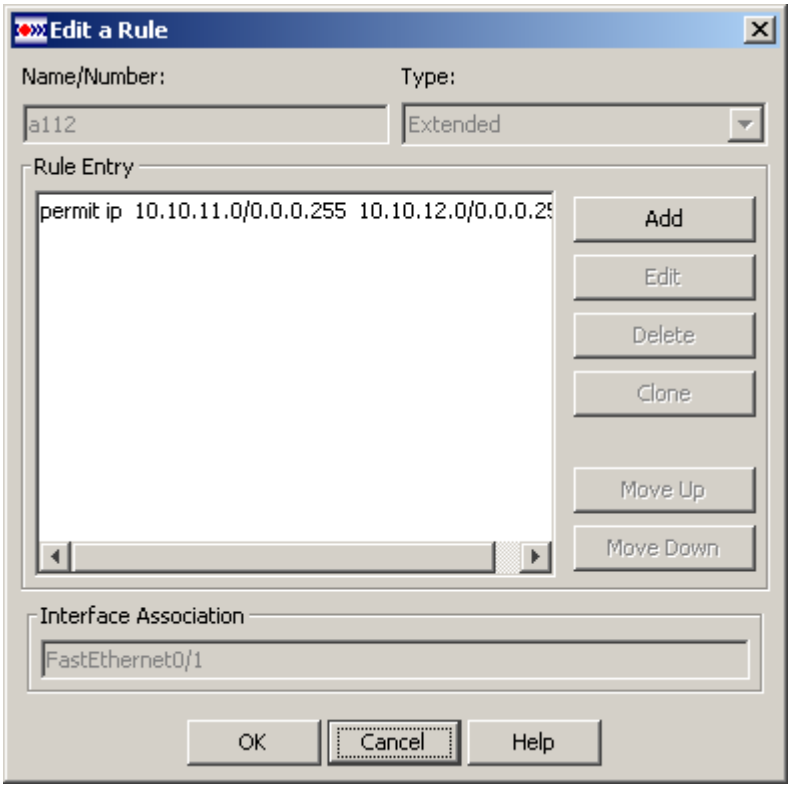

Рисунок 22

Удаление выделенного правила доступа

Удаление выделенного правила в окне Rules производится с помощью кнопки Delete. Если выделенное правило не привязано ни к интерфейсу, ни к криптографической карте, то будет открыто окно с требованием подтверждения удаления.

Если выделенное правило привязано к интерфейсу, то будет выдано сообщение о необходимости сначала устранить привязку к интерфейсу.

Если удаляемое правило привязано к криптографической карте, то выдается сообщение о необходимости устранить данную привязку к криптографической карте.

IPSec Rules

В этом разделе (Рисунок 23) можно просматривать, создавать, редактировать и удалять правила IPsec.

Правило IPsec задает исходящий трафик, который следует или не следует защищать средствами IPsec. Для входящего трафика используется то же самое правило IPsec для выявления трафика для расшифрования, при этом адреса отправителя и получателя в правиле просматриваются в обратном порядке.

Правило IPsec привязывается к криптографической карте в политике IPsec. Эта привязка осуществляется в разделе IPSec Policies.

Главная форма в этом разделе имеет тот же вид, что и в Access Rules, но с одним отличием – этот раздел содержит только расширенные правила.

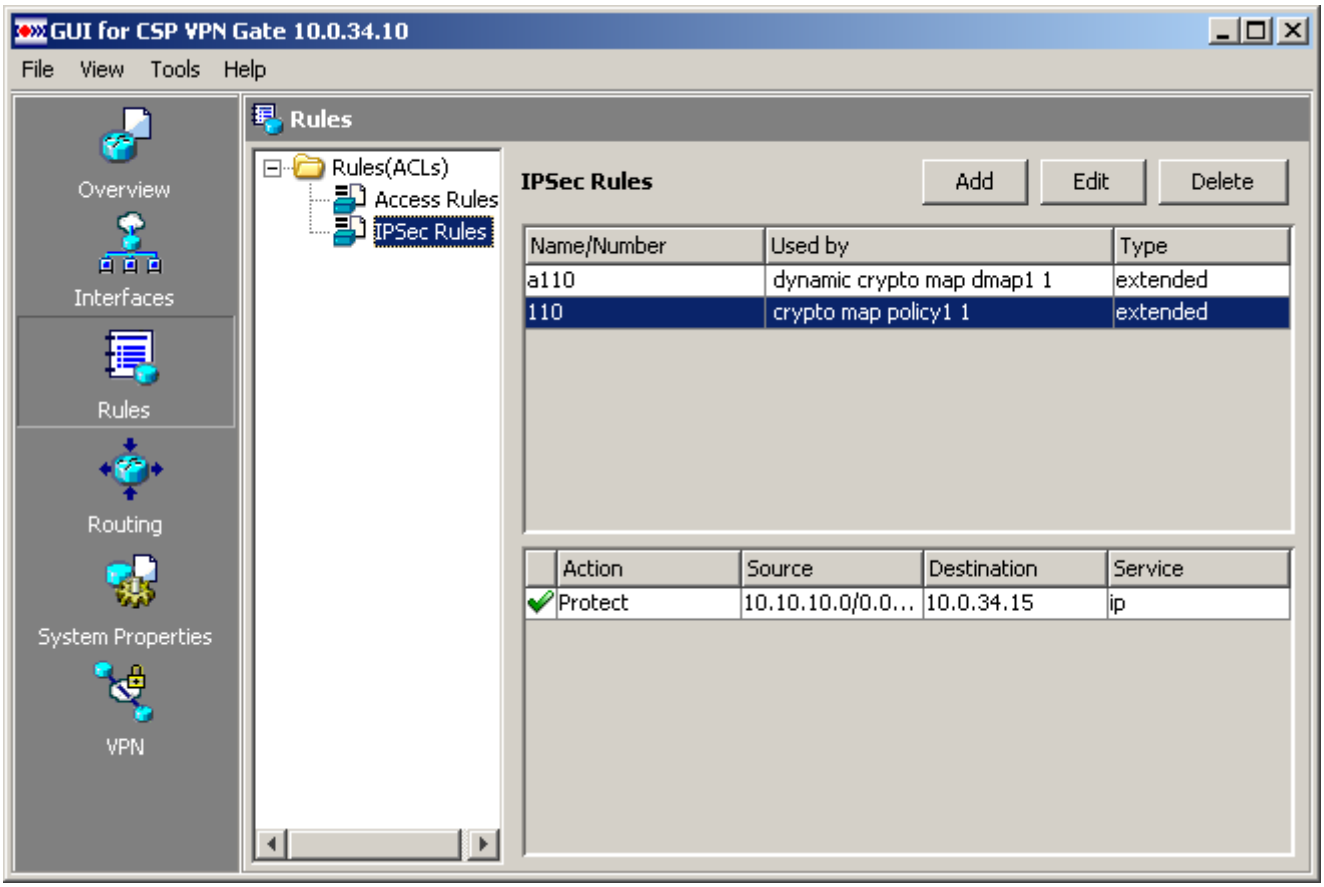

Рисунок 23

Создание нового правила IPsec

Кнопка Add в разделе IPSec Rules вызывает окно Add a Rule (Рисунок 24), которое совпадает с окном создания нового правила доступа. Отличие будет только в том, что поля Type и Interface Association являются блокированными. Поле Type блокировано на значении Extended.

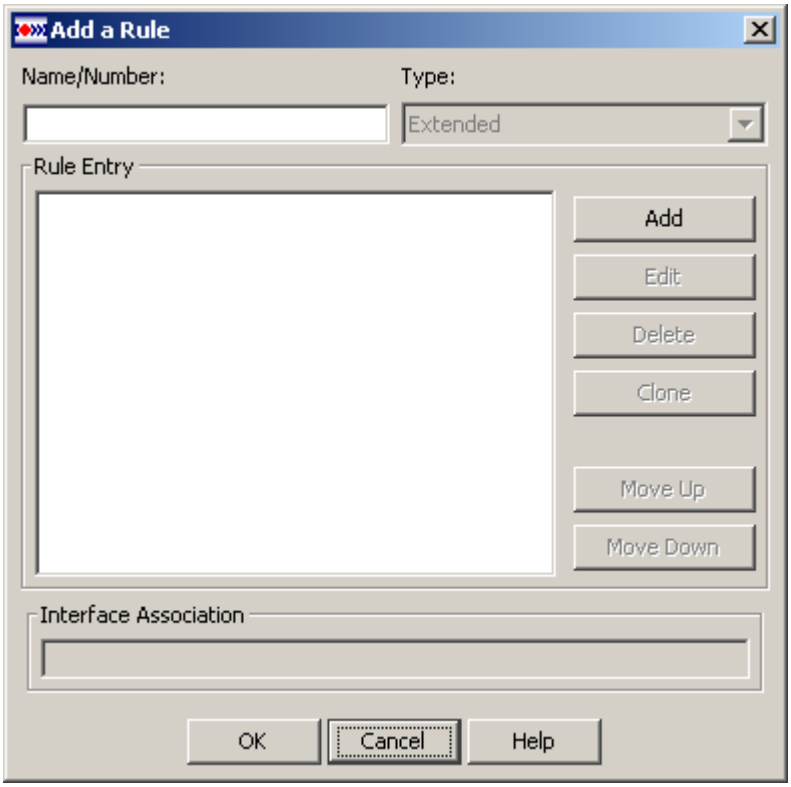

Рисунок 24

Создание записи в правиле IPsec

Кнопка Add в окне Add a Rule открывает окно Add an Extended Rule Entry (Рисунок 25), аналогичное окну в правиле доступа и описанное в разделе "Создание записи в расширенном правиле доступа".

- Группа Action – выбрать действие, которое будет применяться к трафику, подпадающему под данную запись правила:
  - Protect – защищать трафик на основе политики, заданной криптографической картой. Значение по умолчанию
  - Do not protect – не защищать трафик, пакет будет пропущен шлюзом без IPsec обработки. Если имеется правило доступа, привязанное к интерфейсу, то для пропускания пакета необходимо, чтобы он подпадал под действие записи этого правила с Action = Permit.
- Группа Source Host/Network – в этой группе указывается IP-адрес или диапазон IP-адресов, защищаемых данным шлюзом безопасности
- Группа Destination Host/Network – в этой группе указывается IP-адрес или диапазон IP-адресов, защищаемых партнером данного шлюза по IPsec-соединению.

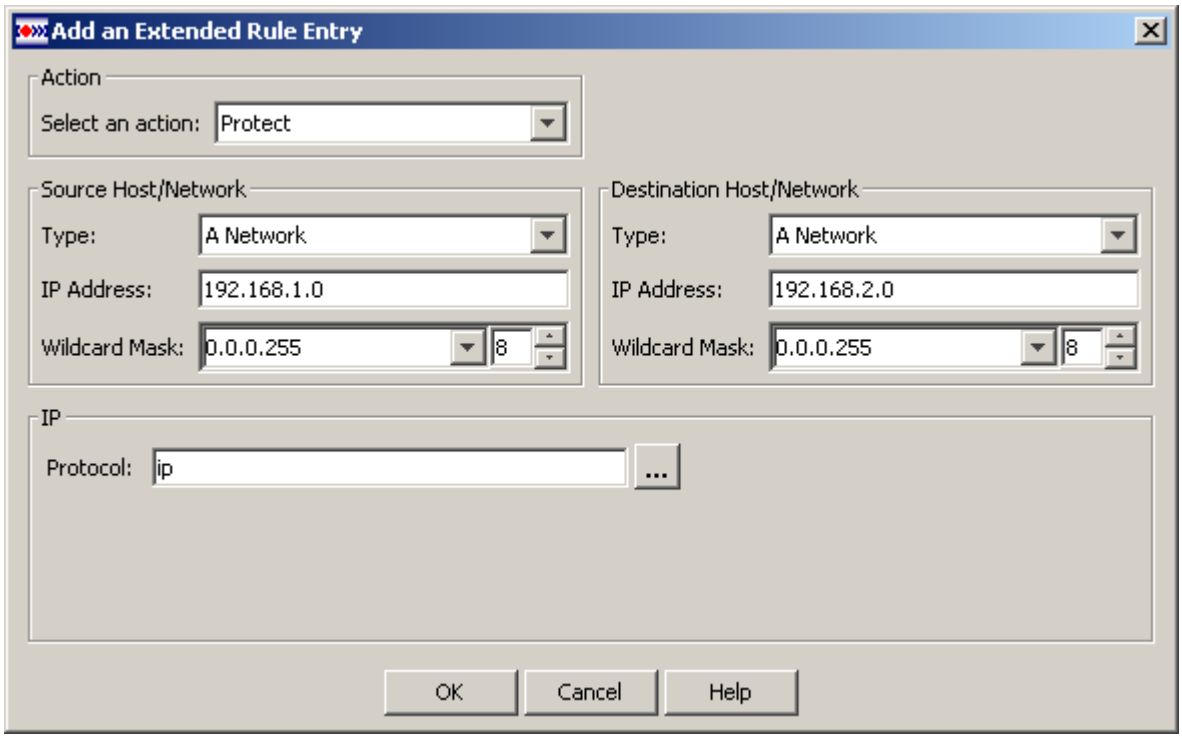

Рисунок 25

При нажатии кнопки OK, в окне Add a Rule появится первая запись.

Редактирование записи в правиле IPsec

Редактирование выделенной записи правила IPsec производится в окне Edit an Extended Rule Entry, которое вызывается кнопкой Edit. Это окно аналогично окну Add an Extended Rule Entry.

Клонирование записи в правиле IPsec

Нажатие кнопки Clone в окне создания правила Add a Rule открывает окно Add an Extended Rule Entry, в котором все поля заполнены параметрами записи, которая была выбрана для клонирования.

Удаление выделенной записи в правиле IPsec

Удаление выделенной записи производится кнопкой Delete в окне Add a Rule. Нажатие этой кнопки вызывает окно с предупреждением о необходимости подтвердить удаление записи. После получения подтверждения запись удаляется.

Редактирование выделенного правила IPsec

Редактирование выделенного правила IPsec в окне Rules осуществляется в окне Edit a Rule, которое вызывается кнопкой Edit в этом же окне. Редактирование правила IPsec ничем не отличается от описанного выше редактирования правила в Access Rules (см. "Редактирование выделенного правила доступа").

Удаление выделенного правила IPsec

Удаление выделенного правила в окне Rules производится с помощью кнопки Delete в этом же окне. Разрешается удаление только несвязанных с интерфейсами или криптографическими картами правил. Если попытаться удалить правило, связанное с криптографической картой, то будет выдано сообщение о необходимости сначала устранить связь с криптографической картой:

Если будет предпринята попытка удалить правило, связанное с интерфейсом, то будет выдано сообщение о необходимости сначала устранить связь с интерфейсом:

Удаление несвязанного правила предваряется сообщением с требованием подтверждения удаления.

Routing

Главная форма раздела Routing (Рисунок 26) содержит таблицу маршрутизации. Каждая запись в этой таблице связывает адрес сети назначения пакета с адресом следующего маршрутизатора или именем выходного интерфейса шлюза безопасности, на который нужно передать пакет для продвижения его по сети. В этом окне можно просмотреть существующие маршруты, создать новые, редактировать и удалять существующие.

При выдаче IP-адресов из IKE CFG пула мобильным пользователям в таблицу роутинга необходимо внести запись.

Если из IKE CFG пула с диапазоном 10.10.10.240 – 10.10.10.247, который соответствует подсети 10.10.10.240/29, выделены адреса, то в таблицу роутинга вносится запись:

- Prefix – 10.10.10.240
- Prefix Mask – 29 – битовая маска

IP Address – IP-адрес внешнего роутера, например 10.2.2.1, который стоит перед шлюзом безопасности, защищающим подсеть 10.10.10.0/24.

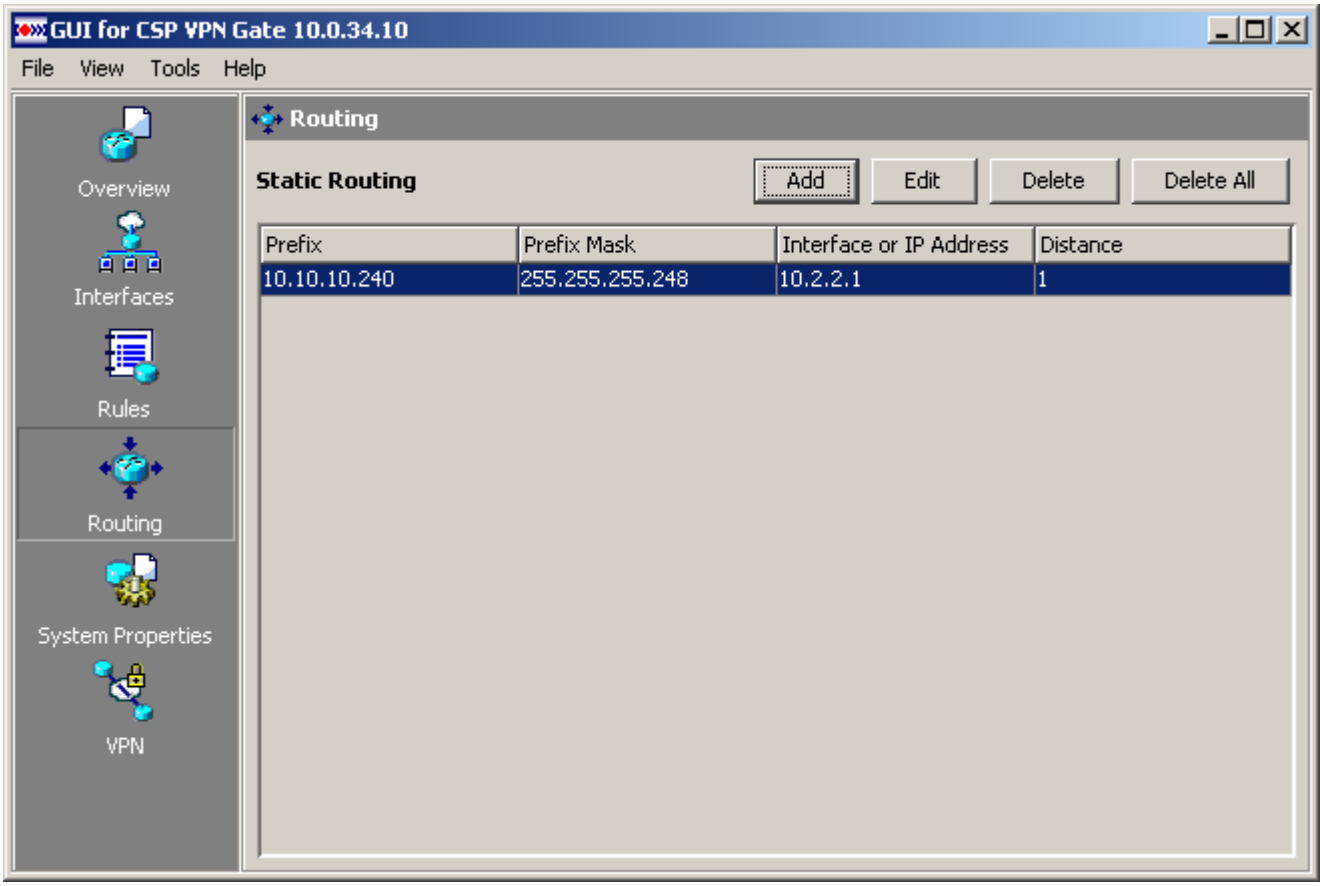

Рисунок 26

Главная форма раздела Routing содержит следующие элементы:

- Кнопки управления:
  - Add – кнопка вызова окна для создания нового маршрута
  - Edit – кнопка вызова окна для редактирования выделенного маршрута. Если в таблице не выделено ни одной строки, то кнопка блокируется

- Delete – кнопка удаления выделенного маршрута. Если в таблице не выделено ни одной строки, то кнопка блокируется
- Delete All – кнопка удаления всех маршрутов в таблице Static Routing. Если таблица не содержит ни одной строки, то эта кнопка блокируется.

- Таблица Static Routing состоит из столбцов:
  - Prefix – IP-адрес подсети получателя пакета
  - Prefix Mask – маска подсети получателя пакета
  - Interface or IP Address – IP-адрес следующего маршрутизатора либо имя выходного интерфейса шлюза безопасности, на который нужно передать пакет для продвижения его к получателю пакета
  - Distance – метрика маршрута.

Создание записи в таблице Static Routing

Создание записи в таблице Static Routing производится в окне Add Static Route (Рисунок 27), которое вызывается кнопкой Add.

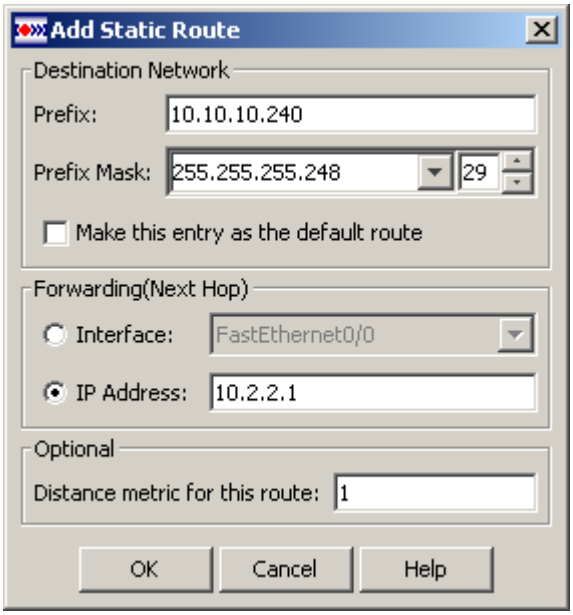

Рисунок 27

Это окно содержит следующие элементы:

- Группа Destination Network (Сеть получателя пакета):
  - Prefix – IP-адрес сети получателя пакета. При открытии окна это поле незаполнено. При закрытии окна младшие биты адреса обнуляются по маске.
  - Prefix Mask –маска подсети получателя пакета. Содержит выпадающий список установки сетевой маски и спинбокс установки битовой маски. При первом открытии окна эти элементы не содержат значений (пустые поля). После того, как было установлено какое-либо значение, вернуться в состояние незаполненных элементов нельзя.
    Выпадающий список содержит пять предустановленных значений:
    0.0.0.0
    255.0.0.0

255.255.0.0
255.255.255.0
255.255.255.255
В поле редактирования показывается значение, отличающееся от предустановленных и выставленное с помощью спинбокса.
Спинбокс позволяет устанавливать значения в диапазоне от 0 до 32.

- Make this entry as the default route –при установке этого флажка введенный маршрут будет использоваться по умолчанию. При этом поля Prefix и Prefix Mask блокируются, но значения в них сохраняются. По нажатию кнопки ОК в этом окне в таблице Static Routing для маршрута, который будет использоваться по умолчанию, в полях Prefix и Prefix Mask устанавливаются значения 0.0.0.0 и 0.0.0.0. После снятия флажка, поля Prefix и Prefix Mask с сохраненными в них значениями разблокируются.

  Маршрут по умолчанию – маршрут, по которому будет отправлен пакет, если IP-адрес назначения, указанный в заголовке пакета, не совпадает ни с одним адресом назначения в таблице маршрутизации.


Note

Если пользователь хочет задавать маршрут по умолчанию из GUI, то надо отключить системные настройки маршрута по умолчанию. В противном случае может возникнуть конфликт, и роутинг не будет работать правильно (в поставляемых программно-аппаратных комплексах CSP VPN Gate настройки маршрута по умолчанию отсутствуют). Для этого необходимо:

- в ОС Solaris удалить файл `/etc/defaultroute`, если он существует. Перезагрузить систему.
- в ОС Linux в файле `/etc/config` удалить значение во втором столбце строки с ключевым словом `DEFAULTROUTER`, если строка существует. Перезагрузить систему.

- Группа Forwarding (Next Hop) (следующий маршрутизатор). Здесь выставляется IP-адрес следующего маршрутизатора либо имя выходного интерфейса шлюза безопасности, на который нужно передать пакет для продвижения его по сети к получателю:
  - Interface – режим, активирующий список зарегистрированных сетевых интерфейсов. При его установке блокируется поле ввода IP Address. Список показывает первое значение. Этот режим установлен по умолчанию.
  - IP Address – режим, активирующий поле ввода IP-адреса следующего маршрутизатора. При его установке блокируется список зарегистрированных интерфейсов.
- Группа Optional
  - Distance metric for this route – поле ввода метрики маршрута. В качестве метрики маршрута пользователь может установить любой показатель: длину маршрута, число промежуточных маршрутизаторов, надежность, задержку, затраты на передачу и др. Разрешены значения из диапазона 1 – 255. По умолчанию установлено значение 1.
    В ОС Solaris этот параметр не имеет смысла и игнорируется, потому что в ОС Solaris метрика назначается интерфейсу, а не маршруту, как в данной команде.

Редактирование строки таблицы Static Routing

Редактирование выделенного маршрута в таблице Static Routing производится в окне Edit Static Route, которое вызывается кнопкой Edit. Это окно полностью совпадает с окном создания нового маршрута и отличается только названием.

Удаление строки таблицы Static Routing

Удаление выделенного маршрута в таблице производится с помощью кнопки Delete. Нажатие этой кнопки открывает стандартное окно, требующее подтверждения удаления строки. После получения подтверждения выделенная строка будет удалена из таблицы.

Очистка таблицы Static Routing

Очистка таблицы Static Routing (удаление всех строк таблицы) производится с помощью кнопки Delete All. Нажатие на эту кнопку вызывает стандартное окно с требованием подтверждения удаления всех маршрутов. После получения подтверждения все маршруты будут удалены.

System Properties

Раздел System Properties (Рисунок 28) состоит из четырех подразделов:

- Device – этот раздел показывает имя хоста и доменное имя хоста, на котором установлен CSP VPN Gate. Позволяет устанавливать пароль доступа к привилегированному режиму специализированной консоли, который используется при работе с интерфейсом командной строки
- SNMP – содержит настройки SNMP-агента в составе CSP VPN Gate и настройки получателей SNMP-трапов
- Syslog – содержит настройки для отправки сообщений о протоколируемых событиях. В этом окне можно посмотреть и произвести настройки вывода на syslog сервер.
- User Accounts – содержит имена и пароли пользователей с разными уровнями привилегий.

Кнопка управления:

- Edit – вызывает окно редактирования в каждом подразделе.

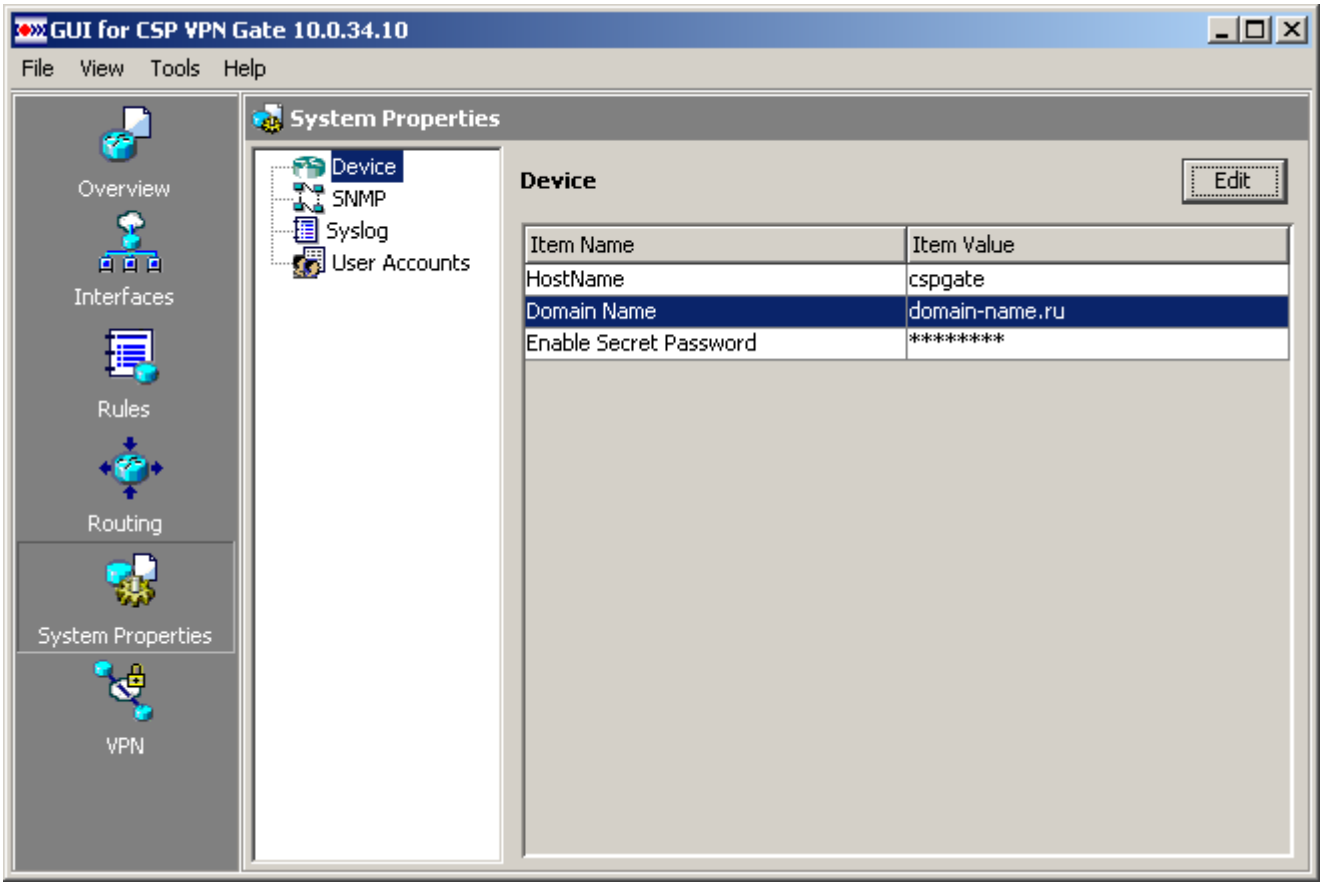

Рисунок 28

Device

Подраздел Device содержит таблицу свойств хоста, на котором установлен CSP VPN Gate (Рисунок 28):

- Item Name содержит параметры:
  - Host Name – имя хоста, на котором установлен CSP VPN Gate, и который мы настраиваем
  - Domain Name – доменное имя для хоста, на котором установлен настраиваемый CSP VPN Gate. Используется при работе на Preshared Key, когда в конфигурации присутствует команда crypto isakmp identity hostname. В этом случае шлюз безопасности при установлении IKE SA посылает партнеру в качестве идентификационной информации строку <HostName>.<Domain Name>. Установка Domain Name не влияет на настройки операционной системы, в которой работает шлюз безопасности. При посылке DNS-запросов неполные DNS-имена хостов не будут дополняться данной строкой. При SNMP-опросе шлюза безопасности для параметра sysName будет выдаваться значение, соответствующее HostName"
  - Enable Secret Password – пароль доступа к привилегированному режиму специализированной консоли, может использоваться только в интерфейсе командной строки.
- Item Value содержит значения этих параметров:
  - звездочки напротив пункта Enable Secret Password показывают, что пароль доступа в привилегированный режим является не пустым.

Редактирование параметров Device

Вызов окна редактирования параметров хоста (Рисунок 29) производится нажатием кнопки Edit или двойным щелчком на любой строчке.

Окно редактирования параметров состоит из следующих элементов:

- Вкладка Device:
  - Host Name – поле ввода имени хоста. Имя состоит из одного или нескольких слов, разделенных точкой. Каждое слово обязательно должно начинаться с буквы латинского алфавита и может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака "-" (дефис)
  - Domain Name – поле ввода доменного имени. Имя состоит из одного или нескольких слов, разделенных точкой. Каждое слово обязательно должно начинаться с буквы латинского алфавита и может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака "-" (дефис).

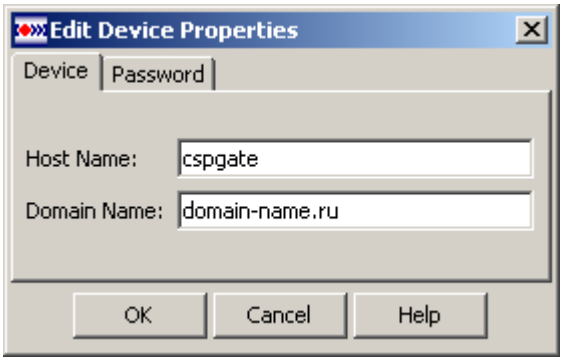

Рисунок 29

- Вкладка Password (Рисунок 30):

- Change password – флажок, отвечающий за блокировку двух полей вкладки. При открытии окна этот флажок всегда снят.
- Enter New Password – поле ввода нового пароля доступа к привилегированному режиму консоли.
- Re-Enter Password – поле повторного ввода нового пароля доступа.

Рисунок 30

SNMP

В подразделе SNMP можно просматривать и редактировать настройки SNMP-агента для получения запросов от SNMP-менеджера и выдачи ему статистики из базы данных MIB, которую поддерживает SNMP-агент. Здесь же задаются и получатели SNMP-трапов, которым отсылаются сообщения о происходящих событиях на шлюзе безопасности (Рисунок 31). Главная форма этого раздела содержит два подраздела – SNMP Polling и SNMP Traps.

