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

Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.1”

Руководство администратора

Настройка с помощью Cisco Security Manager

РЛКЕ.00005-01 90 03

10.05.2011

Содержание

Настройка с помощью Cisco Security Manager

Cisco Security Manager 3.2 (CSM), который входит в состав Cisco Security Management Suite, используется для централизованной удаленной настройки шлюзов безопасности CSP VPN Gate.

В данном документе описывается совместимость CSM с шлюзами CSP VPN Gate версии 3.1.

Добавление шлюза в CSM

Для работы с CSM предварительно должен быть установлен Cisco Security Manager Client.

Для коммуникации CSP VPN Gate с CSM используется протокол SSH.

CSM допускает использование протокола SSH версии 1 и 2, но рекомендуется использовать протокол SSH версии 2.

Протокол SSL, используемый в CSM по умолчанию, не поддерживается.

Для переключения CSM на протокол SSH нужно выполнить:

- выбрать в меню **Tools -> Security Manager Administration**
- далее выбрать вкладку **Device Communication**
- в параметре **Transport Protocol (IOS Router)** выбрать **SSH**
- сохранить изменения **Save** и закрыть окно **Close**

Поддерживается добавление устройства по сценарию ”Add Device From Network” (**File -> New Device -> Add Device From Network**).

Поддерживается получение текущей конфигурации с работающего устройства, уже добавленного в CSM (**Policy -> Discover Policies on Device**).

В CSM шлюз безопасности идентифицируется аналогично устройству Cisco Router 2811 с установленной операционной системой IOS v.12.4(13a).

В данном документе описаны основные шаги, которые следует выполнить для создания политики безопасности, а также особенности и ограничения, которые в данный момент существуют при настройке CSP VPN Gate.

Рассмотрим основные разделы графического интерфейса CSM, поддерживаемые в данной версии CSP VPN Gate.

Настройка пакетной фильтрации

В разделе **Firewall** поддерживается только настройка пакетной фильтрации – подраздел **Access Rules**.

В **подразделе Access Rules** поддерживается блокирование/разрешение прохождения пакетов по следующим признакам:

- Source, Destination, Subnet
- весь IP-трафик или конкретные предустановленные протоколы
- для UDP и TCP протоколов допускается задание отдельных портов и диапазонов портов.

При создании правил пакетной фильтрации следует использовать рекомендуемые настройки и учитывать некоторые **ограничения**:

- не поддерживается перечисление портов и диапазонов портов
- не допускается фильтрация по отдельным типам ICMP сообщений, только протокол ICMP целиком
- перечисление в одном правиле нескольких сервисов (поле Services), принадлежащих UDP или TCP протоколу приведет к ошибке (например, HTTP и HTTPS, SNMP и SNMP-TRAP). Рекомендуется создавать отдельные правила для каждого из протоколов. Сочетание сервисов, основанных на разных протоколах (например, HTTP, IPSec-ESP, SNMP) допустимо, но рекомендуется вообще отказаться от перечисления нескольких сервисов в одном правиле;
- при создании или редактировании своего сервиса следует соблюдать следующие ограничения:
  - не следует задавать типы ICMP сообщений
  - для UDP и TCP протоколов:
    - допускается задать единичный номера порта
    - допускается задать один диапазон портов
    - допускается слово any для обозначения всего диапазона портов
    - не допускается перечисление портов и диапазонов портов
    - не допускаются модификаторы lt, gt, neq. Модификатор eq допускается, но его писать не обязательно.
- при добавлении и редактировании Access Rule не следует менять следующие настройки Advanced:
  - Traffic Direction допускается только “In” (значение по умолчанию: для исходящего трафика будут работать неявные правила, симметричные правилам для входящего трафика);
  - не поддерживаются никакие дополнительные опции: Enable Logging (IOS), Options (IOS) – Fragment и Established и т.п.

Настройка Site to Site VPN

В разделе **Site to Site VPN** поддерживаются следующие топологии:

- “звезда” (Hub and Spoke VPN)
- “точка-точка” (Point to Point VPN)
- “каждый с каждым” (Full Mesh VPN).

В топологии Hub and Spoke VPN не поддерживается вариант конфигурации с резервированием шлюза.

В IPSec Technology допускается только Regular IPSec (GRE не поддерживается).

Существуют некоторые **ограничения** в подразделах раздела Site to Site VPN. Чтобы увидеть эти подразделы надо нажать кнопку **Edit VPN Policies**.

Подраздел IKE Proposal

- IKE Proposal допускается задавать с использованием Authentication Certificate или Preshared Key
- чтобы использовать алгоритмы ГОСТ Р 34.11.94 и ГОСТ 28147-89 следует указать следующие алгоритмы: Hash – MD5, Encryption – DES
- если есть необходимость использовать в Modulus Group алгоритм VKO, надо скорректировать файл настроек конвертора cs_conv.ini, расположенный в каталоге продукта Шлюз безопасности:
  - выбрать неиспользуемую в IKE Diffie-Hellman группу.
    Рекомендуется выбирать минимальную неиспользуемую группу:
    Для полностью новой инфраструктуры – группу 1. Если в существующей инфраструктуре группа 1 уже используется, то группа 2 и т.п.
  - для выбранной группы в файле cs_conv.ini прописать конвертирование в алгоритм VKO_1B:

    ```
    ike-group-vko = VKO_1B
    ike-group-1 = VKO_1B
    ike-group-2 = MODP_1024
    ike-group-5 = MODP_1536.
    ```

Подраздел IPSec Proposal

- для использования алгоритмов ГОСТ в IPSec Transform Sets следует использовать следующие алгоритмы: ESP Hash и AH Hash – MD5, ESP Encryption – DES
- не поддерживается компрессия, поэтому флажок **Compression** должен быть снят
- если установлен флаг Enable Perfect Forward Secrecy и есть необходимость использовать в Modulus Group алгоритм VKO, надо скорректировать файл настроек конвертора cs_conv.ini, расположенный в каталоге продукта Шлюз безопасности:
  - выбрать неиспользуемую в PFS Diffie-Hellman группу.
    Для простоты рекомендуется выбрать ту же самую группу, что и для IKE
  - для выбранной группы в файле cs_conv.ini прописать конвертирование в алгоритм VKO_1B:

    ```
    pfs-group-vko = VKO_1B
    pfs-group-group1 = VKO_1B
    pfs-group-group2 = MODP_1024
    pfs-group-group5 = MODP_1536.
    ```

  - поддерживается **Reverse Route**

Подраздел Public Key Infrastructure

- при использовании Authentication Certificate требуется ввод CA-сертификата в разделе **PKI Enrollment/CA Information** – (**Enter Manually**)
  Получение CA сертификата по SCEP протоколу не поддерживается
- не поддерживается enrollment, поэтому любые введенные значения будут игнорироваться. Однако, их следует заполнить, чтобы не спровоцировать ошибку в CSM
- при использовании Authentication Certificate допускаются варианты Revocation Check Support: **Checking Not Performed**, **CRL Check Required**, **CRL Check Attempted**. **OSCP Check** не поддерживается.

Подраздел VPN Global Settings

Подраздел ISAKMP Settings / IPSec Settings

В **ISAKMP Settings** допускается:

- устанавливать/сбрасывать флаг **Enable Keepalive** и настраивать параметры **Interval и Retry**, флаг **Periodic** (Router except 7600) устанавливать не рекомендуется
- настраивать **Identity**
- настройки остальных параметров менять не следует.

В **IPSec Settings** допускается:

- устанавливать/сбрасывать флаг **Enable Lifetime** и настраивать параметры **Lifetime sec. и Lifetime Kbytes**
- настройки остальных параметров менять не следует.

Подраздел NAT Settings не поддерживается

Подраздел General Settings/ Fragmentation Settings

- допускается настройка **DF Bit**
- независимо от установки флага **Enable Fragmentation before Encryption** драйвером VPN будет самостоятельно принято решение фрагментировать пакет или нет, и такая фрагментация осуществляется только после IPsec инкапсуляции. Команды в конфигурации, порождаемые CSM установкой или отсутствием указанного флага, будут проигнорированы
- остальные настройки данной вкладки не следует менять.

Настройка Interfaces

В разделе **Interfaces** можно посмотреть настройки всех Cisco-интерфейсов.

