ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Web-based интерфейс управления: инструкция по установке и использованию

РЛКЕ.00009-01 90 03

16.09.2014

Содержание

Web-based интерфейс управления: инструкция по установке и использованию

Настроить шлюз безопасности S-Terra Gate можно удаленно, используя Web-based графический интерфейс управления (GUI). Графический интерфейс является опциональной частью Продукта S-Terra Gate и выделен в отдельный пакет. Инсталляция GUI производится отдельно.

Для получения опционального пакета sterragategui_4.1-xxxxx_all.deb обратитесь в службу поддержки по адресу support@s-terra.com.

Инсталляция

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

```
dpkg –i sterragategui_4.1-xxxxx_all.deb
```

Во время инсталляции выполняется настройка Apache:

```
DocumentRoot /opt/VPNagent/cspmc
<Directory /opt/VPNagent/cspmc>
 Options Indexes FollowSymLinks MultiViews
 AllowOverride None
 Order allow,deny
 Allow from all
</Directory>
```


Деинсталляция

Для деинсталляции GUI выполните команду:

```
dpkg –P sterragategui
```

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.

Начальная конфигурация шлюза для удаленного управления

После инициализации S-Terra Gate и инсталляции GUI рекомендуется загрузить начальную конфигурацию, которая позволит в дальнейшем создать защищенный канал для удаленной настройки политики безопасности. Создание начальной конфигурации описано в документе «Настройка шлюза», раздел «Общие настройки шлюза», подраздел «Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза».

Старт графического интерфейса управления

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

После этого происходит проверка наличия на компьютере установленного Продукта Java SE 7. Если этот Продукт не установлен или установлена версия ниже, то появляется окно с предложением инсталлировать последнюю версию. После инсталляции Java и перезагрузки системы в окне браузера (Рисунок 1) появится заставка S-Terra Gate GUI 4.1:

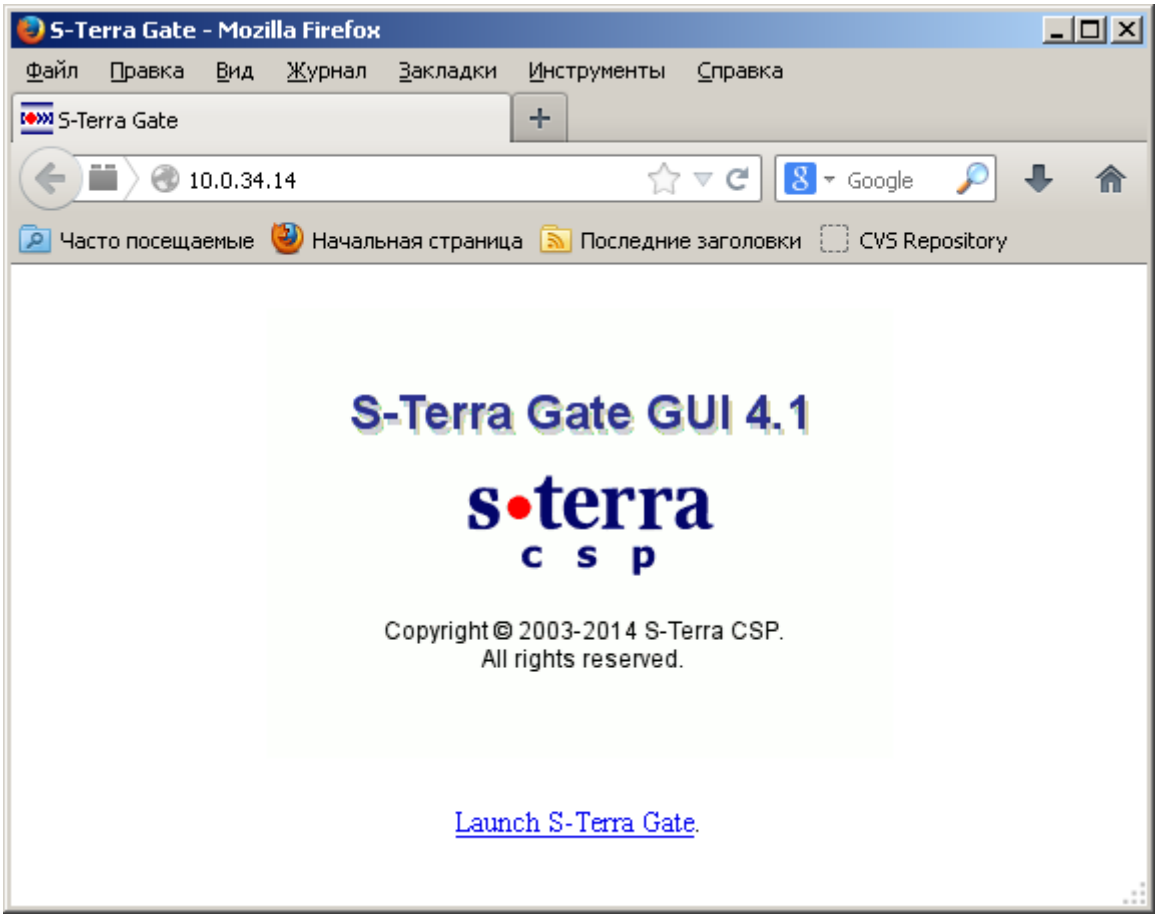

Рисунок 1

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

Нажмите на ссылку Launch S-Terra Gate, чтобы запустить GUI, либо через несколько секунд будет запуск по умолчанию. Появится окно (Рисунок 2), в котором надо разрешить запуск S-Terra Gate GUI.

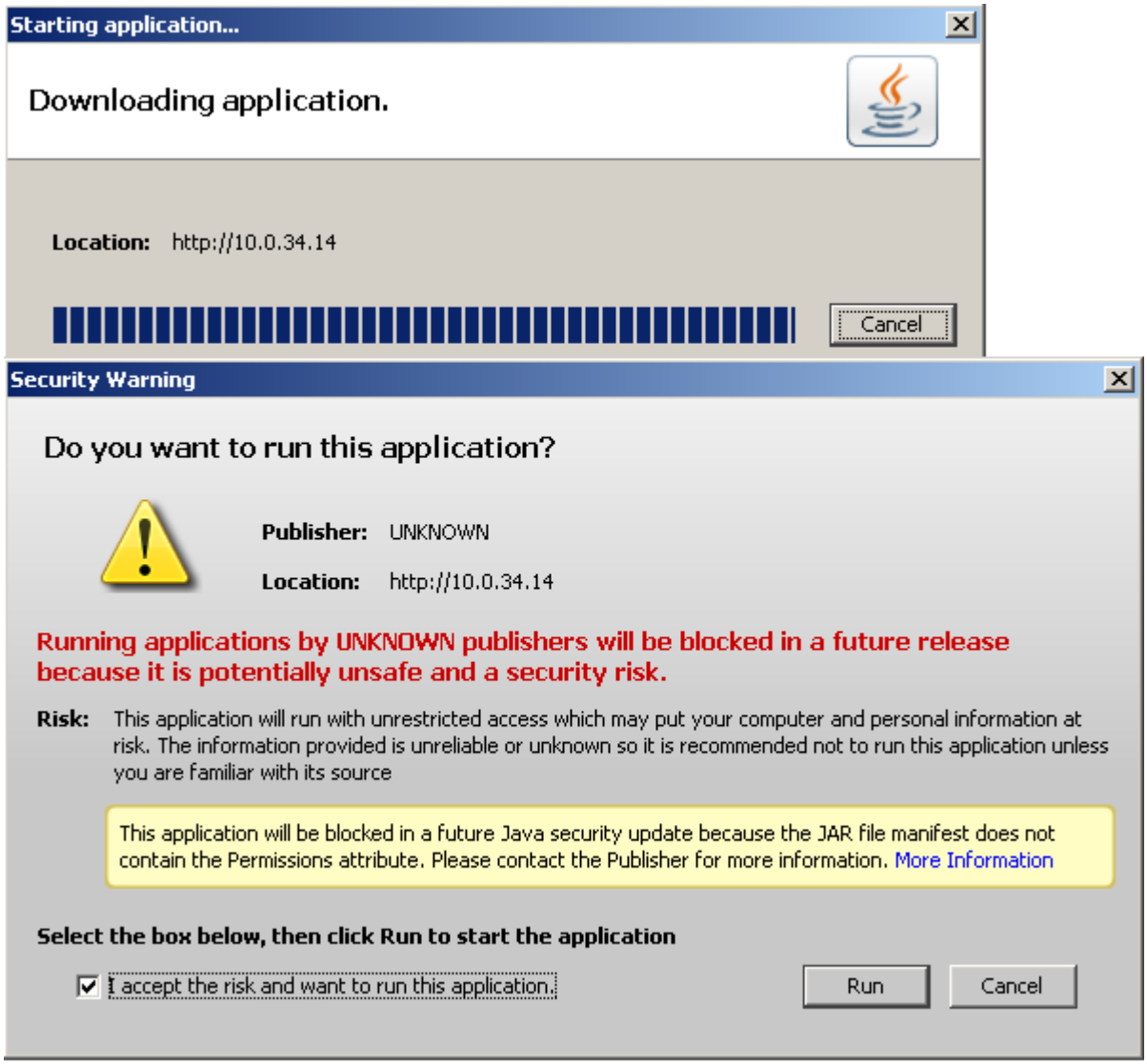

Рисунок 2

Откроется окно ввода имени пользователя и пароля (Рисунок 3). При инициализации Продукта S-Terra Gate создается специальный пользователь с именем "cscons" и паролем "csp". Этот пароль рекомендовалось изменить после окончания инициализации.

В окне *S-Terra Gate Login* нужно ввести имя пользователя "cscons" и его новый пароль:

Рисунок 3

После ввода имени пользователя и пароля, и нажатия кнопки OK будет открыто окно (Рисунок 4), сообщающее о том, что Продукт S-Terra Gate загружает конфигурацию со шлюза безопасности:

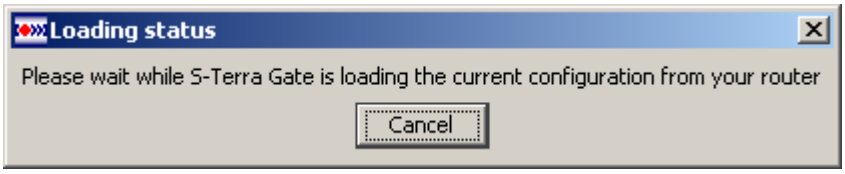

Рисунок 4

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 5) на разделе *Overview* (Обзор). Рассмотрим элементы главной формы, описание раздела *Overview* будет дано ниже.

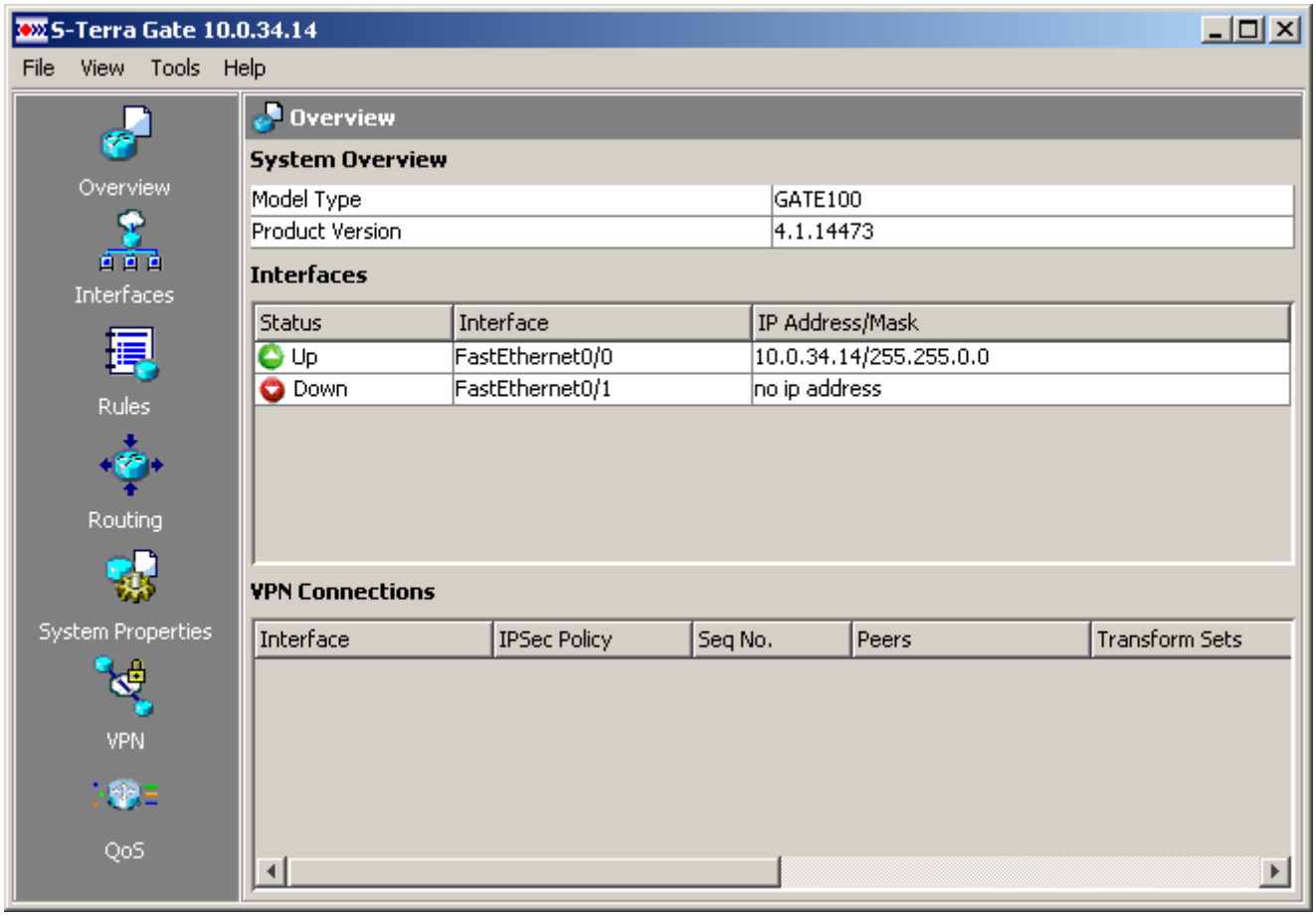

Рисунок 5

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

Нижеследующие пункты меню открывают соответствующие разделы графического интерфейса:

- *Overview*
- *Interfaces*
- *Rules*
- *Routing*
- *System*
- *VPN*
- *Quality of Service.*

Эти пункты меню продублированы на панели инструментов слева от браузера.

Посмотреть конфигурацию можно с помощью следующих команд:

- *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 S-Terra 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 6).

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

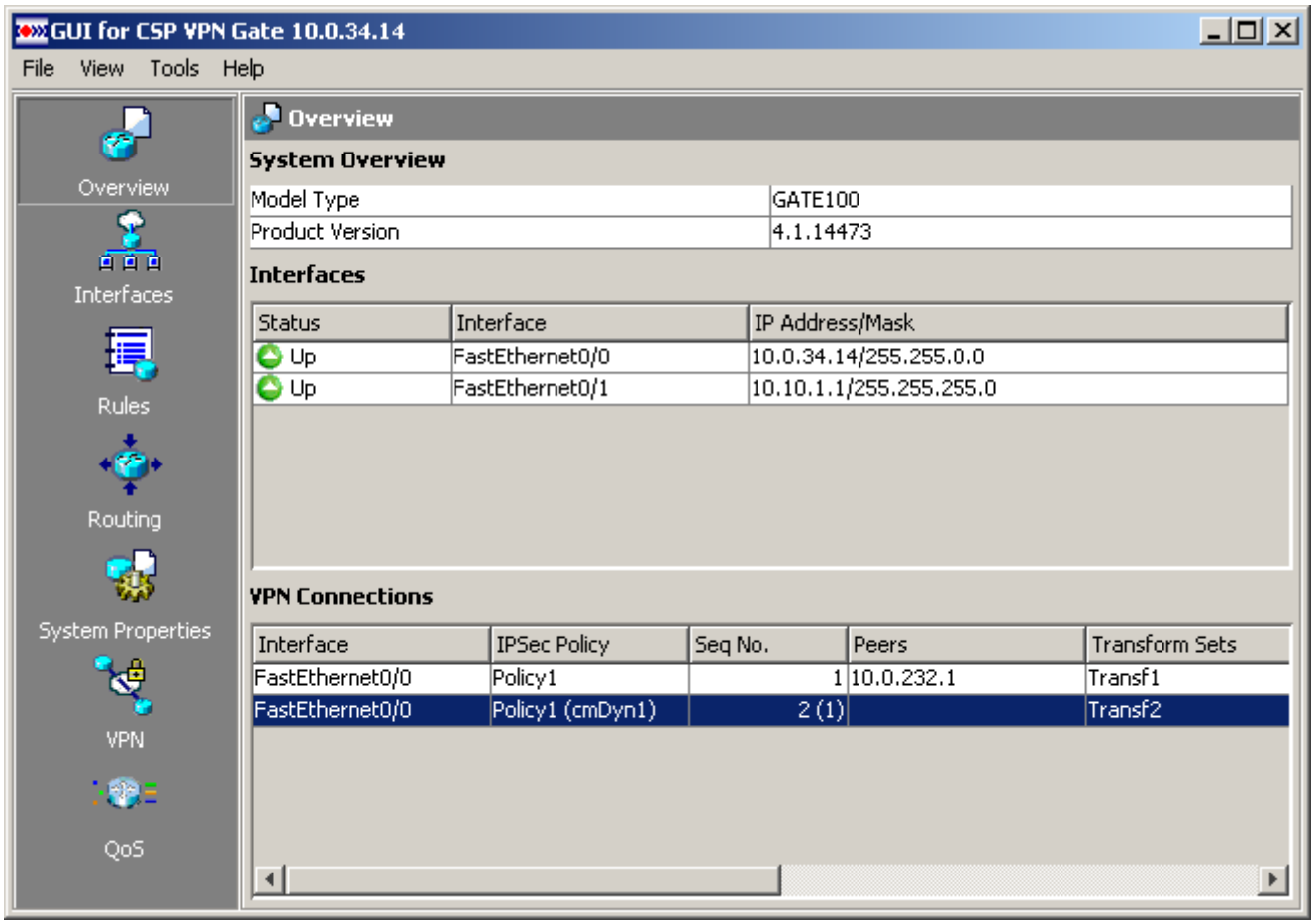

Рисунок 6

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 S-Terra 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* – 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.
- *IKECFG pool* – имя пула адресов, используемого криптографической картой.
- *RRI* – показывает включен или выключен (*On/Off)* механизм RRI (Reverse Route Injection) для соединений, создаваемых с помощью данной криптографической карты.
- *Identities* – имя списка идентификаторов.

Interfaces

Раздел *Interfaces* (Рисунок 7) предназначен для редактирования параметров сетевых интерфейсов. Физические интерфейсы не создаются, а считываются из конфигурации устройства. В разделе *Interfaces* отображаются все сетевые интерфейсы, на которые установлен драйвер Продукта. В этом разделе можно назначить или поменять IP-адрес и маску интерфейса, установить MTU, можно привязать к интерфейсу правила фильтрации трафика, задать для интерфейса политику безопасности и качество сервиса. Эти правила и политики могут быть заранее созданы в соответствующих разделах, а также имеется возможность создать их при редактировании параметров интерфейса.

Коротко рассмотрим назначение некоторых параметров, связанных с интерфейсом:

- Правила доступа (Access Rules) предназначены для пакетной фильтрации входящего и исходящего трафика.
- Политики IPsec (IPSec Policy) задают параметры построения защищенного соединения.
- Правила проверки (Inspect Rules) предназначены для контекстной фильтрации входящего и исходящего трафика.
- Политики (Policy Maps) задают необходимый сервис обслуживания входящего и исходящего сетевого трафика, основанного на классификации трафика и его маркировке.

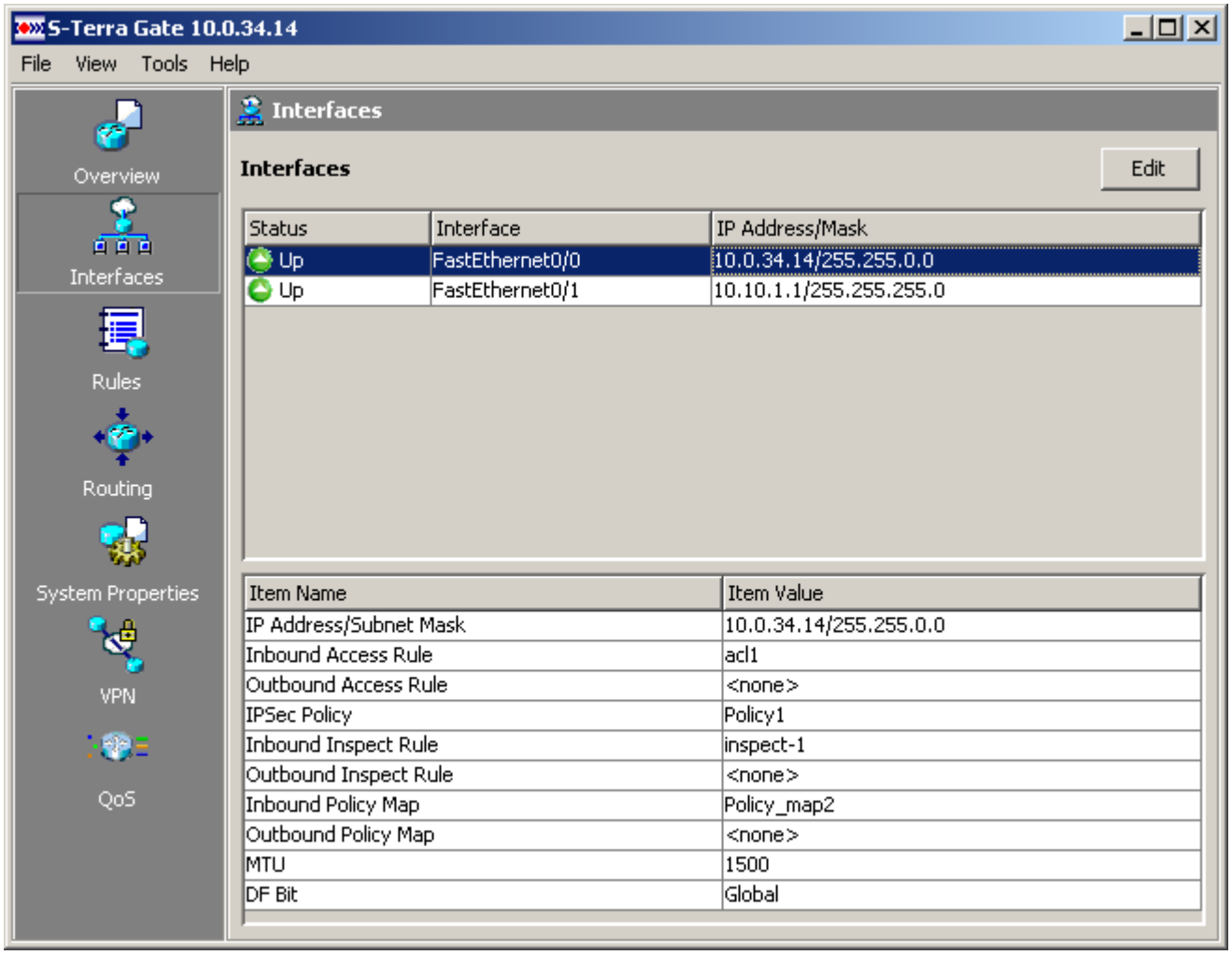

Рисунок 7

Состав элементов браузера раздела *Interfaces*:

- *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.
- Кнопки управления:
  - Edit – кнопка вызова окна редактирования выделенного интерфейса. 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.
    - *Inbound Access Rule* – правило доступа для входящего трафика, привязанное к данному интерфейсу.
    - *Outbound Access Rule* – правило доступа для исходящего трафика.
    - *IPSec Policy* – политика IPsec, связанная с данным интерфейсом.
    - *Inbound Inspect Rule* – правило проверки для входящего трафика, привязанное к данному интерфейсу.
    - *Outbound Inspect Rule* – правило проверки для исходящего трафика, привязанное к данному интерфейсу.
    - *Inbound Policy Map* – политика, задающая сервис обслуживания для входящего трафика.
    - *Outbound Policy Map* – политика, задающая сервис обслуживания для исходящего трафика.
    - *MTU* – максимальный размер пакета, передаваемый без фрагментации через интерфейс.
    - *DF Bit* – устанавливает DF-бит внешнего IP-заголовка пакета.
  - *Item Value* – столбец со значениями описанных выше параметров интерфейса. Если не задан адрес, то показывается значение *no ip address*. Если правила не установлены, то столбец будет содержать значение <*none*>. Для *MTU* и *DF Bit* изначально показываются значения, установленные по умолчанию.

Редактирование параметров физического интерфейса

Чтобы отредактировать параметры физического интерфейса, в разделе *Interfaces* (Рисунок 7) выберите интерфейс и нажмите кнопку Edit. Появится окно *Edit Interface Properties* (Рисунок 8).

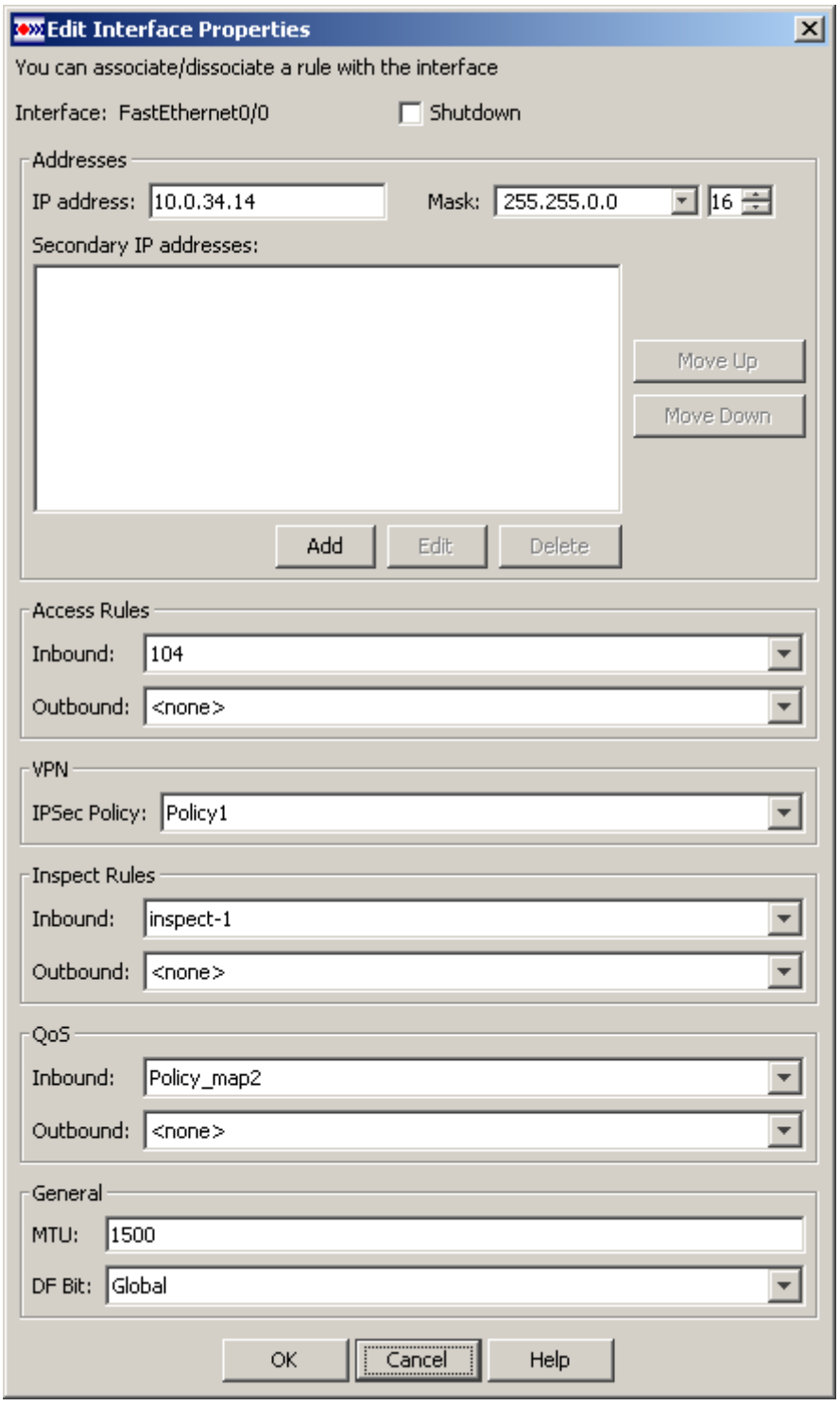

Рисунок 8

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.
  - *Secondary IP addresses* – список вторичных адресов назначенных на интерфейс.
  - Add – при нажатии на кнопку появляется окно *Add secondary address* (Рисунок 9), в котором можно назначить вторичные адреса на интерфейс.
  - Edit – кнопка предназначена для редактирования выделенного вторичного адреса интерфейса.
  - Delete – кнопка предназначена для удаления выделенного вторичного адреса с интерфейса.
  - Move Up – управляет порядком вторичных адресов на интерфейсе, сдвигает выделенный адрес на одну позицию вверх.
  - Move Down – управляет порядком вторичных адресов на интерфейсе, сдвигает выделенный адрес на одну позицию вниз.
- Группа *Access Rule* – позволяет задать или выбрать правило доступа для входящего и исходящего трафика для выбранного интерфейса. В поле *Inbound* указывается правило для входящего трафика, в поле *Outbound* – для исходящего 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 выбора правила доступа *Rule Pane* (Рисунок 10). Выбранное правило доступа будет отображаться в поле выбора Access Rule для заданного направления трафика.
  - *Create new* – открывает диалог создания правила доступа *Add a Rule*, подробно описанный в разделе Rules «Создание нового правила доступа» (Рисунок 16). В открывшемся окне, кнопка *Associate* будет отсутствовать, в отличие от окна, изображенного на Рисунок 16, так как уже подразумевается связь правила доступа с текущим интерфейсом. После создания правила и нажатия кнопки OK, имя или номер правила будут отображаться в поле выбора Access Rule для заданного направления трафика, а правило доступа заносится в список Access Rules (Рисунок 15).
- 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 *IPSec Policy Pane* (Рисунок 11). Выбранная политика IPsec отобразится в поле выбора IPSec Policy.
  - *Create new* – открывает диалог *Add IPSec Policy* (Рисунок 61) создания новой IPsec Policy. Создание новой политики IPsec описано в разделе «Создание IPsec Policy». Созданная политика IPsec заносится в список IPSec Policy.

- Группа *Inspect Rule* – позволяет задать или выбрать правило проверки для входящего и исходящего трафика на выбранном интерфейсе. В поле *Inbound* указывается правило для входящего трафика, в поле *Outbound* – для исходящего трафика. Поле выбора правила проверки содержит выпадающий список значений:
  - *<none>* – к интерфейсу правило доступа не привязано.
  - *Use Inspect Rule Pane for selection* – при выборе этого предложения будет открыто окно выбора правила проверки *Inspect Rule Pane* (Рисунок 12). Выбранное правило проверки заносится в поле выбора Inspect Rules для заданного направления трафика.
  - *Create new* – открывает диалог создания правила проверки *Add Inspect Rule*, подробно описанный в разделе «Inspect Rules. Создание правила проверки» (Рисунок 28). После создания правила и нажатия кнопки OK, имя правила будут отображаться в поле выбора правила проверки для заданного направления трафика, а также добавится в список Inspect Rules в разделе Inspect Rules.
- Группа *QoS* – позволяет выбрать политику (Policy Map), задающую необходимый сервис обслуживания сетевого трафика на выбранном интерфейсе, основанный на классификации трафика и его маркировке. В поле *Inbound* указывается политика для входящего трафика, в поле *Outbound* – для исходящего трафика. Поле выбора Policy Map содержит выпадающий список значений:
  - *<none>* – к интерфейсу политика (Policy Map) не привязана.
  - *Use Policy Map Pane for selection* – при выборе этого предложения будет открыто окно выбора *Policy Map Pane* (Рисунок 13). Выбранная Policy Map отобразится в поле выбора для заданного направления трафика.
  - *Create new* – открывает диалог создания политики, задающей сервис обслуживания *Add Policy Map*, подробно описанный в разделе «Quality of Service. Policy Maps.Создание Policy Map» (Рисунок 99). После создания Policy Map и нажатия кнопки OK, новая Policy Map будет отображаться в поле выбора Policy Map для заданного направления трафика, а также добавится в список Policy Map в разделе QoS.
- Группа *General*:
  - *MTU* – максимальный размер пакета, передаваемого без фрагментации через интерфейс. Допустимые значения находятся в диапазоне 68–65535.
  - *DF Bit* – устанавливает DF-бит внешнего IP-заголовка пакета. Список возможных значений:
    - *Global* – берется значение, установленное в разделе *VPN – Global Settings.*
    - *Copy* – DF-бит внешнего IP-заголовка устанавливается в то же значение, какое было у оригинального пакета.
    - *Clear* – DF-бит внешнего IP-заголовка будет очищен и пакет может быть фрагментирован после IPsec инкапсуляции.
    - *Set* – DF-бит внешнего IP-заголовка будет установлен, фрагментация пакета запрещена.

Добавление вторичных адресов на интерфейс

В окне *Add secondary address* (Рисунок 9) происходит добавление новой пары IP-адрес/маска в список *Secondary IP addresses*. Добавление осуществляется в конец списка. 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.

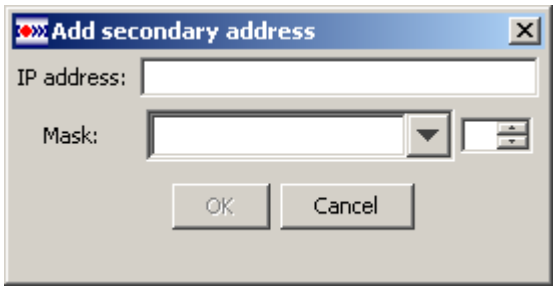

Рисунок 9

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.
- Кнопки управления:
  - Add – вызывает окно *Add a Rule*, в котором можно создать новое правило.
  - Edit – вызывает окно *Edit a Rule*, в котором можно отредактировать уже существующее правило.
  - Delete – удаляет 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.

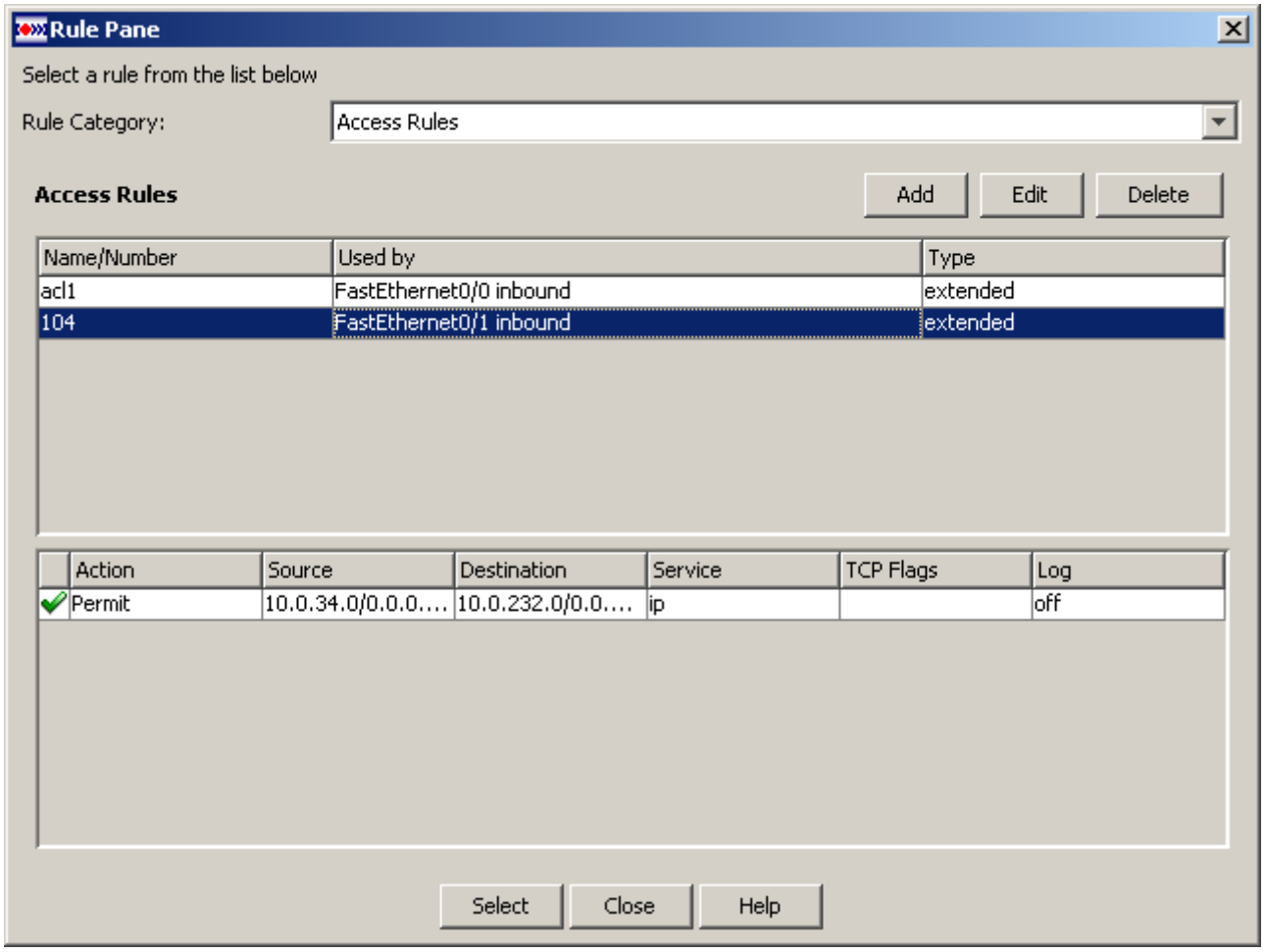

Рисунок 10

Окно выбора политики IPsec

В окне *IPSec Policy Pane* производится выбор политики IPsec (Рисунок 11).

Кнопки управления:

- Add – вызывает окно *Add IPSec Policy*, в котором можно создать новую политику IPsec.
- Edit – вызывает окно *Edit IPSec Policy*, в котором можно отредактировать уже существующую политику IPsec.
- Delete – удаляет политику 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 политики IPsec в верхней таблице и нажатии кнопки Select – политика будет выбрана.

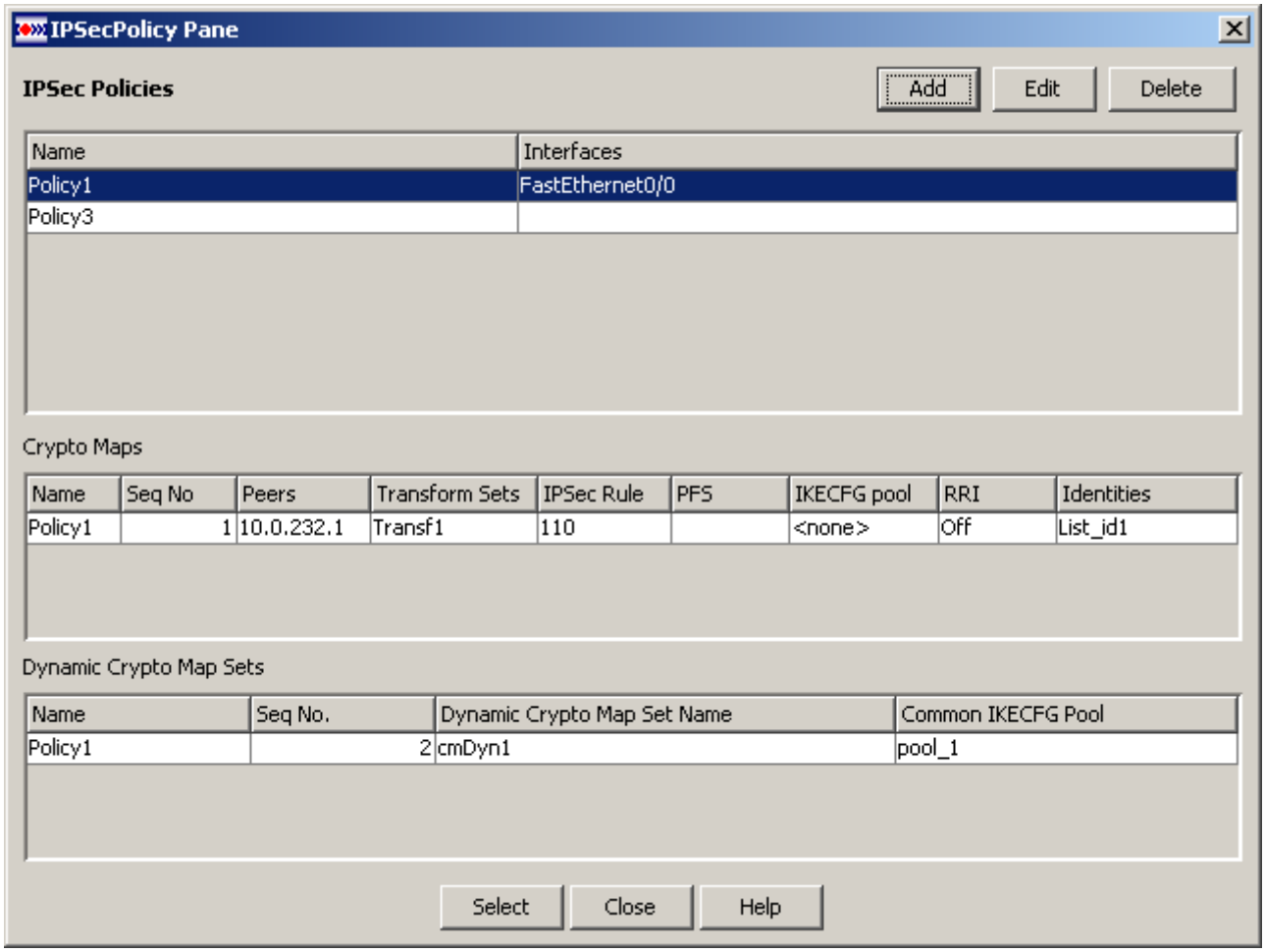

Рисунок 11

Окно выбора правила проверки

Окно *Inspect Rule Pane* (Рисунок 12) содержит следующие элементы:

Кнопки управления:

- Add – вызывает окно *Add Inspect Rule*, в котором можно создать новое правило проверки.
- Edit – вызывает окно *Edit Inspect Rule*, в котором можно отредактировать уже существующее правило проверки.
- Delete – удаляет правило проверки.

