Пример конфиграции "Thin-Client SSL VPN (WebVPN) на ASA с ASDM"

Содержание

Введение

Технология тонкого клиента SSL VPN позволяет предоставить защищенный доступ для некоторых приложений, имеющих статические порты, например Telnet (23), SSH (22), POP3 (110), IMAP4 (143) и SMTP (25). Сеть SSL VPN с тонким клиентом можно применять как приложение на основе пользователей, политик или обоих типов. Другими словами, можно настроить доступ на уровне отдельных пользователей, либо создать разные группы политик, в которые поместить одного или нескольких пользователей.

- **Бесклиентная SSL VPN (WebVPN) . Предоставляет удаленному клиенту, имеющему браузер с поддержкой SSL, доступ к веб-серверам HTTP или HTTPS в корпоративной локальной сети (LAN).** Кроме того, Clientless SSL VPN обеспечивает доступ к файлам Windows через протокол CIFS. Web-клиент Outlook (OWA) представляет собой пример клиента доступа HTTP.Дополнительные сведения о бесклиентской сети SSL VPN см. в

документе Пример конфигурации бесклиентской сети SSL VPN (WebVPN) на базе ASA.

- **Тонкий клиент SSL VPN (переадресация портов). В этом варианте конфигурации предусматривается удаленный клиент, загружающий небольшой Java-апплет и обеспечивающий защищенный доступ к приложениям TCP, использующим статические номера портов.** Примерами защищенного доступа являются почтовые протоколы POP3, SMTP и IMAP, защищенный сеанс интерпретатора (ssh) и Telnet. Пользователю необходимы локальные административные привилегии, так как производятся изменения в файлах локальной машины. Данный метод SSL VPN не функционирует с приложениями, использующими динамическое назначение портов, такими как некоторые приложения, использующие протокол передачи файлов (FTP).**Примечание:** Протокол UDP не поддерживается.
- **Клиент SSL VPN (туннельный режим). На удаленную рабочую станцию загружается небольшой клиент, который обеспечивает полный защищенный доступ к ресурсам внутренней корпоративной сети.** Клиент SSL VPN Client (SVC) может загружаться на удаленный узел на постоянной основе или удаляться по завершении защищенного сеанса.Дополнительные сведения о клиенте SSL VPN см. в документе Пример конфигурации клиента SSL VPN (SVC) на ASA с ASDM.

В этом документе демонстрируется простая конфигурация SSL VPN с тонким клиентом на устройстве адаптивной защиты (ASA). Эта конфигурация позволяет пользователю Telnet устанавливать защищенный сеанс с маршрутизатором, расположенным во внутренней сети устройства ASA. Конфигурация в этом документе поддерживается для версий ASA 7.x и выше.

Предварительные условия

Требования

Прежде чем использовать эту конфигурацию, убедитесь, что для удаленных рабочих станций клиентов выполняются следующие требования:

- Web-браузер с поддержкой шифрования SSL
- Среда выполнения SUN Java JRE версии 1.4 или выше
- Файлы Cookie разрешены
- Средства блокировки всплывающих окон отключены
- Полномочия локального администратора (не требуются, но настоятельно рекомендуются)

Примечание: Последняя версия JRE Java SUN доступна как бесплатная закачка от Веб-сайта Java.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройство адаптивной защиты Cisco ASA серии 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2 (1)**Примечание:** Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.