В CSM интерфейсы разделены по ролям. Например, по умолчанию есть деление на Internal и External интерфейсы. Чтобы изменить данную настройку надо:

- нажать правую кнопку мыши на устройстве, выбрать **Device Properties**…
- **Policy Object Overrides -> Interface Roles**.

Настройка Platform

Существуют некоторые ограничения в подразделах раздела Platform.

Подраздел Device Admin – поддерживаются следующие подразделы:

Accounts and Credentials

Device Access

Hostname

Подраздел Accounts and Credentials

- не допускается выставление флага **Enable Password Encryption Service**

Подраздел Device Access / SNMP

- в подразделе **Permissions** следует соблюдать следующие ограничения:
  - нельзя создавать больше одной записи;
  - не допускается тип записи **Read-Write**, только **Read-Only**
  - не допускается привязка **Access Control Lists**
- в подразделе **Trap Receiver** следует соблюдать следующие ограничения:
  - не следует пользоваться кнопкой **Configure Traps**… Если необходимо отсылать SNMP traps, следует в cs_console, не используя CSM, задать команду **snmp-server enable traps**
  - при добавлении или редактировании Trap Receiver нельзя задавать **SNMP Version 3**. Допускаются только **1** или **2c**.

Подраздел Logging

Подраздел Logging Setup

- допускается включать/отключать флаг **Enable Logging**. Отключение флага вызывает полное отключение логирования
- допускается настраивать **Trap / Trap Level**
- остальные настройки: **Logging Buffer, Rate Limit, Origin Id** не поддерживаются.

Подраздел Syslog Servers

- нельзя создавать больше одной записи
- не допускается выставление флага **Forward Messages in XML Format**.

Подраздел Routing – поддерживается только Static Routing:

Подраздел Static Routing

- не допускается выставлять флаг **Permanent route**
- не рекомендуется задавать **Distance Metric**.

Особенности при работе с конфигурацией

1. Рекомендуется не использовать сценарии, в которых настройка CSP VPN Gate выполняется как через CSM, так и вручную. Если потребность в таком сценарии существует, то надо стараться задавать вручную только те команды, которые CSM не использует в процессе настраивания CSP VPN Gate.

   Следует учитывать, что при отгрузке конфигурации, CSM может изменить или удалить некоторые из команд, которые существовали в изначально импортированной конфигурации, например `ip local pool` или `crypto isakmp policy`.

   Для примера, рассмотрим, почему создание политики безопасности шлюза через CSM для работы с мобильными клиентами невозможно.

   Порядок действий, который приводит к данному ограничению, следующий:

   - шлюз добавлен в CSM для работы по одной из топологий
   - при помощи CSM проведена централизованная настройка шлюзов по одной из топологий – FullMesh, Hub and Spoke, Point to Point
   - затем, например, по SSH отредактировать конфигурацию одного из шлюзов для работы с мобильными клиентами – создать пул адресов, привязать к криптокарте, создать identity и др.
   - после загрузки на шлюз созданной конфигурации через CSM, работа с мобильными клиентами будет невозможна в созданной топологии.

   Причина состоит в том, что все пулы адресов, не привязанные к команде `crypto isakmp client configuration address-pool local`, CSM удаляет.

2. В случае применения сценария с резервированием шлюзов и использованием предопределенных ключей, необходимо учитывать, что CSP VPN Gate не поддерживает возможность задания различных preshared ключей для основного и резервного шлюза.

   Для успешной работы подобных сценариев необходимо задать одинаковые preshared ключи для всех партнеров либо вручную, либо, если указана автоматическая генерация ключей – в разделе View –> Policy View –>Site-to-Site VPN –> Preshared Key установить флажок `Same Key for All Tunnels`.

3. Возможны некоторые проблемы с восстановлением конфигурации. В некоторых случаях изменение или удаление существующих команд может быть безвозвратным: даже если в CSM удалить изменения, внесенные в конфигурацию, например, удалить VPN Topology, первоначальная конфигурация (которая была до Deploy) может не восстановиться в полном объеме. Более того, возможны ситуации, когда какие-то элементы конфигурации могут быть испорчены именно при отмене изменений, сделанных в CSM. Например:

   - в первоначальной конфигурации была настройка `crypto isakmp identity dn`
   - в CSM, в VPN Global Setings выставлена настройка `Identity – Distinguished Name`
   - в прогружаемой из CSM конфигурации команда `crypto isakmp identity` отсутствует
   - если потом удалить VPN Topology и снова прогрузить конфигурацию, то будет прописана команда `crypto isakmp identity address` (значение по умолчанию), что отличается от того, что было в первоначальной конфигурации.

4. CSP VPN Gate не поддерживает функциональность **Rollback**, позволяющую вернуться к конфигурациям, которые были загружены в устройство ранее (**Tools / Configuration Archive…**).

Пример создания политики безопасности

Сценарий

Две подсети защищаются шлюзами безопасности CSP VPN Gate 3.1. Трафик между шлюзами безопасности защищен туннелем. Аутентификация сторон осуществляется на предустановленных ключах.

Запуск Cisco Security Manager

При запуске указываем имя сервера (ip адрес), на котором установлен Cisco Security Manager, логин и пароль пользователя.

Подключение CSP VPN Gate к CSM

Подключение CSP VPN Gate к CSM производится через добавление нового устройства **File -> New Device**:

- выбрать предложение Add Device From Network
- в разделе Identity ввести IP Type. IP Address, Display Name (если необходимо), OS Type.

  Вводим IP Type – Static, IP-Address – 10.0.34.11, OS Type – IOS

  В разделе Discover Device Settings оставляем настройки, предлагаемые по умолчанию.
- в разделе Primary Credentials ввести Username, Password (пользовательский пароль) и Confirm. Если пользователь непривилегированный, необходимо еще ввести Enable Password и Confirm.

  Например, вводим Username – cscons, Password – csp, Confirm – csp.

  В разделе HTTP Credentials оставим рекомендуемые настройки:

  HTTP Port – 80, HTTPS Port – 443, Mode – HTTPS.

  Нажимаем кнопку Finish

Подключим второй CSP VPN Gate с IP-адресом 10.0.34.12.

Описание топологии сети

В разделе **Site to Site VPN** выберем топологию создаваемой защищенной сети Point to Point VPN.

IPSec Technology – укажем **Regular IPSec** (Рисунок 1)

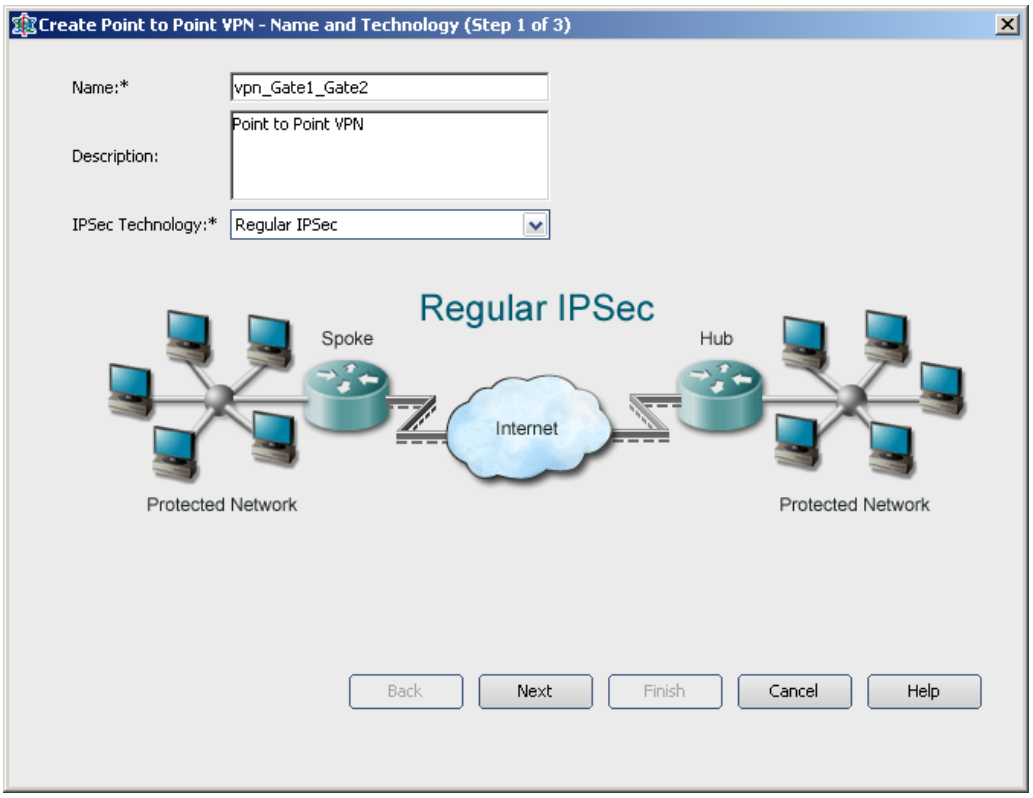

Рисунок 1

Выберем устройства, между которыми будет создаваться защищенное соединение: CSP VPN Gate, с адресом внешнего интерфейса 10.0.34.11 и CSP VPN Gate, с адресом внешнего интерфейса 10.0.34.12 (Рисунок 2).

