04.06.2009

Программные комплексы ”Шлюз безопасности CSP VPN Gate. Версия 3.0” и ”Шлюз безопасности CSP RVPN. Версия 3.0”

Руководство администратора

Конфигурирование с помощью CiscoWorks

Настройка шлюзов безопасности CSP VPN Gate и CSP RVPN производится одинаково, выполняют они одни и те же функции, поэтому в дальнейшем будем использовать только одно наименование – шлюз безопасности CSP VPN Gate или Продукт CSP VPN Gate, или Продукт.

В данном разделе будет описано удаленное централизованное конфигурирование шлюзов безопасности с помощью Cisco Works Management Center for VPN Routers версии 1.2, который входит в состав продукта CiscoWorks VPN/Security Management Solution версии 2.3.

Предполагается, что читатель имеет опыт работы с CiscoWorks, поэтому в данном документе не будут детально описаны все элементы графического интерфейса этого программного Продукта. В данном разделе будут описаны основные шаги, которые следует произвести для создания политики безопасности, а также особенности и ограничения, которые в данный момент существуют для конфигурирования CSP VPN Gate.

Особенности конфигурирования CSP VPN Gate

Все операции по конфигурированию CSP VPN Gate производятся в разделе графического интерфейса **Management Center for VPN Routers версии 1.2**.

Ниже описаны разделы графического интерфейса Router MC, которые имеют особенности при конфигурировании устройств типа CSP VPN Gate или же не поддерживаются в данной версии Продукта:

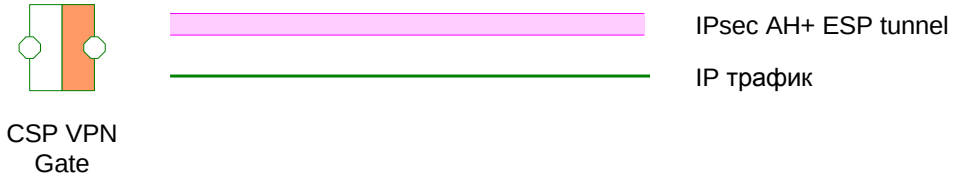
- Devices
  - Device Import
    Не рекомендуется изменять версию IOS у импортированных CSP VPN Gate. Все устройства серии CSP VPN при импорте представляются роутерами Cisco 2611XM с установленной операционной системой IOS v.12.2(13)T. Изменение версии IOS может привести к ошибкам в генерируемых конфигурациях.
  - Устройства типа CSP VPN Gate нельзя помещать в High Availability группы
- Configuration
  - Settings
    - General VPN
    - Failover and Routing – не поддерживается в данной версии
    - Fragmentation – не поддерживается в данной версии
    - General Firewall
    - Fragmentation Rules – не поддерживается в данной версии
    - Timeouts and Performance – не поддерживается в данной версии
    - Half Open Connection – не поддерживается в данной версии
    - Logging – не поддерживается в данной версии
    - ACL Ranges – не поддерживается в данной версии
    - Spoke
    - NAT Traversal – не поддерживается в данной версии
    - Hub Assignment
      В данной версии Продукта не поддерживается тип устройства failover hubs. Также не поддерживается указание в качестве Primary Hub объекта ‘HA group’.
  - Access Rules
    - Mandatory Rules
      При создании правил на этапе выбора интерфейса предлагается установить параметр Direct в положение In или Out. Для устройств CSP VPN Gate следует установить значение In. Значение Out не поддерживается. CSP VPN Gate не поддерживает асимметричные правила доступа, т.е. одинаково обрабатывает как входящий, так и исходящий трафик. Поэтому как входящий, так и исходящий трафик будут обрабатываться по списку доступа со значением In. При этом для исходящего трафика значения Source и Destination меняются местами.
    - Default Rules
      То же ограничение, что и для Mandatory Rules
  - IKE
    - IKE Policies
      - При создании IKE политики для устройств CSP VPN Gate следует обратить внимание на значения Encryption Algorithm и Hash Algorithm.

- CSP VPN Gate при выборе значения DES будет использовать алгоритм шифрования ГОСТ 28147-89, а при выборе значения MD5 будет использовать хэш-алгоритм ГОСТ Р 34.11-94.

- Dynamic Preshared Key – не поддерживается в данной версии
- CA Parameters
  - В данной версии CSP VPN Gate не поддерживается enrollment. Поэтому любые введенные значения будут игнорироваться. Однако, их следует заполнить, чтобы не спровоцировать ошибку в Router MC. Установите опцию CA URL и заполните параметры.
  - В данной версии Продукта не поддерживается получение CA сертификата по SCEP протоколу. Следует установить параметр ‘Enter Manually’ и ввести (через буфер обмена) сертификат в шестнадцатеричном формате.
  - В блоке настроек работы с CRL следует обратить внимание на формат ввода URL, по которому будут запрашиваться листы отозванных сертификатов (CRL). LDAP Server URL следует вводить в формате ldap://IPAddress:Port
  - При установке параметра CRL ‘Optional’ обработка CRL не производится.
    При установке параметров CRL ‘Best-Effort’ и ‘Enable’ включается обработка CRL, в том числе и по указанному LDAP URL. Если CRL не найден, то соединения, инициированные с использованием сертификатов, которые должны обрабатываться этим CRL, не будут созданы.
- Tunnels
  - Dynamic Crypto Policies
    - При описании динамических туннелей следует иметь ввиду, что CSP VPN Gate не поддерживает subinterfaces.
- Translation Rules - не поддерживается в данной версии
- Building Blocks
  - Transform Sets
    - При назначении или создании набора преобразований (transform set) следует учитывать что CSP VPN Gate при выборе значения DES будет использовать алгоритм шифрования ГОСТ 28147-89, а при выборе значения MD5 будет использовать хэш-алгоритм ГОСТ Р 34.11-94.
    - В данном релизе не поддерживается компрессия, поэтому флажок Compression должен быть снят.

Пример создания политики безопасности

Условные обозначения:



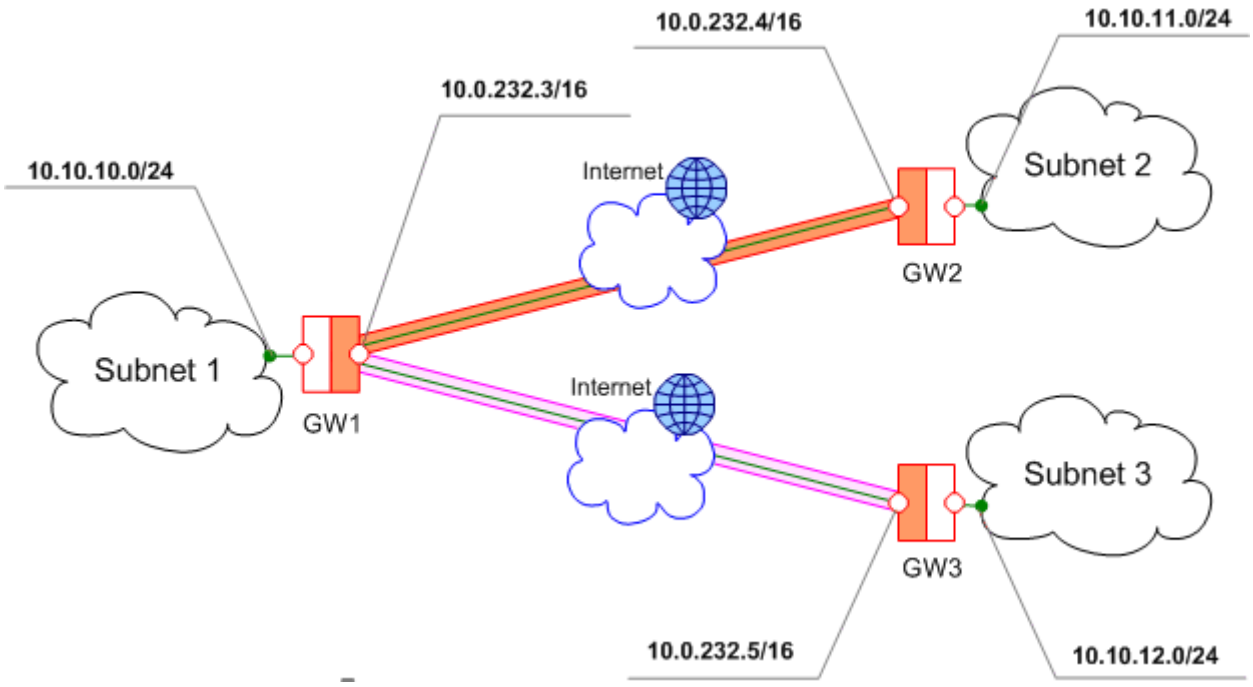


Рисунок 1

Сценарий

Три шлюза безопасности (CSP VPN Gate), защищающие участки корпоративной сети. IP-трафики между шлюзами безопасности GW1, GW2, GW3 защищены туннелями, работающими по протоколу AH и ESP. Аутентификация сторон осуществляется на предустановленных ключах. На внешних интерфейсах шлюзов безопасности GW1, GW2 и GW3 защита снимается. Трафик, приходящий на другие интерфейсы шлюза безопасности, пропускается открытым (незащищенным).