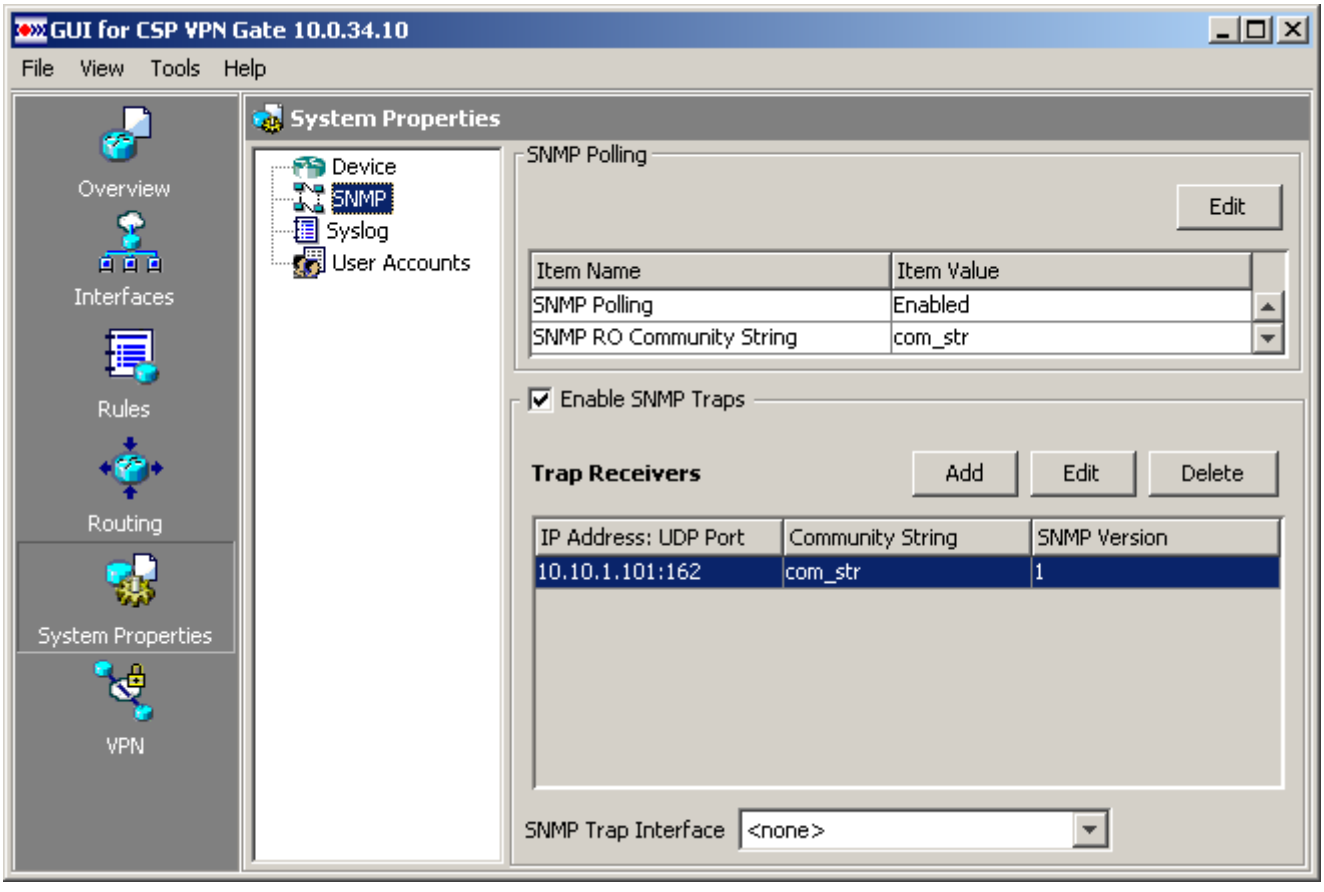

Рисунок 31

В подразделе SNMP Polling задаются настройки SNMP-агента для выдачи статистики по запросу SNMP-менеджера. Таблица этого подраздела включает элементы:

- Item Name содержит следующие параметры:
  - SNMP Polling – включение/выключение настроек SNMP-агента
  - SNMP RO Community String – текстовая строка, играющая роль пароля при аутентификации сообщений SNMP. Эта же строка должна быть задана на стороне SNMP-менеджера. Этот параметр обязателен, если SNMP Polling включен.
  - SNMP Server Location – текстовая строка, в которой указывается физическое размещение SNMP-агента (например, "room1"). Может содержать пустую строку.
  - SNMP Server Contact – текстовая строка, в которой указываются данные контактного лица, ответственного за работу SNMP-агента (например, e-mail). Может содержать пустую строку.
- Item Value содержит значения этих параметров:
  - SNMP Polling – имеет два значения – Enabled/Disabled – включение/выключение настроек SNMP-агента. При значении Disabled остальные параметры не появляются.

В подразделе SNMP Traps задается список получателей SNMP трапов, в которых SNMP-агент сообщает менеджеру о возникших событиях. Таблица этого подраздела содержит список получателей SNMP-трапов и их настройки:

- IP Address : UDP Port – IP-адрес получателя SNMP-трапов; UDP-порт, на который SNMP-менеджеру будут высылаться трап-сообщения. У всех получателей адреса должны быть различны.
- Community String – строка, играющая роль идентификатора отправителя трап-сообщения
- SNMP Version – версия SNMP, в которой формируются трап-сообщения.
- Enable SNMP Traps – установка этого флажка включает данный подраздел и позволяет вводить получателей.
- SNMP Trap Interface – выпадающий список интерфейсов шлюза безопасности, на который будут передаваться трап-сообщения для отсылки получателям. Параметр необязательный.

Необходимо отметить, что параметры SNMP Traps сохраняются при загрузке-редактировании даже в том случае, если SNMP Traps отключен.

Редактирование параметров SNMP Polling

Вызов окна редактирования Edit SNMP Polling (Рисунок 32) параметров SNMP производится нажатием кнопки Edit.

Состав элементов окна:

- Enable SNMP Polling – установка этого флажка позволяет настраивать SNMP-агента.
- Community String – поле ввода текстовой строки. Допускаются латинские буквы, цифры, знаки `!"#$%&'()*+,-./;:>=<@[\]^_`{|}~?.` Первым символом обязательно должна быть буква. Нельзя использовать пробелы. Поле обязательно для заполнения.
- SNMP Server Location – поле ввода текстовой строки. Допускаются латинские буквы, цифры, знаки `!"#$%&'()*+,-./;:>=<@[\]^_`{|}~?` и пробелы.
- SNMP Server Contact – поле ввода текстовой строки. Допускаются латинские буквы, цифры, знаки `!"#$%&'()*+,-./;:>=<@[\]^_`{|}~?` и пробелы.

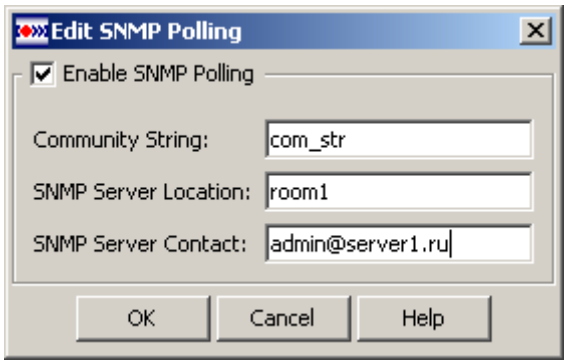

Рисунок 32

При снятии флажка Enable SNMP все поля окна будут заблокированы, но значения в них не будут удалены (повторная установка флажка позволит использовать эти значения). Если после этого в окне нажать кнопку OK, то будет открыто стандартное окно с требованием подтверждения выполняемой операции.

Настройки получателей SNMP трапов

Выставление флажка Enable SNMP Traps позволяет создавать, редактировать и удалять получателей SNMP-трапов. В подразделе SNMP Traps (Рисунок 31) имеются три функциональные кнопки:

- Add – вызов окна Add Trap Receiver для ввода настроек получателя SNMP трапов
- Edit – вызов окна редактирования настроек выделенного в таблице получателя
- Delete – удаление выделенной строки.

Создание и редактирование настроек получателя. Все поля в окне Add/Edit Trap Receiver являются обязательными для заполнения:

- IP Address – IP-адрес получателей SNMP-трапов. У всех получателей IP-адреса должны быть различны.
- UDP Port – диапазон допустимых портов 1 – 65535. Значение по умолчанию -162.
- Community String – допускаются латинские буквы, цифры, знаки !"#$%&'()*+,-./;:>=<@[\]^_`{|}~?.Первым символом обязательно должна быть буква. Нельзя использовать пробелы. Запрещено в качестве community использовать слова – version, traps, informs, а также любые их формы – типа Version, vErsion и т. п. У всех получателей SNMP-трапов Community должны быть различны.
- SNMP Version – поддерживаются две версии, по умолчанию используется версия SNMPv1.

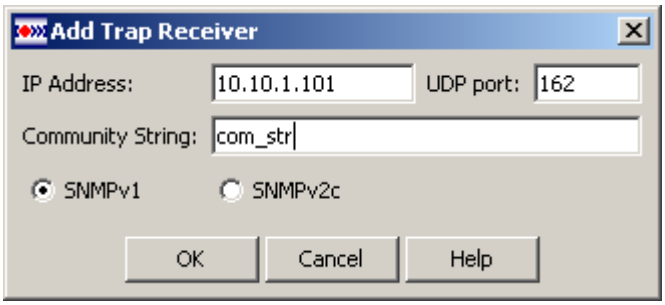

Рисунок 33

Syslog

Главная форма подраздела Syslog (Рисунок 34) содержит настройки Syslog-клиента для отправки сообщений о протоколируемых событиях на Syslog-сервер.

Этот подраздел содержит таблицу со столбцами:

- Item Name содержит следующие параметры:
  - Syslog – включение/выключение настроек Syslog
  - Syslog Server – IP-адрес компьютера, на который будут отсылаться лог-сообщения
  - Facility – показывает источник выдаваемых сообщений
  - Severity – показывает уровень важности протоколируемых событий.
- Item Value содержит значения этих параметров:
  - Syslog – имеет два значения – Enabled/Disabled – включение/выключение настроек Syslog, отличных от прописанных в файле syslog.ini. При значении Disabled остальные параметры не показываются.

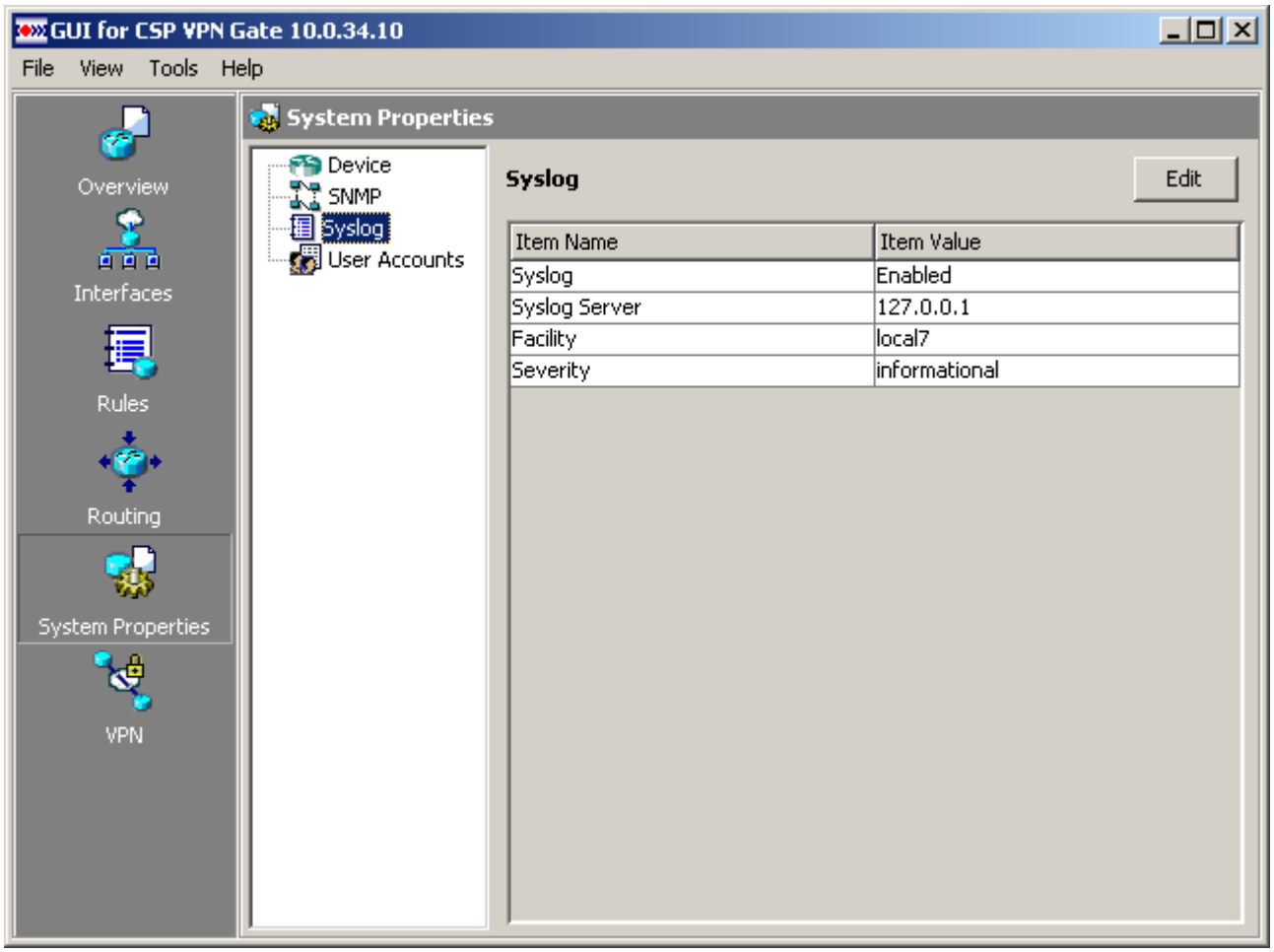

Рисунок 34

Редактирование параметров Syslog

Редактирование настроек логирования производится в окне Syslog Properties, которое вызывается кнопкой Edit.

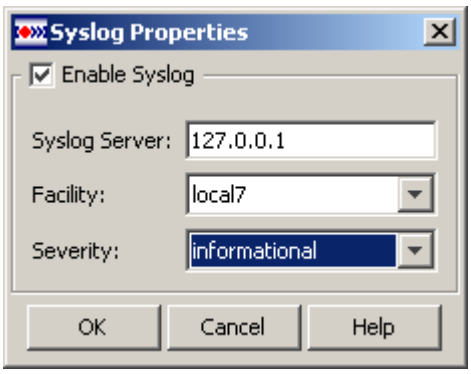

Рисунок 35

Состав элементов окна редактирования:

- Enable Syslog – установка этого флажка позволяет делать настройки Syslog. При снятии флажка блокируются элементы окна, при этом запоминаются введенные в эти поля значения на время редактирования.
- Syslog Server – поле ввода IP-адреса хоста, на который будут отсылаться сообщения о протоколируемых событиях. Задать можно только одного получателя лог-сообщений. По умолчанию – значение 127.0.0.1.
- Facility – выпадающий список источников сообщений:
  - auth – система безопасности и авторизации
  - cron – системные часы
  - daemon – прочие процессы
  - kern – сообщения ядра
  - local0
  - local1
  - local2
  - local3
  - local4
  - local5
  - local6
  - local7 – значение по умолчанию
  - lpr – подсистема печати
  - mail – почтовая система
  - news – подсистема сетевых сообщений
  - sys9
  - sys10
  - sys11
  - sys12
  - sys13

  - sys14
  - syslog – вырабатываются самим syslog
  - user – пользовательские программы
  - uucp – подсистема UUCP
- Severity – выпадающий список со значениями важности сообщений:
  - emergencies – аварийные сообщения при выходе из строя системы
  - alerts – предупредительные сообщения для срочного вмешательства
  - critical – сообщения о критических событиях
  - errors – сообщения об ошибках
  - warnings – предупреждения
  - notifications – важные замечания, уведомления
  - informational – информационные сообщения, значение по умолчанию
  - debugging – отладочные сообщения.

User Accounts

В подразделе User Accounts (Рисунок 36) можно создавать пользователей, изменять имена и пароли пользователей, удалять пользователей, назначать уровни привилегий.

Этот подраздел содержит таблицу со столбцами:

- User Name – имя пользователя
- Password – пароль пользователя, отображаемая строка всегда содержит 6 звездочек, независимо от количества символов в пароле
- Privilege Level – уровень привилегий.

Пользователю может быть назначен уровень привилегий из диапазона 0 – 15. Этот диапазон разделен на два класса: в первом – пятнадцатый уровень, а во втором – с 0 по 14 уровни. Пользователи с уровнем привилегий от 0 до 14 имеют одинаковые права.

Пользователь с пятнадцатым уровнем привилегий имеет право доступа к графическому интерфейсу CSP VPN Gate – могут настраивать шлюз безопасности. Пользователей с пятнадцатым уровнем может быть несколько.

Пользователи с уровнем привилегий с 0 по 14 имеют право доступа только к пользовательскому режиму специализированной консоли в интерфейсе командной строки и не имеют права настраивать шлюз безопасности в GUI.

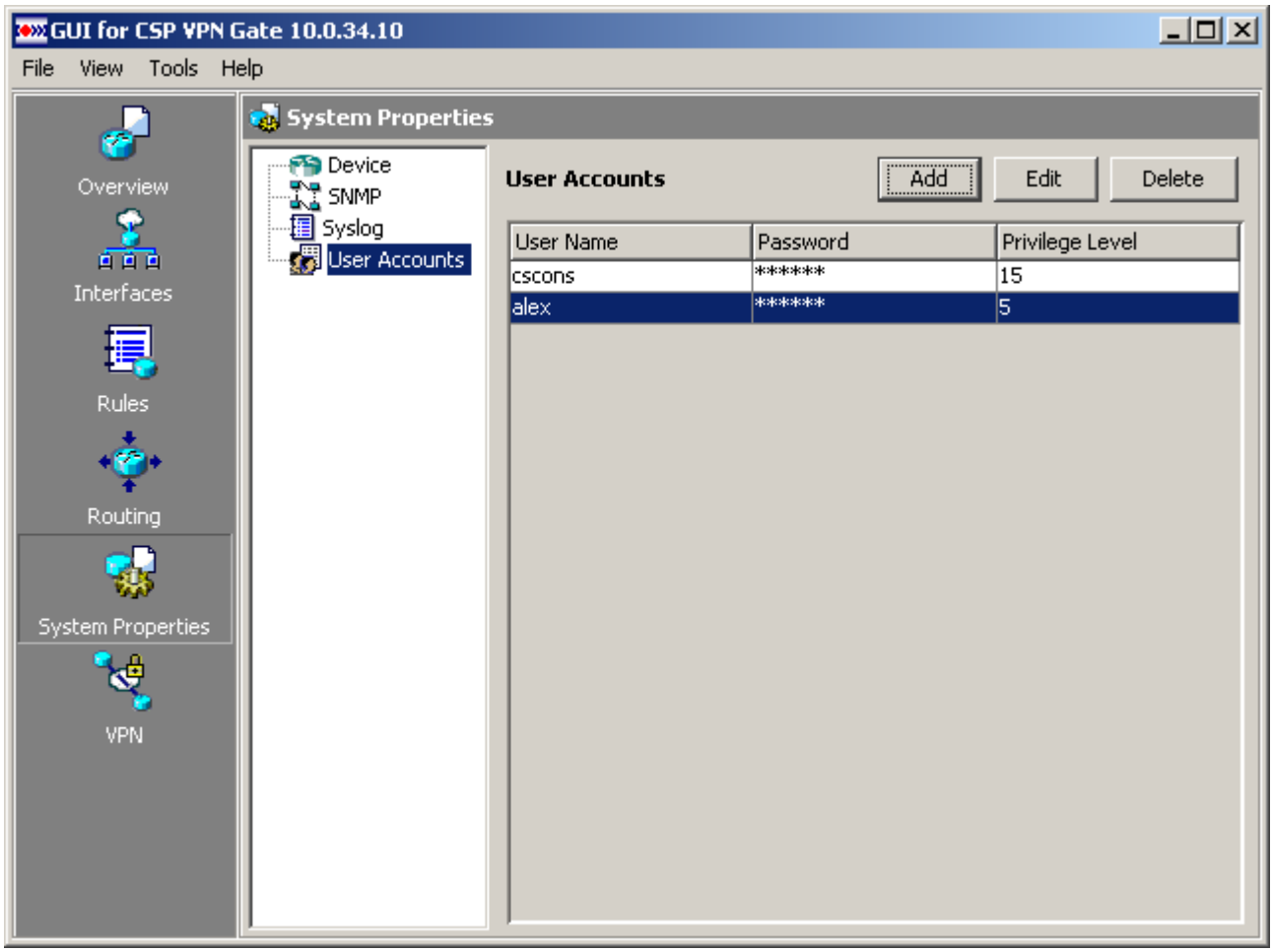

Рисунок 36

Создание пользователя

Создание пользователя производится в окне Add User Account (Рисунок 37), вызываемое по нажатию кнопки Add.

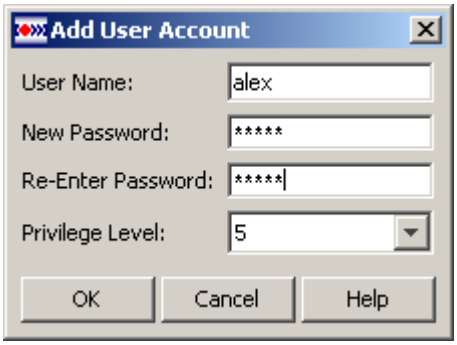

Рисунок 37

Состав элементов окна:

- User Name – имя пользователя. Имя должно начинаться с буквы латинского алфавита. Далее могут идти буквы латинского алфавита, цифры, _ (подчеркивание) и – (дефис). Имя должно быть уникальным и не превышать 8 символов. Поле обязательно для заполнения.
- New Password – пароль пользователя. Допускаются латинские буквы, цифры и спецсимволы. Нельзя использовать пробелы и нелатинские символы.

- Re-Enter Password – повторный ввод пароля
- Privilege Level – число от 0 до 15. Значение по умолчанию – 0.

Создание пользователя в GUI и назначение ему пароля, в текущей конфигурации отображается в виде команды

```
username {name} [privilege level] secret 0 {pwd}
```

При загрузке конфигурации на шлюз пароль передается в открытом виде и только после загрузки вычисляется функция хэширования пароля и в действующей конфигурации пароль хранится как результат функции хэширования. Действующая конфигурация показывает уже другую команду:

```
username {name} [privilege level] secret 5 {pwd_encrypted}.
```

Редактирование данных о пользователе

Для внесенения изменений данных о пользователе вызывается окно Edit User Account кнопкой Edit.

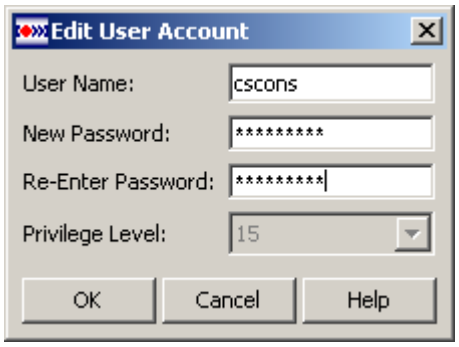

Рисунок 38

При открытии окна редактирования поля New Password и Re-Enter Password отображаются в виде звездочек. Если эти поля не менялись (редактировались другие поля), то пароль пользователя не изменяется.

Если имеется только один пользователь с уровнем 15, то при его редактировании поле Privilege Level будет блокировано, в остальных случаях – поле доступно для редактирования.

Переименование пользователя, от имени которого установлена текущая сессия, запрещено.

Не рекомендуется изменять уровень привилегий пользователя, от имени которого установлена текущая сессия. При попытке сделать это выдается предупреждение. Если изменения все же сделаны, то по завершении доставки конфигурации на шлюз, для продолжения работы будет предложено ввести имя и пароль пользователя с уровнем привилегий, позвляющим работать с графическим интерфейсом CSP VPN Gate. В случае отказа приложение будет закрыто.

При редактировании пароля пользователя в конфигурации, созданной ранее в интерфейсе командной строки и загруженной с использованием предложения Restore Current Config from PC меню File, в целях безопасности команда

```
username {name} [privilege level] secret 0 {pwd}
```

будет заменена на другую

```
username {name} [privilege level] secret 5 {pwd_encrypted}.
```

При редактировании имени пользователя или уровня привилегий, пароль продолжает храниться в том же виде, как и до редактирования.

Произведенные изменения вступят в силу после доставки конфигурации командой Deliver to Router.

Удаление пользователя

Удаление пользователя осуществляется выделением строки в таблице User Accounts (Рисунок 36) и нажатием кнопки Delete.

Удаление единственного пользователя с уровнем привилегий 15 запрещено.

При попытке удаления пользователя, под которым установлена текущая сессия GUI, выдается сообщение о запрете такой операции.

В других случаях удаление пользователя осуществляется с выдачей запроса на подтверждение удаления.

VPN

В разделе VPN (Рисунок 39) можно просмотреть созданные VPN соединения, создать новые и удалить существующие. Соединение VPN – установление связи между интерфейсом и политикой IPsec. Для создания соединения VPN сначала нужно создать политику IPsec.

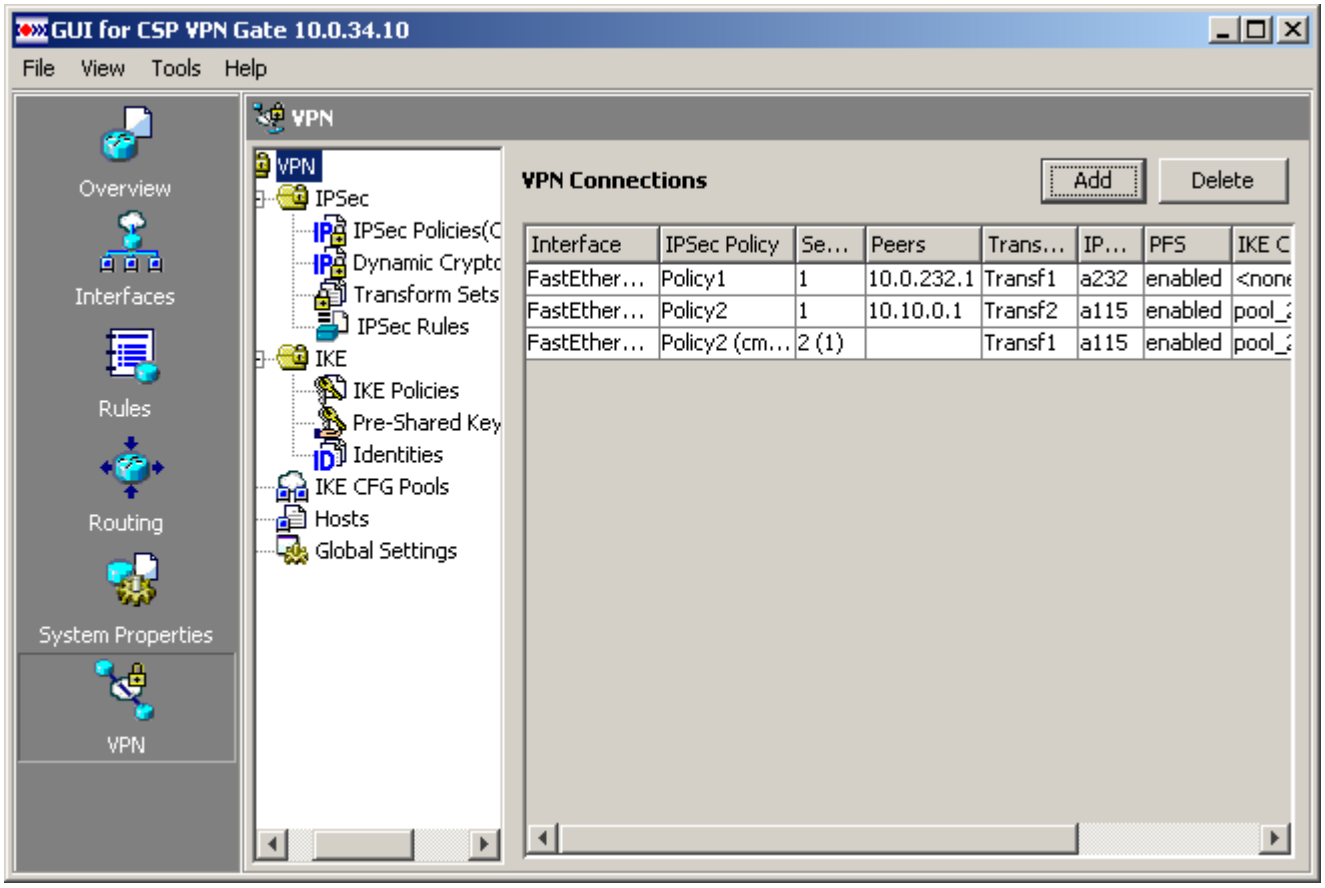

Рисунок 39

Состав элементов конфигурационного окна.

Кнопки управления:

- Add – нажатие этой кнопки открывает окно Add VPN Connection (Рисунок 40) для создания соединения VPN. После того, как созданы соединения со всеми интерфейсами, по нажатию этой кнопки будет открываться окно с текстом "New VPN connection cannot be created. All interfaces are used in other VPN connections."
- Delete – вызывает процедуру удаления выделенного VPN Connection

VPN Connections – таблица с набором созданных соединений VPN:

- Interface – имя сетевого интерфейса
- IPSec Policy – имя политики IPsec (имя набора криптографических карт), задействованной в данном соединении. Если соединение образовано на основе связи IPsec политики с набором динамических криптокарт, то в скобках указывается имя этого набора динамических криптокарт.

    - Seq No. – Sequence Number – порядковый номер криптографической карты в политике IPsec или номер набора динамических криптокарт, связанных с политикой IPsec. В последнем случае, в скобках указывается также номер динамической криптокарты в этом наборе.
  - Peers – список партнеров, при работе с которыми будет использоваться данная криптографическая карта
  - Transform Sets – список наборов преобразований, используемых криптографической картой для защиты трафика
  - IPSec Rule – номер или имя правила IPsec, на которое ссылается данная криптографическая карта
  - PFS – опция, включение которой усиливает защиту ключей (Enable|Disable) – Включена/Выключена
  - IKE CFG – имя пула адресов, из которого будет выделяться адреса по запросу партнеров. Возможные значения:
    - <none> – если у криптографической карты нет назначенного пула
    - {Pool Name} – имя пула адресов при явном назначении пула криптографической карте
    - {Pool Name}<effective> – это значение появляется для динамических криптокарт в случае, когда набор динамических криптокарт, у которых не задан пул адресов, связан с политикой IPsec, у которой указан пул адресов, помеченный как IOS pooll (общий пул). Это же значение – {Pool Name}<effective> будет отображаться, если описанная выше ситуация присутствует в действующей на шлюзе конфигурации. Pool Name – имя IOS пула в текущей конфигурации.
  - Identities – имя списка идентификаторов, которому должны удовлетворять сертификаты партнеров.

Общее количество строк таблицы:

```
TotalNum= NInterfaces1 * (NCryptoMaps1 + NdynamicTemplates1) +
          NInterfaces2 * (NCryptoMaps2 + NdynamicTemplates2) +...
      ...+NinterfacesM * (NcryptoMapsM + NdynamicTemplatesM),
```

где:

`NinterfacesX`	количество интерфейсов, связанных с IPSecPolicyX
`NcryptoMapsX`	количество криптографических карт (crypto map), входящих в IPSecPolicyX
`NdynamicTemplatesX`	количество crypto map, входящих в наборы динамических crypto map, связанных с IPSecPolicyX.

Строки в таблице формируются следующим образом:

- вначале, когда таблица пустая, есть возможность создания только нового VPN Connection. В зависимости от количества криптографических карт в политике IPsec для этого VPN соединения, в таблице будет формироваться соответствующее количество строк. Фактически, строка таблицы демонстрирует связку криптографической карты с интерфейсом.
- если политика IPsec связана с набором динамических криптографических карт, то в таблице будет формироваться количество строк, равное числу динамических криптографических карт в наборе.

- если в разделе IPSec Policies отредактировать состав входящих в политку IPsec криптографических карт, аналогичные изменения произойдут и в таблице VPN Connections – при добавлении крибптографических карт будут добавлены строки, а при удалении – удалены строки таблицы.
  При этом, если несколько интерфейсов используют одну и ту же политку IPsec, для каждого из них будет создана строка с добавленной криптографической картой.
  - аналогичное поведение таблицы будет и при удалении строки с криптографической картой. Если эта карта используется в политике IPsec, которую используют несколько интерфейсов, то будут удалены все строки, ссылающиеся на удаляемую криптографическую карту. Криптографическая карта может быть удалена из состава политики IPsec как в этом разделе, так и в разделе IPSec Policies (Crypto Map Sets). Удаление в этом разделе одной или нескольких криптографических карт из состава политики IPsec (а также удаление самой политики IPsec) приводит к удалению строк, ссылающихся на удаляемые объекты.
  - удаление через разрыв ассоциации с политикой IPsec приводит к удалению всех строк с именем интерфейса, которое было у удаляемой строки. В представлении Cisco под VPN Connection понимается связь интерфейса с политикой IPsec. Реализация же VPN Connection в таблице выполняется не в виде одной строки, а в виде нескольких строк – по числу криптографических карт, входящих в состав политики IPsec.