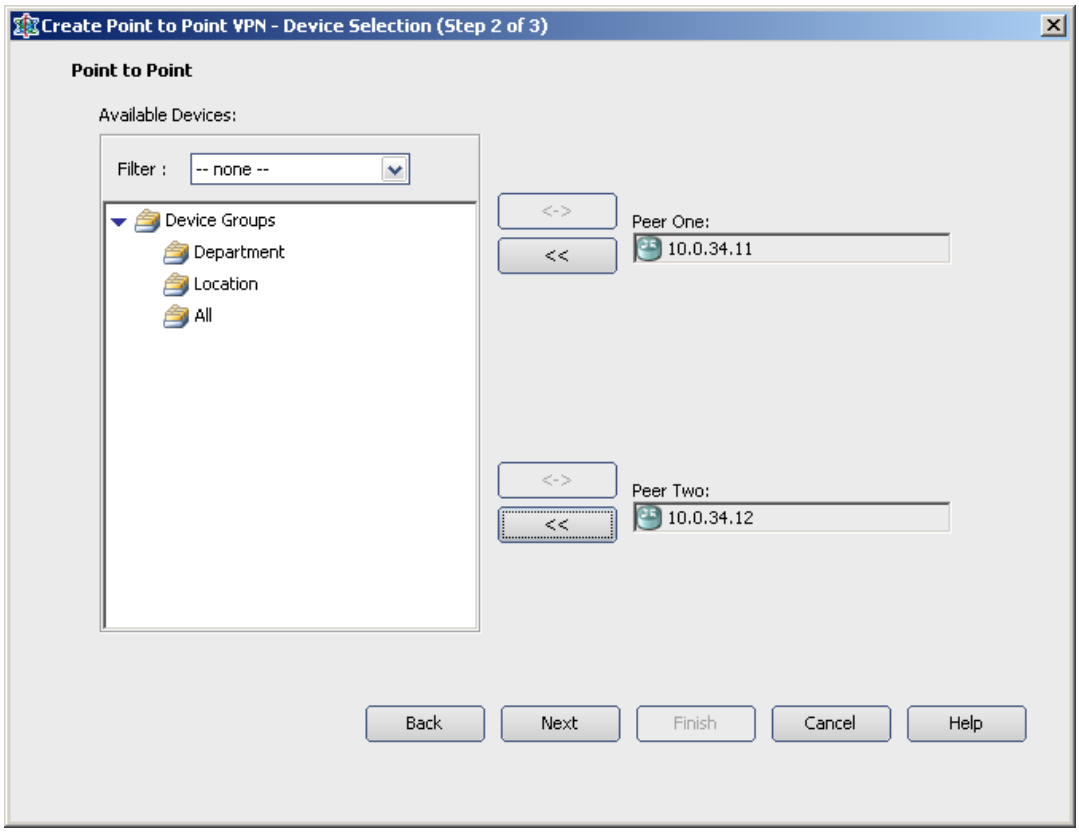

Рисунок 2

Затем для каждого устройства можно отредактировать такие параметры соединения как VPN Interface и Protected Networks:

- для VPN Interface укажем FastEthernet0/0, установим переключатель Peer IP Address в положение VPN Interface IP Address
- для Protected Networks укажем FastEthernet0/1.

Установленные параметры отображает Рисунок 3.

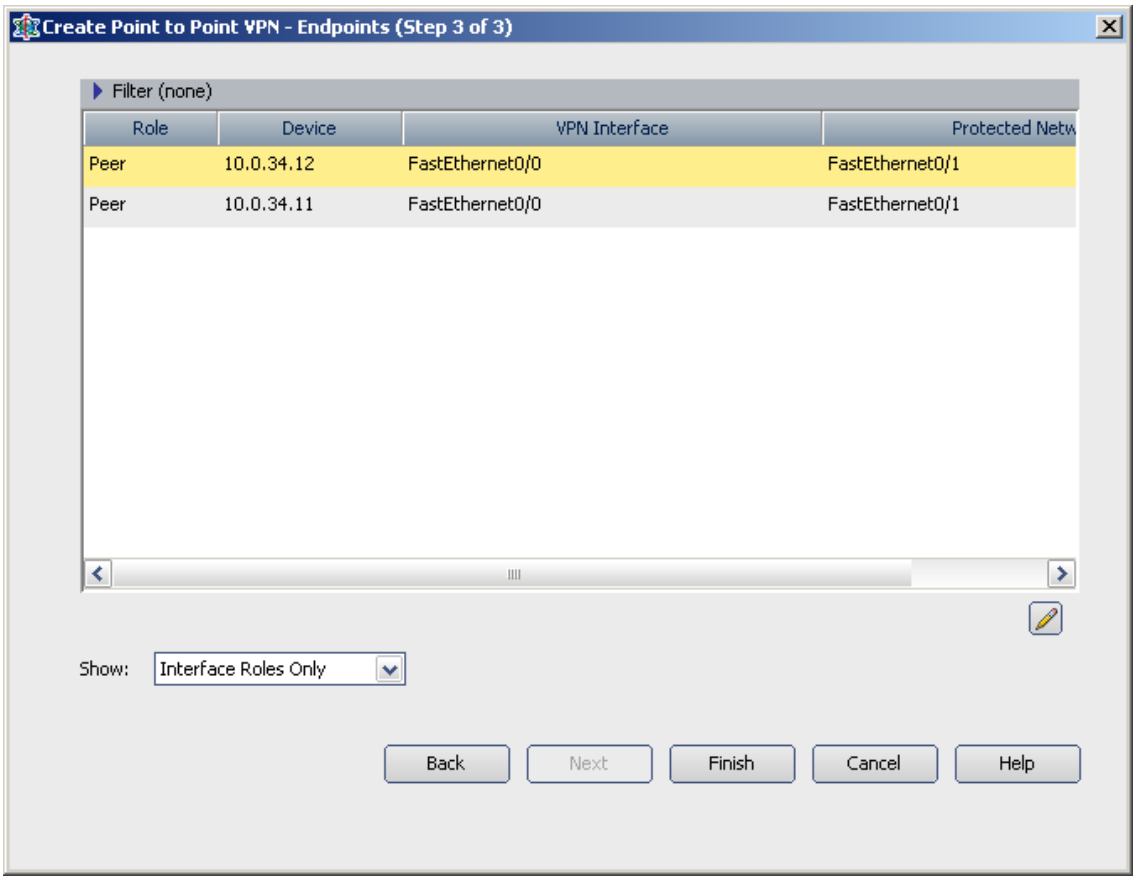

Рисунок 3

Нажмем кнопку Finish. Созданная VPN появится в окне Cisco Security Manager в разделе Devices (Рисунок 4).