Параметры элементов проекта **Таблица**

Имя устройства	Модель устройства	Защищаемый ресурс	Тип устройства	Версия программного обеспечения	VPN интерфейс
GW1	CSP VPN Gate	Subnet1 = 10.10.10.0/24	Hub	Cisco IOS 12.2T*	10.0.232.3
GW2	CSP VPN Gate	Subnet2 = 10.10.11.0/24	Spoke	Cisco IOS 12.2T*	10.0.232.4
GW3	CSP VPN Gate	Subnet3 =10.10.12.0/24	Spoke	Cisco IOS 12.2T*	10.0.232.5

Создание политики безопасности средствами CiscoWorks предполагает выполнение следующих этапов:

- создание групп устройств. При построении рекомендуется создавать отдельные группы для устройств от Cisco Systems и для устройств CSP VPN Gate
- импорт устройств в созданные группы
- описание защищаемых устройствами ресурсов (подсетей и отдельно взятых хостов)
- настройка VPN параметров
- настройка IKE политики
- создание туннельной политики
- доставка конфигураций на Агенты Безопасности.

Запуск CiscoWorks

Запускаем интернет - браузер и указываем URL хоста, на котором установлен CiscoWorks. При написании URL указываем не 80 порт, а 1741.

Предъявляем логин и пароль администратора или пользователя, имеющего соответствующие права.

В левой части окна выбираем раздел VPN/Security Management Solution =>Management Center=>VPN Routers.

Попадаем в **Management Center for VPN Routers**. Все действия по конфигурированию системы будем производить в этом окне.

Создание групп устройств

Для реализации нашего примера нам потребуется создать группу устройств, в которую входят GW1, GW2 и GW3, защищающие периметры Subnet 1, Subnet 2 и Subnet 3.

Создаем группу GW. Для этого выполняем следующие шаги:

- переходим в раздел Device Hierarchy: Devices => Device Hierarchy
- кнопкой Create Group вызываем окно создания группы
- вводим уникальное имя группы (GW) (Рисунок 2)

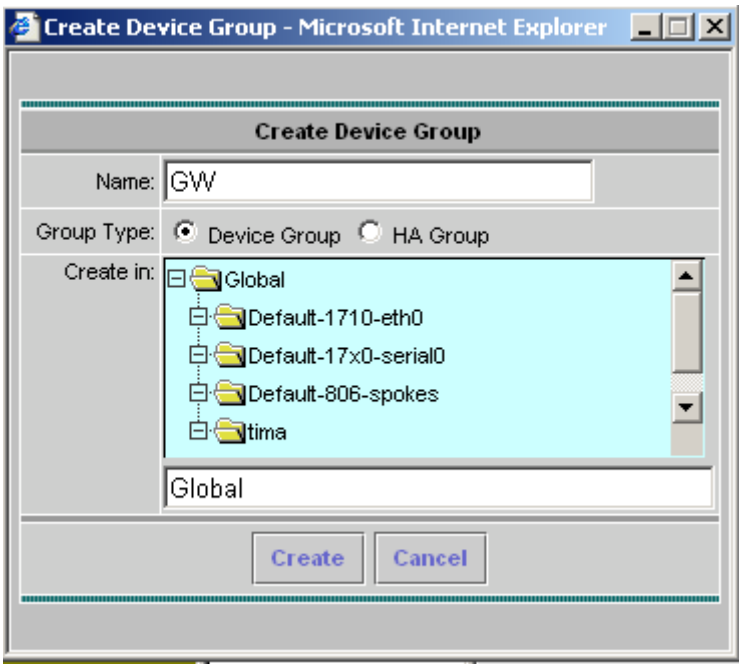


Рисунок 2

- выбираем родительскую папку, в которой будет размещаться созданная группа. В нашем случае это папка Global
- нажимаем кнопку Create.

Группа GW создана и ее можно увидеть внутри папки Global.

Далее переходим к импорту устройств.

Импорт устройств

На этом этапе импортируем устройства GW1, GW2 и GW3 в созданную группу GW. Выполним следующие шаги:

- переходим в раздел Device Import
- выделяем группу GW
- нажимаем кнопку Import. Откроется окно выбора метода импорта
- выбираем опцию "Single device import"
- нажимаем Next. Откроется окно ввода параметров
- вводим IP-адрес или доменное имя импортируемого объекта, Username, Password и Enable Password. Импортируем устройство GW1, вводим его IP-адрес 10.0.232.3, имя пользователя – cscons, пароль – csp, enable password - csp (Рисунок 3)

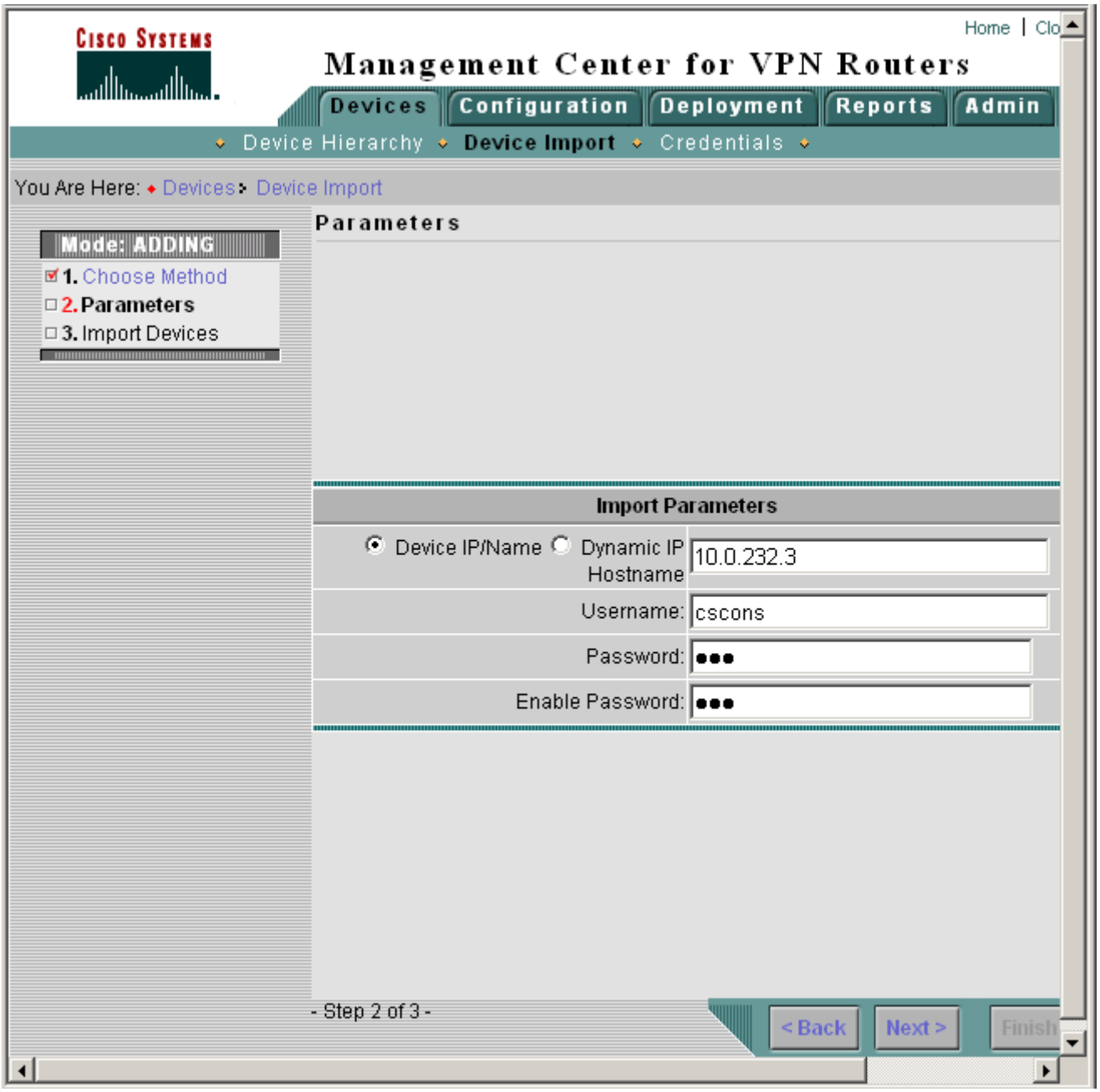


Рисунок 3

- нажимаем кнопку Next. Откроется окно назначения роли импортируемому устройству
- выбираем роль для импортируемого устройства GW1 – Hub. Эту роль мы заранее определили в Таблице
- нажимаем Finish. Откроется окно о состоянии импортирования устройства. По окончании импортирования нажмите Close.

