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

Программный комплекс CSP VPN Gate. Версия 3.11

Руководство администратора

Настройка с помощью Cisco Security Manager

РЛКЕ.00005-02 90 03

20.04.2012

Содержание

Настройка с помощью Cisco Security Manager

Cisco Security Manager 4.3 (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 3.11.

Добавление шлюза в CSM

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 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 /opt/VPNagent/bin/ 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 /opt/VPNagent/bin/ 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

Построение VPN туннеля между двумя подсетями, защищаемыми шлюзами безопасности CSP VPN Gate, при помощи Cicso Security Manager 4.3. Устройства Host1 и Host2 смогут общаться между собой по защищенному каналу (VPN). Все остальные соединения разрешены, но защищаться не будут. Аутентификация сторон осуществляется с использованием сертификатов. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6.

Схема стенда

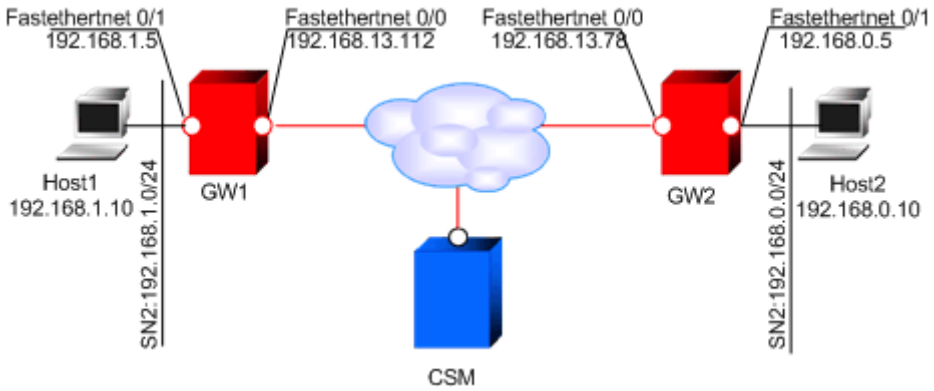

Рисунок 1

Параметры защищенного соединения:

- Аутентификация на сертификатах
- IKE parameters:
  - Encryption algorithm – GOST 28147-89
  - Hash algorithm – GOST R 34.11-94 Hash
  - DH-group – VKO GOST R 34.10-2001
- IPsec parameters:
  - ESP encryption algorithm – GOST 28147-89
  - ESP integrity – GOST R 34.11-94 HMAC.

Первоначальные настройки

Первоначальные настройки шлюзов производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Для начала требуется зарегистрировать на шлюзах сертификаты: сертификат CA (УЦ), локальный сертификат.

Настройка шлюза безопасности GW1

Регистрация CA сертификата (сертификата УЦ)

Для регистрации CA сертификата (сертификата УЦ) необходимо выполнить следующие действия:

1. Установите правильное системное время

   Например:

   date 070414282012

   Что соответствует 4 июля 2012 года 14:28.

2. Доставьте файл CA сертификата на шлюз безопасности в предварительно созданный на нем каталог /certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, применив команду:

   pscp <CA file path><CA file name> root@<gate address>:/certs

   Например:

   pscp D:\ca.cer root@192.168.1.1:/certs

3. С помощью утилиты cert_mgr, входящей в состав продукта, зарегистрируйте сертификат в базе продукта:

   [root@GW1 /]# cert_mgr import -f /certs/ca.cer -t

   Параметр –t в данной команде указывает на то, что импортируемый сертификат – корневой (сертификат УЦ).

Регистрация локального сертификата

Для регистрации локального сертификата в базе продукта выполните следующие действия:

1. Сформируйте запрос на сертификат при помощи утилиты cert_mgr.

```
[root@GW1 /]# cert_mgr create -subj "C=RU,OU=Sales,CN=GW1" -
GOST_R3410EL

Press keys...

[.......................................]


-----BEGIN CERTIFICATE REQUEST-----

MIIBBzCBtQIBADArMQswCQYDVQQGEwJSVTEOMAwGA1UECxMFU2FsZXMxDDAK

BgNVBAMTA0dXMTBjMBwGBiqFAwICEzASBgcqhQMCAiMBBgcqhQMCAh4BA0MA

BEC/os2KuckK6BdcdEtKbgixrMcUUa+8DqWn4eXwwtHbArCxHZBazjVjPkzH

8iXV8D+nqRcPGJ2mJRkaa1NUZthOoB4wHAYJKoZIhvcNAQkOMQ8wDTALBgNV

HQ8EBAMCB4AwCgYGKoUDAgIDBQADQQA9JLnfZBNAuuwCTSa2K6AVdPLIQMVX

UWiTeLhW9zoT0BSX7Kc8u4eXyAdUQJ6koa6TTRBc9nPXOi6AolFMneRv

-----END CERTIFICATE REQUEST-----
```

2. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в Документации на продукт (Приложение, раздел «Создание локального сертификата»).
3. Перенесите полученный файл на шлюз безопасности (параметры pscp описаны выше):

```
pscp gw1.cer root@192.168.1.1:/certs
```

4. Зарегистрируйте локальный сертификат в базе продукта, применив утилиту cert_mgr.

```
[root@GW1 /]# cert_mgr import -f /certs/gw1.cer
1 OK C=RU,OU=Sales,CN=GW1
```

5. Убедитесь, что сертификаты импортированы успешно:

```
[root@GW1 /]# cert_mgr show
Found 2 certificates. No CRLs found.
1 Status: trusted 1.2.840.113549.1.9.1=presale@s-
terra.com,C=RU,L=Moscow,O=S-Terra CSP,OU=Presale,CN=PresaleCA
2 Status: local   C=RU,OU=Sales,CN=GW1
```

Дополнительные настройки

После регистрации сертификатов необходимо создать политику безопасности для GW1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль перейдите в директорию /opt/VPNagent/bin/ и запустите cs_console.

```
[root@GW1 /]# cs_console
GW1>en
Password:
```

Пароль по умолчанию: csp. ВАЖНО: пароль по умолчанию нужно сменить.

Перейдите в режим настройки:

```
GW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GW1(config)#
```

Смена пароля по умолчанию осуществляется при помощи команды:

```
GW1(config)#username cscons password <пароль>
```

В настройках интерфейсов задайте ip-адреса, если этого не было сделано раньше:

```
GW1 (config)#interface FastEthernet0/0
GW1 (config-if)#ip address 192.168.13.112 255.255.255.0
GW1 (config-if)#no shutdown
GW1 (config-if)#exit
GW1 (config)#interface FastEthernet0/1
GW1 (config-if)#ip address 192.168.1.5 255.255.255.0
GW1 (config-if)#no shutdown
GW1 (config-if)#exit
```

Задайте адрес шлюза по умолчанию:

```
GW1 (config)#ip route 0.0.0.0 0.0.0.0 192.168.13.15
```

Отключите обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-terra_technological_trustpoint
GW1(ca-trustpoint)# revocation-check none
```

```
GW1(ca-trustpoint)#exit
```

Отредактируйте файл /opt/VPNagent/bin/cs_conv.ini так, как показано ниже:

```
ike-group-vko        = VKO_1B
ike-group-1          = VKO_1B
ike-group-2          = VKO_1B
```

Настройка устройства GW1 завершена. При выходе из конфигурационного режима происходит загрузка конфигурации.

В Приложении представлен текст cisco-like конфигурации и текст LSP для GW1.

Настройка шлюза GW2

Настройка шлюза безопасности GW2 происходит аналогично настройке устройства GW1, с заменой IP-адресов в соответствующих разделах конфигурации.

В Приложении представлен текст cisco-like конфигурации и текст LSP для GW2.

Настройка устройства Host1

На устройстве Host1 в качестве шлюза по умолчанию нужно указать адрес внутреннего интерфейса шлюза безопасности GW1 – 192.168.1.5.

Настройка устройства Host2

На устройстве Host2 в качестве шлюза по умолчанию нужно указать адрес внутреннего интерфейса шлюза безопасности GW2 – 192.168.0.5.

Создание защищенного туннеля между шлюзами при помощи Cisco Security Manager 4.3

Запуск Cisco Security Manager

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

Рисунок 2

Подключение CSP VPN Gate к CSM

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

- В появившемся окне `New Device - Choose Method` выберите предложение `Add Device From Network` и нажмите `Next`.

- В следующем окне `New Device - Device Information` (Рисунок 3) в разделе `Identity` введите:

  `Host Name` – `GW1`,

  `IP-Address` – `192.168.13.112`,

  `OS Type` – `IOS 12.3+`

  `Transport Protocol` – `SSH`

  В разделе `Discover Device Settings` выберите `Discover` – `Policies and Inventory` и установите флажок `Platform Settings`.

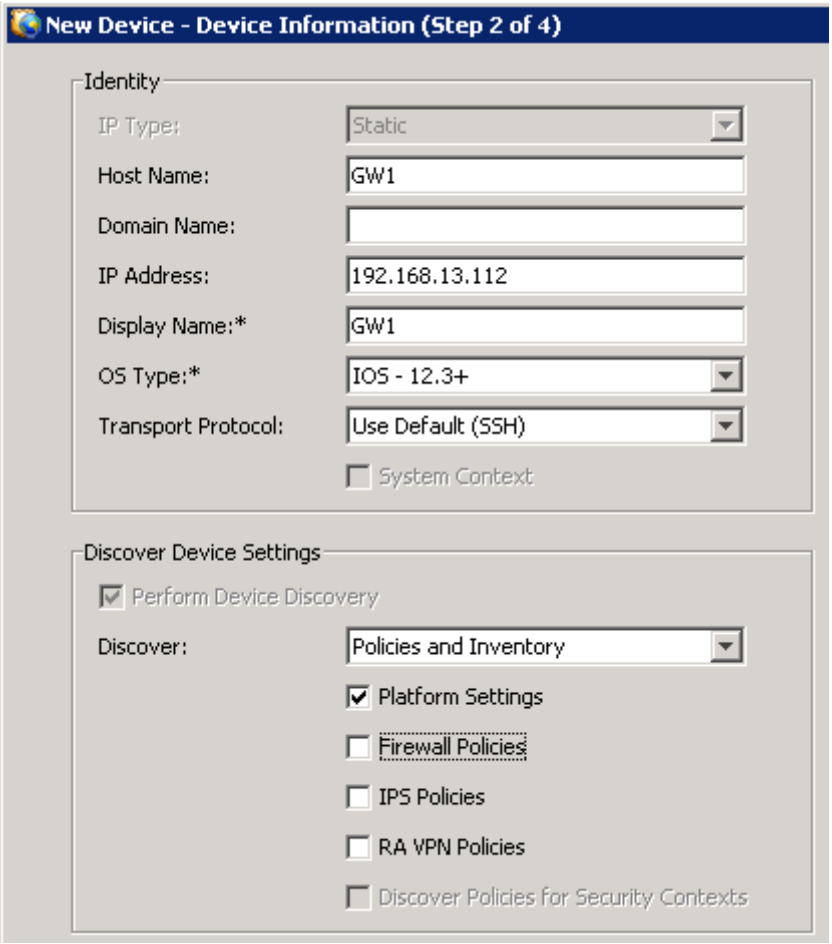

Рисунок 3

Нажмите `Next`.

- В окне `New Device - Device Credentials` (Рисунок 4) в разделе `Primary Credentials` введите:

  `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` оставьте рекомендуемые настройки.

  Нажмите `Next`.

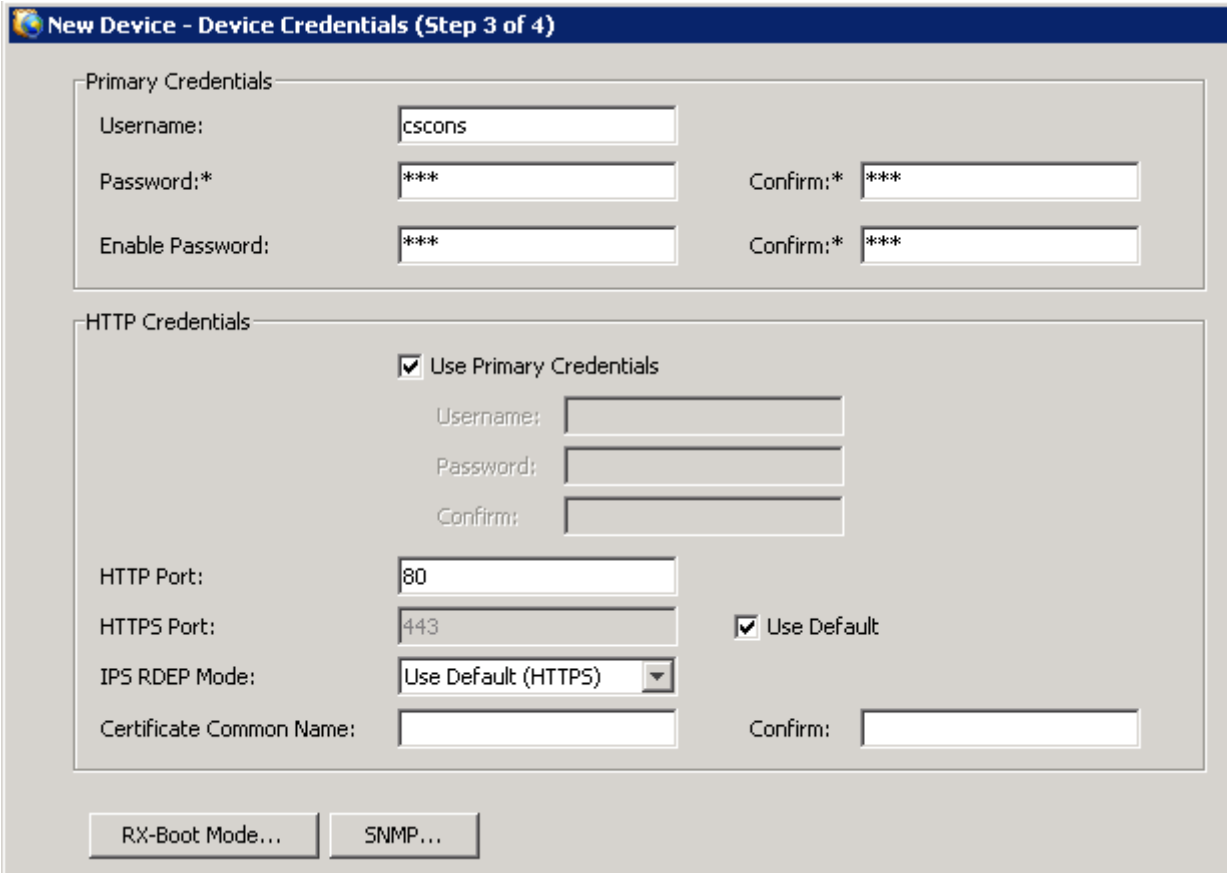

Рисунок 4

- Согласитесь с созданием нового тикета (Рисунок 5).

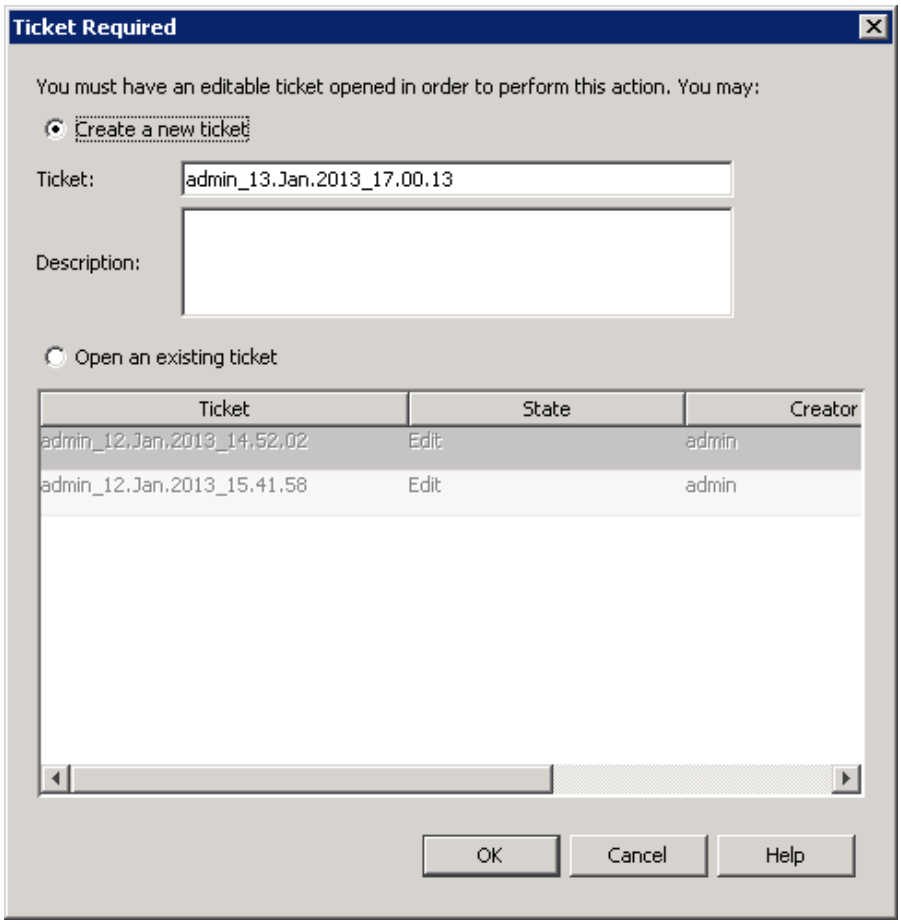

Рисунок 5

- Во время процесса обнаружения устройства появится предупреждение (Рисунок 6), нажмите `OK`.

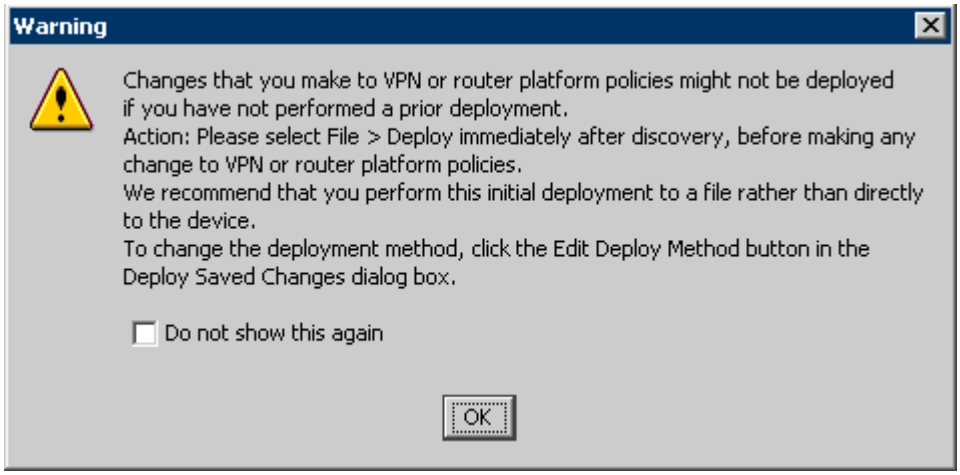

Рисунок 6

- Для сохранения настроек в меню верхней панели нажмите **Ticket–>Submit Ticket**.

Аналогично добавьте новое устройство CSP VPN Gate, присвоив ему:

`Host Name` – `GW2`,

`IP-Address` – `192.168.13.78`,

Далее, чтобы применить сделанные изменения выберите в меню верхней панели **File–>Deploy…**.

В появившемся окне `Deploy Saved Changes` отметьте добавленные шлюзы безопасности GW1 и GW2, нажмите `Deploy`.

Устройства готовы к настройке.

Описание топологии сети

В меню верхней панели выберите **Manage>Site-to-Site VPNs…**