Создание нового соединения VPN

Создание нового соединения VPN выполняется в окне Add VPN Connection (Рисунок 40), которое открывается кнопкой Add:

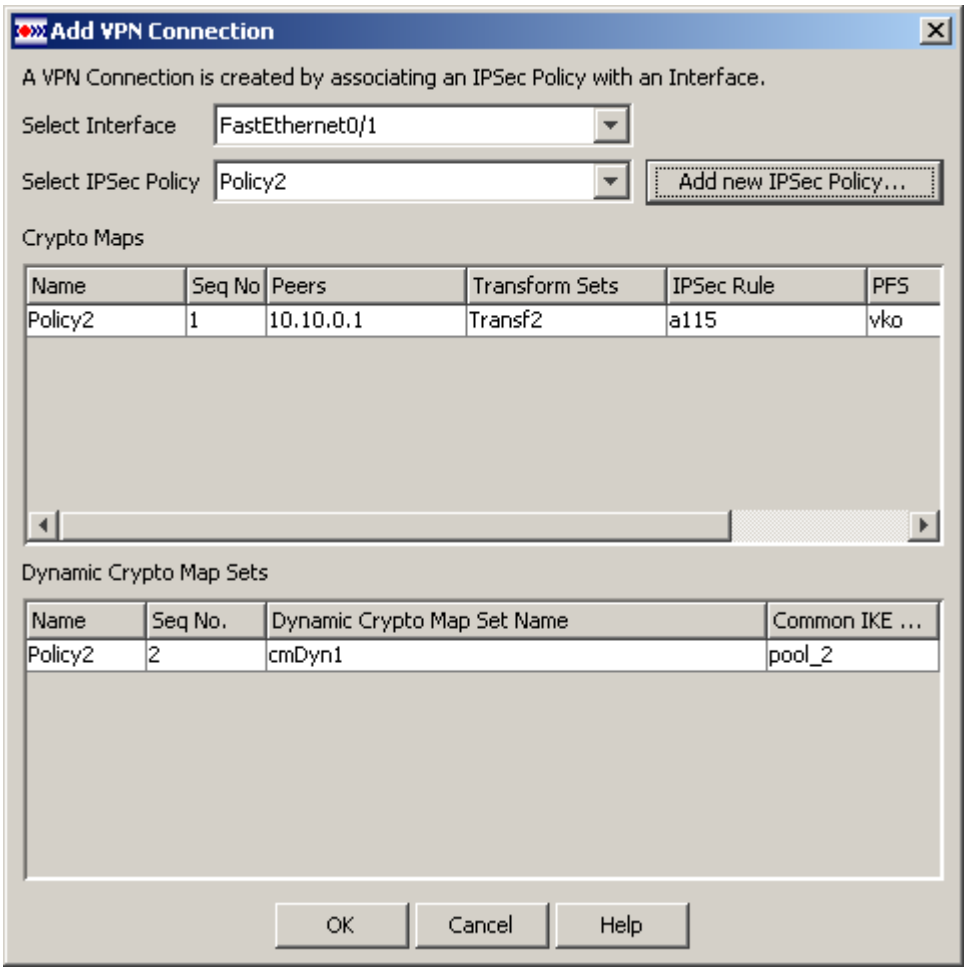

Рисунок 40

Создание нового VPN Connection заключается в связывании политики IPsec с интерфейсом. Для этого имеются следующие поля:

- Select Interface – выпадающий список физических интерфейсов, для которых еще не создавались соединения VPN
- Select IPSec Policy – выпадающий список созданных ранее политик IPsec.

Add new IPSec Policy – кнопка вызова диалога Add IPSec Policy (Рисунок 44) для создания новой политики IPsec.

- Crypto Maps – таблица отображает детали статических криптографических карт, входящих в состав выбранной IPsec Policy.
- Dynamic Crypto Map Sets – таблица показывает наборы динамических криптографических карт, которые связаны с выбранной политикой IPsec.

При выборе интерфейса и политики IPsec, и нажатии кнопки OK соединение VPN будет создано. В таблице VPN Connections (Рисунок 39) появится строка с новым созданным соединением VPN.

Удаление VPN Connection

Удаление выделенного VPN Connection производится с помощью кнопки Delete. Нажатие этой кнопки открывает окно Delete VPN Connection (Рисунок 41).

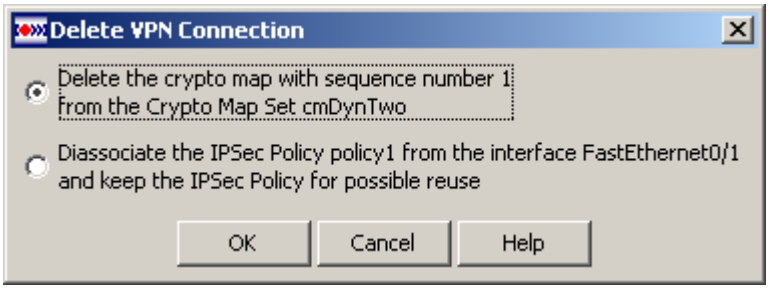

Рисунок 41

Окно содержит переключатель с двумя положениями:

- Delete the crypto map with sequence number {номер} from the Crypto Map Set {имя Crypto Map Set}. Выбор этого положения переключателя приводит к удалению указанной криптографической карты из набора криптокарт – политики IPsec.
- Disassociate the IPSec Policy {имя IPsec Policy} from the interface {имя интерфейса} and keep the IPSec Policy for possible reuse. Выбор этого положения переключателя приводит к удалению связи интерфейса и политики IPsec. При этом будут удалены все строки, ссылающиеся на криптографические карты из состава указанной политики IPsec, связанные с данным интерфейсом.

IPSec

Протокол IPsec используется для защиты передаваемых данных по сети, обеспечивая конфиденциальность, целостность и достоверность данных, передаваемых через недоверенные сети. Этот раздел включает три подраздела, в которых и определяются алгоритмы и параметры IPsec, которые будут использоваться для защиты трафика.

Данное окно (Рисунок 42) содержит только текст, поясняющий базовые термины.

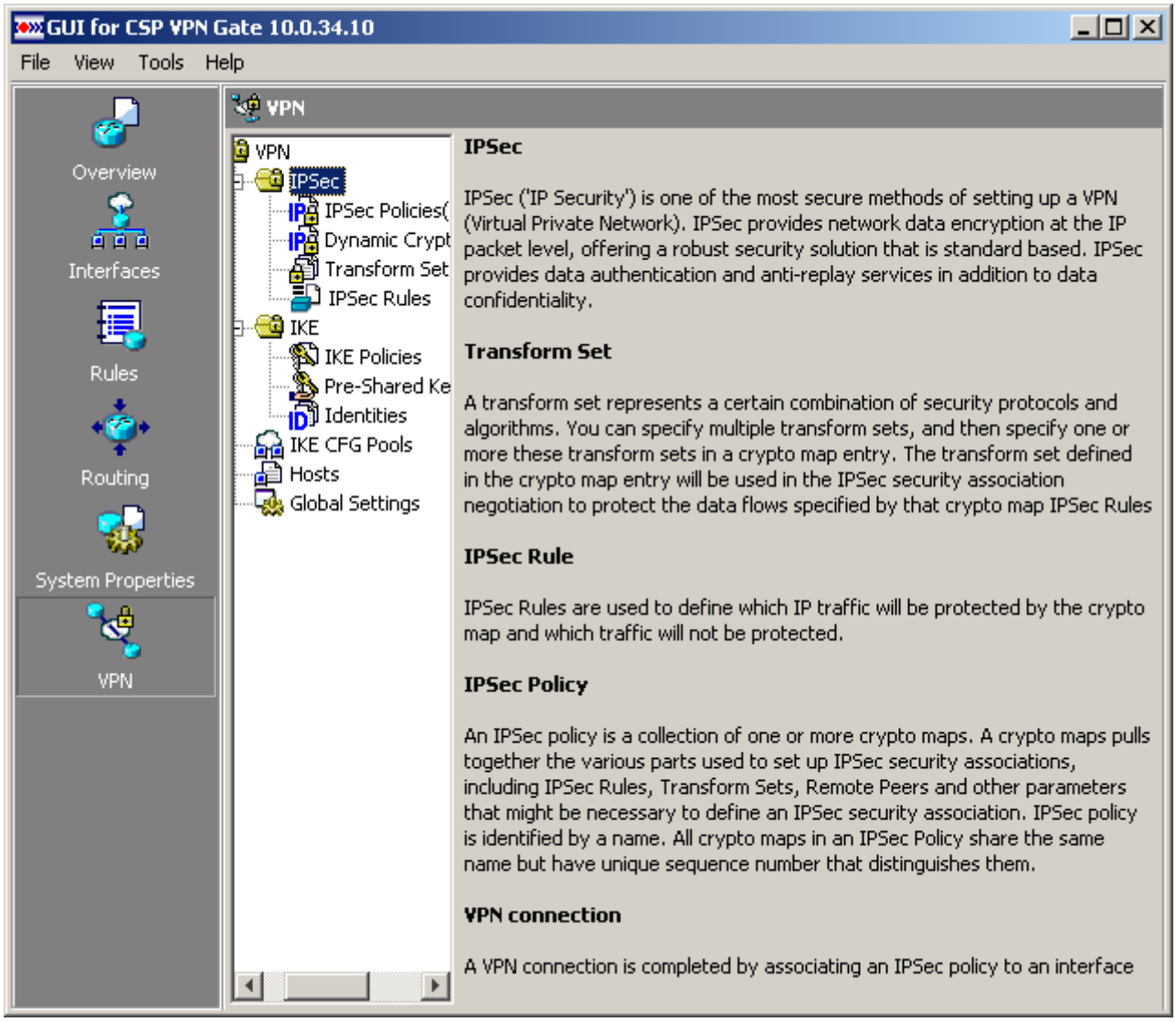

Рисунок 42

IPSec Policies

В разделе IPSec Policies (Рисунок 43) можно просматривать все созданные политики IPsec и интерфейсы, к которым привязаны эти политики. Здесь же можно вызывать окна для создания и редактирования политик IPsec, а также удалять эти политики. Политика IPsec – набор криптографических карт. В политику IPsec могут входить как статические криптографические карты, так и наборы динамических криптографических карт.

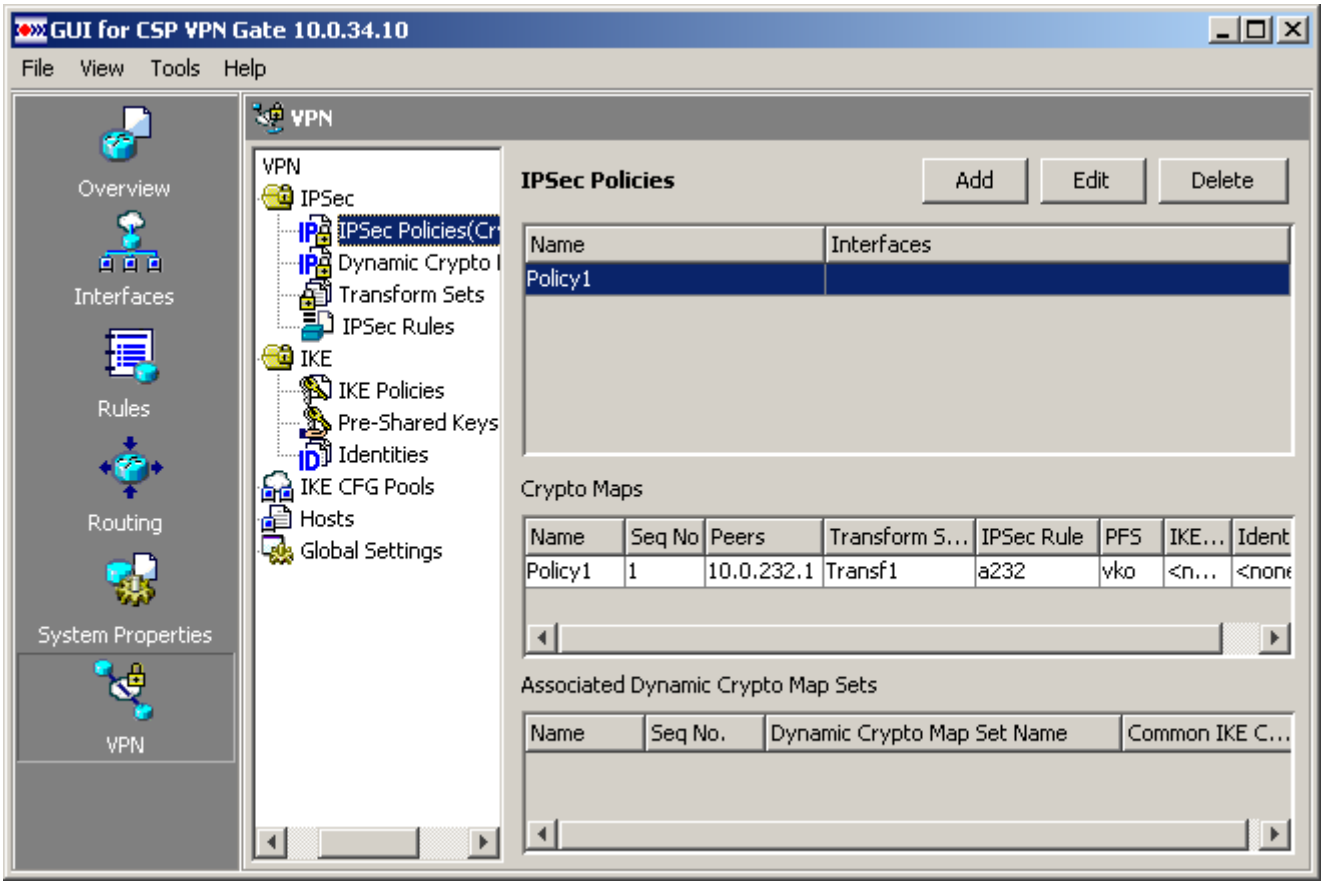

Рисунок 43

Главная форма этого раздела содержит три таблицы.

- Таблица IPSec Policies показывает созданные политики IPsec:
  - Name – имя политики IPsec,
  - Interfaces – имя интерфейса, к которому привязана данная политика IPsec. Если политика IPsec не связана с интерфейсом – поле не заполняется.
- Таблица Crypto Maps отображает детали криптографических карт, входящих в выделенную политику IPsec.
- Таблица Associated Dynamic Crypto Map Sets – показывает наборы динамических криптографических карт, входящие в выделенную политику IPsec.

Создание политики IPsec

Для создания политики IPsec необходимо наличие хотя бы одного Transform Sets и одного правила IPsec. Если нет ни одного трансформа и ни одного правила, то при нажатии кнопки Add для создания политики IPsec будет выдано сообщение о необходимости их создания.

Создание политики IPsec производится в окне Add IPSec Policy (Рисунок 44), которое открывается при нажатии кнопки Add в окне IPSec Policies (Рисунок 43):

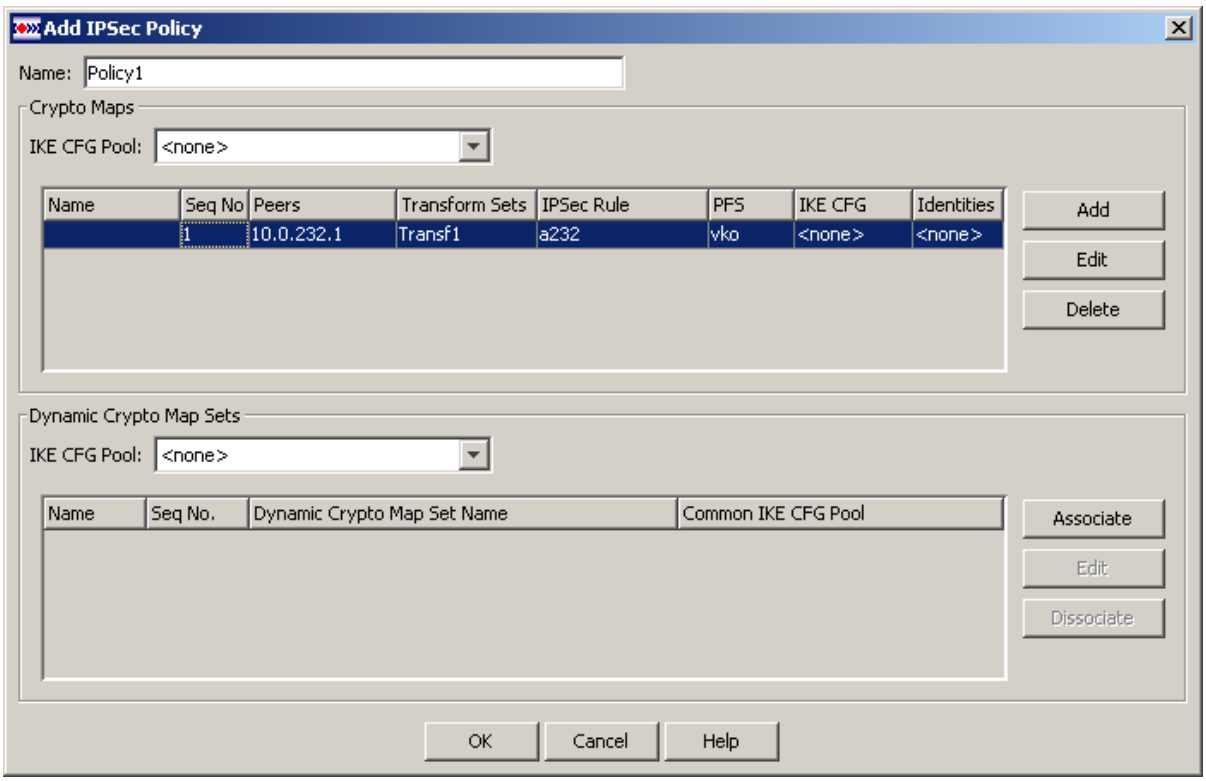

Рисунок 44

Состав элементов окна:

- Name – имя создаваемой политики IPsec
- Группа Crypto Maps
  - IKE CFG Pool – выпадающий список, позволяющий изменить IKE CFG пулы у всех записей в наборе статических криптографических карт.
    Список активен, если пулы всех привязанных криптокарт совпадают либо отсутствуют.
    В активном состоянии показывается значение списка, соответствующее привязанному IKE CFG пулу, или <none>, если у всех карт в наборе нет привязанного пула.
    В неактивном состоянии всегда показывается значение <none>.
  - Таблица со списком криптографических карт, входящих в создаваемую политику IPsec. Поля таблицы:
    - Name – имя политики IPsec
    - Seq No – порядковый номер криптографической карты (приоритет) в данной политике
    - Peers – список партнеров, обрабатываемый данной криптографической картой
    - Transform Sets – список преобразований, используемых данной криптографической картой для защиты трафика

- IPSec Rule – имя правила IPsec, на которое ссылается данная криптографическая карта
- PFS – опция, включение которой усиливает защиту ключей:
  - показывает выбранный алгоритм, который будет использоваться для генерации ключевого материала, если опция включена
  - пустое поле, если опция отключена.
- IKE CFG – имя пула адресов, из которого будет выделяться адрес по запросу партнеров. Возможные значения:
  - <none> – если у криптографической карты нет назначенного пула
  - {Pool Name} – при явном назначении пула криптографической карте.

  Если для данной криптографической карты был включен механизм Reverse Route Injection, то после имени пула адресов появится «+».
- Identities – имя списка идентификаторов, которому должны удовлетворять сертификаты партнеров.

Кнопки управления:

- Add – вызывает диалог Add Static CryptoMap (Рисунок 45) для создания статической криптографической карты
- Edit – вызывает диалог Edit Static CryptoMap (Рисунок 45) для редактирования выделенной статической криптографической карты, совпадающий с окном Add Static CryptoMap
- Delete – вызывает процедуру удаления выделенной криптографической карты

- Группа Dynamic Crypto Map Sets
  - IKE CFG Pool – выпадающий список, позволяющий изменить IKE CFG пулы у всех записей в наборе динамических криптографических карт. Список активен, если пулы всех привязанных криптокарт совпадают либо отсутствуют.
    В активном состоянии показывается значение списка, соответствующее привязанному IKE CFG пулу, или <none>, если у всех карт в наборе нет привязанного пула.
    В неактивном состоянии показывается значение <none>.
  - Таблица со списком наборов динамических криптографических карт, связанных с политикой IPsec. Поля таблицы:
    - Name – имя политики IPsec
    - Seq No – порядковый номер (приоритет) набора динамических криптографических карт в данной политике
    - Dynamic Crypto Map Set Name – имя набора динамических криптографических карт, связанного с политикой IPsec
    - Common IKE CFG Pool – показывает наличие одинакового пула адресов у всего набора динамических карт. Возможные значения:
      - {Pool Name} – имя пула адресов, если все карты в наборе используют одинаковый пул
      - <none> – если у всех карт в наборе нет привязанного пула
      - {Pool Name}<effective> – это значение появляется в случае, когда набор динамических криптокарт, у которых не задан пул адресов, связан с политикой IPsec, у которой указан пул адресов, помеченный как IOS pool (общий пул). Это же значение – {Pool Name}<effective> будет отображаться, если описанная выше ситуация присутствует в действующей на шлюзе конфигурации. Pool Name – имя IOS пула в текущей конфигурации.
      - <no common pool> – карты в наборе используют разные пулы адресов.

Кнопки управления:

- Associate – вызывает окно Associate Dynamic Crypto Map Set (Рисунок 54) для выбора набора динамических криптографических карт для связывания с политикой IPsec.
- Edit – кнопка доступна при выделении строки в таблице Dynamic Crypto Map Sets и вызывает окно Edit Dynamic Crypto Map Set Association для редактирования номера набора динамических криптокарт, связанного с политикой IPsec.
- Dissociate – кнопка доступна при выделении строки в таблице Dynamic Crypto Map Sets и удаляет связь между выделенным набором динамических криптокарт и политикой IPsec.

Создание статической криптографической карты

Нажатие кнопки Add (Рисунок 44) открывает окно Add Static CryptoMap (Рисунок 45) для создания статической криптографической карты. Это окно содержит шесть вкладок.

Вкладка General

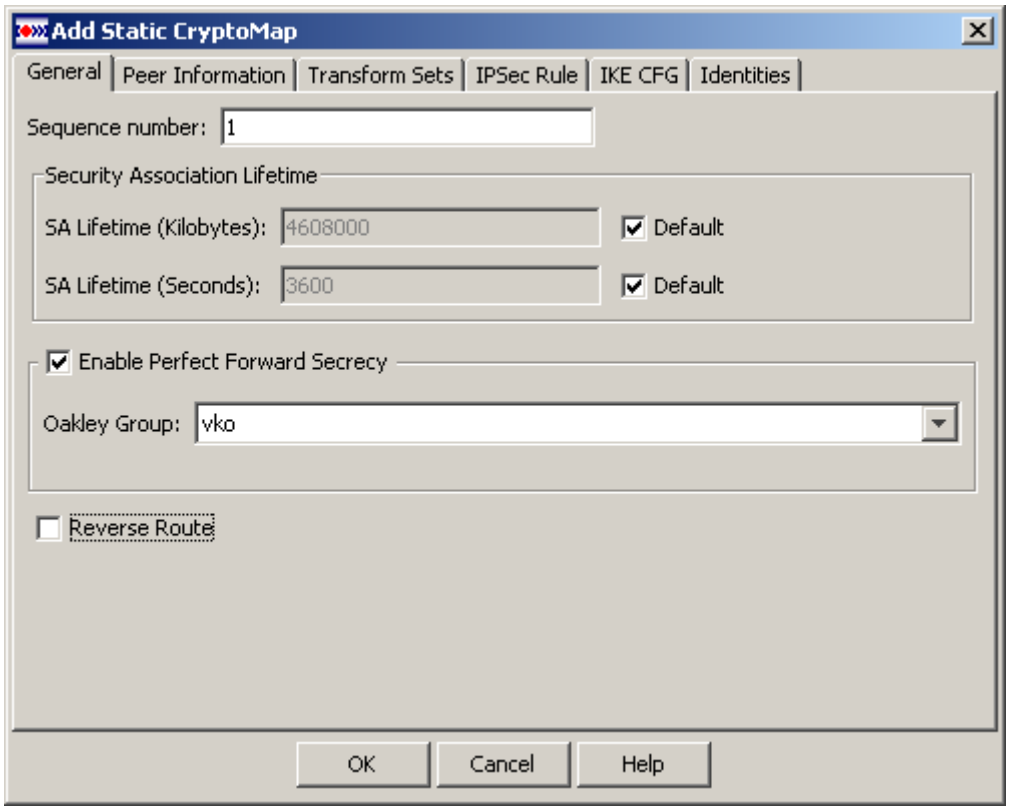

Рисунок 45

Вкладка General (Рисунок 45) содержит следующие элементы:

- Sequence Number – порядковый номер криптографической карты в политике IPsec. Порядковый номер показывает уровень приоритета карты в данной политике: чем меньше номер карты – тем выше приоритет. По умолчанию, при открытии окна это поле заполняется целым числом, которое на единицу превышает наибольшее значение криптографической карты, входящей в политику IPsec. Например, если IPsec Policy содержит криптографические карты с номерами 1, 2 и 8, то при добавлении новой криптографической карты в качестве Sequence Number будет предложено значение 9.

Однако, можно вручную исправить это значение на любое, не занятое (в нашем случае занятыми будут числа 1, 2 и 8) целое число из диапазона 1 – 65535.

- Группа Security Association Lifetime – содержит элементы настройки времени жизни SA:
  - SA Lifetime (Kilobytes) – предельный объем (в килобайтах) передаваемых данных сторонами, в результате превышения которого SA становится недействительным. Допустимые значения лежат в диапазоне от 1 до 4294967295.
    - Default – выставление этого флажка означает, что будет установлено время жизни SA по умолчанию – 4608000 килобайт. Это значение определяется в разделе Global Settings.
  - SA Lifetime (Seconds) – время жизни SA в секундах, по истечении которого связь становится недействительной. Допустимые значения лежат в диапазоне от 1 до 4294967295. Значение по умолчанию 3600.
    - Default – выставление этого флажка означает, что будет установлено время жизни SA по умолчанию – 3600 секунд. Это значение определяется в разделе Global Settings.
- Enable Perfect Forward Secrecy – флажок, установка которого включает опцию PFS. При включенной опции PFS при каждом согласовании новой SA будет производиться новый обмен ключами. Эта опция обеспечивает дополнительную защиту секретным ключам, хотя и снижает производительность системы:
  - Oakley group – производится выбор алгоритма для выработки ключевого материала:
    - vko – используется алгоритм VKO GOST R 34.10-2001 [RFC4357] (длина ключа 256 бит). Значение по умолчанию
    - group1 – используется алгоритм Diffie-Hellman (длина ключа 768 бит)
    - group2 – используется алгоритм Diffie-Hellman (длина ключа 1024 бит)
    - group5 – используется алгоритм Diffie-Hellman (длина ключа 1536 бит).
- Reverse Route – флажок, установка которого включает механизм RRI (Reverse Route Injection) для соединений, установленных с помощью данной криптографической карты. **Предупреждение:** недопустимо вручную изменять или удалять правила маршрутизации, которые автоматически формируются при использовании RRI. Более подробное описание применения RRI дано в документе «Использование RRI» (RRI.pdf)

Вкладка Peer Information

Во вкладке Peer Information (Рисунок 46) указываются партнеры по защищенному взаимодействию. Для одной криптографической карты можно определить несколько партнеров, которые располагаются в списке в порядке снижения приоритета. Сначала будет предпринята попытка установить соединение с первым партнером, потом со вторым и т.д.

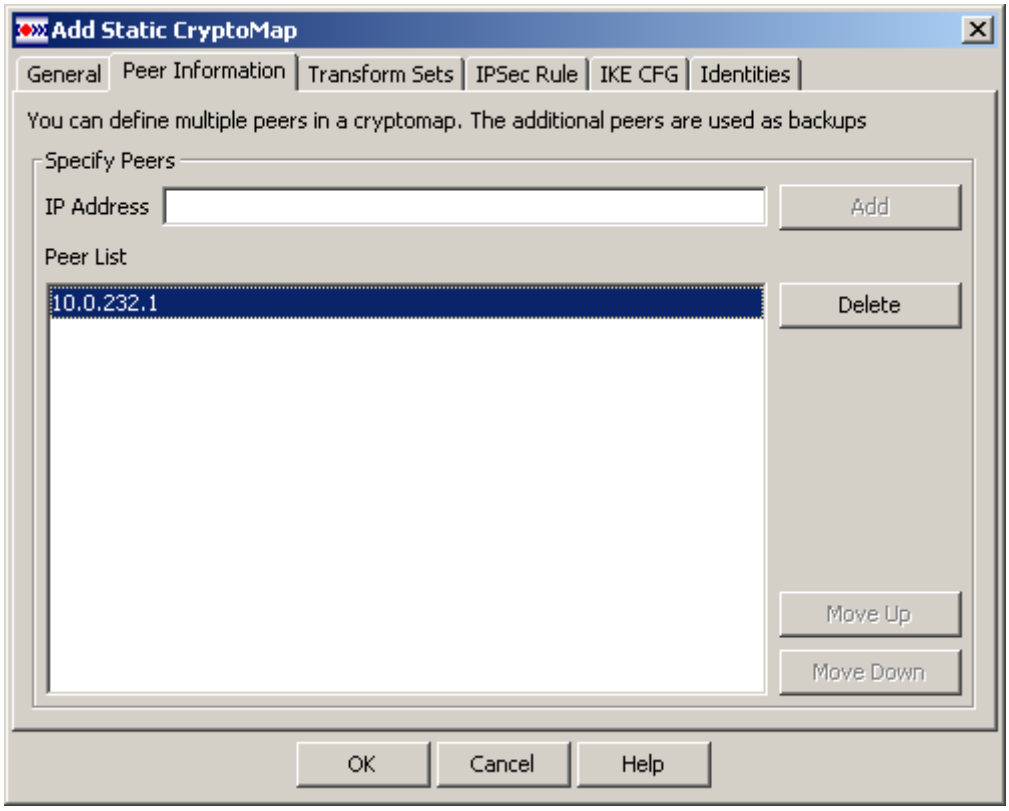

Рисунок 46

Вкладка Peer Information (Рисунок 46) содержит следующие элементы:

- Группа Specify Peers
  - IP Address – поле для ввода IP-адреса партнера для помещения его в список партнеров (Peer List). После того, как введенное значение перемещено в список при помощи кнопки Add, поле обнуляется
  - Peer List – список IP-адресов партнеров, которые нужно расположить в порядке снижения приоритета. Этот список не должен быть пустым.
- Кнопки управления:
  - Add – кнопка для перемешения введенного IP-адреса в список партнеров
  - Delete – кнопка удаления выделенного в списке IP-адреса. Если в списке ничего не выделено, кнопка блокируется.
  - Move UP – кнопка перемещения выделенного IP-адреса в списке на одну позицию вверх для увеличения приоритета. Если выделенной строкой является первая, то кнопка будет блокирована.
  - Move Down – кнопка перемещения выделенного IP-адреса в списке на одну позицию вниз для снижения приоритета. Если выделенной строкой является последняя, то кнопка будет блокирована.

Вкладка Transform Sets

Во вкладке Transform Sets (Рисунок 47) выбираются наборы преобразований для реализации политики защиты, которые будут использоваться данной криптографической картой.

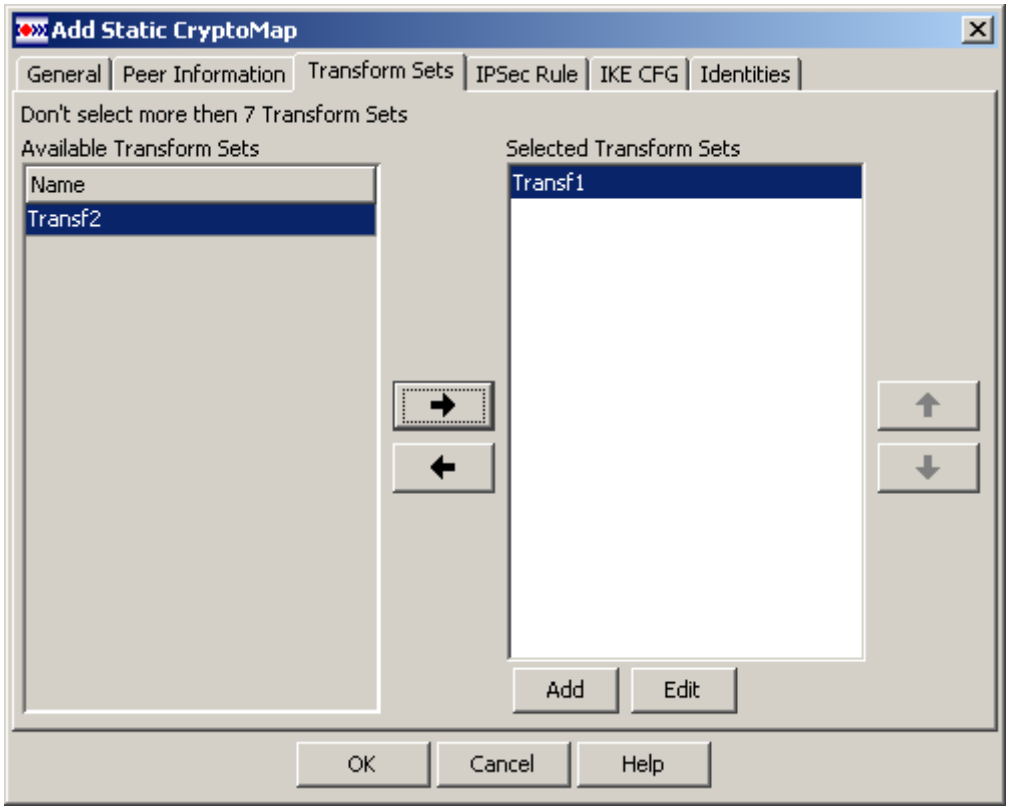

Рисунок 47

Вкладка содержит два поля:

- Available Transform Sets – поле со списком зарегистрированных наборов преобразований. При перемещении наборов преобразований в список Selected Transform Sets они удаляются из списка Available Transform Sets
- Selected Transform Sets – поле со списком наборов преобразований, которые используются данной криптографической картой. Может содержать только 7 наборов преобразований, при достижении этой границы кнопка перемещения в этот список и кнопка Add блокируются. Наборы преобразований должны быть размещены в порядке убывания приоритета – набор с наивысшим приоритетом следует указать первым. Этот список не должен быть пустым.

Кнопки управления:

- Add /Edit – кнопка вызова диалога Add/Edit Transform Set для создания/редактирования набора преобразований
-  – кнопка перемещения выделенного трансформа в списке Available Transform Sets в список Selected Transform Sets
-  – кнопка перемещения трансформа из списка Selected Transform Sets в список Available Transform Sets
-  – кнопка перемещения выделенной строки в списке Selected Transform Sets на одну позицию вверх для увеличения приоритета. Если выделенной строкой является первая, то кнопка будет блокирована
-  – кнопка перемещения выделенной строки в списке Selected Transform Sets на одну позицию вниз для снижения приоритета. Если выделенной строкой является последняя, то кнопка будет блокирована.

Вкладка IPSec Rule

Во вкладке IPSec Rule (Рисунок 48) выбирается правило, которое определяет IP-трафик, который следует или не следует шифровать средствами IPsec. Для шифрования будут использоваться преобразования, выбранные во вкладке Transform Sets.