Верхняя таблица содержит список всех созданных правил проверки. Состав столбцов таблицы:

- *Name* – имя правила проверки.
- *Inbound* – имя интерфейса, на котором правило проверки применяется к входящему трафику.
- *Outbound* – имя интерфейса, на котором правило проверки применяется к исходящему трафику.

В нижней таблице детализируется содержание выделенного правила проверки.

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

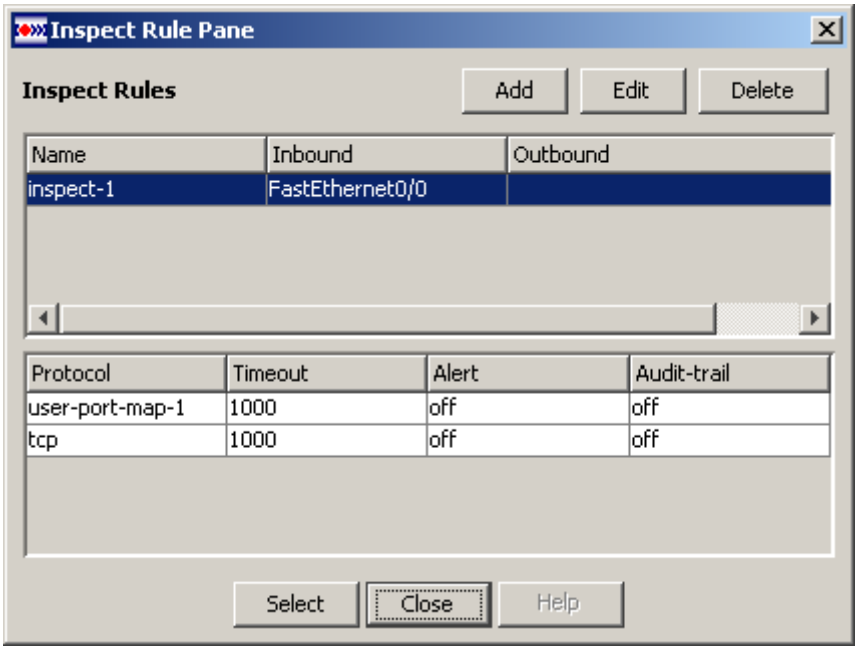

Рисунок 12

Окно выбора Policy Map

В окне *Policy Map Pane* (Рисунок 13) выбирается политика, определяющая сервис обслуживания сетевого трафика.

Кнопки управления:

- Add – вызывает окно *Add Policy Map*, в котором можно создать новую политику работы с классами трафика.
- Edit – вызывает окно *Edit Policy Map*, в котором можно отредактировать уже существующую политику работы с классами трафика.
- Delete – удаляет политику Policy Map.

В верхней таблице окна *Policy Map Pane* содержатся созданные Policy Maps. Таблица состоит из трех столбцов:

- *Name* – имя Policy Map.
- *Input* – имя интерфейса, на котором данная Policy Map будет применяться к входящему трафику.
- *Output* – имя интерфейса, на котором данная Policy Map будет применяться к исходящему трафику.

Нижняя таблица отображает классы с заданными параметрами, относящиеся к выбранной в верхней таблице Policy Map.

Выбор осуществляется выделением Policy Map в верхнем окне и нажатием кнопки Select.

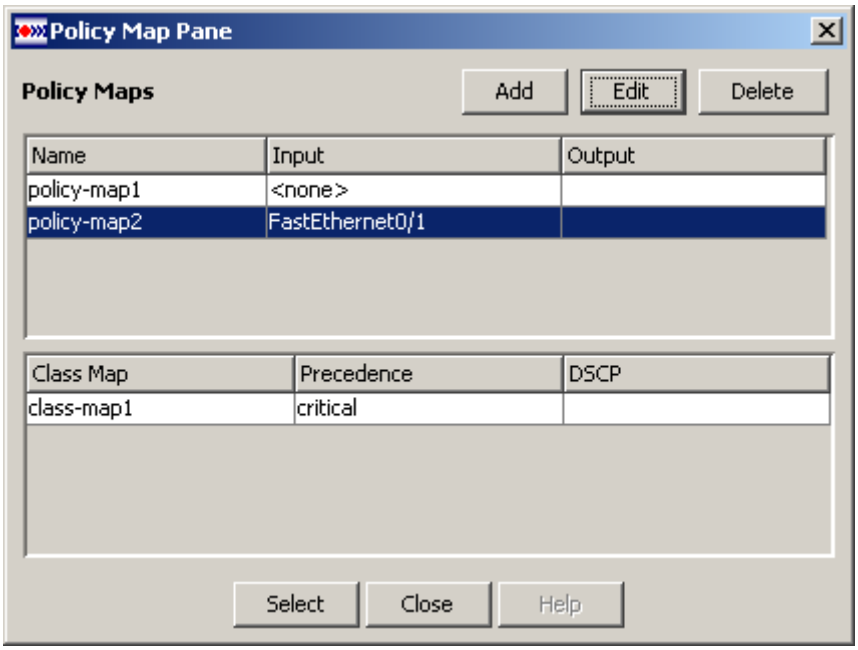

Рисунок 13

Rules

В разделе *Rules* создаются и редактируются правила доступа, правила проверки и правила IPsec. Для расширенных правил доступа можно задать расписание.

Правила доступа и правила проверки привязываются к сетевым интерфейсам. Эти правила используются для пакетной фильтрации и контекстной фильтрации трафика соответственно.

Правила IPsec привязываются к криптографическим картам и применяются для защиты трафика.

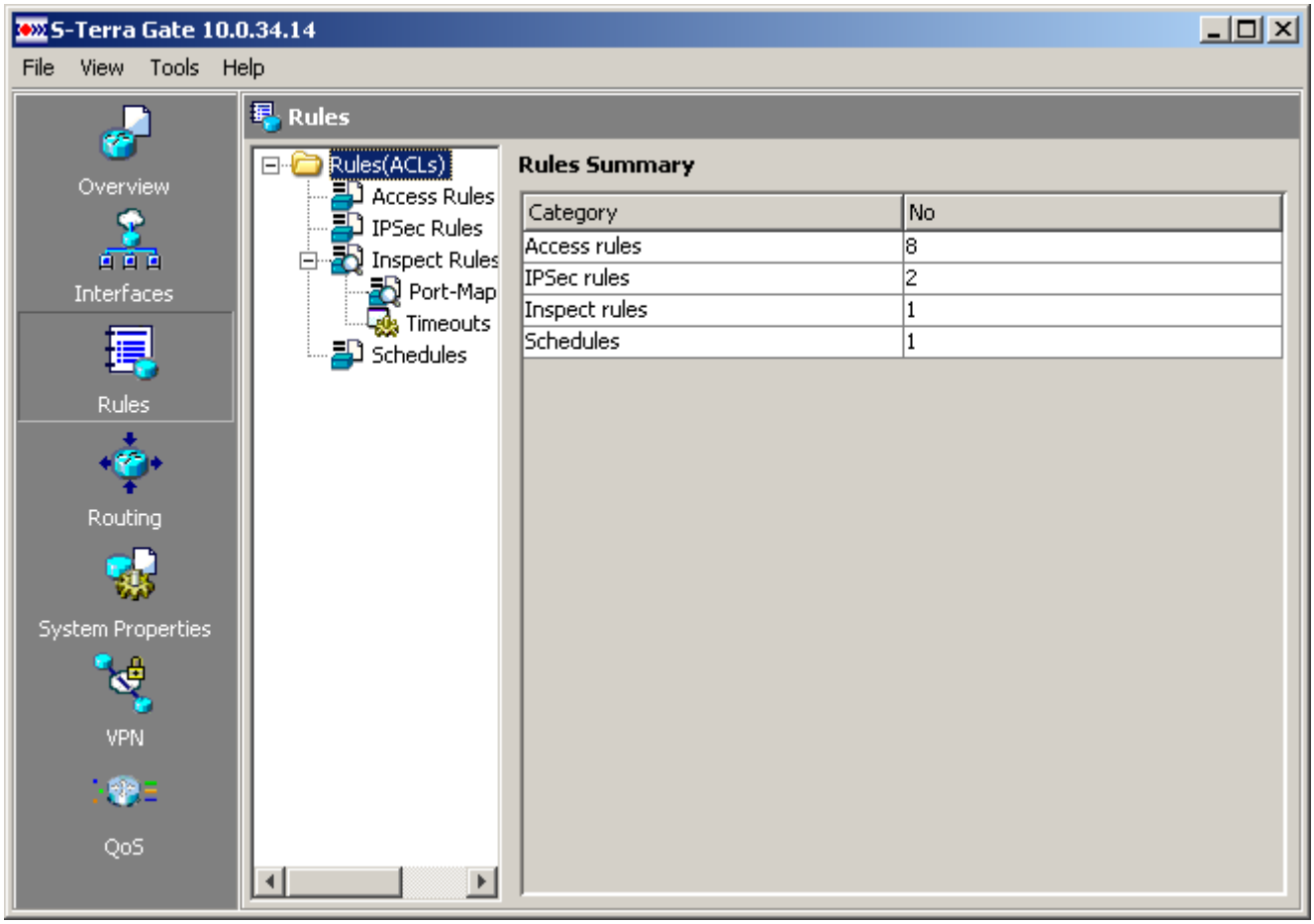

Рисунок 14

Корневой элемент *Rules* имеет четыре раздела:

- *Access Rules* – в этом разделе размещаются стандартные и расширенные правила доступа, которые предназначены для связи с интерфейсами для осуществления пакетной фильтрации трафика.
- *IPSec Rules* – в этом разделе размещаются только расширенные правила IPsec, которые предназначены для связи с криптографическими картами (Crypto Maps – криптографические карты) для защиты трафика.
- *Inspect Rules* – в этом разделе находятся правила проверки трафика для протокола TCP и протоколов прикладного уровня. В этом случае шлюз безопасности выполняет функции межсетевого экрана, используя средства CBAC (управление доступом на основе контекста).
- *Schedules* – в этом разделе задается расписание для расширенных правил доступа.

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

- *Category* – содержит названия правил и расписание.
- *No* – показывает количество правил в каждом разделе и количество созданных расписаний.

Логика размещения правил в Access Rules и IPSec Rules

В политике, которая загружается в S-Terra 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 S-Terra 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* или 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. Пакеты можно фильтровать либо только по адресу отправителя, либо по адресу отправителя пакета, адресу получателя пакета, типу протокола, порту отправителя и порту получателя.

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.

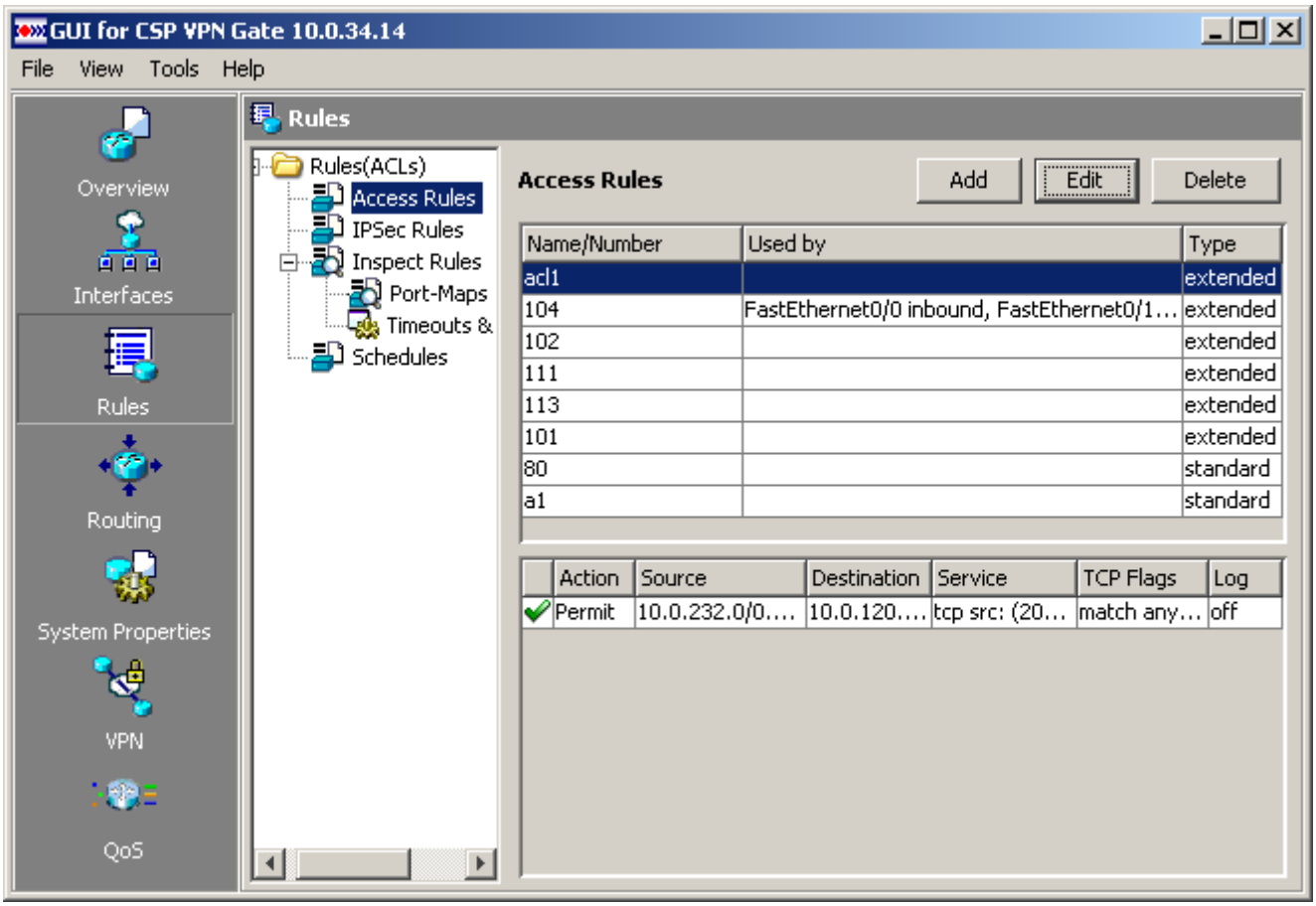

Рисунок 15

Состав элементов браузера раздела *Access Rules*:

- 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/маска отправителя пакета. Возможно значение any.
  - *Destination* – IP-адрес/маска получателя пакета. Возможно значение any.
  - *Service* – сетевой сервис.
  - *TCP Flags* – условие фильтрации по TCP-флагам (для TCP-протокола).
  - *Log* – протоколирование сообщений о пакетах, удовлетворяющих условиям данного правила доступа (*on*/*off* – протоколирование включено/выключено).

Информация в столбце *Service* выводится в соответствии со следующей логикой:

- Если в качестве сетевого сервиса установлен протокол IP или протоколы семейства IP, 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 OK 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 16), которое вызывается кнопкой Add в разделе *Access Rules*.

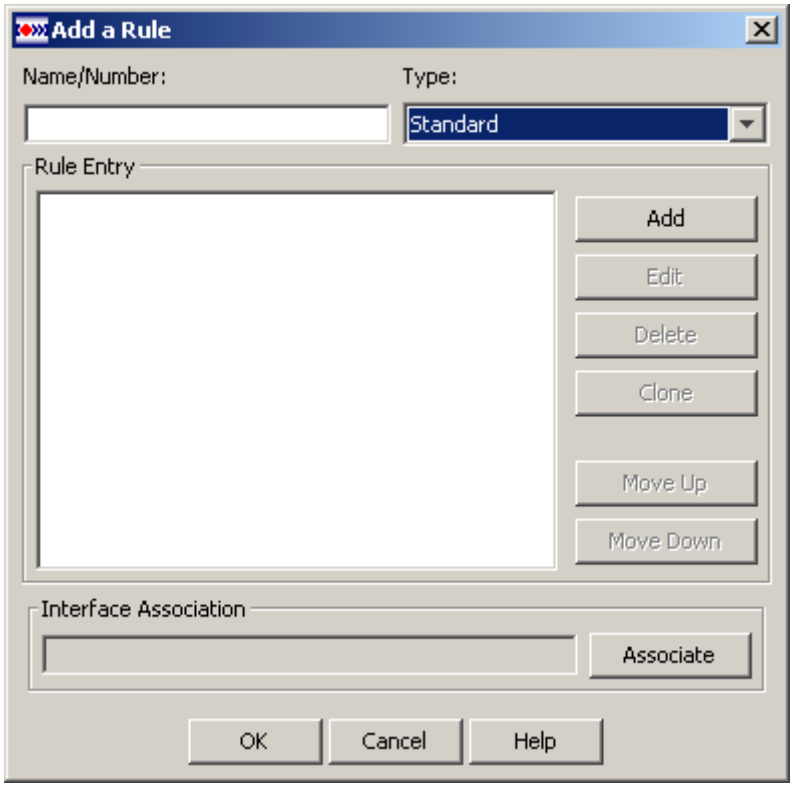

Рисунок 16

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 или Extended.
  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. Для TCP-протокола возможна также фильтрация по TCP-флагам.
  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

Запись для стандартного правила создается в окне *Add a Standard Rule Entry* (Рисунок 17), которое вызывается кнопкой Add в окне *Add a Rule* при выборе типа правила Standard (Рисунок 16).

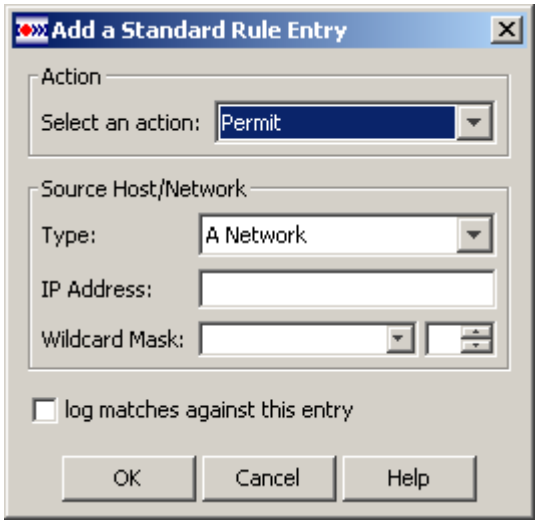

Рисунок 17

Окно *Add a Standard Rule Entry* 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* –этой группе указывается IP-адрес или диапазон IP-адресов отправителя пакетов.
  - *Type* – тип отправителя:
    - *Any IP Address* – любой IP-адрес. Значение по умолчанию.
    - *A Host* – хост.
    - *A Network* – подсеть.
  - *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 16) 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
- при установке значения A Host блокируется элемент Wildcard Mask
- при установке значения Any IP Address будут блокированы элементы IP Address и Wildcard Mask.

- *Log matches against this entry* – установка флажка включает протоколирование сообщения о пакетах, удовлетворяющих условиям данного правила доступа.

Создание записи в расширенном правиле доступа

Для создания записи в расширенном правиле используется окно *Add an Extended Rule Entry* (Рисунок 18), которое вызывается кнопкой Add в окне *Add a Rule* при выборе типа правила Extended (Рисунок 16).

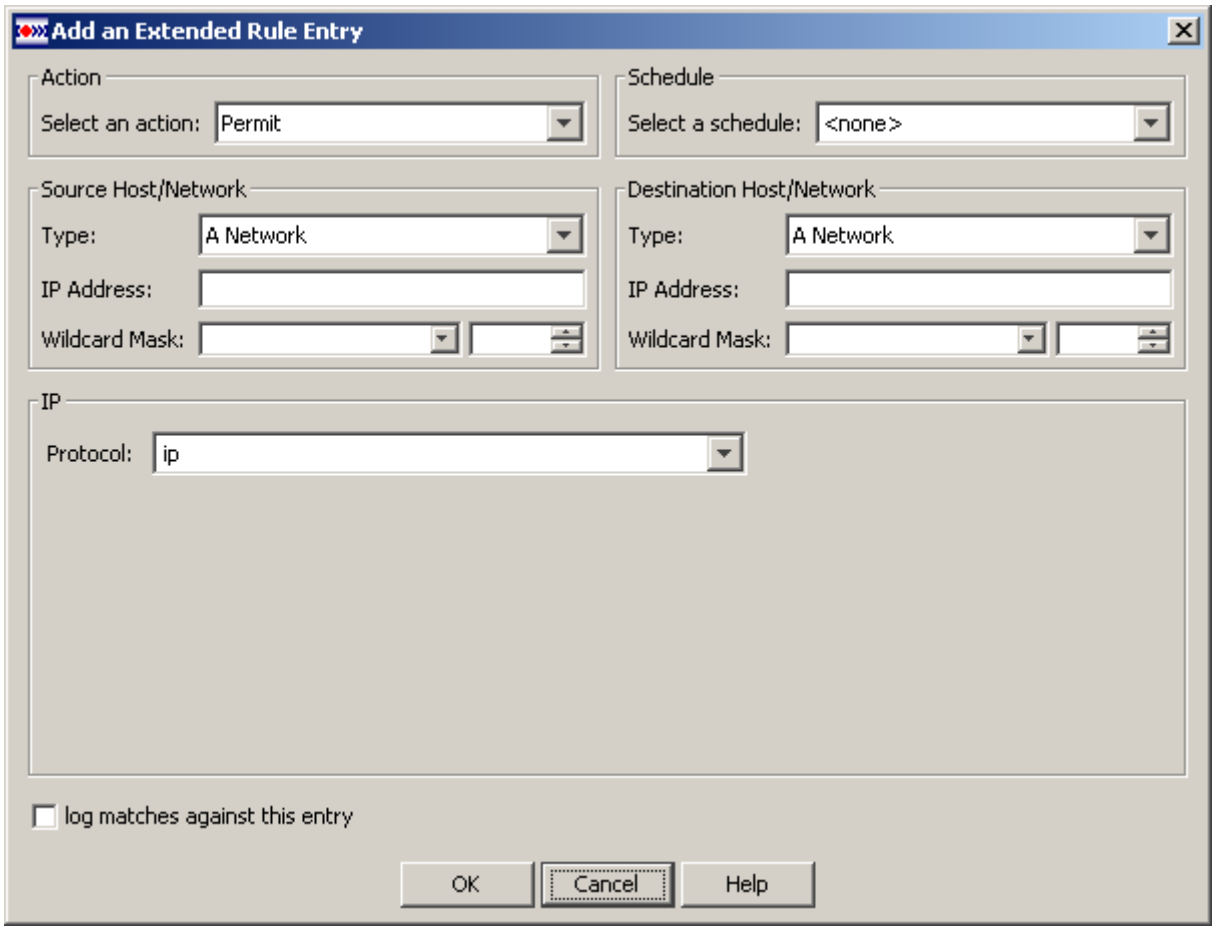

Рисунок 18

Окно *Add an Extended Rule Entry* содержит следующие элементы:

- Группа *Action* – позволяет выбрать действие, которое будет применяться к пакету, подпадающему под данную запись правила: пропускать или не пропускать пакет.
- Группа *Select a schedule* – задает расписание для расширенных правил доступа.
- Группа *Source Host/Network* – в этой группе указывается IP-адрес или диапазон IP-адресов отправителя пакетов.
- Группа *Destination Host/Network* – в этой группе указывается IP-адрес или диапазон IP-адресов получателя пакетов.

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* – протокол выбирается из списка предопределенных протоколов.

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

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

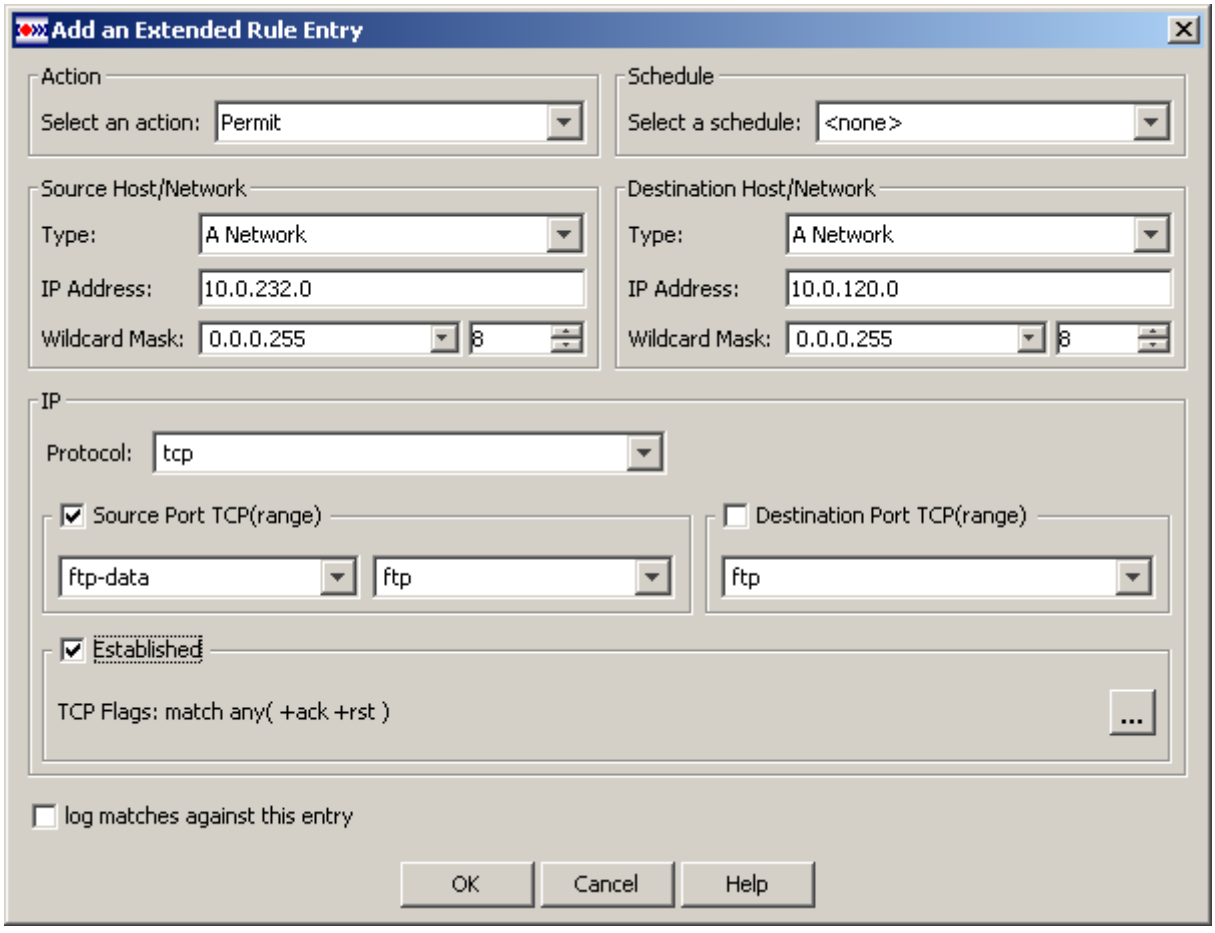

Рисунок 19

- 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 выбрать из предопределенного списка. При вводе вручную возможен ввод как цифровых значений от 0 до 65535, так и названий портов. Если задается одиночный порт, то после выбора значения вместо номера порта будет подставлено его имя.
  Если задается диапазон портов, то после выбора значения 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.
- Группа *Established* – задает дополнительные условия фильтрации для TCP-соединений.
  Флажок *Established* позволяет выделить установленные соединения. Установка или сброс флажка *Established* выставляет или снимает фильтрацию по флагам ack и rst.
  
  – кнопка вызывает окно *TCP Flags Editor* (Рисунок 20), в котором можно указать условие сравнения TCP-флагов в заголовке пакете и правиле.
  Выставленный флажок *Established* эквивалентен условию *match-any* и установленным TCP-флагам ack и rst.
  Диалог правки TCP флагов работает в двух режимах формата ввода – старом и новом. Старый формат ввода включается для расширенных правил с численным идентификатором. При старом формате невозможно задание TCP флага со знаком «-» и значения *match all* (Рисунок 21).
  - Переключатель *match-any* означает, что должно выполняться одно из указанных далее условий по TCP-флагам, *match-all* означает, что должны выполняться все заданные условия по TCP-флагам.
  - Группа *TCP Flags Editor* – задает дополнительные условия фильтрации для TCP-соединений.
    Переключатели:
    «+» – означает, что флаг должен быть установлен,
    «-» – флаг сброшен,
    «any» – любое состояние флага (флаг не проверяется).

Рисунок 20

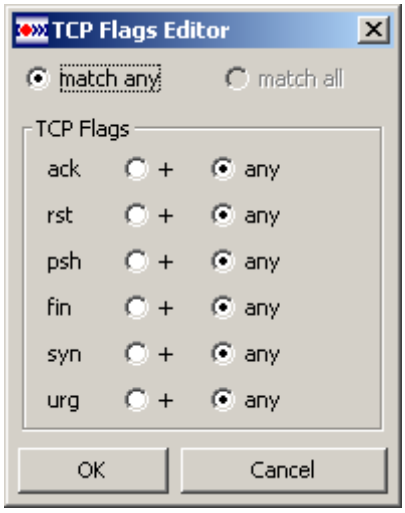

Рисунок 21

Состояние match any +ack, +rst (established) и выставленный флаг +syn является подозрительным с точки зрения безопасности при установленном состоянии *Action* – Permit, делая отправителя уязвимым к syn-атакам и подвергая его опасности несанкционированного доступа. Совпадение всех этих условий приведёт к появлению сообщения:

```
The combination of established and syn TCP flags makes rule
destination vulnerable to syn flooding attacks or undesirable success
```

- *Log matches against this entry* – установка флажка включает протоколирование сообщений о пакетах, удовлетворяющих условиям данного правила доступа.

Редактирование 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 записи в правиле

Нажатие кнопки Clone в окне *Add a Rule* или *Edit a Rule* открывает окно создания новой записи в правиле на основе существующей записи. Клонируется выделенная строка. 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 записи в правиле

Удаление выделенной записи производится кнопкой Delete в окне *Add a Rule/Edit 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 22):

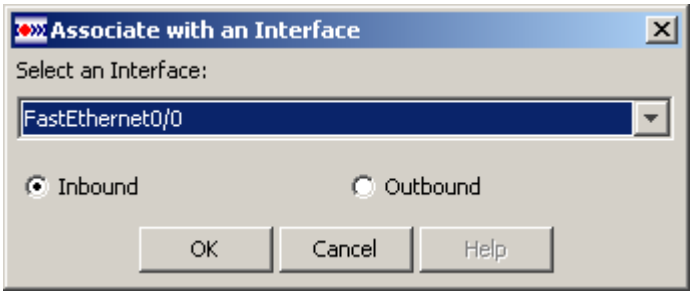

Рисунок 22

Ассоциация правила с интерфейсом означает, что правило начинает работать как фильтрующее для выбранного направления трафика на интерфейсе.

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.

- Переключатели *Inbound* и *Outbound* позволяют выбрать направление трафика на интерфейсе, к которому будет применяться правило доступа.

Если выбранный интерфейс уже имеет связанное с ним правило, то при нажатии кнопки OK 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:

```
The rule <old rule name> already associated to the interface <selected
interface name>. Are you sure you want to dissolve this association?
```

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 правила доступа

Кнопка Edit в разделе *Access Rules* вызывает окно редактирования выделенного правила *Edit a Rule* (Рисунок 23), 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.

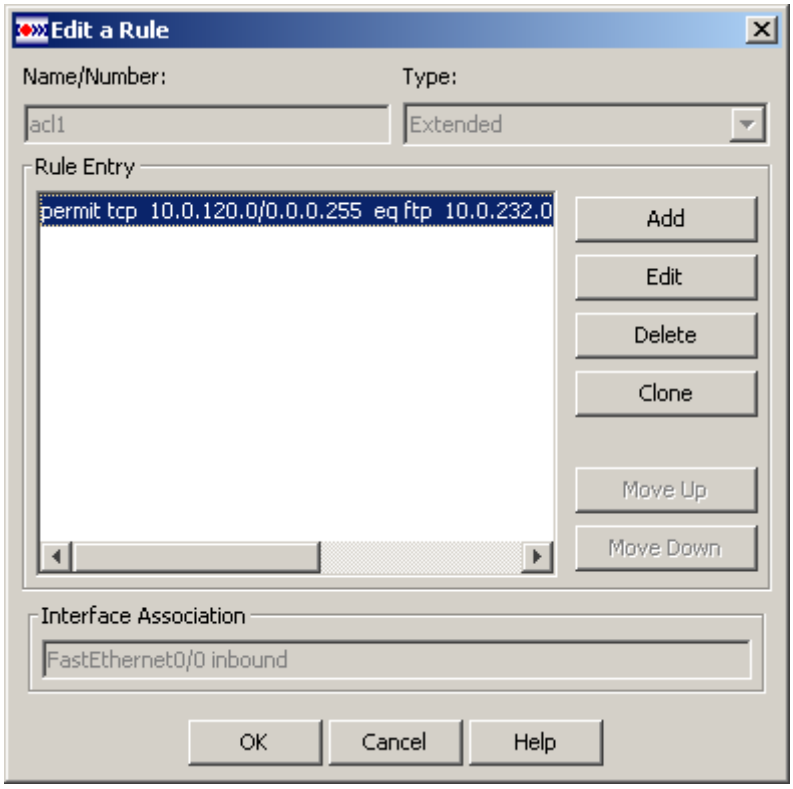

Рисунок 23

Удаление правила доступа

Удаление выделенного в разделе *Access Rules* правила, 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:

```
Cannot delete this rule since it is being used by [Interface Name]. To
delete this rule, firs remove its association with [Interface Name].
```

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

```
Cannot delete this rule since it is being used by crypto map [Map
Name]. To delete this rule, firs remove its association with crypto map
[Map Name].
```


IPSec Rules

В разделе IPSec Rules (Рисунок 24) 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 VPN, подразделе 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.

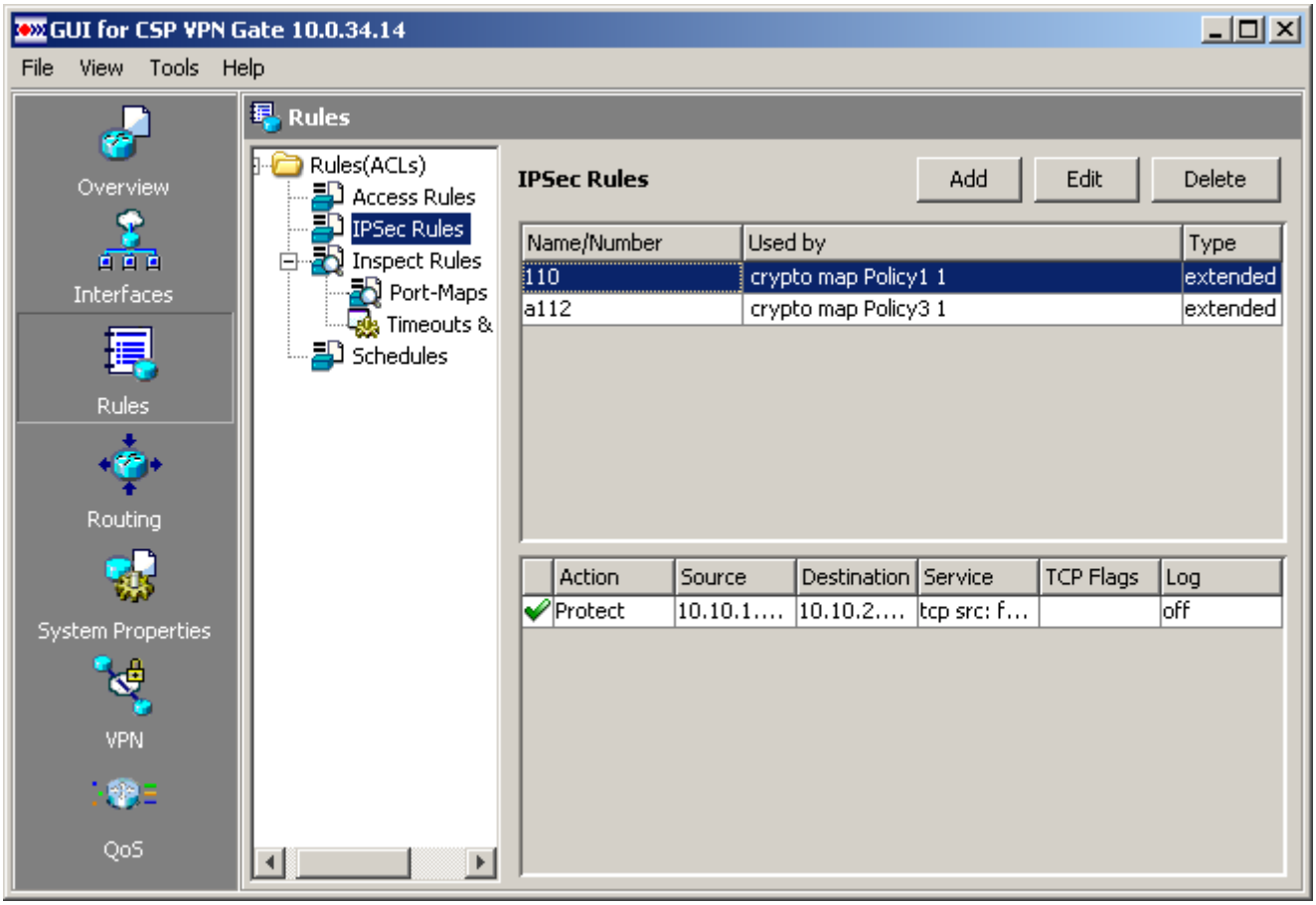

Рисунок 24

Создание нового правила IPsec

Кнопка Add в разделе *IPSec Rules* вызывает окно *Add a Rule* (Рисунок 25), которое совпадает с окном создания нового правила доступа. Отличие только в том, что поля *Type* и *Interface Association* будут блокированы. Поле *Type* блокировано на значении *Extended*.

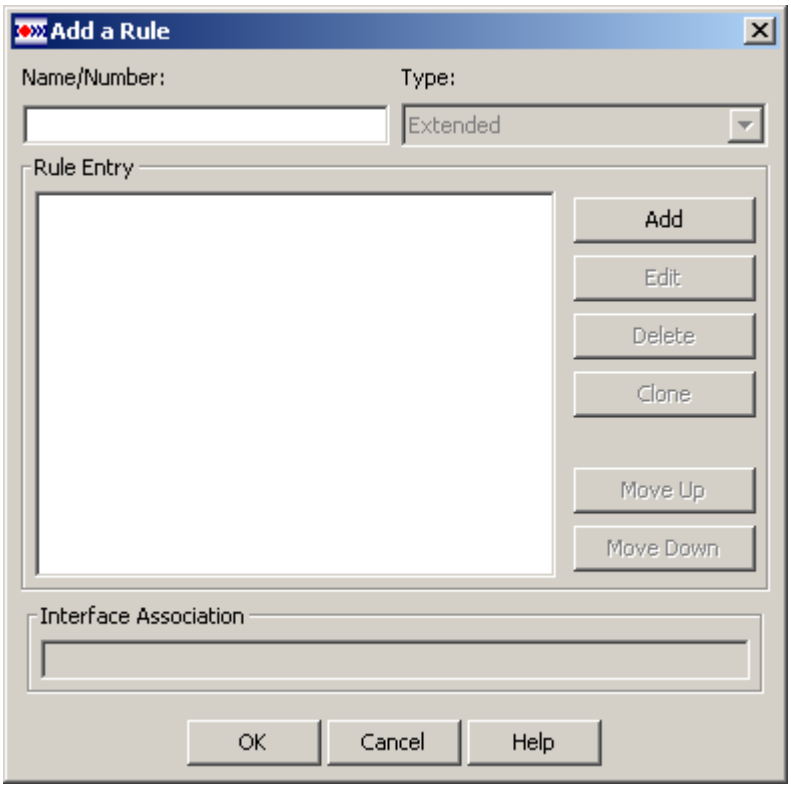

Рисунок 25

Создание записи в правиле IPsec

Кнопка Add в окне *Add a Rule* открывает окно *Add an Extended Rule Entry* (Рисунок 26), аналогичное окну в правиле доступа и описанное в разделе «Создание записи в расширенном правиле доступа». Если правило IPsec связано с криптокартой, то группа *Schedule* будет недоступна.

- 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.