В появившемся окне `Site-to-Site VPN Manager` нажмите `Create a VPN Topology` («+» сверху, в левой панели) и выберите топологию создаваемой защищенной сети – `Point-to-Point VPN`.

Появится окно `Create Point to Point VPN` (Рисунок 7), в котором укажите:

имя создаваемого vpn-соединения – `s-terra_vpn`

`IPSec Technology` – `Regular IPSec`

`IKE Version` – `IKE v1`

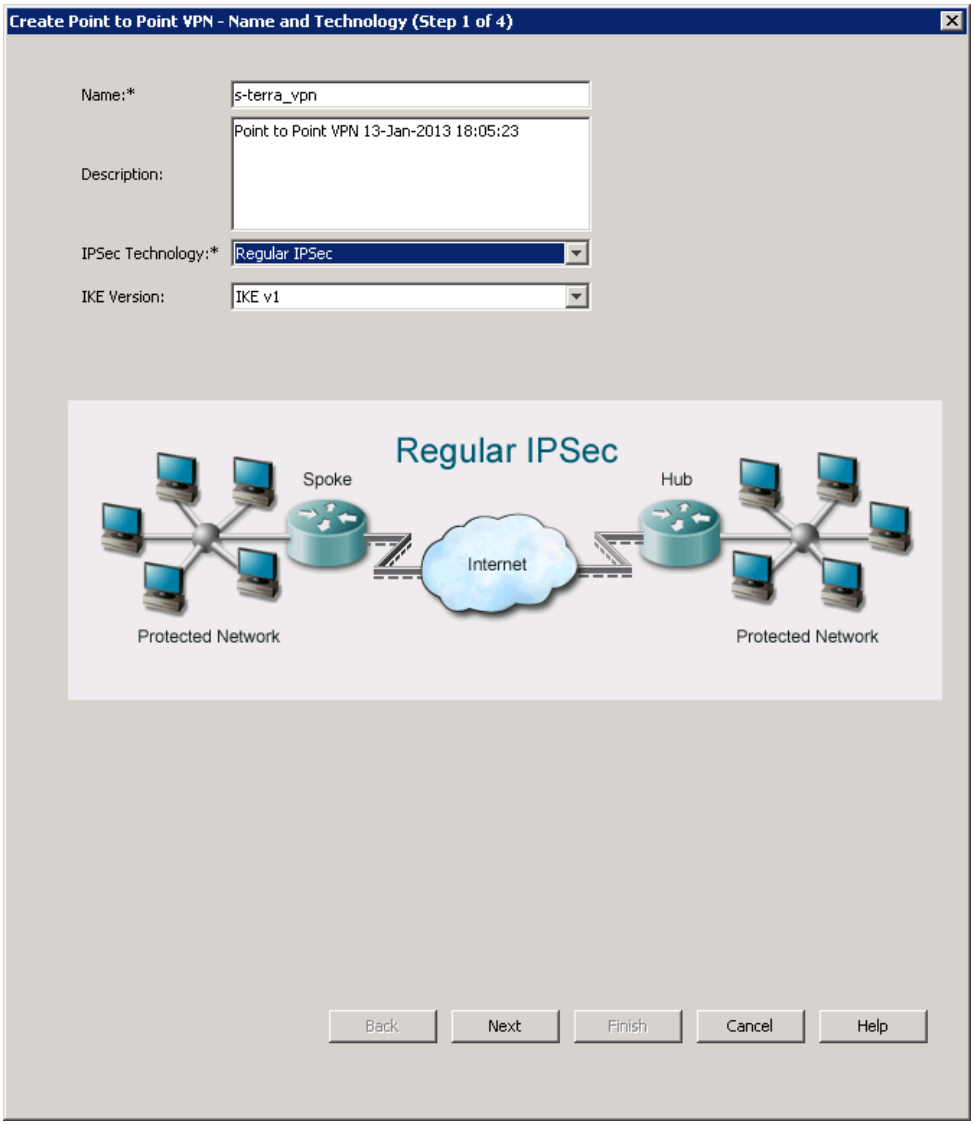

Рисунок 7

Выберите устройства, между которыми будет создаваться защищенное соединение (Рисунок 8).

Поместите, используя кнопку `>>`, `GW1` в поле `Peer One`, а `GW2` в поле `Peer Two`. Нажмите `Next`.

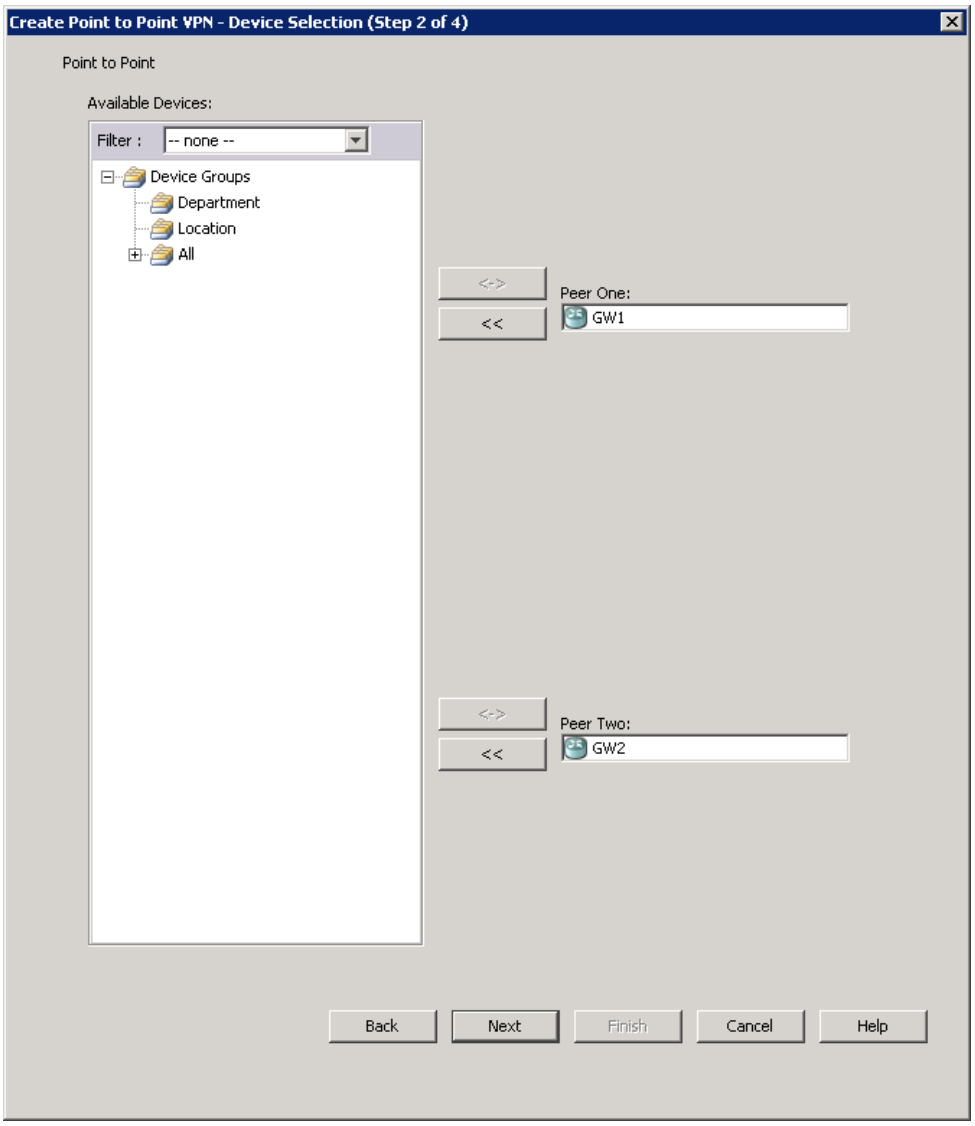

Рисунок 8

Затем для каждого устройства отредактируйте параметры соединения (Рисунок 9). Выберите устройство и нажмите правую кнопку мыши или значок внизу окна.

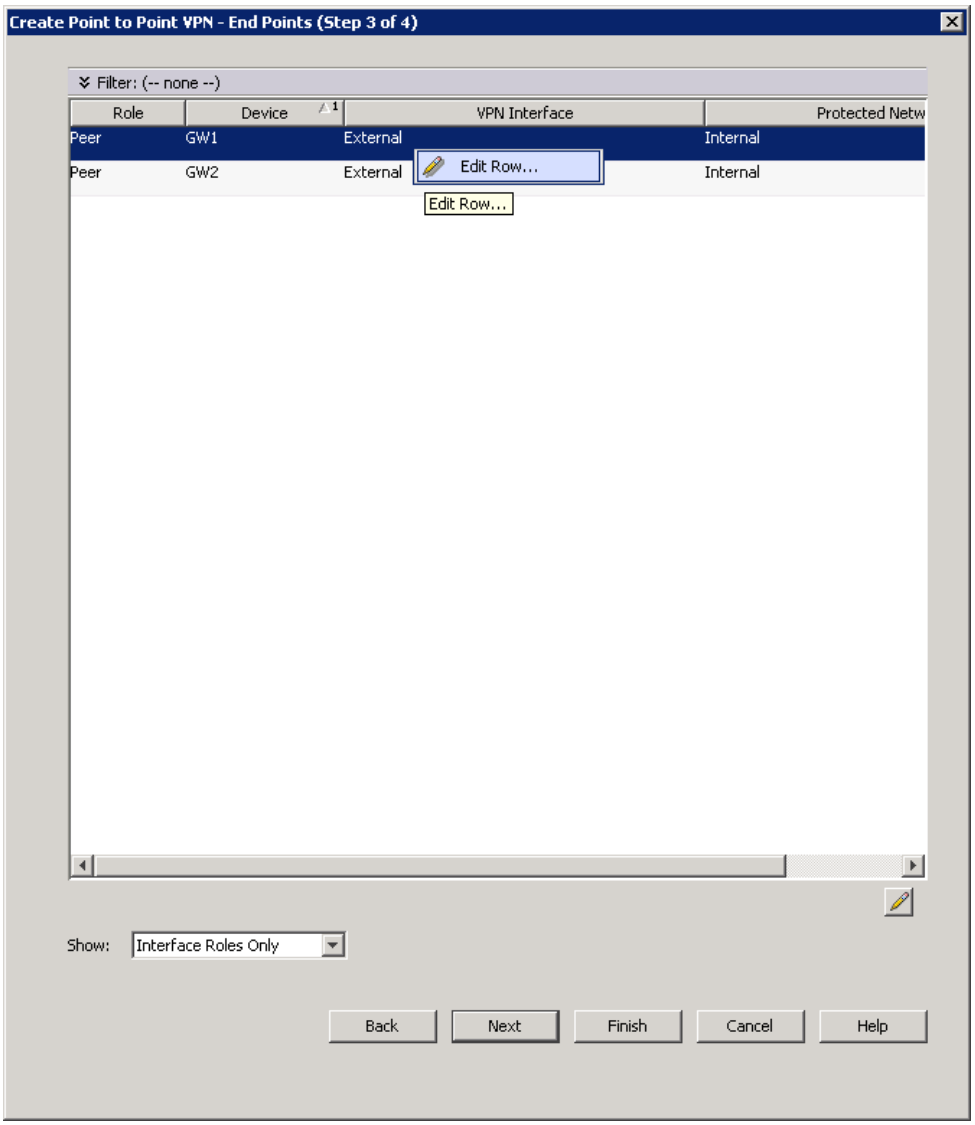

Рисунок 9

В окне `Edit Endpoints for Device GW1` (Рисунок 10) во вкладке `VPN Interface` для поля `VPN Interface` нажмите кнопку `Select`. В открывшемся окне `Interface Selector` выберите `FastEthernet0/0`.

Установите переключатель `Peer IP Address` в положение `VPN Interface IP Address`.

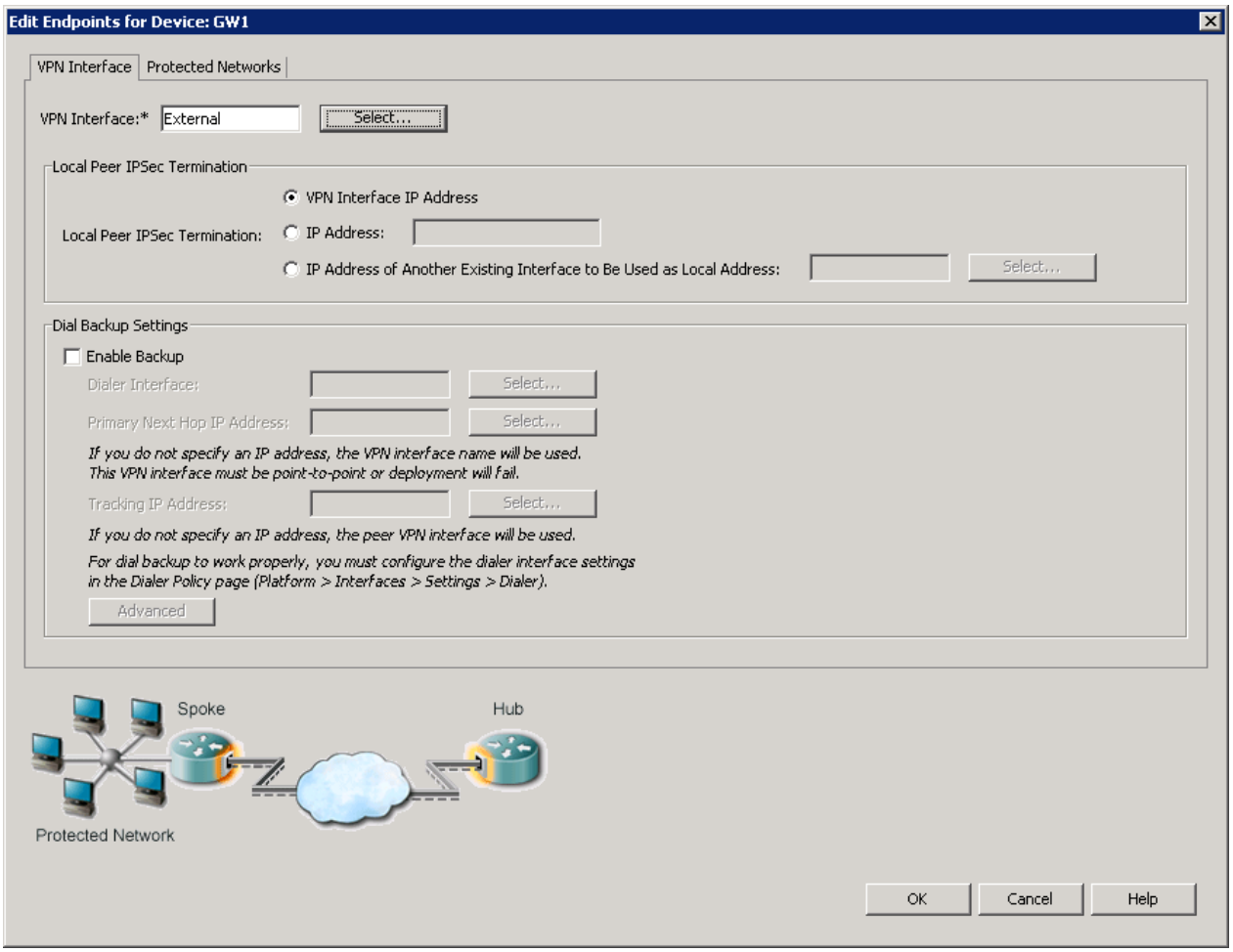

Рисунок 10

Перейдите на вкладку `Protected Networks` (Рисунок 11) и выберите интерфейс из защищаемой сети:

для Protected Networks укажите FastEthernet0/1.

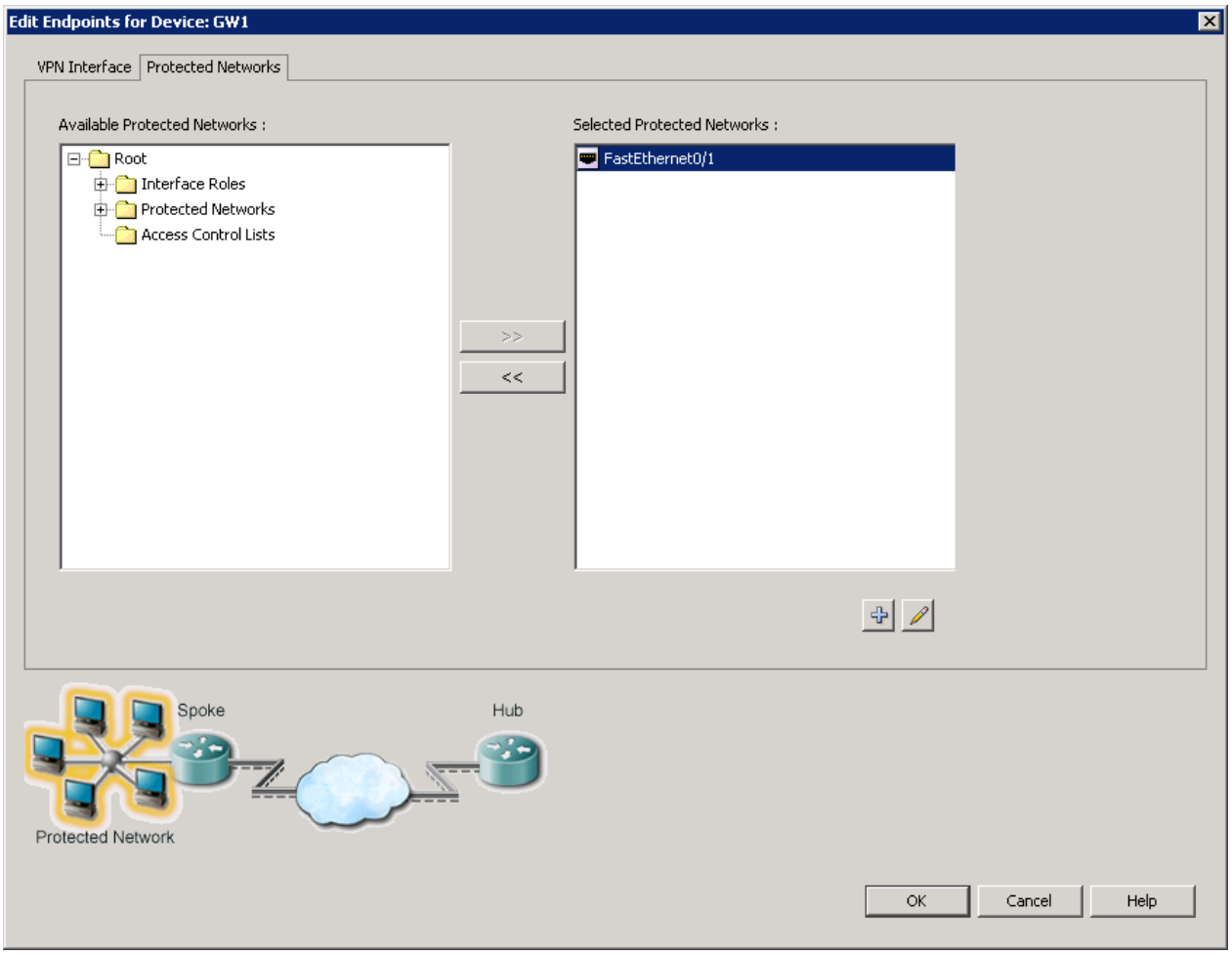

Рисунок 11

Повторите процедуру по выбору шифрующих и защищаемых интерфейсов для шлюза GW1. Полученный результат показан на Рисунок 12.

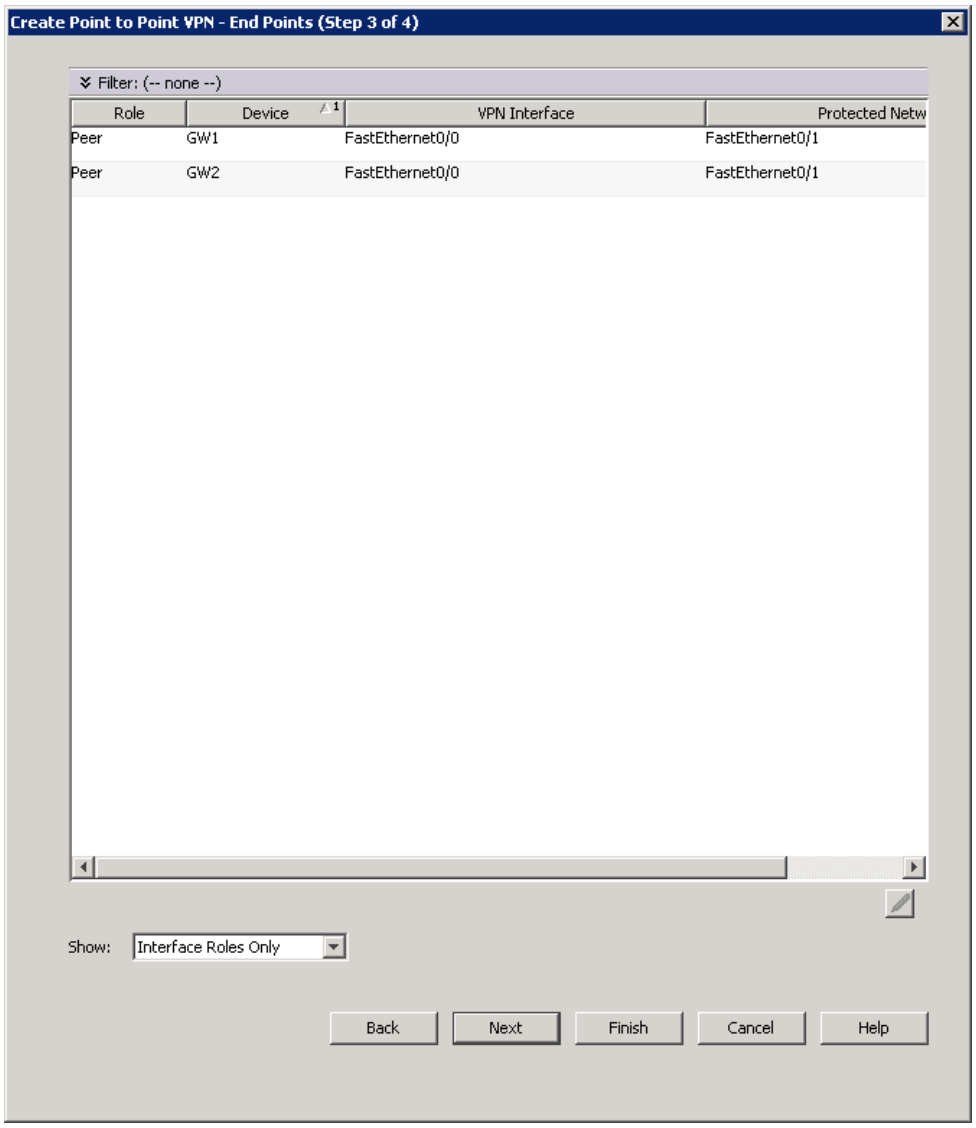

Рисунок 12

Нажмите кнопку `Finish`.

Далее перейдем к настройке IKE политики.

Настройка IKE политики

В окне `Site-to-Site VPN Manager` в панеле слева в разделе `Policies` выберите `IKE Proposal`. Для выбора значения Ikev1 Proposals нажмите кнопку `Select` (Рисунок 13).

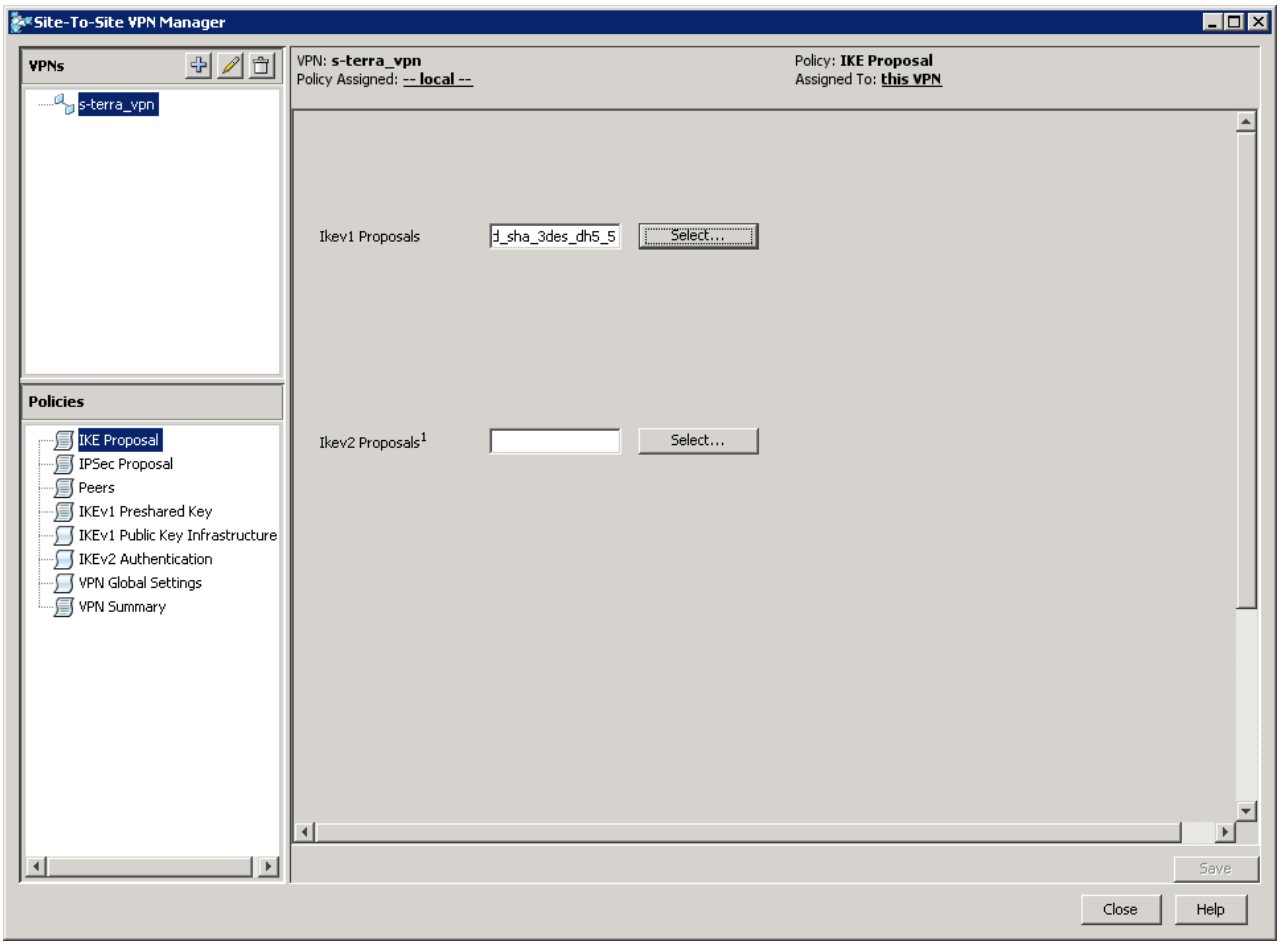

Рисунок 13

В появившемся окне `IKE Proposal Selector` (Рисунок 14) нажмите на кнопку «+».

В окне `Add IKEv1 Proposal` настройте параметры IKE политики: выберите алгоритмы шифрования и аутентификации; метод аутентификации; группу Diffie-Hellman; установите время жизни SA (Рисунок 15):

- из списка `Encryption Algorithm` выберите значение des, которое будет интерпретироваться CSP VPN Gate как алгоритм шифрования ГОСТ 28147-89;
- из списка `Hash Algorithm` выберите значение MD5, которое будет интерпретироваться CSP VPN Gate как алгоритм хеширования ГОСТ Р 34.11-94;
- укажите `Modulus Group` – 2 (VKO GOST R 34.10-2001);
- задайте значение `Lifetime` – 3600 сек;
- из списка `Authentication Method` выберите Certificate.