Вкладка содержит только одно поле – выпадающий список правил IPsec. Значения списка следующие:

- none – правило еще не выбрано
- Use Rule Pane for selection – при выборе этого значения будет открыто окно Rule Pane (Рисунок 49) для выбора правила. Правило можно выбрать только расширенное как из раздела Access Rules, так и из раздела IPSec Rules. Если будет выбрано стандартное правило – кнопка Select будет блокирована и выбрать это правило будет невозможно. Примечание: в cs_console к криптографической карте можно привязать как стандартный, так и расширенный список доступа командой `match address`. Если загрузить конфигурацию с криптокартой и стандартным списком доступа в GUI, то она отобразится в GUI без проблем, несмотря на то, что такую привязку в GUI создать нельзя
- Create new – открывает окно Add a Rule для создания правила IPsec (Рисунок 24), описанное в разделе "Создание нового правила IPsec".

Правило обязательно должно быть выбрано, значение none не допускается.

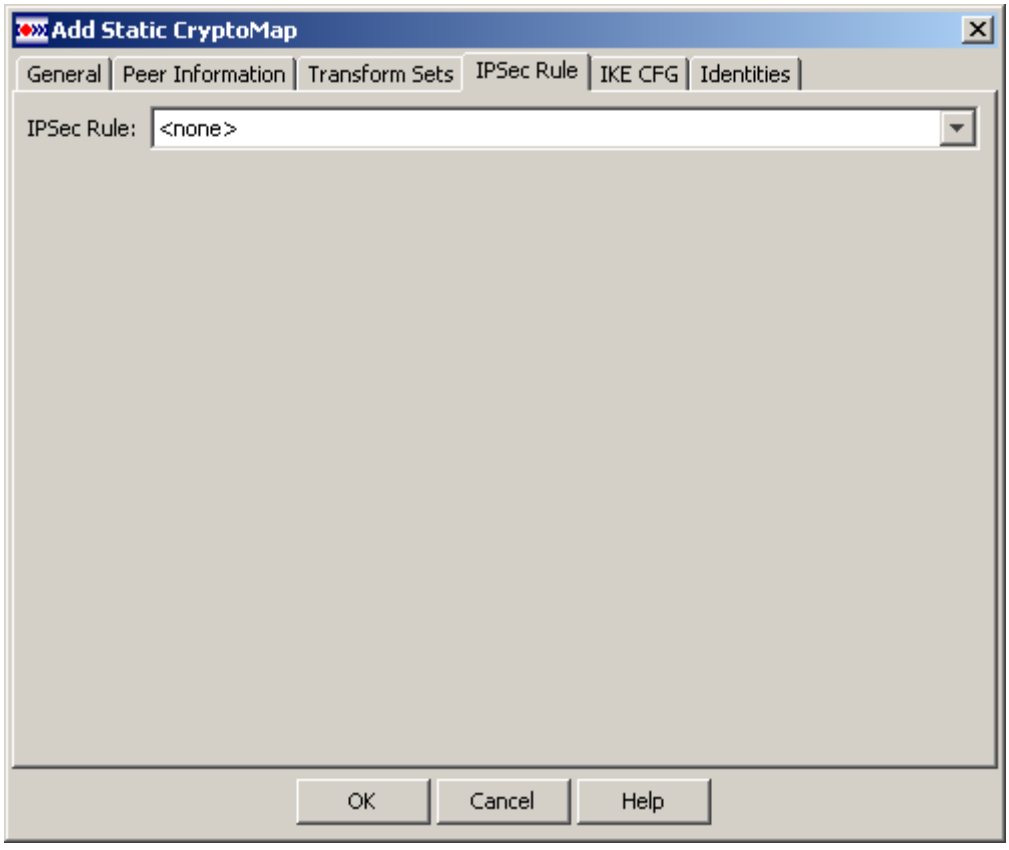

Рисунок 48

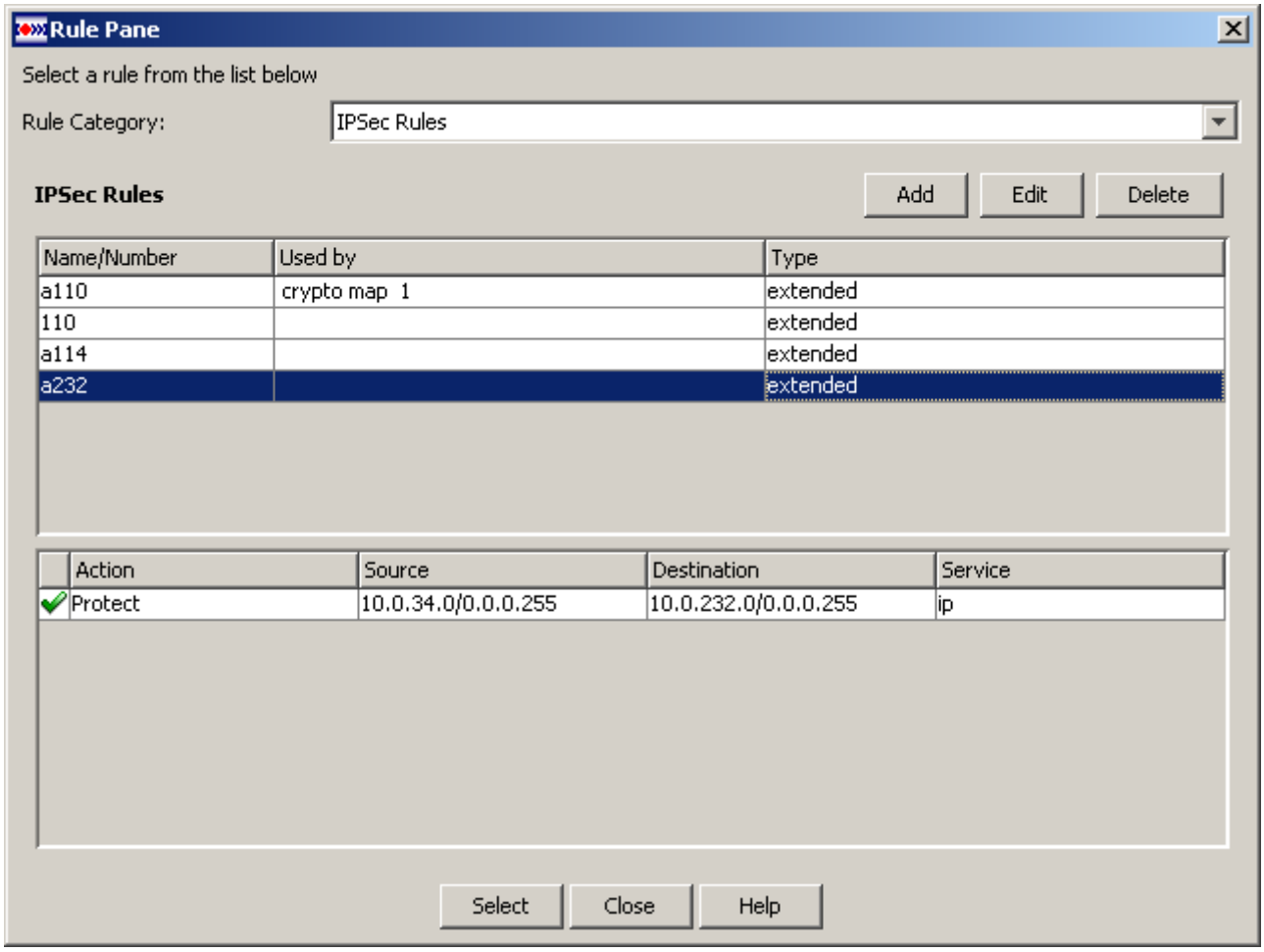

Рисунок 49

При выделении нужного правила в окне Rule Pane (Рисунок 49) и нажатии кнопки Select выбранное правило появится во вкладке IPSec Rule.

Вкладка IKE CFG

Вкладка IKE CFG (Рисунок 50) используется в основном в динамической криптографической карте для выбора пула адресов, из которого будут выделяться адреса для партнеров.

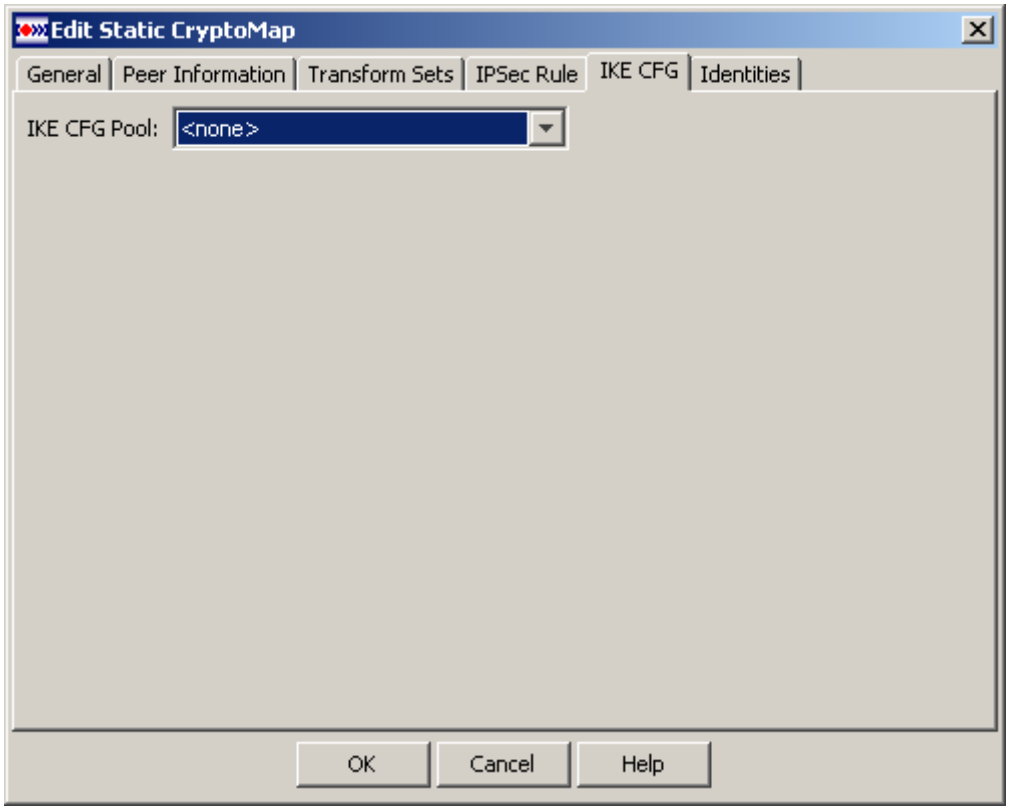

Рисунок 50

Вкладка содержит следующие элементы:

- IKE CFG Pool – выпадающий список:
  - <none> – специальное значение означающее, что пул адресов не задан (т.е. данная криптокарта никакой пул не использует).
    В случае если другие карты в наборе используют IOS pooll (общий пул), то при установке значения <none>, в cisco-like конфигурации для данной криптокарты будет задана команда `set pool <none>`, означающая, что заданный общий пул адресов игнорируется
  - Use IKE CFG Pool Pane for selection – при выборе этого предложения будет открыто окно IKE CFG Pool Pane для выбора пула адресов (Рисунок 51)
  - Create new – открывается окно Add IKE CFG Pool для создания нового пула адресов (Рисунок 74)

Кроме того, выпадающий список хранит в памяти имя последнего выбранного пула до завершения сессии редактирования параметров криптографической карты.

Окно выбора IKE CFG пула

Окно выбора пула IKE CFG Pool Pane состоит из двух таблиц:

- верхняя таблица содержит все созданные пулы адресов и имеет элементы:
  - Name – имя пула адресов
  - Crypto Maps – имена криптографических карт, использующих данный пул. Имя криптографической карты выводится в формате crypto map <имя политики IPsec>|<имя набора динамических криптографических карт> <Sequence number>
- нижняя таблица показывает диапазон адресов выделенного пула в верхней таблице.

Окно IKE CFG Pool Pane содержит функциональные кнопки Add, Edit и Delete для вызова диалогов создания, редактирования и удаления IKE CFG пула, описанных в разделе "IKECFG Pools".

Двойной щелчок на выделенном пуле или нажатие кнопки Select закрывает окно, и пул считается выбранным

.

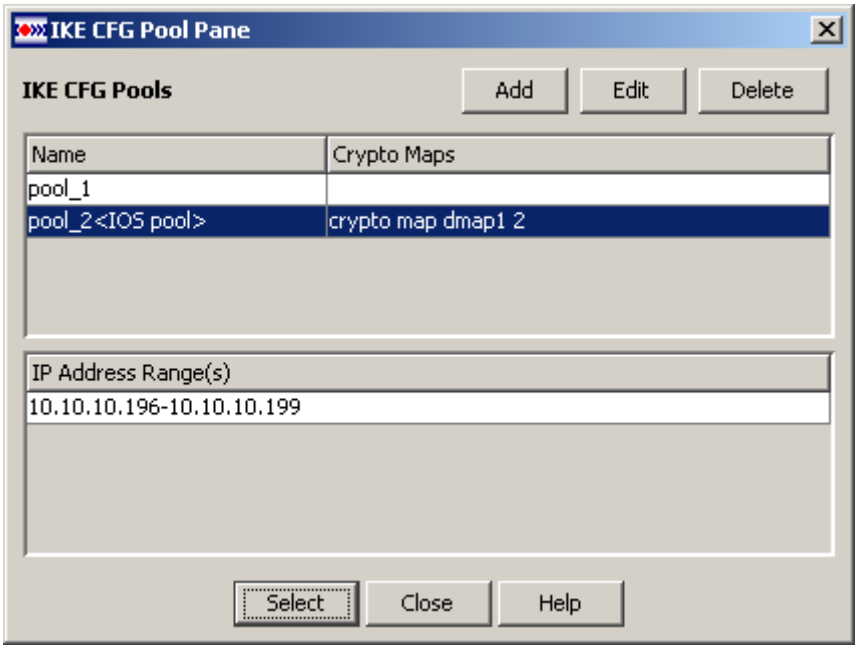

Рисунок 51

Вкладка Identities

Во вкладке Identities (Рисунок 52) можно указать список идентификаторов, которому должны удовлетворять сертификаты партнеров. Эта вкладка необязательна для заполнения. Списки идентификаторов создаются в разделе Identities. Вкладка содержит только одно поле Identity List с выпадающим списком значений:

- none – установлено по умолчанию
- Use Identity List Pane for selection – при выборе этого значения будет открыто окно Identity List Pane (Рисунок 53) для выбора списка идентификаторов
- Create new – вызывает диалог Add Identity List (Рисунок 71) для создания нового списка идентификаторов, описанный в разделе "Создание нового списка идентификаторов".

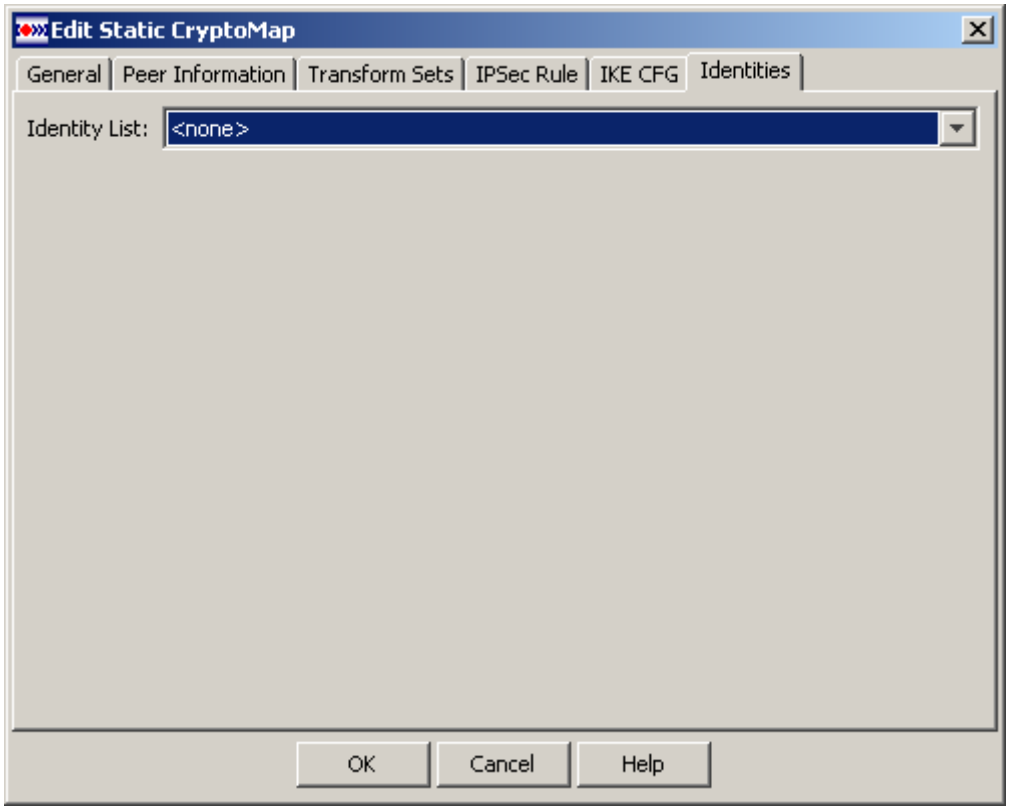

Рисунок 52

Окно выбора идентификаторов

Окно Identity List Pane (Рисунок 53) состоит из двух таблиц, полностью совпадающих с аналогичными таблицами раздела Identities.

Выделите нужный список идентификаторов и нажмите кнопку Select, список идентификаторов будет выбран. Окно Identity Pane имеет функциональные кнопки для создания, редактирования и удаления списков идентификаторов.

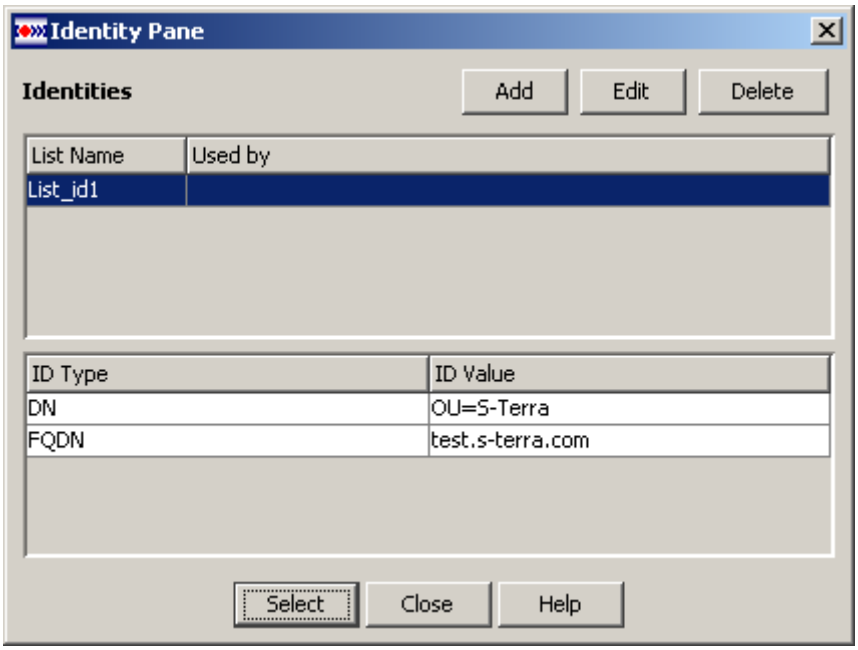

Рисунок 53

После заполнения всех вкладок окна Add Static CryptoMap (Рисунок 45) и нажатии кнопки OK, статическая криптографическая карта будет создана и в окне Add IPSec Policy (Рисунок 44) в таблице Crypto Maps появится строка с созданной криптокартой.

Редактирование криптографической карты

Редактирование выделенной криптографической карты в окне Add IPSec Policy (Рисунок 44) производится в окне Edit Static CryptoMap, которое вызывается кнопкой Edit. Окно редактирования полностью совпадает с окном создания новой криптографической карты данного типа и все параметры в этом окне заполнены значениями выделенной криптографической карты. Редактирование криптографической карты, не привязанной к интерфейсу, происходит также. Как правило, сообщения об ошибках возникают, если очистить список Peers или же очистить поле IPSec Rule. Эти поля обязательны к заполнению.

Удаление криптографической карты

Удаление выделенной криптографической карты в таблице в окне Add IPSec Policy (Рисунок 44) производится с помощью кнопки Delete. Нажатие этой кнопки открывает окно с требованием подтверждения процедуры удаления. После получения подтверждения, криптографическая карта будет удалена. Если удаляемая криптографическая карта была задействована в VPN Connection, то будет удалена и соответствующая ей строка (или строки) в таблице VPN Connection.

Связывание с набором динамических криптокарт (Associate)

При нажатии кнопки Associate в окне Add IPSec Policy (Рисунок 44) вызывается диалог Associate Dynamic Crypto Map Set (Рисунок 54). В этом окне можно создать связь между политикой IPsec и одним из наборов динамических криптографических карт, созданных в разделе Crypto Dynamic Map Sets. Возможен также вызов диалога для создания нового динамического набора карт.

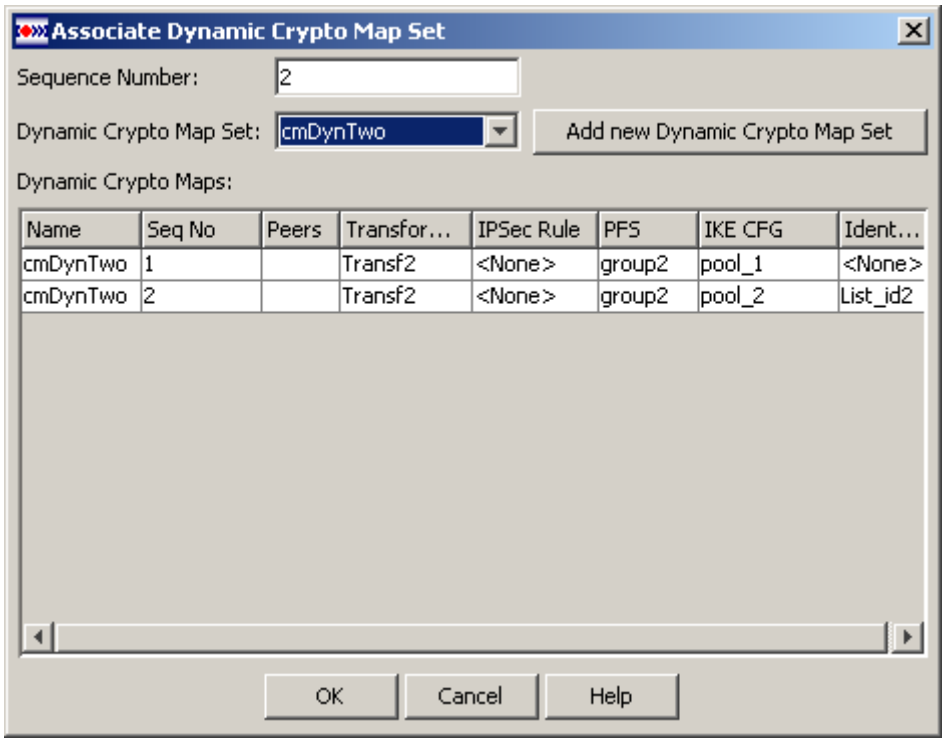

Рисунок 54

Состав элементов окна:

- Sequence Number – порядковый номер, который присваивается набору динамических криптографических карт в составе политики IPsec. Порядковый номер показывает уровень приоритета в данной политике: чем меньше номер – тем выше приоритет. При открытии окна это поле не заполняется автоматически. Его нужно заполнить вручную целым числом, которое не совпадает с уже существующими номерами. Например, политика IPsec содержит криптографические карты с номерами 1, 2 и 8, то вручную можно внести любое, не занятое (в нашем случае занятыми будут числа 1, 2 и 8) целое число из диапазона 1 – 65535. Рекомендуется для набора динамических карт, назначить порядковый номер больший, чем используемые номера других статических карт.
- Dynamic Cypto Map Set – выпадающий список наборов созданных динамических криптографических карт, которые не связаны с политикой IPsec. Если свободных динамических наборов нет, то выпадающий список показывает значение <none>. Выбранный набор динамических карт будет связываться с политикой IPsec.
- Dynamic Cypto Maps – таблица отображает детали динамических криптографических карт, входящих в выделенный набор динамических криптокарт. Таблица доступна только на чтение и не имеет элементов управления.

Add new Dynamic Cypto Map Set – кнопка вызывает диалог Add Dynamic Cypto Map Set (Рисунок 56) для создания нового набора динамических криптографических карт.

Редактирование связи

Нажатие кнопки Edit в окне Add IPSec Policy (Рисунок 44) при выделенной строке в таблице Dynamic Crypto Map Sets вызывает диалог Edit Dynamic Crypto Map Set Association, совпадающий с окном Associate Dynamic Crypto Map Set (Рисунок 54). Для редактирования доступно только поле с номером криптографической карты в политике IPsec, связанной с набором динамических карт. Остальные поля блокируются.

Устранение связи с набором динамических криптокарт (Dissociate)

Нажатие кнопки Dissociate в окне Add IPSec Policy (Рисунок 44) при выделенной строке в таблице Dynamic Crypto Map Sets удаляет выделенную криптографическую карту из политики IPsec, связанную с набором динамических криптокарт. Удаление происходит без предупреждения.

Редактирование IPsec Policy

Редактирование выделенной политики IPsec в таблице IPSec Policy (Рисунок 43) производится в окне Edit IPSec Policy (Рисунок 44), вызываемом кнопкой Edit. Окно Edit IPSec Policy полностью совпадает с окном создания Add IPSec Policy.

Процедуры создания, редактирования и удаления криптографической карты из политики IPsec полностью совпадают с процедурами, описанными в разделе "Создание IPsec Policy".

Удаление IPsec Policy

Процедура удаления выделенной политики IPsec в таблице IPSec Policies (Рисунок 43) вызывается кнопкой Delete. После нажатия кнопки Delete будет открыто окно с требованием подтверждения операции удаления. После получения подтверждения выделенная строка будет удалена из таблицы. Если удаляемая IPsec Policy связана с интерфейсом, то после получения подтверждения на удаление будут также удалены и все VPN соединения, связанные с политикой IPsec.

Dynamic Crypto Map Sets

В этом разделе можно просматривать созданные наборы динамических криптографических карт, вызывать окна для создания и редактирования наборов карт, а также удалять эти наборы. Динамические криптокарты используются для создания защищенных соединений с теми партнерами, адрес которых заранее неизвестен, например, с мобильными пользователями. По запросу таких партнеров будет выдаваться адрес из IKECFG пула шлюза безопасности.

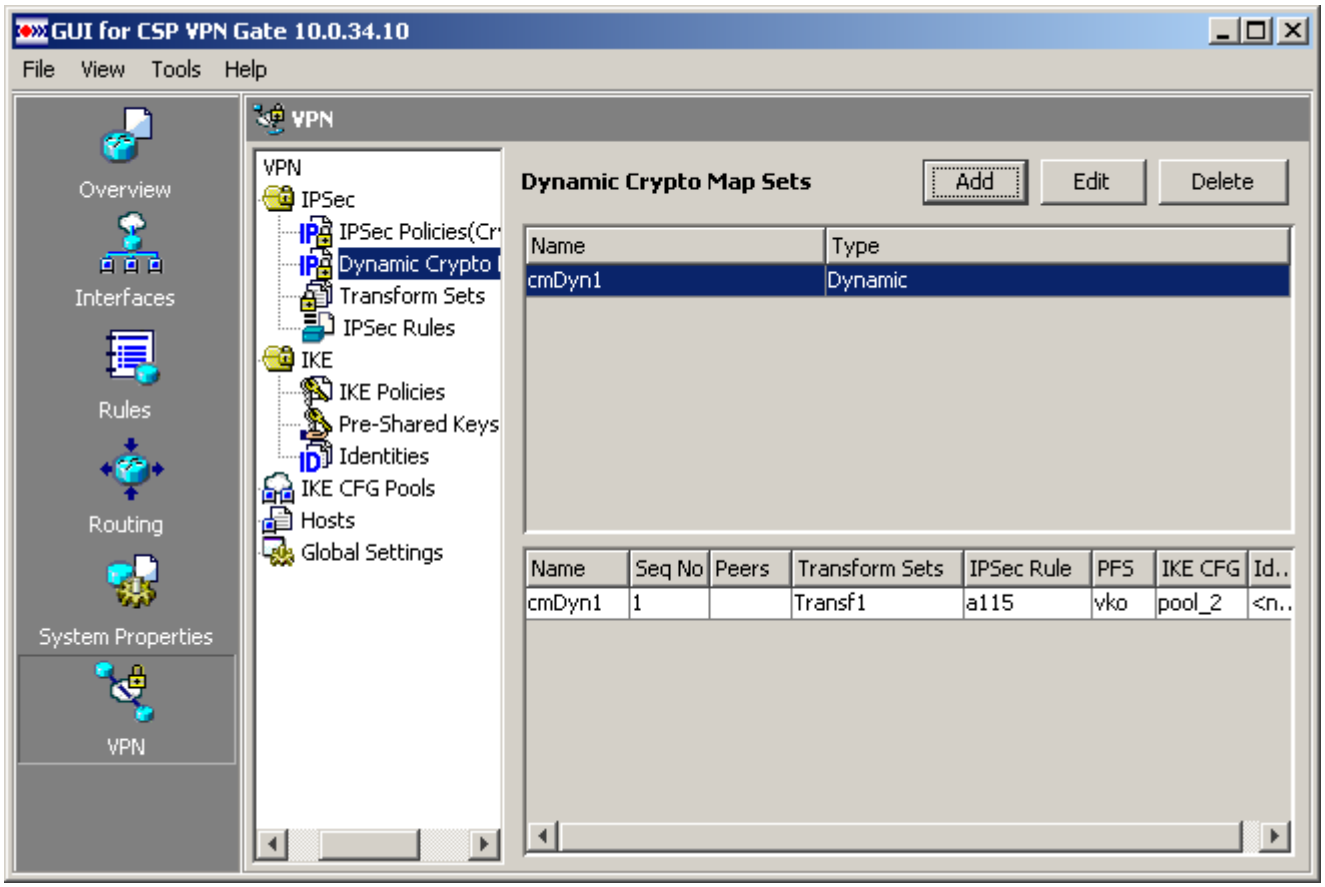

Рисунок 55

Главная форма этого раздела содержит две таблицы.

- Верхняя таблица показывает созданные наборы динамических криптографических карт:
  - Name – имя набора динамических криптографических карт
  - Type – тип набора криптографических карт – динамический
- Нижняя таблица отображает детали криптографических карт, входящих в выделенный набор динамических криптокарт.

Создание набора динамических криптокарт

Для создания набора динамических криптографических карт используется диалог Add Dynamic Crypto Map Set (Рисунок 56), который вызывается кнопкой Add в окне Dynamic Crypto Map Sets (Рисунок 55).

Для создания набора динамических криптокарт необходимо наличие хотя бы одного Transform Sets. Если нет ни одного трансформа, то при нажатии кнопки Add для создания криптокарты в наборе будет выдано сообщение о необходимости его создания.

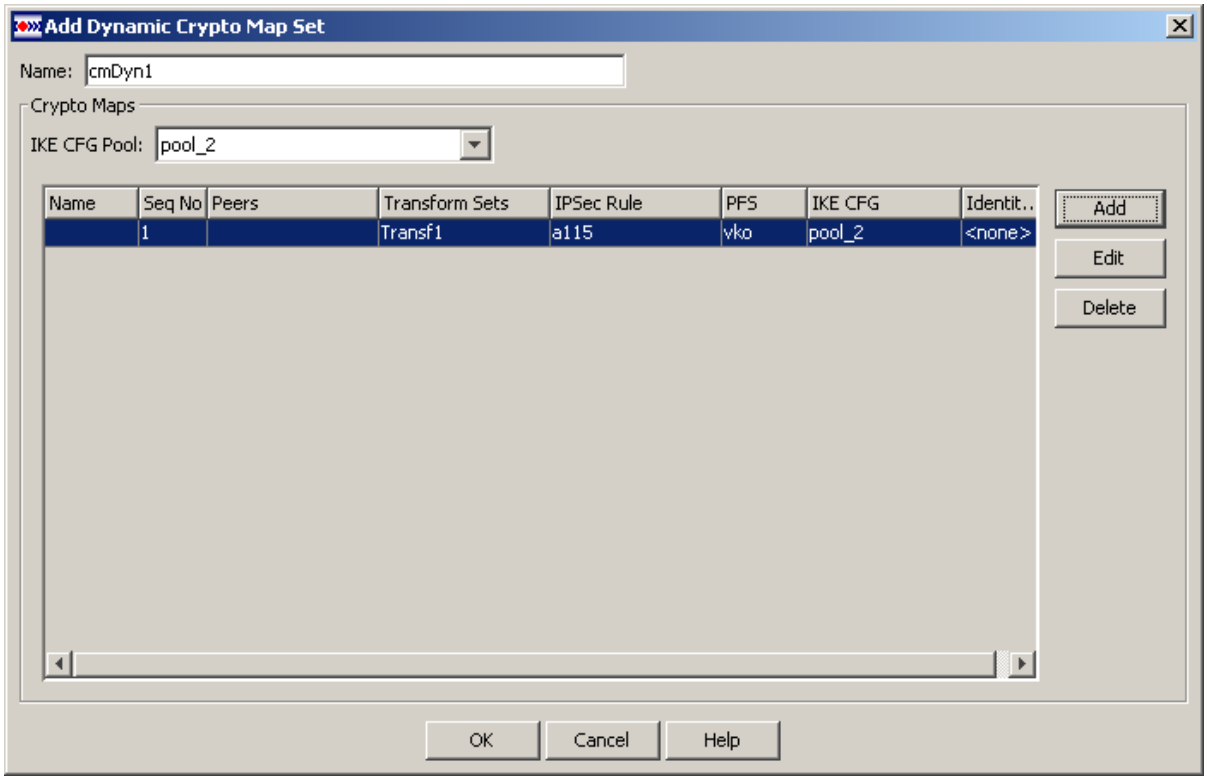

Рисунок 56

Состав элементов окна:

- Name –имя набора динамических криптографических карт
- Crypto Maps – таблица со списком динамических криптографических карт, входящих в создаваемый набор динамических криптокарт. Поля таблицы:
  - Name – имя набора динамических криптографических карт, заполняется автоматически после нажатия кнопки ОК
  - Seq No – порядковый номер криптографической карты (приоритет) в наборе
  - Peers – список партнеров для динамической карты не заполняется
  - Transform Sets – список преобразований, используемых данной криптографической картой для защиты трафика
  - IPSec Rule – имя правила IPsec, на которое ссылается данная криптографическая карта
  - PFS – опция, включение которой усиливает защиту ключей:
    - показывает выбранный алгоритм, который будет использоваться для генерации ключевого материала, если опция включена
    - пустое поле – если опция отключена

- IKE CFG – показывает выбранный пул адресов
- Identities – имя списка идентификаторов, которому должны удовлетворять сертификаты партнеров

Кнопки управления:

- Add – вызывает диалог Add Dynamic CryptoMap (Рисунок 57) для создания динамической криптографической карты в наборе
- Edit – вызывает диалог Edit Dynamic CryptoMap для редактирования выделенной динамической криптографической карты, совпадающий с окном Add Dynamic CryptoMap
- Delete – вызывает процедуру удаления выделенной криптографической карты в наборе динамических криптокарт.