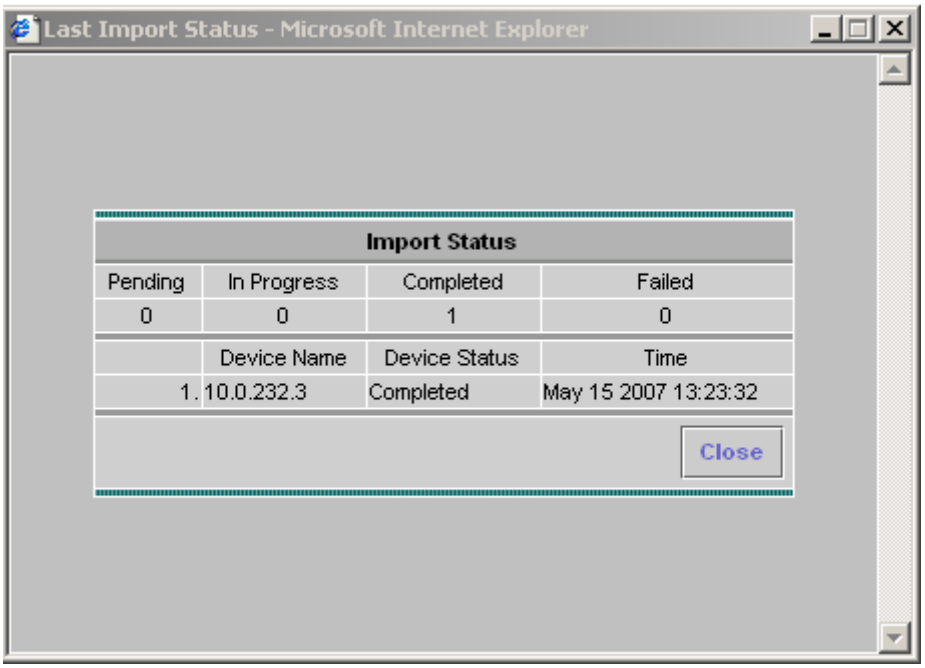


Рисунок 4

Импортируемое устройство (GW1) появится в группе GW. Повторим описанные выше шаги для импортируемых устройств GW2 и GW3, назначая им роли Spoke.

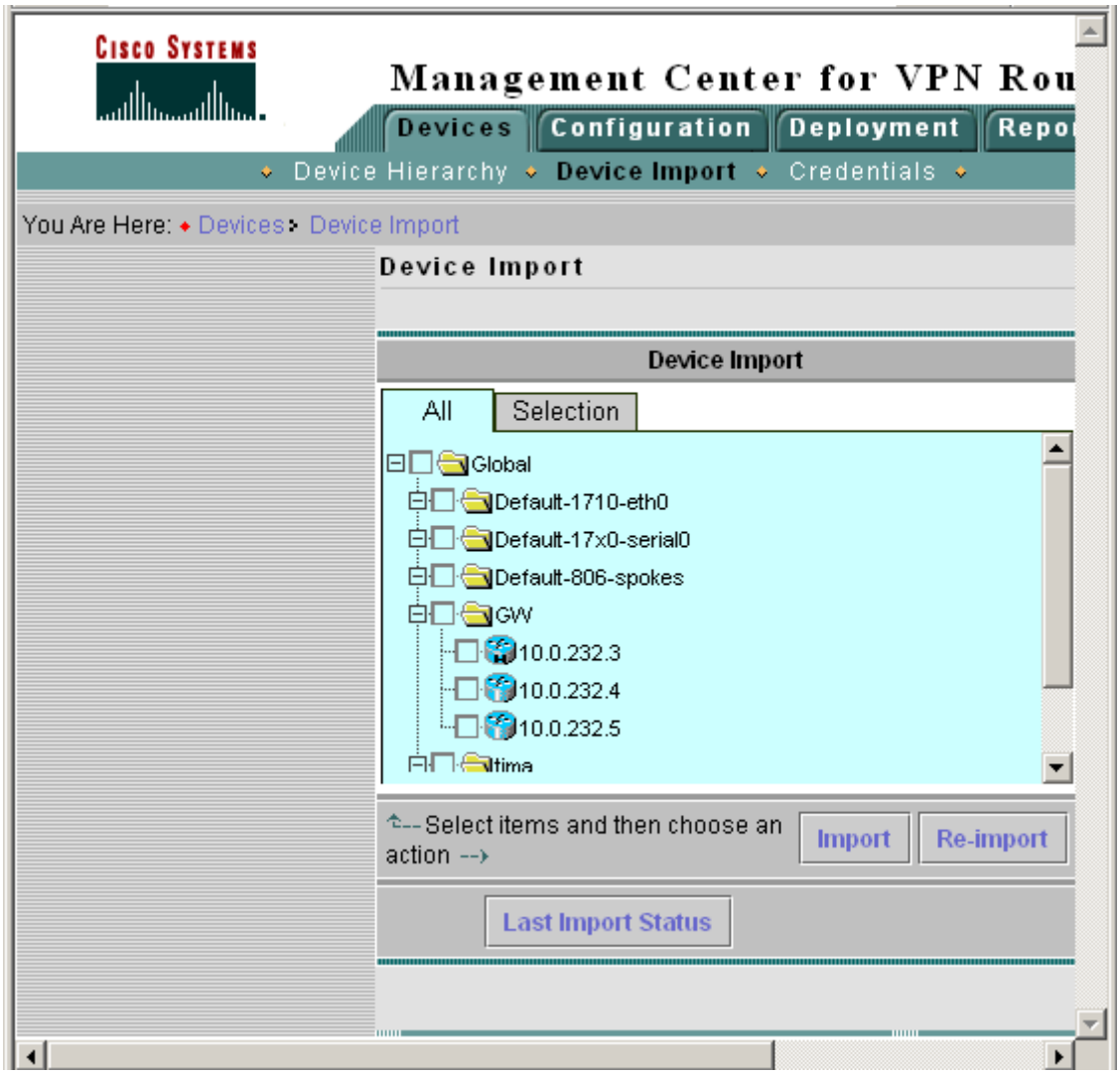


Рисунок 5

После того, как все устройства импортированы и помещены в группу, можно переходить к настройке VPN параметров.

Описание защищаемых ресурсов

На этом этапе опишем защищаемые ресурсы и прикрепим их к соответствующим устройствам.

Выполним следующие шаги:

- перейдем в раздел Building Blocks: Configuration => Building Blocks
- из меню выберем пункт Network Groups. Откроется страница Network Groups
- откроем Object Selector и выберем группу GW. Информация на странице обновится
- нажмем кнопку Create. Откроется страница Name and Comment
- введем в поле Name уникальное имя создаваемого сетевого объекта. Для нашего примера опишем подсеть Subnet1. Вводим имя Subnet1.
- введем комментарий
- нажмем Next. Откроется страница Networks
- в поле Enter Network/Host вводим адресное пространство (или адрес) защищаемого ресурса. Так как мы описываем подсеть Subnet1, вводим адресное пространство этой подсети: 10.10.10.0/24
- нажимаем кнопку >>. Введенное адресное пространство добавлено в список
- нажимаем Finish.

Произойдет возврат на страницу Network Groups. В таблице мы увидим строку с параметрами созданного объекта (подсети Subnet1) (Рисунок 6):