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

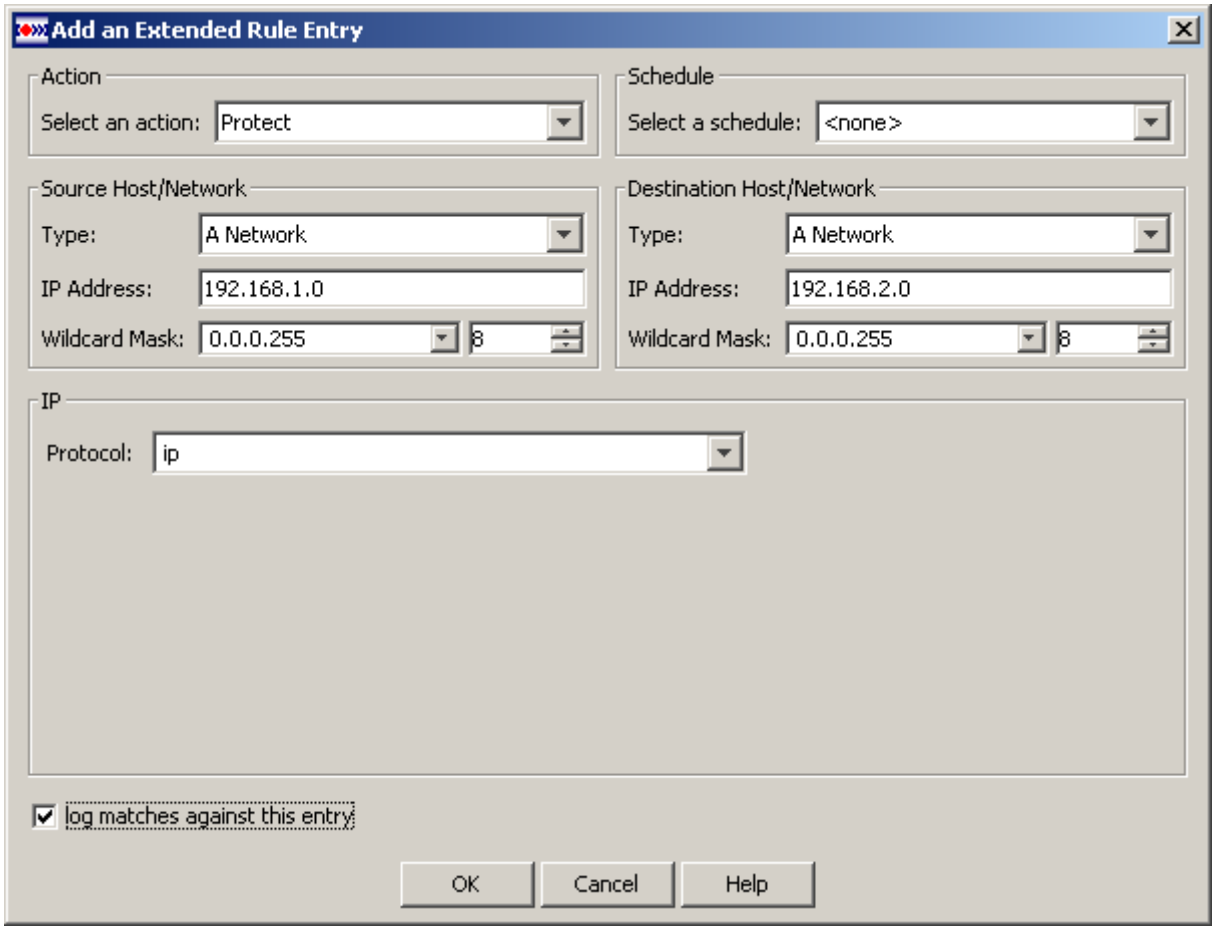

Рисунок 26

Редактирование записи в правиле IPsec

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

Клонирование записи в правиле IPsec

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

Удаление записи в правиле IPsec

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

Редактирование правила IPsec

Редактирование выделенного в разделе *IPSec Rules* правила IPsec, осуществляется в окне *Edit a Rule*, которое вызывается кнопкой Edit. Редактирование правила IPsec ничем не отличается от описанного выше редактирования правила в *Access Rules* (см. «Редактирование правила доступа»).

Удаление правила IPsec

Удаление выделенного в разделе *IPSec Rules* правила, производится с помощью кнопки Delete. Разрешается удаление только не связанных 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:

```
Cannot delete this rule since it is being used by crypto map {map
name}. To delete this rule, first remove its association with crypto
map {map name}
```

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

```
Cannot delete this rule since it is being used by {Interface name}.To
delete this rule, first remove its association with {Interface name}
```

Удаление несвязанного правила предваряется сообщением с требованием подтверждения удаления:

```
Are you sure you want to delete the selected rule (rule name/number)?
Click Yes to confirm, No to quit
```


Inspect Rules

В разделе *Inspect Rules* (Рисунок 27) можно создать, отредактировать и удалить правила проверки. Правила проверки определяют, какие протоколы прикладного уровня, а также TCP будут проверяться средствами CBAC (Context-Based Access Control – управление доступом на основе контекста). В этом случае шлюз безопасности выполняет функции межсетевого экрана, используя средства CBAC.

В подразделе *Port-Maps* можно перенаправить трафик стандартных протоколов, а также сервисов, заданных пользователем, на любой TCP-порт.

В подразделе *Timeouts & Thresholds* возможно задать глобальные параметры управления состоянием сеанса в системе CBAC.

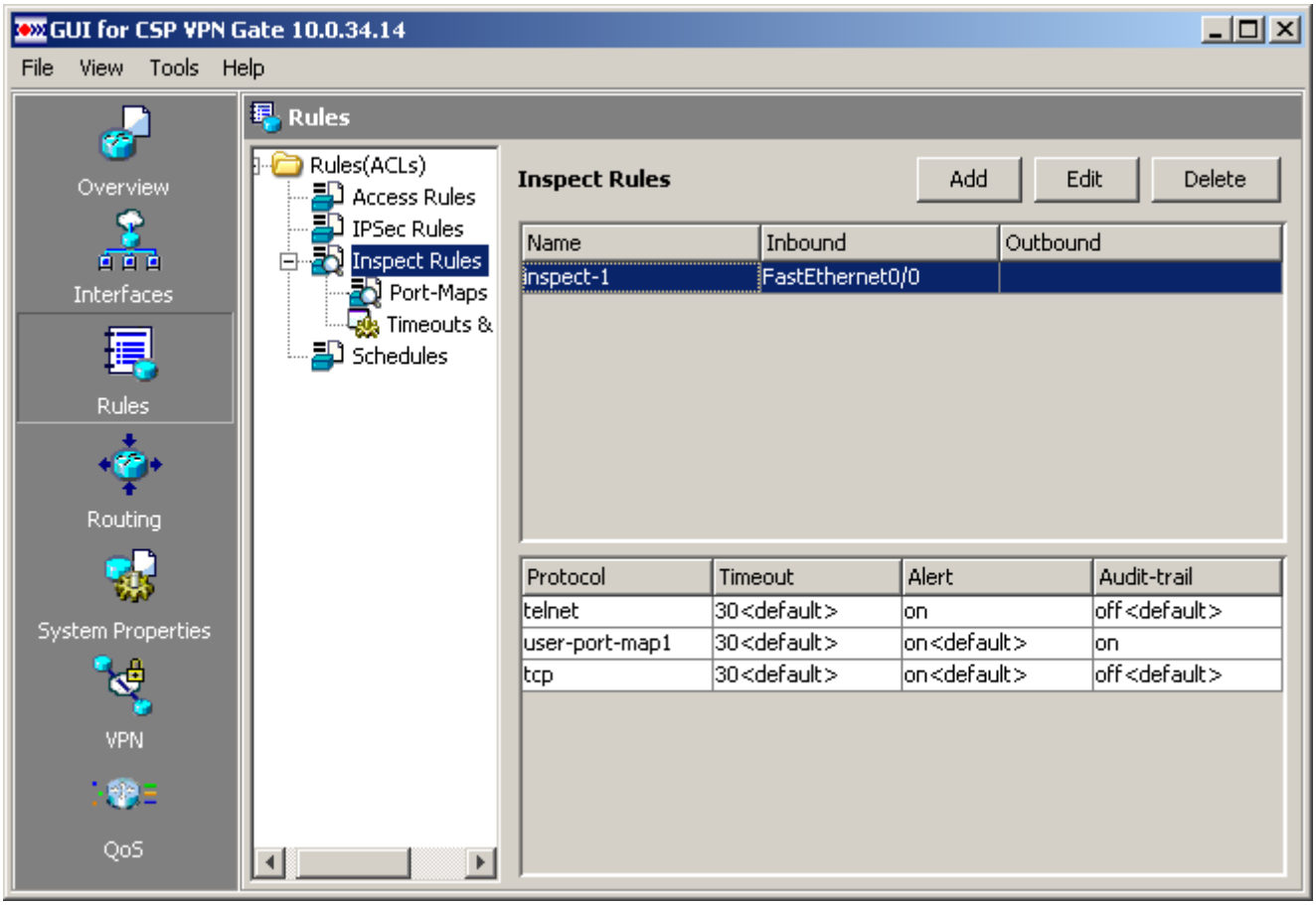

Рисунок 27

Главная форма раздела *Inspect Rules* содержит следующие элементы:

- Кнопки управления:
  - Add – кнопка вызова окна для создания нового Inspect Rule.
  - Edit – кнопка вызова окна для редактирования выделенного Inspect Rule.
  - Delete – кнопка удаления выделенного Inspect Rule.
- В верхней таблице размещаются правила проверки. Состав столбцов таблицы:
  - *Name* – имя правила проверки.
  - *Inbound* – имя интерфейса, на котором правило проверки применяется к входящему трафику.

- *Outbound* – имя интерфейса, на котором правило проверки применяется к исходящему трафику.

- В нижней таблице детализируется содержание выделенного Inspect Rule:
  - *Protocol* – имя притокола или имя пользовательского сервиса.
  - *Timeout* – время, в течение которого допускается существование неактивного сеанса tcp (дополняется словом <default>, если используется настройка по умолчанию).
  - *Alert* – задает выдачу тревожных сообщений. Значение *on* означает, что сообщения выдаются, *off* – сообщения не выдаются (дополняется словом <default>, если используется настройка по умолчанию).
  - *Audit-trail* – задает ведение журнала аудита. Значение *on* означает, что журнал ведется, *off* – журнал не ведется (дополняется словом <default>, если используется настройка по умолчанию).

Создание правила проверки

Создание нового правила проверки осуществляется в окне *Add Inspect Rule* (Рисунок 28), которое вызывается кнопкой Add в окне *Inspect Rules* (Рисунок 27).

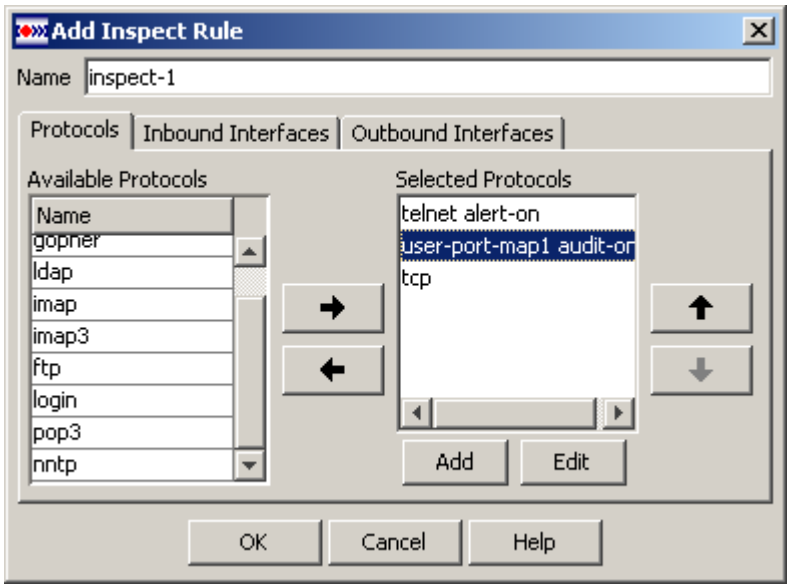

Рисунок 28

Окно *Add Inspect Rule* содержит:

- *Name* – поле ввода имени правила проверки. Имя должно быть уникальным, длиной не более 19 символов и должно начинаться с буквы. В имени используются только латинские буквы, цифры и символы: `!"#$%&'()*+,-./;:<=>@[\]^_`{|}~`, пробелы не допускаются.
- Три вкладки:
  - *Protocol*s.
  - *Inbound Interfaces.*
  - *Outbound Interfaces.*

Вкладка Protocols

Во вкладке *Protocols* (Рисунок 28) можно выбрать протокол для текущего правила проверки. Вкладка содержит два поля:

- *Available Protocols* – это список, содержащий TCP-протокол и протоколы (сервисы) прикладного уровня, системные или пользовательские. Вид записи в списках – это имя протокола и настройки (Alert, Audit, Timeout). Если используются настройки по умолчанию, то они не показываются. При перемещении протокола из списка *Available Protocols* в список *Selected Protocols*, он удаляется из списка *Available Protocols*.
- *Selected Protocols* – список выбранных протоколов с настройками, к которым будет применяться правило проверки. Если используются настройки по умолчанию, то они не показываются. Протокол TCP всегда находится внизу списка выбранных протоколов и не может быть перемещен. Протокол UDP не используется. Этот список не должен быть пустым.

Кнопки управления:

-  – кнопка перемещения выделенного протокола в списке *Available Protocols* в список *Selected Protocols.*
-  – кнопка перемещения протокола из списка *Selected Protocols* в список *Available Protocols.*
-  – кнопка перемещения выделенной строки в списке *Selected Protocols* на одну позицию вверх для увеличения приоритета. Если выделенной строкой является первая, то кнопка будет блокирована.
-  – кнопка перемещения выделенной строки в списке *Selected Protocols* на одну позицию вниз для снижения приоритета. Если выделенной строкой является последняя, то кнопка будет блокирована.
- Add – кнопка вызова диалога создания пользовательского сервиса *Add Port Map* (Рисунок 33). Это окно описано в разделе «Назначение портов сервису, определенному пользователем». При подтверждении создания в списке *Selected Protocols* появляется новая запись с настройками по умолчанию.
- Edit – кнопка вызова диалога изменения настроек сервиса – *Edit Protocol* (Рисунок 29).

Редактирование параметров сервиса

В окне *Edit Protocol* можно изменить следующие настройки сервиса:

- *Alert* – выдача тревожных сообщений (уровня alert). Переключатель с тремя положениями:
  - *on* – тревожные сообщения выдаются,
  - off – тревожные сообщения не выдаются,
  - *default* – настройка *Alert* берется из раздела глобальных настроек *Timeout & Thresholds.*
- *Audit* – ведение журнала аудита. Переключатель:
  - *on* – задает ведение журнала аудита,
  - *off* – журнал аудита не ведется,
  - *default* – настройка *Audit* берется из раздела *Timeout & Thresholds.*

- *Timeout* – время (в секундах), в течение которого допускается существование неактивного сеанса tcp. Можно ввести нужное значение в поле ввода или установить флажок *default*, тогда значение будет взято из настройки в разделе *Timeout & Thresholds*. Заданная величина должна быть в интервале от 1 до 2147483.

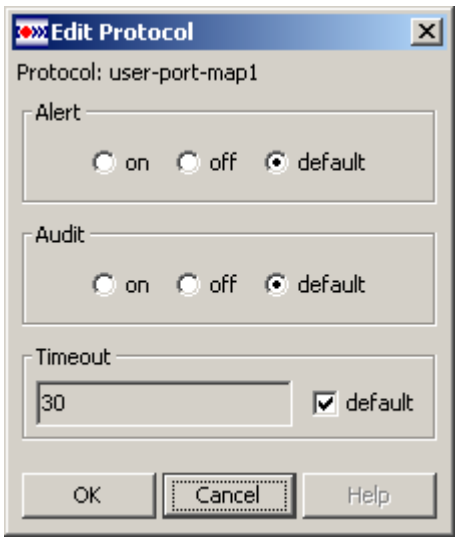

Рисунок 29

Вкладки Inbound Interfaces и Outbound Interfaces

Во вкладке *Inbound Interfaces* выбираются интерфейсы, на которых правило проверки будет применяться к входящему трафику. Во вкладке *Outbound Interfaces* выбираются интерфейсы, на которых правило проверки будет применяться к исходящему трафику.

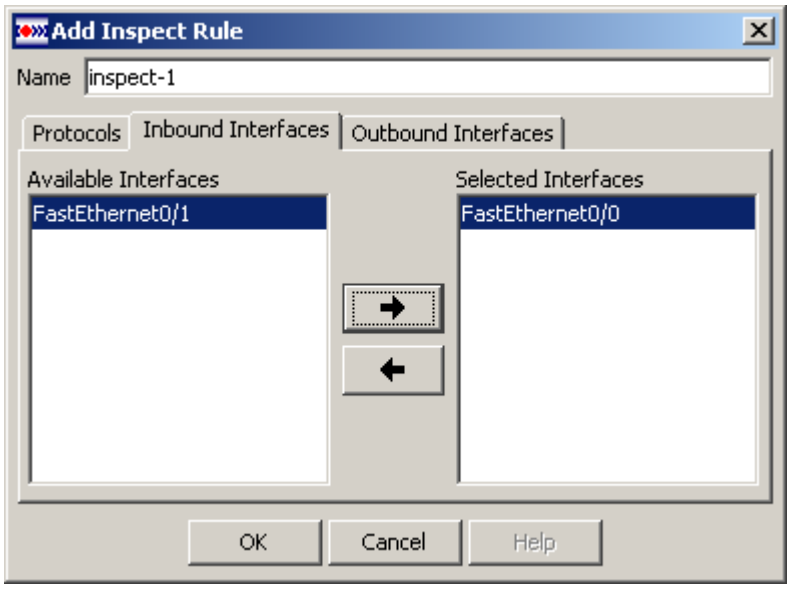

Рисунок 30

- *Available Interfaces* – поле со списком доступных интерфейсов. При перемещении интерфейса в список *Selected Interfaces* он удаляется из *Available Interfaces.*
- *Selected Interfaces* – список выбранных интерфейсов. Список не должен быть пустым. Можно выбрать один или несколько интерфейсов.

Редактирование правила проверки

Редактирование правила проверки осуществляется в окне *Edit Inspect Rule* (Рисунок 31), которое вызывается кнопкой Edit в окне *Inspect Rules*. Состав элементов окна аналогичен описанному выше окну создания нового правила проверки, за исключением поля *Name*, которое недоступно для редактирования..

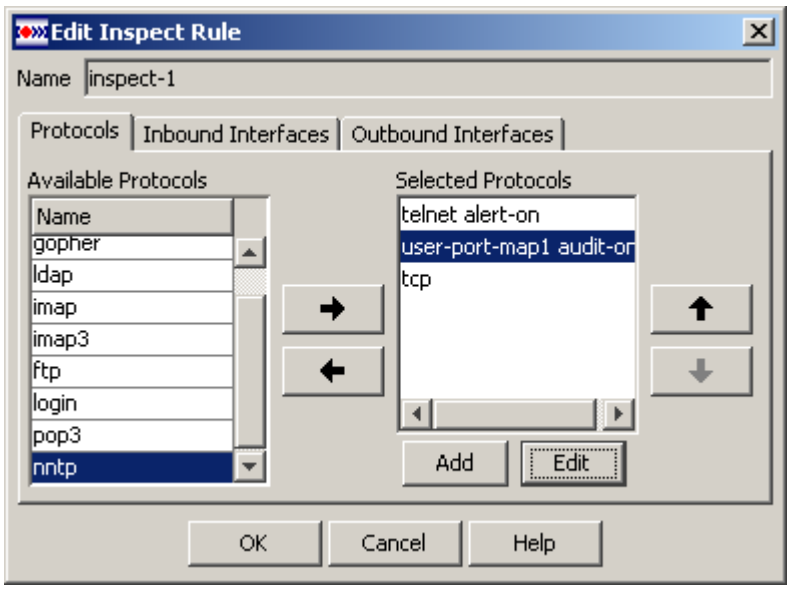

Рисунок 31

Удаление правила проверки

Удалить правило проверки можно в разделе *Inspect Rules* (Рисунок 27). Для этого надо выделить правило проверки в верхней таблице и нажать кнопку Delete.

Port-Maps

В разделе *Port-Maps* (Рисунок 32) выполняется ассоциации протоколов (сервисов) прикладного уровня с номерами TCP-портов. Можно перенаправить трафик стандартных сервисов, а также сервисов, заданных пользователем, на любой TCP-порт. Здесь же можно задать правило доступа для выбранного сервиса.

Изначально в разделе представлены системно-заданные соответствия – имя системного сервиса и стандартный номер порта.

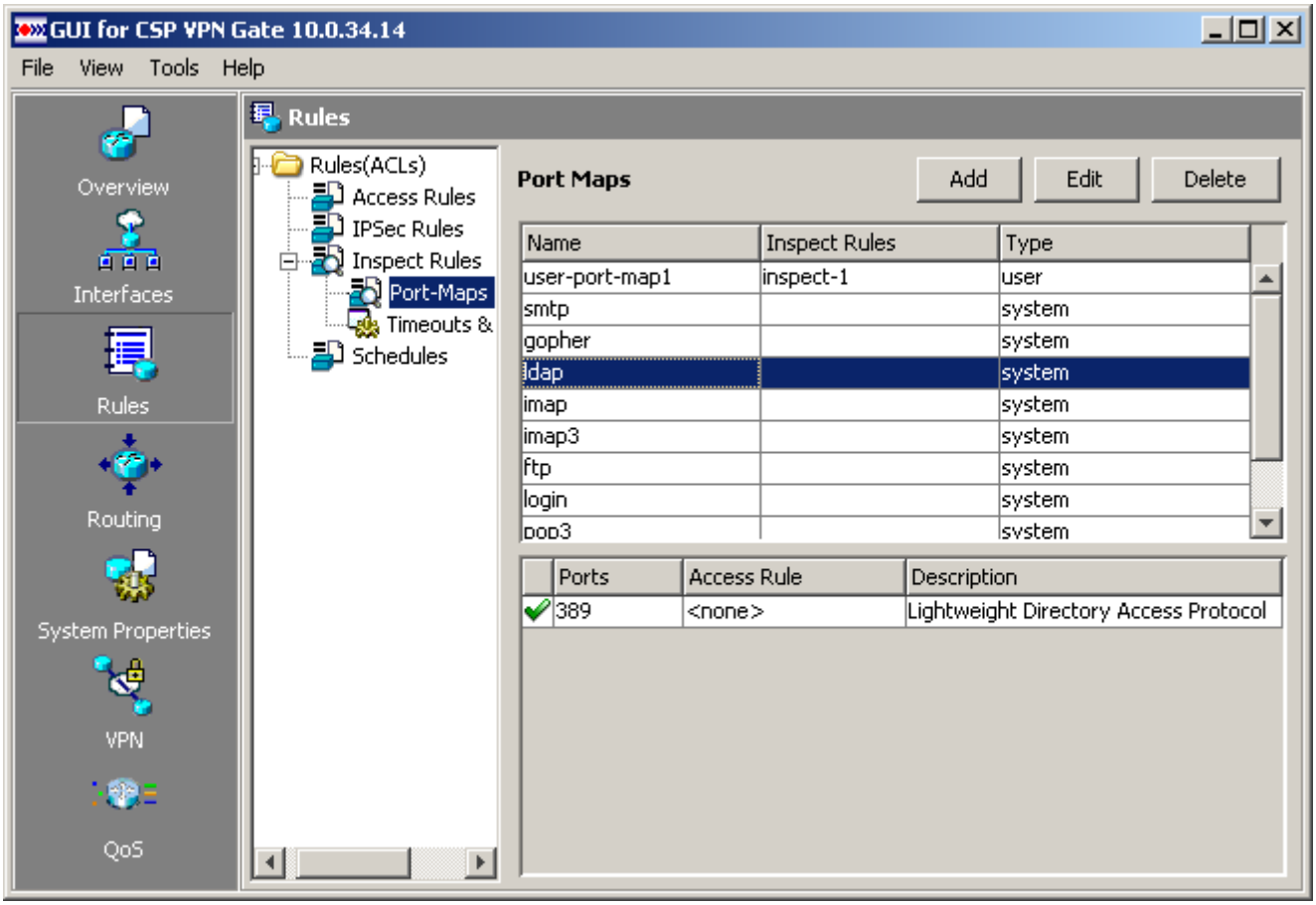

Рисунок 32

Состав элементов окна:

- В верхней таблице показываются сервисы и связанные с ними правила проверки. Состав столбцов таблицы:
  - *Name* – имя стандартного сервиса или сервиса, заданного пользователем.
  - *Inspect Rules* – правило проверки для данного сервиса.
  - *Type* – тип сервиса (пользовательский или системный).
- В нижней таблице описывается выделенный сервис:
  - В первой колонке (без названия) показывается иконка: «галочка» или «крестик» (включено/отключено):
    - Иконка «галочка» для стандартных протоколов (ldap, gofer и т.д.) показывает, что включено системно-заданное соответствие (имя протокола и стандартный номер порта).

Для пользовательских сервисов «галочка» выставляется во всех случаях, за исключением, когда к сервису привязано drop-all правило.

- Иконка «крестик» для стандартных протоколов показывает, что отключено системно-заданное соответствие.
  Для пользовательских сервисов «крестик» выставляется, когда к сервису привязано drop-all правило.

- *Ports* – список портов или диапазон портов, ассоциируемых с выбранным сервисом.
- *Access Rule* – показывает правило доступа, ограничивающее данный сервис.
- *Description* – описание сервиса.

- Три кнопки управления:
  - Add – кнопка вызова окна для создания новой ассоциации сервиса, определенного пользователем с номером порта (Рисунок 33).
  - Edit – кнопка вызова окна для редактирования существующей ассоциации сервиса (системного или пользовательского) и порта.
  - Delete – кнопка удаления выделенной ассоциации сервиса и порта.

Назначение портов сервису, определенному пользователем

Ассоциация сервиса, определенного пользователем, с номерами TCP-портов осуществляется в окне *Add Port-Map* (Рисунок 33), которое вызывается кнопкой Add в разделе Port-Maps. В окне *Add Port-Map* можно добавить новую запись, назначающую порты заданному сервису, а также указать правило доступа для заданного сервиса на заданном порту. Можно отредактировать или удалить уже существующую запись.

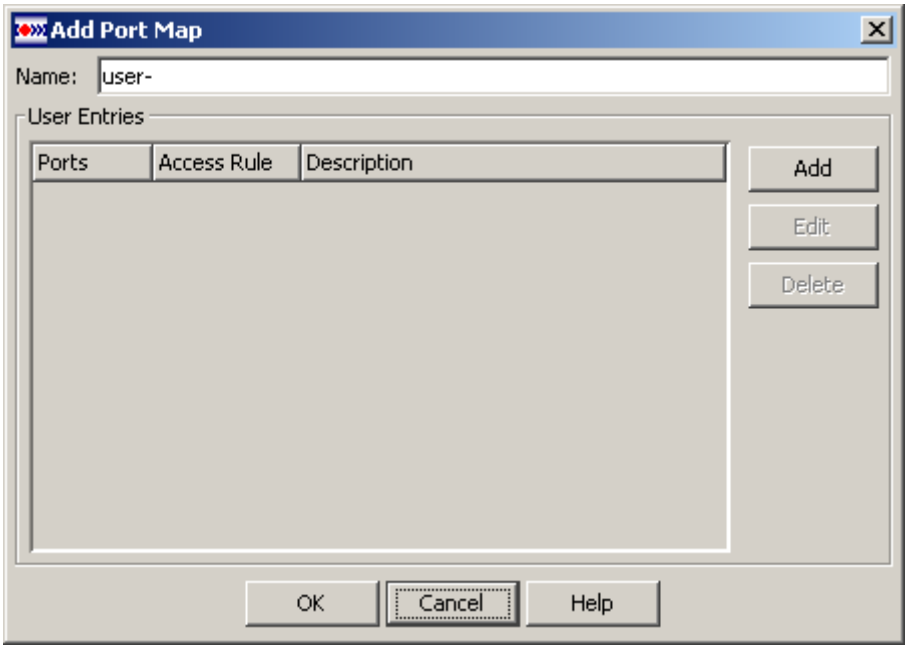

Рисунок 33

Описание элементов окна:

- *Name* – поле ввода имени сервиса пользователя. Имя должно быть уникальным и содержать не более 19 символов. Имя должно начинаться с префикса “user-“.
- Таблица *User Entries*. Состав столбцов таблицы:
  - *Ports* – список портов или диапазонов.
  - *Access Rule* – правило доступа, ограничивающее сервис на назначенном порту.
  - *Description* – описание.
- Кнопки управления:
  - Add – кнопка вызова окна для добавления записи к заданному сервису (Рисунок 34).
  - Edit – кнопка вызова окна, для редактирования записи сервиса.
  - Delete – кнопка удаления выделенного записи.

В окно *Add Port-Map* должна быть добавлена хотя бы одна запись.

Добавление записи

Окно *Add Port-Map Entry* вызывается нажатием кнопки Add в окне *Add Port-Map* (Рисунок 34).

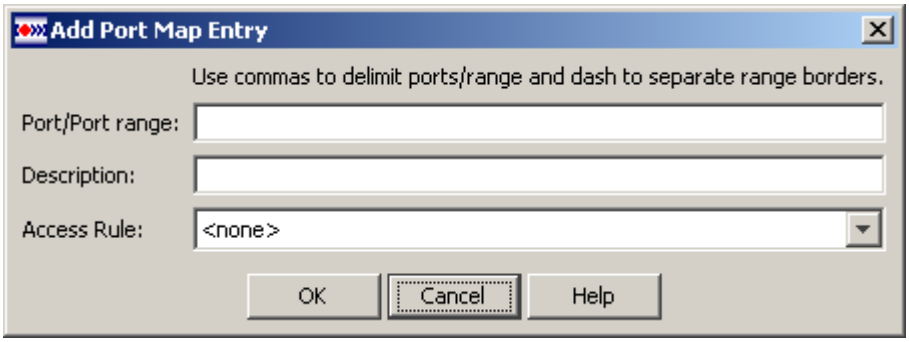

Рисунок 34

- *Port/Port range* – поле ввода портов или диапазона портов. Можно задать не более 5 портов или 1 диапазон. Порты разделяются запятыми, а границы диапазона указываются через тире. Недопустима пустая строка портов. Недопустимо никакое пересечение портов, диапазонов портов: ни внутри одного и того же сервиса, ни с записями другого сервиса, если они ссылаются на одно и тоже правило.
  - Если добавляемая запись пересекается с записями другого сервиса, то выдается сообщение: `Unable to add port-map entry. It conflicts with the entry for <PortMap Name>`
  - Если добавляемая запись пересекается с записью внутри редактируемого сервиса – будет предложено заменить старую запись новой:
    `Unable to add port-map entry. It conflicts with the entry <Список портов> <Описание>`
    `Would you like to replace conflict entry witn new one?`
- *Description* – поле ввода описания сервиса.
- *Access Rule* – поле выбора правила доступа. Правило должно быть стандартным и нумерованым. Возможные значения:
  - *<none>* – правило не выбрано.

- *Use Rule Pane for selection* – при выборе этого значения будет открыто окно *Rule Pane* (Рисунок 10) для выбора правила. Поле *Rule Category* окна *Rule Pane* будет блокировано.
- *Create new* – открывает диалог создания правила доступа *Add a Rule* (Рисунок 16). В этом окне поля *Type* и *Associate with an Interface* будут блокированы. Создаваемое правило доступа должно быть стандартным и нумерованным.

Редактирование назначений портов для пользовательских сервисов

Редактирование назначений портов для пользовательских сервисов осуществляется в окне *Edit Port-Map*, которое вызывается кнопкой Edit в разделе *Port-Maps* при выборе пользовательского сервиса. Состав элементов окна аналогичен описанному выше окну *Add Port-Map* (Рисунок 33), за исключением – поле *Name* недоступно для редактирования.

Редактирование назначений портов для системных сервисов

Окно *Edit Port-Map* (Рисунок 35) вызывается при выборе в разделе *Port-Maps* системного сервиса и нажатии кнопки Edit. В окне *Edit Port-Map* можно перенаправить трафик системного сервиса на другой порт, отличный от стандартного, добавить новый порт к общеизвестному порту, а также назначить правило доступа для данного сервиса на назначенном порту.

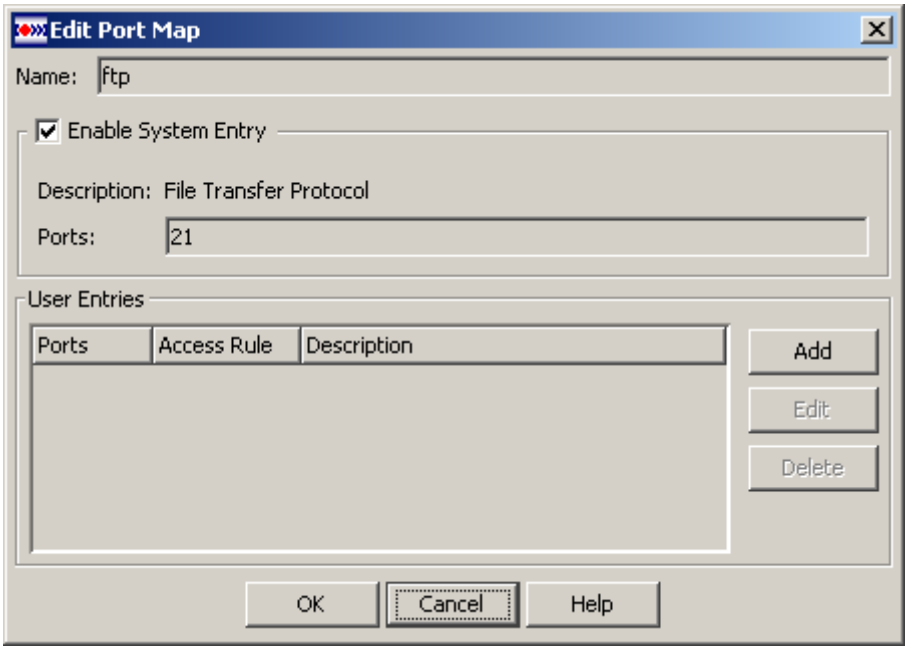

Рисунок 35

Описание элементов окна:

- *Name* –имя сервиса. Поле заблокировано.
- Группа *Enable System Entry*, в которой можно включить/отключить системно-заданное соответствие:

- *Enable System Entry* – выставленный флаг включает системно-заданное соответствие, сброшенный – отключает.
- *Description* – описание. Поле заблокировано.
- *Ports* – номер порта. Поле заблокировано.

- Таблица *User Entries*. Состав столбцов таблицы:
  - *Ports* – список портов или диапазонов.
  - *Access Rule* – показывает правило доступа, ограничивающее сервис на назначенном порту.
  - *Description* – описание.
- Кнопки управления:
  - Add – кнопка вызова окна для добавления записи с назначениями портов к сервису (Рисунок 34).
  - Edit – кнопка вызова окна для редактирования записи сервиса.
  - Delete – кнопка удаления выделенной записи.

Если запись, созданная пользователем, пересекается с системной, то выдается сообщение:

```
User-defined port-map entry port(s) <Перечисление портов> conflicts
with system entry. Would you like to disable system entry?
```

При положительном ответе системная запись отключается.

Удаление ассоциации сервиса с номером порта

Удаление ассоциации сервиса с номером порта выполняется в разделе *Port Maps*. Выделенная запись удаляется при нажатии кнопки Delete.

Если удаляемый сервис был связан с правилом проверки, и эта запись в правиле проверки является последней, и удаление этой port-map влечёт за собой удаление правила проверки с последующим разрывом inbound/outbound связей, или сервис содержит последнюю ссылку на правило доступа, задаваемое непосредственно в объявлении port-map с консоли, то в запрошенном подтверждении на удаление будет выведена соответствующая информация:

The removing of the selected port-map result in consequential deleting of

Inspect Rules: <Список>

Access Rules: <Список>

and breaking of inbound/outbound inspect interface(s) linkage: <Список>

Would you like to confirm deleting?

При согласии будут удалены соотвующие правила, правила проверки и разорваны связи с интерфейсами. В остальных случаях будет запрошено стандартное подтверждение удаления.

При удалении системного сервиса будет выдано предупреждение (Рисунок 36).

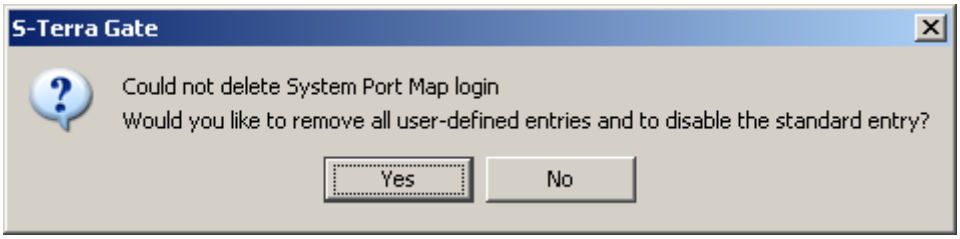

Рисунок 36

Timeouts & Thresholds

В разделе *Timeoust & Thresholds* (Рисунок 37) изначально представлены глобальные параметры управления состоянием сеанса в системе CBAC (управление доступом на основе контекста), заданные по умолчанию.

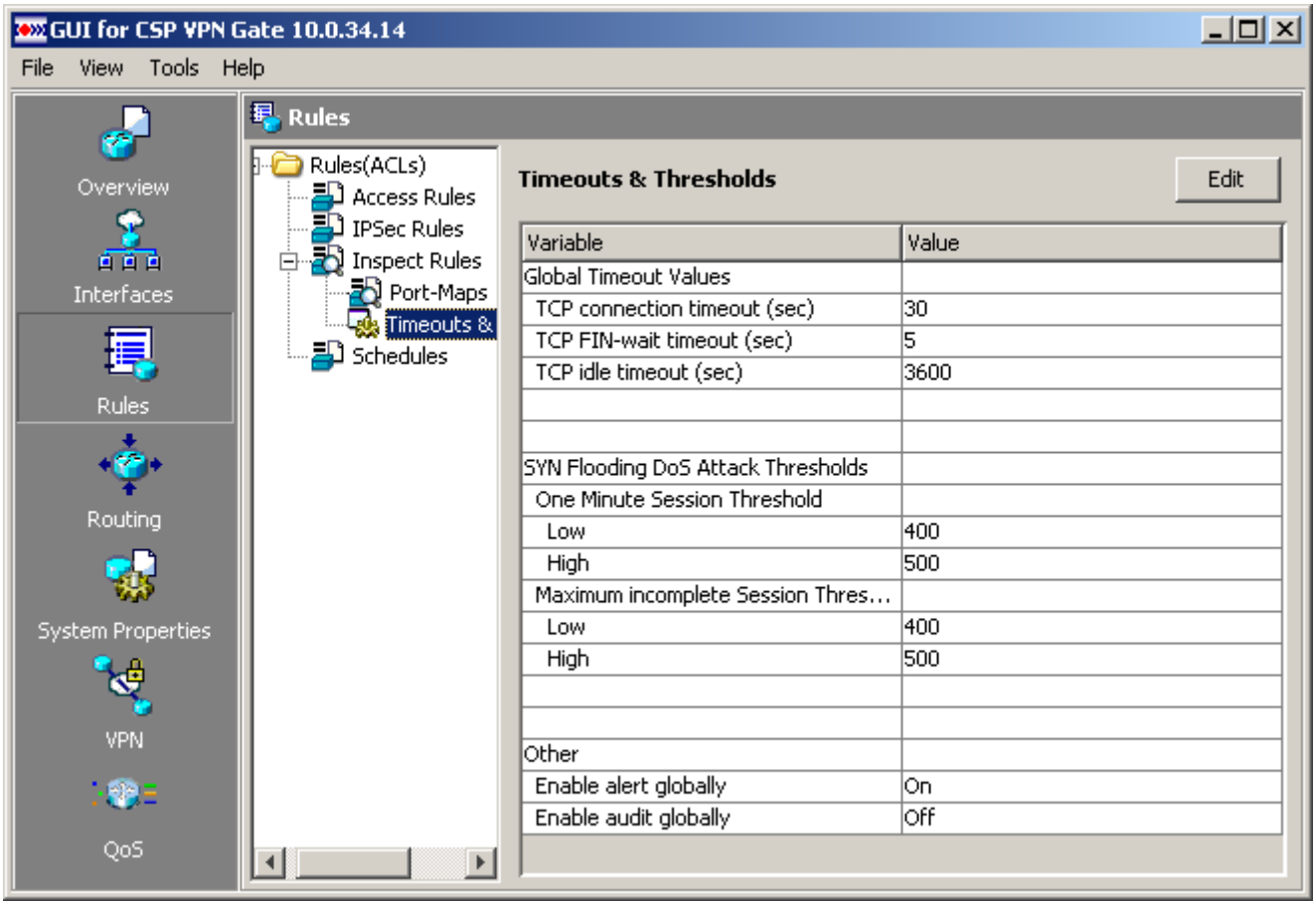

Рисунок 37

Состав элементов браузера раздела *Timeouts & Thresholds*:

- Кнопки управления:
  - Edit – кнопка вызова окна редактирования установленных параметров.
- Таблица *Timeouts & Thresholds* состоит из столбцов *Variable* и *Value.*

  Variable содержит следующие параметры:
  - *TCP connection timeout (sec)* – указывает интервал времени, по истечение которого программное обеспечение закроет сеанс TCP, если он не успеет завершить процесс установки и перейти в установленное состояние.
  - *TCP FIN-wait timeout (sec)* – указывает интервал времени, в течение которого допускается существование сеанса TCP после того как S-Terra Gate зарегистрирует получение пакета с флагом FIN.
  - *TCP idle timeout (sec)* – указывает максимальный интервал времени, в течение которого допускается существование неактивного сеанса TCP.
  - *One Minute Session Threshold*:

- *Low* – частота появления полуоткрытых сеансов, по достижении которой S-Terra Gate прекращает их удаление.
- *High* – частота появления полуоткрытых сеансов, по достижении которой S-Terra Gate начинает их удаление.

- *Maximum incomplete Session Threshold*:
  - *Low* – задает количество одновременно существующих полуоткрытых сеансов, при достижении которого S-Terra Gate прекращает их удаление.
  - *High* – задает количество одновременно существующих полуоткрытых сеансов, при достижении которого S-Terra Gate начинает их удалять.
- *Enable alert globally* – задает выдачу тревожных сообщений (уровня alert).
- *Enable audit globally* – задает ведение журнала аудита. В журнале ведутся записи о времени сессии, адресах хостов источника и получателя, номерах портов, продолжительности существования соединения и количестве переданных байтов.

Value содержит значения указанных параметров либо *ON/Off* – включение или выключение настроек.

Редактирование параметров

Редактирование глобальных параметров производится в окне *Global Timeout and Threshold settings* (Рисунок 38), которое вызывается кнопкой Edit.