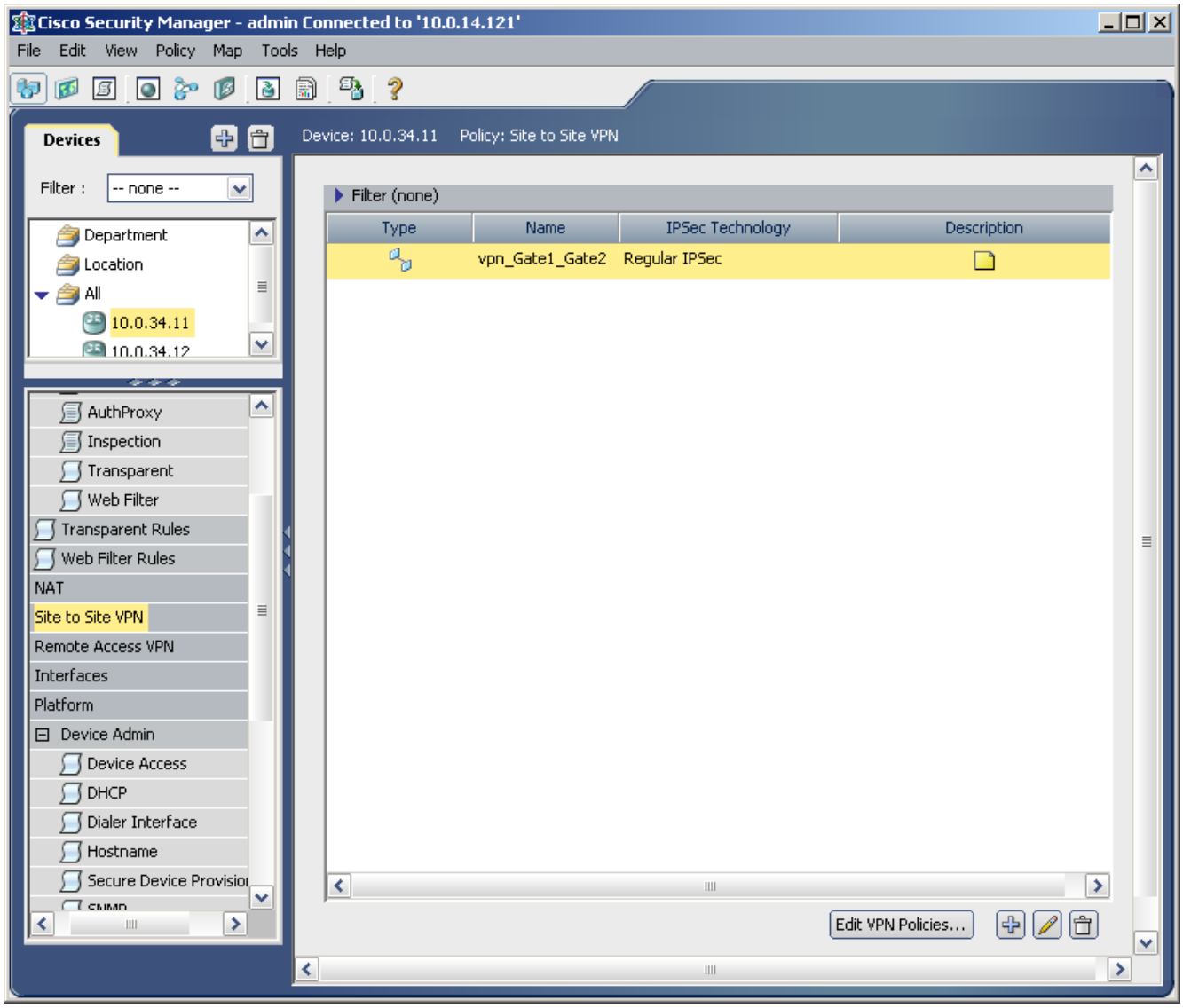

Рисунок 4

Нажав кнопку Edit VPN Policies, перейдем в новое всплывающее окно Site-To-Site VPN Manager (Рисунок 5) в раздел VPNs, где настроим следующие параметры:

- IKE Proposal
- IPSec Proposal
- Preshared Key
- VPN Global Settings

Если бы у нас была аутентификация на сертификатах, то понадобились бы настройки Public Key Infrastructure.

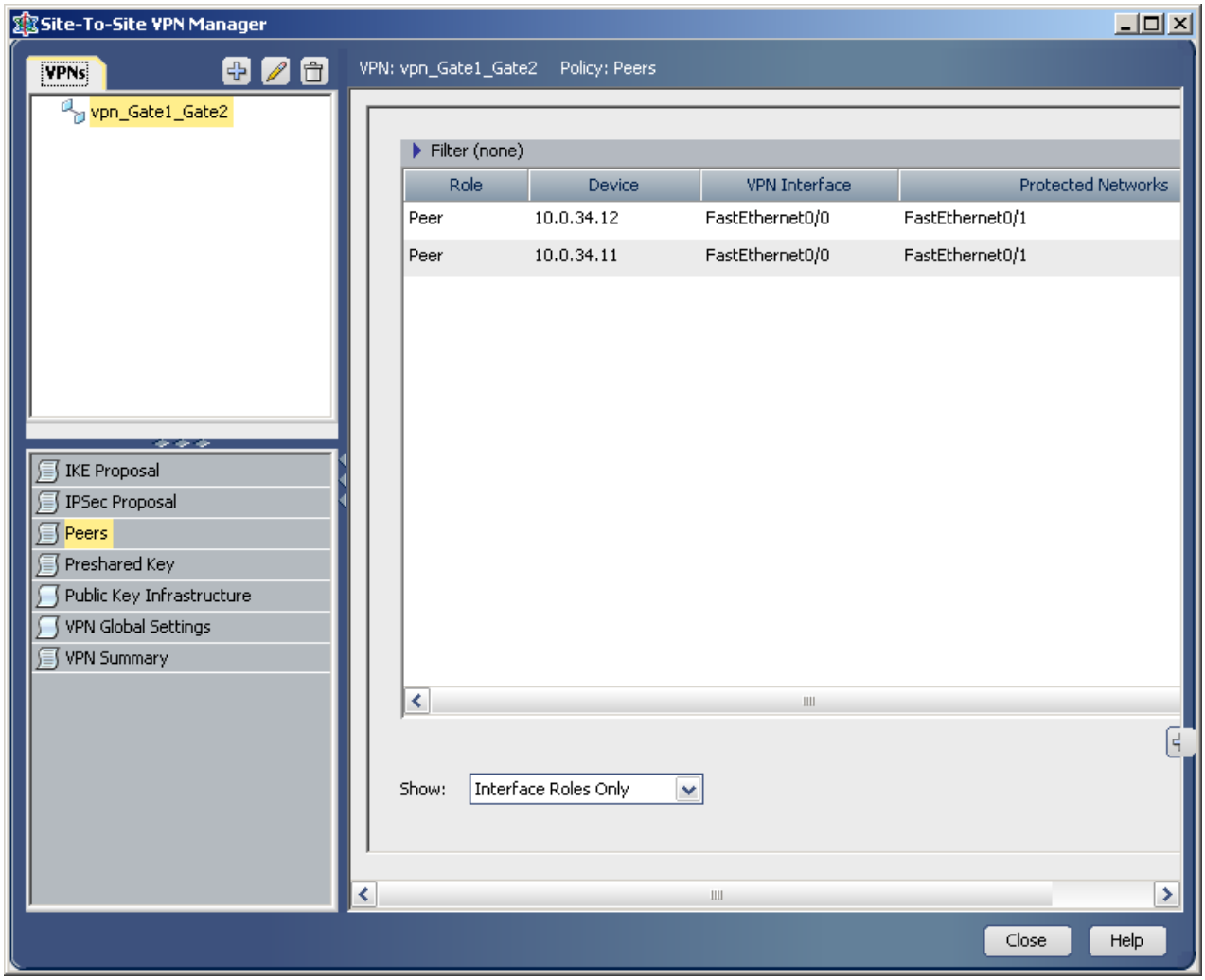

Рисунок 5

Настройка IKE политики

Настроим параметры IKE политики: зададим приоритет, создаваемой политики; выберем алгоритмы шифрования и аутентификации; метод аутентификации; выберем группу Diffie-Hellman; установим время жизни SA. (Рисунок 6)

- Устанавливаем Priority – 10
- Из списка Encryption Algorithm выбираем значение des, которое будет интерпретироваться CSP VPN Gate как алгоритм шифрования ГОСТ 28147-89.
- Из списка Hash Algorithm выбираем значение MD5, которое будет интерпретироваться CSP VPN Gate как алгоритм хеширования ГОСТ Р 34.11-94.
- Указываем Modulus Group – 2 (Diffie-Hellman Group 2)
- Задаем значение Lifetime – 3600 сек.
- Из списка Authentication Method выбираем Preshared Key