Name = Subnet1

Defined On = GW

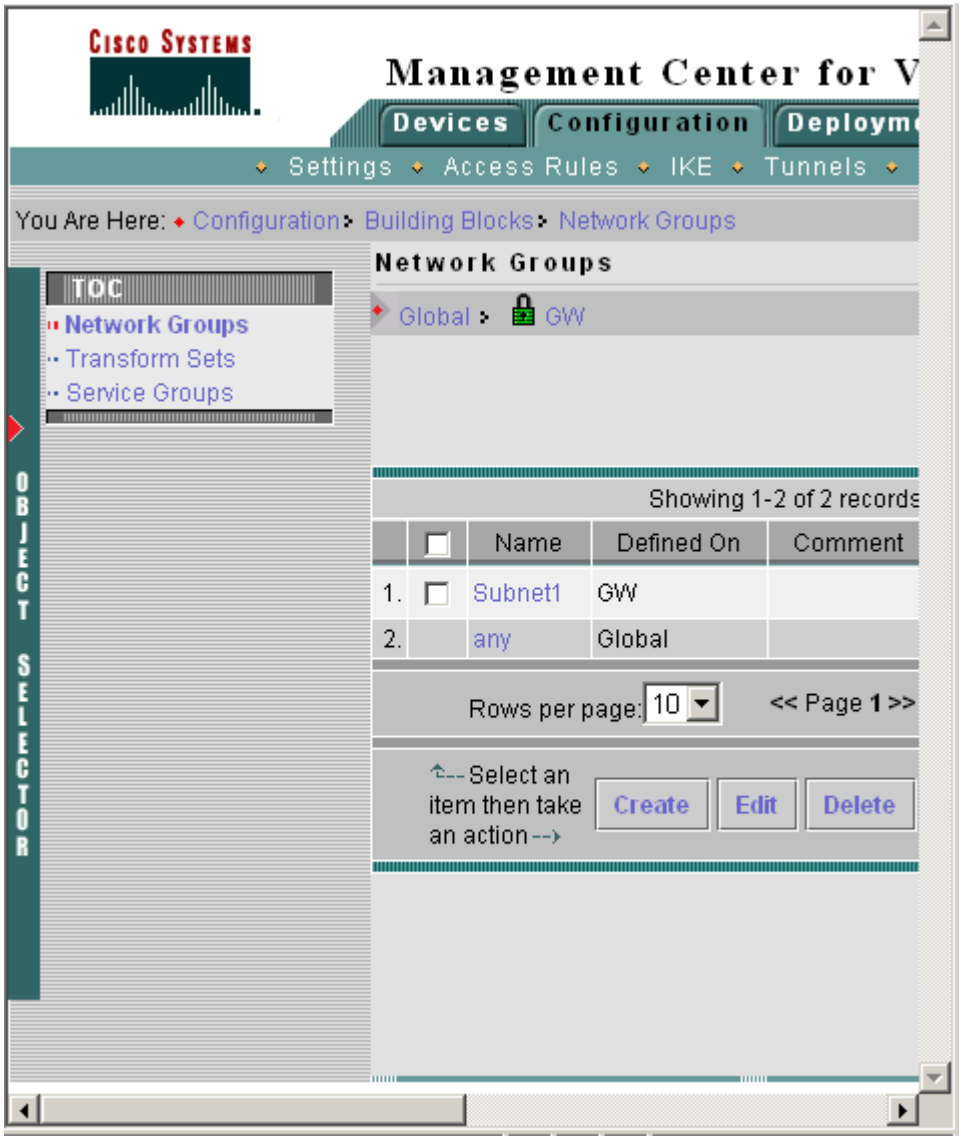


Рисунок 6

- Повторим описанные выше шаги для всех защищаемых ресурсов - Subnet2 (10.10.11.0/24) и Subnet3 (10.10.12.0/24).
- Перейдем в раздел Settings: Configuration => Settings.
- Назначаем созданные сетевые объекты устройству с ролью Hub. В нашем примере устройство с ролью Hub – GW1:
  - откроем Object Selector и выберем в группе GW устройство GW1
  - в меню выберем пункт Hub => Networks. Откроется страница Hub Side Network
  - выберем из списка Add Network Groups подсеть, которую защищает GW1. Это созданная ранее подсеть Subnet1. Нажимаем кнопку >>. Объект Subnet1 переместится в список защищаемых объектов (Рисунок 7)
  - нажимаем Apply.

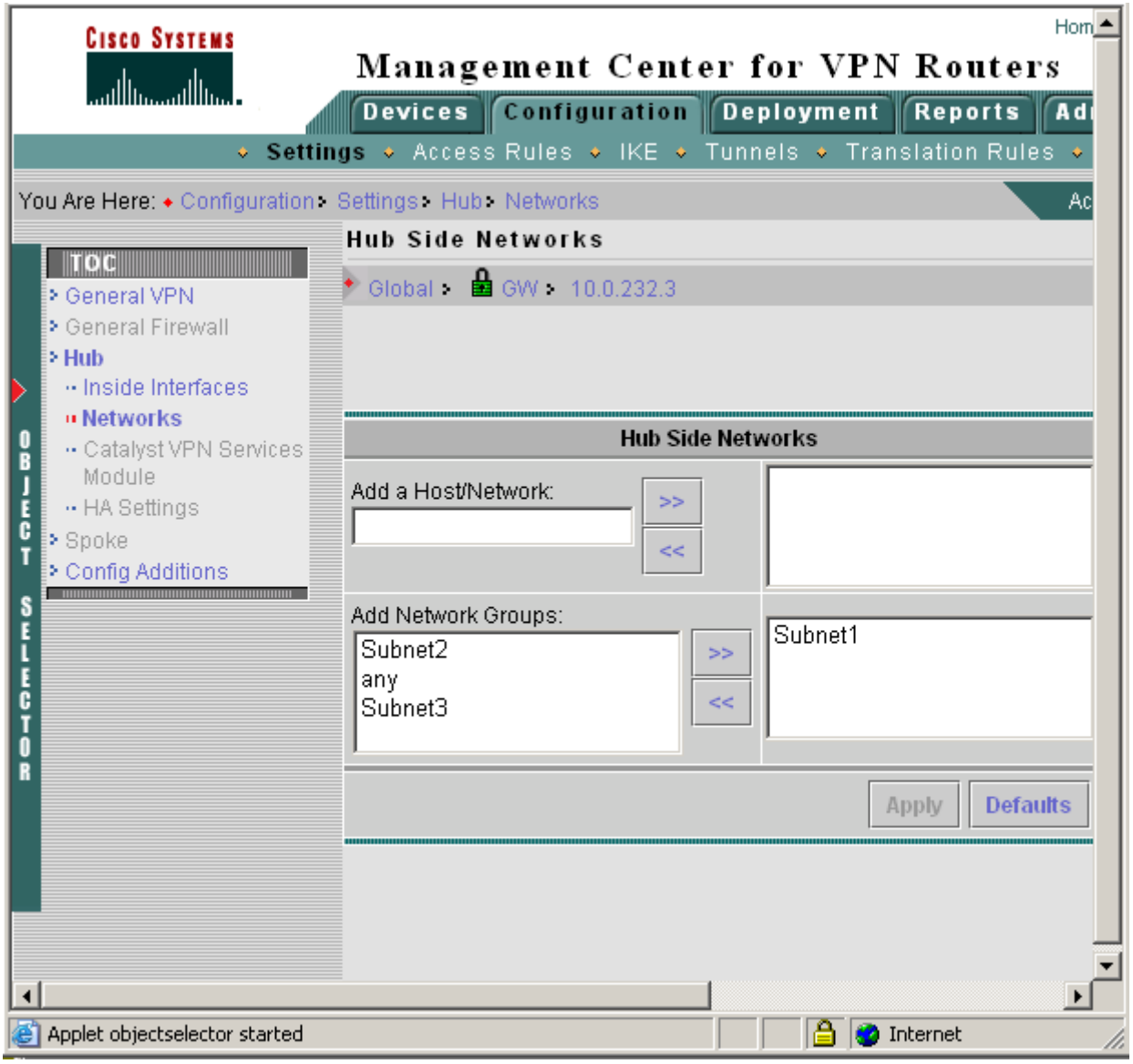


Рисунок 7

- Назначаем созданные сетевые объекты устройствам с ролью Spoke:
  - в меню слева выберем пункт Spoke => Networks. Откроется страница Spoke Side Networks
  - откроем Object Selector и выберем в группе GW устройство с ролью Spoke. В этой группе у нас два таких устройства. Выберем устройство GW2
  - выберем из списка Add Network Groups подсеть, которую защищает GW2. Это созданная ранее подсеть Subnet2. Нажимаем кнопку >>. Объект Subnet2 переместится в список защищаемых объектов
  - нажимаем Apply
  - повторим описанные выше действия для назначения устройству GW3 сетевого объекта Subnet3.

После того, как описаны все защищаемые ресурсы, можно переходить к настройке VPN параметров.

Настройка VPN параметров

На этом этапе мы произведем такие настройки устройств как назначение внутренних интерфейсов для устройств, назначение VPN интерфейсов устройствам с ролью Spoke и назначение устройства Hub устройствам с ролью Spoke. В качестве примера рассмотрим настройку VPN параметров для группы GW, содержащей устройства CSP VPN Gate.

Выполним следующие шаги:

- Переходим в раздел Settings: Configuration => Settings.
- В левой части окна открываем Object Selector и выбираем группу GW.
- Назначаем внутренние интерфейсы устройству с ролью Hub:
  - выбираем из меню в левой части окна пункт Hub = > Inside Interfaces. Будет осуществлен переход на страницу Hub Inside Interfaces
  - нажимаем кнопку Show Interfaces. Откроется окно со списком сетевых интерфейсов
  - выбираем нужный интерфейс в открывшемся списке. Как правило, это FastEthernet 0/1
  - нажимаем Select. На странице Hub Inside Interfaces в списке появится выбранный интерфейс
  - нажимаем Apply. Находящемуся в группе устройству с ролью Hub (в нашем случае это GW1) назначен интерфейс для построения туннелей с устройствами с ролью Spoke.
- Назначаем внутренние интерфейсы устройствам с ролью Spoke.
  - выбираем из меню в левой части окна пункт Spoke = > Inside Interfaces. Откроется страница Spoke Inside Interfaces
  - нажимаем кнопку Show Interfaces. Откроется окно со списком сетевых интерфейсов
  - выбираем нужный интерфейс в открывшемся списке. Как правило, это FastEthernet 0/1
  - нажимаем Apply. Всем устройствам с ролью Spoke назначены внутренние интерфейсы (Рисунок 8).