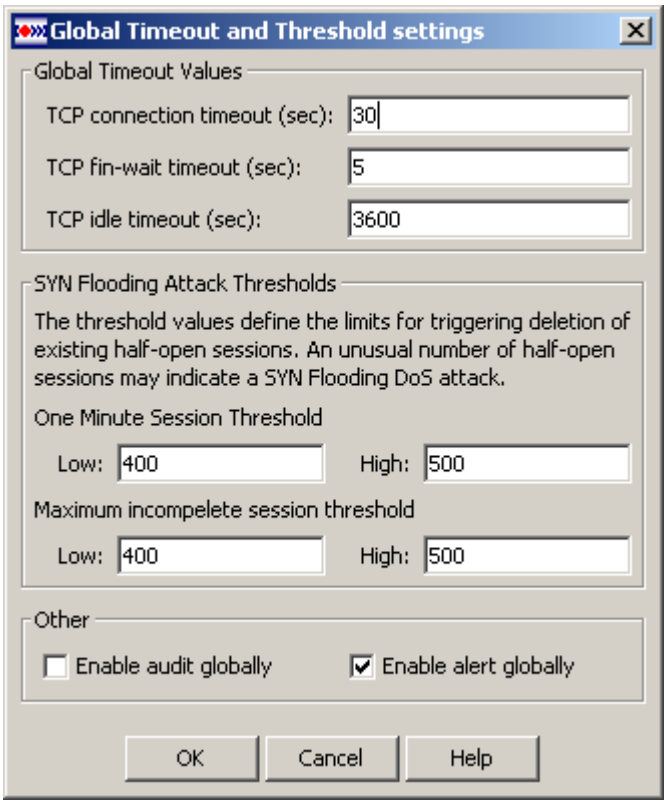

Рисунок 38

Состав элементов окна:

- Группа *Global Timeout Values* – позволяет указать временные параметры TCP сеанса:
  - *TCP connection timeout (sec)* – значение от 1 до 2147483, по умолчанию 30 секунд.
  - *TCP fin-wait timeout (sec)* – значение от 1 до 2147483, по умолчанию 5 секунд.
  - *TCP idle timeout (sec)* – значение от 1 до 2147483, по умолчанию 3600 секунд.
- Группа *SYN Flooding Attack Thresholds* – позволяет задать минимальное и максимальное значение частоты появления полуоткрытых сеансов и количества существующих полуоткрытых сеансов, при достижении которых прекращается или запускается процесс по их удалению. Необычно большое число полуоткрытых сеансов может указывать на SYN Flooding DoS attack (одна из атак блокирования сервиса).
  - *One Minute Session Threshold* (частота появления полуоткрытых сеансов):
    - *Low* – значение от 1 до 2147483647, по умолчанию 400 полуоткрытых сеансов в минуту.
    - *High* – значение от 1 до 2147483647, по умолчанию 500 полуоткрытых сеансов в минуту.

  Значение *Low* не должно превышать значение *High*. Сообщение об ошибке: Invalid One minute session threshold. Low value exceeds High.
  - *Maximum incomplete session threshold* (число одновременно существующих полуоткрытых сеансов):
    - *Low* – значение от 1 до 2147483647, по умолчанию 400.
    - *High* – значение от 1 до 2147483647, по умолчанию 500.

  Значение *Low* не должно превышать значение *High*. Сообщение об ошибке: Invalid Maximum incomplete session threshold range. Low value exceeds High
- Группа *Other* – позволяет задать ведение журнала аудита и выдачу тревожных сообщений:
  - *Enable audit globally* – установка флага задает ведение журнала аудита. По умолчанию журнал аудита не ведется.
  - *Enable alert globally* – установка флага задает выдачу тревожных сообщений (уровня alert). По умолчанию сообщения выдаются.

Schedules

В разделе *Schedules* (Рисунок 39) можно создать новое, отредактировать или удалить существующее расписание, которое привязывается к расширенному правилу доступа. Связь расписания с правилом доступа устанавливается в разделе *Access Rules*, при создании или редактировании расширенного правила доступа (Рисунок 18). Расписание содержит интервалы времени активности правил доступа. Диапазон времени, в течение которого будет действовать правило доступа, может быть абсолютным и периодическим. В расписании может присутствовать только один абсолютный интервал.

Не допускается использование расписания в правилах, используемых при построении IPsec соединений.

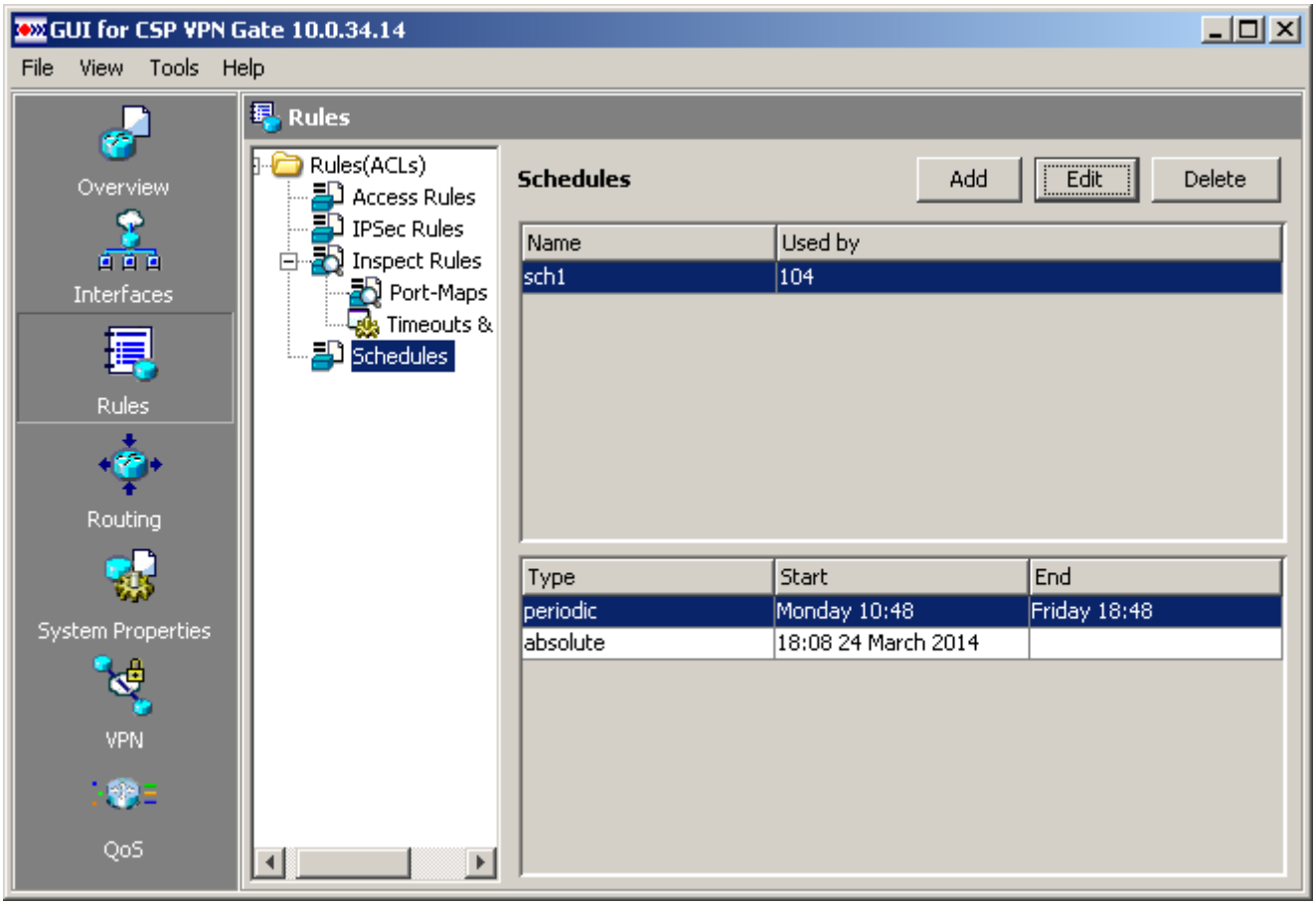

Рисунок 39

Главная форма раздела *Schedules* содержит следующие элементы:

- В верхней таблице показывается имя расписания и связанное с ним правило доступа, работающее по этому расписанию. Состав столбцов таблицы:
  - *Name* – имя расписания.
  - *Used by* – имя правила доступа, связанное с этим расписанием.
- В нижней таблице показываются параметры интервалов времени, заданных в расписании. Состав столбцов таблицы:
  - *Type* – тип интервала, может быть периодический или абсолютный.
  - *Start* – начало интервала времени.
  - *End* – окончание интервала времени.

- Кнопки управления:
  - Add – кнопка вызова окна для создания нового расписания.
  - Edit – кнопка вызова окна для редактирования выделенного расписания.
  - Delete – кнопка удаления выделенного расписания.

Создание расписания

Создание расписания производится в окне *Add a schedule* (Рисунок 40), которое вызывается кнопкой Add в разделе *Schedules*.

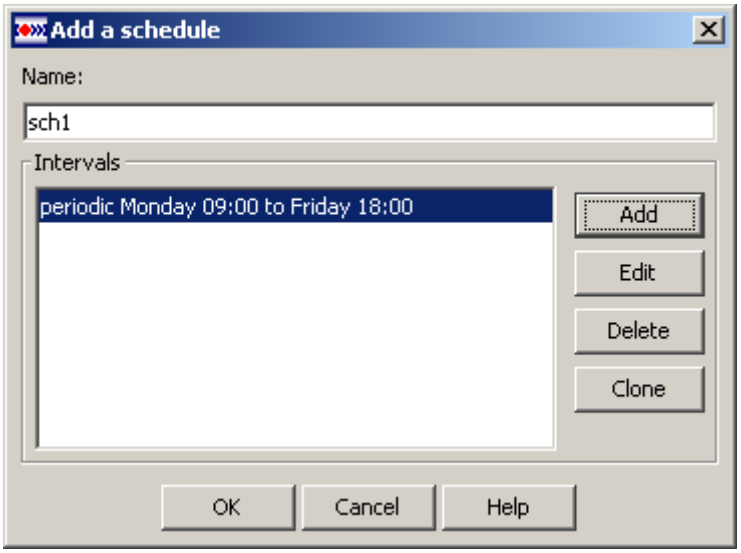

Рисунок 40

Окно содержит элементы:

- *Name* – имя расписания.
- *Intervals* – группа, содержащая список интервалов в расписании.
- Кнопки управления:
  - Add – кнопка вызова окна для создания новой записи в расписании.
  - Edit – кнопка вызова окна для редактирования выделенной записи.
  - Delete – кнопка удаления выделенной записи.
  - Clone – кнопка вызова окна для создания новой записи на базе существующей выделенной записи.

Добавление нового интервала в расписание

Окно *Add an interval* вызывается кнопкой Add в окне *Add a schedule*. Вид окна зависит от типа интервала, выбранного с помощью переключателей *Absolute interval* (Рисунок 41) или *Periodic interval* (Рисунок 42). Если в расписании уже есть абсолютный интервал, то переключатель *Absolute interval* неактивен. По умолчанию установлен периодический интервал.

Абсолютный интервал

Окно содержит две группы *Interval start* и *Interval end*, которые становятся активными при установке соответствующего флажка. По умолчанию флажки сброшены, а элементы группы отображают текущую дату и время.

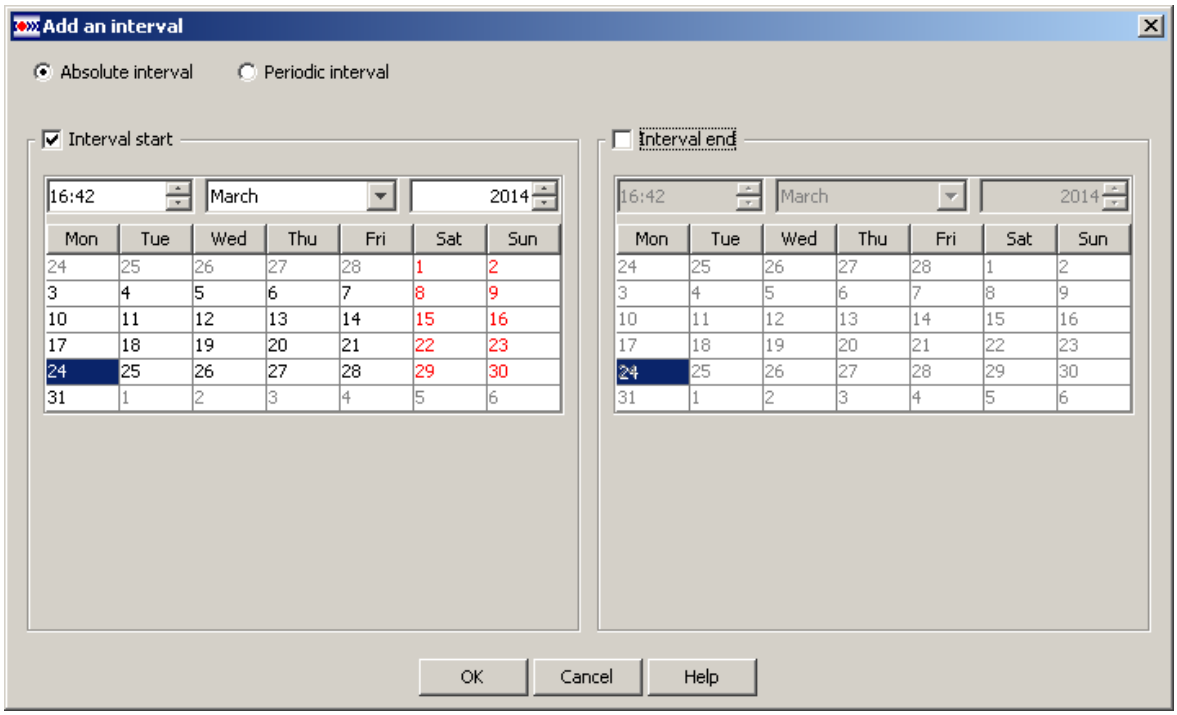

Рисунок 41

Периодический интервал

Окно содержит две группы элементов *from* и *to*, в которых задается начало и окончание периода времени:

- Поле ввода со спиннером для ввода времени. Значение по-умолчанию – текущее время.
- Набор флажков для задания дней недели начала и окончание периода. По умолчанию ни один флажок не установлен. Для предотвращения некорректных сочетаний, по мере выставления флажков некоторая часть флажков становится неактивными по следующим правилам:
  - При выборе дня недели в любой группе отключаются флажки *daily*, *weekdays* и *weeked*.
  - При выборе одного из флажков: *daily*, *weekdays* или *weeked* отключаются все остальные флажки.
  - При выборе в группе *from* более одного дня, в группе *to* отключаются все флажки. Даже если флажок был установлен ранее, то он будет проигнорирован.
  - При выборе дня недели в группе *to*, все остальные флажки в этой группе отключаются.

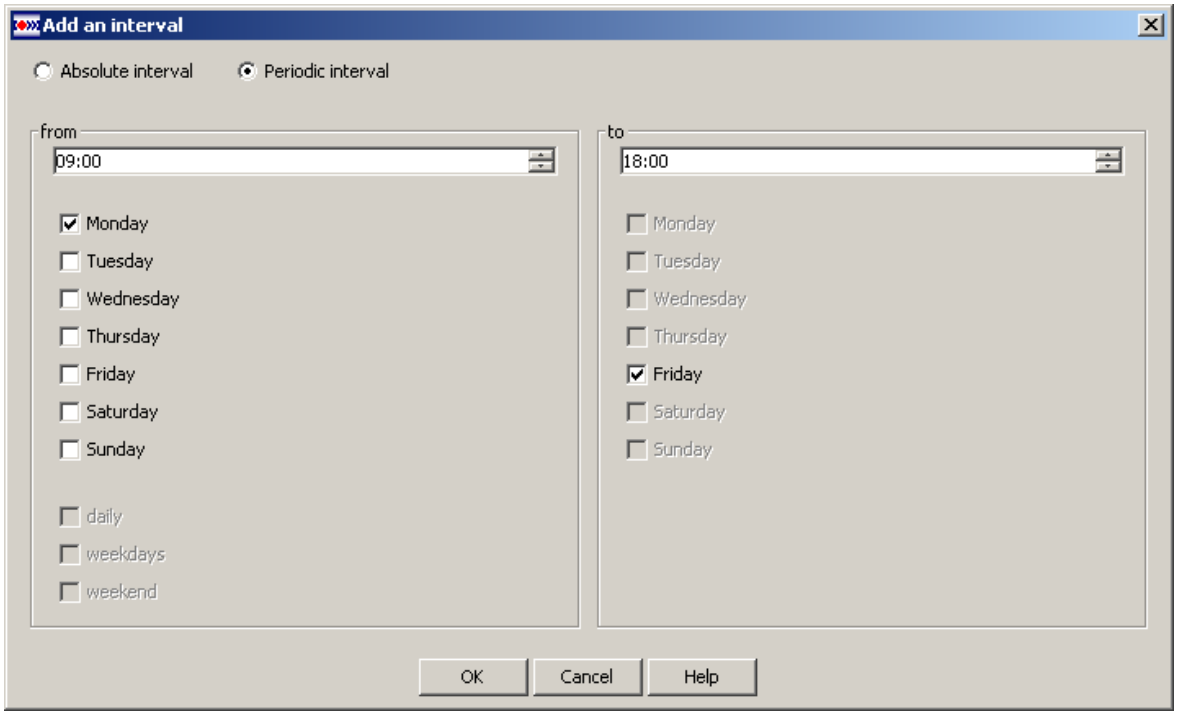

Рисунок 42

Редактирование расписания

Редактирование расписания производится в окне *Edit a schedule*, которое вызывается кнопкой Edit в разделе *Schedules*. Окно аналогично окну *Add a schedule* (Рисунок 40), описанному выше.

Routing

Главная форма раздела *Routing* (Рисунок 43) 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 IKECFG пула мобильным пользователям в таблицу роутинга необходимо внести запись.

Если из IKECFG 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.

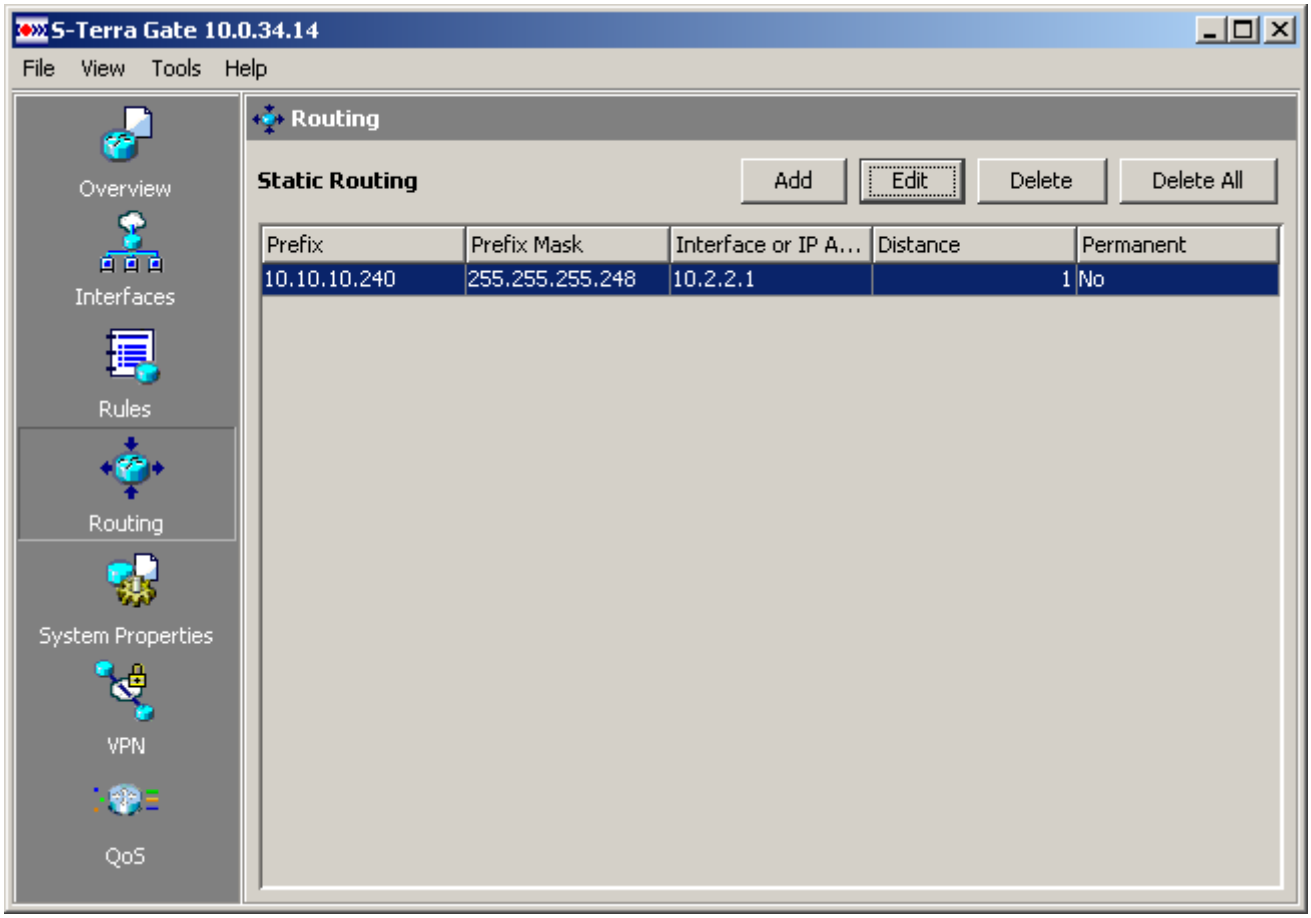

Рисунок 43

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.
  - I*nterface 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.
  - *Permanent* – обозначение постоянного маршрута. Параметр реально не используется и присутствует для совместимости с продуктами управления Cisco.

Создание маршрута

Создание маршрута производится в окне *Add Static Route* (Рисунок 44), которое вызывается кнопкой Add в разделе *Routing*.

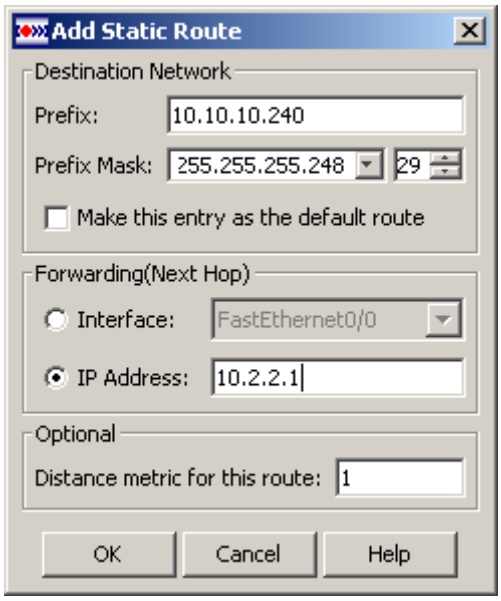

Рисунок 44

Это окно содержит следующие элементы:

- Группа *Destination Network* (Сеть получателя пакета):
  - *Prefix* – IP-адрес сети получателя пакета. При открытии окна это поле не заполнено. 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 *OK* 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 S-Terra Gate настройки маршрута по умолчанию отсутствуют). Для этого необходимо 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.

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 45) состоит из четырех подразделов:

- *Device* – этот раздел показывает имя хоста и доменное имя хоста, на котором установлен S-Terra 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 S-Terra 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.

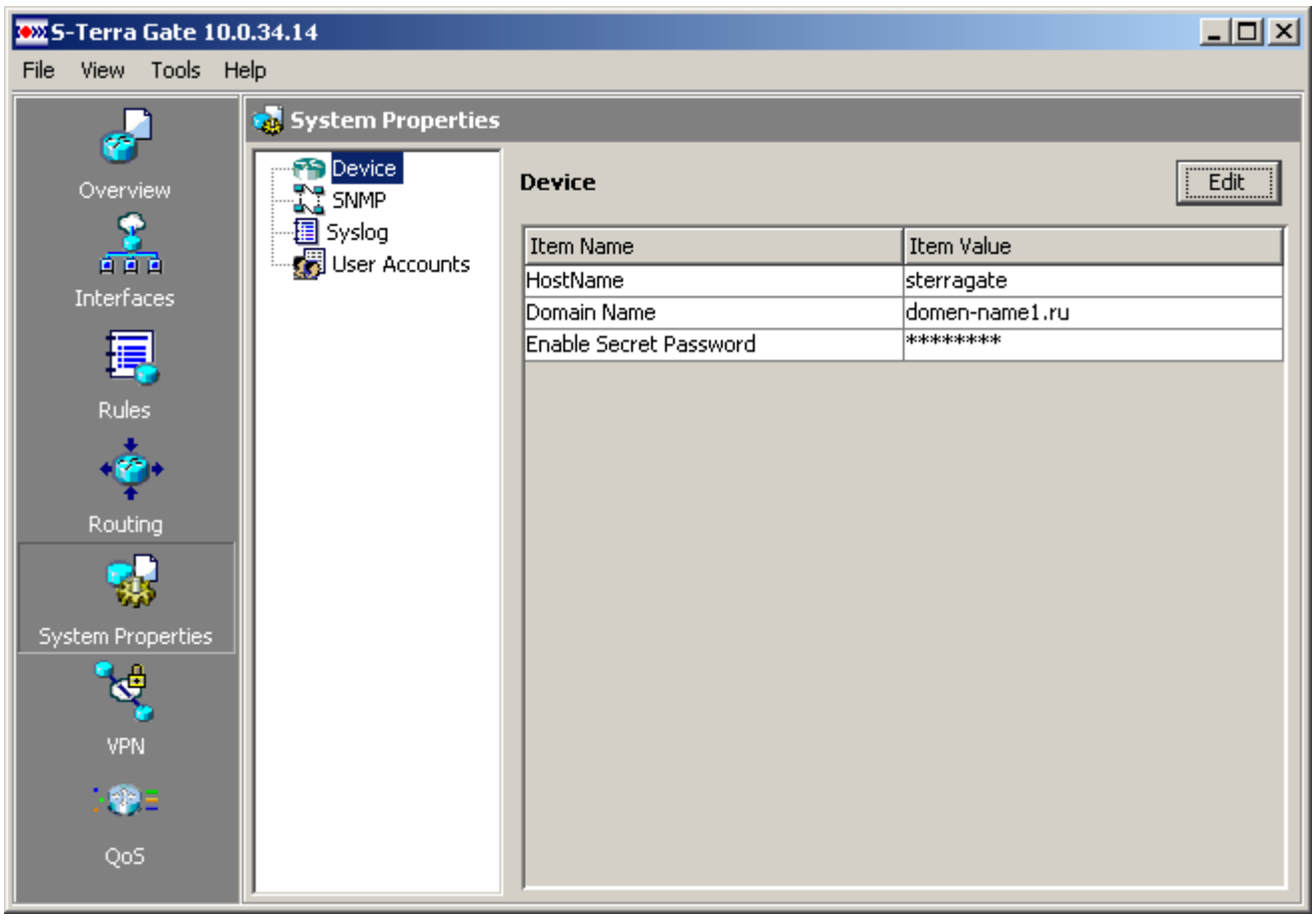

Рисунок 45

Device

Подраздел *Device* содержит таблицу свойств хоста, на котором установлен S-Terra Gate (Рисунок 45):

- *Item Name* содержит параметры:
  - *Host Name* – имя хоста, на котором установлен S-Terra Gate, и который мы настраиваем.
  - *Domain Name* – доменное имя для хоста, на котором установлен настраиваемый S-Terra 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 46) 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).

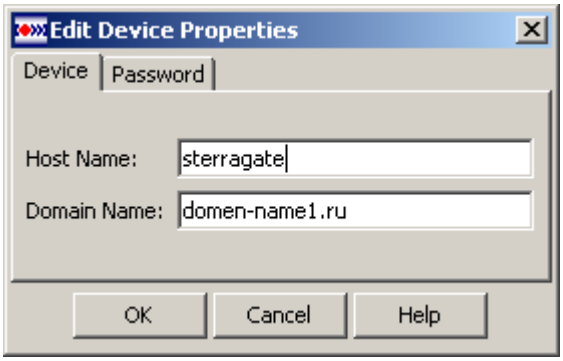

Рисунок 46

- Вкладка *Password* (Рисунок 47):
  - *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 47

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 48). Главная форма этого раздела содержит два подраздела – *SNMP Polling* и *SNMP Traps*.

В подразделе *SNMP Polling* задаются настройки SNMP-агента для выдачи статистики по запросу SNMP-менеджера.

В подразделе *Traps Receivers* задается список получателей SNMP трапов, в которых SNMP-агент сообщает менеджеру о произошедших событиях.

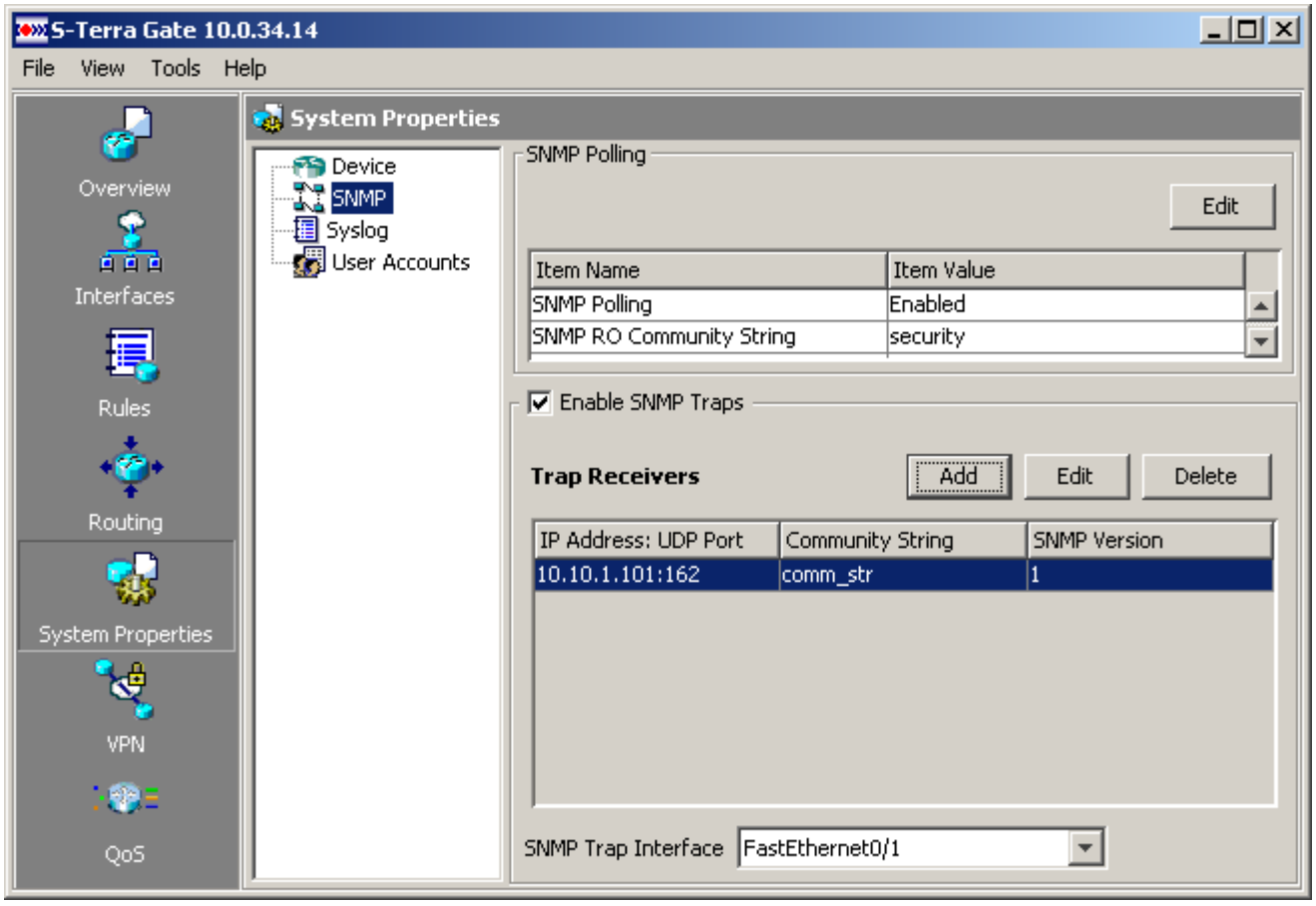

Рисунок 48

Таблица подраздела *SNMP Polling* 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.

Кнопка Edit – вызывает окно редактирования параметров SNMP.

Таблица подраздела *Traps Receivers* содержит список получателей SNMP-трапов и их настройки:

- *Enable SNMP Traps* – установка этого флажка включает данный подраздел и позволяет вводить получателей SNMP трапов.

- *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.
- *SNMP Trap Interface* – выпадающий список интерфейсов шлюза безопасности, на который будут передаваться трап-сообщения для отсылки получателям. Параметр необязательный.

Кнопки управления:

- Add – вызывает окно для ввода настроек получателя SNMP-трапов.
- Edit – вызывает окно редактирования настроек выделенного в таблице получателя.
- Delete – удаление выделенной строки.

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

Редактирование параметров SNMP Polling

Окно редактирования *Edit SNMP Polling* (Рисунок 49) параметров SNMP вызывается нажатием кнопки Edit в подразделе *SNMP Polling*.

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.

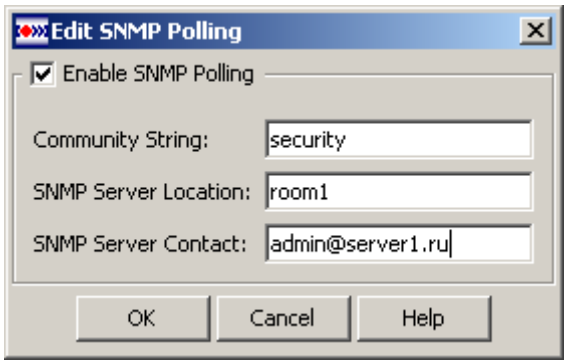

Рисунок 49

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.

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.

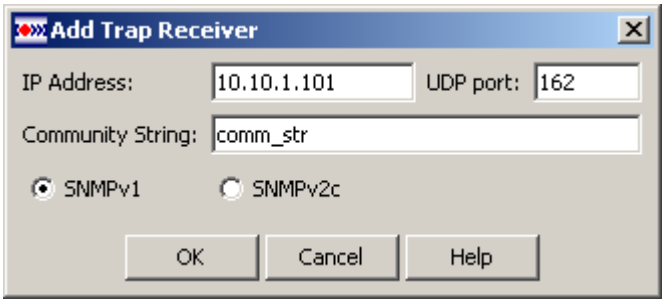

Рисунок 50

Syslog

Главная форма подраздела *Syslog* (Рисунок 51) 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.

Кнопка Edit – вызывает окно редактирования настроек логирования.

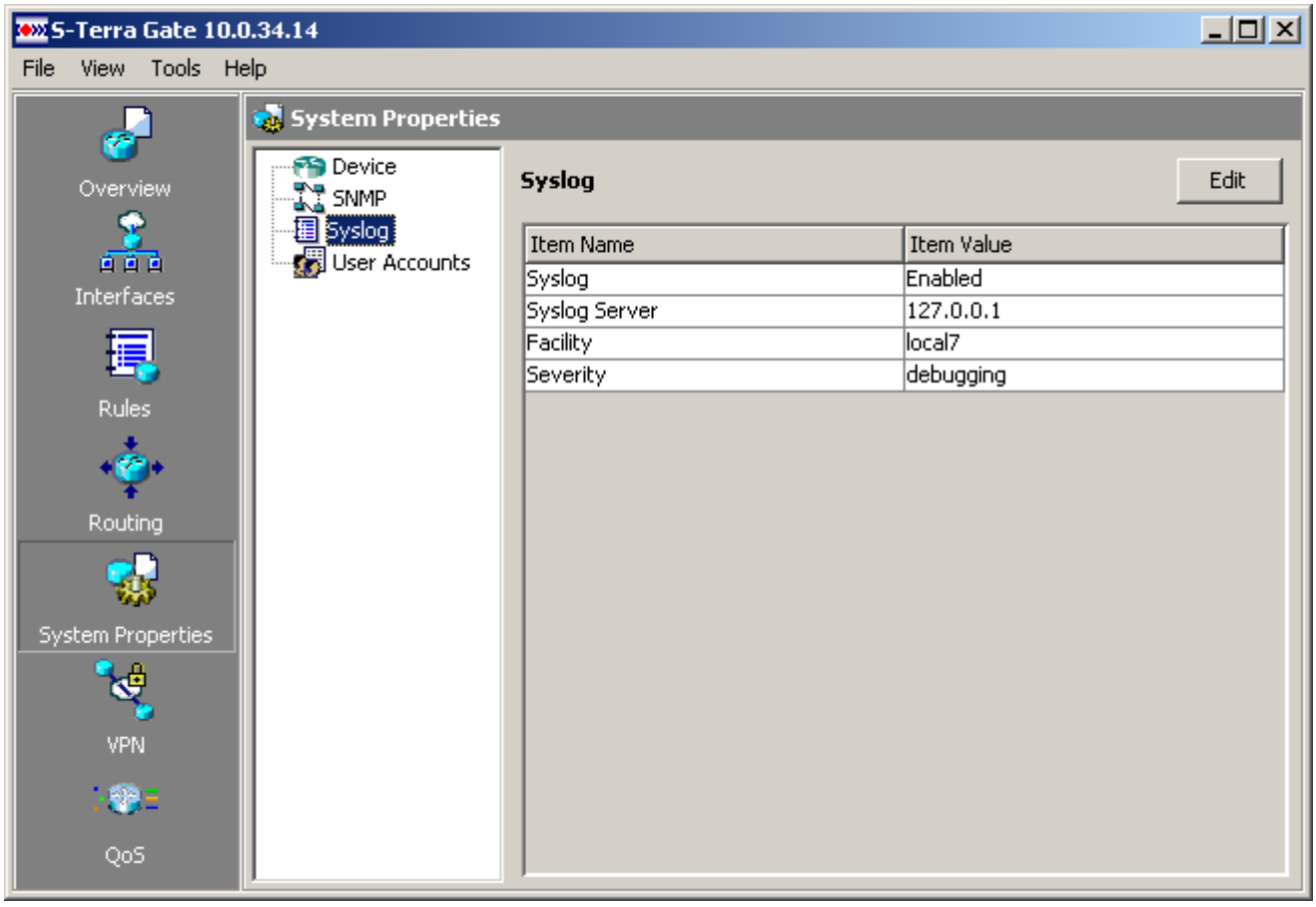

Рисунок 51

Редактирование параметров Syslog

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

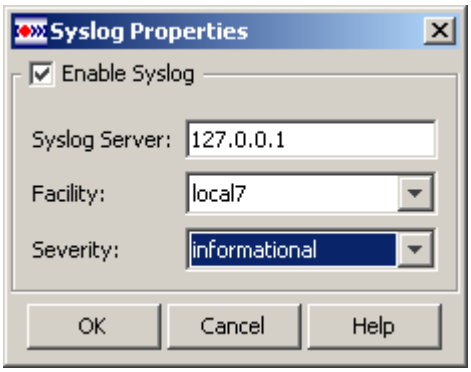

Рисунок 52

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 53) 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 S-Terra 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.

Кнопки управления:

- Add – вызывает окно для ввода нового пользователя.
- Edit – вызов окна редактирования данных выделенного в таблице пользователя.
- Delete – удаление выделенного пользователя.

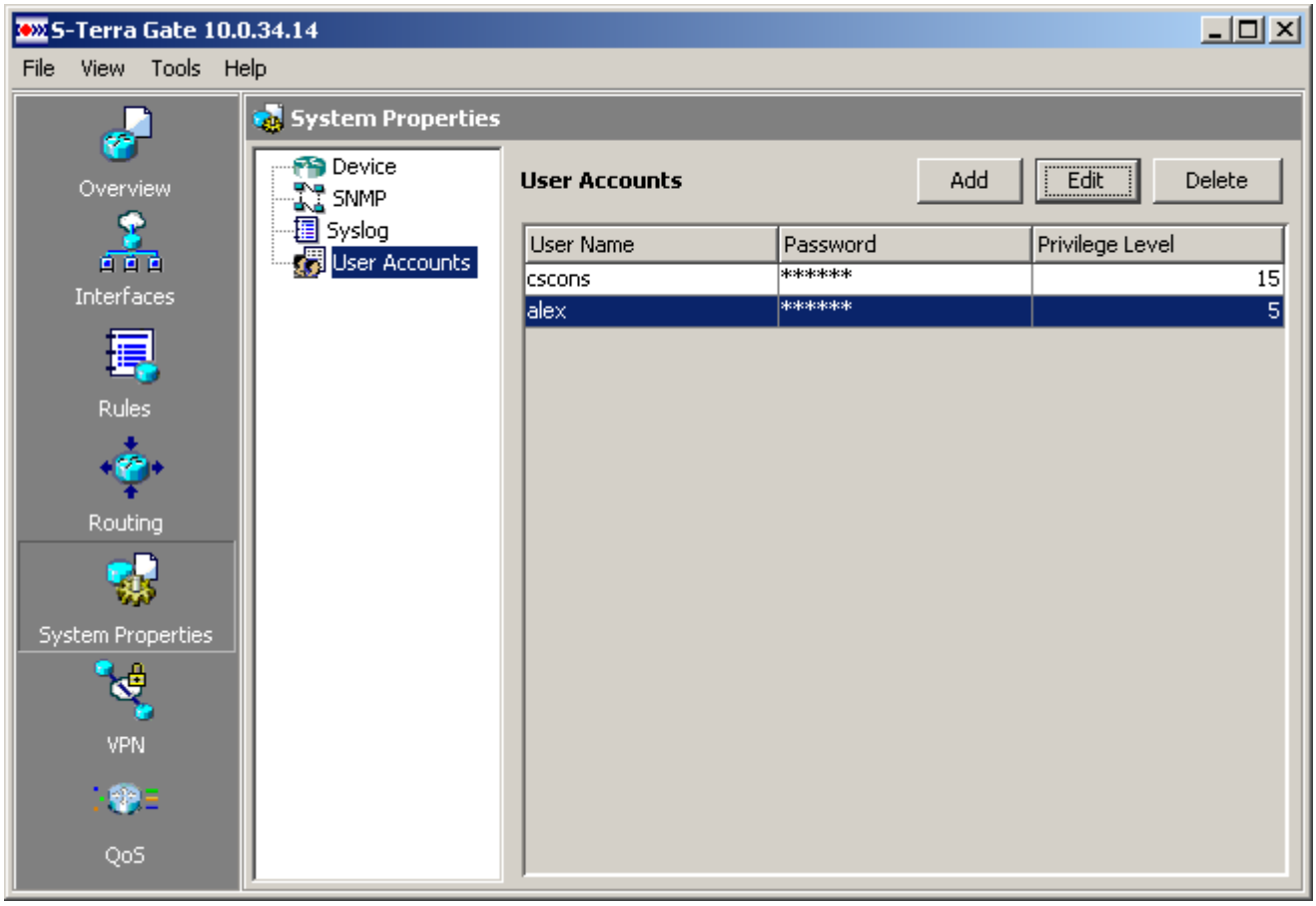

Рисунок 53

Создание пользователя

Создание пользователя производится в окне *Add User Account* (Рисунок 54), вызываемое по нажатию кнопки Add в подразделе *User Accounts*.