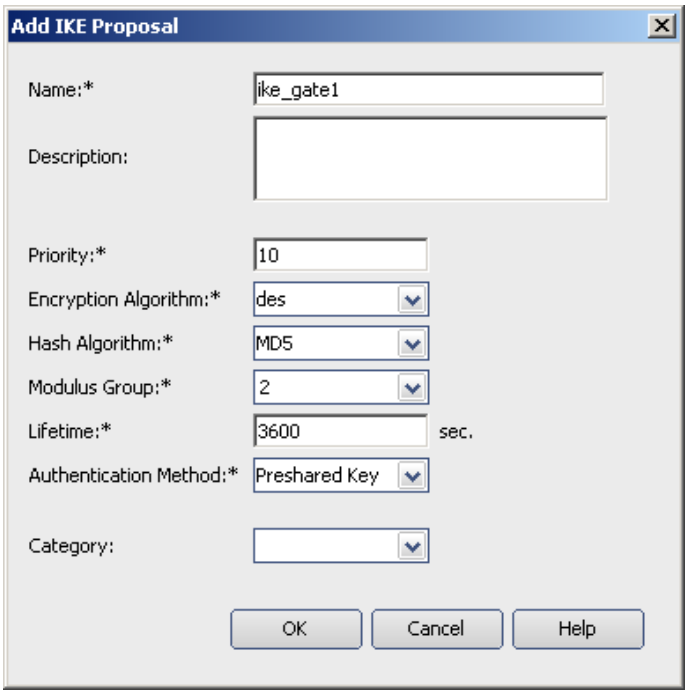

Рисунок 6

Настройка IPSec политики

Настроим параметры IPSec политики.

Создадим Transform Set (Рисунок 7)

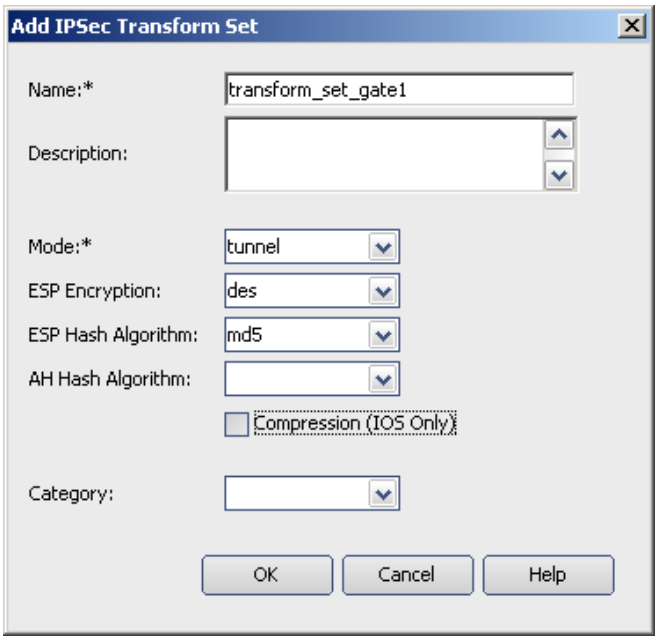

Рисунок 7

- Установим туннельный режим – из списка значений Mode выберем – tunnel
- Из списка ESP Encryption выберем алгоритм шифрования des, это значение будет интерпретироваться CSP VPN Gate как алгоритм шифрования ГОСТ 28147-89.
- Из списка ESP Hash Algorithm выбираем значение md5, которое будет интерпретироваться CSP VPN Gate как алгоритм хеширования ГОСТ Р 34.11-94.

Настроим остальные параметры (Рисунок 8):

- Установим переключатель Crypto Map Type в положение Static
- Установим флаг Enable Perfect Forward Secrecy. Выберем Modulus Group – 2.
- Lifetime – 3600 сек.
- Lifetime – 4608000 kbytes

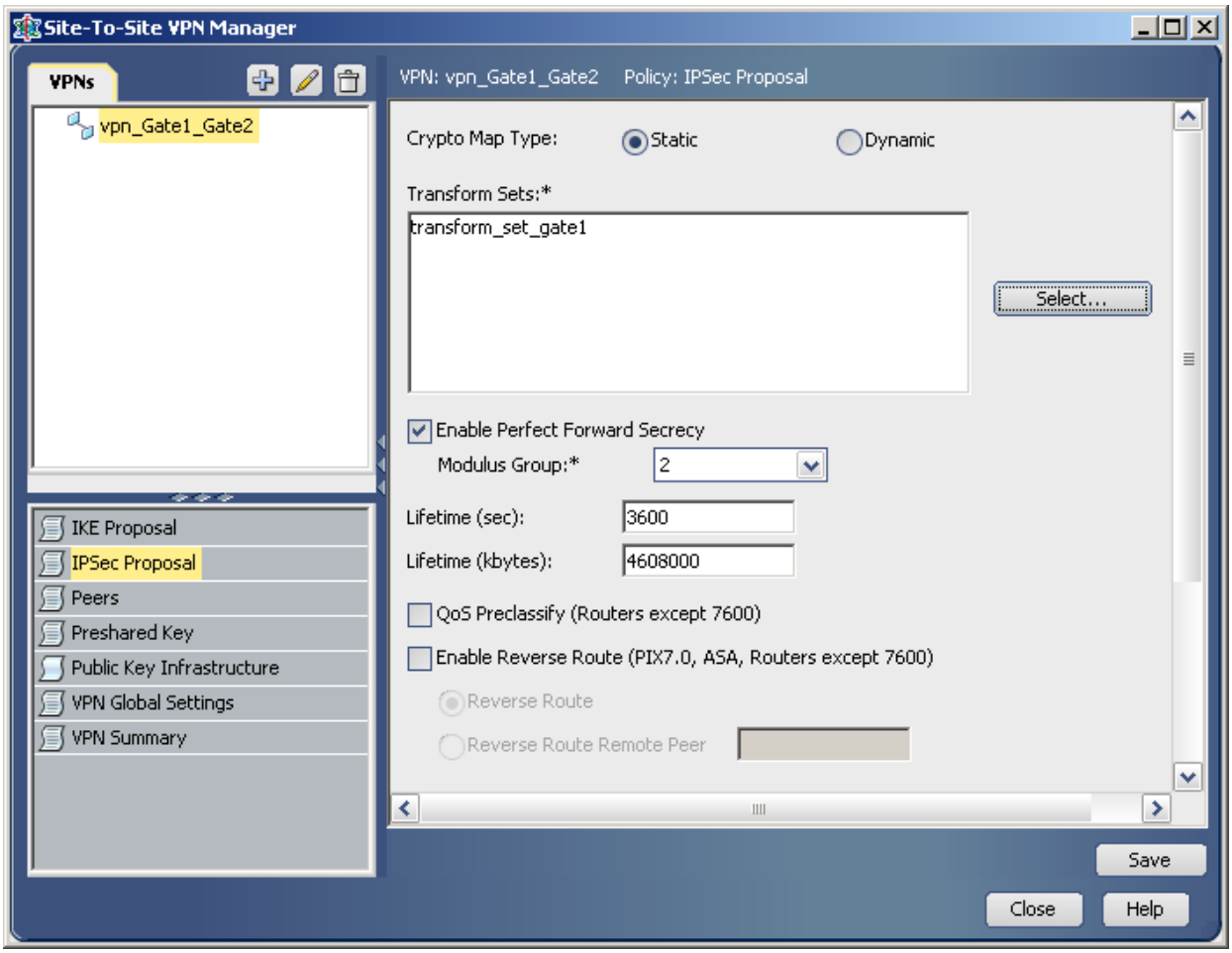

Рисунок 8

Preshared Key

Зададим автоматическую генерацию предопределенных ключей.