Нажмите `OK`. В окне `IKE Proposal Selector` (Рисунок 14) выберите созданный IKE Proposal.

В окне `Site-to-Site VPN Manager` нажмите `Save` и перейдите к настройке IPSec политики.

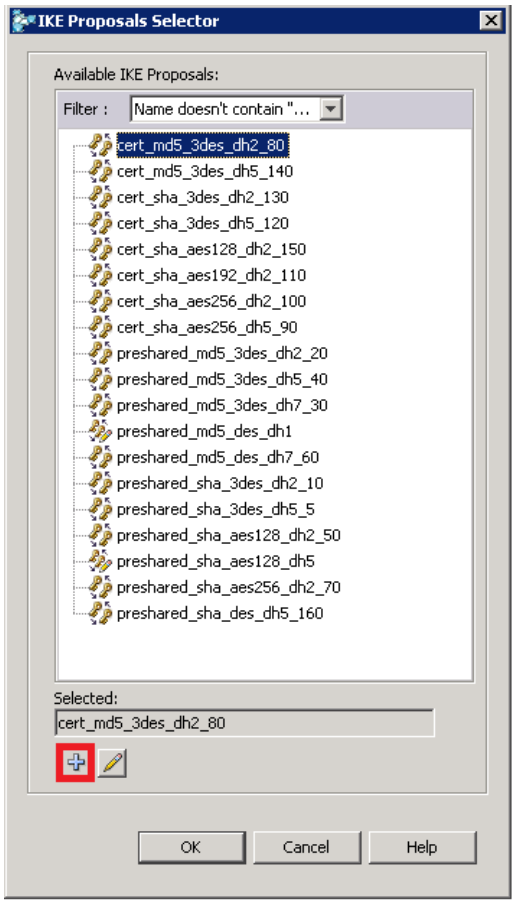

Рисунок 14

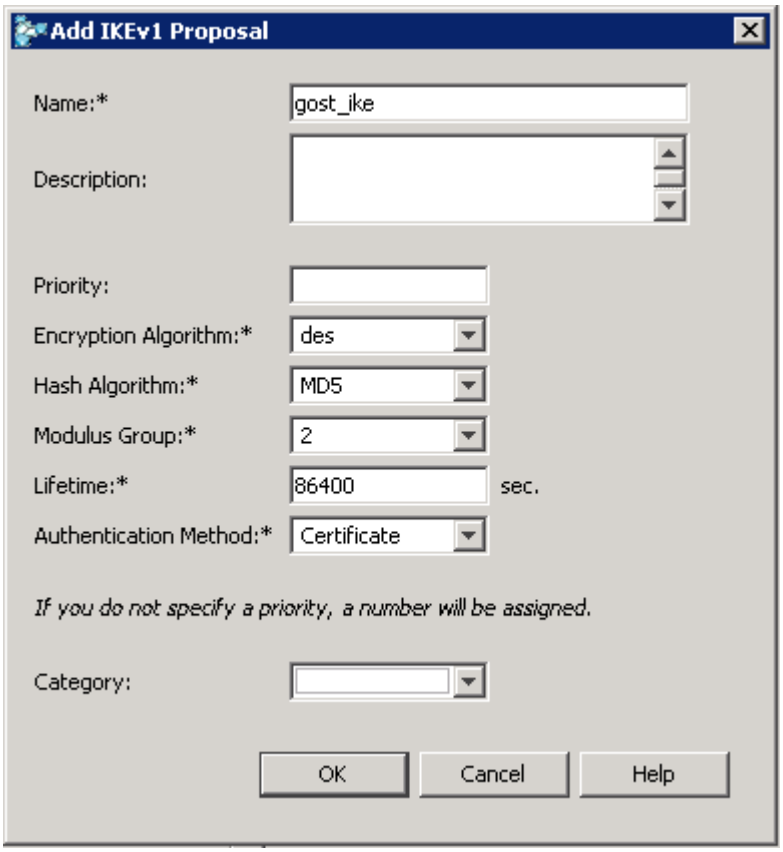

Рисунок 15

Настройка IPSec политики

В окне `Site-to-Site VPN Manager` в панеле слева в разделе `Policies` выберите `IPSec Proposal`.

В появившемся окне (Рисунок 16) установите:

- флажок `Enable Ike1`;
- `Lifetime` – 3600 сек.;
- `Lifetime` – 4608000 kbytes;
- `Reverse Route` – Standard.

Чтобы выбрать `Transform Set` нажмите кнопку `Select`.

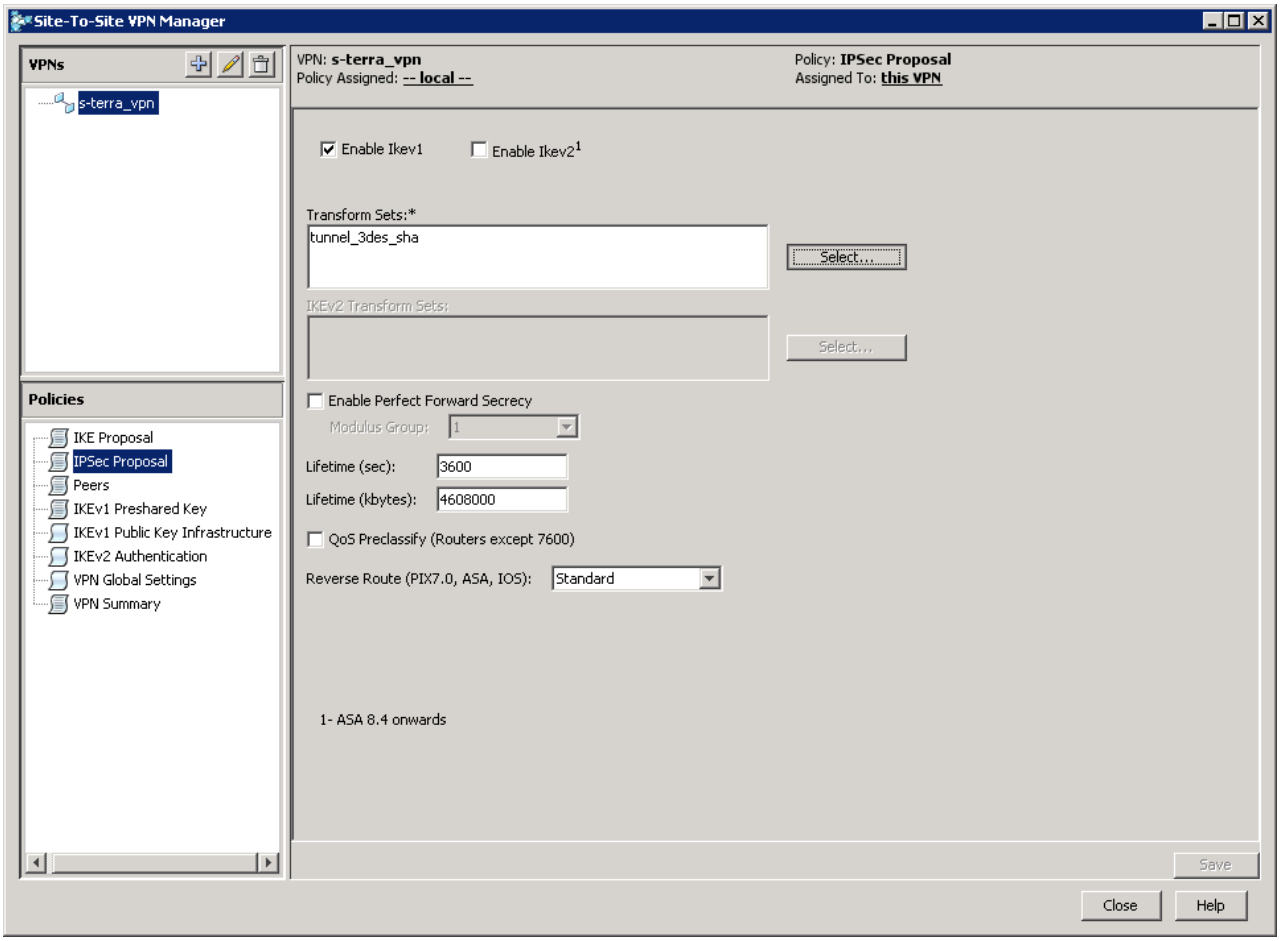

Рисунок 16

Появится окно `IPSec IKEv1 Transform Sets Selector` (Рисунок 17). В поле `Selected IPSec IKEv1 Transform Sets` установите набор преобразований `tunnel_des_md5`.

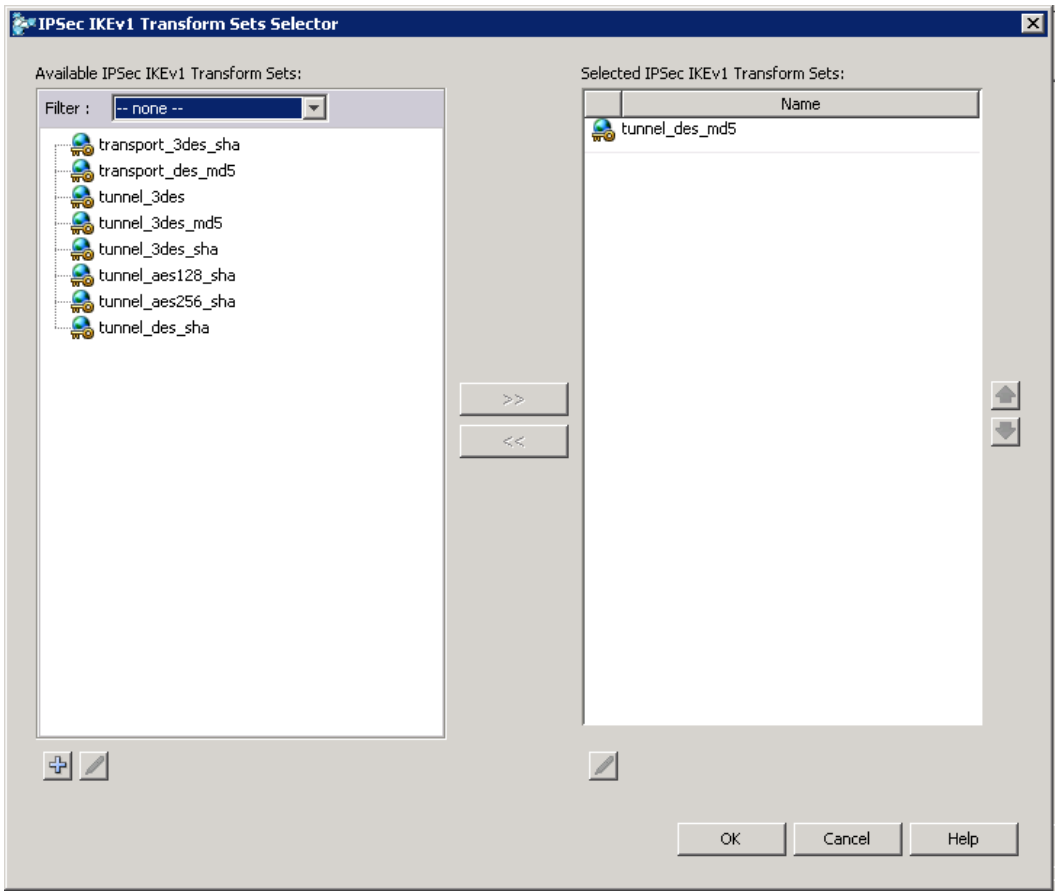

Рисунок 17

В окне `Site-to-Site VPN Manager` нажмите `Save`.

VPN Summary

В окне `Site-to-Site VPN Manager` в панеле слева в разделе `Policies` выберите `VPN Summary`. Здесь можно посмотреть основные установленные VPN параметры (Рисунок 18)

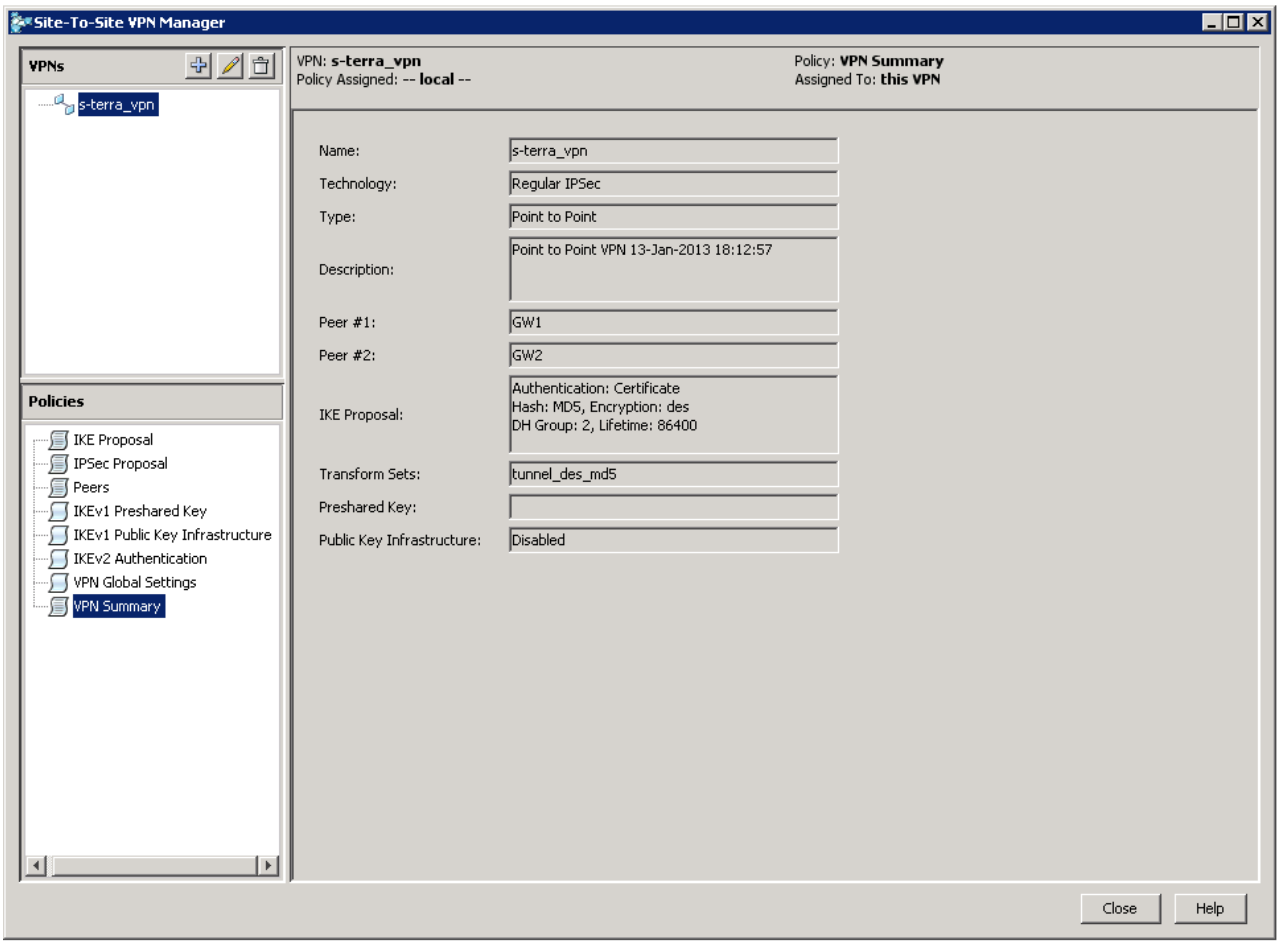

Рисунок 18

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

В окне `Site-to-Site VPN Manager` нажмите `Close` и, чтобы сохранить внесенные изменения, в меню на верхней панели нажмите **Tickets -> Submit Ticket**.