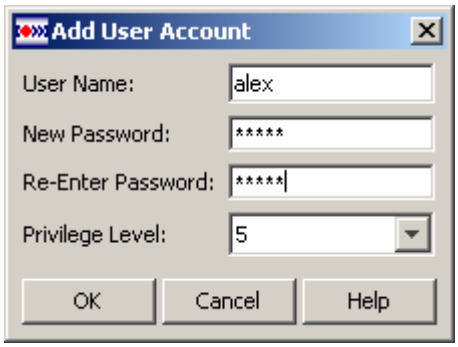

Рисунок 54

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 в данные пользователя, в подразделе *User Accounts* надо выделить пользователя и нажать кнопку Edit. Появится окно *Edit User Account*.

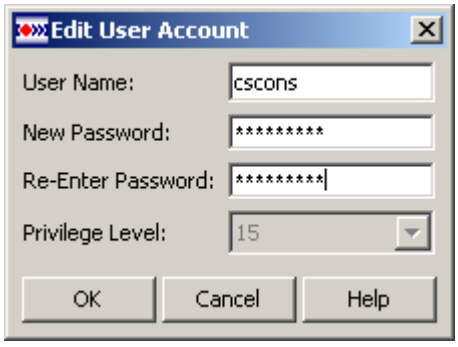

Рисунок 55

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 S-Terra 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 53) 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 56) 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.

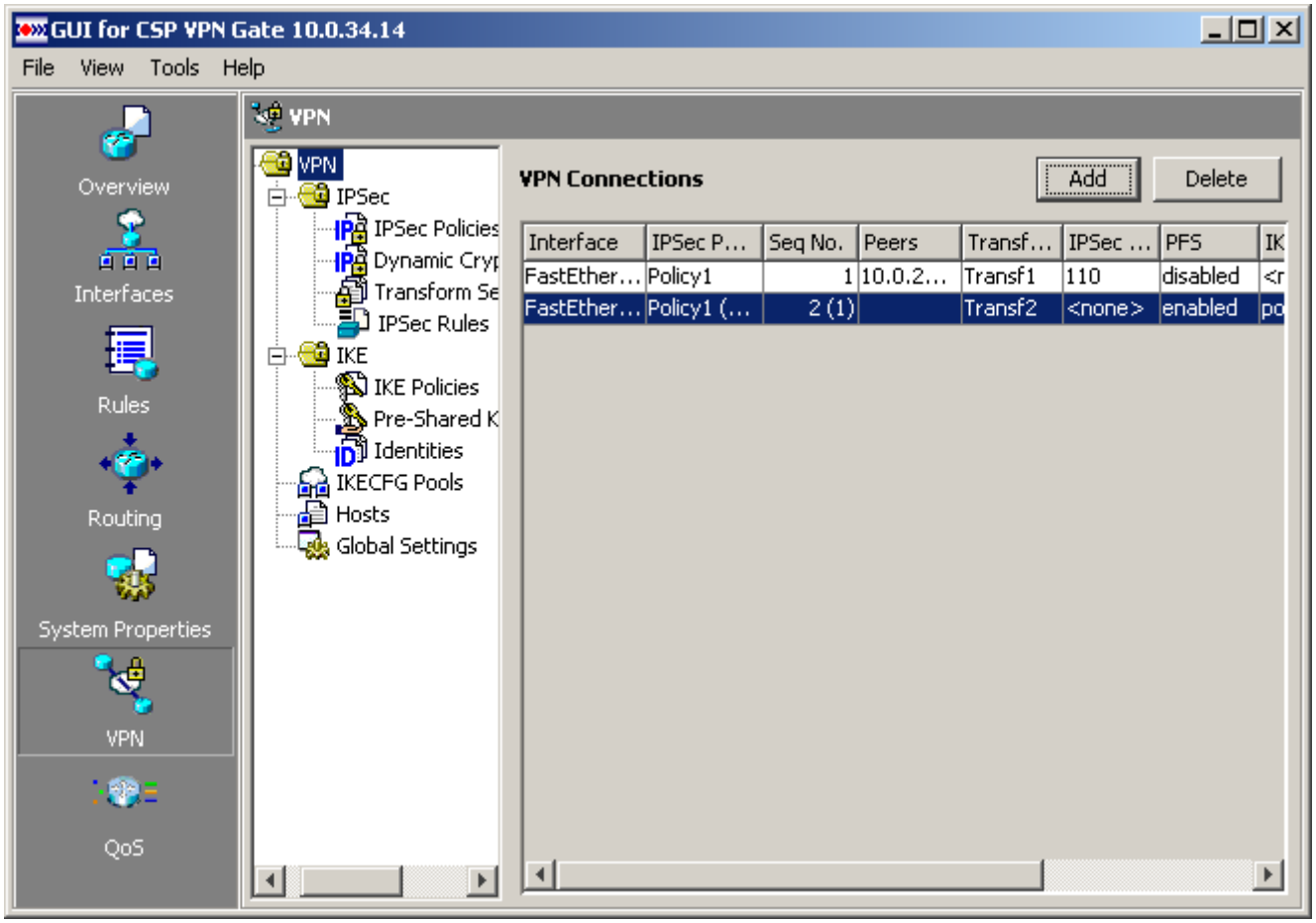

Рисунок 56

Состав элементов конфигурационного окна.

Кнопки управления:

- Add – нажатие этой кнопки открывает окно *Add VPN Connection* (Рисунок 57) 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.
- *IKECFG pool* – 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 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.
- *RRI* – показывает включен или выключен (*On/Off*) механизм RRI (Reverse Route Injection) для соединений, создаваемых с помощью данной криптографической карты.
- *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 57), которое открывается кнопкой Add в разделе *VPN* (Рисунок 56):

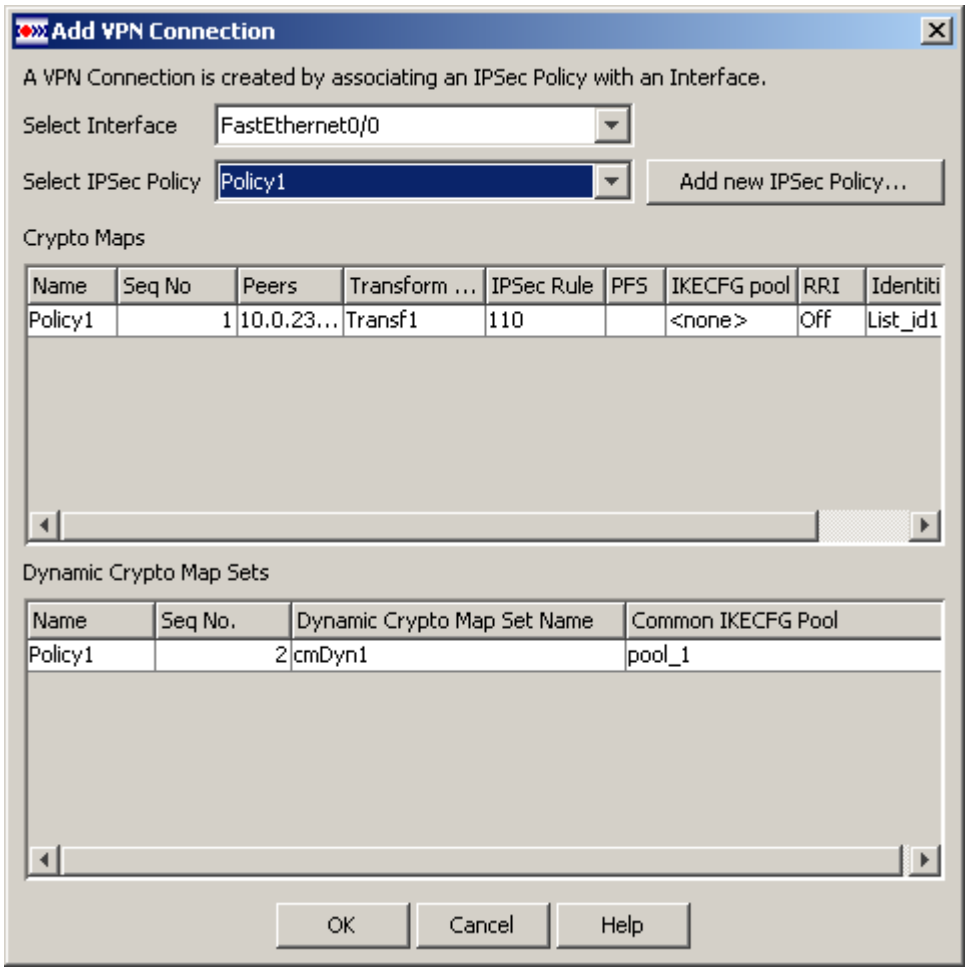

Рисунок 57

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 61) 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 56) появится строка с новым созданным соединением VPN.

Удаление VPN Connection

Удаление выделенного VPN соединения производится с помощью кнопки Delete. Нажатие этой кнопки открывает окно *Delete VPN Connection* (Рисунок 58).

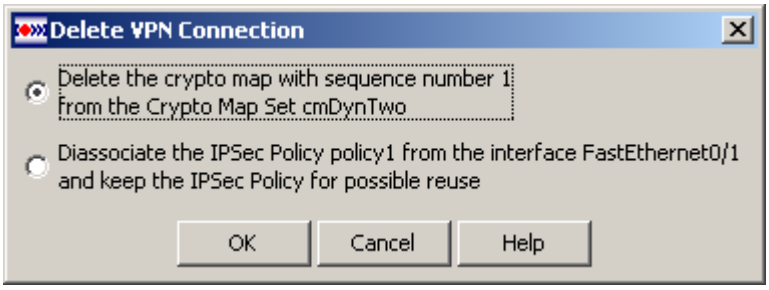

Рисунок 58

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 подразделы, в которых определяются алгоритмы и параметры IPsec, которые будут использоваться для защиты трафика.

Данное окно (Рисунок 59) содержит только текст, поясняющий базовые термины.

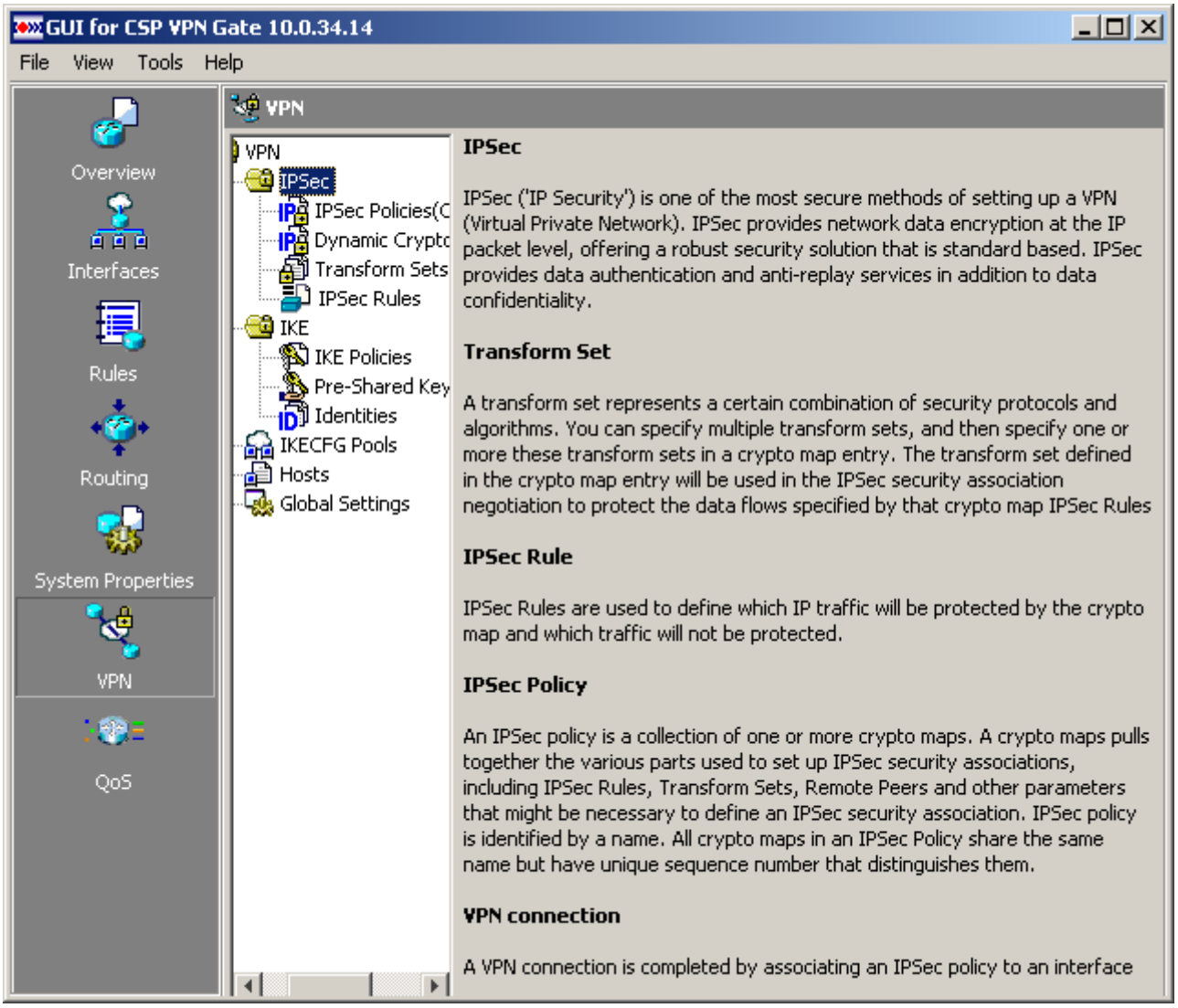

Рисунок 59

IPSec Policies

В разделе *IPSec Policies* (Рисунок 60) 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.

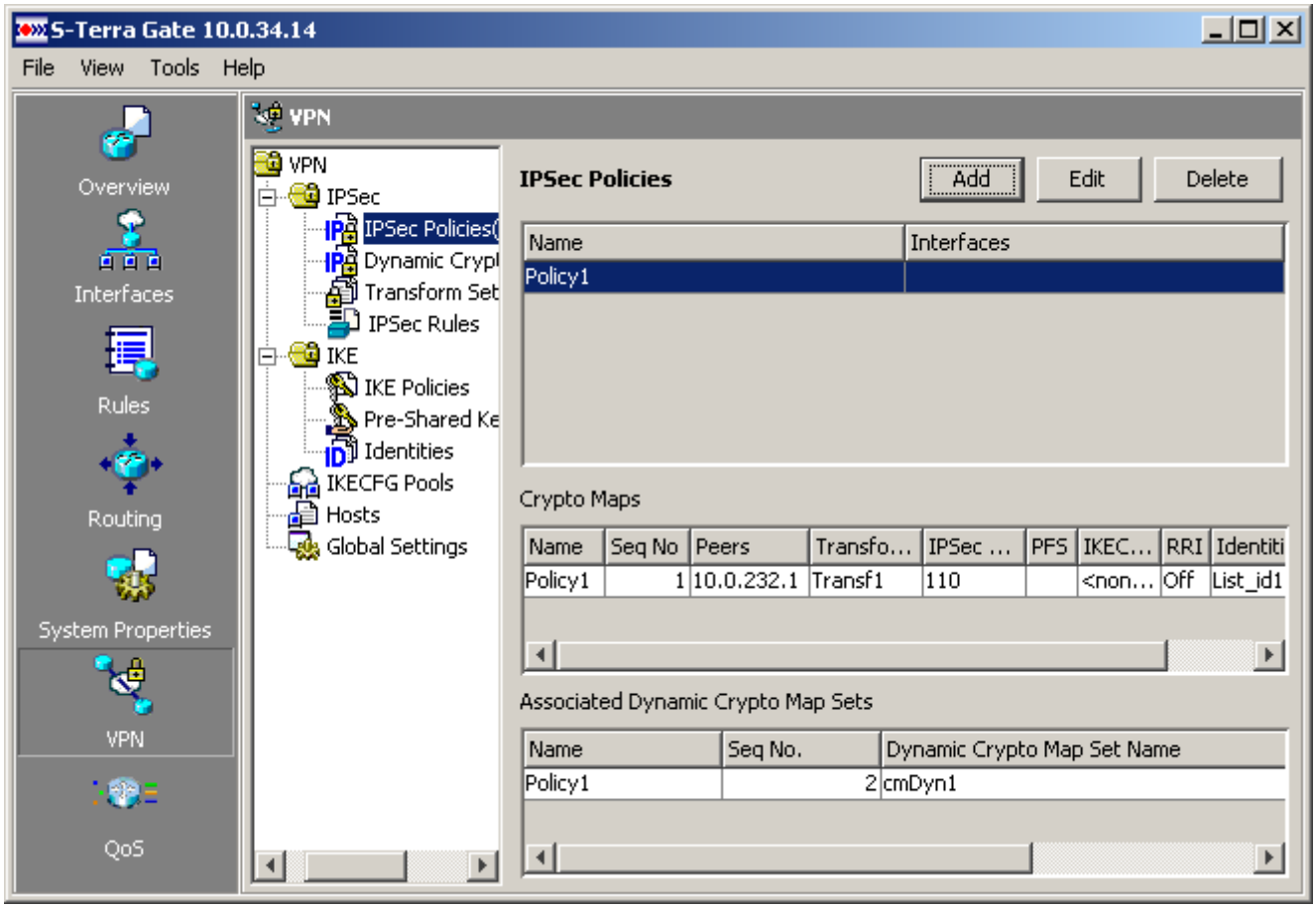

Рисунок 60

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.

Создание политики IPsec производится в окне *Add IPSec Policy* (Рисунок 61), которое открывается при нажатии кнопки Add в окне *IPSec Policies* (Рисунок 60):

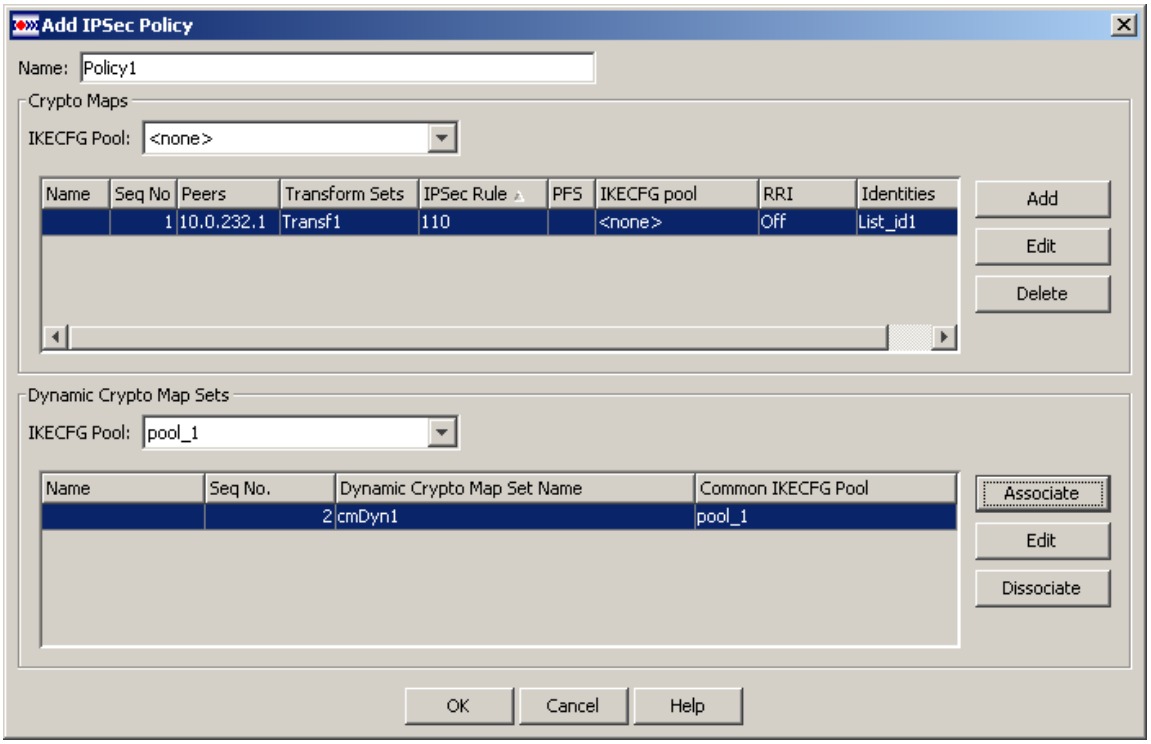

Рисунок 61

Состав элементов окна:

- *Name* – имя создаваемой политики IPsec.
- Группа *Crypto Maps*:
  - *IKECFG Pool* – выпадающий список, позволяющий изменить IKECFG 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 IKECFG 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.
    - *IKECFG pool* – 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.

- *RRI* – показывает включен или выключен (On/Off) механизм RRI (Reverse Route Injection) для соединений, создаваемых с помощью данной криптографической карты.
- *Identities* – имя списка идентификаторов, которому должны удовлетворять сертификаты партнеров.

Кнопки управления:

- Add – вызывает диалог *Add Static CryptoMap* (Рисунок 62) для создания статической криптографической карты.
- Edit – вызывает диалог *Edit Static CryptoMap* (Рисунок 62) для редактирования выделенной статической криптографической карты, совпадающий с окном *Add Static CryptoMap*.
- Delete – вызывает процедуру удаления выделенной криптографической карты.

- Группа *Dynamic Crypto Map Sets*:
  - *IKECFG Pool* – выпадающий список, позволяющий изменить IKECFG 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 IKECFG 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 IKECFG 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 71) 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 в окне *Add IPSec Policy* (Рисунок 61), открывает окно *Add Static CryptoMap* (Рисунок 62) для создания статической криптографической карты. Это окно содержит шесть вкладок.

Вкладка General

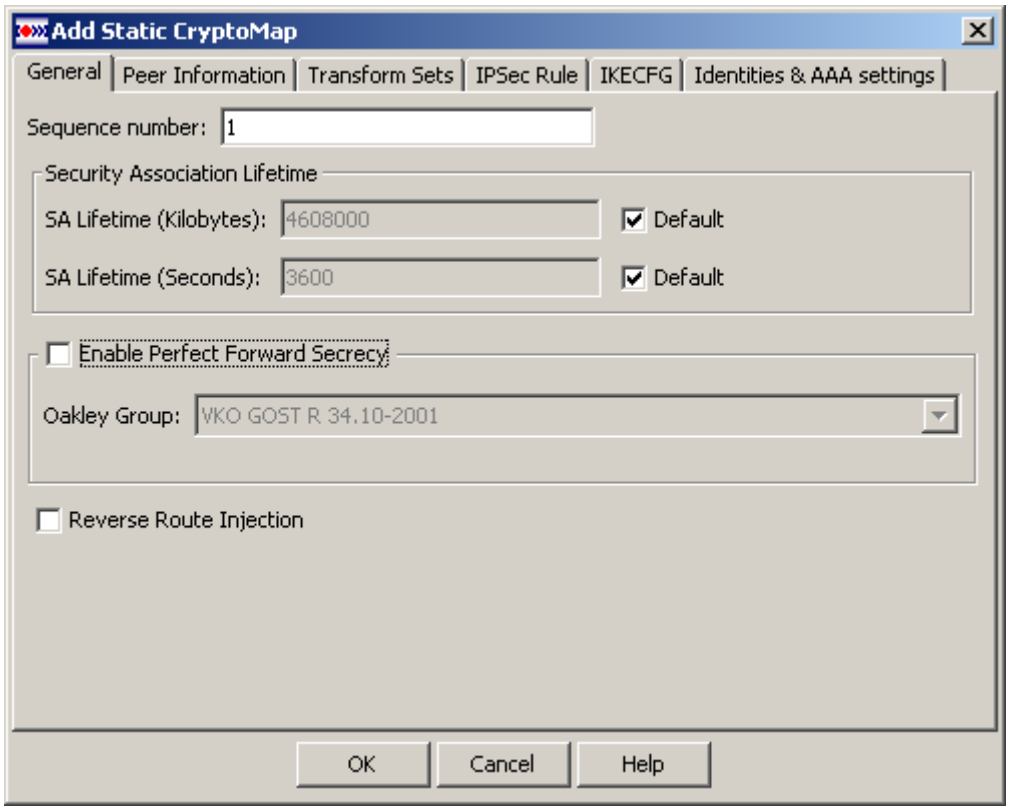

Рисунок 62

Вкладка *General* 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 сторонами данных, 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 GOST R 34.10-2001* – используется алгоритм VKO GOST R 34.10-2001 [RFC4357]. Значение по умолчанию.
    - *VKO GOST R 34.10-2012* – используется алгоритм VKO GOST R 34.10-2012 (256 бит). Алгоритм VKO GOST R 34.10-2012 может применяться, только если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи».
    - *D-H Group1 (768-bit modp)* – используется алгоритм Diffie-Hellman (длина ключа 768 бит).
    - *D-H Group2 (1024-bit modp)* – используется алгоритм Diffie-Hellman (длина ключа 1024 бит).
    - *D-H Group5 (1536-bit modp)* – используется алгоритм Diffie-Hellman (длина ключа 1536 бит).
- *Reverse Route Injection* – 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 «Настройка шлюза» (Settings_gate.pdf)

Вкладка Peer Information

Во вкладке *Peer Information* (Рисунок 63) 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.

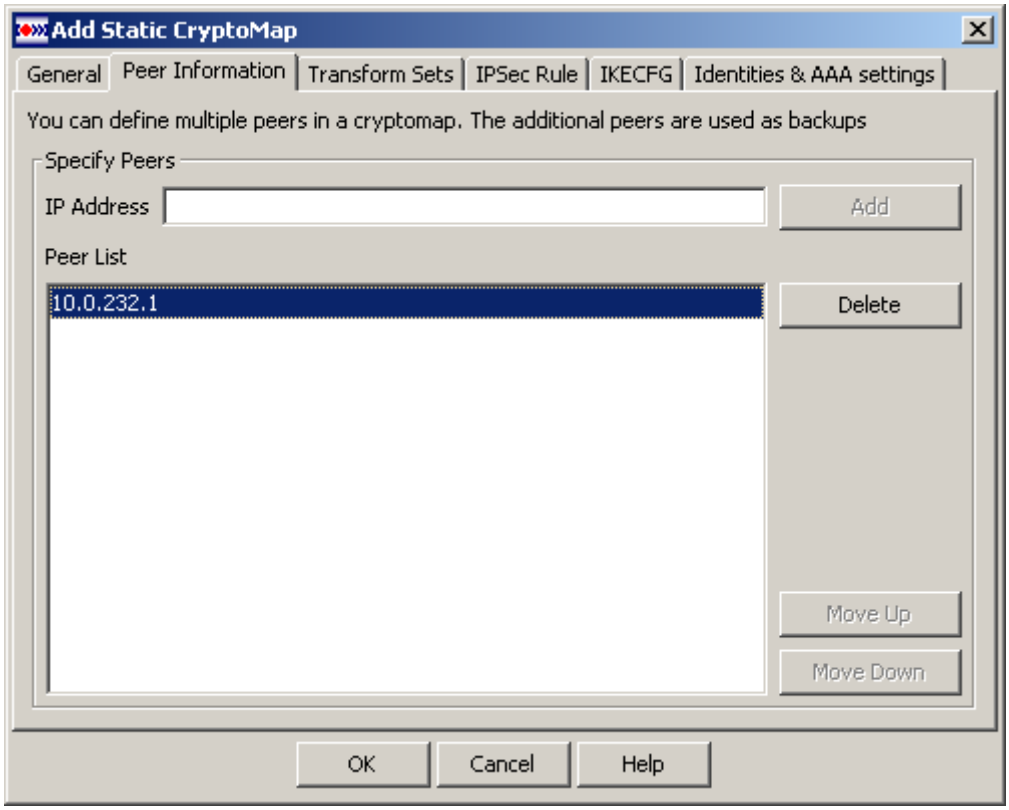

Рисунок 63

Вкладка *Peer Information* 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 T*ransform Sets* (Рисунок 64) выбираются наборы преобразований для реализации политики защиты, которые будут использоваться данной криптографической картой.

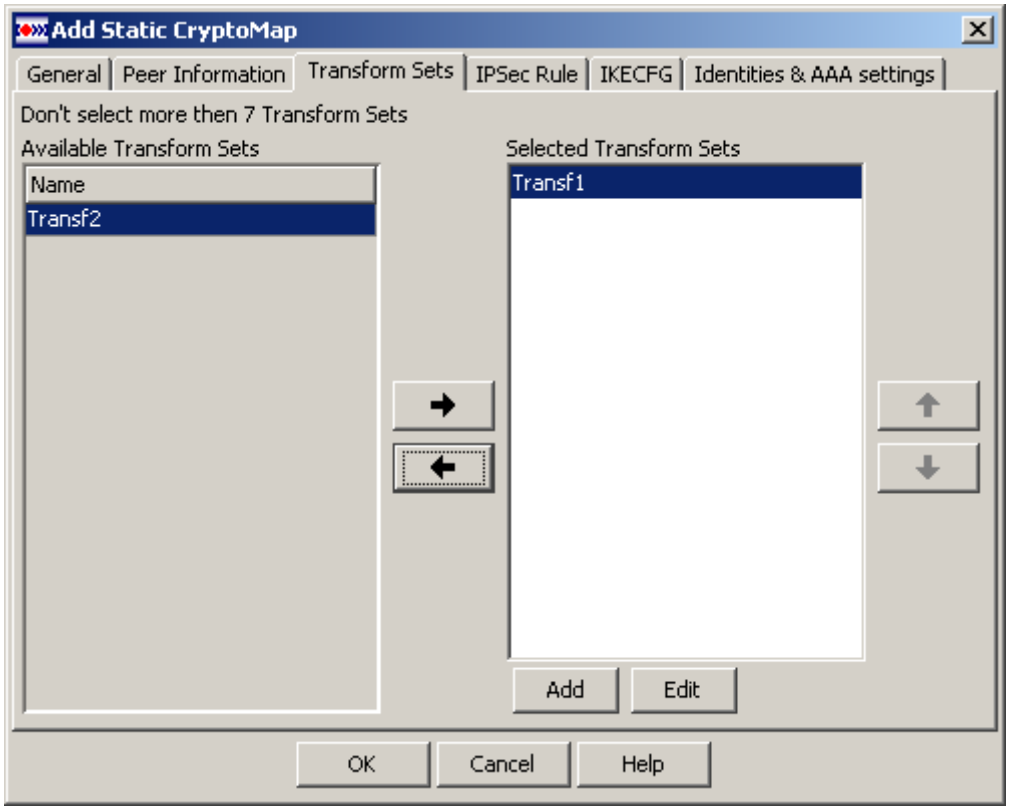

Рисунок 64

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 65) 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 66) 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. Также невозможно выбрать правило, в котором присутствует ссылка на расписание (schedule).
  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 25), описанное в разделе "Создание нового правила IPsec".

Правило обязательно должно быть выбрано, значение *none* не допускается.

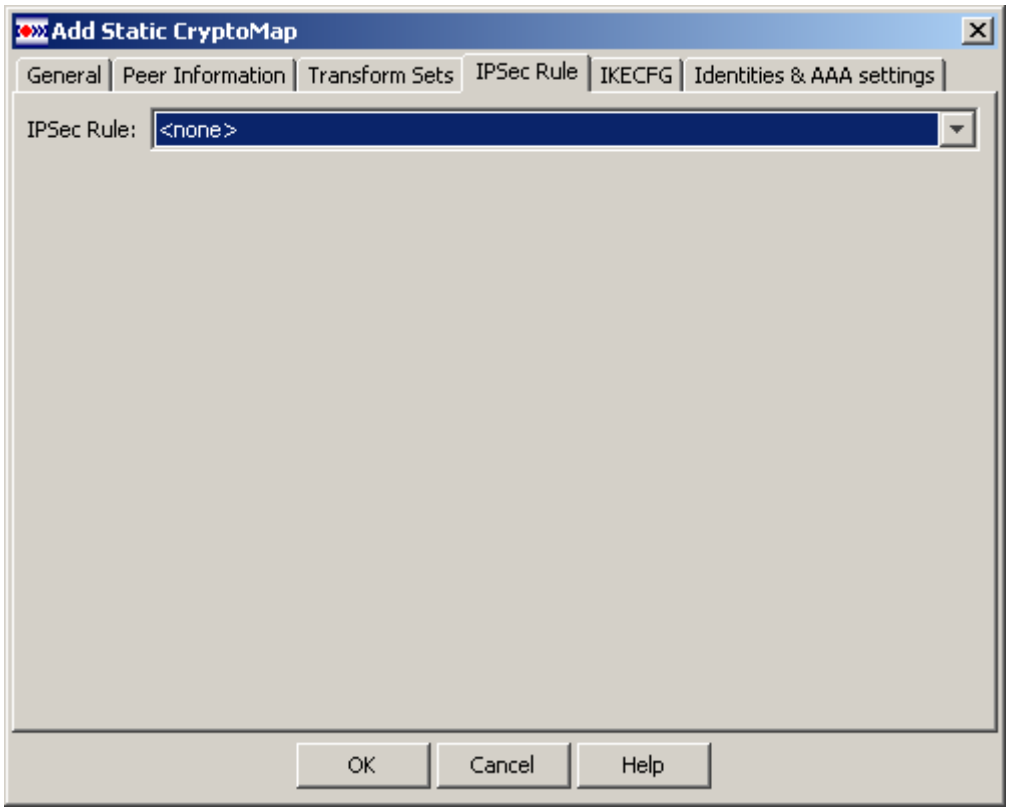

Рисунок 65

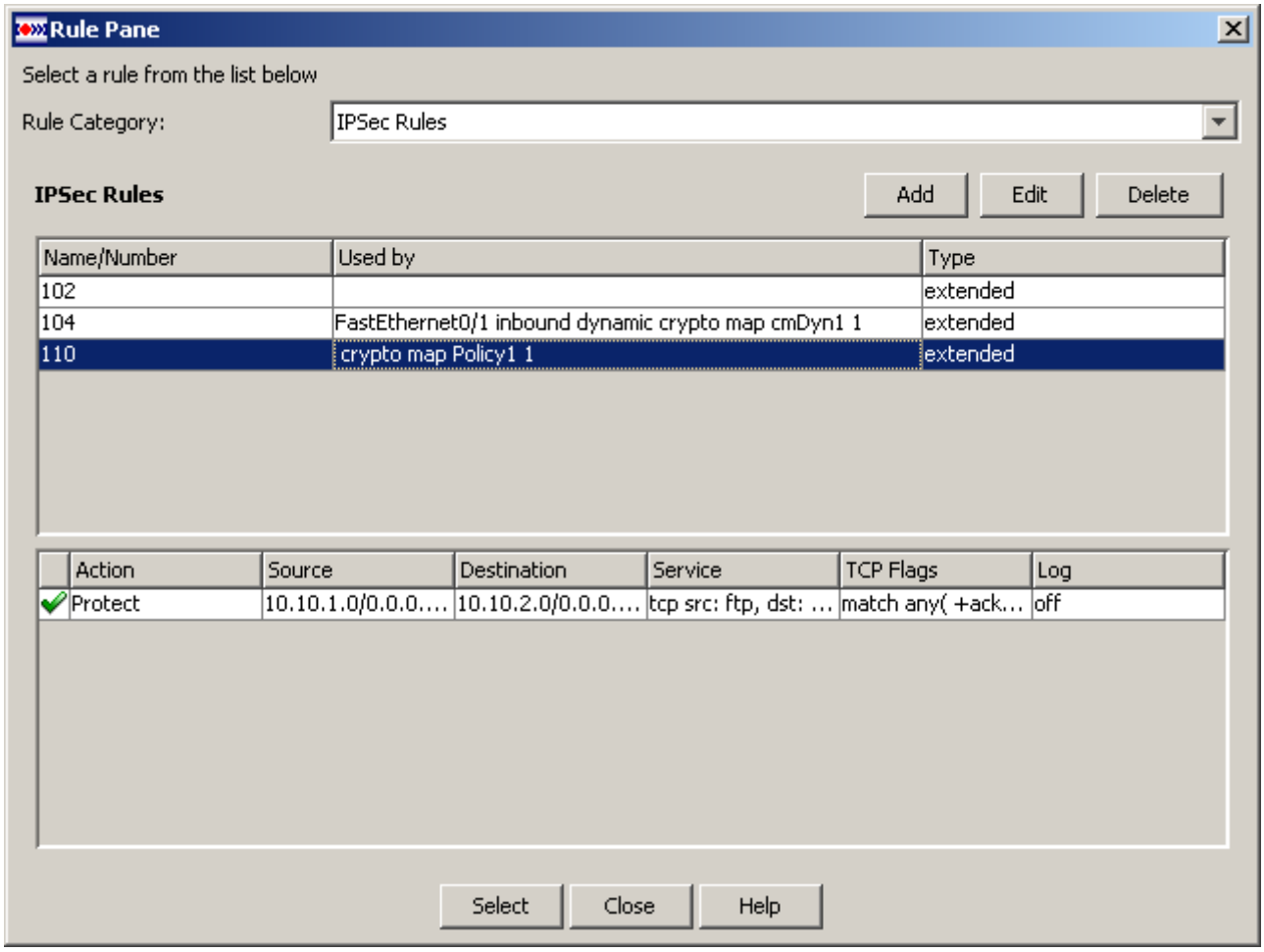

Рисунок 66

При выделении нужного правила в окне *Rule Pane* (Рисунок 66) и нажатии кнопки Select выбранное правило появится во вкладке *IPSec Rule*.

Вкладка IKECFG

Вкладка *IKECFG* (Рисунок 67) используется в основном в динамической криптографической карте для выбора пула адресов, из которого будут выделяться адреса для партнеров.

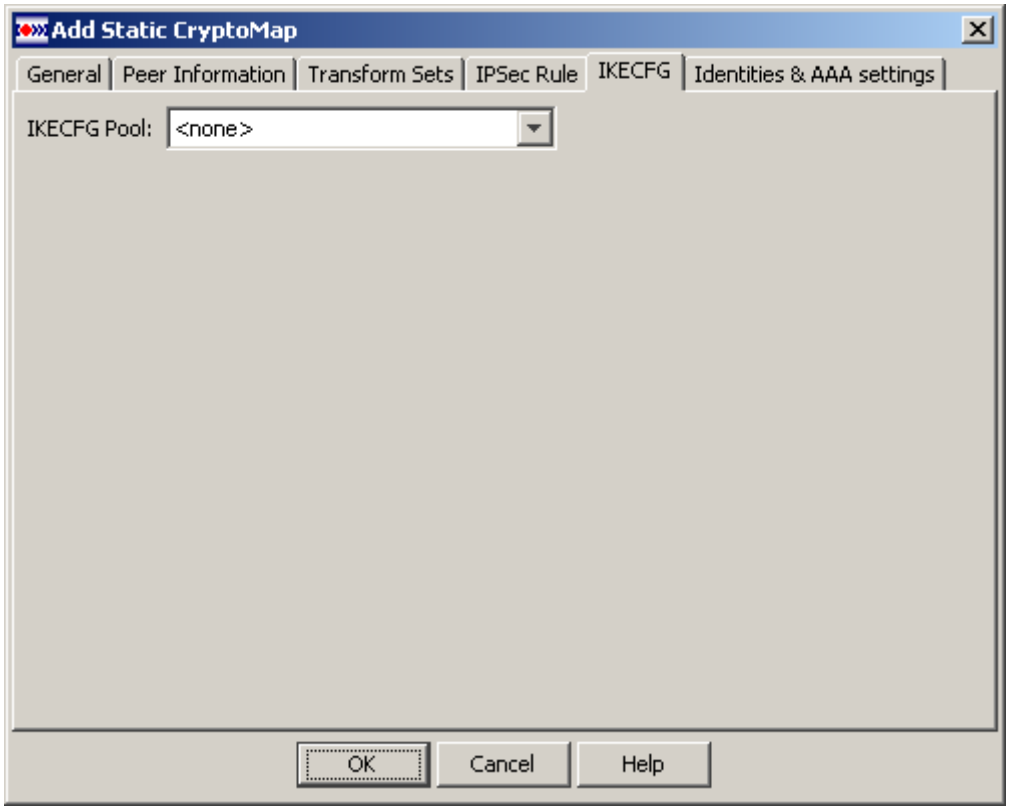

Рисунок 67

Вкладка содержит следующие элементы:

- *IKECFG 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 pool (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 IKECFG Pool Pane for selection* – при выборе этого предложения будет открыто окно *IKECFG Pool Pane* для выбора пула адресов (Рисунок 68).
  - *Create new* – открывается окно *Add IKECFG Pool* для создания нового пула адресов (Рисунок 89).