Создание динамической криптографической карты

Нажатие кнопки Add (Рисунок 56) открывает окно Add Dynamic Crypto Map (Рисунок 57) для создания динамической криптографической карты. Это окно содержит шесть вкладок.

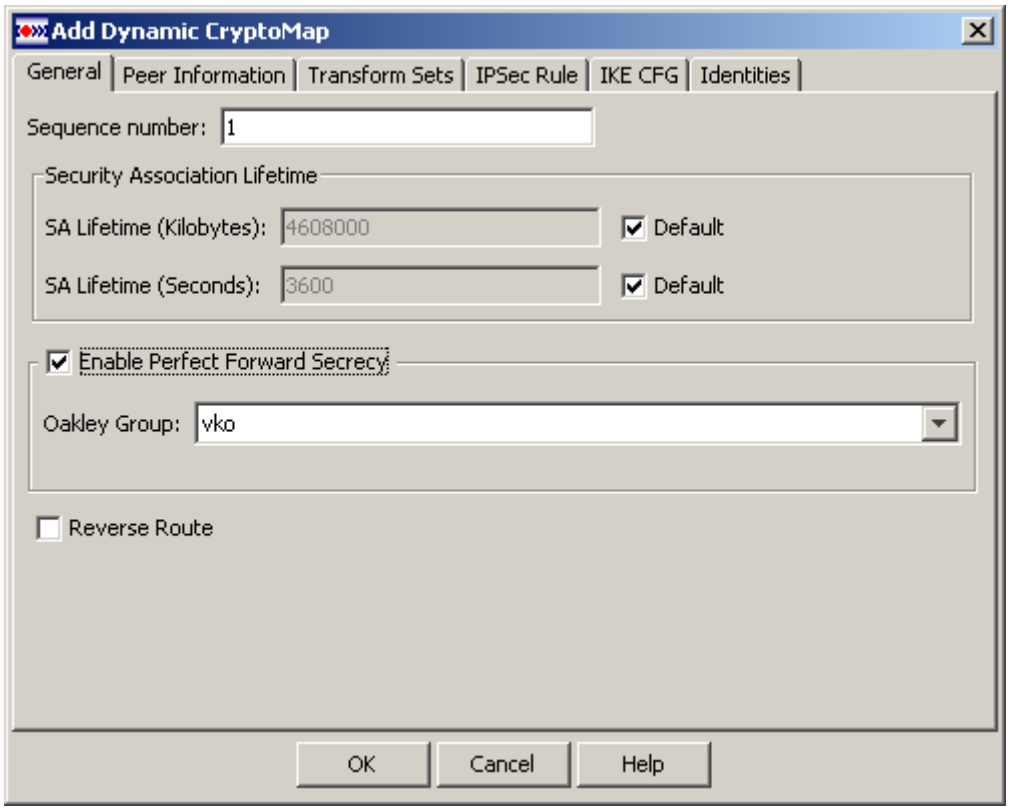

Рисунок 57

Вкладки диалога Add Dynamic CryptoMap полностью совпадают со вкладками при создании статической криптокарты (Рисунок 45), за исключением вкладки Peer Information и IPSec Rule. Вкладка Peer Information обычно не заполняется, потому что заранее неизвестны адреса партнеров. Во вкладке IPSec Rule допускается не указывать правило (выбрать значение none), в этом случае весь трафик будет шифроваться.

Редактирование динамической криптокарты

Для выделенной криптокарты при нажатии кнопки Edit в окне Add Dynamic Crypto Map Set (Рисунок 56) вызывается диалог Edit Dynamic Crypto Map, который совпадает с диалогом Add Dynamic Crypto Map. В этом окне все вкладки заполнены значениями выделенной криптографической карты, которые можно редактировать. Редактирование криптографической карты, не привязанной к интерфейсу, происходит также.

Удаление динамической криптокарты

Выделенная криптокарта в окне Add Dynamic Crypto Map Set (Рисунок 56) при нажатии кнопки Delete удаляется с требованием подтверждения процедуры удаления.

Редактирование набора динамических криптокарт

Редактирование выделенного набора динамических криптокарт окне Dynamic Crypto Map Sets (Рисунок 55) производится в окне Edit Dynamic Crypto Map Set, вызываемом кнопкой Edit. Окно Edit Dynamic Crypto Map Set совпадает с окном Add Dynamic Crypto Map Set. (Рисунок 56).

Удаление набора динамических криптокарт

При удалении выделенного набора динамических криптокарт кнопкой Delete (Рисунок 55) в окне Dynamic Crypto Map Sets открывается окно с требованием подтверждения операции удаления. После получения подтверждения выделенная строка будет удалена из таблицы. Если удаляемый набор криптокарт связан с политикой IPsec, то сначала нужно удалить эту связь, а затем уже удалить выбранный набор динамических карт.

Transform Sets

В этом разделе (Рисунок 58) просматриваются, создаются, редактируются и удаляются наборы преобразований, которые используются криптографической картой для защиты соединений. Набор преобразований – это комбинация наборов преобразований IPsec, реализующих политику защиты для определенного трафика. Во время IKE SA происходит согласование набора преобразований, который будет использоваться для защиты.

Главная форма в этом разделе содержит одну таблицу с созданными наборами преобразований, каждый из которых состоит из следующих элементов:

- Name – имя набора преобразований
- ESP Encryption – алгоритм шифрования
- ESP Integrity – алгоритм проверки целостности данных для протокола ESP
- AH Integrity – алгоритм проверки целостности данных для протокола AH
- Mode – режим использования протокола ESP (транспортный или туннельный).

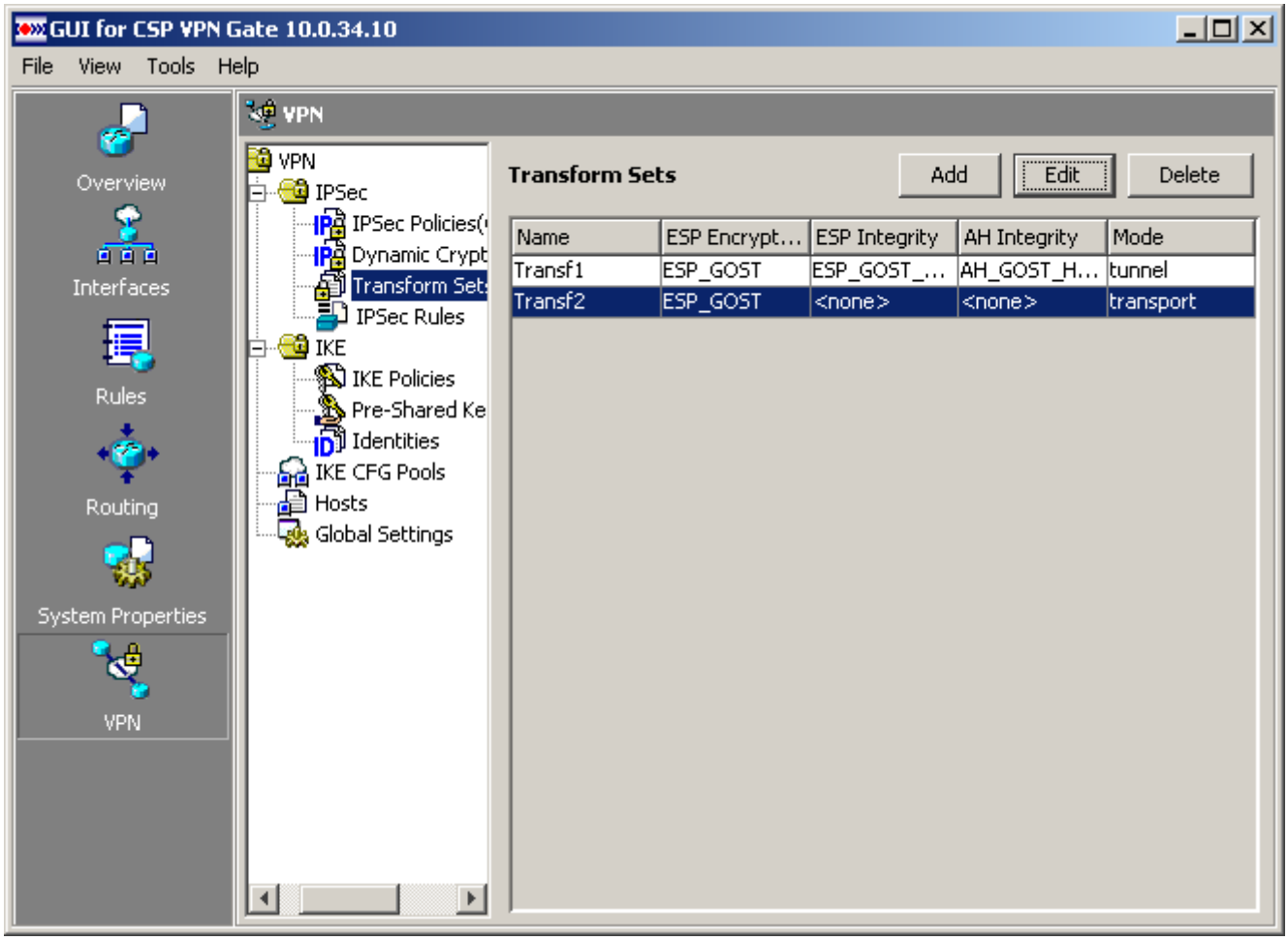

Рисунок 58

Создание нового Transform Set

Нажатие кнопки Add в окне Transform Set (Рисунок 59) открывает окно создания набора преобразований. Для обеспечения аутентификации и целостности данных выбираются алгоритмы для протокола AH, а для обеспечения шифрования и целостности данных выбираются алгоритмы для протокола ESP.

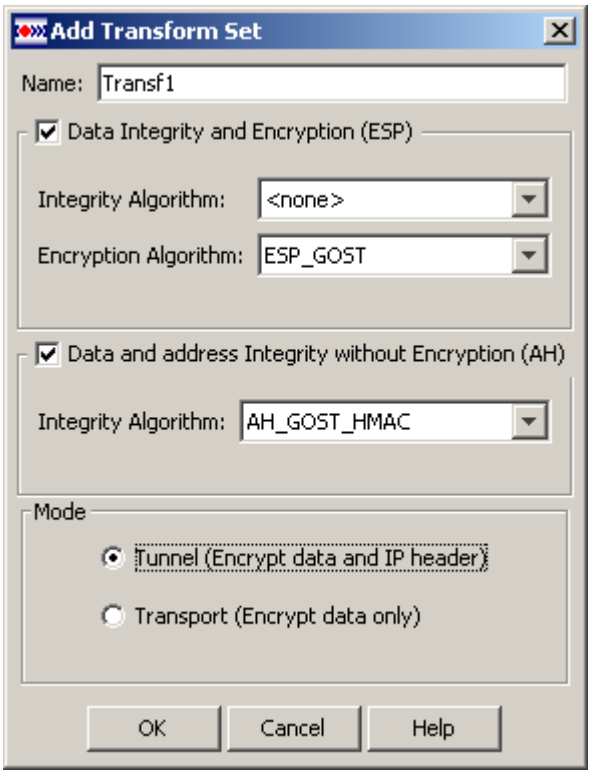

Рисунок 59

Окно состоит из следующих элементов:

- Name – имя создаваемого набора преобразований
- Группа Data Integrity and Encryption (ESP):
  - Флажок на группе – отвечает за активацию элементов группы
  - Integrity Algorithm –выпадающий список предустановленных алгоритмов проверки целостности данных для протокола ESP (см. раздел "Список поддерживаемых криптографических алгоритмов"). Список также содержит значение <None>, которое показывается в списке при открытии окна создания нового трансформа
  - Encryption Algorithm – выпадающий список предустановленных алгоритмов шифрования для протокола ESP (см. раздел "Список поддерживаемых криптографических алгоритмов"). Список также содержит значение <None>. Не допускается комбинация ESP_Null алгоритма и <None> для ESP Integrity алгоритма.
- Группа Data and address Integrity without Encryption (AH):
  - Флажок на группе – отвечает за активацию элементов группы
  - Integrity Algorithm – выпадающий список предустановленных алгоритмов проверки целостности для протокола AH (см.раздел "Список поддерживаемых криптографических алгоритмов"). По умолчанию устанавливается алгоритм AH_GOST_HMAC. При использовании NAT не активируйте эту группу.
- Группа Mode содержит переключатель с двумя положениями:
  - Tunnel (Encrypt data and IP header) – устанавливается туннельный режим использования протокола ESP
  - Transport (Encrypt data only) – устанавливается транспортный режим использования протокола ESP.

Редактирование Transform Set

Для редактирования выделенного набора преобразований в таблице Transform Sets используется кнопка Edit для вызова окна редактирования Edit Transform Set (Рисунок 60). Окно по составу элементов совпадает с окном создания нового набора преобразований, за исключением поля Name, которое иногда является блокированным. Для набора преобразований, который не задействован в IPsec Rules, поле Name не блокируется и его можно отредактировать.

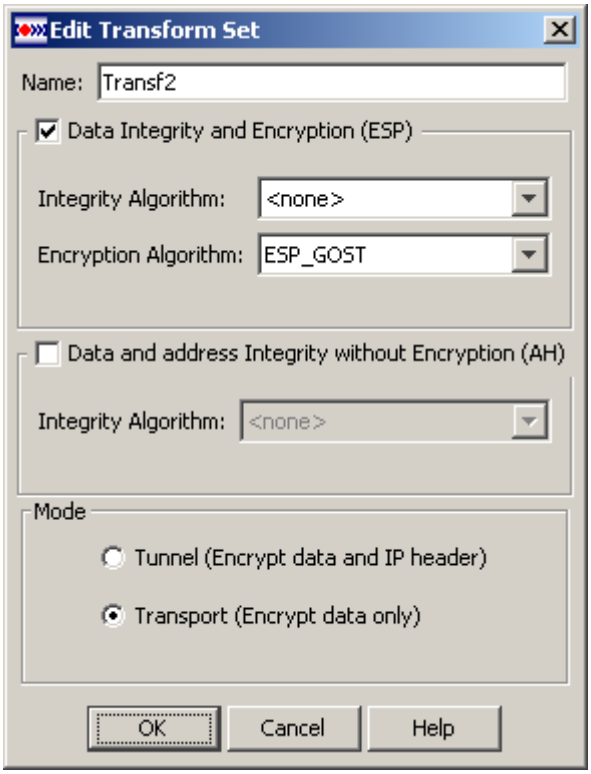

Рисунок 60

Удаление выделенного Transform Set

Удаление выделенного набора преобразований в таблице Transform Sets производится кнопкой Delete. После нажатия кнопки будет открыто окно с требованием подтверждения удаления набора преобразований, не связанного с криптографической картой. При получении подтверждения, набор преобразований удаляется. Если же набор преобразований связан с криптографической картой, то этот набор не может быть удален.

IPSec Rules

В этом разделе (Рисунок 61) можно просматривать созданные правила IPsec, создавать новые, редактировать и удалять существующие. Правила IPsec содержат критерии отбора пакетов, которые нужно защищать средствами IPsec. Этот раздел ничем не отличается от раздела IPSec Rules, расположенного в дереве Rules, которое появляется при нажатии одноименной кнопки в панели инструментов. Правила IPsec можно создавать, редактировать и удалять в любом из этих двух узлов. Эти функции были подробно описаны ранее в таком же разделе "IPSec Rules".

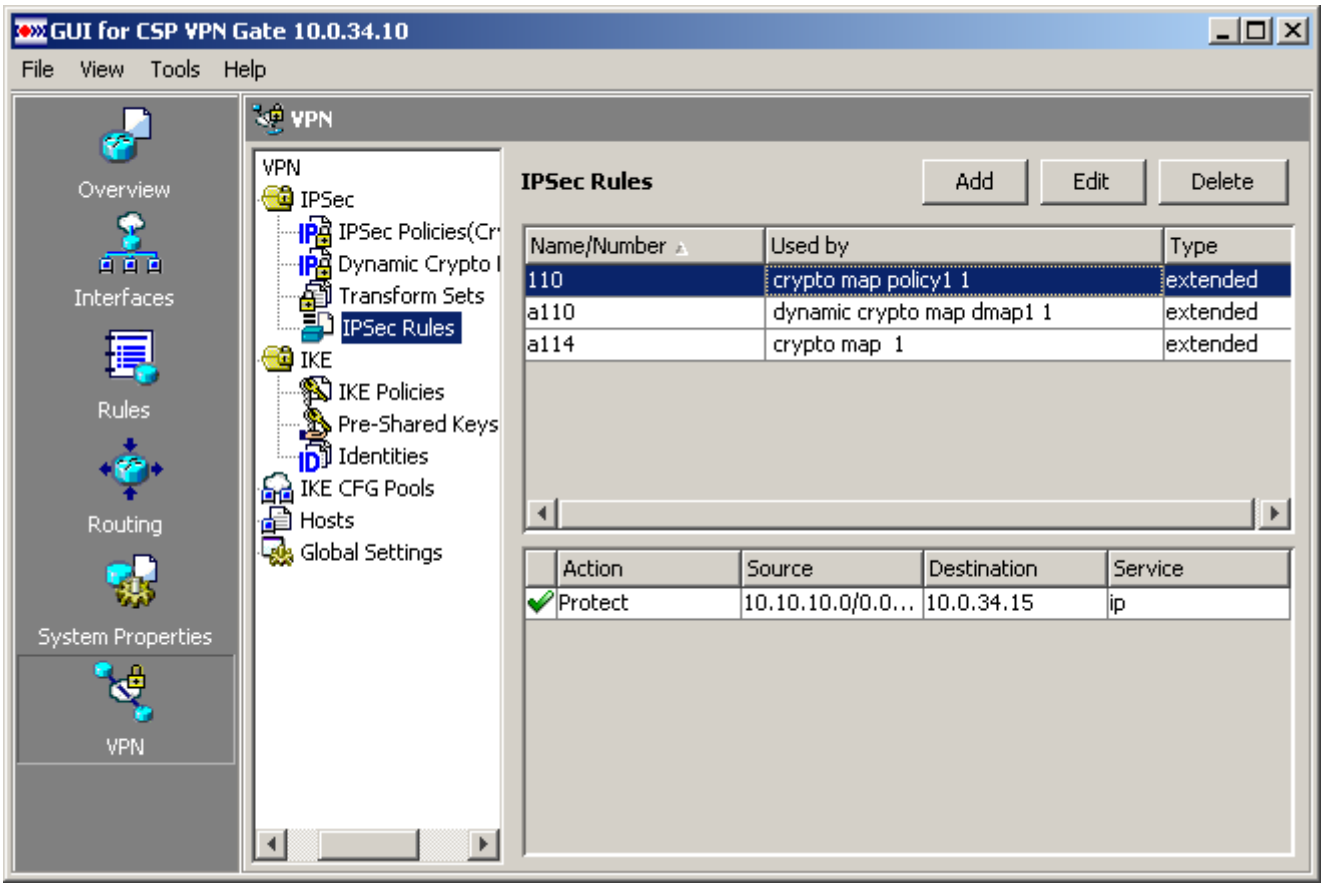

Рисунок 61

IKE

В разделе IKE главная форма принимает вид информационной панели. Никаких действий по конфигурированию в этой панели не предусмотрено. Для настройки IPsec нужно создать политики IKE, согласовать ключи и установить режим идентификации

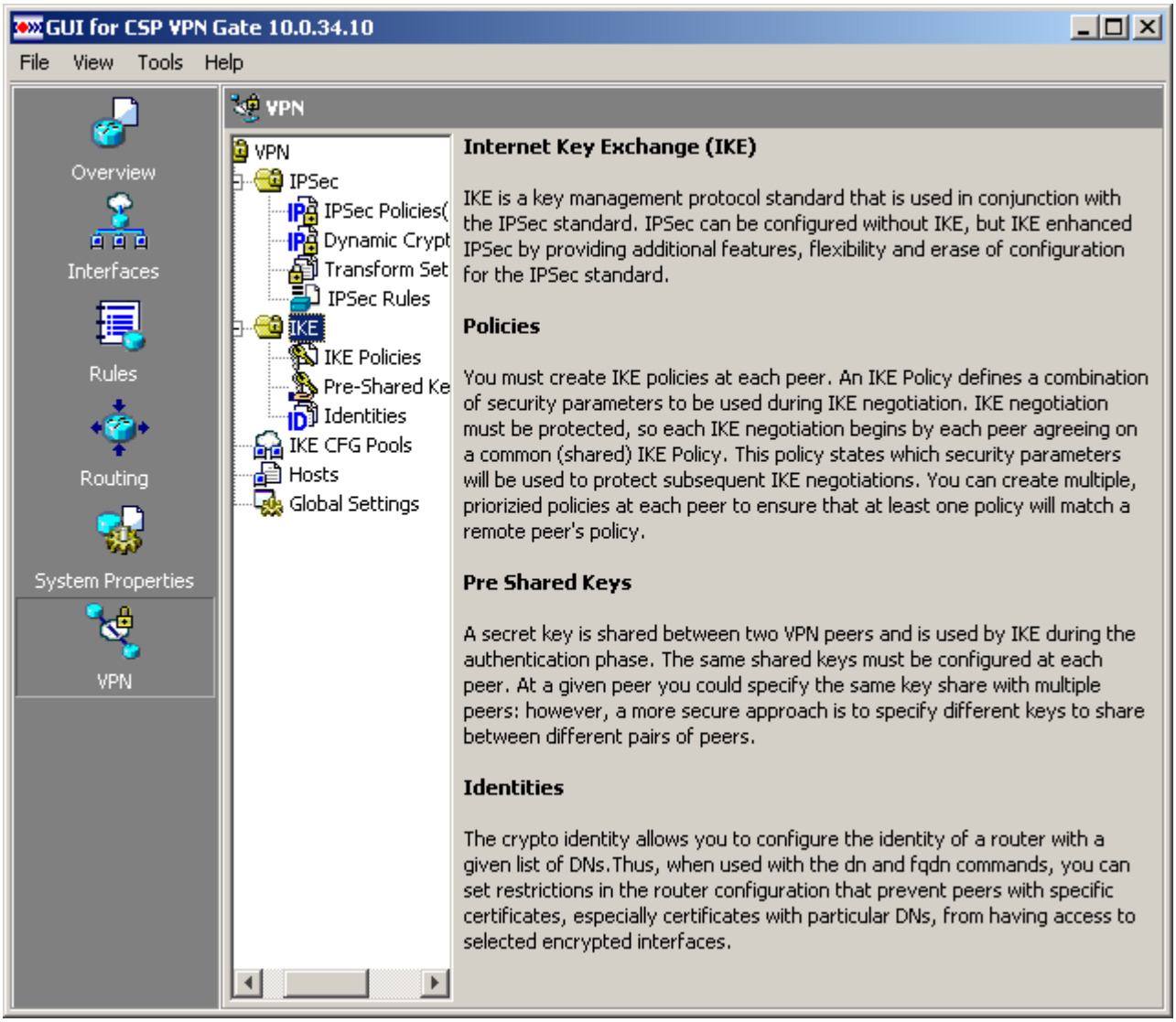

Рисунок 62

IKE Policies

Перед созданием IKE SA между партнерами нужно создать политики IKE с разными приоритетами. Политика IKE определяет набор параметров, которые используются в процессе согласования IKE.

В главной форме этого раздела (Рисунок 63) расположена таблица с разными политиками IKE. Здесь можно просматривать политики IKE, создавать, редактировать и удалять политики IKE.

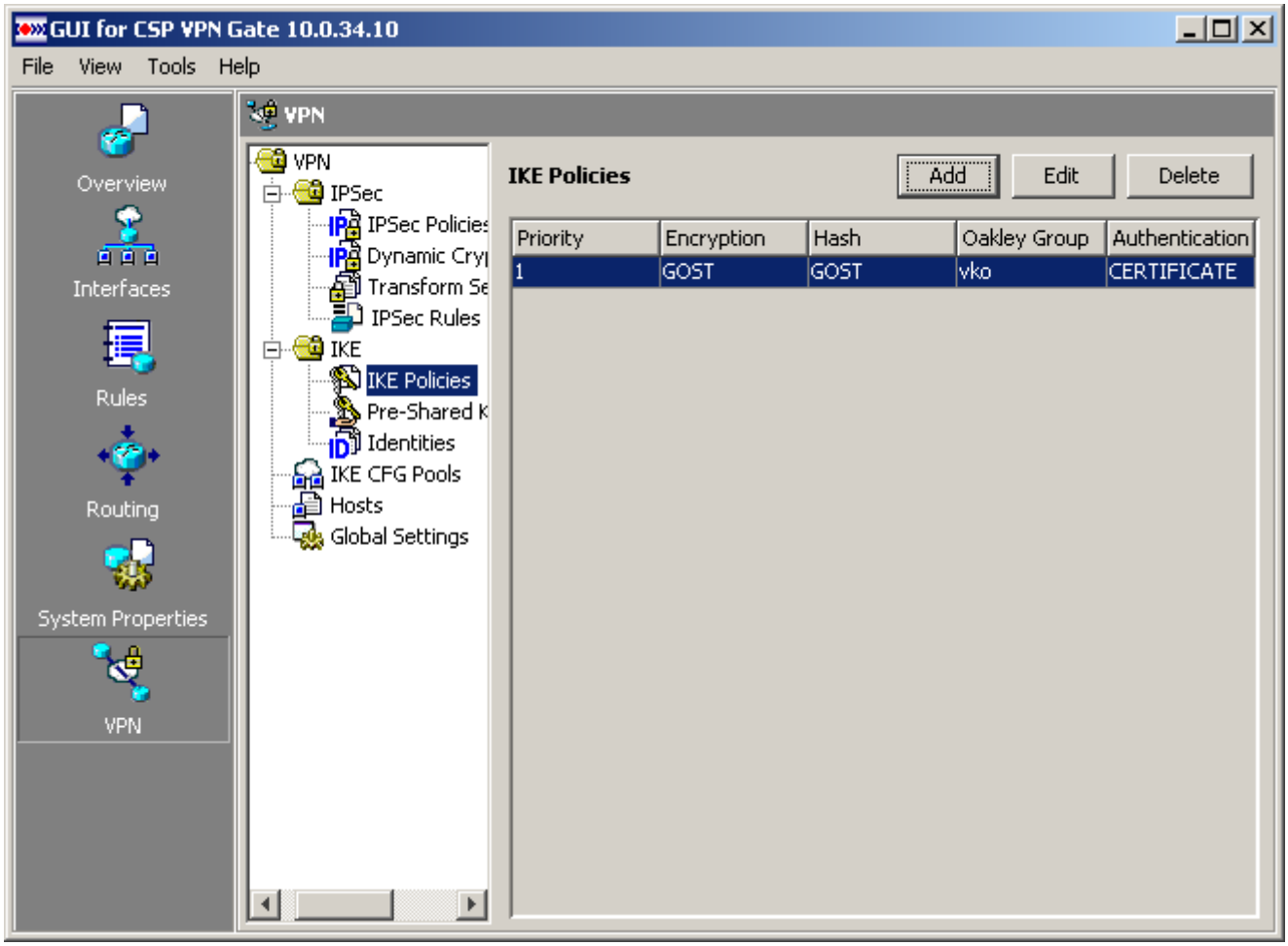

Рисунок 63

Создание IKE Policy

Нажатие кнопки Add открывает окно Add IKE Policy (Рисунок 64) для создания политики IKE. Окно состоит из следующих элементов:

- Priority – приоритет создаваемой политики IKE. Допустимый диапазон значений от 1 до 10000
- Authentication method – метод аутентификации сторон. Возможные значения:
  - PRE_SHARE – предустановленный ключ
  - CERTIFICATE – сертификат открытого ключа
- Encryption Algorithm – выпадающий список алгоритмов шифрования сообщений.

- Hash Algorithm – выпадающий список алгоритмов хэширования сообщений. Примечание: если предполагается строить соединение с аутентификацией на ГОСТ-сертификатах, то необходимо использовать ГОСТовый алгоритм хэширования.
- Oakley Group – выбирается Oakley группа, с помощью которой вырабатываются сеансовые ключи. Значение по умолчанию – vko (при задействовании значения vko, при генерации сессионных ключей IKE и вычислении разделяемого ключа вместо алгоритма Diffie-Hellman используется алгоритм VKO GOST R 34.10-2001 [RFC4357]).
- SA Lifetime (Sec) – время жизни SA, установленное с помощью IKE. Значение по умолчанию – 86400 (24 часа). Диапазон допустимых значений от 1 до 4294967295. В поле можно ввести не более 10 знаков. Разрешается ввод только цифр.

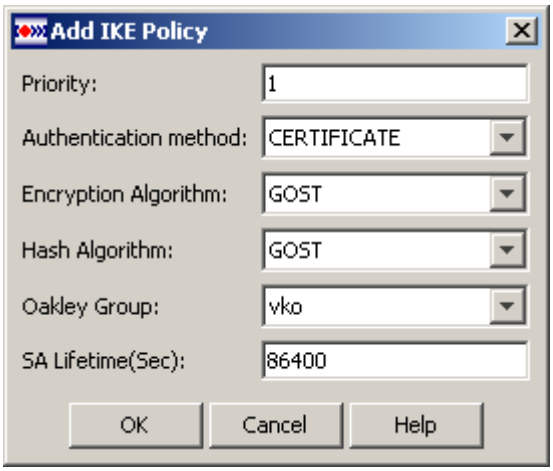

Рисунок 64

Редактирование IKE Policy

Редактирование параметров выделенной в таблице политики IKE производится в окне Edit IKE Policy, которое вызывается кнопки Edit. Окно редактирования полностью совпадает с окном создания IKE Policy.

Удаление IKE Policy

Удаление выделенной в таблице политики IKE производится кнопкой Delete. Нажатие этой кнопки открывает окно с требованием подтверждения процедуры удаления. При получении подтверждения выделенная политика IKE удаляется.

Pre-Shared Keys

Если для аутентификации сторон используется предустановленный ключ, то ключ следует создавать в этом разделе. Для каждого партнера согласовывается отдельный предустановленный ключ. В данном разделе можно создавать, редактировать и удалять предустановленные ключи для разных партнеров.

Главная форма этого раздела (Рисунок 65) содержит одну таблицу с зарегистрированными предустановленными ключами:

- Peer IP/Name – IP-адрес хоста партнера или имя партнера, для которого создан Pre-Shared Key
- Subnet Mask – маска подсети партнера
- Pre-Shared Key – в этом столбце демонстрируются только звездочки. Количество звездочек соответствует количеству введенных символов в предустановленном ключе.