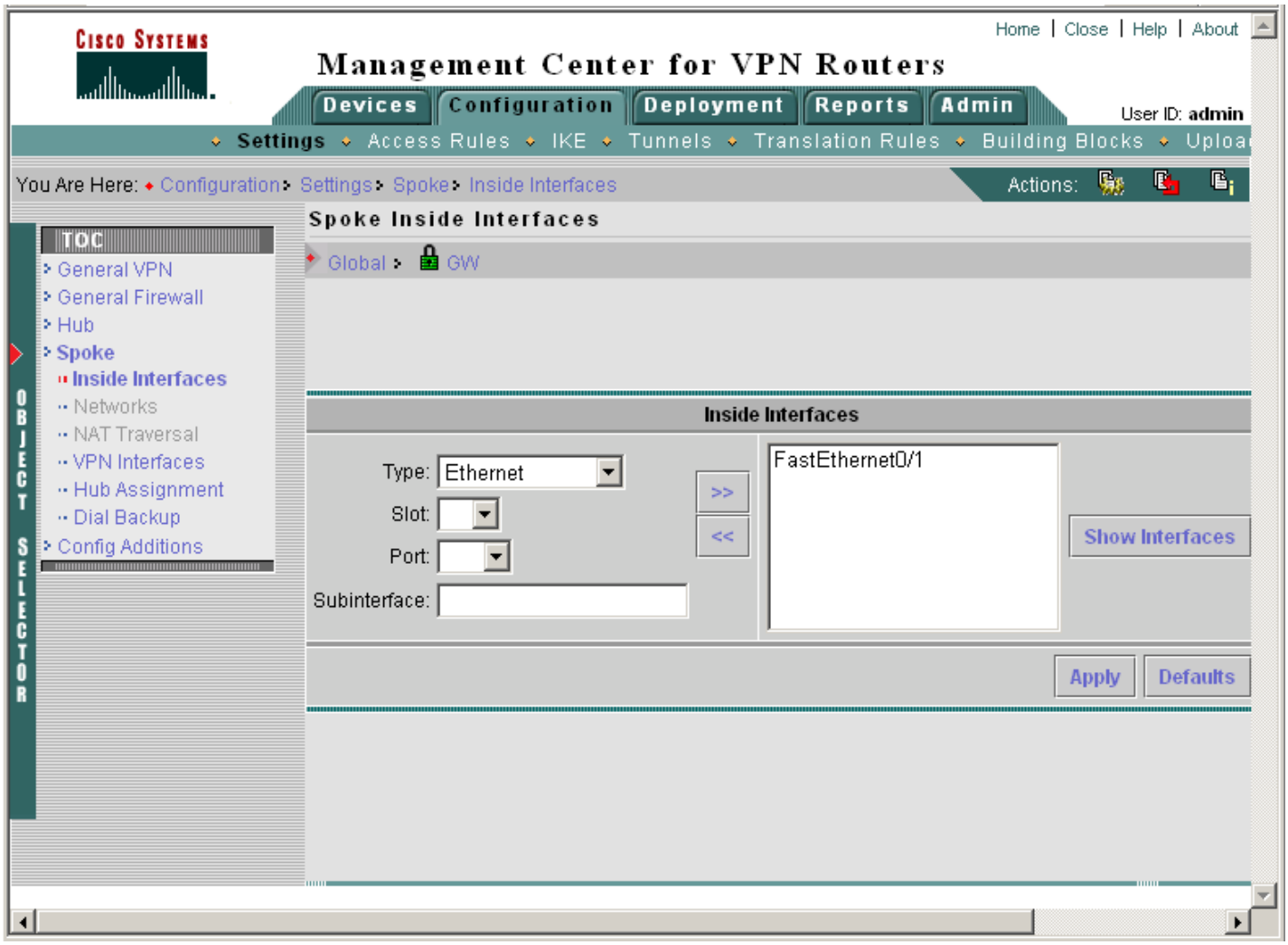


Рисунок 8

- Назначаем VPN интерфейс устройствам с ролью Spoke:
  - выбираем из меню в левой части окна пункт Spoke = > VPN Interfaces. Открывается страница Spoke VPN Interface
  - нажимаем кнопку Show Interfaces. Откроется окно со списком сетевых интерфейсов
  - выбираем нужный интерфейс в открывшемся списке. Как правило, это FastEthernet 0/0
  - нажимаем Apply. Всем устройствам с ролью Spoke назначены VPN интерфейсы (Рисунок 9).

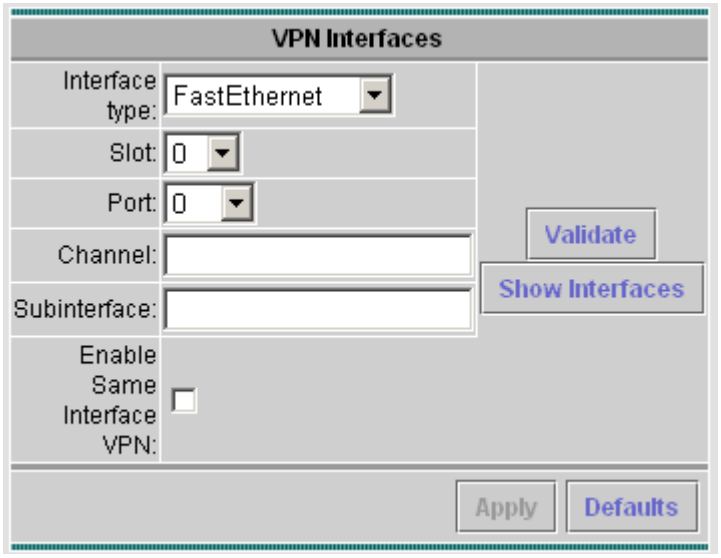


Рисунок 9

- Назначаем для устройств с ролью Spoke устройство с ролью Hub:
  - выбираем из меню в левой части окна пункт Hub Assignment. Откроется страница Hub Assignment
  - из списка выбираем имя устройства с ролью Hub
  - из списка выбираем интерфейс, через который будет осуществляться взаимодействие с устройствами с ролью Spoke (построение VPN туннелей), нажимаем Apply (Рисунок 10).

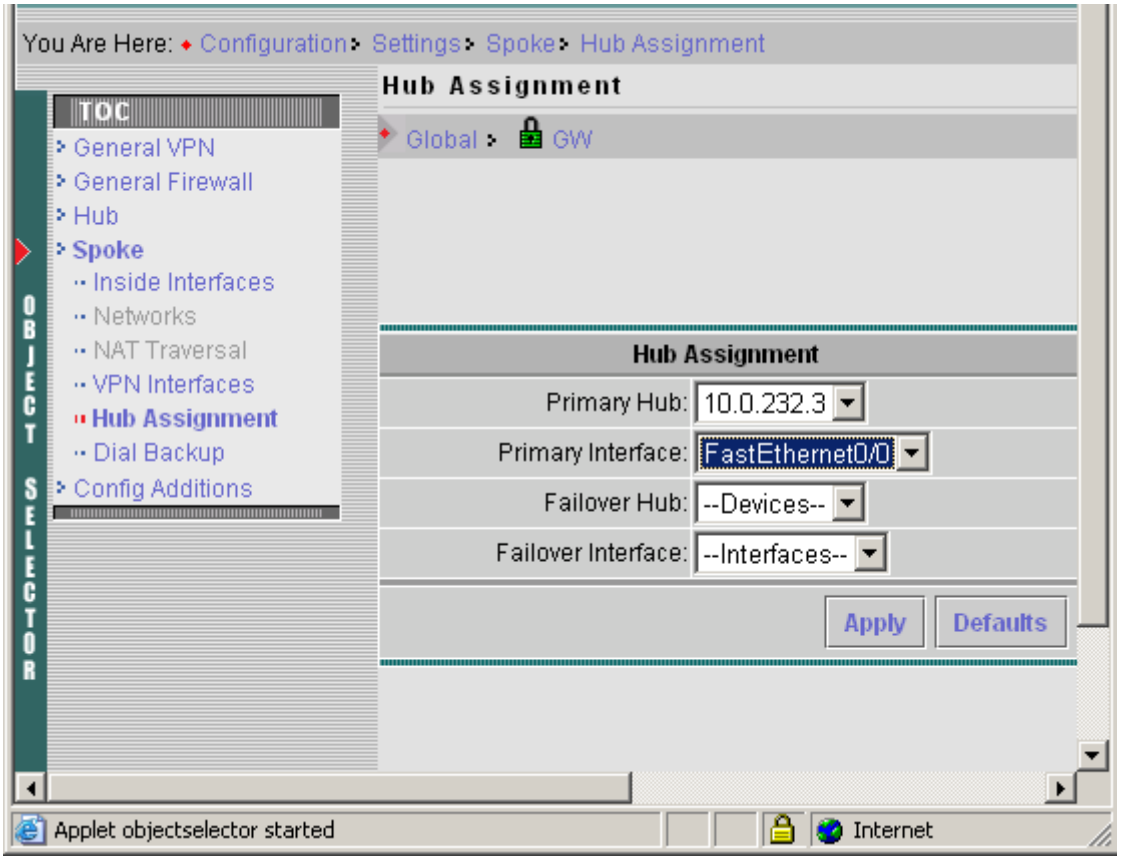


Рисунок 10

На этом настройки VPN закончены и можно переходить к настройкам IKE политики.