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

Окно выбора IKECFG пула

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

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

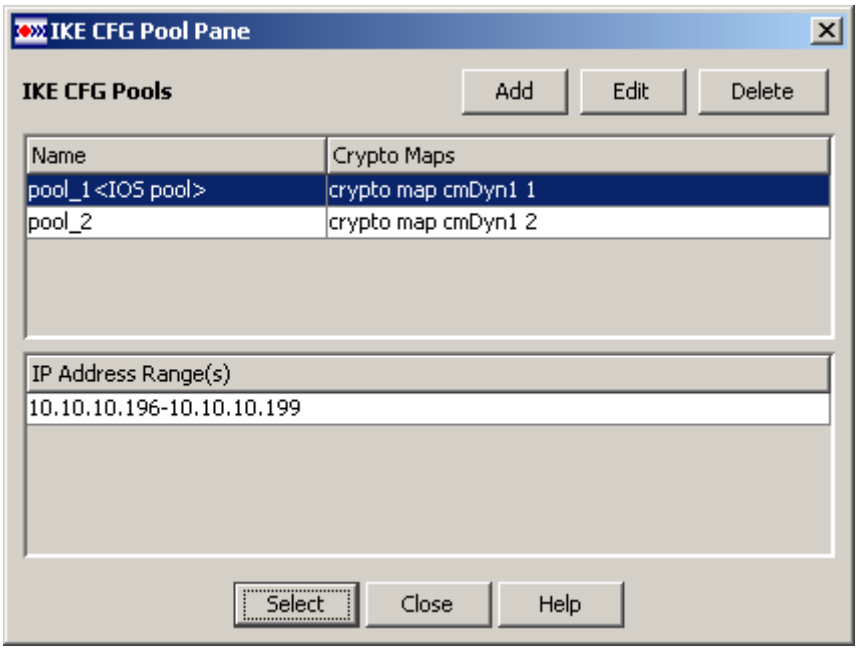

Рисунок 68

Вкладка Identities & AAA settings

Во вкладке *Identities & AAA settings* (Рисунок 69) можно указать список идентификаторов, которому должны удовлетворять сертификаты партнеров, а также идентификатора пользователя в запросе к серверу RADIUS. Эта вкладка необязательна для заполнения. Списки идентификаторов создаются в разделе *Identities*.

Вкладка содержит:

- поле *Identity List* с выпадающим списком значений:
  - *<none>* – идентификатор не задан.
  - *Use Identity List Pane for selection* – при выборе этого значения будет открыто окно *Identity List Pane* (Рисунок 70) для выбора списка идентификаторов.
  - *Create new* – вызывает диалог *Add Identity List* (Рисунок 85) для создания нового списка идентификаторов, описанный в разделе «Создание нового списка идентификаторов».
- поле *Radius username* с выпадающим списком значений служит для задания идентификатора пользователя в запросе к серверу RADIUS:
  - *<none>* – запрос к серверу RADIUS не отправляется.
  - *IKE identificator* – значение IKE-идентификатора партнёра ISAKMP соединения.
  - *CN from cert subj* – в качестве идентификатора используется значение поля CommonName (“CN=…”) из описания (Subject) сертификата партнёра.
  - *OU from cert subj* – в качестве идентификатора используется значение поля OrganizationUnit (“OU=…”) из описания (Subject) сертификата партнёра.

- *EMAIL from cert altsubj* – в качестве идентификатора используется значение поля EMail (“EMAIL=…”) из альтернативного описания (Alternative subject) сертификата партнёра.
- *DNS from cert altsubj* – в качестве идентификатора используется значение поля DNS (“DNS=…”) из альтернативного описания (Alternative subject) сертификата партнёра.

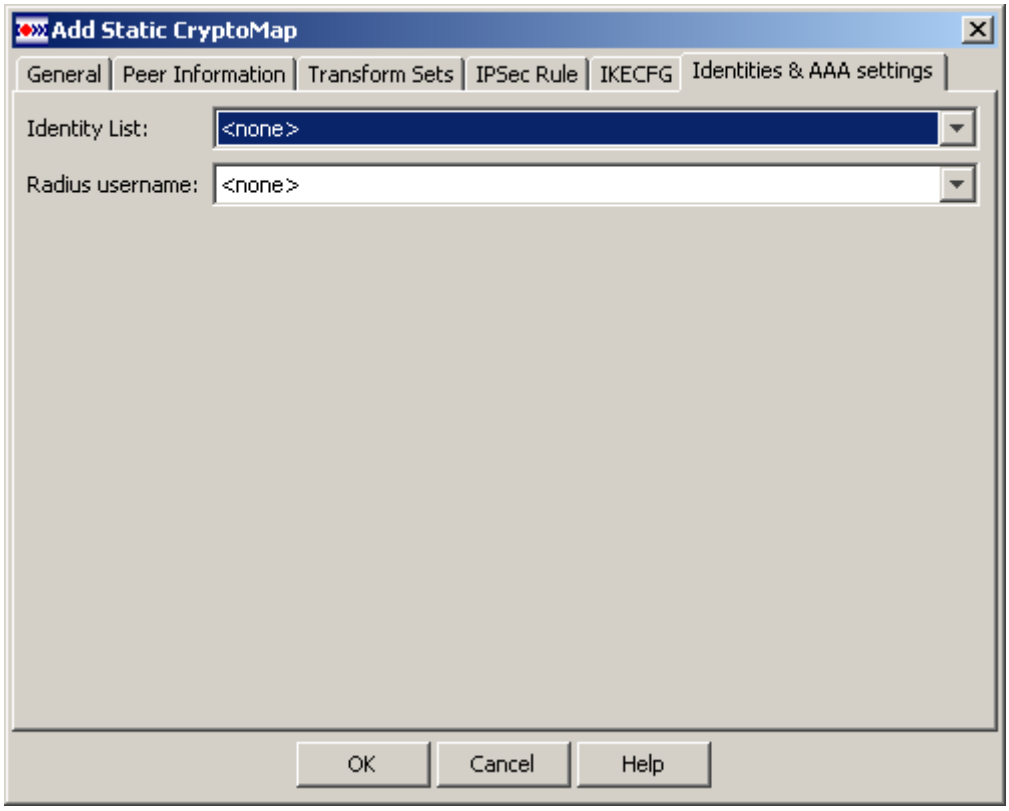

Рисунок 69

Окно выбора идентификаторов

Окно *Identity List Pane* (Рисунок 70) 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.

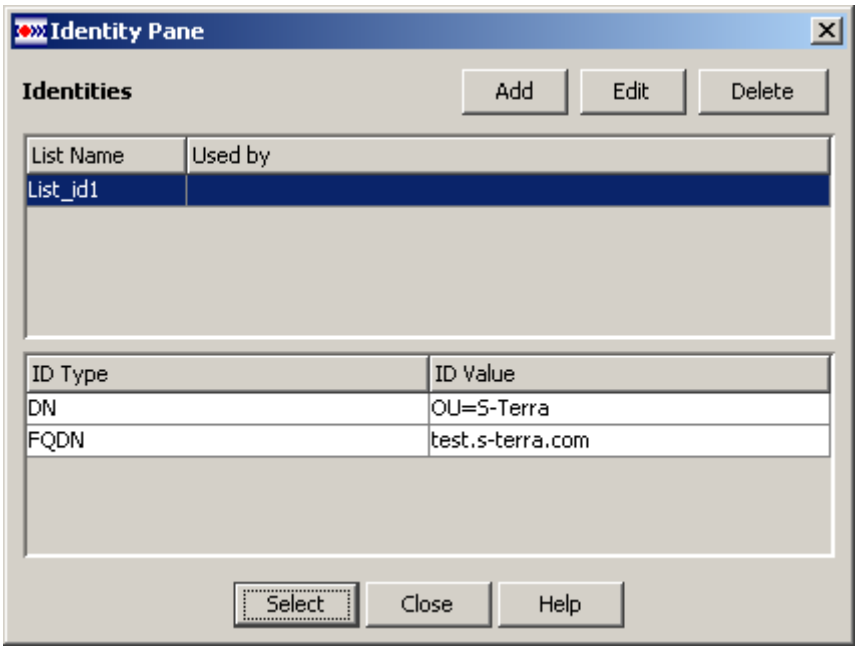

Рисунок 70

После заполнения всех вкладок окна A*dd Static CryptoMap* (Рисунок 62) и нажатии кнопки OK, статическая криптографическая карта будет создана и в окне *Add IPSec Policy* (Рисунок 61) в таблице *Crypto Maps* появится строка с созданной криптокартой.

Редактирование криптографической карты

Редактирование выделенной криптографической карты в окне *Add IPSec Policy* (Рисунок 61) 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 61) производится с помощью кнопки Delete. При этом открывается 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 61) вызывается диалог *Associate Dynamic Crypto Map Set* (Рисунок 71). 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.

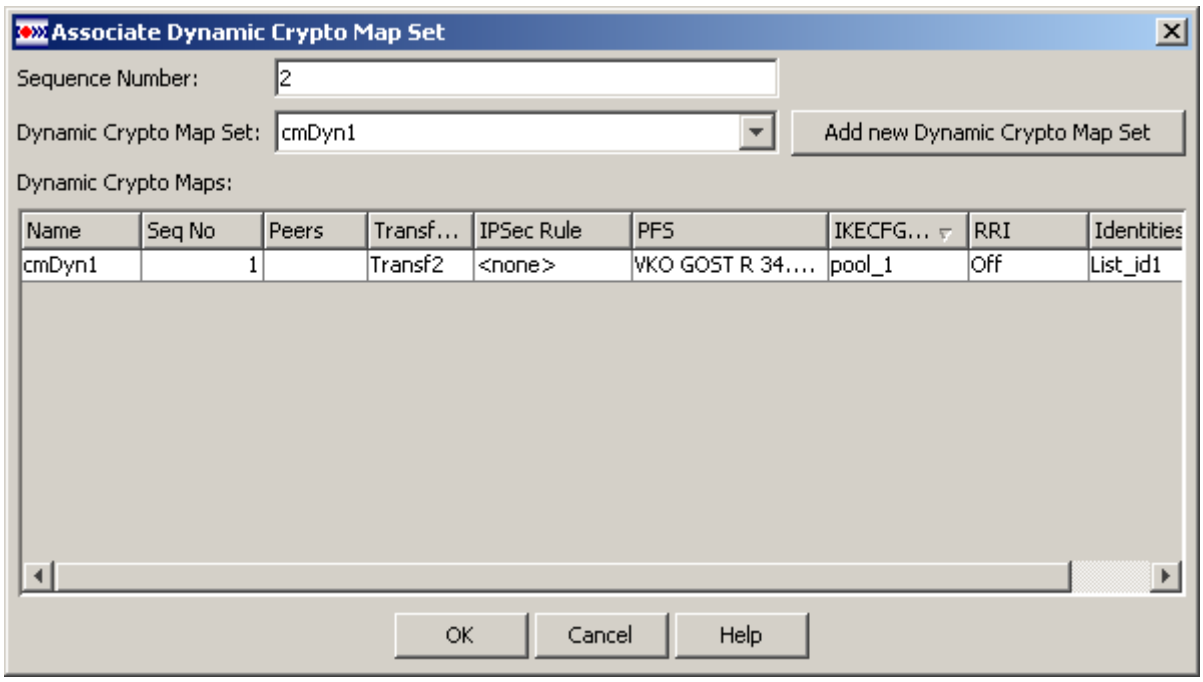

Рисунок 71

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 73) для создания нового набора динамических криптографических карт.

Редактирование связи

Нажатие кнопки Edit в окне *Add IPSec Policy* (Рисунок 61) 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 71). 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 61) 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 60) производится в окне *Edit IPSec Policy*, 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 60) 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.

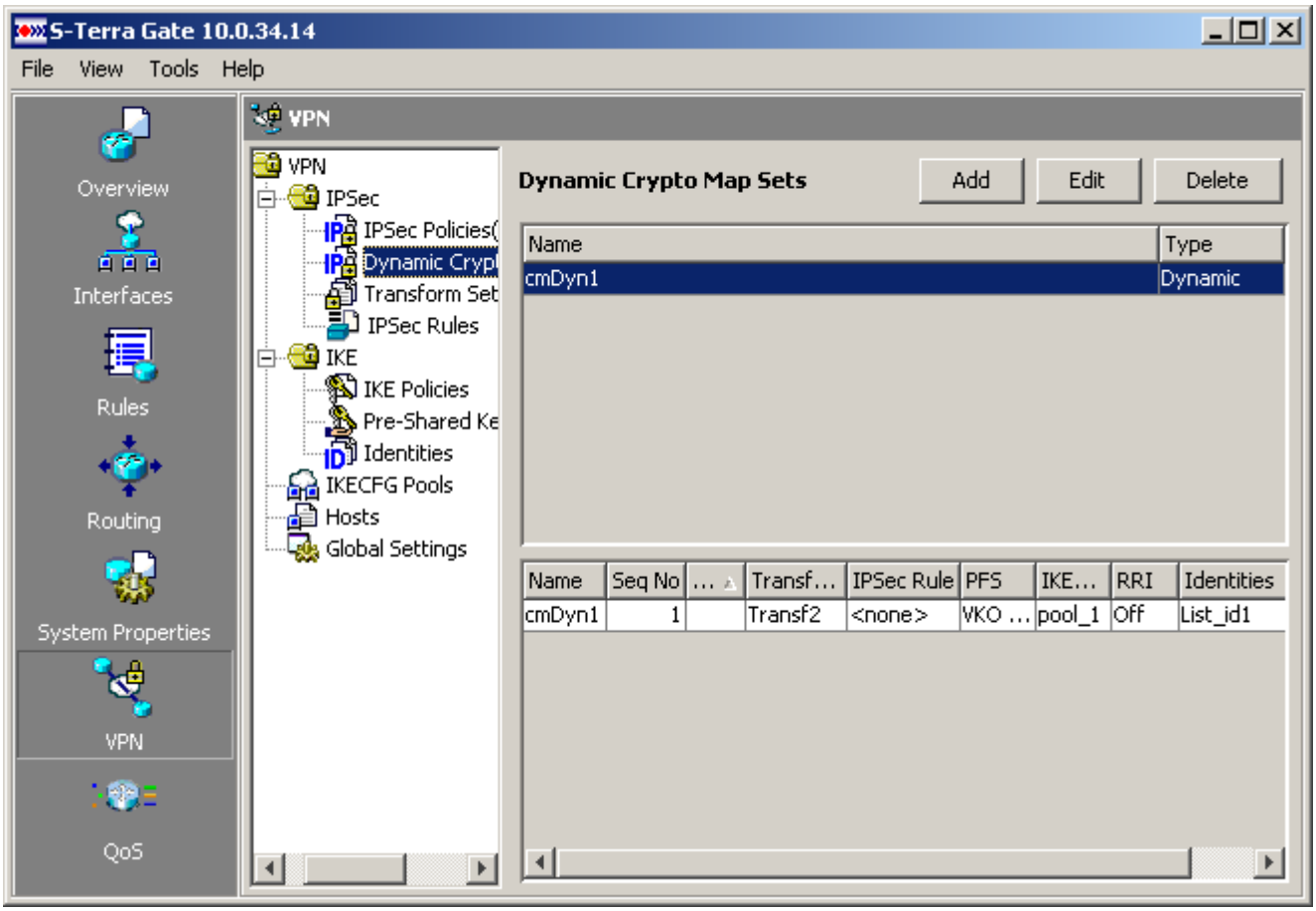

Рисунок 72

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 73), который вызывается кнопкой Add в разделе *Dynamic Crypto Map Sets* (Рисунок 72).

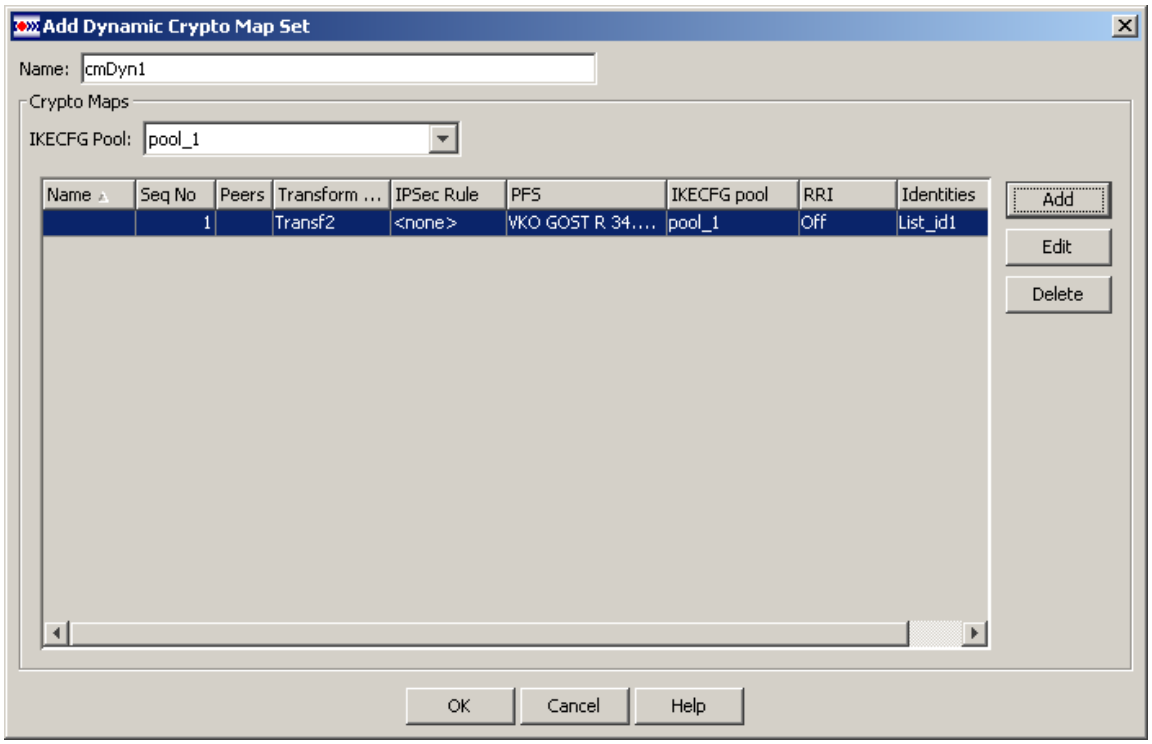

Рисунок 73

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 OK.
  - *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.
  - *IKECFG pool* – показывает выбранный пул адресов.
  - *RRI* – показывает включен или выключен (On/Off) механизм RRI (Reverse Route Injection) для соединений, создаваемых с помощью данной криптографической карты.

- *Identities* – имя списка идентификаторов, которому должны удовлетворять сертификаты партнеров.

Кнопки управления:

- Add – вызывает диалог *Add Dynamic CryptoMap* (Рисунок 74) 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 73) открывает окно *Add Dynamic Crypto Map* (Рисунок 74) для создания динамической криптографической карты. Это окно содержит шесть вкладок.

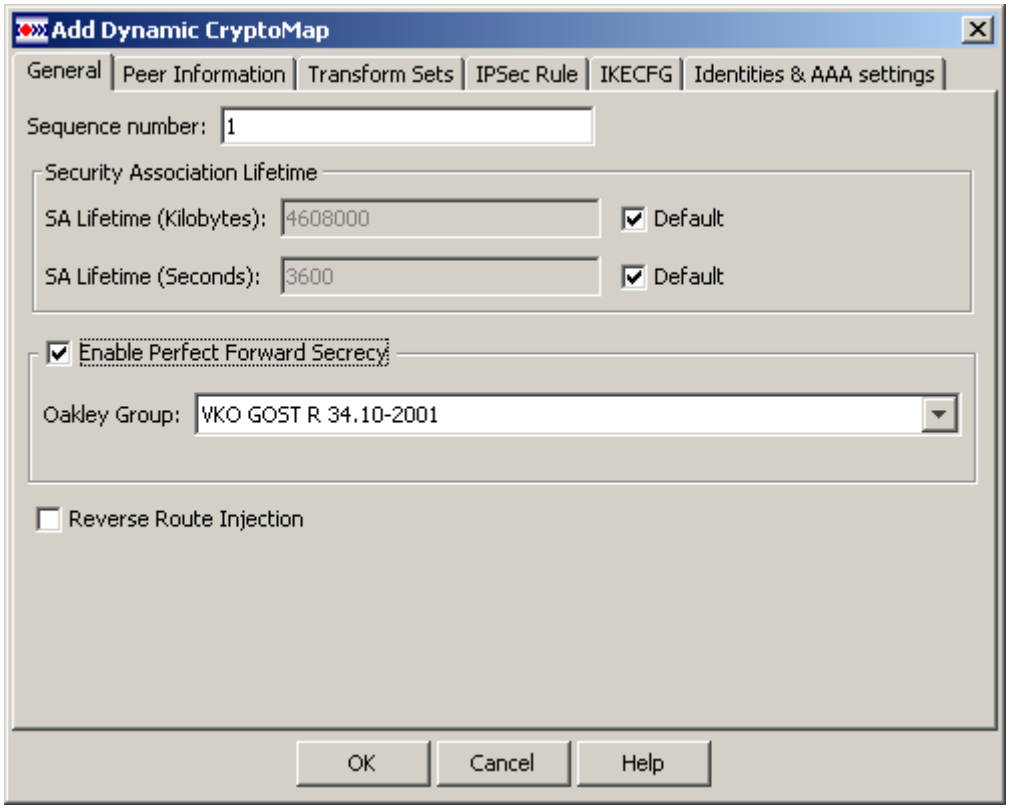

Рисунок 74

Вкладки диалога *Add Dynamic CryptoMap* полностью совпадают с вкладками при создании статической криптокарты (Рисунок 62), за исключением вкладок *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 73) 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

Криптокарта, выделенная в окне *Add Dynamic Crypto Map Se*t (Рисунок 73), при нажатии кнопки Delete удаляется, при подтверждении процедуры удаления.

Редактирование набора динамических криптокарт

Редактирование выделенного в окне *Dynamic Crypto Map Sets* (Рисунок 72) набора динамических криптокарт 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 73).

Удаление набора динамических криптокарт

При удалении выделенного набора динамических криптокарт кнопкой Delete (Рисунок 72) 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 75) 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).

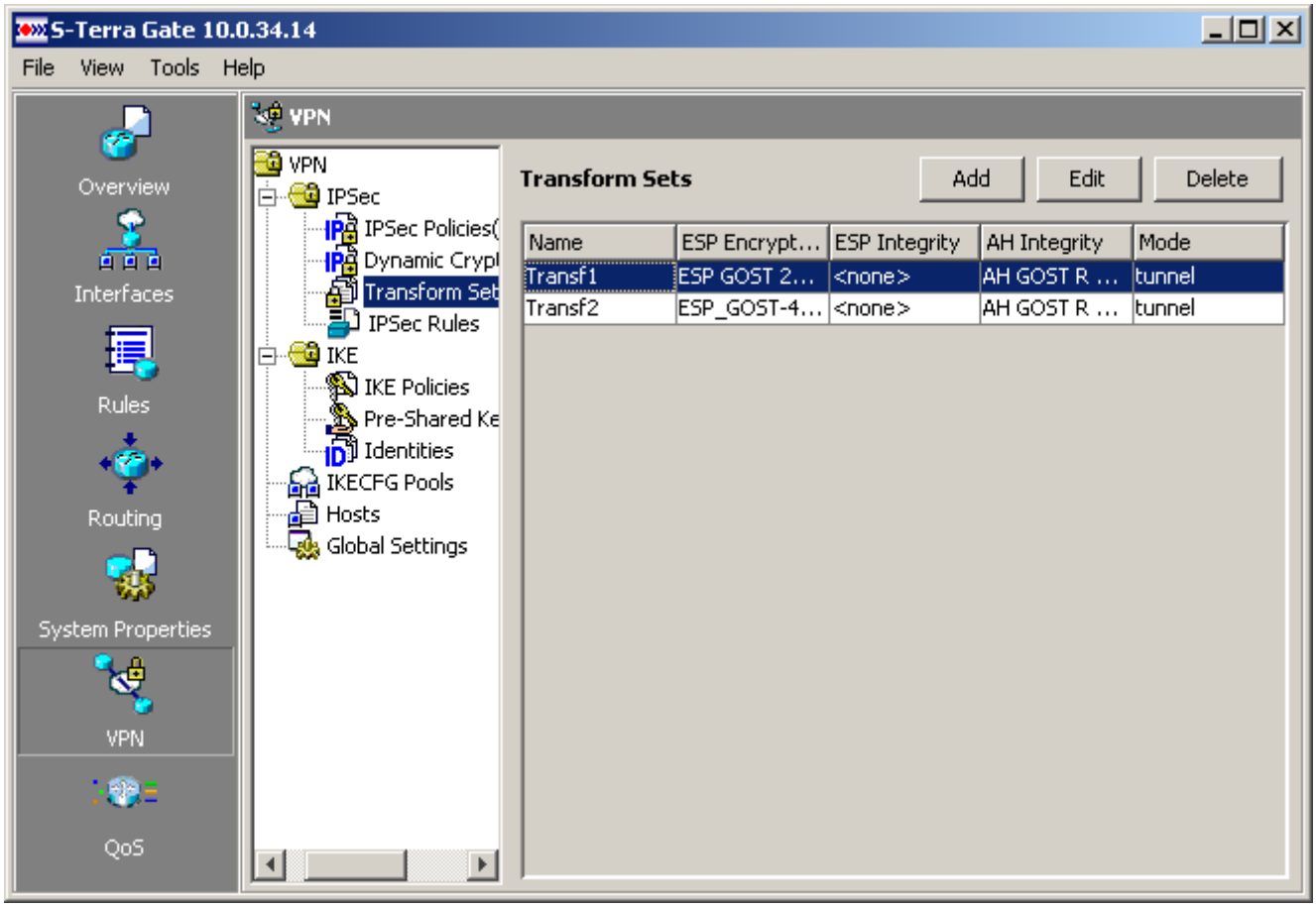

Рисунок 75

Создание нового Transform Set

Нажатие кнопки Add в окне *Transform Set* (Рисунок 76) 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.

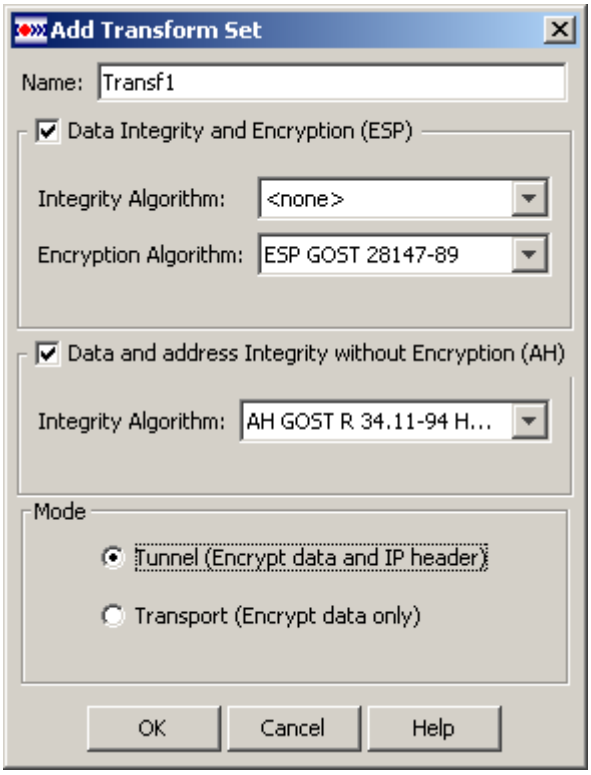

Рисунок 76

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.
    - *<none>* – алгоритм не выбран.
    - *ESP GOST R 34.11-94 HMAC96* – протокол ESP с алгоритмом ГОСТ Р 34.11-94.
    - *ESP GOST 28147-89 MAC* – протокол ESP с алгоритмом ГОСТ 28147-89 (в режиме выработки имитовставки).
    - *ESP SHA HMAC* – протокол ESP с алгоритмом аутентификации SHA.
    - *ESP MD5 HMAC* – протокол ESP с алгоритмом аутентификации MD5.
  - *Encryption Algorithm* – выпадающий список предустановленных алгоритмов шифрования для протокола ESP. Не допускается комбинация ESP Null алгоритма и *<none>* для ESP Integrity алгоритма:
    - *<none>* – алгоритм не выбран.
    - *ESP GOST 28147-89* – протокол ESP с алгоритмом ГОСТ 28147-89 (в режиме простой замены с зацеплением).
    - *ESP GOST_4M-IMIT* – протокол ESP с алгоритмом ГОСТ 28147-89 (в комбинированном режиме: гаммирование и вычисление имитовставки в соответствии со спецификацией ESP_GOST-4M-IMIT).
    - *ESP DES* – протокол ESP с 56-битным алгоритмом DES.
    - *ESP 3DES* – протокол ESP с 168-битным алгоритмом 3DES.

- *ESP AES 128* – протокол ESP с 128-битным алгоритмом AES.
- *ESP AES 192* – протокол ESP с 192-битным алгоритмом AES.
- *ESP AES 256* – протокол ESP с 256-битным алгоритмом AES.
- *ESP NULL* – протокол ESP с алгоритмом Null.

- 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. При использовании NAT не активируйте эту группу.
    - *<none>* – алгоритм не выбран.
    - *AH GOST R 34.11-94 HMAC96* – протокол AH с алгоритмом ГОСТ Р 34.11-94.
    - *AH GOST R 28147-89 MAC* – протокол AH с алгоритмом ГОСТ 28147-89 (в режиме выработки имитовставки).
    - *AH SHA HMAC* – протокол AH с алгоритмом аутентификации SHA.
    - *AH MD5 HMAC* – протокол AH с алгоритмом аутентификации MD5.
- 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*. 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.

Удаление 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 77) 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.

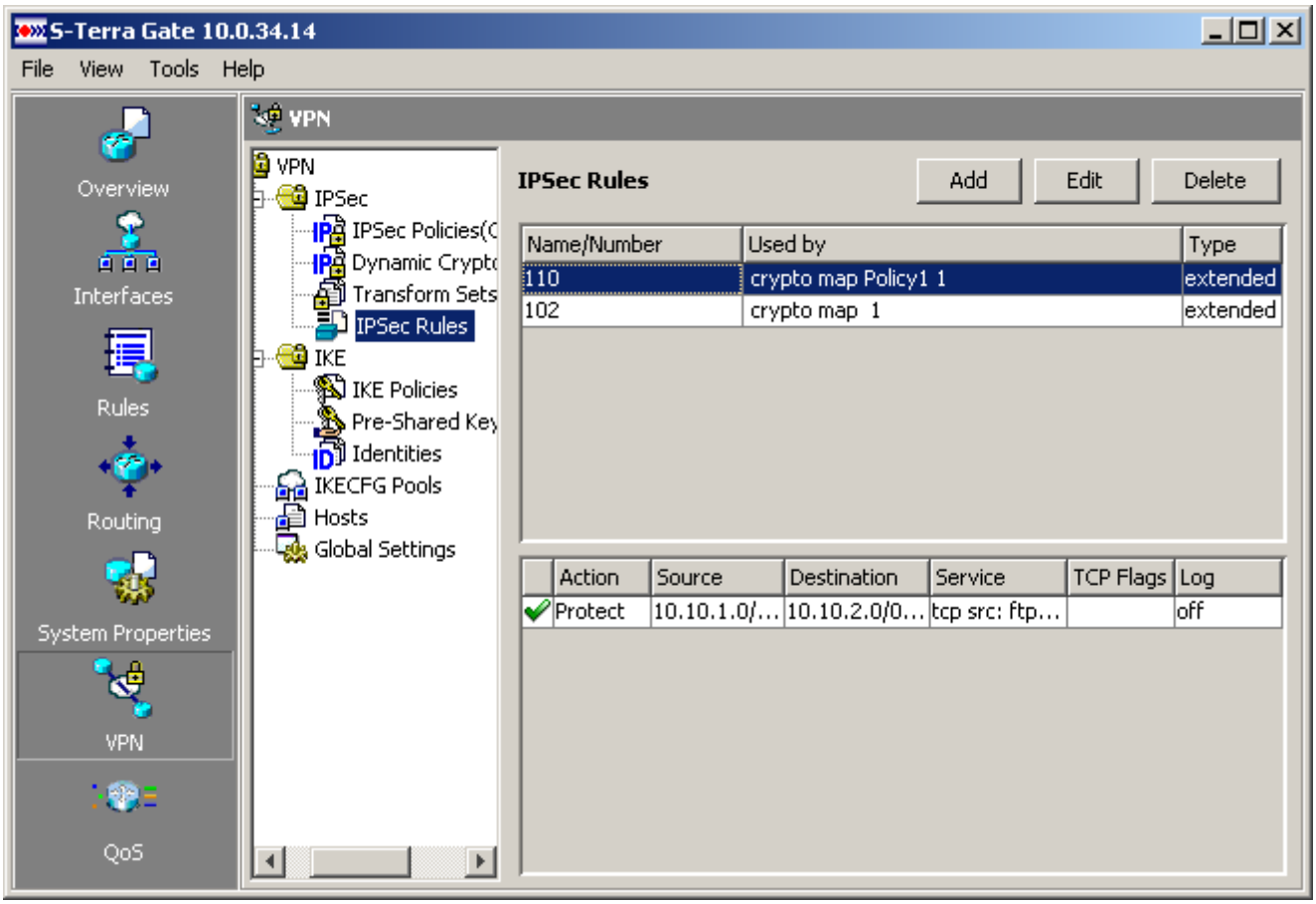

Рисунок 77

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

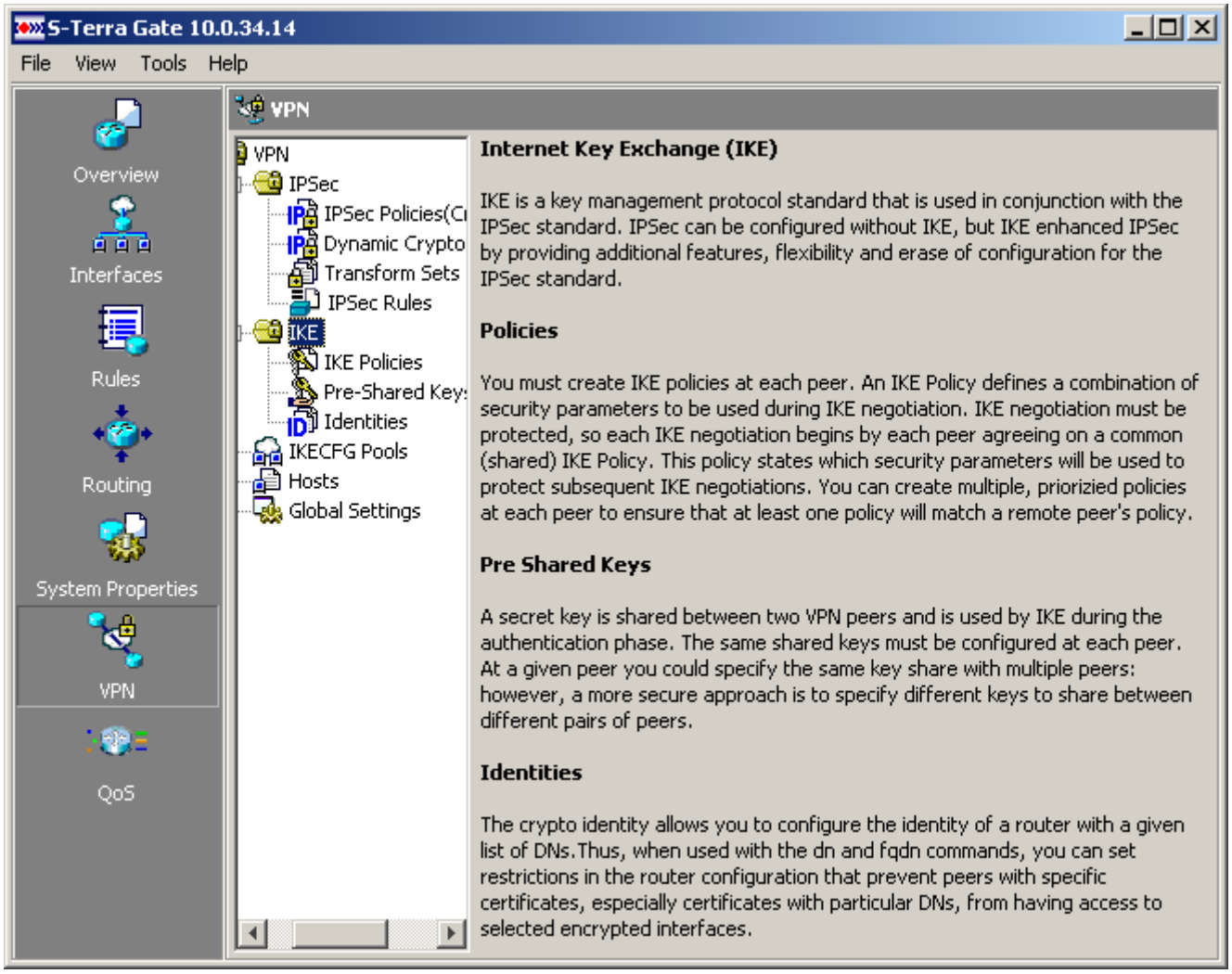

Рисунок 78

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 79) расположена таблица с разными политиками IKE. Здесь можно просматривать политики IKE, создавать, редактировать и удалять политики IKE.

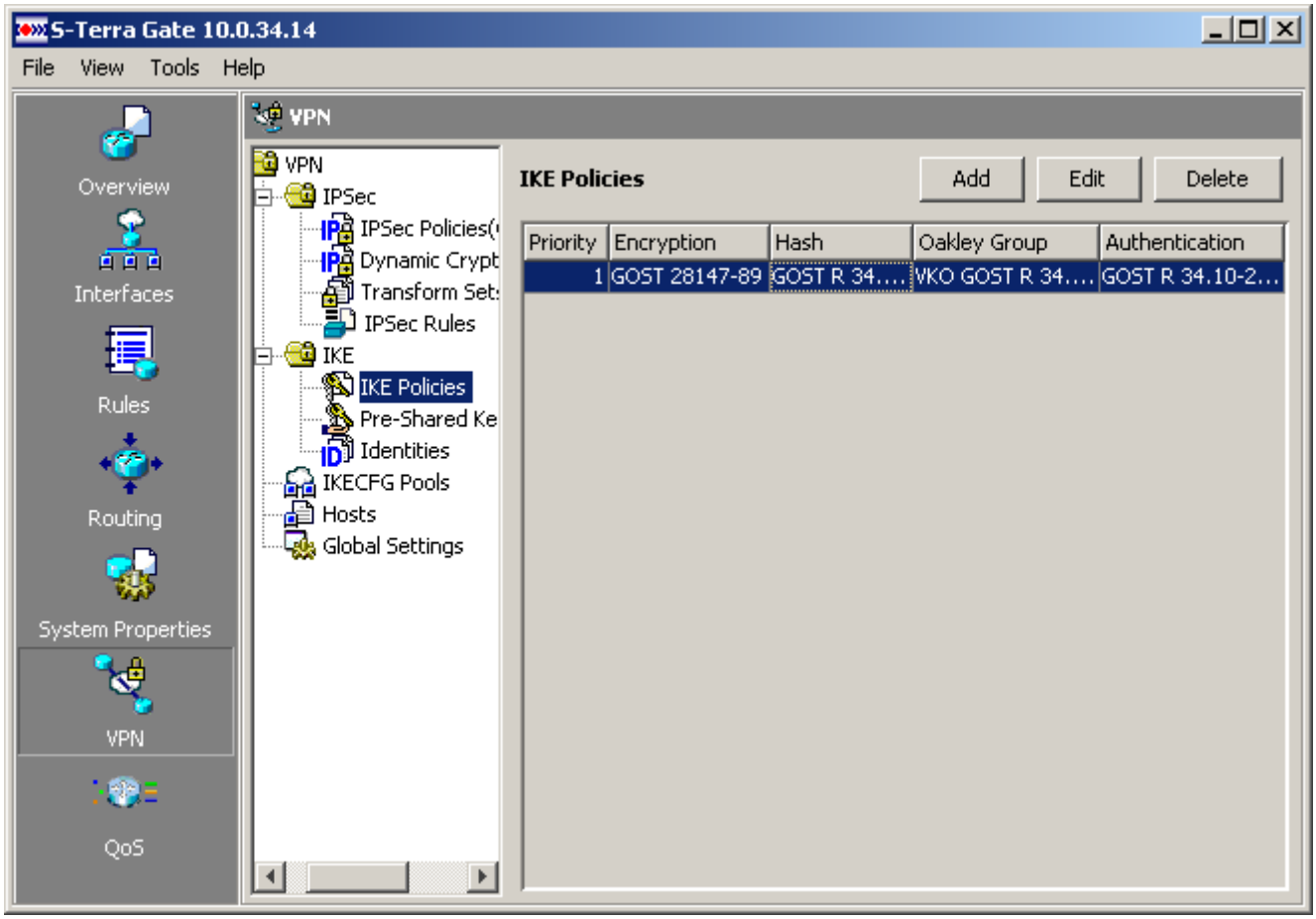

Рисунок 79

Создание IKE Policy

Нажатие кнопки Add в разделе *IKE Policies* открывает окно *Add IKE Policy* (Рисунок 80) 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:
  - *GOST R 34.10-2001 Signature* – аутентификация осуществляется с использованием цифровых сертификатов, созданных по алгоритму ГОСТ Р 34.10-2001.
  - *Pre-Shared Key* – аутентификация осуществляется с использованием предопределенных ключей.
  - *RSA Signature* – аутентификация осуществляется с использованием цифровых сертификатов, созданных по алгоритму RSA.

- *DSS Signature* – аутентификация осуществляется с использованием цифровых сертификатов, созданных по алгоритму DSA.
- *Signature selected by CA type* – выбор конкретного типа аутентификации (RSA, DSA или ГОСТ) осуществляется по типу CA-сертификата, лежащего в базе.

- *Encryption Algorithm* – выпадающий список алгоритмов шифрования сообщений:
  - *GOST 28147-89* – в качестве алгоритма шифрования используется алгоритм ГОСТ 28147-89.
  - *DES* – в качестве алгоритма шифрования используется алгоритм 56bit DES.
  - *3DES* – в качестве алгоритма шифрования используется 168-bit DES-CBC (3DES).
  - *AES 128* – в качестве алгоритма шифрования используется 128-bit AES.
  - *AES 192* – в качестве алгоритма шифрования используется 192-bit AES.
  - *AES 256* – в качестве алгоритма шифрования используется 256-bit AES.
- *Hash Algorithm* – выпадающий список алгоритмов хэширования сообщений:
  - *GOST R 34.11-94* – указывает, что в качестве хэш-алгоритма должен использоваться алгоритм ГОСТ Р 34.11-94 HMAC.
  - *GOST R 34.11-12 TC26 (256 bit keys)* – указывает, что в качестве хэш-алгоритма должен использоваться алгоритм ГОСТ Р 34.11-12 с длиной ключа 256 (применяется только при использовании криптобиблиотеки компании «С-Терра СиЭсПи»).
  - *GOST R 34.11-12 TC26 (512 bit keys)* – указывает, что в качестве хэш-алгоритма должен использоваться алгоритм ГОСТ Р 34.11-12 с длиной ключа 512 (применяется только при использовании криптобиблиотеки компании «С-Терра СиЭсПи»).
  - *SHA1* – указывает, что в качестве хэш-алгоритма дожен использоваться алгоритм SHA (HMAC вариант).
  - *MD5* – указывает, что в качестве хэш-алгоритма должен использоваться алгоритм MD5 (HMAC вариант).