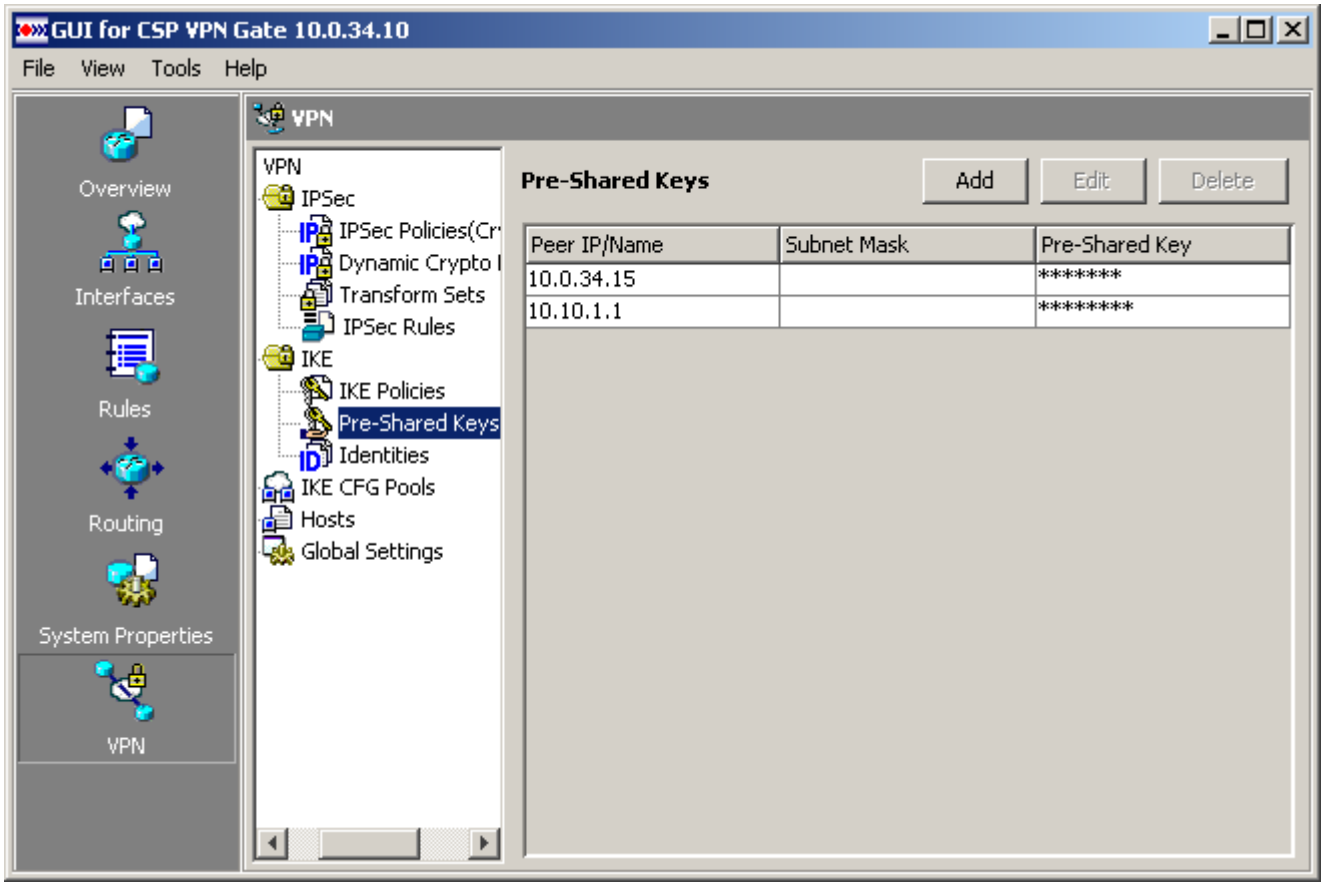

Рисунок 65

Создание Pre-Shared Key

Создание Pre-Shared Key производится в окне Add Pre-Shared Key (Рисунок 66), которое открывается по нажатию кнопки Add:

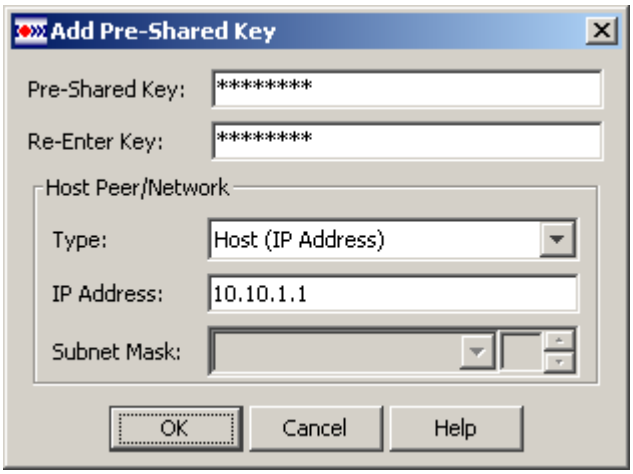

Рисунок 66

Состав элементов окна:

- Pre-Shared Key – поле ввода предустановленного ключа. Ключ может содержать только цифры и буквы латинского алфавита, а также символы `!"#$%&'()*+,-./;:>=<@[\]^_`{|}~?.` Пробелы не допускаются
- Re-Enter Key – поле повторного ввода предустановленного ключа. Значение ключа в обоих полях должны совпадать
- Группа Host Peer /Network задает партнера, при соединении с которым используется данный предустановленный ключ.
  - Type – выбор типа идентификатора IKE. Возможны три значения:
    - Network – задает идентификацию IKE по IP-адресу и маске подсети партнера (Рисунок 67).
    - Host (IP Address) – идентификация по IP-адресу. В поле IP Address задается адрес интерфейса удаленного партнера. Такая идентификация может применяться, когда удаленным хостом в процессе IKE обмена используется один интерфейс и известен IP-адрес этого интерфейса (Рисунок 66).
    - Host (Name) – идентификация по FQDN. В поле Host Name задается полное доменное имя удаленного партнера. В качестве имени домена должно использоваться имя, введенное в GUI партнера в разделе System Properties\Device\Domain Name или с помощью команды ip domain name в специализированной консоли партнера. Такая идентификация применяется, когда может использоваться несколько интерфейсов или IP-адрес интерфейса партнера неизвестен (Рисунок 68).
      Примечание: локальное полное доменное имя хоста будет сформировано из указанного имени хоста и доменного имени в разделе System Properties\Device.
  - IP Address – поле ввода IP-адреса хоста или подсети партнера.
  - Host Name – поле ввода полного доменного имени хоста партнера. Имя хоста должно соответствовать формату доменного имени: состоит из одного или нескольких слов, разделенных точкой; каждое слово обязательно должно начинаться с буквы латинского алфавита и состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака `"-"` (дефис)
  - Subnet Mask – выпадающий список установки сетевой маски и спинбокс установки битовой маски. Выпадающий список содержит пять предустановленных значений. Спинбокс позволяет устанавливать значения в диапазоне от 0 до 32.

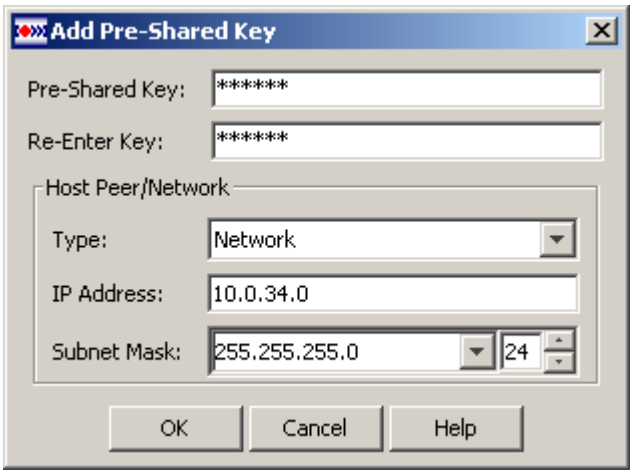

Рисунок 67

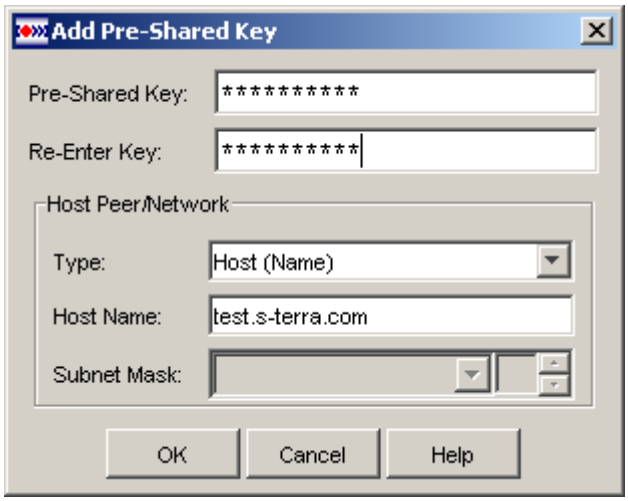

Рисунок 68

Редактирование Pre-Shared Key

Редактирование выделенного в таблице Pre-Shared Key производится в окне Edit Pre-Shared Key (Рисунок 69), которое вызывается кнопкой Edit. Окно полностью совпадает с окном создания Pre-Shared Key.

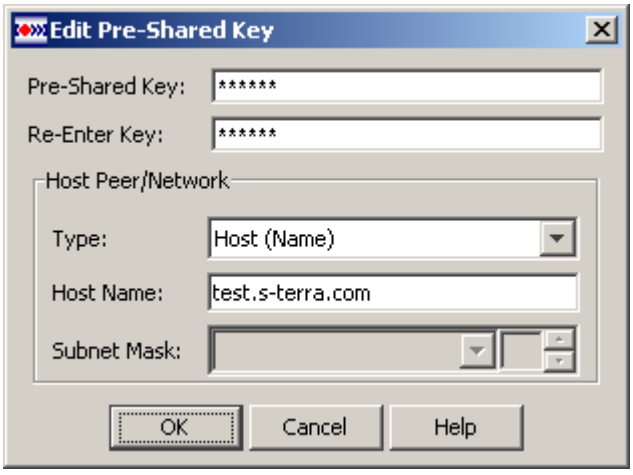

Рисунок 69

Удаление Pre-Shared Key

Удаление выделенного в таблице Pre-Shared Key производится с помощью кнопки Delete. После нажатия кнопки Delete будет открыто окно с требованием подтверждения удаления выделенной строки. При получении подтверждения строка удаляется.

Identities

Если в политике IKE используется метод аутентификации на сертификатах, то можно указать дополнительные условия, которым должен удовлетворять сертификат партнера. Только в этом случае партнер будет иметь возможность устанавливать защищенные соединения с данным шлюзом безопасности. Для заданий дополнительных условий используются списки идентификаторов (Identities). Каждый элемент списка определяет допустимые значения для полей сертификата. Для того, чтобы осуществлялась такая проверка, необходимо создать список идентификаторов, а затем указать его во вкладке Identities для криптокарты (Рисунок 52).

В окне Identities (Рисунок 70) можно просматривать списки созданных идентификаторов, вызывать окна для создания и редактирования, а также удалять списки идентификаторов.

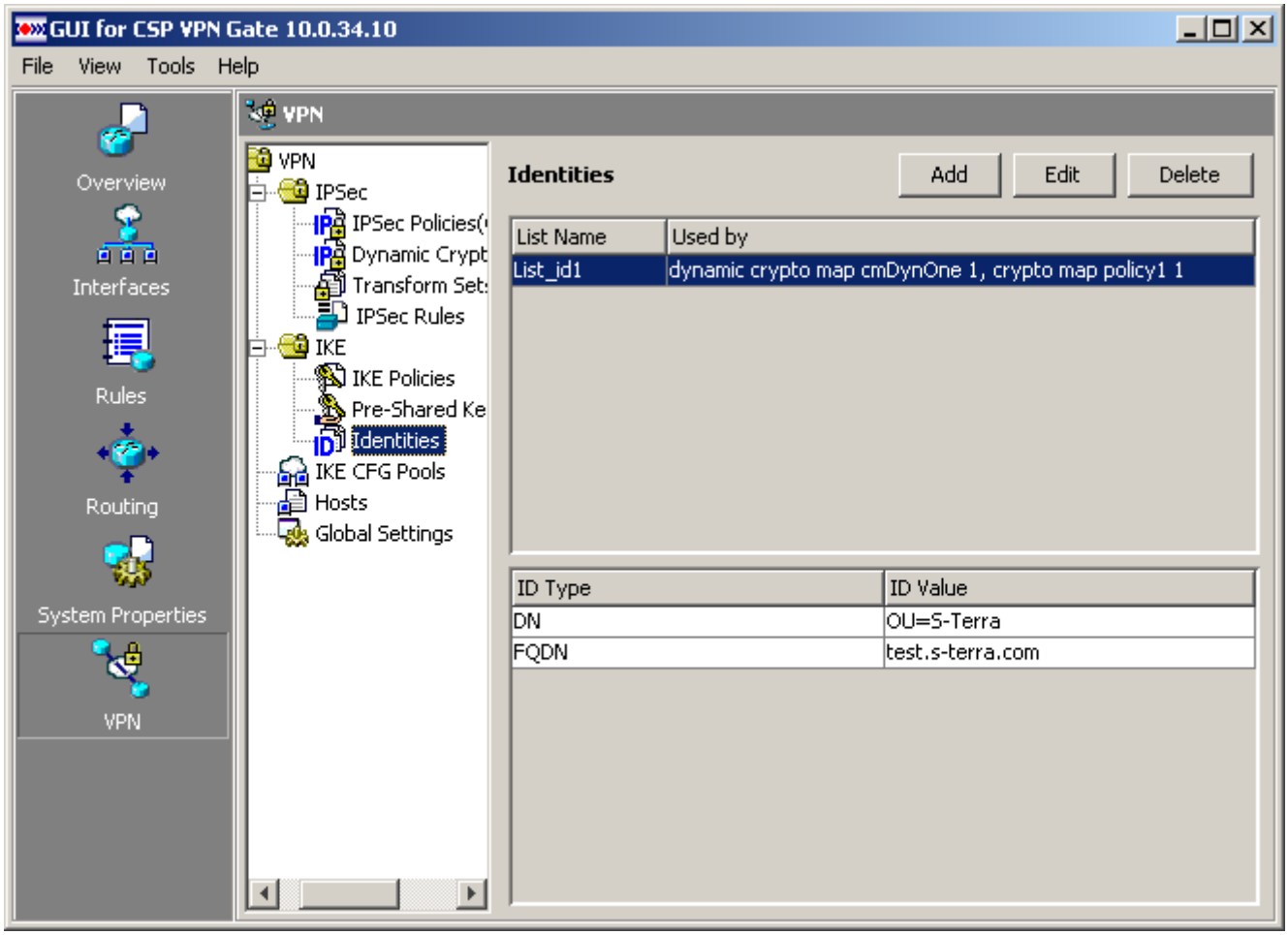

Рисунок 70

Главная форма этого раздела содержит две таблицы.

- Верхняя таблица содержит списки идентификаторов:
  - List Name – имя списка идентификаторов
  - Used by – имена криптографических карт, в которых указывается данный список идентификаторов.
- Нижняя таблица детализирует выделенный список в верхней таблице:
  - ID Type – тип идентификатора:
    - DN (Distinguished Name – уникальное имя) владельца сертификата

- FQDN (Fully Qualified Domain Name – полностью определенное доменное имя) хоста

- ID Value – значение идентификатора.

Создание нового списка идентификаторов

Создание нового списка производится в окне Add Identity List (Рисунок 71), которое вызывается кнопкой Add.

Состав элементов окна:

- Name – имя списка идентификаторов. В имени должны использоваться только латинские буквы, цифры и символы `!"#$%&'()*+,-./;:>=<@[\]^_`{|}~?.` Не допускаются пробелы. Имя обязательно должно начинаться с буквы.
- Identity List – список идентификаторов, содержит два столбца:
  - ID Type – тип идентификатора. DN или FQDN
  - ID Value – значение идентификатора.

Каждый элемент списка определяет допустимые значения для полей сертификата. Элементы списка объединяются логическим сложением (ИЛИ), то есть сертификат партнера удовлетворяет условию в целом, если значения его полей совпадают хотя бы с одним элементом этого списка.

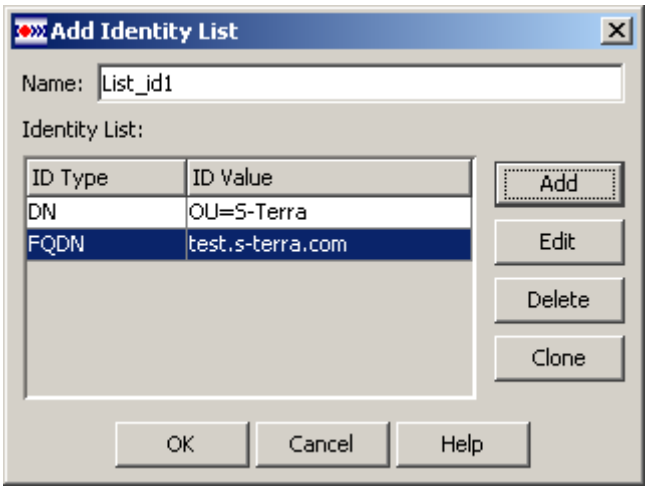

Рисунок 71

Создание нового идентификатора в списке

Создание нового идентификатора в списке производится в окне Add Identity (Рисунок 72), которое вызывается кнопкой Add в окне создания списка:

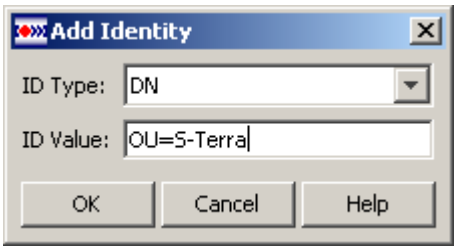

Рисунок 72

Окно содержит два поля: ID Type – для выбора типа идентификатора, ID Value – для ввода значения идентификатора.

Формат значений идентификатора DN:

- DN представляет собой последовательность пар <Тип>=<Значение>, разделенных либо запятой, либо знаком + (плюс), либо точкой с запятой (`;`). Перед и после разделителей могут быть пробелы.
- Тип (Attribute Type) – может быть OID (числа, разделенные точкой) либо один из предопределенных типов (все Case-sensitive):
  - CN – Common Name
  - L – Locality
  - ST – State
  - O – Organization
  - OU – Organization Unit
  - C – Country
  - STREET
  - DC – Domain Component
  - UID –User ID.
- Значение может быть одного из двух видов:
  - Hex-представление, которое начинается символом # (решетка). Это представление должно использоваться, если тип представлен в виде OID
  - Строка (Attribute Value). Такие символы, как `+ " < > ; #` должны предваряться символом `\(escape)`. Сам символ `\ (escape)` также должен предваряться символом `\ (escape)`, если он не предваряет пару Hex-чисел, управляющие спецсимволы и префиксные/постфиксные пробелы. Также допустимо использование спецсимволов (кроме символа `\(escape)и "`) как значащих символов без символа `\ (escape)`,если значение строки заключить в кавычки.

    В строке могут встречаться пробелы, предваряющие/ограничивающие (Attribute Value). Пробелы, являющиеся значащими символами, должны предваряться символом `\(escape)`.Также может быть последовательность типа `\<hexpair>`, где `<hexpair>` - две Hex-цифры: это обозначает, что вводится символ с данным кодом.Строка (Attribute Value).

Пример:

```
O = "Harry & Walter"
O = Harry \+Walter
```

В Продукте, введённый пользователем DN, преобразуется к виду, заданному RFC2253. Сначала раскрываются кавычки, спецсимволы дополняются символом `\ (escape)`, а также вставляется символ `\ (escape)` там, где пользователь мог забыть его вставить, за исключением самого символа `\ (escape)` и #, открывающей строку Attribute Value. Также разделитель `;` (semicolon), который можно интерпретировать как таковой, будет заменён запятой. Поскольку такие преобразования неоднозначны – пользователю будет предложен на утверждение наш вариант преобразования: `Distinguished Name OLDNAME will be transformed to NEWNAME Press Yes to confirm, press No to continue editing.`

Таким образом, Distinguished Name записывается в виде:

`CN=xxx,L=xxx,ST=xxx,O=xxx,OU=xxx,C=xxx,STREET=xxx,DC=xxx,UID=xxx.`

Достаточно задать не полный список атрибутов DN, а какое-то его подмножество, например, O=S-Terra.

Предупреждение: DN в строке должен быть задан точно также, как он задан в сертификате: необходимо строго соблюдать количество пробелов и регистр символов.

Проверка будет считаться успешной, если заданные значения полей совпадают с соответствующими значениями в сертификате.

Формат значений идентификатора `FQDN` соответствует формату доменного имени:

- состоит из одного или нескольких слов, разделенных точкой
- каждое слово обязательно должно начинаться с буквы латинского алфавита
- может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака `"-"` (дефис).

Клонирование идентификатора

Для создания нового идентификатора, с использованием части информации выделенного идентификатора в списке (Рисунок 71), используется кнопка Clone. Кнопка Clone активна только при выделении строки в списке. Если ни одна строка не выделена, кнопка блокируется. Нажатие кнопки Clone открывает окно создания идентификатора, в котором оба поля заполнены значениями выделенной строки.

Редактирование идентификатора

Редактирование выделенного идентификатора производится в окне, которое открывается с помощью кнопки Edit. Если нет выделенной строки – кнопка Edit блокируется. Нажатие кнопки Edit открывает окно редактирования, в котором поле ID Value заполнено значением выделенной строки.

Удаление идентификатора

Удаление выделенного идентификатора производится с помощью кнопки Delete. Кнопка доступна только при выделении строки в списке. В противном случае кнопка блокирована. После нажатия кнопки Delete будет открыто окно с требованием подтверждения операции удаления.

Редактирование списка идентификаторов

Редактирование списка идентификаторов производится в окне Edit Identity List, которое по составу элементов совпадает с окном Add Identity List, и открывается по нажатию кнопки Edit. Кнопка активна только при выделении строки в верхней таблице. Редактирование списка производится также как и при создании списка.

Удаление списка идентификаторов

Удаление списка идентификаторов производится с помощью кнопки Delete. Кнопка активна только при выделении строки в верхней таблице. Нажатие кнопки Delete вызывает проверку связанности удаляемой строки с криптографическими картами:

- если связей не обнаружено, то будет открыто окно с требованием подтверждения операции удаления

- если удаляемый список связан с одной или несколькими криптографическими картами, то будет открыто окно с требованием подтверждения операции удаления. Если получено подтверждение, то выделенный список удаляется, а у связанных криптографических карт в соответствующем разделе будет удалена ссылка на этот список и установлено значение <none>.

IKE CFG Pools

В разделе IKE CFG Pools (Рисунок 73) просматриваются созданные пулы адресов, создаются новые, редактируются и удаляются существующие пулы. IKE CFG пул создается для выдачи адреса партнеру по его запросу, например, мобильному клиенту для доступа в защищаемую подсеть. Выдача адреса происходит во время установления защищенного соединения между клиентом и шлюзом безопасности. В состав пула могут входить адреса из защищаемой подсети или с ней не пересекающиеся. Для использования созданного пула нужно в окне Add/Edit Dynamic Crypto Map (Рисунок 57) во вкладке IKE CFG указать имя пула адресов. Для правильной работы соединений необходимо отредактировать таблицу маршрутизации.

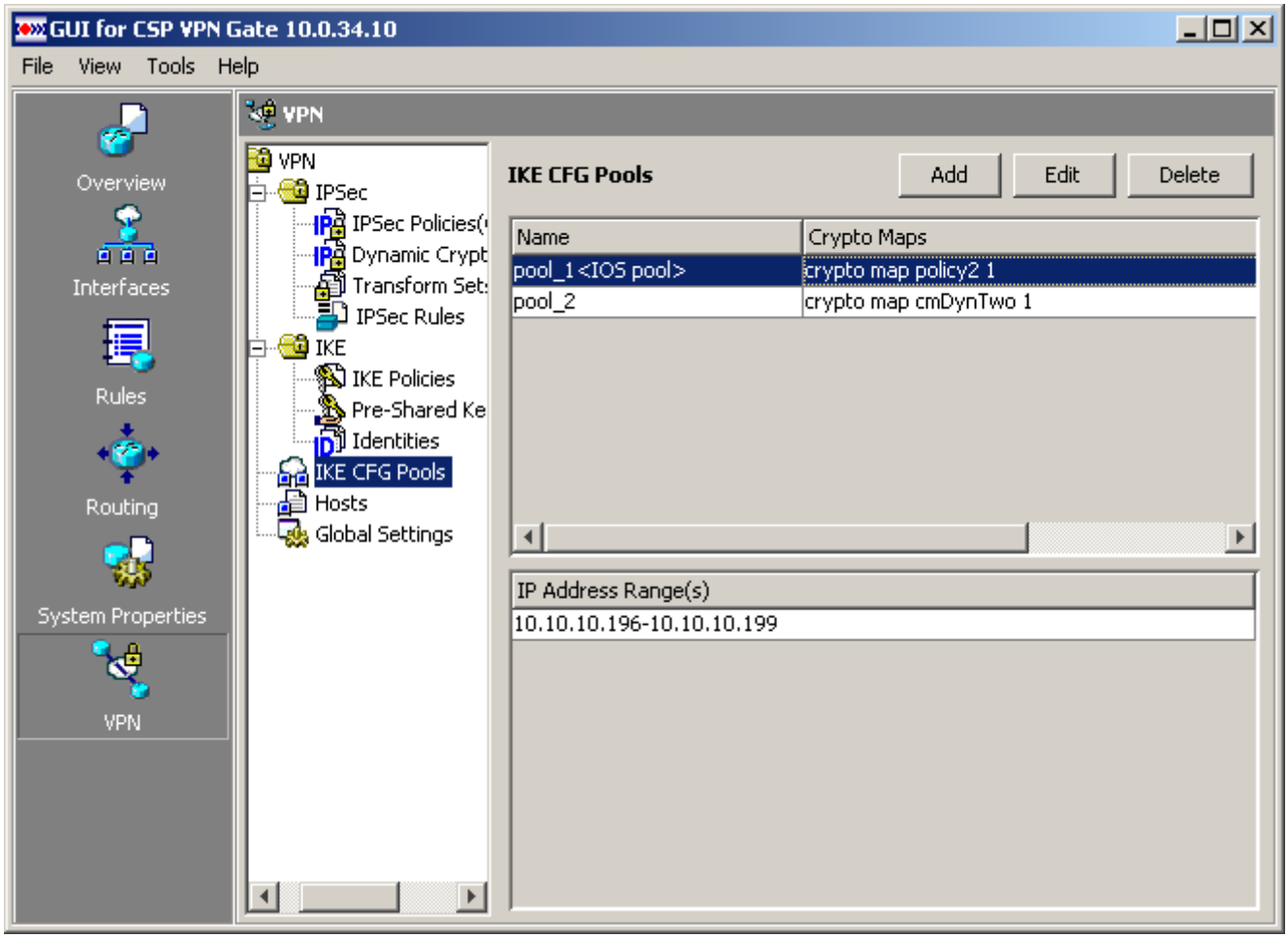

Рисунок 73

Главная форма этого раздела содержит две таблицы.

Верхняя таблица с элементами:

- Name – имя пула адресов. Пул, которому назначен статус IOS (общий), отображается именем и надписью <IOS pool>
- Crypto Maps – имена криптографических карт, использующих данный пул адресов

Нижняя таблица:

- IP Address Range(s) – показывает диапазоны IP-адресов выделенного пула в верхней таблице.

Создание пула адресов

Создание пула адресов производится в окне Add IKE CFG Pool (Рисунок 74), которое появляется при нажатии кнопки Add.

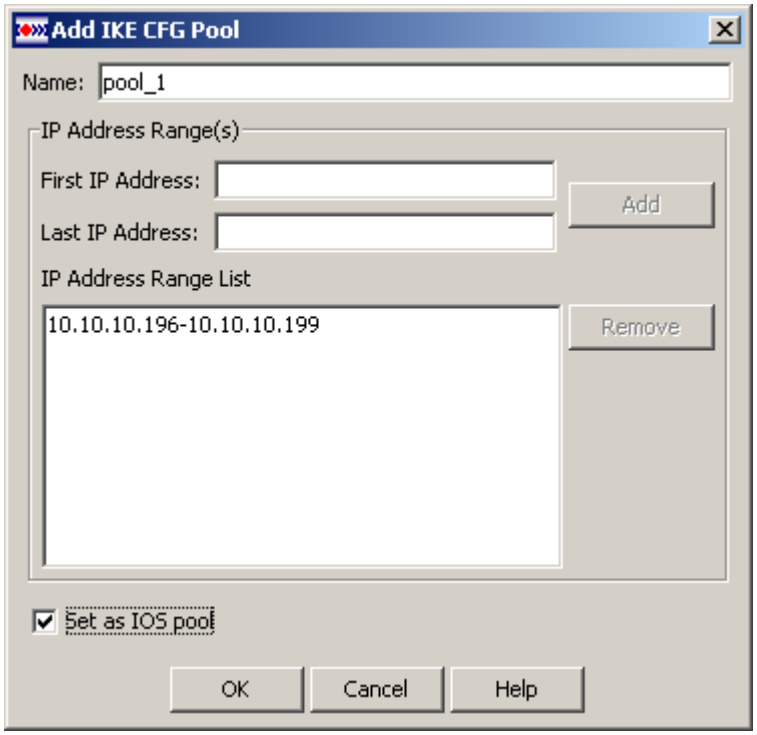

Рисунок 74

Состав элементов окна:

- Name – имя IKE CFG пула. В имени должны использоваться только латинские буквы, цифры и символы `!"#$%&'()*+,-./;:>=<@[\]^_`{|}~?.` Не допускаются пробелы. Имя обязательно должно начинаться с буквы.
- IP Address Range(s) – группа элементов формирования диапазона IP-адресов. Например, из подсети 10.10.10.0/24 можно выделить диапазон адресов 10.10.10.196-10.10.10.199. Или выделить другой диапазон 10.10.10.240 – 10.10.10.243.
  - First IP Address – поле ввода первого IP-адреса диапазона или единичного IP-адреса. Первый адрес диапазона должен быть меньше последнего адреса диапазона. Это поле не должно быть пустым.
  - Last IP Address – поле ввода последнего IP-адреса диапазона.
  - IP Address Range List – список диапазонов IP-адресов. В списке запрещено выделение нескольких строк. Список может содержать как диапазоны, так и отдельные IP-адреса. В списке не должно быть диапазонов, которые пересекаются или входят в другие диапазоны списка, а также в адресные пространства других IKE CFG пулов.
- Set as IOS pooll – флажок, устанавливающий статус IOS создаваемому пулу адресов. Пул с таким статусом является общим и может быть только один.

  В файле конфигурации это назначение отображается командой `crypto isakmp client configuration address-pool local pool_name`.

  Для привязки такого пула к криптографическим картам используется команда `crypto map имя_политики_IPsec client configuration address {initiate|respond}`

или
`crypto dynamic-map имя_набора_динамических_криптокарт client configuration address {initiate|respond}`,
а не `set pool`, в случае, когда пул не имеет статуса IOS.

Примечание: если набор динамических криптокарт, у которых не задан пул адресов, связан с политикой IPsec, у которой указан пул адресов, помеченный как IOS pooll, то в разделах Overview, VPN (VPN Connections), IPSec Policies у данного набора динамических криптокарт вместо значения <none> будет отображаться имя IOS pooll пула с пометкой <effective>. Это же значение будет отображаться, если описанная выше ситуация присутствует в действующей на шлюзе конфигурации.

Кнопки управления:

- Add – кнопка добавления диапазона, указанного в полях First IP Address и Last IP Address, в список диапазонов IP-адресов. Кнопка блокируется при пустом поле First IP Address. Если заполнено только поле First IP Address, то по нажатию этой кнопки в список будет помещен указанный адрес.
- Remove – кнопка удаления выделенного диапазона из списка. Если в списке нет выделенной строки, кнопка блокируется.

После создания IKE CFG пула необходимо отредактировать таблицу маршрутизации для правильной работы соединений. Для этого в разделе "Routing" нужно добавить запись для обратного трафика от подсети к клиентам, получившим адрес из данного IKE CFG пула. При этом параметры записи задаются следующим образом:

Prefix, Prefix Mask	указывается диапазон адресов данного IKE CFG пула
IP Address	задает адрес внешнего маршрутизатора, через который поступают пакеты клиентам.

Редактирование выделенного пула адресов

Редактирование выделенного в таблице пула адресов производится в окне, аналогичном окну создания нового пула (Рисунок 74), которое вызывается кнопкой Edit.

Редактирование заключается в изменении списка зарегистрированных диапазонов путем удаления существующих или добавления новых диапазонов IP-адресов.

По завершении редактирования могут быть выданы сообщения:

Удаление выделенного пула адресов

Удаление выделенного пула адресов в верхней таблице (Рисунок 73) происходит при нажатии кнопки Delete.

При удалении всегда будет открываться окно с требованием подтверждения удаления, независимо от связи данного пула с криптографическими картами или статуса <IOS pool>.

Hosts

При аутентификации сторон с использованием Pre-Shared Key для удаленного хоста в качестве идентификатора используется либо имя хоста, либо IP-адрес интерфейса этого хоста. Если известно имя удаленного хоста и IP-адрес(а) его интерфейса, то для установления такой ассоциации предназначен данный раздел.

Главная форма этого раздела (Рисунок 75) содержит таблицу со столбцами:

- Name – имя удаленного хоста партнера
- IP Addresses –IP-адрес(а) интерфейса (ов) удаленного хоста.

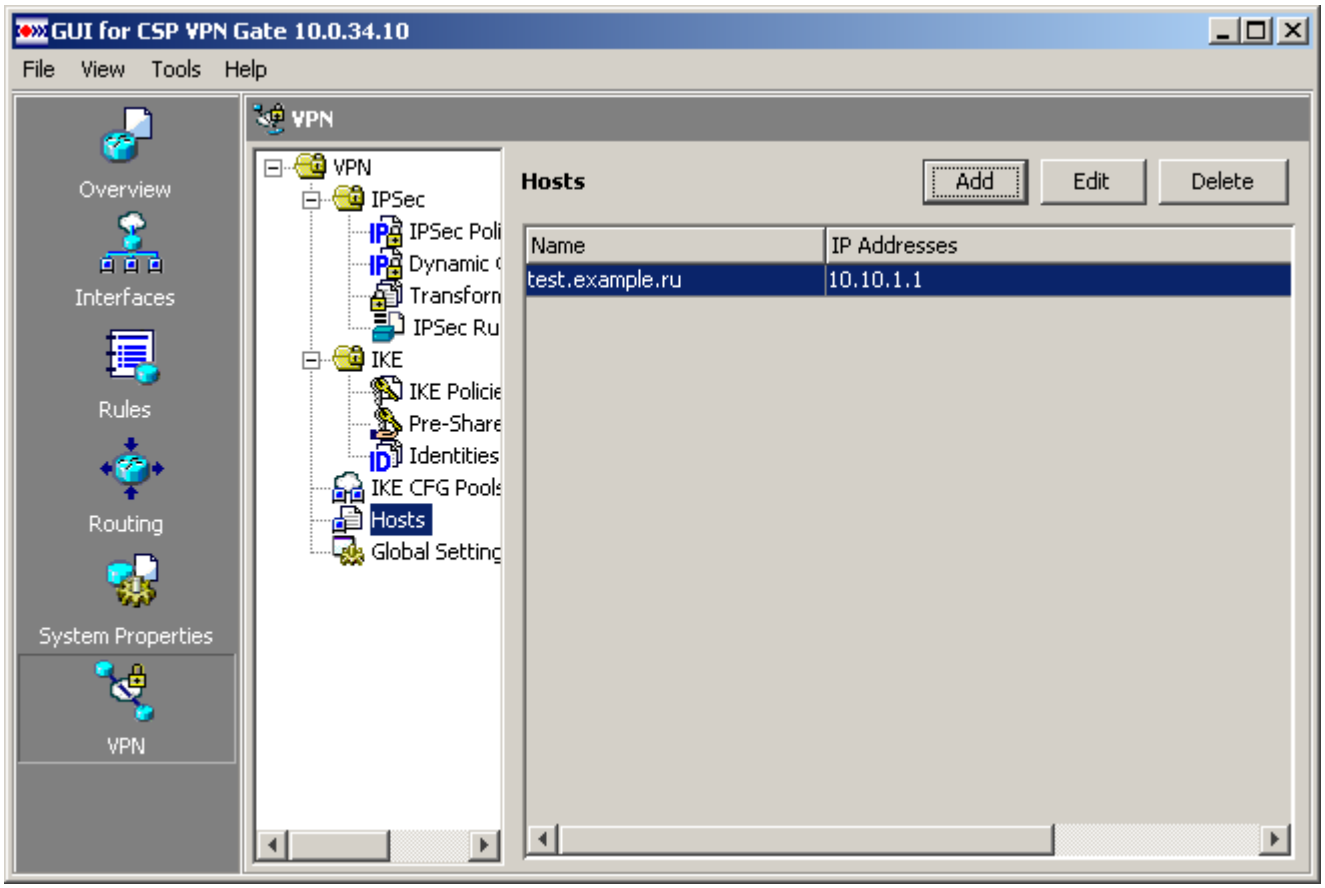

Рисунок 75

Создание новой записи для хоста

Создание новой записи производится в окне Add Host (Рисунок 76), которое вызывается кнопкой Add.