Настройка глобальных параметров

На верхней панели нажмите `Device`, слева в разделе `Devices` выберите шлюз безопасности, в разделе `Policies` разверните `Remote Access VPN > Global Settings` (Рисунок 19).

Во вкладке `ISAKMP/IPSec Settings` установите значение параметра `Identity*` в `Distinguished Name`.

Проделайте аналогичную операцию для второго шлюза безопасности.

Чтобы сохранить внесенные изменения, в меню на верхней панели нажмите **Tickets -> Submit Ticket**.

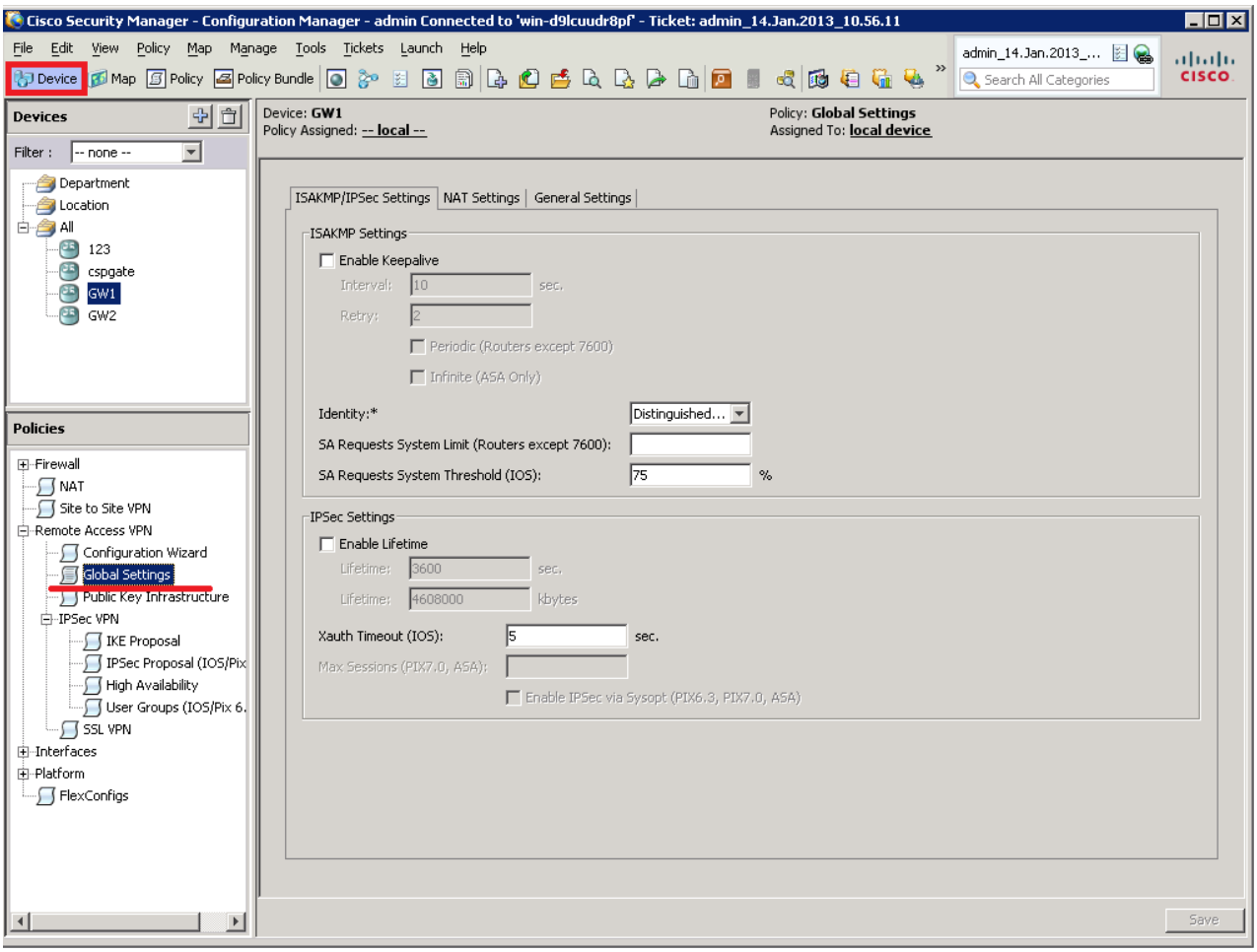

Рисунок 19

Доставка конфигурации на устройство

В меню на верхней панели выберите **File -> Deploy…**. Будет предложено выбрать устройства, на которые будет доставляться конфигурация. CSM автоматически определяет устройства, для которых были сделаны изменения, но конфигурация на которые не была загружена.

Отметьте добавленные шлюзы безопасности и нажмите `Deploy`.

Будет выполнена попытка загрузить конфигурацию на устройство. Если конфигурация будет доставлена на устройство успешно, то выдается соответствующее сообщение (Рисунок 20), в случае неудачи – будет выдано сообщение об ошибке.

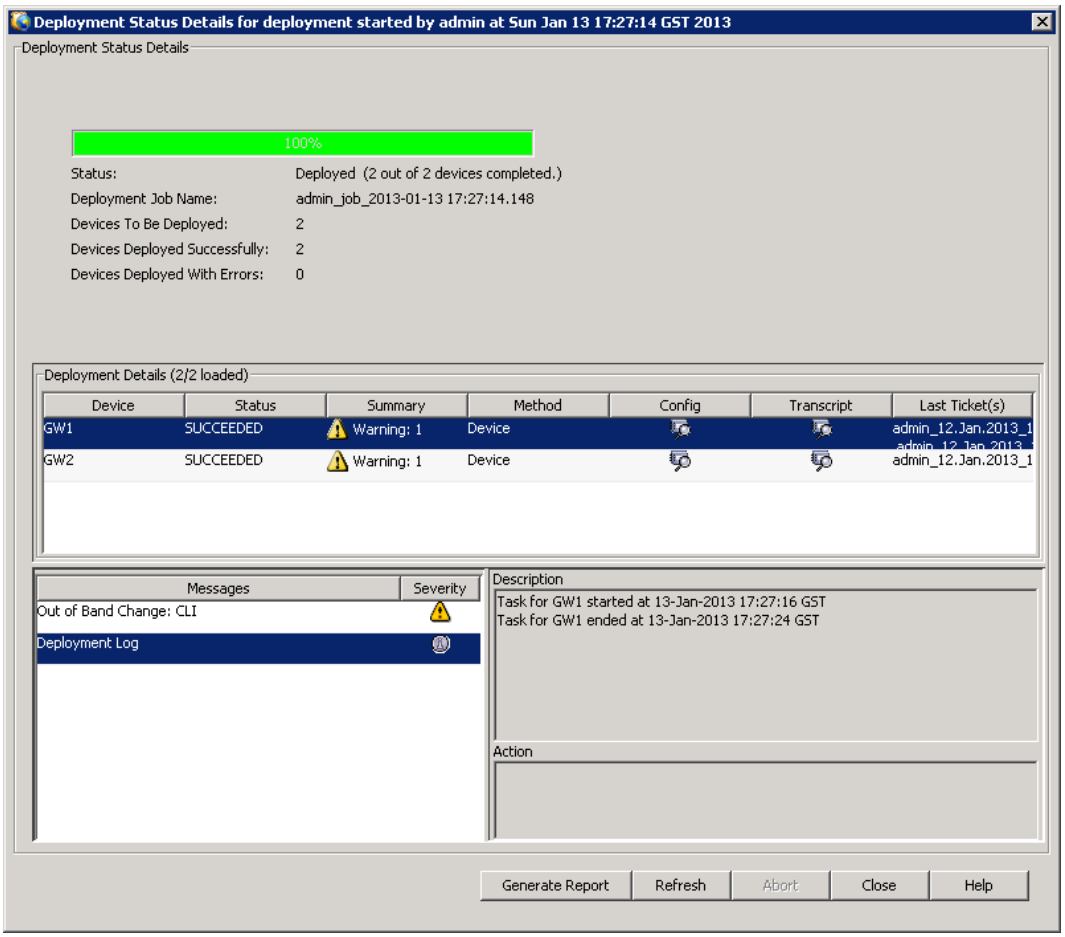

Рисунок 20

Проверка работоспособности стенда

После того, как все настройки завершены, инициируйте создание защищенного соединения.

На Host1 выполните команду:

```
ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10): 56 data bytes
64 bytes from 192.168.0.10: icmp_seq=0 ttl=61 time=1201.3 ms
64 bytes from 192.168.0.10: icmp_seq=1 ttl=61 time=2.8 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=61 time=1.3 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=61 time=1.6 ms
```

В результате выполнения этой команды между устройствами GW1 и GW2 будет установлен VPN туннель.

Убедиться в этом можно, выполнив на устройстве GW1 команду:

```
[root@GW1 /]# sa_mgr show

ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
```

Num Conn-id (Remote Addr,Port)-(Local Addr,Port) State Sent Rcvd

1 18 (192.168.13.78,500)-(192.168.13.112,500) active 1759 1715

IPsec connections:

Num Conn-id (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type Sent Rcvd

1 2 (192.168.0.0-192.168.0.255,*)-(192.168.1.0-192.168.1.255,*) * ESP tunn 176 176

Согласно созданной политике безопасности весь трафик между сетями SN1 и SN2 будет зашифрован. Прохождение остального трафика будет разрешено, но защищаться шифрованием не будет.

Приложение

Текст cisco-like конфигурации для устройства GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp keepalive 10
username cscons privilege 15 password 0 csp
hostname GW1
enable password csp
ip domain name s-terra
!
crypto isakmp policy 31
 hash md5
 encr des
 group 2
!
crypto ipsec transform-set CSM_TS_1 esp-des esp-md5-hmac
!
ip access-list extended CSM_IPSEC_ACL_1
 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
!
crypto map CSM_CME_FastEthernet0/0 2 ipsec-isakmp
 match address CSM_IPSEC_ACL_1
 set transform-set CSM_TS_1
 set peer 192.168.13.78
 reverse-route
!
interface FastEthernet0/0
 ip address 192.168.13.112 255.255.255.0
 crypto map CSM_CME_FastEthernet0/0
!
interface FastEthernet0/1
 ip address 192.168.1.5 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.13.15
!
```



```
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 50DB2211454963AC4DA770AC855D607E
3082028A30820239A003020102021050DB2211454963AC4DA770AC855D607E30
…
F6A3D58BA218B621D2B6F403477F

quit
!
end
```

Текст LSP для устройства GW1

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Thu Feb 14 11:22:43 2013

GlobalParameters(
   Title                    = "This LSP was automatically generated by CSP Converter at Thu Feb 14
11:22:43 2013"
   Version                  = "3.1"
   CRLHandlingMode          = OPTIONAL
   LDAPLogMessageLevel      = DEBUG
   SystemLogMessageLevel    = DEBUG
   PolicyLogMessageLevel    = DEBUG
   CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
   Server = 127.0.0.1
   Facility = LOG_LOCAL7
)

RoutingTable(
   Routes *=
      Route(
         Destination = 0.0.0.0/0
         Gateway = 192.168.13.15
         Metric = 1
      )
```

```
)
IKETransform IKETransform_31
(
   CipherAlg   *= "G2814789CPRO1-K256-CBC-65534"
   HashAlg     *= "GR341194CPRO1-65534"
   GroupID     *= VKO_1B
   LifetimeSeconds = 86400
)

ESPProposal ESP_CSM_TS_1
(
   Transform* = ESPTransform
   (
      IntegrityAlg*       = "GR341194CPRO1-H96-HMAC-65534"
      CipherAlg*          = "G2814789CPRO1-K256-CBC-254"
      LifetimeSeconds     = 3600
      LifetimeKilobytes   = 4608000
   )
)

CertDescription ca
(
   Issuer          *= "1.2.840.113549.1.9.1=vnovikov@s-
terra.com,C=RU,L=\d0\97\d0\b5\d0\bb\d0\b5\d0\bd\d0\be\d0\b3\d1\80\d0\b0\d0\b4,O=S-terra
CSP,OU=IT department,CN=S-terra CSP Root CA"
   SerialNumber     =  "50db2211454963ac4da770ac855d607e"
   Subject         *= "1.2.840.113549.1.9.1=vnovikov@s-
terra.com,C=RU,L=\d0\97\d0\b5\d0\bb\d0\b5\d0\bd\d0\be\d0\b3\d1\80\d0\b0\d0\b4,O=S-terra
CSP,OU=IT department,CN=S-terra CSP Root CA"
)

AuthMethodGOSTSign auth_ca
(
   LocalID        =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
   DoNotMapRemoteIDToCert = TRUE
   AcceptCredentialFrom      *= ca
   SendRequestMode    =  ALWAYS
   SendCertMode       =  ALWAYS
)

IKERule IKE_CSM_CME_FastEthernet0_0_2
(
```

```
    Transform* = IKETransform_31
    AggrModeAuthMethod  *= auth_ca
    MainModeAuthMethod  *= auth_ca
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
    DPDResponseDuration = 2
    DPDRetries          = 5
)

IPsecAction CSM_CME_FastEthernet0_0_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.13.78

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_CSM_TS_1 )
    ReverseRoute = TRUE
    IKERule = IKE_CSM_CME_FastEthernet0_0_2
)

FilteringRule Filter_nil_acl_CSM_CME_FastEthernet0_0_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.0.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CSM_CME_FastEthernet0_0_2 )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth0"
    Action *= ( PASS )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
```

```
    NetworkInterfaces *= "eth1"
    Action *= ( PASS )
)
```

Текст cisco-like конфигурации для устройства GW2

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp keepalive  10
username cscons privilege 15 password 0 csp
hostname GW2
enable password csp
ip domain name s-terra
!
crypto isakmp policy 36
 hash md5
 encr des
 group 2
!
crypto ipsec transform-set CSM_TS_1 esp-des esp-md5-hmac
!
ip access-list extended CSM_IPSEC_ACL_1
 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
crypto map CSM_CME_FastEthernet0/0 1 ipsec-isakmp
 match address CSM_IPSEC_ACL_1
 set transform-set CSM_TS_1
 set peer 192.168.13.112
 reverse-route
!
interface FastEthernet0/0
 ip address 192.168.13.78 255.255.255.0
 crypto map CSM_CME_FastEthernet0/0
!
interface FastEthernet0/1
```



```
 ip address 192.168.0.5 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.13.15
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 50DB2211454963AC4DA770AC855D607E
3082028A30820239A003020102021050DB2211454963AC4DA770AC855D607E30
…
F6A3D58BA218B621D2B6F403477F

quit
!
End
```

Текст LSP для устройства GW2

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Thu Feb 14 04:43:50 2013

GlobalParameters(
   Title                    = "This LSP was automatically generated by CSP Converter at Thu Feb 14
04:43:50 2013"
   Version                  = "3.1"
   CRLHandlingMode          = OPTIONAL
   LDAPLogMessageLevel      = DEBUG
   SystemLogMessageLevel    = DEBUG
   PolicyLogMessageLevel    = DEBUG
   CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
   Server = 127.0.0.1
   Facility = LOG_LOCAL7
)

RoutingTable(
   Routes *=
      Route(
```

```
            Destination = 0.0.0.0/0
            Gateway = 192.168.13.15
            Metric = 1
        )
)
IKETransform IKETransform_36
(
    CipherAlg   *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg     *= "GR341194CPRO1-65534"
    GroupID     *= VKO_1B
    LifetimeSeconds = 86400
)

ESPProposal ESP_CSM_TS_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "GR341194CPRO1-H96-HMAC-65534"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4608000
    )
)

CertDescription ca
(
    Issuer          *= "1.2.840.113549.1.9.1=vnovikov@s-
terra.com,C=RU,L=\d0\97\d0\b5\d0\bb\d0\b5\d0\bd\d0\be\d0\b3\d1\80\d0\b0\d0\b4,O=S-terra
CSP,OU=IT department,CN=S-terra CSP Root CA"
    SerialNumber     =  "50db2211454963ac4da770ac855d607e"
    Subject          *= "1.2.840.113549.1.9.1=vnovikov@s-
terra.com,C=RU,L=\d0\97\d0\b5\d0\bb\d0\b5\d0\bd\d0\be\d0\b3\d1\80\d0\b0\d0\b4,O=S-terra
CSP,OU=IT department,CN=S-terra CSP Root CA"
)

AuthMethodGOSTSign auth_ca
(
    LocalID        =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    DoNotMapRemoteIDToCert = TRUE
    AcceptCredentialFrom      *= ca
    SendRequestMode    =  ALWAYS
    SendCertMode       =  ALWAYS
```

```
)

IKERule IKE_CSM_CME_FastEthernet0_0_1
(
   Transform* = IKETransform_36
   AggrModeAuthMethod  *= auth_ca
   MainModeAuthMethod  *= auth_ca
   DoAutopass          = TRUE
   DPDIdleDuration     = 10
   DPDResponseDuration = 2
   DPDRetries          = 5
)

IPsecAction CSM_CME_FastEthernet0_0_1
(
   TunnelingParameters *= TunnelEntry(
      PeerIPAddress = 192.168.13.112

      DFHandling=COPY
   )
   ContainedProposals *= ( ESP_CSM_TS_1 )
   ReverseRoute = TRUE
   IKERule = IKE_CSM_CME_FastEthernet0_0_1
)

FilteringRule Filter_nil_acl_CSM_CME_FastEthernet0_0_1
(
   LocalIPFilter *= FilterEntry( IPAddress *= 192.168.0.0/24 )
   PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.1.0/24 )
   NetworkInterfaces *= "eth0"
   Action *= ( CSM_CME_FastEthernet0_0_1 )
)

FilteringRule Filter_nil_acl
(
   LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
   PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
   NetworkInterfaces *= "eth0"
   Action *= ( PASS )
)
```

```
FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth1"
    Action *= ( PASS )
)
```