  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 GOST R 34.10-2001* [RFC4357]:
  - *VKO GOST R 34.10-2001* – используется алгоритм VKO GOST R 34.10-2001.
  - *VKO GOST R 34.10-2012* – используется алгоритм VKO GOST R 34.10-2012 (256 бит). Алгоритм VKO GOST R 34.10-2012 может применяться, только если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи».
  - *D-H Group 1 (768-bit modp)* – используется алгоритм Диффи-Хеллмана, длина ключа 768 бит.
  - *D-H Group 2 (1024-bit modp)* – используется алгоритм Диффи-Хеллмана, длина ключа 1024 бит.
  - *D-H Group 5 (1536-bit modp)* – используется алгоритм Диффи-Хеллмана, длина ключа 1536 бит.
- *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.

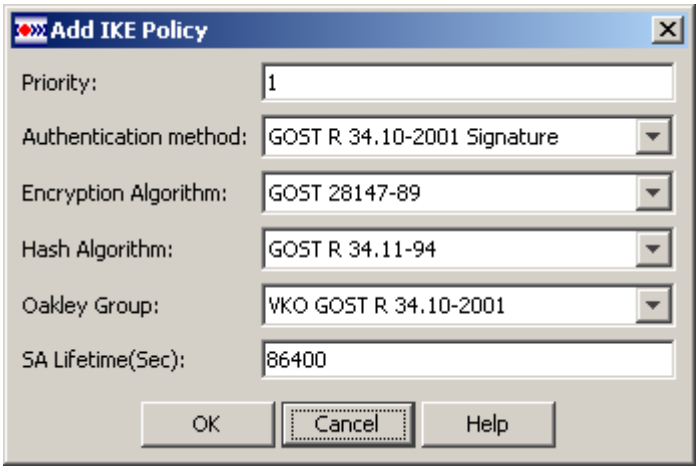

Рисунок 80

Редактирование IKE Policy

Редактирование параметров выделенной в таблице политики IKE производится в окне *Edit IKE Policy*, которое вызывается кнопкой 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 предопределенный ключ, то ключ следует создавать в этом разделе. Для каждого партнера согласовывается отдельный предопределенный ключ. В данном разделе можно создавать, редактировать и удалять предопределенные ключи для разных партнеров.

Главная форма этого раздела (Рисунок 81) содержит одну таблицу с зарегистрированными предопределенными 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 предопределенном ключе.

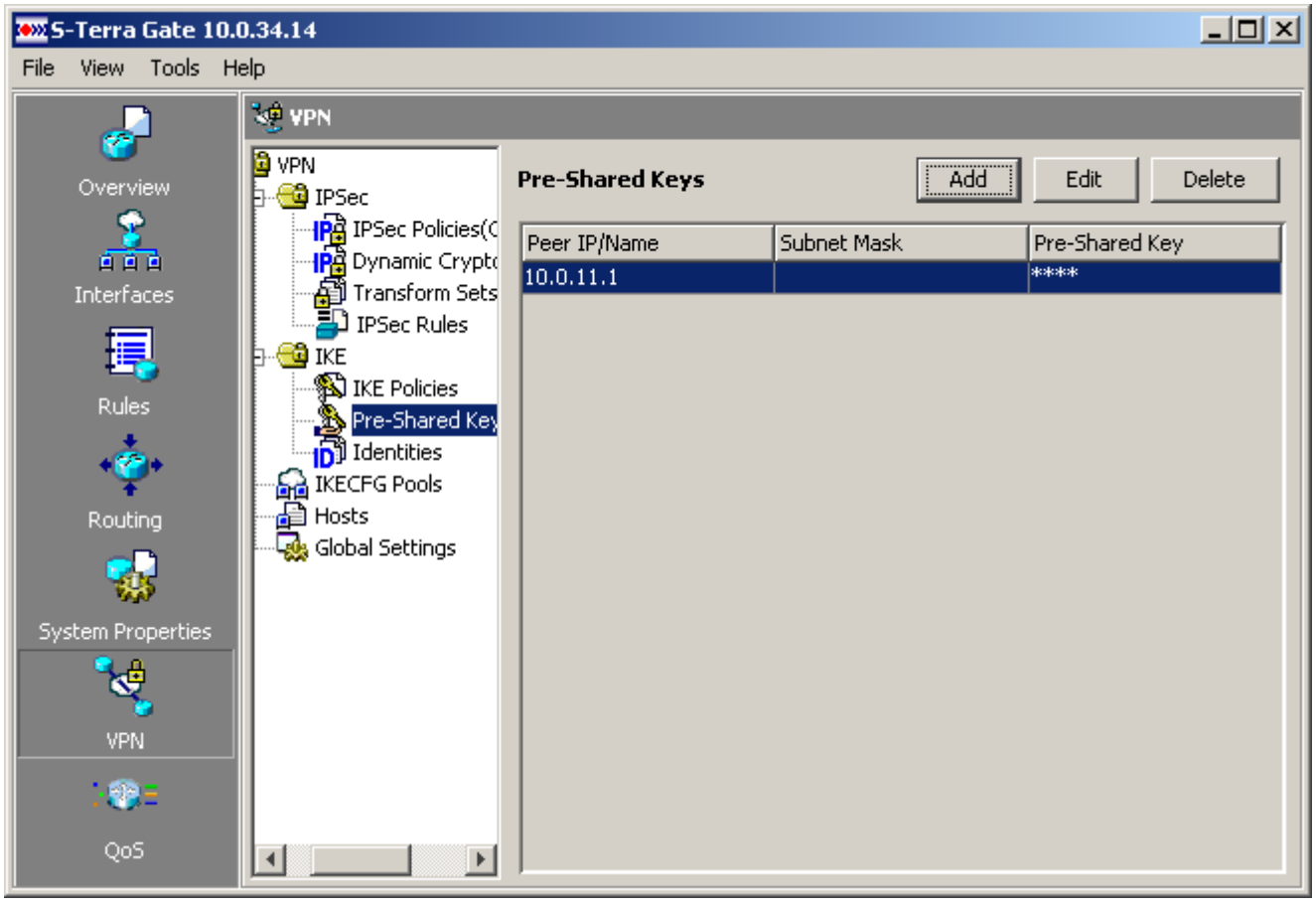

Рисунок 81

Создание Pre-Shared Key

Создание предопределенного ключа производится в окне *Add Pre-Shared Key* (Рисунок 82), которое открывается по нажатию кнопки Add в разделе *Pre-Shared Keys*:

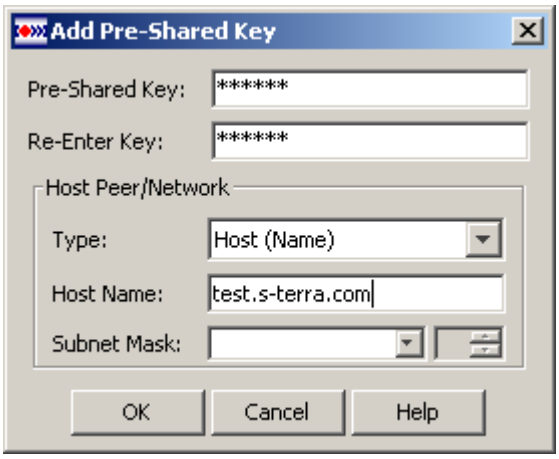

Рисунок 82

Состав элементов окна:

- *Pre-Shared Key* – поле ввода предопределенного ключа. Ключ может содержать только цифры и буквы латинского алфавита, а также символы: `!"#$%&'()*+,-./;:>=<@[\]^_`{|}~?`. Пробелы не допускаются.
- *Re-Enter Key* – поле повторного ввода предопределенного ключа. Значение ключа в обоих полях должны совпадать.
- Группа *Host Peer /Network* задает партнера, при соединении с которым используется данный предопределенный ключ.
  - *Type* – выбор типа идентификатора IKE. Возможны три значения:
    - *Network* – задает идентификацию IKE по IP-адресу и маске подсети партнера.
    - *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.
    - *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 используется несколько интерфейсов или IP-адрес интерфейса партнера неизвестен.
      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.

Редактирование Pre-Shared Key

Редактирование выделенного в таблице (Рисунок 81) предопределенного ключа производится в окне *Edit Pre-Shared Key* (Рисунок 83), которое вызывается кнопкой Edit. Окно полностью совпадает с окном создания Pre-Shared Key.

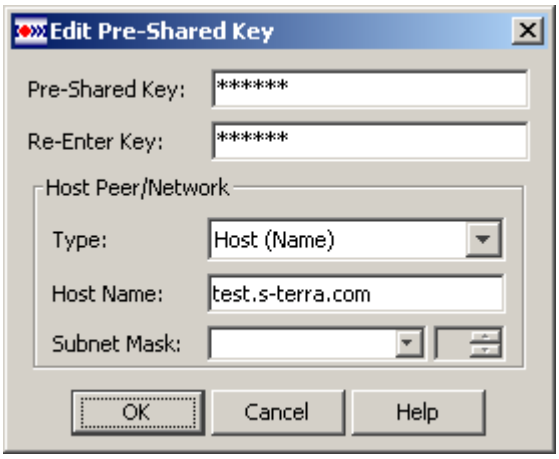

Рисунок 83

Удаление Pre-Shared Key

Удаление выделенного в таблице (Рисунок 81) предопределенного ключа 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 69).

В разделе *Identities* (Рисунок 84) можно просматривать списки созданных идентификаторов, вызывать окна для создания и редактирования, а также удалять списки идентификаторов.

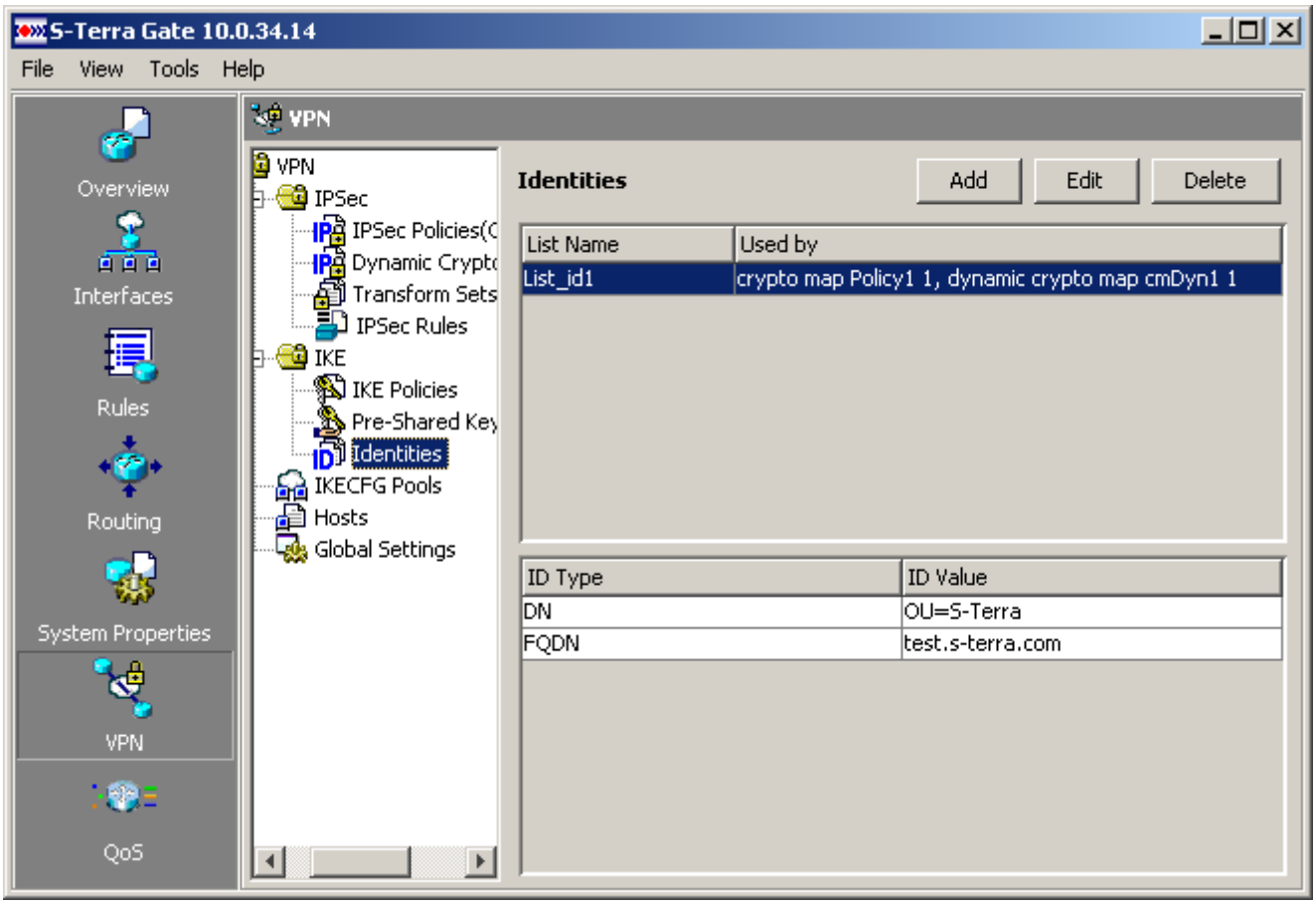

Рисунок 84

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 85), которое вызывается кнопкой Add из раздела *Identities*.

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.

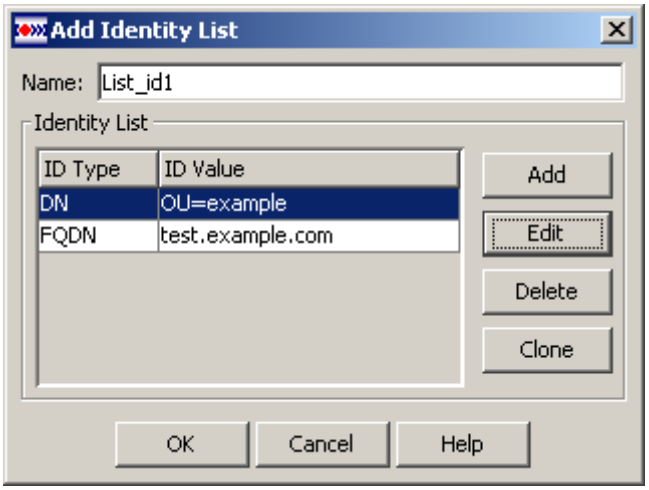

Рисунок 85

Создание нового идентификатора в списке

Создание нового идентификатора в списке производится в окне *Add Identity* (Рисунок 86), которое вызывается кнопкой Add в окне создания списка:

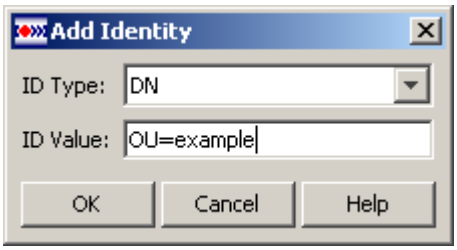

Рисунок 86

Окно содержит два поля: *ID Type* – для выбора типа идентификатора (*DN* или *FQDN*), *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 – streetAddress;
  - 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.

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 85), 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 в окне *Add/Edit Identity List*. Если нет выделенной строки – кнопка *Edit* блокируется. Нажатие кнопки Edit открывает окно редактирования, в котором поле ID Value заполнено значением выделенной строки (Рисунок 87).

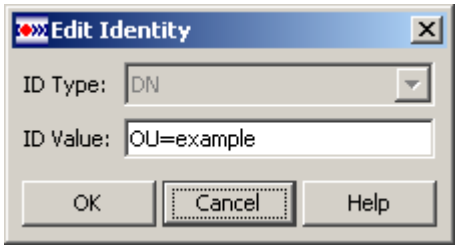

Рисунок 87

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 в разделе *Identities.* Кнопка активна только при выделении строки в верхней таблице. Редактирование списка производится также как и создание списка.

Удаление списка идентификаторов

Удаление списка идентификаторов производится с помощью кнопки Delete в разделе *Identities.* Кнопка активна только при выделении строки в верхней таблице. Нажатие кнопки Delete вызывает проверку связи 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*>.

IKECFG Pools

В разделе *IKECFG Pools* (Рисунок 88) просматриваются созданные пулы адресов, создаются новые, редактируются и удаляются существующие пулы. IKECFG 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 74) во вкладке *IKECFG pool* указать имя пула адресов. Для правильной работы соединений необходимо отредактировать таблицу маршрутизации.

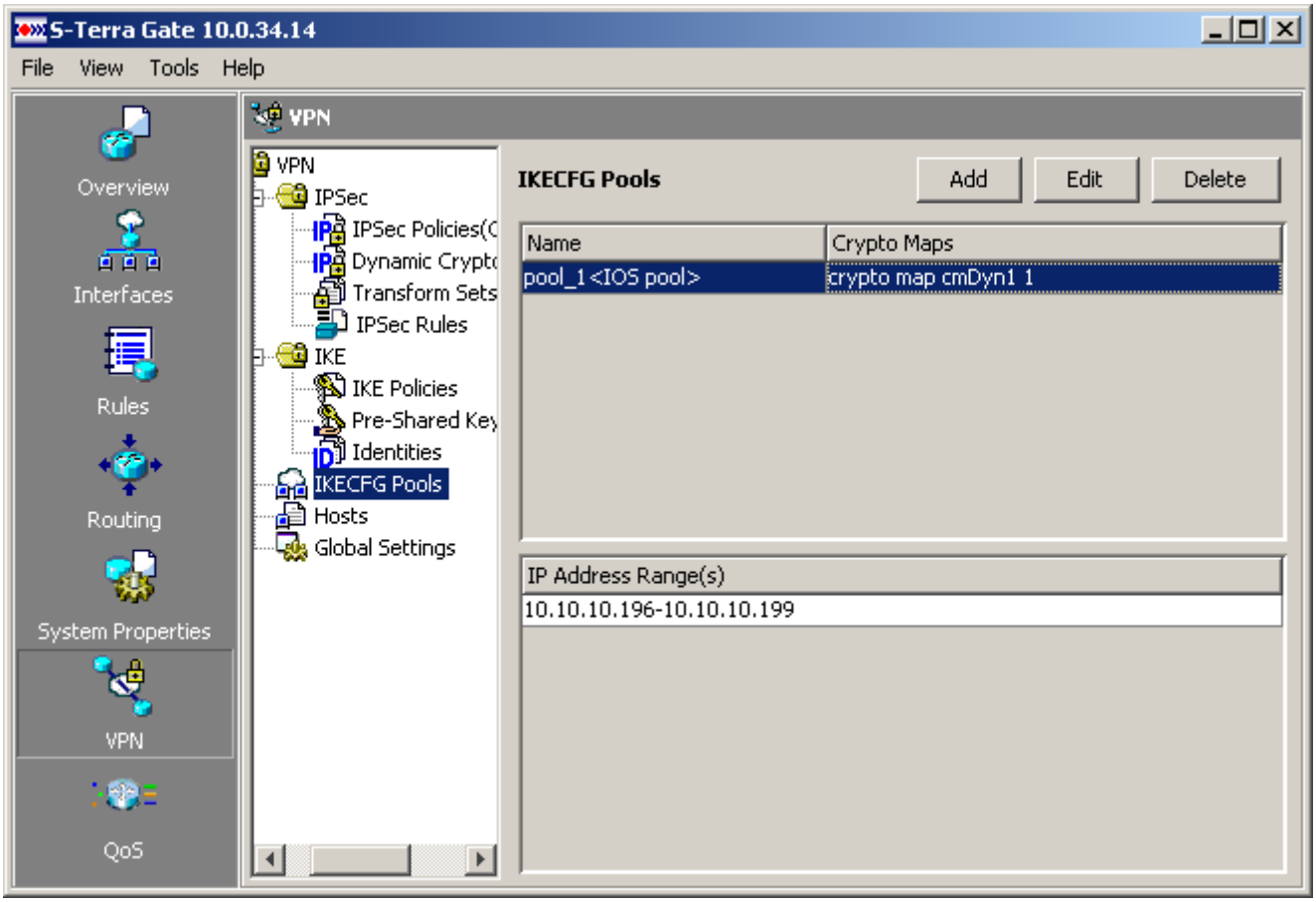

Рисунок 88

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 IKECFG Pool* (Рисунок 89), которое появляется при нажатии кнопки Add в разделе *IKECFG Pools*.

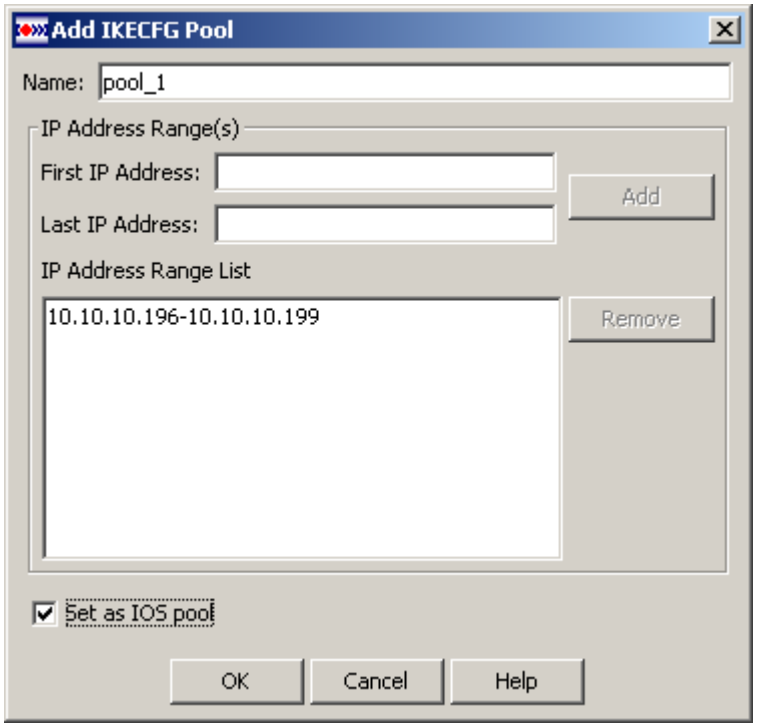

Рисунок 89

Состав элементов окна:

- *Name* – имя IKECFG 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 IKECFG пулов.
- *Set as IOS pool* – 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 pool, то в разделах Overview, VPN (VPN Connections), IPSec Policies у данного набора динамических криптокарт вместо значения <none> будет отображаться имя 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 IKECFG 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 IKECFG пула. При этом параметры записи задаются следующим образом:

Prefix, Prefix Mask	указывается диапазон адресов данного IKECFG пула
IP Address	задается адрес внешнего маршрутизатора, через который поступают пакеты клиентам.

Редактирование пула адресов

Редактирование выделенного в таблице раздела *IKECFG Pools* пула адресов производится в окне, аналогичном окну создания нового пула (Рисунок 89), 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 пула адресов

Удаление выделенного пула адресов в верхней таблице раздела *IKECFG Pools* (Рисунок 88) 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 90) содержит таблицу со столбцами:

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

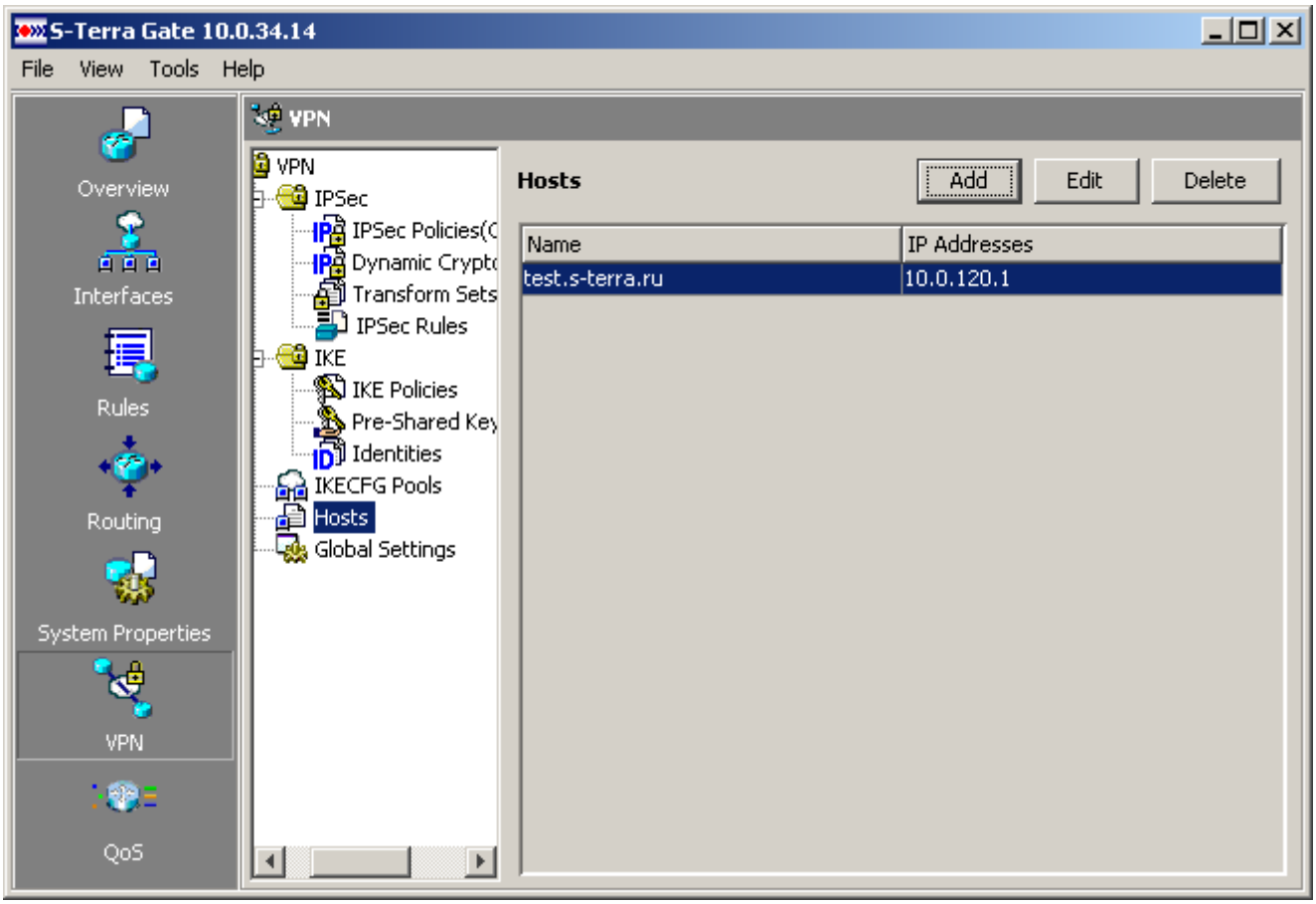

Рисунок 90

Создание новой записи для хоста

Создание новой записи производится в окне *Add Host* (Рисунок 91), которое вызывается кнопкой Add в разделе *Hosts*.

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).

- I*P 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.

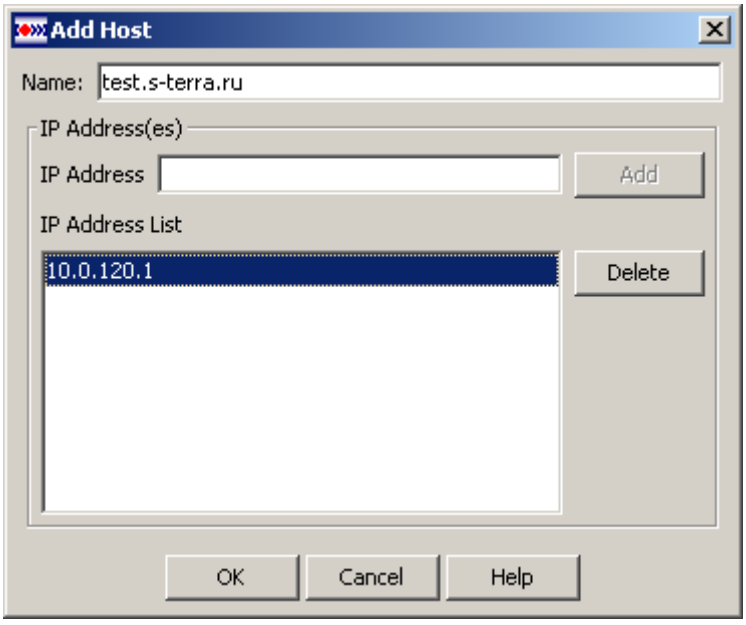

Рисунок 91

Редактирование данных хоста

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

Удаление хоста

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

Global Settings

В разделе *Global Settings* (Рисунок 92) просматриваются и редактируются глобальные параметры VPN для шлюза безопасности.

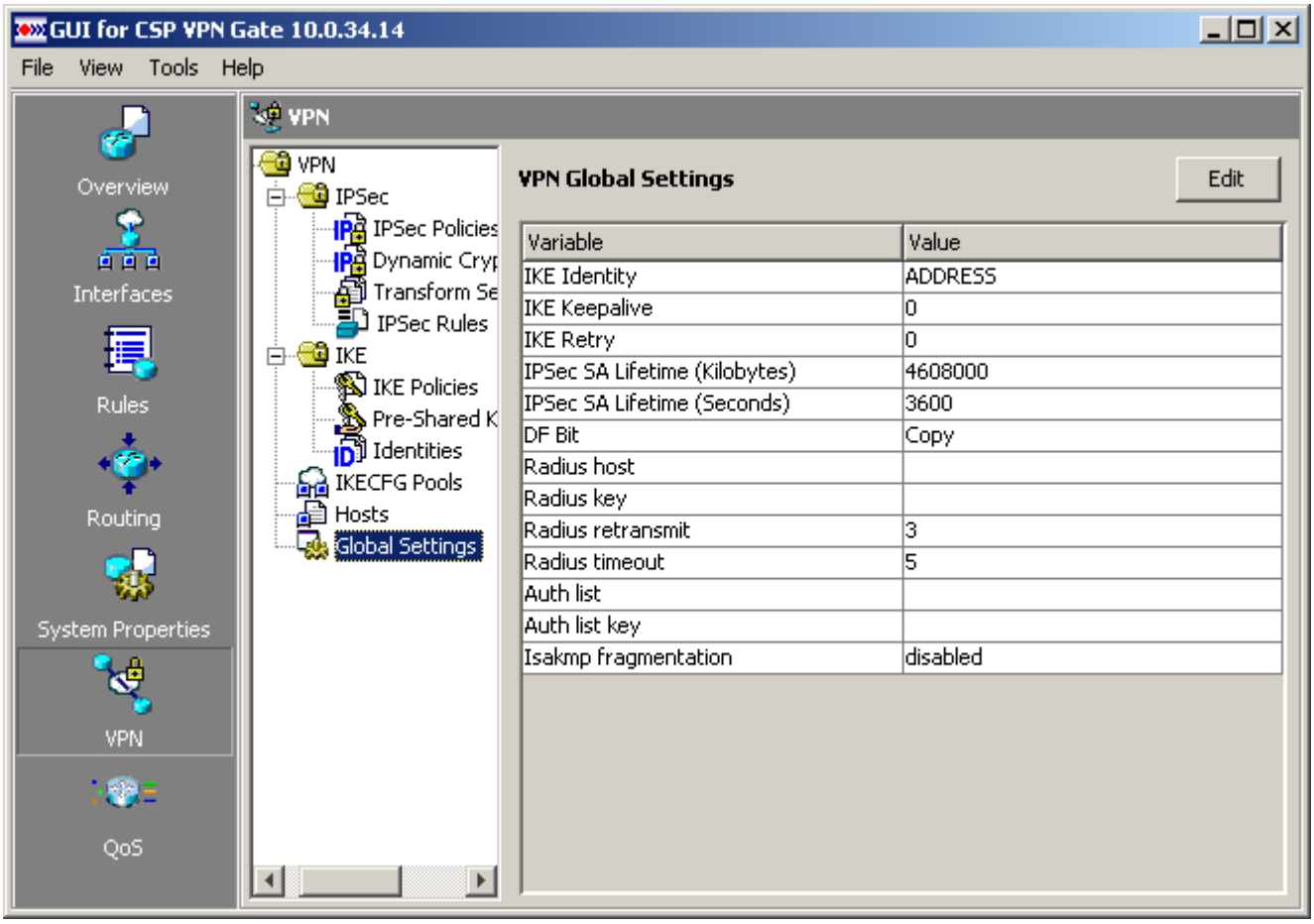

Рисунок 92

Состав элементов браузера раздела *Global Settings*:

- Кнопки управления:
  - Edit – кнопка вызова окна редактирования установленных параметров.
- Таблица *VPN Global Settings* состоит из столбцов *Variable* и *Value.*
  - *Variable* содержит следующие параметры:
    - *IKE Identity* –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 изменен 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*.
- *DF Bit* – установленное значение DF-бита для заголовка инкапсуляции в туннельном режиме.
- *Radius host* – адрес RADIUS-сервера.
- *Radius key* – пароль доступа к RADIUS-серверу.
- *Radius retransmit* – количество попыток перепосылок запроса к RADIUS-серверу.
- *Radius timeout* – время ожидания ответа от RADIUS-сервера.
- *Auth list* – имя списка аутентификации на RADIUS-сервере.
- *Auth list key* – неинтерактивный пароль пользователя (единый).
- *Isakmp fragmentation* – режим фрагментирования IKE-пакетов.

Редактирование глобальных параметров VPN

Нажатие кнопки Edit в разделе *Global Settings* открывает окно редактирования глобальных параметров *Edit VPN Global Settings* (Рисунок 93).

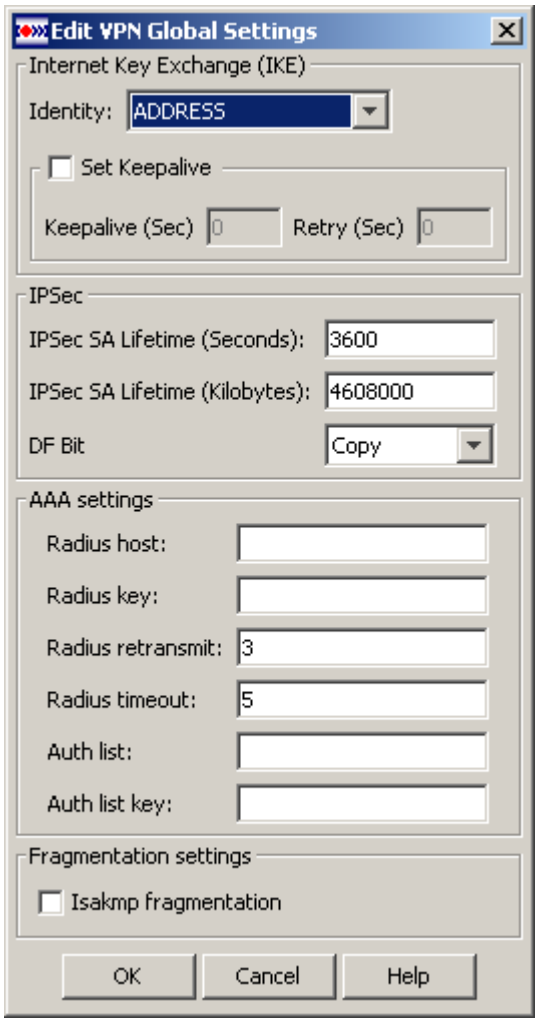

Рисунок 93

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 флажок сброшен.
  - *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.
  - DF Bit – установка DF-бита для заголовка инкапсуляции в туннельном режиме. Список значений:
    - *Copy* – DF-бит внешнего IP-заголовка устанавливается в то же значение, какое было у оригинального пакета. Значение по умолчанию.
    - *Clear* – DF-бит внешнего IP-заголовка будет очищен и шлюз может фрагментировать пакет после IPsec инкапсуляции.
    - *Set* – DF-бит внешнего IP-заголовка будет установлен, фрагментация пакета будет запрещена.
- Группа *AAA settings*:
  - *Radius host* – IP-адрес RADIUS-сервера.
  - *Radius key* – пароль доступа к RADIUS-серверу (предопределенный ключ, представляющий собой строку произвольной комбинации буквенно-цифровых символов).
  - *Radius retransmit* – количество попыток перепосылок запроса к RADIUS-серверу, это число не включает первый запрос к серверу. Значение в диапазоне 0-9, по умолчанию – 3.
  - *Radius timeout* – время ожидания ответа от RADIUS-сервера. Значение в диапазоне 1-1000, по умолчанию – 5.
  - *Auth list* – имя списка аутентификации на RADIUS-сервере.
  - *Auth list key* – неинтерактивный пароль пользователя (единый).
- Группа *Fragmentation settings*:

- *Isakmp fragmentation* – выставленный флажок включает режим фрагментирования IKE-пакетов (максимальный размер пакета устанавливается равным 576 байт). По умолчанию флажок сброшен.

Quality of Service

В разделе *QoS* (Рисунок 94) можно задать необходимый сервис обслуживания сетевого трафика, основанный на классификации трафика и его маркировке. Раздел содержит две вкладки *Class Maps* и *Policy Maps*. Во вкладке *Class Maps* производится задание классов и критериев этих классов, на основании которых сетевой трафик будет группироваться в классы (классифицироваться). Во вкладке *Policy Maps* задается маркировка пакетов, принадлежащих разным классам – редактируется поле ToS заголовка пакета.

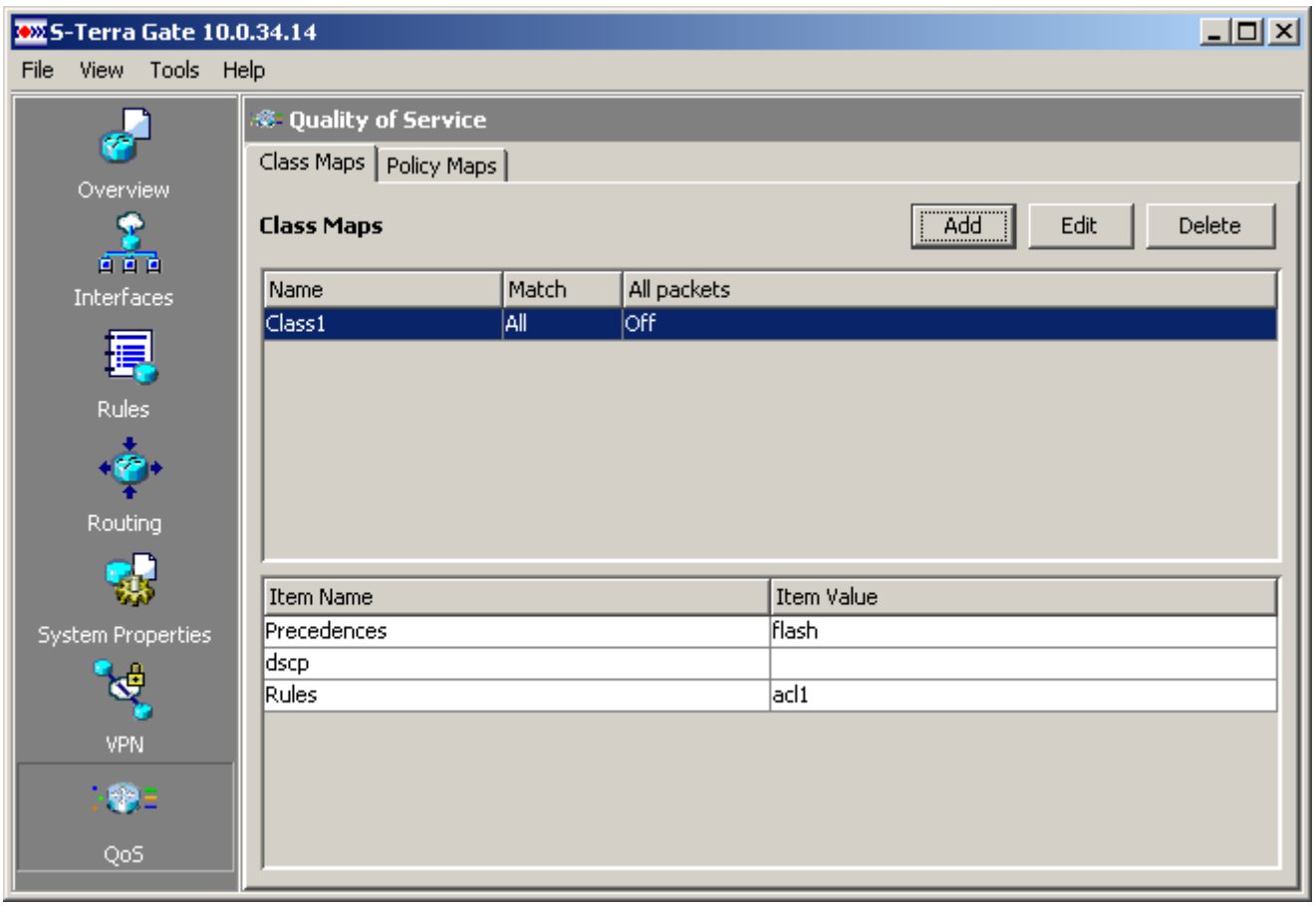

Рисунок 94

Class Maps

Во вкладке *Class Maps* можно задать разные классы трафика и критерии для каждого класса, на основе которых трафик будет группироваться в классы. Вкладка *Class Maps* состоит из двух таблиц и кнопок управления (Рисунок 94).

Верхняя таблица показывает созданные классы для трафика:

- *Name* – имя класса трафика.
- *Match* – параметр отбора пакетов, принимает одно из значений:
  - *Any* – это значение показывает, что классу будут принадлежать пакеты, которые удовлетворяют хотя бы одному заданному критерию.