Состав элементов окна:

- Name – поле ввода имени хоста. Предполагает ввод полного имени, включая домен первого уровня. Имя хоста состоит из одного или нескольких слов, разделенных точкой; каждое слово обязательно должно начинаться с буквы латинского алфавита и может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака "-" (дефис)
- IP Address(es) – группа элементов формирования списка IP-адресов:
  - IP Address – поле ввода IP-адреса интерфейса удаленного хоста
  - IP Address List – список IP-адресов, когда используется несколько интерфейсов хоста

Кнопки управления:

- Add – кнопка добавления IP-адреса из поля IP Address в список IP Address List. По нажатию этой кнопки проверяется формат ввода данных
- Delete – кнопка удаления выделенного IP-адреса из списка IP Address List. Если в списке нет выделенной строки, кнопка блокируется.

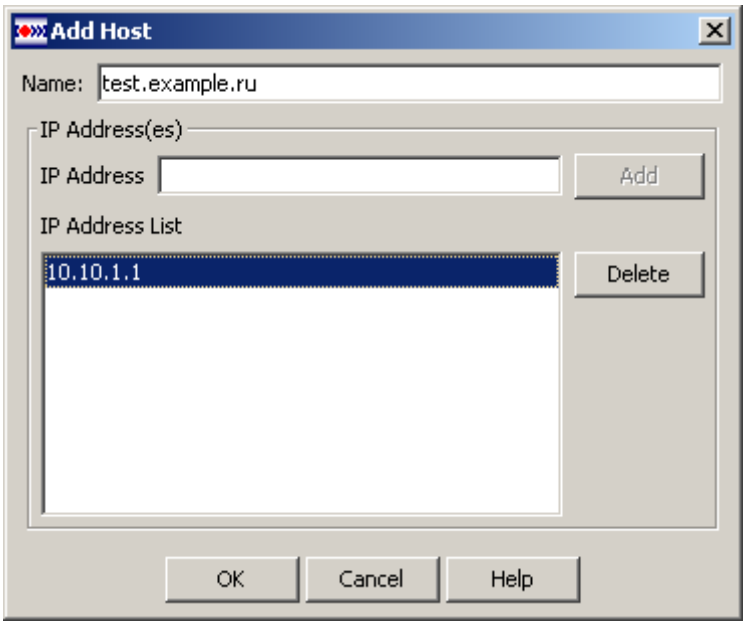

Рисунок 76

Редактирование выделенной строки

Редактирование выделенного в таблице хоста производится в окне Edit Hosts, которое вызывается кнопкой Edit и совпадает с окном Add Hosts.

Удаление выделенной строки

Для удаления выделенной строки в таблице служит кнопка Delete. Нажатие этой кнопки вызывает окно с требованием подтверждения удаления.

Global Settings

В разделе Global Settings (Рисунок 77) просматриваются и редактируются глобальные параметры VPN для шлюза безопасности:

- IKE Identity – задается тип идентификатора, используемого в рамках протокола IKE
- IKE Keepalive – допустимый период времени (в секундах) отсутствия входящего трафика от партнера, по истечению которого, при наличии исходящего трафика, активируется DPD-сессия
- IKE Retry – время ожидания ответа (в секундах) от партнера на DPD-запрос
- IPSec SA Lifetime (Kilobytes) – объем данных в килобайтах, который могут передать партнеры в рамках одной IPsec SA. Применяется ко всем криптографическим картам, но может быть изменено для конкретной криптокарты во вкладке General
- IPSec SA Lifetime (Seconds) – время в секундах, в течение которого IPsec SA будет существовать. Применяется ко всем криптографическим картам, но может быть изменено для конкретной криптокарты во вкладке General.

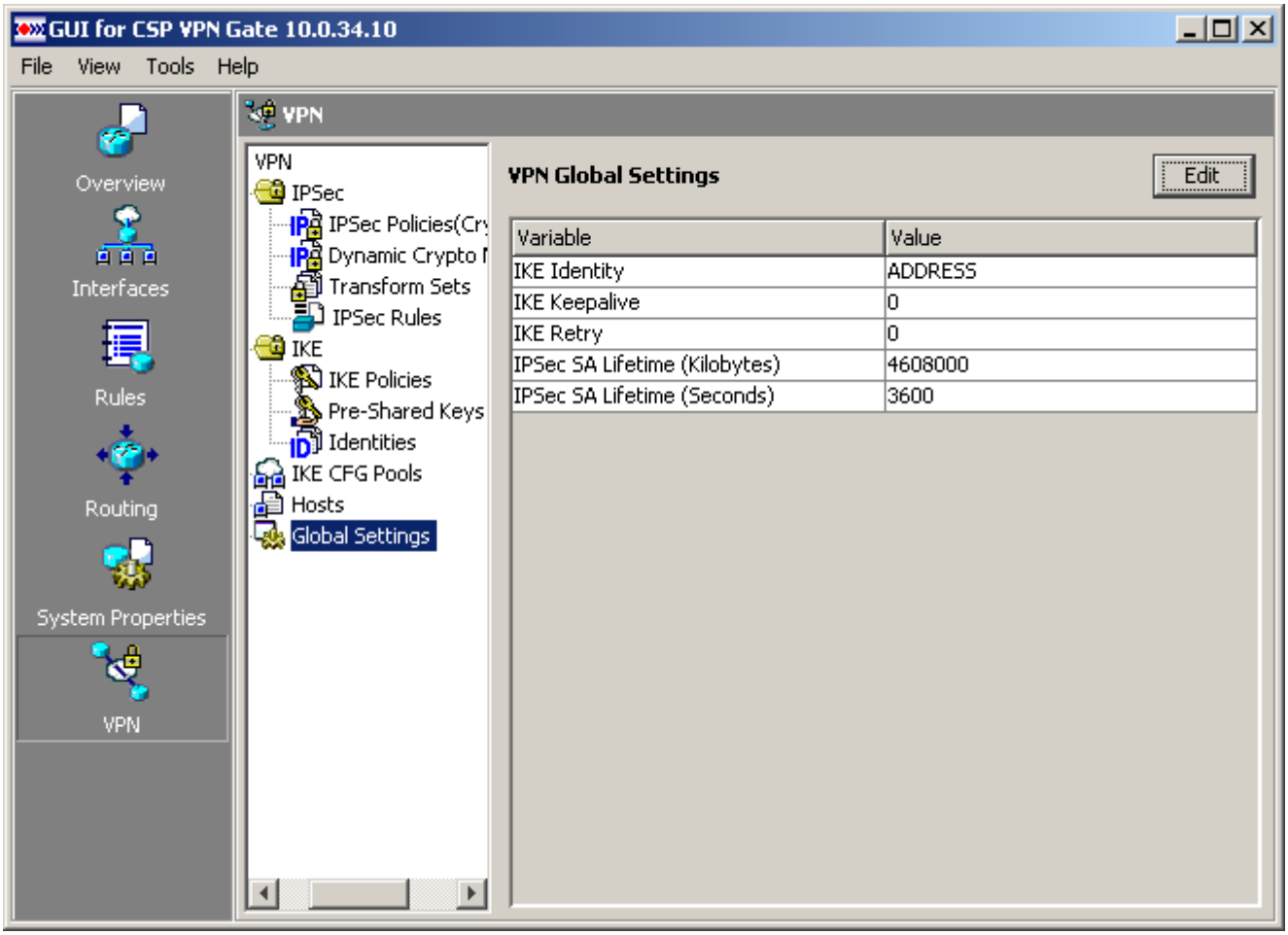

Рисунок 77

Редактирование глобальных параметров VPN

Нажатие кнопки Edit открывает окно редактирования глобальных параметров Edit VPN Global Settings.

Рисунок 78

Состав элементов окна:

- Группа Internet Key Exchange (IKE):
  - Identity – выбор типа идентификатора:
    - ADDRESS – IP-адрес хоста
    - HOSTNAME – имя хоста
    - DN – уникальное имя заданного формата
- Set Keepalive – флажок активации элементов группы. По умолчанию – выключен.
  - Keepalive (Sec) – поле ввода временного интервала (в секундах) отсутствия входящего трафика от партнера, по истечению которого, при наличии исходящего трафика, активируется DPD-сессия. Это поле должно иметь значение из диапазона 10..3600. По умолчанию – блокировано и равно 0.
  - Retry (Sec) – поле ввода временного интервала (в секундах) ожидания ответа от партнера на DPD-запрос. Это поле должно иметь значение из диапазона 2..60. По умолчанию – блокировано и равно 0.
- Группа IPSec:
  - IPSec SA Lifetime (Seconds) – поле ввода времени жизни IPsec SA в секундах. Введенное значение должно принадлежать диапазону от 1 до 4294967295. По умолчанию – 3600. Установленное значение будет использоваться при создании новой криптографической карты.
  - IPSec SA Lifetime (Kilobytes) – поле ввода времени жизни IPsec SA в килобайтах. Введенное значение должно принадлежать диапазону от 1 до 4294967295. По умолчанию – 4608000. Установленное значение будет использоваться при создании новой криптографической карты.

Окно Ping

Окно "Ping" (Рисунок 79) вызывается одноименной командой меню Tools. Команда ping используется для проверки работоспособности соединения.

Состав элементов окна:

- Destination – поле ввода IP-адреса партнера
- Ping – кнопка, инициализирующая ping
- Информационное поле. В поле отображается результат выполнения команды Ping
- Clear Output – кнопка для очистки информационного поля
- Close – кнопка для закрытия окна Ping
- Help – кнопка вызова страницы Help для данного окна.

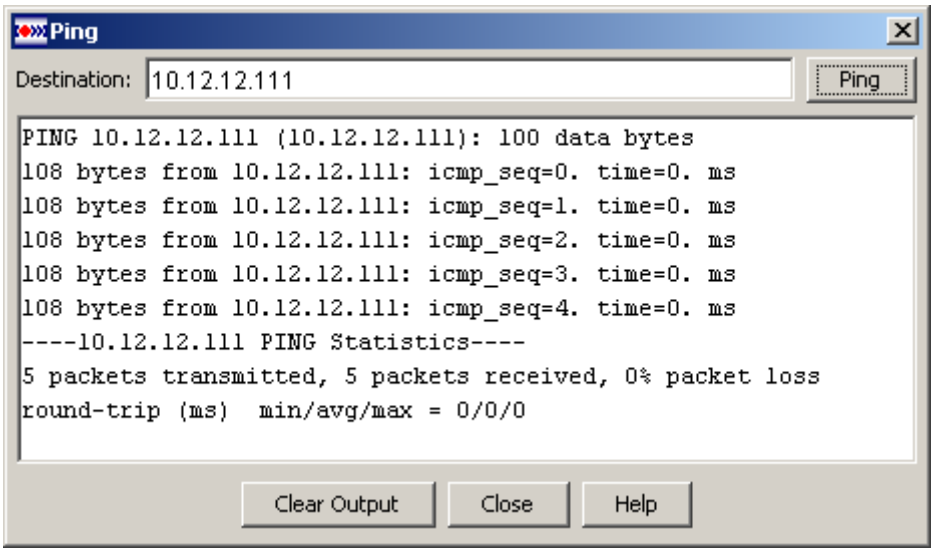

Рисунок 79

Окно SA Manager

Окно "SA Manager" (Рисунок 80) вызывается одноименной командой меню Tools. В окне отображается информация о существующих на шлюзе безопасности SA (Security Association), а также имеется возможность удалять SA.

Перед открытием окна устанавливается SSH соединение со шлюзом безопасности, которое закрывается при закрытии окна.

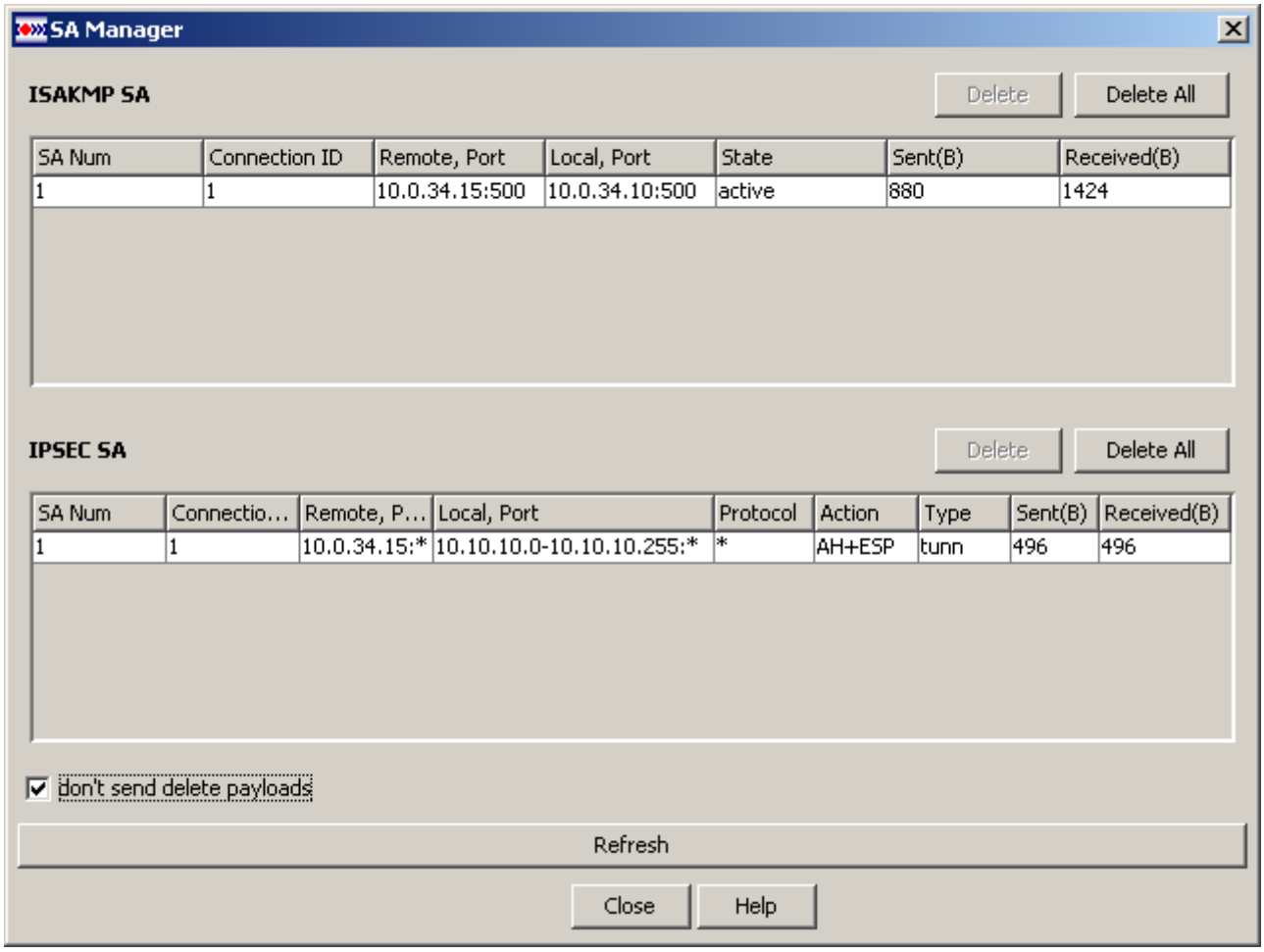

Рисунок 80

Состав элементов окна:

Кнопки управления ISAKMP SA:

- Delete – кнопка для удаления выделенного ISAKMP SA
- Delete All – кнопка для удаления всех ISAKMP SA.

Таблица ISAKMP SA содержит список SA для ISAKMP сессий:

- SA Num – порядковый номер ISAKMP соединения
- Connection ID – уникальный идентификатор ISAKMP SA
- Remote, Port – IP-адрес и порт удаленной точки соединения (если номер порта не указан, то выдается *)

- Local, Port – IP-адрес и порт локальной точки соединения (если номер порта не указан, то выдается *)
- State – состояние SA:
  - incomplete – недостроенное соединение
  - active – активное соединение
  - configuration – для данного SA проводится дополнительная настройка (IKECFG XAuth, etc.)
  - deleted – SA не используется, подготовлен к удалению
  - unknown – статус соединения неизвестен
- Sent(B) – количество переданных байтов
- Received(B) – количество принятых байтов.

Кнопки управления IPsec SA:

- Delete – кнопка для удаления выделенного IPsec SA
- Delete All – кнопка для удаления всех IPsec SA.

Таблица IPSEC SA содержит список SA, построенных в процессе работы IPsec:

- SA Num – порядковый номер IPsec соединения
- Connection ID – уникальный идентификатор SA в системе
- Remote, Port – IP-адрес и порт удаленной точки соединения (если номер порта не указан, то выдается *)
- Local, Port – IP-адрес и порт локальной точки соединения (если номер порта не указан, то выдается *)
- Protocol – протокол, для которого построен этот SA (если протокол не указан, то выводится *)
- Action – протоколы IPsec – ESP, AH или AH+ESP
- Type – тип
  - tunn – туннельный режим
  - trans – транспортный режим
  - nat-t-tunn – туннельный режим через NAT
  - nat-t-trans – транспортный режим через NAT
- Sent(B) – количество переданных байтов
- Received(B) – количество принятых байтов.

Флажок don’t send delete payloads – установка флажка отключает уведомление партнеров при удалении SA.

Кнопки управления:

- Refresh – кнопка обновления данных
- Close – кнопка для закрытия окна SA Manager
- Help – кнопка вызова страницы Help для данного окна.

Доставка конфигурации на шлюз безопасности

Доставка (загрузка) конфигурации на шлюз безопасности производится выбором предложения Deliver to Router в меню File. При этом открывается окно Deliver Configuration to Router (Рисунок 81). Состав элементов окна:

- Список команд, которые были добавлены в последнем сеансе конфигурирования (т.е. отличия текущей конфигурации от действующей).
- Кнопки управления:
  - Deliver – кнопка, инициализирующая доставку команд на шлюз безопасности
  - Save to file – кнопка, вызывающая стандартный Save as диалог
  - Close – кнопка, закрывающая окно без каких-либо действий.

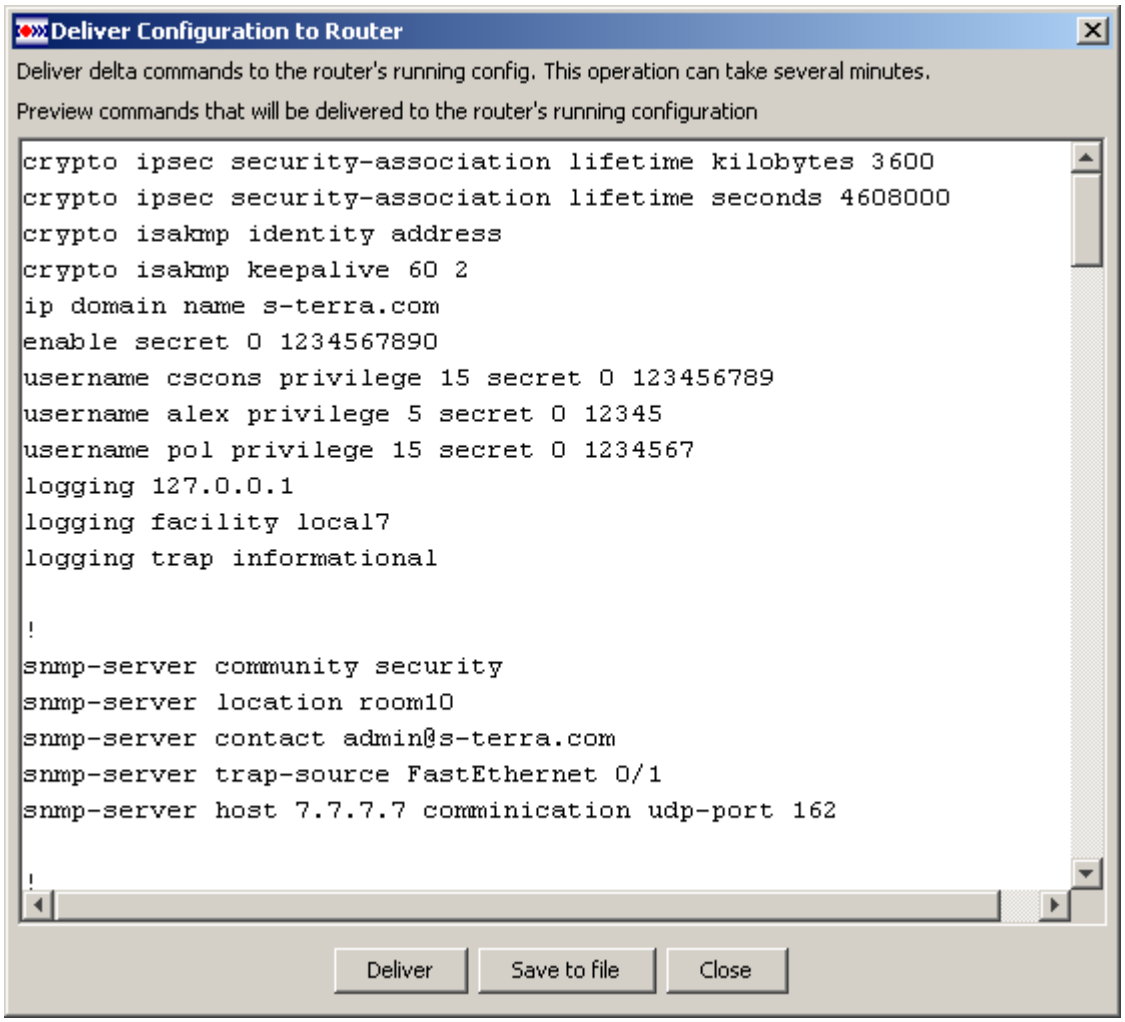

Рисунок 81

Доставка конфигурации разделена на 4 этапа:

- получение действующей конфигурации
- сравнение действующей конфигурации шлюза с текущей, подготовленной в GUI для доставки на шлюз, формирование инкрементальной конфигурации
- доставка инкрементальной конфигурации на шлюз безопасности

- получение новой действующей конфигурации со шлюза.

В процессе доставки выводится окно Delivering Status (Рисунок 82) с отображением процесса доставки конфигурации:

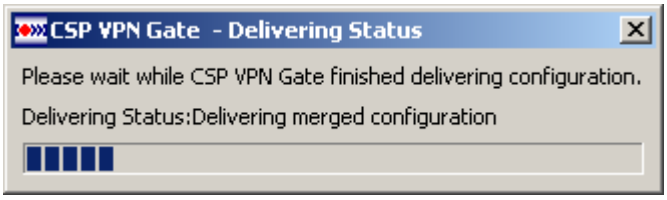

Рисунок 82

Если во время доставки в конфигурации будет обнаружена ошибка, то появится окно с предупреждением (Рисунок 83). По кнопке “Show Details” будет отображен протокол сессии доставки конфигурации на шлюз безопасности.

Рисунок 83

Возможна ситуация, когда конфигурация не может быть доставлена на шлюз безопасности по различным причинам (не удалось установить соединение со шлюзом, произошел обрыв соединения или ошибка появилась при обработке конфигурации), в этом случае будет выдано соответствующее сообщение.

Просмотр конфигурации

Окно просмотра действующей конфигурации Show Running Config (Рисунок 84), которое открывается командой Running Config в разделе View меню.

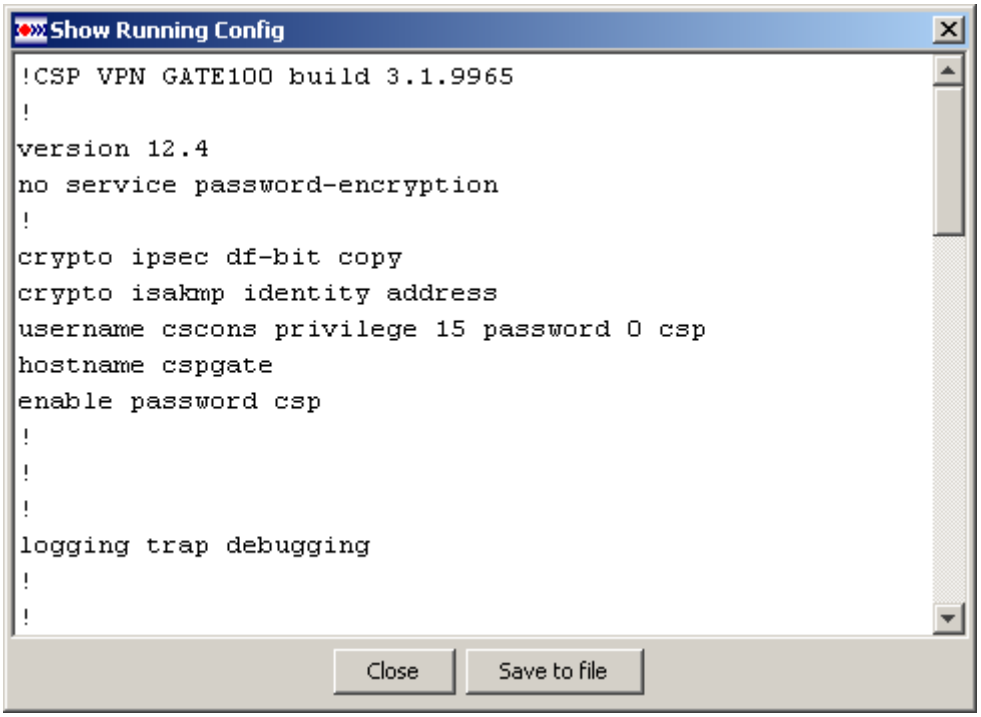

Рисунок 84

Состав элементов окна:

- Поле с текстом конфигурации
- Кнопка Save to file – открывает стандартный Save As диалог, в котором следует указать путь, по которому будет сохранен файл с действующей конфигурацией. В окне предустановлен фильтр txt. Фактически отрабатывается команда Save Running Config to PC.
- Кнопка Close – закрывает окно просмотра действующей конфигурации.

Окно просмотра текущей (отображаемой в GUI) конфигурации, подготовленной для доставки на шлюз, открывается командой Current Config в разделе View меню. Состав элементов окна Show Current Config аналогичен элементам окна Show Running Config.

Проверка конфигурации

Проверка конфигурации перед ее доставкой на шлюз безопасности производится в том случае, если был снят флажок Don't test config at delivering в меню File. По умолчанию тестирование запрещено.

Окно проверки конфигурации Configuration testing (Рисунок 85) появляется, если в результате анализа конфигурации были обнаружены какие-либо ошибки.

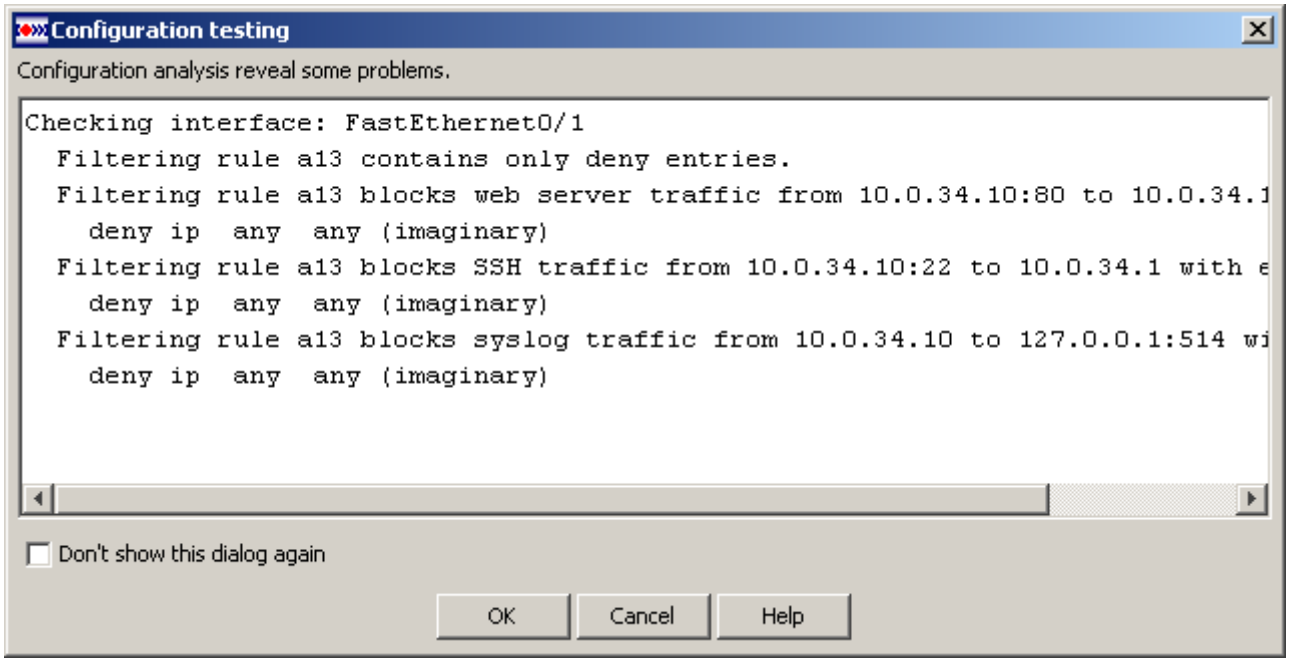

Рисунок 85

Состав элементов окна:

- Поле с текстом вывода результатов анализа конфигурации
- Don't show this dialog again – флажок синхронизирован с пунктом меню Don't test config at delivering и предназначен для той же цели – запрещает/разрешает тестировать текущую конфигурацию при доставке на шлюз
- OK – кнопка закрывает окно и переходит к отправке конфигурации
- Cancel – кнопка возвращает в окно главной формы.

Во время анализа конфигурации проводится последовательная проверка набора условий. Логика работы правил доступа и правил IPsec устроена так, что проверяемый IP пакет, не попавший под условие ни одного из правил фильтра, отбрасывается, т.е. эффект такой же, как если бы в каждом наборе записей последним стояло правило «deny ip any any». Алгоритм проверки учитывает эту особенность в работе и сообщает о «мнимых» правилах мешающих нормальной работе. Но поскольку необходимо различать их от явно заданных, то в текстовых сообщениях «мнимые» правила выглядят как «deny ip any any (imaginary)».

В описании синтаксиса сообщений используются специальные обозначения:

- вертикальной чертой разделяются варианты, в сообщении обязательно используется один из вариантов;
- в квадратных скобках указываются необязательные части сообщений;

- в угловых скобках указаны сущности, текстовые представления которых будут использованы в сообщении.

Проверяются только входящие фильтрующие правила, привязанные к интерфейсам, как напрямую (Access Rules), так и косвенно через политику IPsec (IPsec Rules).

Результаты проверки группируются по интерфейсам под заголовком:
`Checking interface: <interface name>.`

Для каждого интерфейса производятся следующие проверки:

- Выполняется анализ правил доступа привязанных к интерфейсу на предмет отсутствия в них разрешающих записей (permit). Должна быть хотя бы одна разрешающая запись, иначе выводится сообщение:
  `Filtering rule rrr contains only deny entries`
- Выполняется анализ правил в статических и динамических криптокартах на предмет отсутствия в них разрешающих записей. Если такие записи отсутствуют, то выводится сообщение:
  `Crypto rule rrr in [dynamic ] crypto map <cryptomap name> <seq. num> contains only deny entries`
- Определяется IP-адрес шлюза безопасности
- Определяется локальный адрес, с которого был запущен графический интерфейс для удаленной настройки шлюза безопасности
- Проверяется возможность общения со шлюзом безопасности с данного локального адреса
- Если включена отсылка сообщения о протоколируемых событиях syslog, то выполняется проверка разрешения трафика от шлюза безопасности к получателю сообщений. Критерии проверки: протокол UDP, адрес отправителя (любой порт), адрес получателя из настроек (порт 514).
  - В случае если трафик блокируется фильтрующим правилом, то выводится сообщение:
    `Filtering rule <filter acl name> blocks syslog traffic from <server addr> to <receiver addr>:514 with entries:`
    `<filter acl entry>`
  - Если трафик к получателю syslog шифруется, то выводится сообщение:
    `Crypto rule <crypto acl name> in [dynamic ] crypto map <cryptomap name> <seq. num> protects syslog traffic from <server addr> to <receiver addr>:514 with entries:`
    `<filter acl entry>`
- Если были заданы настройки SNMP, то проверяется разрешение трафика от шлюза безопасности к получателям SNMP-трапов. Критерии проверки: протокол UDP, адрес отправителя (любой порт), адрес получателя из конфигурации.
  - В случае если трафик блокируется фильтрующим правилом, то выводится сообщение:
    `Filtering rule <filter acl name> blocks SNMP traps from <server addr> to <receiver addr>:<receiver port> with entries:`
    `<filter acl entry>`
  - Если трафик к получателю syslog шифруется, то выводится сообщение:
    `Crypto rule <crypto acl name> in [dynamic ] crypto map <cryptomap name> <seq. num> protects SNMP traps from <server addr> to <receiver addr>:<receiver port> with entries:`
    `<filter acl entry>`

Выполняется поиск записей в IPsec правилах, связанных со статическими и динамическими криптокартами, которые полностью заблокированы правилами доступа.