Настройка IKE политики

На этапе настройки IKE политики произведем настройки параметров шифрования и аутентификации для группы GW. Будем использовать аутентификацию на предопределенных ключах. После выполнения последнего этапа у нас все еще выделена группа GW (если эта группа не выбрана, нужно ее выбрать в Object Selector). Создаем IKE политику для этой группы.

- Переходим в раздел IKE Policies: Configuration => IKE => IKE Policies. Откроется страница IKE Policies
- нажимаем Create. Откроется страница IKE Policy Name and Comment
- заполняем поле Name уникальным именем, которое присваиваем создаваемой IKE политике, например IKE_GW_group
- в поле описания вводим комментарий: IKE Policy for GW Group
- нажимаем Next. Открывается страница Algorithm Settings (Рисунок 11)
- выбираем из списка Encryption Algorithm значение DES. В устройствах CSP VPN Gate это значение будет интерпретироваться, как указание использовать алгоритм шифрования ГОСТ 28147-89
- выбираем из списка Hash Algorithm значение MD5. В устройствах CSP VPN Gate это значение будет интерпретироваться, как указание использовать хэш-алгоритм ГОСТ Р 34.11-94
- выбираем из списка Modulus Group значение 2

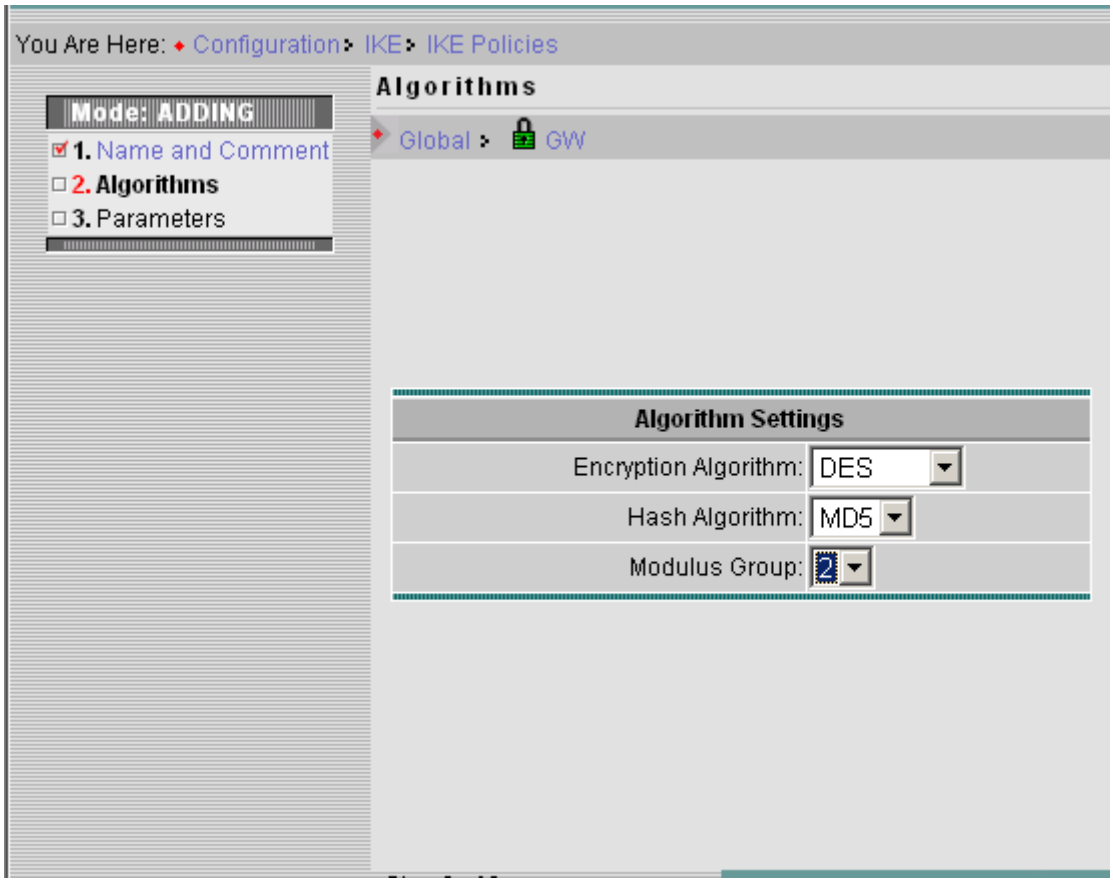


Рисунок 11

- нажимаем Next. Открывается страница IKE Policy Parameters
- в поле Lifetime оставляем значение по умолчанию (86400)
- из списка Authentication выбираем значение Preshared Key

- нажимаем Finisht. Открывается страница IKE Policies
- проверяем правильность параметров, которые мы установили на предыдущих шагах. Должна быть выведена такая информация (Рисунок 12):

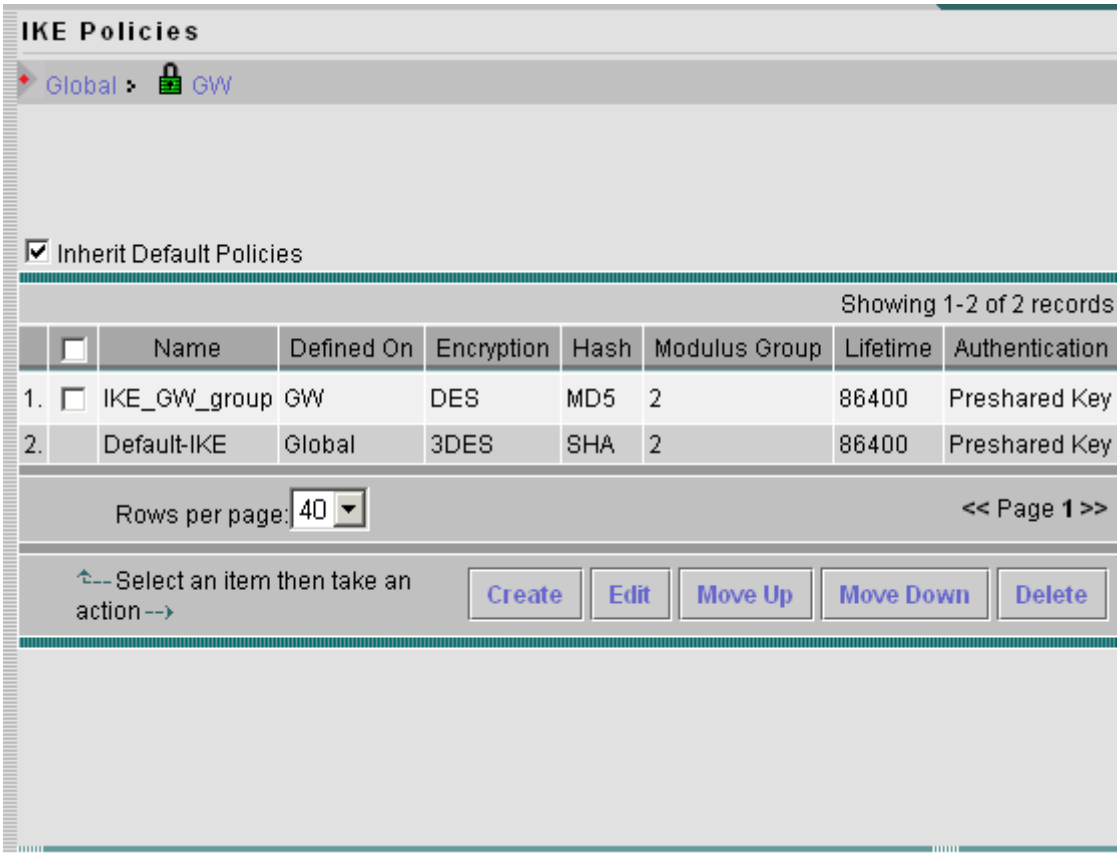


Рисунок 12

IKE политика для группы GW создана и ее параметры отображаются в таблице.