Выберем метод согласования Main Mode Address. Установим Main Mode Address Type – Peer Address. (Рисунок 9)

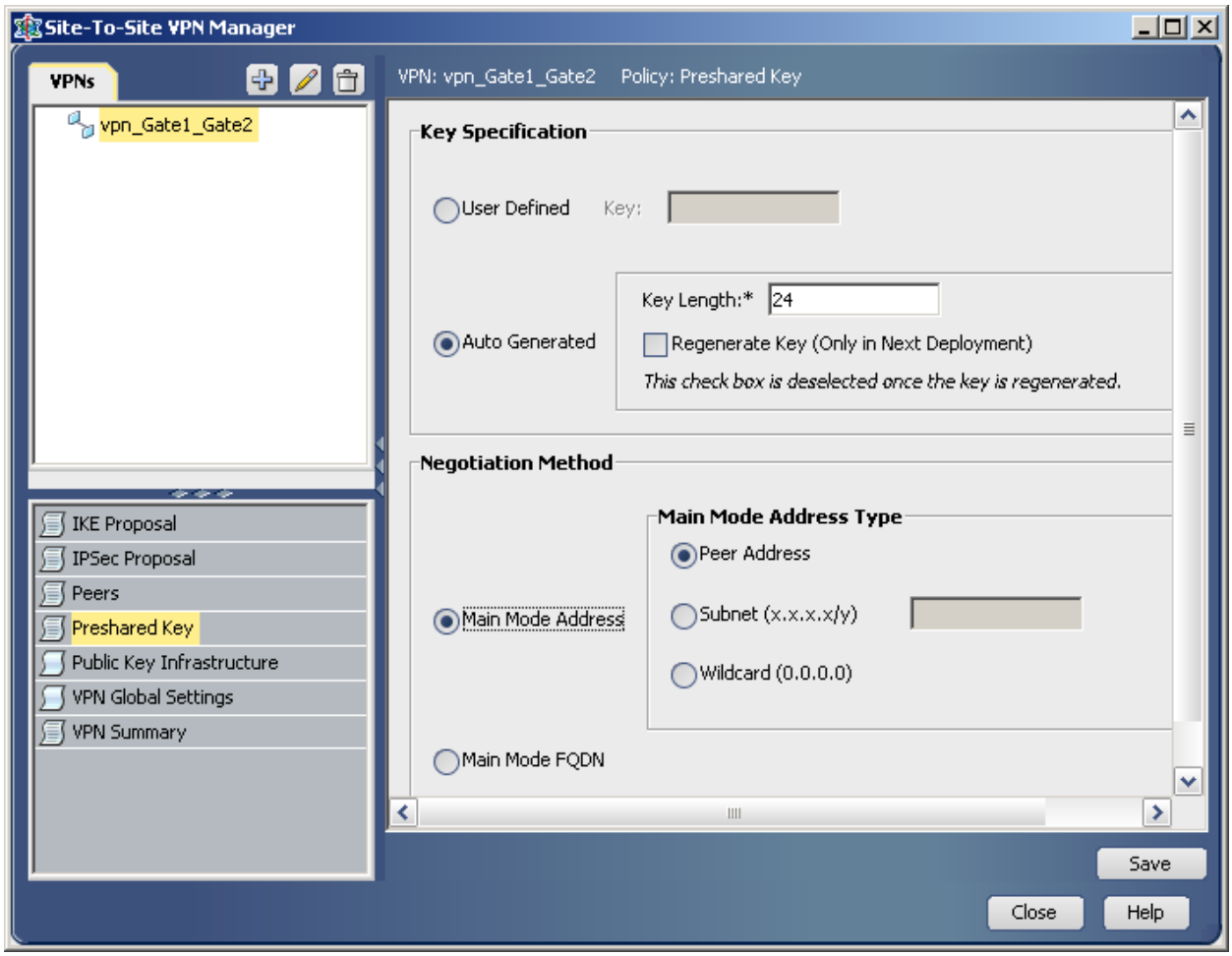

Рисунок 9

VPN Global Settings

Установим глобальные параметры VPN в подразделе ISAKMP/IPSec Settings (Рисунок 10):

ISAKMP Settings

- Установим флаг Enable Keepalive
- Значения Keepalive – Interval и Retry принимаем по умолчанию
- Для Identity выбираем значение Address

IPSec Settings

- Установим флаг Enable Lifetime
- Значение Lifetime принимаем по умолчанию – 3600 секунд и 4608000 кбайт

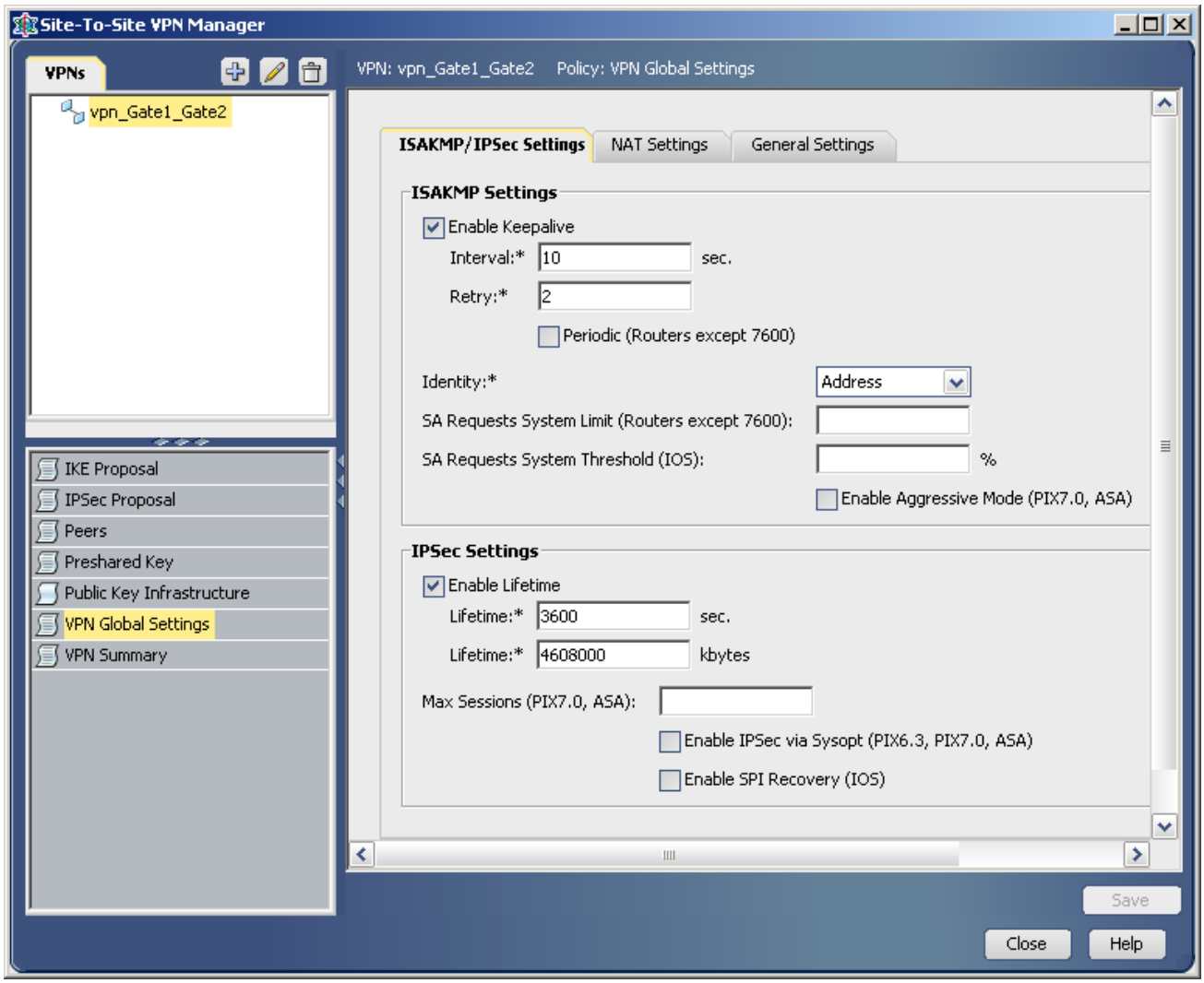

Рисунок 10

В подразделе General Settings (Рисунок 11)

Fragmentation Settings

- Выбираем для Fragmentation Mode (IOS) значение No Fragmentation
- Для DF Bit выбираем значение Copy