    - *All* – показывает, что классу будут принадлежать пакеты, которые удовлетворяют всем заданным критериям.
- *All packets* – один из критериев отбора пакетов, принимает одно из значений:
    - *On* – это значение показывает, что задан критерий (задается установкой флажка *Establish matching for all packets* в окне *Add Class Map*), означающий, что все пакеты будут принадлежать данному классу.
    - *Off* – показывает, что этот критерий не задан.

Нижняя таблица отображает критерии отбора класса, выбранного в верхней таблице:

- *Precedences* – список значений Precedence (приоритет), использующихся для указания желаемого качества доставки пакета.
- *dscp* – список значений DSCP (Differentiated Services Code Point), задающих приоритет и тип обслуживания пакета.
- *Rules* – список правил доступа, под действие которых должен попадать пакет.

Кнопки управления:

- Add – кнопка вызова окна для задания нового класса трафика.
- Edit – кнопка вызова окна для редактирования существующего класса трафика.
- Delete – кнопка удаления выделенного класса.

Создание Class Map

Создание класса трафика осуществляется в окне *Add Class Map* (Рисунок 95), которое вызывается нажатием кнопки Add во вкладке *Class Maps*. Здесь задается имя нового класса, указываются критерии этого класса и условие соответствия критериям.

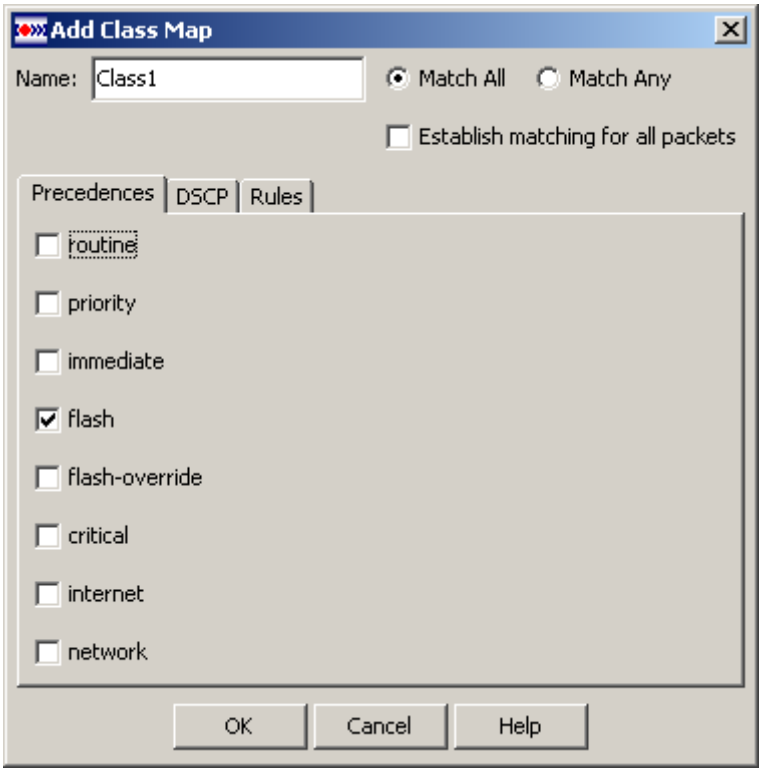

Рисунок 95

Состав элементов окна *Add Class Map*:

- *Name* – поле ввода имени класса трафика. Имя должно быть уникальным и начинаться с буквы. В имени используются только латинские буквы, цифры и символы: `!"#$%&'()*+,-./;:<=>@[\]^_`{|}~` и не допускаются пробелы.
- Переключатели:
  - *Match All* – установка переключателя означает, что классу будут принадлежать только те пакеты, которые одновременно удовлетворяют всем заданным критериям (во вкладках *Precedences*, *DSCP*, *Rules* и флажку *Establish matching for all packets*) (пересечение критериев).
  - *Match Any* – установка переключателя означает, что классу будут принадлежать те пакеты, которые удовлетворяют хотя бы одному заданному критерию (во вкладках *Precedences*, *DSCP*, *Rules* и флажку *Establish matching for all packets*) (объединение критериев).
- *Establish matching for all packets* – установка этого флажка означает, что все пакеты должны принадлежать данному классу.
- Вкладки: *Precedences*, *DSCP*, *Rules.*

Вкладка Precedences

Во вкладке *Precedence* (Рисунок 95) задаются значения Precedence (приоритет), на основе которых будет определяться принадлежность пакета к заданному классу. Значение Precedence задает желаемое качество доставки пакета путем назначения общего приоритета IP-пакету, который показывает уровень важности передаваемых данных.

Пакеты, у которых в IP-заголовке в поле типа сервиса ToS указаны заданные значения Precedence будут принадлежать к данному классу.

В этой вкладке можно установить следующие флаги, которые задают приоритет для каждого пакета и уровень важности передаваемых данных:

- *routine* – обычный пакет (0)
- *priority* – приоритетный пакет (1)
- *immediate* – немедленный пакет (2)
- *flash* – срочный пакет (3)
- *flash-override* – экстренный пакет (4)
- *critical* – критический пакет (5)
- *internet* – пакет межсетевого управления (6)
- *network* – пакет управляющей информации (7).

Чем больше номер, указанный в скобках, тем выше приоритет пакета.

Вкладка DSCP

Во вкладке *DSCP* (Рисунок 96) задаются значения DSCP (Differentiated Services Code Point), на основе которых будет определяться принадлежность пакета к заданному классу. Значение DSCP задает приоритет и тип обслуживания пакета. Пакеты, у которых в IP-заголовке в поле типа сервиса ToS указаны заданные значения DSCP, будут принадлежать данному классу.

Дифференцированное обслуживание не гарантирует определенный уровень сервиса, а стремится упорядочить весь трафик по классам таким образом, чтобы каждый класс получил лучший или худший уровень обслуживания по отношению к остальным.

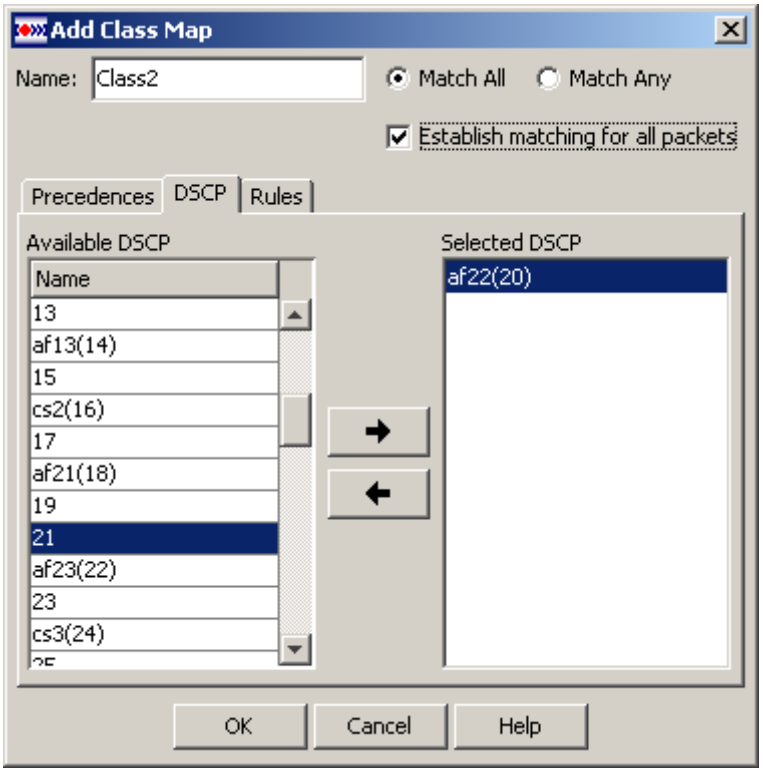

Рисунок 96

Вкладка содержит два поля:

- *Available DSCP* – поле со списком доступных значений DSCP. При перемещении значения DSCP из списка *Available DSCP* в список *Selected DSCP*, оно удаляется из списка *Available DSCP*.
- *Selected DSCP* – поле со списком выбранных значений DSCP, которые будут использоваться для отбора пакетов.

Кнопки управления:

- – кнопка перемещения выделенного значения DSCP в списке *Available DSCP* в список *Selected DSCP.*
- – кнопка перемещения выделенного значения DSCP из списка *Selected DSCP* в список *Available DSCP.*

Значения DSCP могут быть выражены в цифровой форме или с использованием специальных ключевых слов, называемых поведением сетевых участков (PHB – Per-Hop Behavior). Определено три класса DSCP маркировки:

- по возможности (BE – best effort или DSCP 0)
- гарантированная доставка (AF – Assured Forwarding)
- срочная доставка (EF – Express Forwarding)

В дополнение к этим трем определенным классам существуют коды селектора классов (CS1-CS7), которые идентичны значениям IP precedence (1-7).

Определено четыре класса гарантированной доставки, они начинаются с AF и далее две цифры. Первая цифра определяет AF класс и принимает значения от 1 (низкий приоритет обработки) до 4 (высокий приоритет обработки пакета). Вторая цифра определяет уровень вероятности сброса пакета в пределах каждого класса и принимает значения от 1

(минимальная вероятность сброса) до 3 (максимальная вероятность сброса). Значения DSCP могут быть выражены в десятичном формате или с использованием ключевых слов.

Код селектора классов (CS)	Описание		PHB-политика
CS7	Stays the same (link layer and routing protocol keep alive)		
CS6	Stays the same (used for IP routing protocols)		
CS5	Express Forwarding (EF)		PHB-политика немедленной передачи пакетов, срочная доставка. Рекомендуется для голосового трафика
CS4	Class 4	Assured Forwarding (AF)	PHB-политика гарантированной доставки пакетов. Используется для видеотрафика. Для видеоконференций рекомендуется значение DSCP AF41. Подробнее см. нижеследующую таблицу
CS3	Class 3		
CS2	Class 2		
CS1	Class 1		
DSCP 0	Best Effort (BE) – default		PHB-политика негарантированной доставки пакетов, доставка по возможности. Рекомендуется для трафика данных – передача файлов, приложения электронной почты, HTTP и др.

Классы гарантированной доставки пакетов

Приоритет отбрасывания пакета	Class 1	Class 2	Class 3	Class 4
Низкий	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Средний	001100 AF12 DSCP 12	010100 AF22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Высокий	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Вкладка Rules

Во вкладке Rules (Рисунок 97) задаются правила доступа и пакеты, разрешенные по этим правилам, будут принадлежать данному классу.

Вкладка содержит два поля:

- *Available Rules* – это список правил доступа. При перемещении правила из списка *Available Rules* в список *Selected Rules*, оно удаляется из списка *Available Rules*.
- *Selected Rules* – поле со списком выбранных правил доступа, которые будут использоваться для отбора пакетов.

Кнопки управления:

-  – кнопка перемещения выделенного правила доступа в списке *Available Rules* в список *Selected Rules.*
-  – кнопка перемещения правила доступа из списка *Selected Rules* в список *Available Rules.*
-  – кнопка перемещения выделенной записи в списке *Selected Rules* на одну позицию вверх для увеличения приоритета. Если выделенной строкой является первая, то кнопка будет блокирована.
-  – нопка перемещения выделенной записи в списке *Selected Rules* на одну позицию вниз для снижения приоритета. Если выделенной строкой является последняя, то кнопка будет блокирована.
- Add – вызывает окно *Add a Rule*, позволяющее создать новое правило доступа. Вызываемое окно аналогично окну, изображенному на Рисунок 16, за исключением кнопки Associate.
- Edit – вызывает окно *Edit a Rule*, позволяющее отредактировать выделенное правило доступа. Вызываемое окно аналогично окну *Add a Rule*.

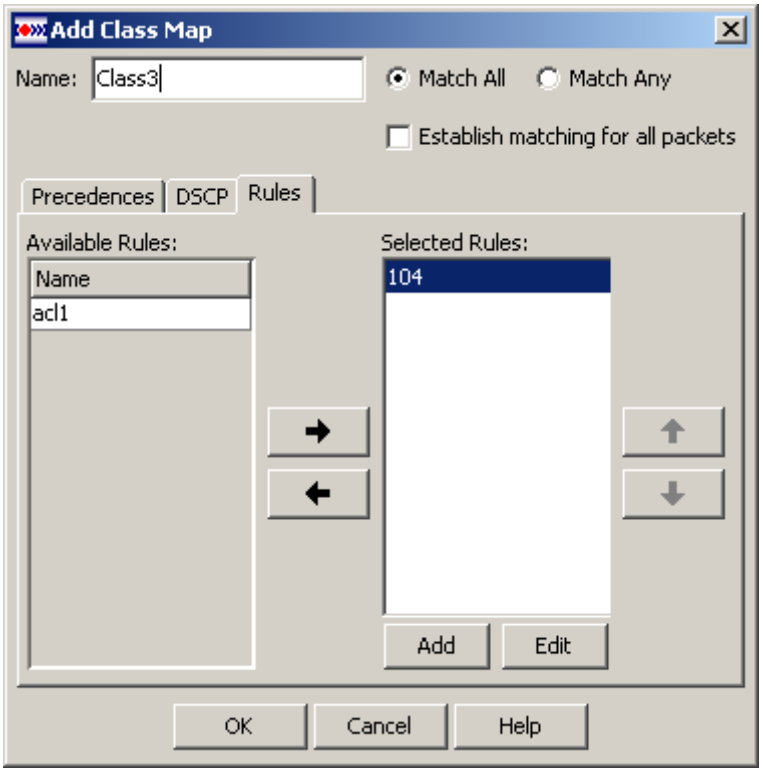

Рисунок 97

Редактирование Class Map

Редактирование class-map осуществляется в окне *Edit Class Map*, которое вызывается кнопкой Edit во вкладке *Class Maps* раздела *Quality of Service*. Состав элементов окна аналогичен описанному выше окну создания class-map, за исключением – поле *Name* недоступно для редактирования.

Policy Maps

Во вкладке *Policy Maps* задается политика работы с классами трафика. Для каждого класса можно установить значения DSCP или Precedence, в сответствии с которыми будут маркироваться пакеты, принадлежащие этому классу. Установленные значения Precedence и DSCP определяют набор процедур, которые будут обеспечивать заданный класс обслуживания трафика. Заданный класс обслуживания осуществляется с помощью утилиты `drv_mgr`, позволяющей управлять загрузкой процессора по обработке трафика – включать/выключать механизм уничтожения неприоритетных пакетов (по полю ToS), управлять стратегией очередей, включать/выключать механизм защиты от перегрузки и др.

При IPsec обработке исходящего пакета классификация и маркирование пакета будет производиться до его инкапсуляции, для входящего пакета – после его декапсуляции.

При IPsec обработке пакетов будет происходить копирование поля ToS из внутреннего заголовка во внешний заголовок.

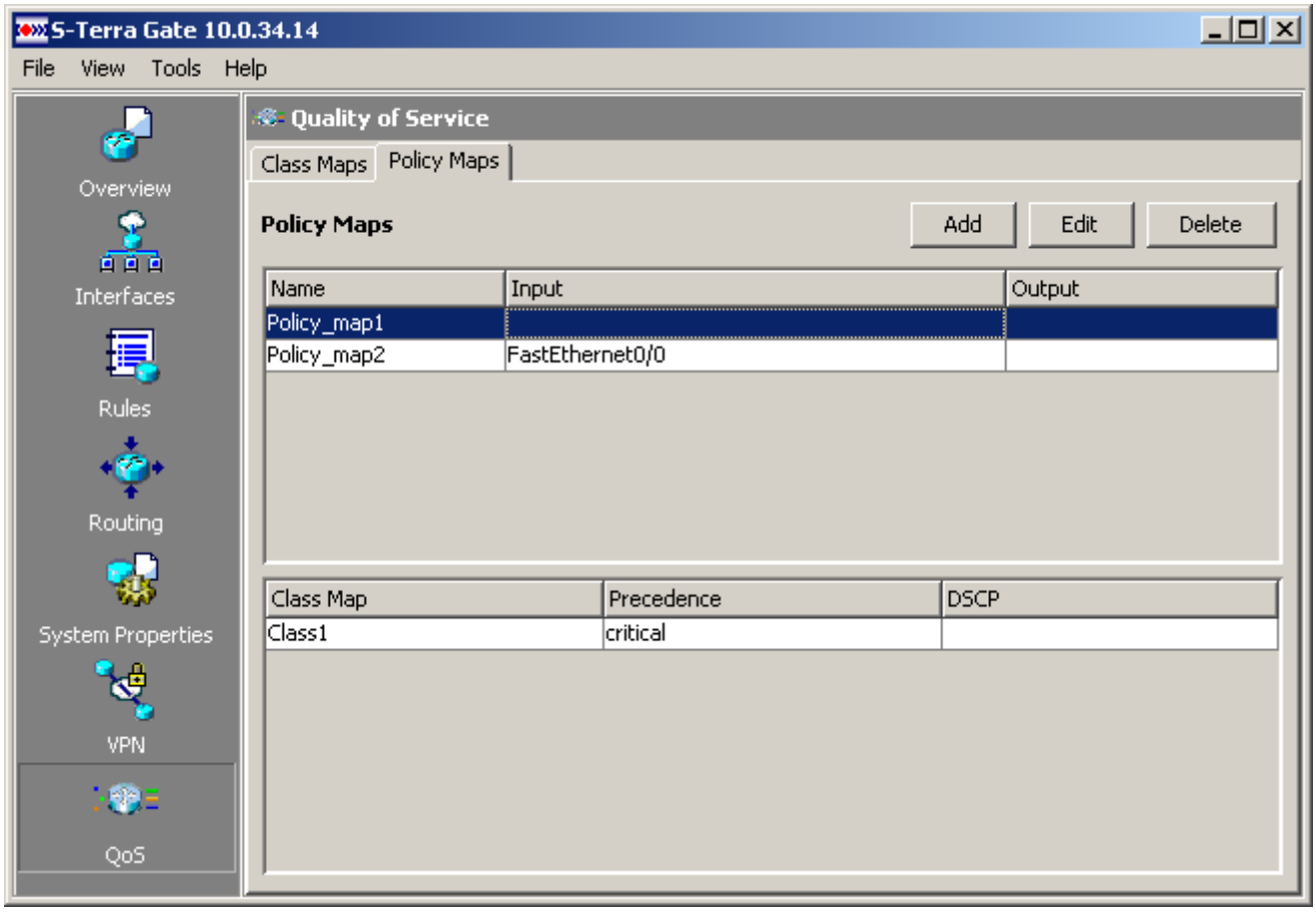

Рисунок 98

Верхняя таблица содержит следующие столбцы:

- *Name* – имя политики работы с классами.
- *Input* – имя интерфейса, на котором данная Policy Map будет применяться к входящему трафику.
- *Output*– имя интерфейса, на котором данная Policy Map будет применяться к исходящему трафику.

Нижняя таблица отображает классы трафика и параметры маркирования, относящиеся к Policy Map, выбранной в верхней таблице:

- *Class Map* – имя класса, к которому будет применяться заданная политика.
- *Presedence* – установленное значение Precedence для данного класса, которым будут маркироваться пакеты.
- *DSCP* – установленное значение DSCP для данного класса, которым будут маркироваться пакеты.

Кнопки управления:

- Add – кнопка вызова окна для создания политики работы с классами.
- Edit – кнопка вызова окна для редактирования политики работы с классами.
- Delete – кнопка удаления выбранной политики работы с классами.

Создание Policy Map

Создание политики работы с классами трафика осуществляется в окне *Add Policy Map* (Рисунок 99).

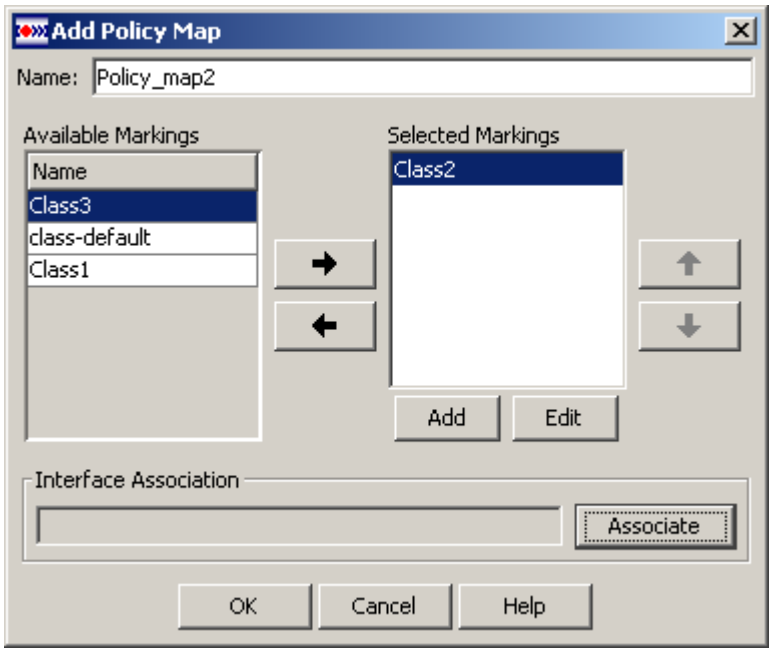

Рисунок 99

Состав элементов окна *Add Policy Map*:

- *Name* – поле ввода имени Policy Map. Имя должно быть уникальным и начинаться с буквы. В имени используются только латинские буквы, цифры и символы: `!"#$%&'()*+,-./:<=>@[\]^_`{|}~`, пробелы не допускаются.
- *Available Markings* – поле со списком созданных классов трафика. При перемещении класса в список *Selected Marking* он удаляется из списка *Available Markings*.
- *Selected Markings* – поле со списком выбранных классов. Для каждого выбранного класса можно будет задать значение DSCP или Precedence, в соответствии с которым трафик будет маркироваться. Этот список не должен быть пустым.

Кнопки управления:

-  – кнопка перемещения выделенного классв в списке *Available Markings* в список *Selected Markings.*
-  – кнопка перемещения класса из списка *Selected Markings* в список *Available Markings.*
-  – кнопка перемещения выделенной записи в списке *Selected Markings* на одну позицию вверх для увеличения приоритета. Если выделенной строкой является первая, то кнопка будет блокирована.
-  – нопка перемещения выделенной записи в списке *Selected Markings* на одну позицию вниз для снижения приоритета. Если выделенной строкой является последняя, то кнопка будет блокирована.

- Add – вызывает окно *Add Class Map* (Рисунок 97), в котором можно создать новый класс.
- Edit – вызывает окно *Edit Marking*, в котором можно для выбранного класса задать значения, в соответствии с которыми будет маркироваться пакеты (Рисунок 100).
- Associate – вызывает диалоговое окно *Associate with an Interface* (Рисунок 101), позволяющее связать Policy Map с интерфейсом.

Маркирование трафика

Окно *Edit Marking* (Рисунок 100) вызывается нажатием кнопки Edit в окне *Add Policy Map*. В окне *Edit Marking* устанавливаются значения DSCP или Precedence, в соответствии с которыми будут маркироваться пакеты, принадлежащие к выбранному классу.

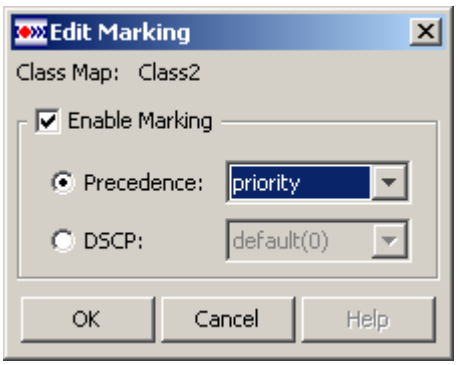

Рисунок 100

Состав элементов окна *Edit Marking*:

- *Enable Marking* – установка флага позволяет задать параметры маркирования трафика, принадлежащего данному классу. Если флаг не установлен, то маркирование трафика не производится.
- Переключатель с двумя положениями, позволяющий выброть одно из значений *Precedence* или *DSCP*, на которое будет изменено значение поля ToS заголовка пакета:
  - *Precedence* – при установке переключателя в это положение, станет доступен выпадающий список значений Precedence (приоритет, показывающий уровень важности передаваемых данных).

- *DSCP* – при установке переключателя в это положение, станет доступен выпадающий список значений DSCP (приоритет и уровень обслуживания трафика).

Выбор интерфейса

Окно *Associate with an Interface* (Рисунок 101) вызывается нажатием кнопки Associate в окне *Add Policy-Map*. Здесь можно привязать политику работы с классами к интерфейсу. На каждом интерфейсе можно задать независимую классификацию и маркирование для входящего и исходящего трафика.

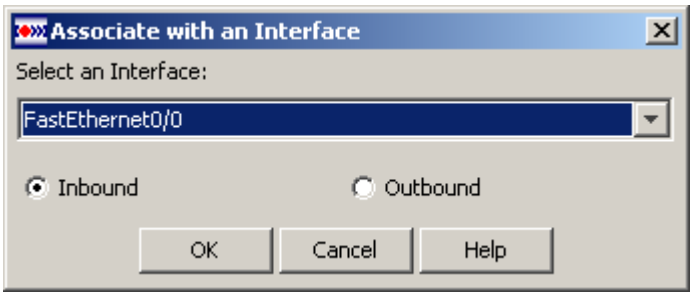

Рисунок 101

Состав элементов окна *Associate with an Interface*:

- *Select an Interface* – поле с выпадающим списком интерфейсов, из которого выберите интерфейс, к которому будет привязываться данная Policy Map. Содержит выпадающий список интерфейсов:
  - *none* – значение по умолчанию. При выборе этого значения политика не будет привязана к интерфейсу. Классификация и маркировка трафика (заданная этой Policy Map) производиться не будет.
- Переключатель с двумя положениями:
  - *Inbound* – при установке переключателя в это положение, классификация и маркирование трафика (в соответствии с созданными Class Map и Policy Map) будет применяться для входящего трафика на выбранном интерфейсе.
  - *Outbound* – при установке переключателя в это положение, классификация и маркирование трафика (в соответствии с созданными Class Map и Policy Map) будет применяться для исходящего трафика на выбранном интерфейсе.

Редактирование Policy Map

Редактирование Policy Map осуществляется в окне *Edit Policy Map*, которое вызывается кнопкой Edit во вкладке *Policy Maps* раздела *Quality of Service*. Состав элементов окна аналогичен описанному выше окну создания policy-map, за исключением:

- поле *Name* недоступно для редактирования;
- поле *Interface Association* недоступно и показывает присоединенный интерфейс, с указанием направления связи, если он был выбран;
- кнопка Associate отсутствует.

Окно Ping

Окно *Ping* (Рисунок 102) 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.

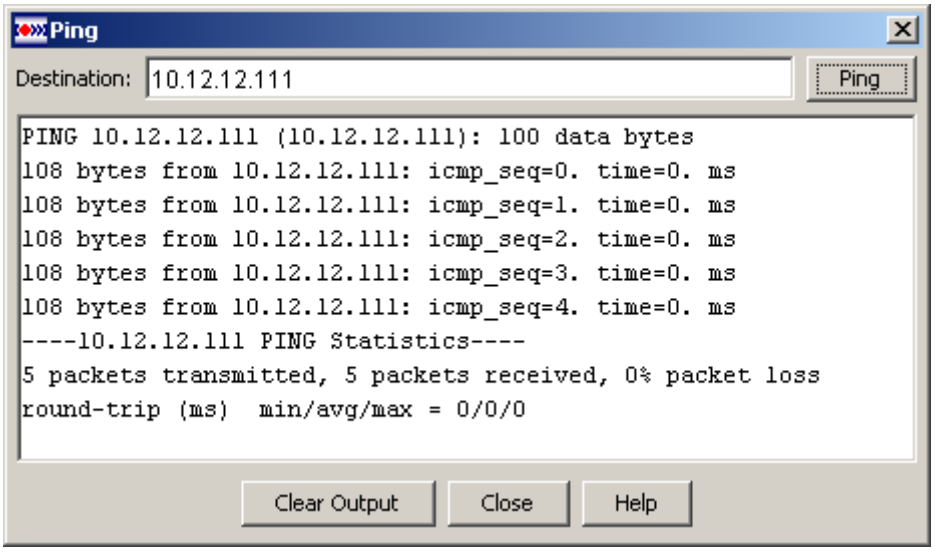

Рисунок 102

Окно SA Manager

Окно *SA Manager* (Рисунок 103) 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.

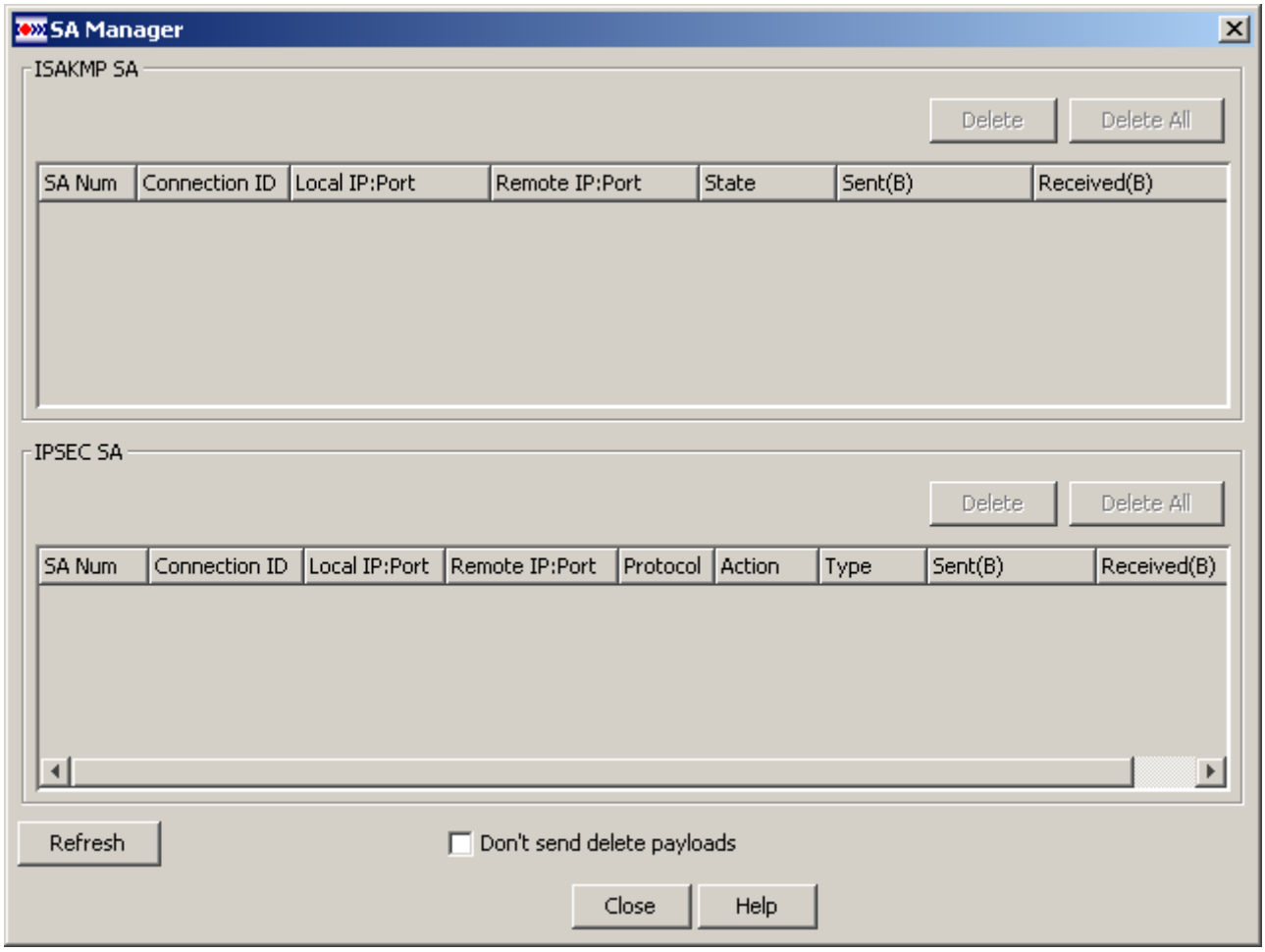

Рисунок 103

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;
- *Local IP:Port* – IP-адрес и порт локальной точки соединения (если номер порта не указан, то выдается *);

- *Remote IP: Port* – IP-адрес и порт удаленной 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;
- *Local IP:Port* – IP-адрес и порт локальной точки соединения (если номер порта не указан, то выдается *);
- *Remote IP:Port* – IP-адрес и порт удаленной 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 104). 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.

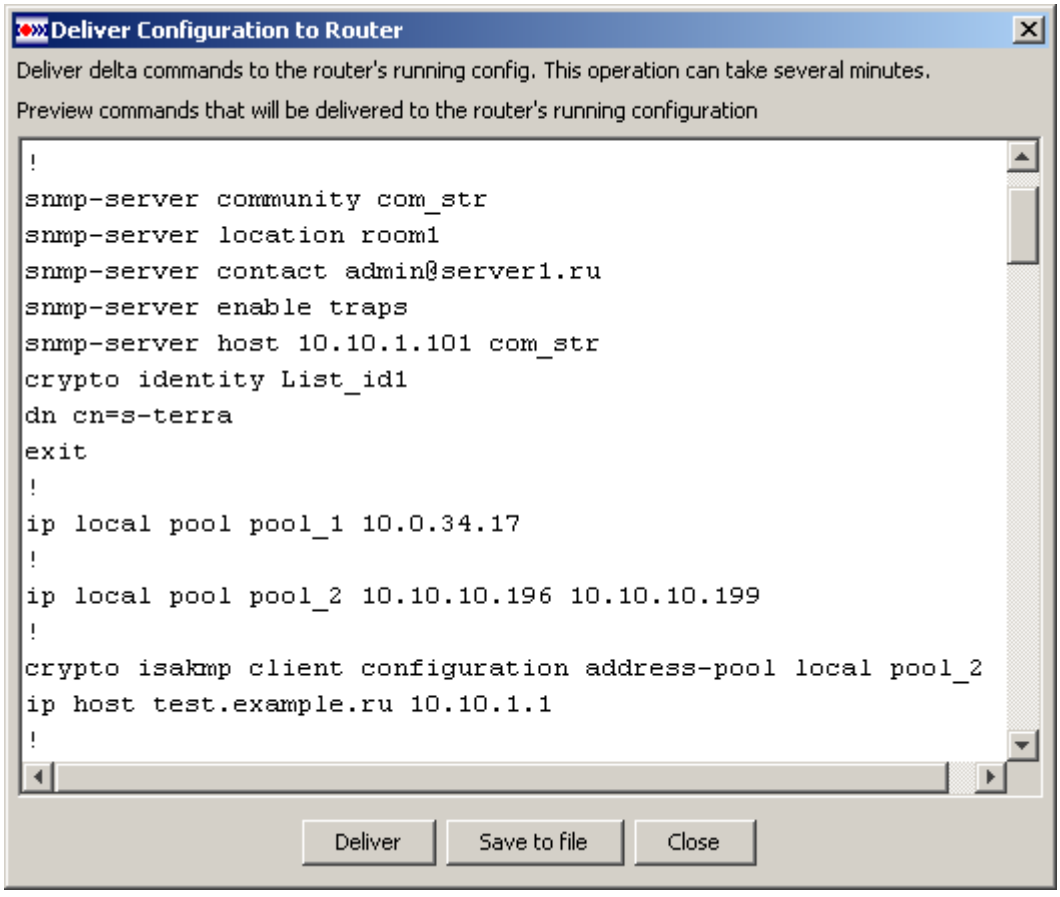

Рисунок 104

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* с отображением процесса доставки конфигурации.

Если во время доставки в конфигурации будет обнаружена ошибка, то появится окно с предупреждением: `Configuration loaded with warnings or errors`. По кнопке Show Details будет отображен протокол сессии доставки конфигурации на шлюз безопасности.

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 105), которое открывается командой *Running Config* в разделе *View* меню.

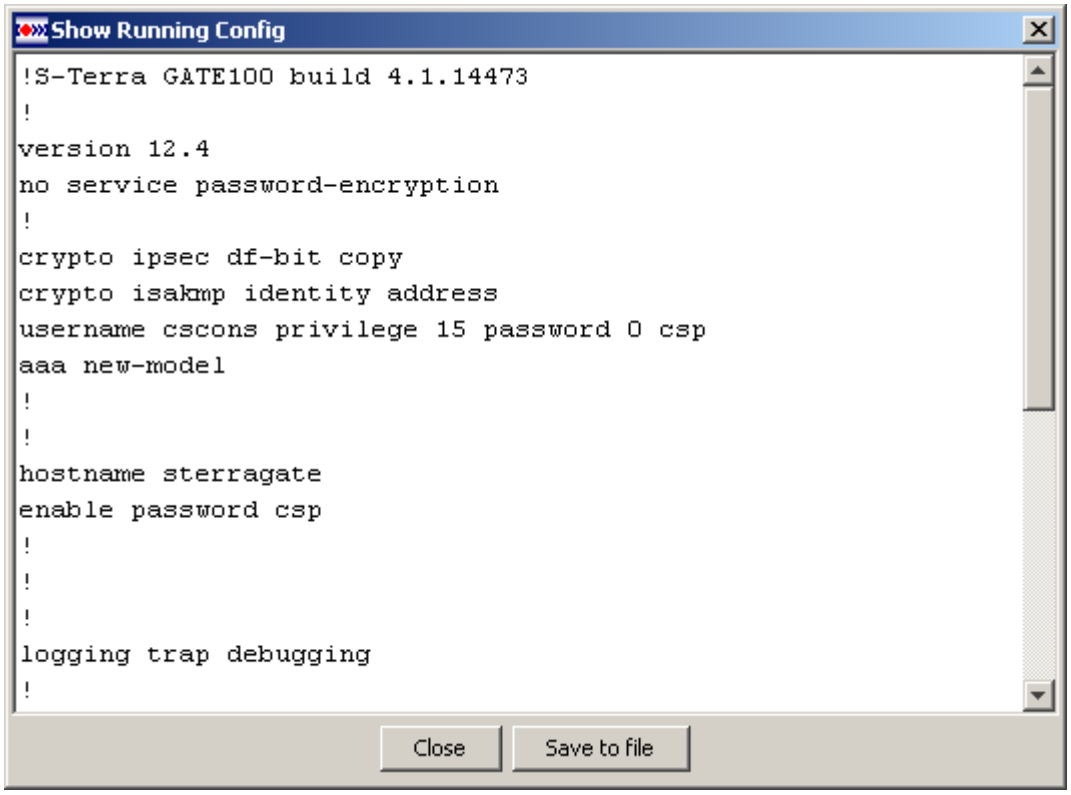

Рисунок 105

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 106) появляется, если в результате анализа конфигурации были обнаружены какие-либо ошибки.

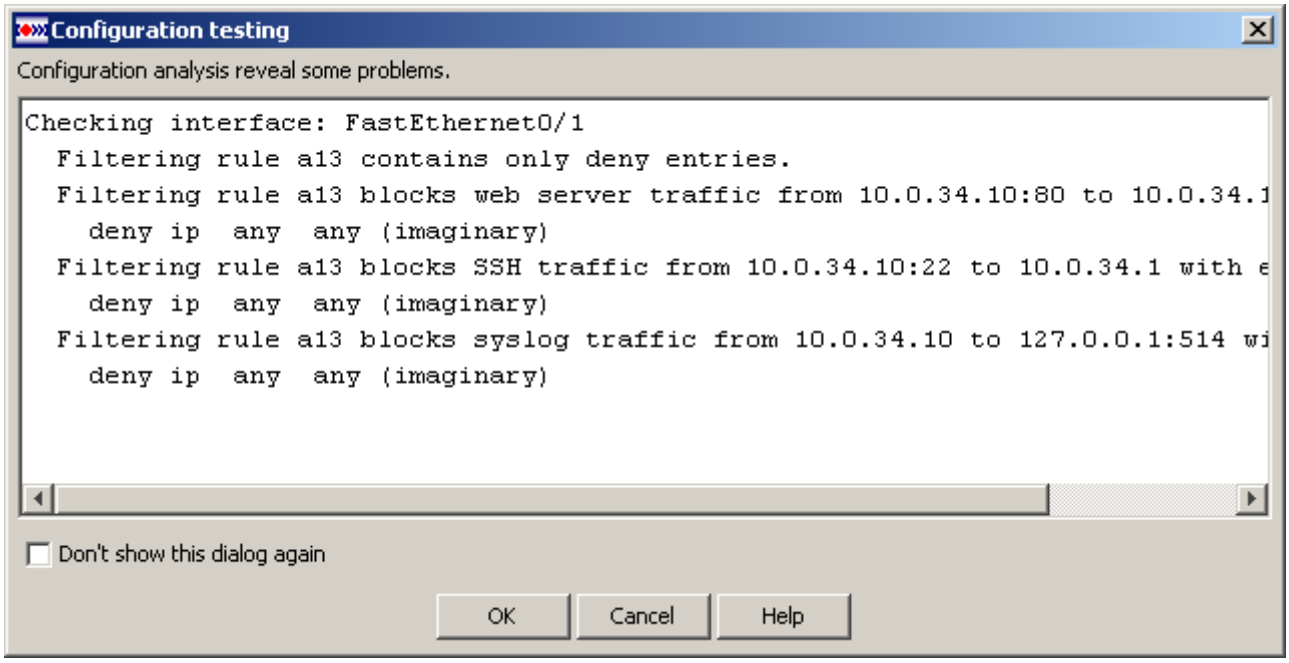

Рисунок 106

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 (Рисунок 107).

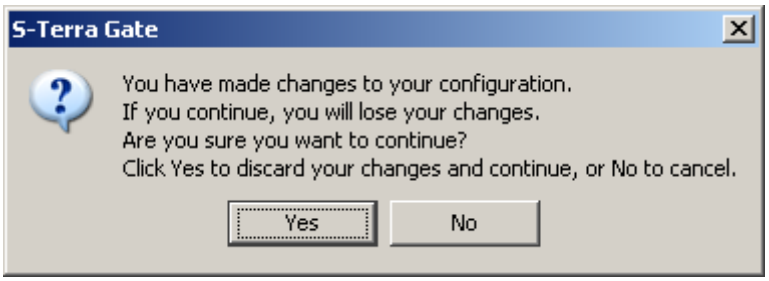

Рисунок 107

Нажатие кнопки No отменяет закрытие приложения.

Нажатие кнопки Yes закрывает приложение и происходит потеря сделанных изменений.