Назначим режим автоматической генерации предопределенных ключей для всех устройств проекта. Для этого выполним следующие шаги:

- выберем в меню пункт Preshared Key. Откроется страница Preshared Key
- откроем Object Selector и выберем группу Global
- установим значение Auto-Generate.

После этого можно переходить к этапу создания туннельной политики.

Создание туннельной политики

Создаем туннельную политику для группы GW. Для этого убедимся, что в Object Selector выбрана эта группа и выполним следующие шаги:

- переходим в раздел Tunnels: Configuration => Tunnels
- выбираем пункт меню Tunnel Policies. В открывшемся окне видим таблицу туннельных политик
- нажимаем кнопку Create. Откроется окно ввода имени туннельной политики
- вводим уникальное имя туннельной политики, например, GW_Tunnel. Также можно заполнить поле комментария
- нажимаем Next. Откроется окно Traffic Filter (Рисунок 13)

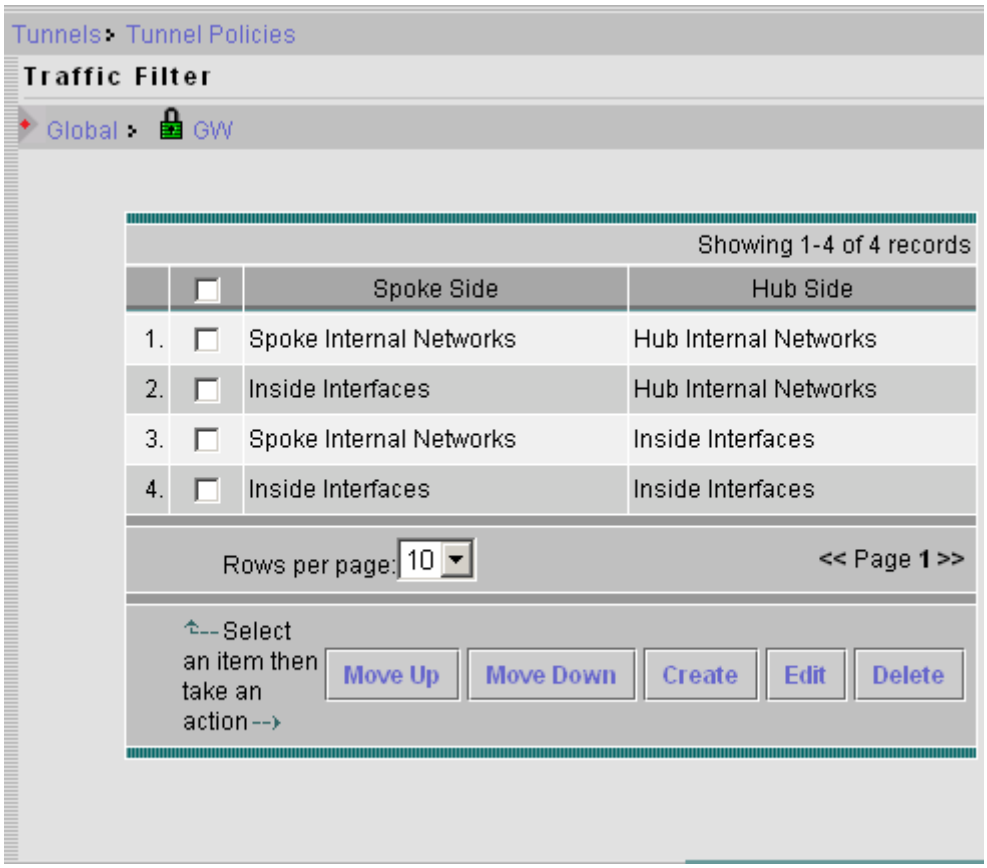


Рисунок 13

- оставляем в таблице только одну строку – Spoke Internal Networks/Hub Internal Networks. Остальные строки удаляем. Для этого устанавливаем флажки рядом с удаляемыми строками и нажимаем кнопку Delete
- нажимаем Next. Откроется окно Transform Sets
- создаем новый набор преобразований (transform set):
  - нажимаем кнопку Create. Откроется страница ввода имени и комментария
  - вводим уникальное имя для создаваемого набора преобразований. Например, DES_MD5. Также можно ввести комментарий
  - нажимаем Next. Откроется страница Transform Set Protocols (Рисунок 14)
  - выбираем из списка Mode значение Tunnel
  - выбираем из списка AH Hash значение MD5. В устройствах CSP VPN Gate это значение будет интерпретироваться, как указание использовать хэш-алгоритм ГОСТ Р 34.11-94
  - выбираем из списка ESP Encryption значение DES. В устройствах CSP VPN Gate это значение будет интерпретироваться, как указание использовать алгоритм шифрования ГОСТ 28147-89
  - выбираем из списка ESP Hash значение MD5. В устройствах CSP VPN Gate это значение будет интерпретироваться, как указание использовать хэш-алгоритм ГОСТ Р 34.11-94

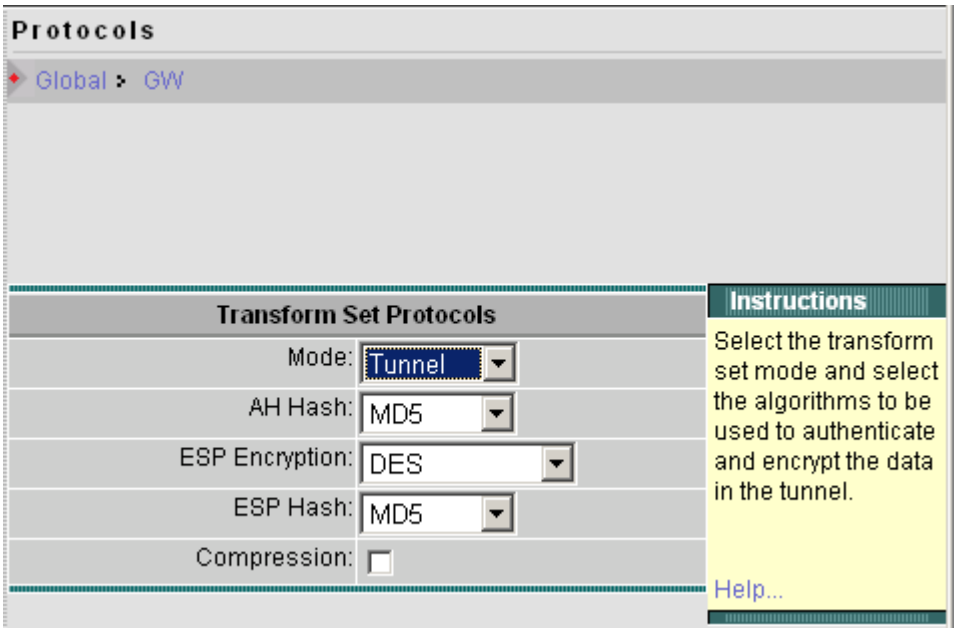


Рисунок 14

- снимаем флажок Compression, если он был взведен. CSP VPN Gate не поддерживает компрессию
- нажимаем Finish.

Мы только что создали набор преобразований DES_MD5. Созданный набор дополнил список наборов преобразований, которые доступны для выбора в списках Transform Set 1, 2, 3.

- выбираем из списка Transform Set 1 значение DES_MD5.
- нажимаем Next. Откроется страница PFS.
- устанавливаем флажок Use PFS.
- выбираем из списка Modulus Group значение 2.
- нажимаем Finish. Открывается страница Tunnel Policies.