- Устанавливаем флаг Enable Split Tunneling

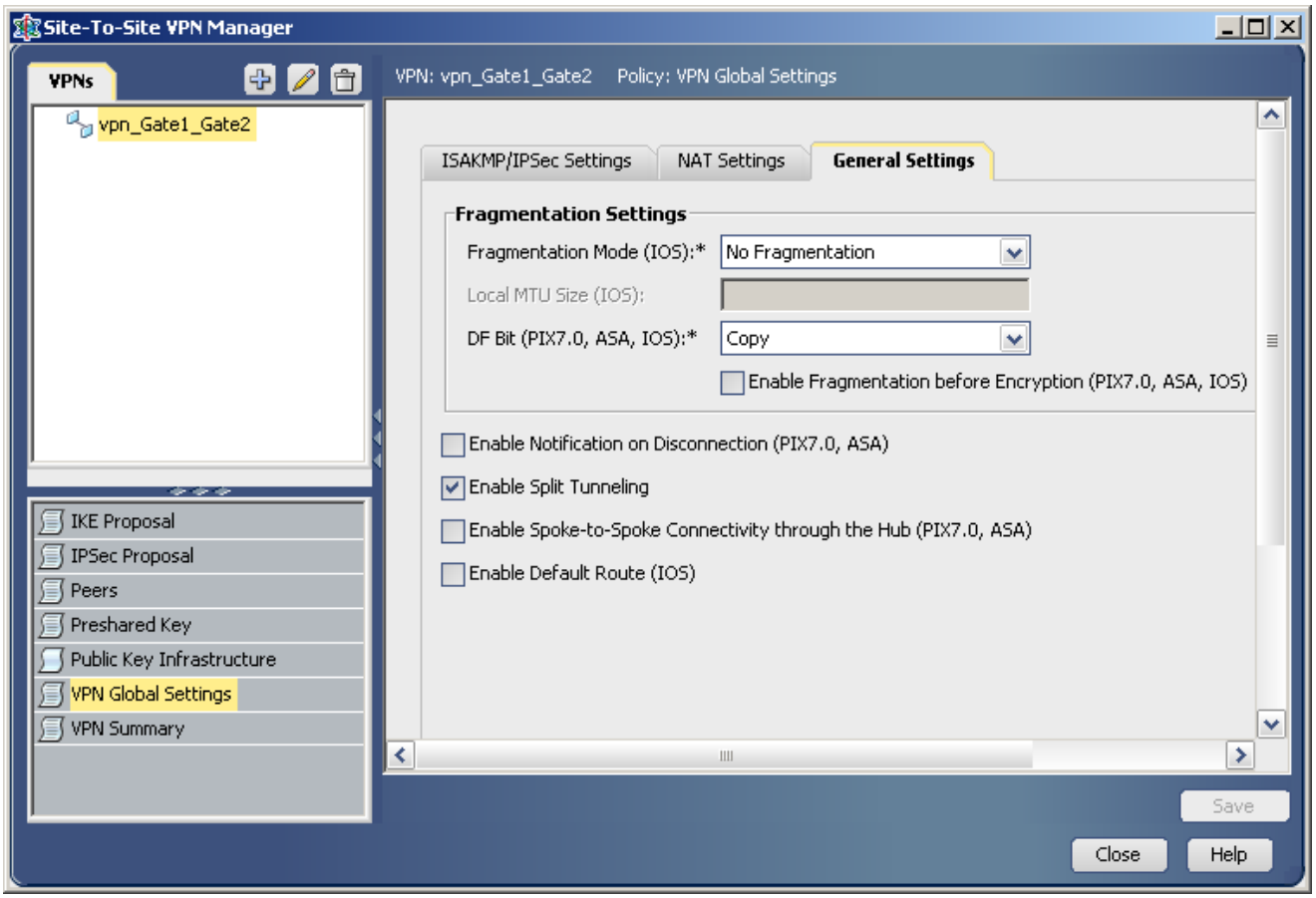

Рисунок 11

VPN Summary

Посмотреть основные установленные VPN параметры для CSP VPN Gate можно в разделе VPN Summary (Рисунок 12)

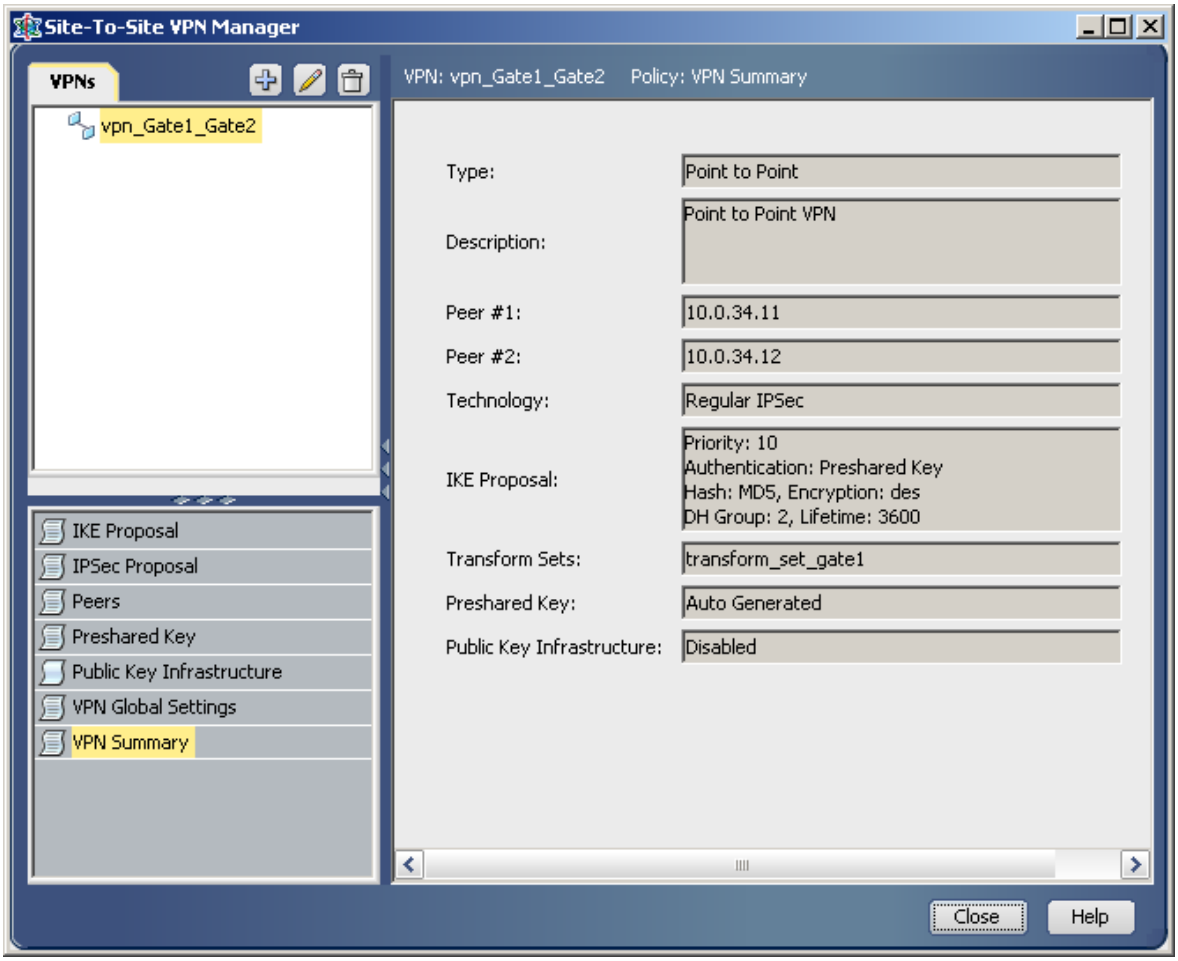

Рисунок 12

Более подробно посмотреть созданную конфигурацию можно по команде меню **Tools -> Preview Configuration**.