- В данном случае подразумевается ситуация, когда весь трафик, попадающий под правило IPsec, блокируется правилом доступа. При этом отдельное фильтрующее правило может блокировать только часть IPsec правила. При оценке пересечения правил учитывается соотношение указанных в них протоколов, IP-адресов и (для протоколов TCP и UDP протоколов) портов.

  Синтаксис сообщений:

  ```
  Interaction between IPsec and filter ACL Interfaces:
    Filter rule <filter acl name> at interface <interface name>
  blocks crypto maps rules
   [  Dynamic templates at: <dynamic cryptomap name> <template
  sequence number>]
      In [dyanmic] crypto map: <cryptomap name> <cm sequence
  number>
      Blocked entries of rule: <crypto acl name>
        <crypto acl entry>
  ```

  В случае возникновения ошибок дальнейшая проверка не производится и выдается сообщение:

  ```
  Could not estimate filter ACL – Crypto Map interaction.
  ```

Завершение работы Продукта

Завершение работы Продукта производится с помощью команды `Exit (меню File)`, либо нажатием крестика в верхнем правом углу главной формы.

Если в процессе работы были сделаны и не доставлены какие-либо изменения в конфигурации, то вызов команды `Exit` открывает окно с текстом: "You have made changes to your configuration. If you continue, you will lose your changes. Are you sure you want to continue? Click Yes to discard your changes and continue, or No to cancel."

Нажатие кнопки No отменяет закрытие приложения.

Нажатие кнопки Yes закрывает приложение и происходит потеря.. При этом будет произведена попытка закрыть окно браузера. Это действие производится путем открытия html страницы (close.html) с функцией закрытия окна броузера. Также эта страница содержит текст: "Your session with CSP VPN Gate is finished. Don't use this window to another session with CSP VPN Gate." Как правило (во всяком случае IE это делает) при попытке закрыть окно браузера открывается окно предупреждающее, что в данный момент производится попытка закрыть окно броузера и предлагающее на выбор – закрывать это окно или нет. Если пользователь по каким-либо причинам отказывается от закрытия окна, то ему демонстрируется текст страницы close.html.

Если в процессе работы никаких изменений сделано не было, то поведение будет аналогично нажатию кнопки Yes в окне, описанном выше.

Список поддерживаемых криптографических алгоритмов

Алгоритмы, поддерживаемые в разделе Transform Sets:

- ESP Integrity Algorithms:
  - ESP_GOST_HMAC
  - ESP_SHA_HMAC
- ESP Encryption Algorithms:
  - ESP_NULL
  - ESP_GOST
  - ESP_3DES
  - ESP_AES_128
  - ESP_AES_192
  - ESP_AES_256
- AH Integrity Algorithms:
  - AH_GOST_HMAC
  - AH_SHA_HMAC

Алгоритмы, поддерживаемые в разделе IKE Policies:

- Encryption Algorithms:
  - GOST
  - 3DES
  - AES_128
  - AES_192
  - AES_256
- Hash Algorithms:
  - GOST
  - SHA_1

Сценарий построения VPN туннеля между двумя подсетями, защищаемыми шлюзами безопасности CSP VPN Gate

Описание стенда

Демонстрационный стенд (Рисунок 86) представлен двумя шлюзами безопасности CSP VPN Gate, которые защищают две локальные подсети (SN1 и SN2). Подсети могут общаться между собой только по защищенному каналу (VPN), создаваемому между шлюзами безопасности. Внутри подсетей SN1 и SN2 трафик является “открытым”. Настройку шлюзов будем проводить с рабочей станции Host1.

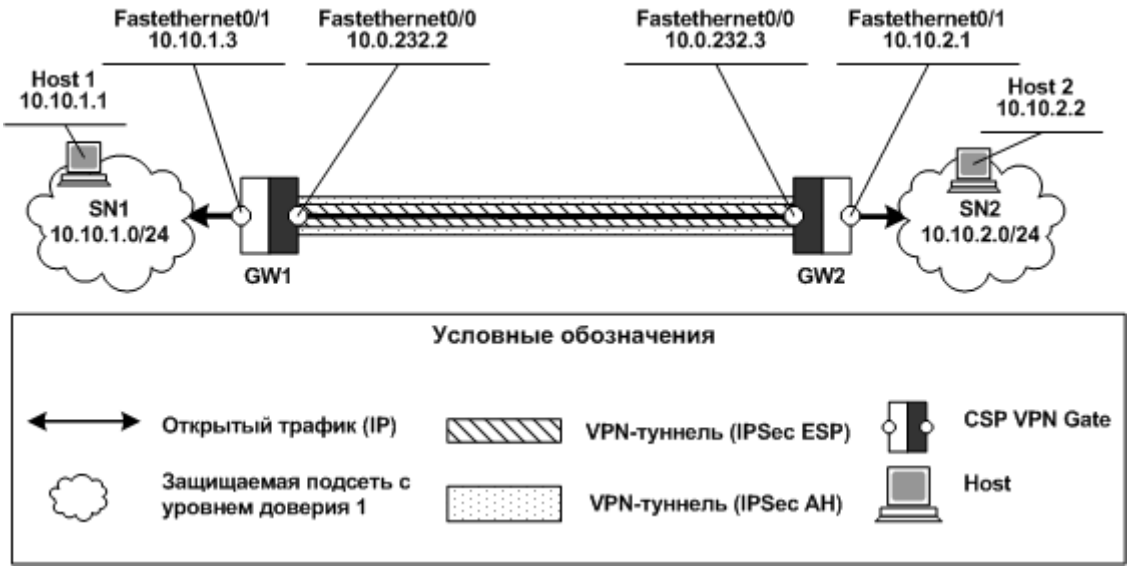

Рисунок 86

Параметры защищенного соединения:

- 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

Перед созданием политик безопасности шлюзов необходимо настроить маршрутизацию и убедиться в том, что на устройствах стенда сделаны корректные настройки.

Настройка шлюза безопасности GW1

На Host1 в окне браузера введем адрес интерфейса шлюза безопасности GW1 – http://10.10.1.3. Появится окно с заставкой CSP VPN Gate и текстом, предупреждающим о запрете закрытия этого окна во время сессии работы с продуктом.

Одновременно будет запущен Java апплет, который откроет окно CSP VPN Login (Рисунок 3). В окне нужно ввести имя пользователя "cscons" и его пароль ("csp"). После ввода логина и пароля будет загружена действующая конфигурация со шлюза безопасности GW1, и откроется окно главной формы на разделе Overview (Рисунок 7).

Нам необходимо настроить GW1 таким образом, чтобы он защищал весь трафик, направляемый из подсети SN1 в подсеть SN2. Для этого мы должны построить VPN туннель между GW1 и GW2. Для построения туннеля нам потребуется:

- создать набор преобразований (transform set) с параметрами, которые будут использоваться при шифровании трафика
- описать IKE политику – указать параметры и алгоритмы, необходимые для создания SA 1 фазы, который будет использоваться GW1 и GW2 при согласовании параметров SA 2 фазы
- создать предопределенный ключ, который будет использоваться для аутентификации
- создать правило для защиты трафика между подсетями (IPsec Rule)
- создать IPsec Policy, описывающую параметры создаваемого VPN туннеля
- создать VPN Connection, связывающее IPsec Policy с внешним интерфейсом GW1
- загрузить созданную конфигурацию на GW1.

Первые четыре пункта могут быть выполнены в произвольном порядке. Мы начнем с создания IPsec Rule.

Создание IPsec Rule

Для создания IPsec Rule перейдем в раздел Rules, нажав одноименную кнопку на тулбаре.

Выделяем в дереве узел IPSec Rules и нажимаем кнопку Add. В открывшемся окне (Рисунок 87) в поле Name/Number вводим номер для создаваемого IPsec Rule, например, 110.

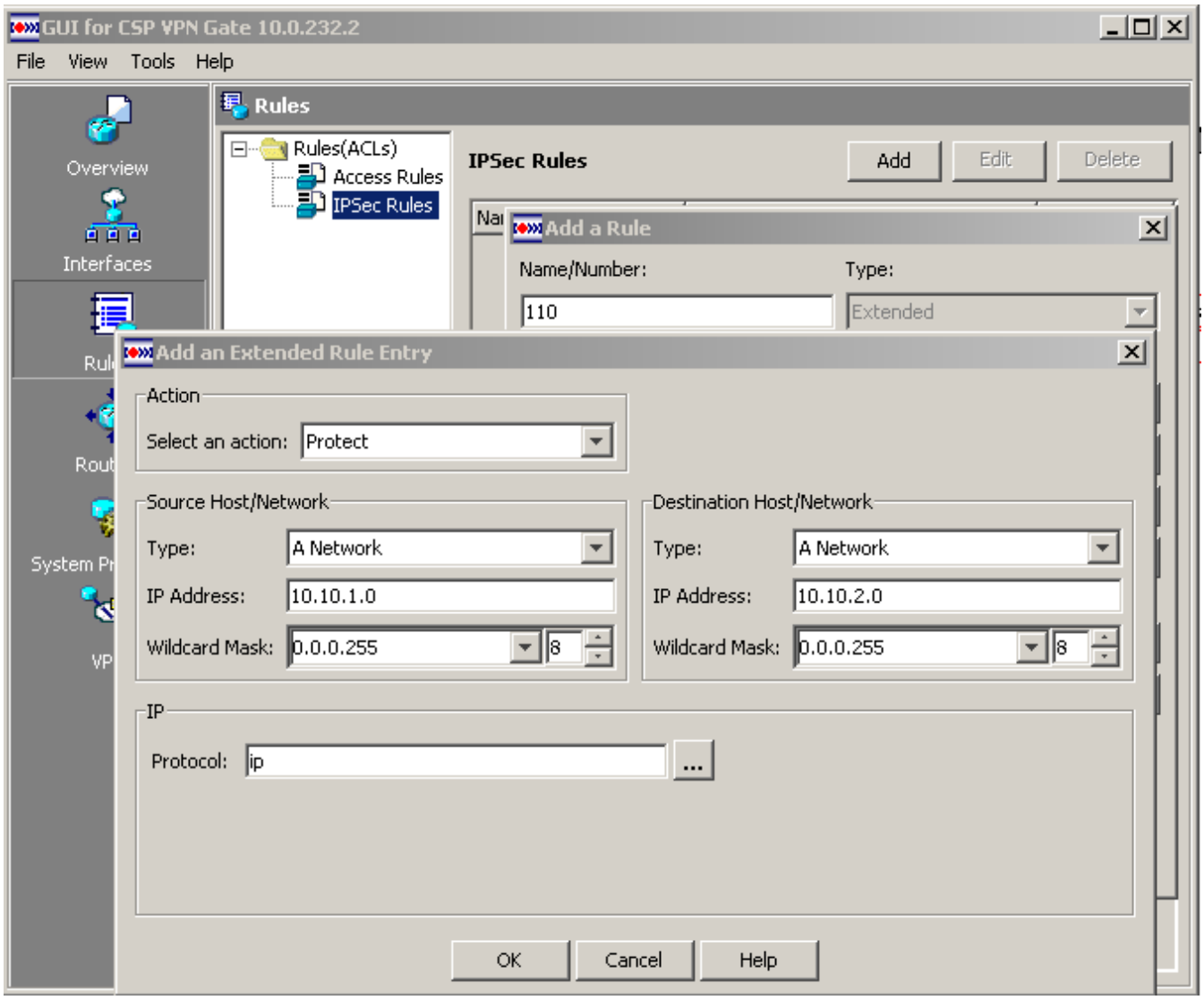

Рисунок 87

После этого переходим к созданию записи правила - нажимаем кнопку Add, откроется окно (Рисунок 87), в котором выполняем следующие настройки:

Action = ‘Protect’

Source Host/Network:

Type = ‘A Network’
IP Address = 10.10.1.0 – адрес подсети, защищаемой GW1
Wildcard Mask = 0.0.0.255

Destination Host/Network:

Type = ‘A Network’
IP Address = 10.10.2.0 – адрес подсети, с которой строим VPN туннель
Wildcard Mask = 0.0.0.255

IP Protocol = ‘ip’

Нажимаем ОК и возвращаемся в главное окно продукта.

Теперь нужно настроить параметры VPN и построить VPN Connection. Для этого переходим в раздел VPN нажатием одноименной кнопки на вертикальном тулбаре. Нам предстоит настроить следующие параметры:

- Transform Set
- IKE Policy

- Pre-Shared Key
- Global Settings.

Создание Transform Set

Для создания Transform Set переходим в соответствующий раздел, выделив в дереве узел Transform Sets. Изначально в нем отсутствует какая-либо информация (Рисунок 88). Нажимаем кнопку Add и в открывшемся окне устанавливаем параметры:

Name = ‘TS1‘

Устанавливаем флажок Data Integrity and Encryption (ESP)

Integrity Algorithm = ‘none‘

Encryption Algorithm = ‘ESP_GOST‘

Устанавливаем флажок Data and address Integrity without Encryption (AH)

Integrity Algorithm = ‘AH_GOST_HMAC‘

Устанавливаем переключатель в положение Tunnel (Encrypt data and IP header).

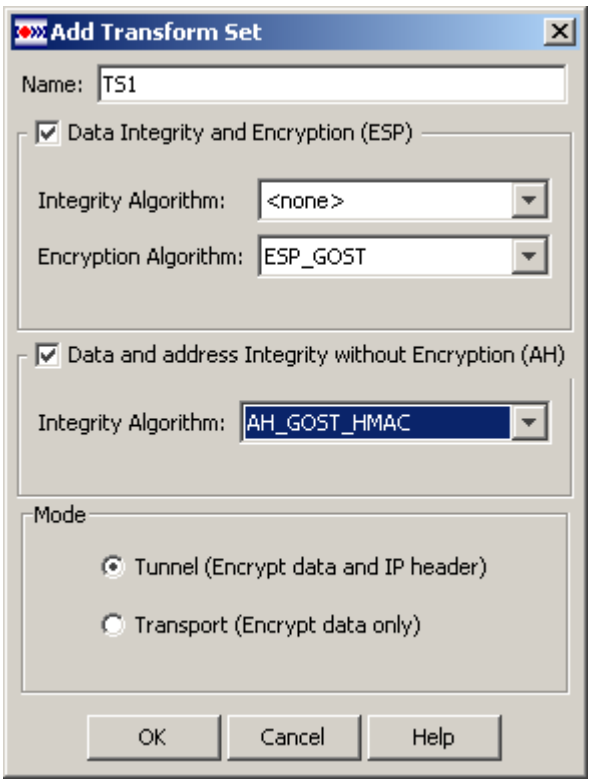

Рисунок 88

Нажимаем ОК и возвращаемся в главную форму.

Политика IKE

Укажем параметры для создания безопасного соединения и выберем метод аутентификации партнеров. В дереве IKE выбираем узел IKE Policies и нажимаем кнопку Add. В открывшемся окне (Рисунок 89) устанавливаем следующие настройки:

Priority – ‘1‘

Authentication method – ‘PRE_SHARE‘

Encryption Algorithm – ‘GOST‘

Hash Algorithm – ‘GOST‘

Oakley Group – ‘group2‘

SA Lifetime (Sec) – ‘86400‘.

Нажимаем ОК и возвращаемся в главную форму.

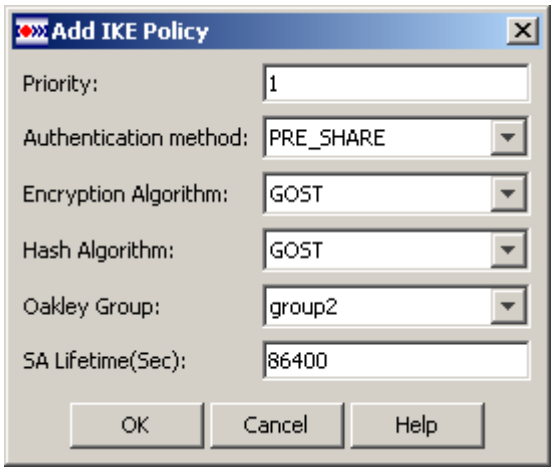

Рисунок 89

Создание Pre-Shared Key

Для создания Pre-Shared Key войдем в раздел Pre-Shared Keys, выделив в дереве одноименный узел. Нажимаем кнопку Add. В открывшемся окне (Рисунок 90) производим следующие действия:

- В поля Pre-Shared Key и Re-Enter Key вводим значение предопределенного ключа. Этот ключ будет использоваться для аутентификации партнеров. Оба партнера должны иметь ключ с одинаковым значением. Об этом стоит помнить при настройке второго шлюза безопасности.
- В качестве типа партнера выбираем Host (IP Address).
- В поле IP Address вводим адрес внешнего интерфейса GW2 – 10.0.232.3.

Нажимаем кнопку ОК и возвращаемся в главную форму.

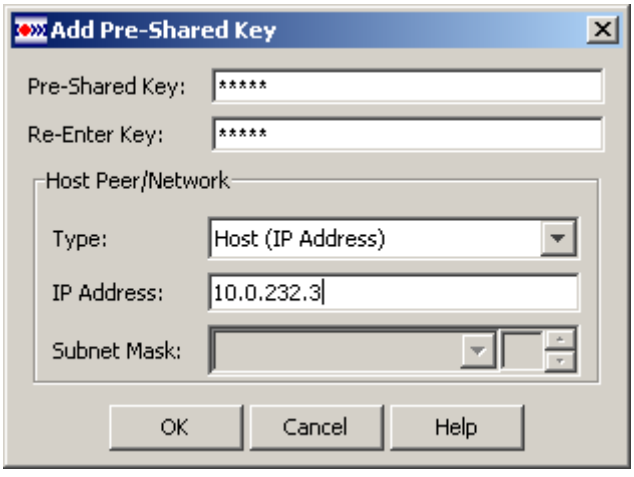

Рисунок 90

Установка Global Settings

Для изменения параметров Global Settings выделяем в дереве одноименный узел и нажимаем кнопку Edit. В открывшемся окне (Рисунок 91) устанавливаем параметры:

Identity – ‘ADDRESS‘

IKE CFG Pool – ‘none‘

IPSec SA Lifetime (Kilobytes – ‘4608000‘

IPSec SA Lifetime (Seconds) – ‘3600‘

Нажимаем кнопку OK и возвращаемся в главную форму.

Рисунок 91

Создание IPsec Policy

Следующий этап – создаем IPsec Policy (криптографическую карту). Для этого выполним следующие действия:

- Выделяем в дереве узел IPSec Policies, что переводит нас в одноименный раздел.
- Нажимаем кнопку Add. Будет открыто окно Add IPSec Policy
- Присваиваем создаваемой IPsec Policy имя, например, site_to_site (вводим это значение в поле Name).
- Добавляем в IPsec Policy статическую криптографическую карту, для чего нажимаем кнопку Add. Будет открыто одноименное окно.

В открывшемся окне производим следующие действия:

- Во вкладке General оставляем значения, установленные по умолчанию.
- Во вкладке Peer Information регистрируем IP Address внешнего интерфейса GW2, с которым мы будем строить VPN туннель. Для этого в поле IP Address вводим адрес 10.0.232.3 и нажимаем кнопку Add. Адрес будет добавлен в список Peer List.
- Во вкладке Transform Sets выделяем в списке Available Transform Sets созданный ранее трансформ с именем TS1 и нажимаем кнопку со стрелкой направо. Выделенный трансформ будет перенесен в список Selected Transform Sets.
- Во вкладке IPSec Rule выбираем из выпадающего списка значение Use Rule Pane for selection.
- Откроется окно выбора ранее созданного IPsec Rule. В этом окне (Rule Pane) выделяем ранее созданное IPsec правило – 110 и нажимаем кнопку Select. Номер выбранного правила будет демонстрироваться в выпадающем списке IPsec Rule.

- Вкладку IKE CFG мы не трогаем, так как не предполагаем работу с удаленным (мобильным) пользователем.
- Во вкладке Identities никаких действий не производим.

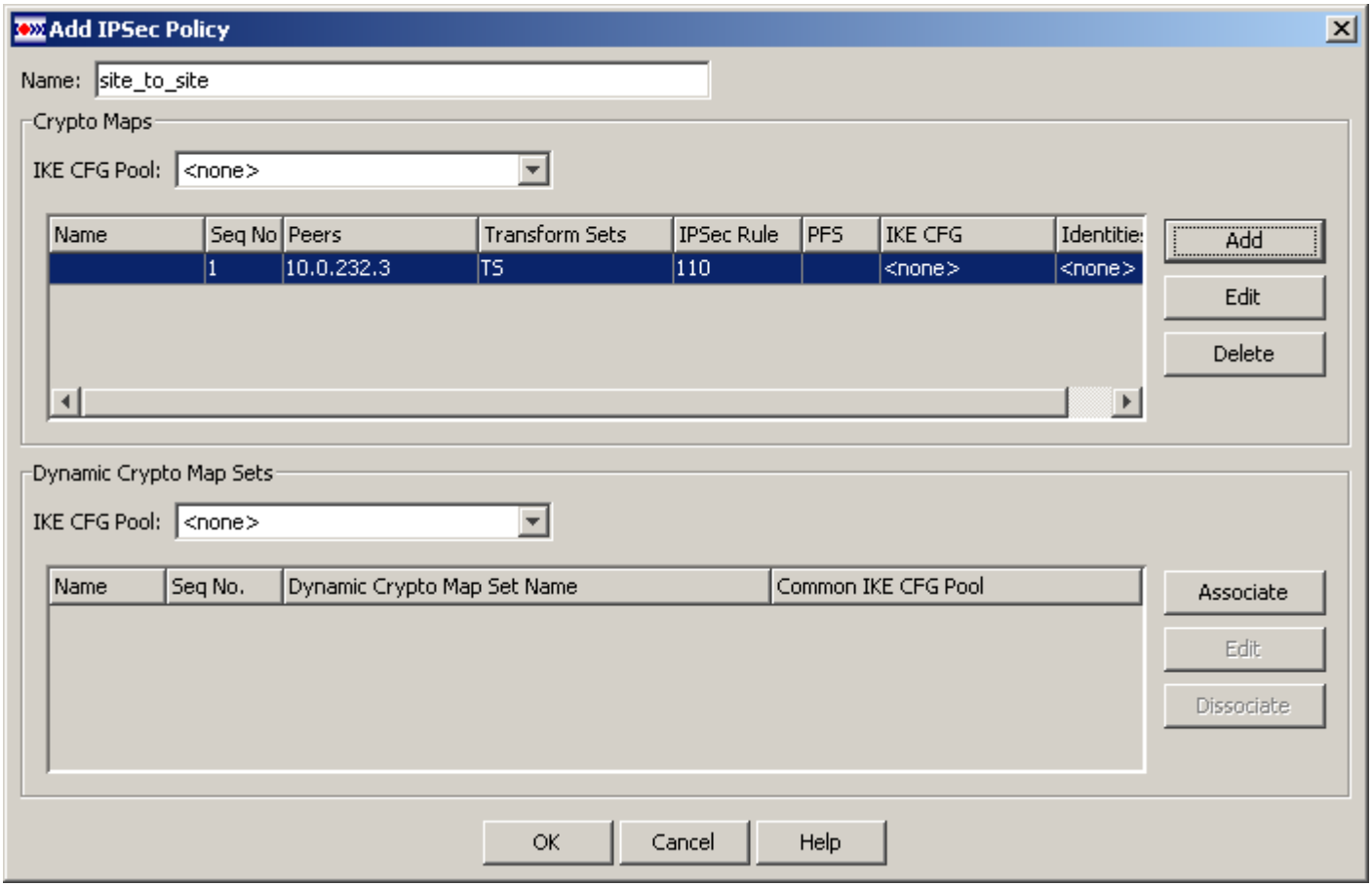

Рисунок 92

Нажимаем кнопку OK и возвращаемся в окно Add IPSec Policy (Рисунок 92). В окне появилась запись о только что созданной криптографической карте. Для реализации нашего сценария этого достаточно, поэтому мы закрываем это окно нажатием кнопки OK и переходим в главное окно.

В таблице IPSec Policies появилась запись о созданной IPsec Policy.

Параметры VPN туннеля

Переходим к выбору параметров для создания VPN туннеля. Для этого выполняем следующие действия:

- В дереве выделяем узел VPN и нажимаем кнопку Add на правой панели. Будет открыто окно Add VPN Connection.
- Из списка Select Interface выбираем внешний интерфейс конфигурируемого шлюза безопасности (GW1) – FastEthernet0/0.
- Из списка Select IPSec Policy выбираем имя только что созданной IPsec Policy – site_to_site (Рисунок 93).

Нажимаем кнопку OK и переходим в главное окно продукта.

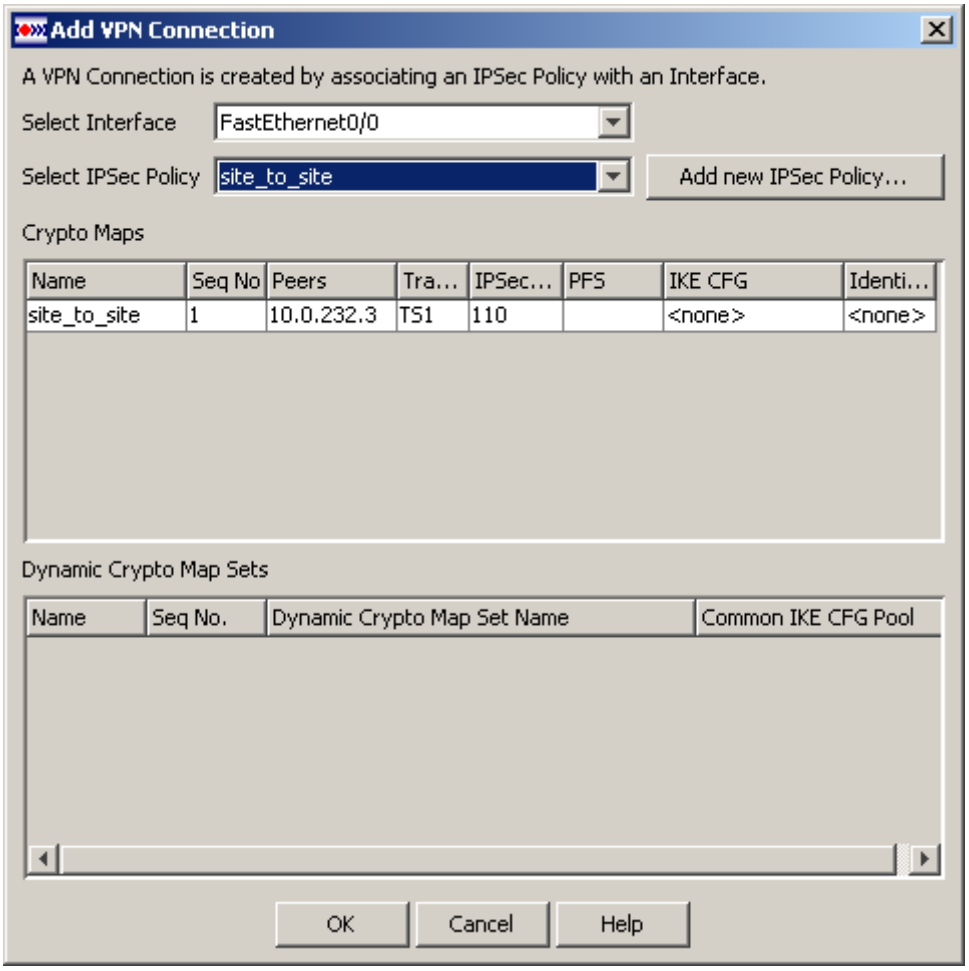

Рисунок 93

Загрузка конфигурации на GW1

Следующим этапом будет загрузка созданной конфигурации на GW1. Для этого в меню File выбираем команду Deliver to Router. Откроется окно Deliver Configuration to Router (Рисунок 94). В этом окне будут отображаться команды, в которые были интерпретированы наши действия по настройке шлюза безопасности GW1. Нажимаем кнопку Deliver. Появится окно с индикатором процесса доставки конфигурации и с предложением подождать его окончания. После успешной доставки окно с индикатором автоматически закроется.

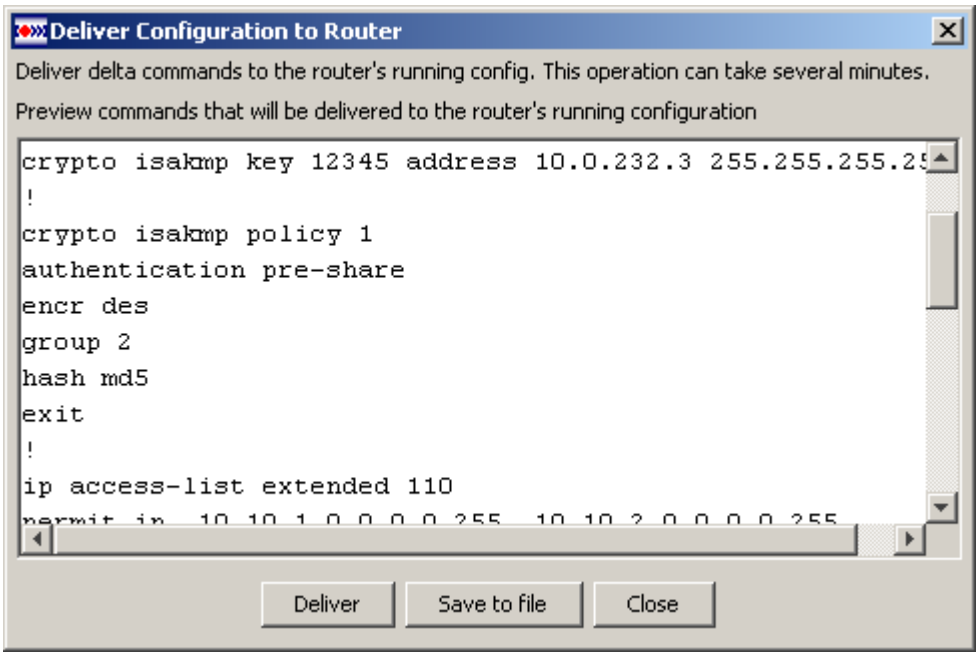

Рисунок 94

На этом настройка шлюза GW1 закончена.

Текст cisco-like конфигурации для GW1

В GUI в меню View выберите команду Current Config для просмотра cisco-like конфигурации GW1:

```
hostname GW
enable password csp
username cscons privilege 15 password 0 csp
crypto isakmp key 12345 address 10.0.232.3 255.255.255.255
!
crypto isakmp policy 1
authentication pre-share
encr des
group 2
hash md5
exit
!
ip access-list extended 110
permit ip  10.10.1.0 0.0.0.255  10.10.2.0 0.0.0.255
exit
!
crypto ipsec transform-set TS1 esp-des ah-md5-hmac
mode tunnel
exit
```



```
!
crypto map site_to_site 1 ipsec-isakmp
match address 110
no reverse-route
set transform-set TS1
set peer 10.0.232.3
exit
!
interface FastEthernet0/0
ip address 10.0.232.2 255.255.0.0
crypto map site_to_site
exit
!
end
```

Настройка шлюза безопасности GW2

В окне браузера на Host1 введем адрес интерфейса шлюза безопасности GW2 – http://10.0.232.3. Появится окно с заставкой CSP VPN Gate , после чего будет открыто окно логина.

Вводим логин и пароль.

После некоторого ожидания будет открыто главное окно графического интерфейса. В этом окне мы повторим практически все те же действия, что и при настройке GW1.

Будут некоторые отличия:

Изменится порядок подсетей при создании записи в IPsec Rule.

Action = ‘Protect’

Source Host/Network:

Type = ‘A Network’

IP Address = 10.10.2.0 – адрес подсети, защищаемой GW2

Wildcard Mask = 0.0.0.255

Destination Host/Network:

Type = ‘A Network’

IP Address = 10.10.1.0 – адрес подсети, с которой строим VPN туннель

Wildcard Mask = 0.0.0.255

IP Protocol = ‘ip’

При создании криптографической карты во вкладке Peer Information мы вводим адрес GW1 – 10.0.232.2.

При создании предопределенного ключа IP-адрес партнера – 10.0.232.2.

Все остальные настройки полностью совпадают с настройками, произведенными для GW1.

Текст cisco-like конфигурации для GW2

```
hostname GW
enable password csp
username cscons privilege 15 password 0 csp
crypto isakmp key 12345 address 10.0.232.2 255.255.255.255
!
crypto isakmp policy 1
authentication pre-share
encr des
group 2
hash md5
exit
!
ip access-list extended 110
permit ip  10.10.2.0 0.0.0.255  10.10.1.0 0.0.0.255
exit
!
crypto ipsec transform-set TS1 esp-des ah-md5-hmac
mode tunnel
exit
!
crypto map site_to_site 1 ipsec-isakmp
match address 110
no reverse-route
set transform-set TS1
set peer 10.0.232.2
exit
!
interface FastEthernet0/0
ip address 10.0.232.3 255.255.0.0
crypto map site_to_site
exit
!
end
```

Проверка работоспособности стенда

После загрузки конфигурации на GW2 проверяем работу VPN туннеля с помощью команды Ping. Для этого выполняем команду Ping 10.10.1.1 с хоста Host 2. Также выполним команду Ping 10.10.2.2 с хоста Host 1. В результате выполнения команды Ping между устройствами GW1 и GW2 должен установиться VPN туннель. Убедимся в этом, запустив из меню Tools

графического интерфейса команду SA Manager, показывающую все созданные защищенные соединения.

Мы только что создали конфигурацию, разрешающую общение между подсетями SN1 и SN2 только по защищенному каналу, т.е. через VPN туннель. Остальные контакты разрешены, но не будут защищаться. В рамках собранного стенда, когда организовано соединение между подсетями не через Интернет, а через общую подсеть, дополнительных фильтров (правил пакетной фильтрации) создавать не требуется.