Туннельная политика создана, о чем свидетельствует новая строка в таблице на странице Tunnel Policies (Рисунок 15)

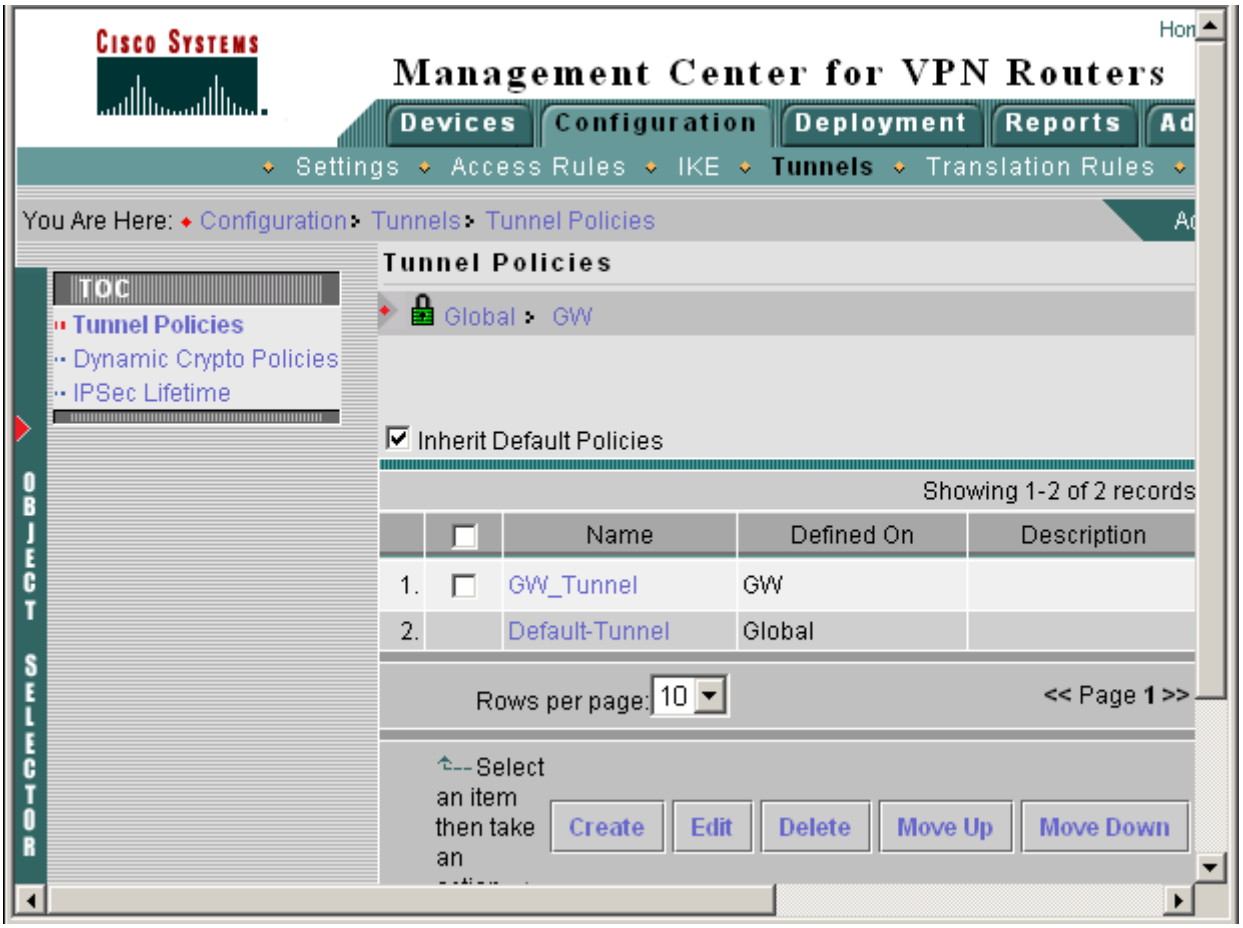


Рисунок 15

Доставка конфигураций на устройства

Для доставки конфигураций на устройства системы нам необходимо создать «работу» - job.

Выполним следующие шаги:

- перейдем в раздел Deployment
- выберем Save and Deploy в предложении If you have made configuration changes, you can Save and Deploy на странице
- откроется страница Select Devices
- отметим устройства, на которые будет доставляться политика. Обычно Router MC автоматически определяет устройства, для которых сделаны изменения, но не доставлены. Поэтому, как правило на этой странице никаких изменений не делается
- нажимаем Next. Будет открыта страница Deployment Options
- установим значение Deploy To равным Device
- нажимаем Next. Откроется страница Error Checking (Рисунок 16). Возможно, данная страница будет содержать различные предупреждения и ошибки. Устраните ошибки.

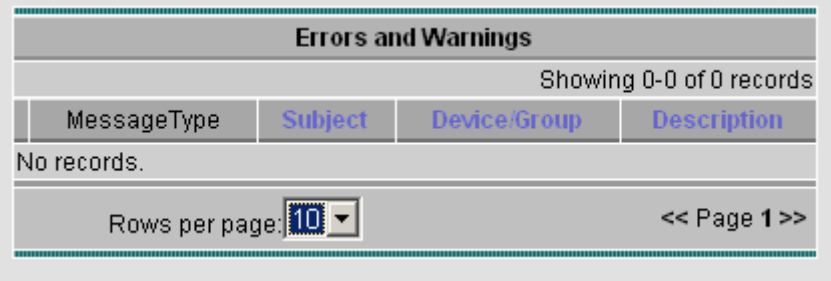


Рисунок 16

- нажимаем Finish. Откроется страница Job Deployment Status с вопросом о том, нужно ли доставлять политики немедленно
- нажимаем кнопку Refresh для обновления статуса Job и устройств.

В процессе доставки на странице Job Deployment Status мы можем наблюдать изменение статусов Job и устройств, для которых генерируются конфигурации (Рисунок 17). На протяжении процесса доставки Job будет иметь статус "Generating" (во время генерации конфигураций), "Deploying" (во время доставки конфигураций на устройства), а после окончания процесса статус изменится на "Deployed". Статус устройств будет меняться от "Pending", когда процесс доставки еще не начался, до "In Progress" – в процессе доставки и "Completed" по окончании доставки. Статусы автоматически не обновляются. Для обновления используем кнопку Refresh. Возможны ошибки на этапе генерации конфигураций и их доставки. В этих случаях будет использоваться статус Failed.

Процесс доставки завершается, когда у Job будет статус "Deployed" (Рисунок 17).

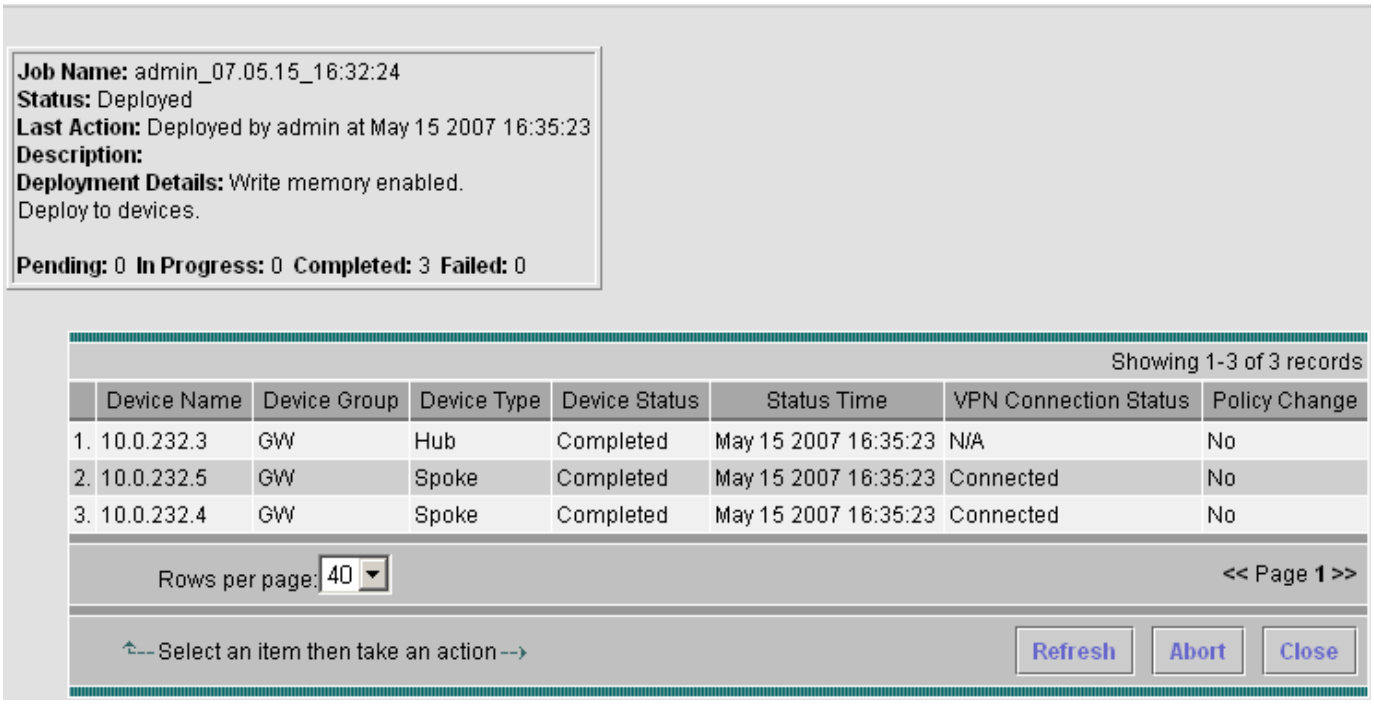


Рисунок 17

Таким образом, конфигурации доставлены на устройства GW1, GW2 и GW3, просмотреть которые можно в конфигурационном режиме командой `do show running-config`.