Доставка конфигурации на устройство

В меню **Tools** выбираем **Deployment Manager**

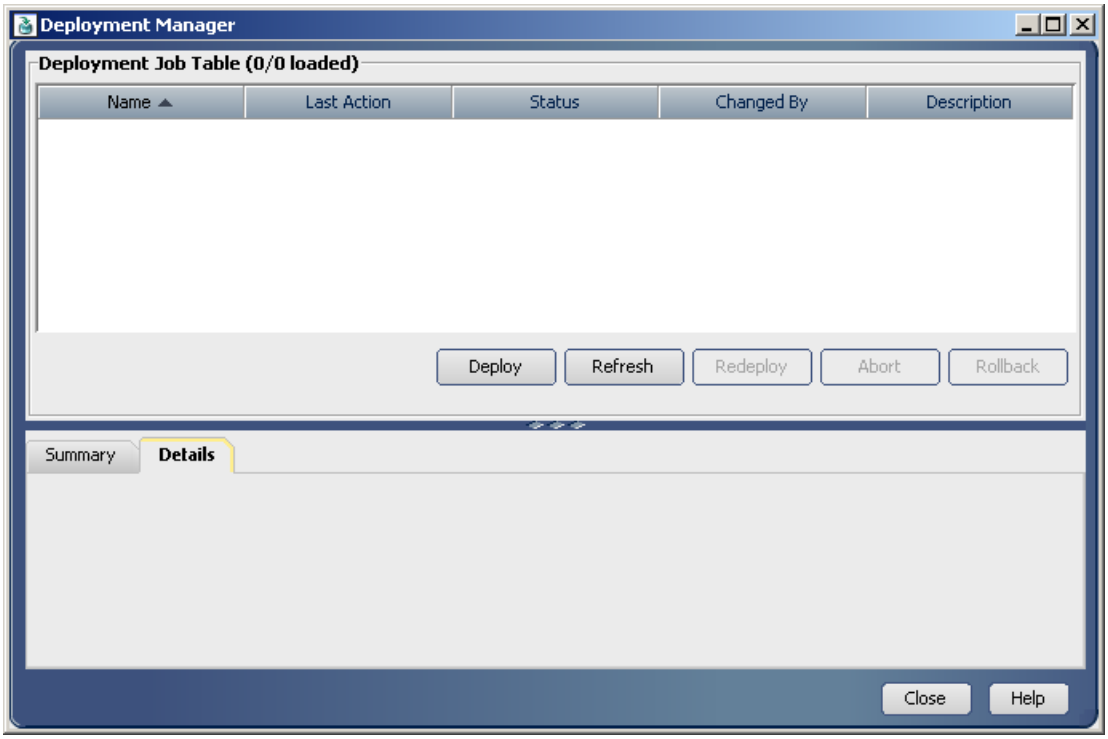

Рисунок 13

В появившемся окне (Рисунок 13) нажимаем кнопку Deploy. Будет предложено выбрать устройства, на которые будет доставляться конфигурация (Рисунок 14). CSM автоматически определяет устройства, для которых были сделаны изменения, но конфигурация на которые не была загружена.

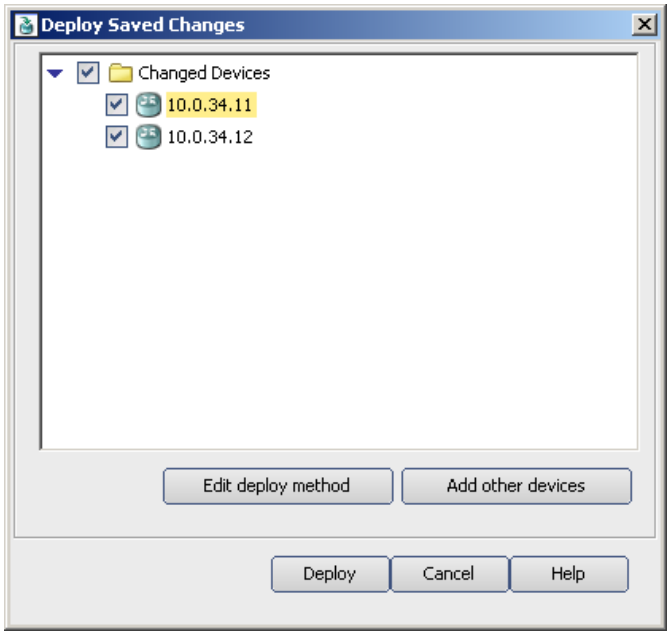

Рисунок 14

По кнопке Deploy, будет выполнена попытка загрузить конфигурацию на устройство. Если конфигурация будет доставлена на устройство успешно, то выдается соответствующее сообщение (Рисунок 15), в случае неудачи – будет выдано сообщение об ошибке.

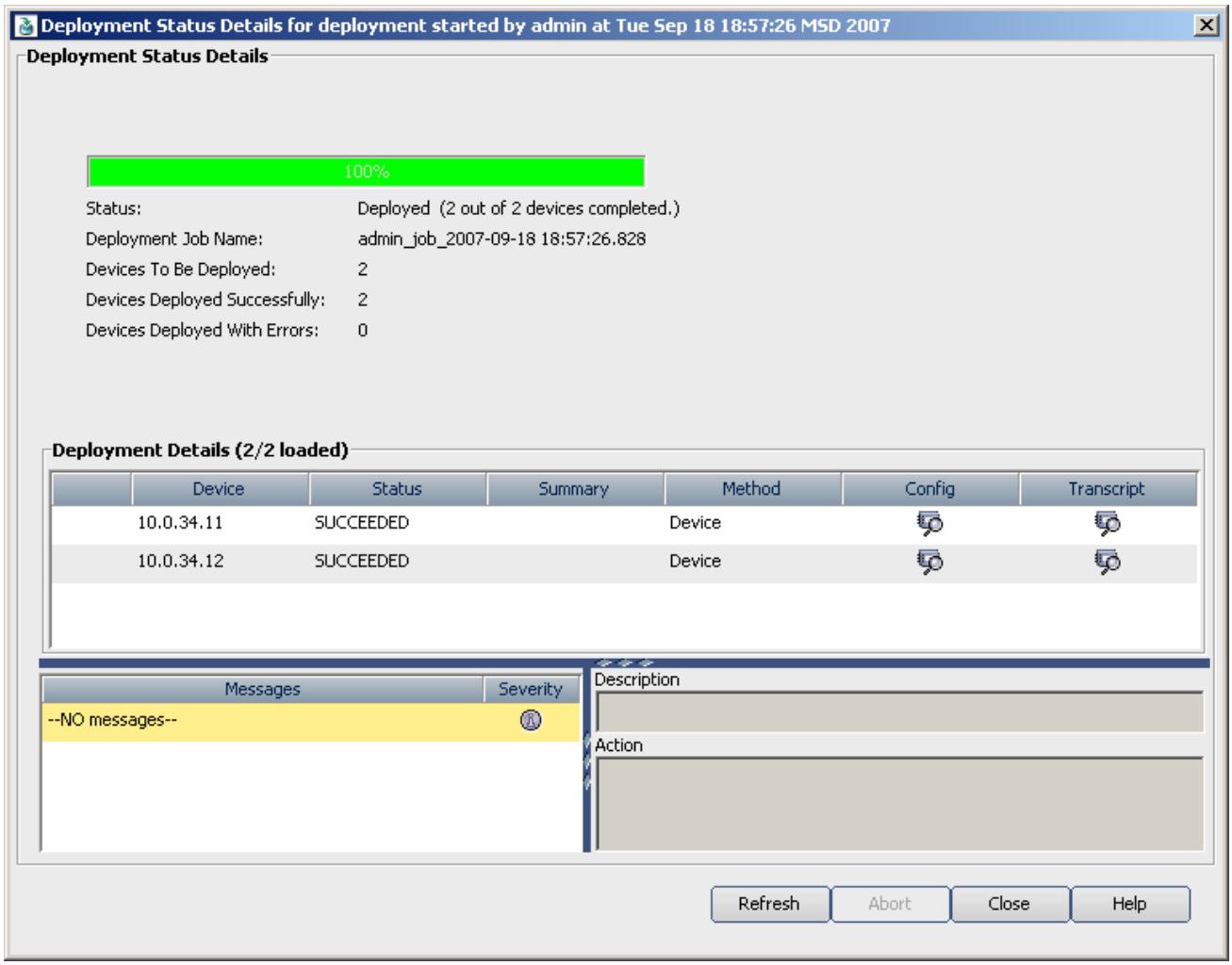

Рисунок 15