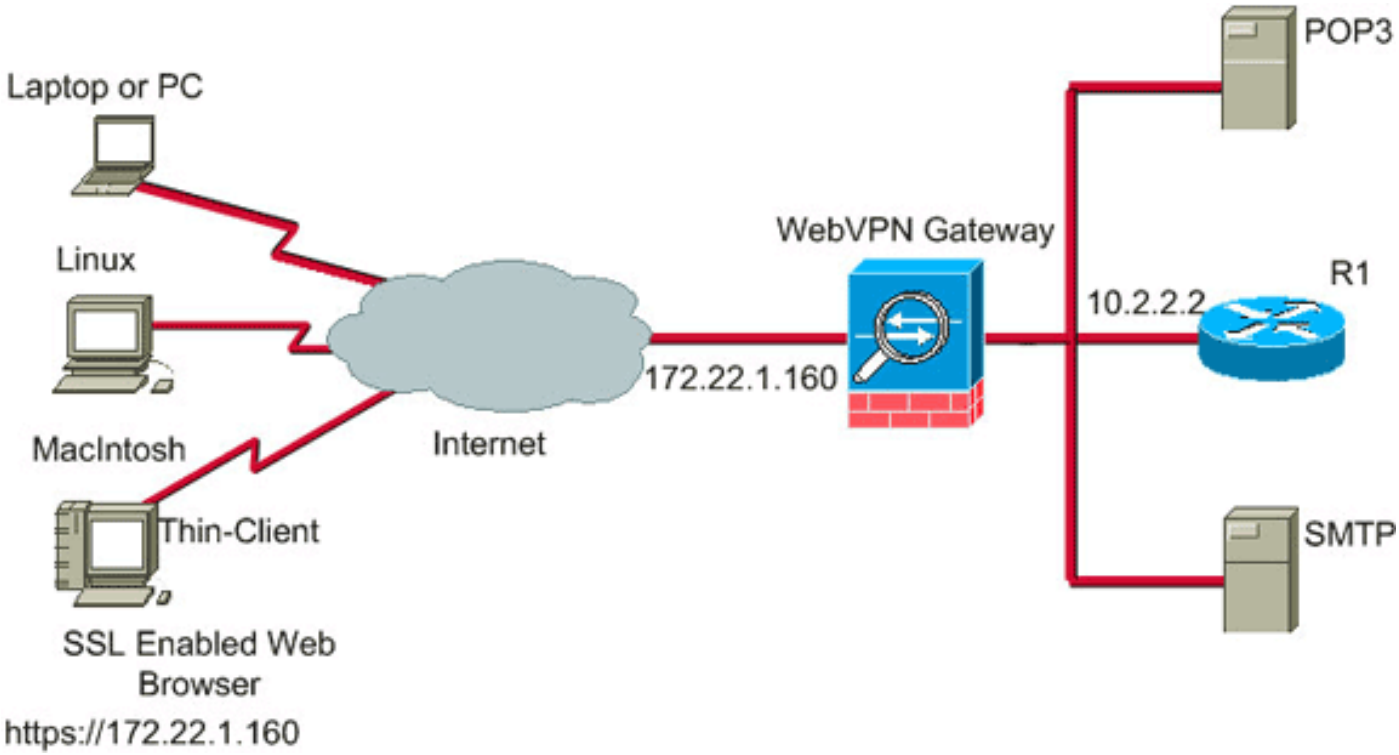
- ПО для устройств адаптивной защиты Cisco версии 7.2(1)
- Удаленный клиент Microsoft Windows XP Professional (SP 2)

Сведения, рассматриваемые в этом документе, были получены в лабораторной среде. Все упоминаемые устройства работали в конфигурации по умолчанию. При работе в действующей сети необходимо изучить все возможные последствия каждой команды. Все IP-адреса, использованные в конфигурации, выбраны в соответствии с документом RFC 1918 для лабораторной среды; эти IP-адреса не могут быть маршрутизированы в сети Интернет и предназначены только для тестовых целей.

Схема сети

В этом разделе описана конфигурация сети, используемая в данном документе.

Когда удаленный клиент инициализирует сеанс с ASA, клиент загружает небольшой Java-апплет на рабочую станцию. Клиенту отображается список предварительно настроенных ресурсов.



Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие сведения

Для запуска сеанса удаленный клиент открывает браузер SSL, устанавливая сеанс с внешним интерфейсом ASA. После установления сеанса пользователь при помощи параметров, настроенных на ASA, может вызвать любой сеанс Telnet или приложение. Устройство ASA служит прокси-сервером для защищенного сеанса и позволяет пользователю обращаться к устройству.

Примечание: Входящие списки контроля доступа для этих подключений не требуются, поскольку критерии легитимности сеанса устройству ASA уже известны.

Настройка тонкого клиента SSL VPN посредством ASDM

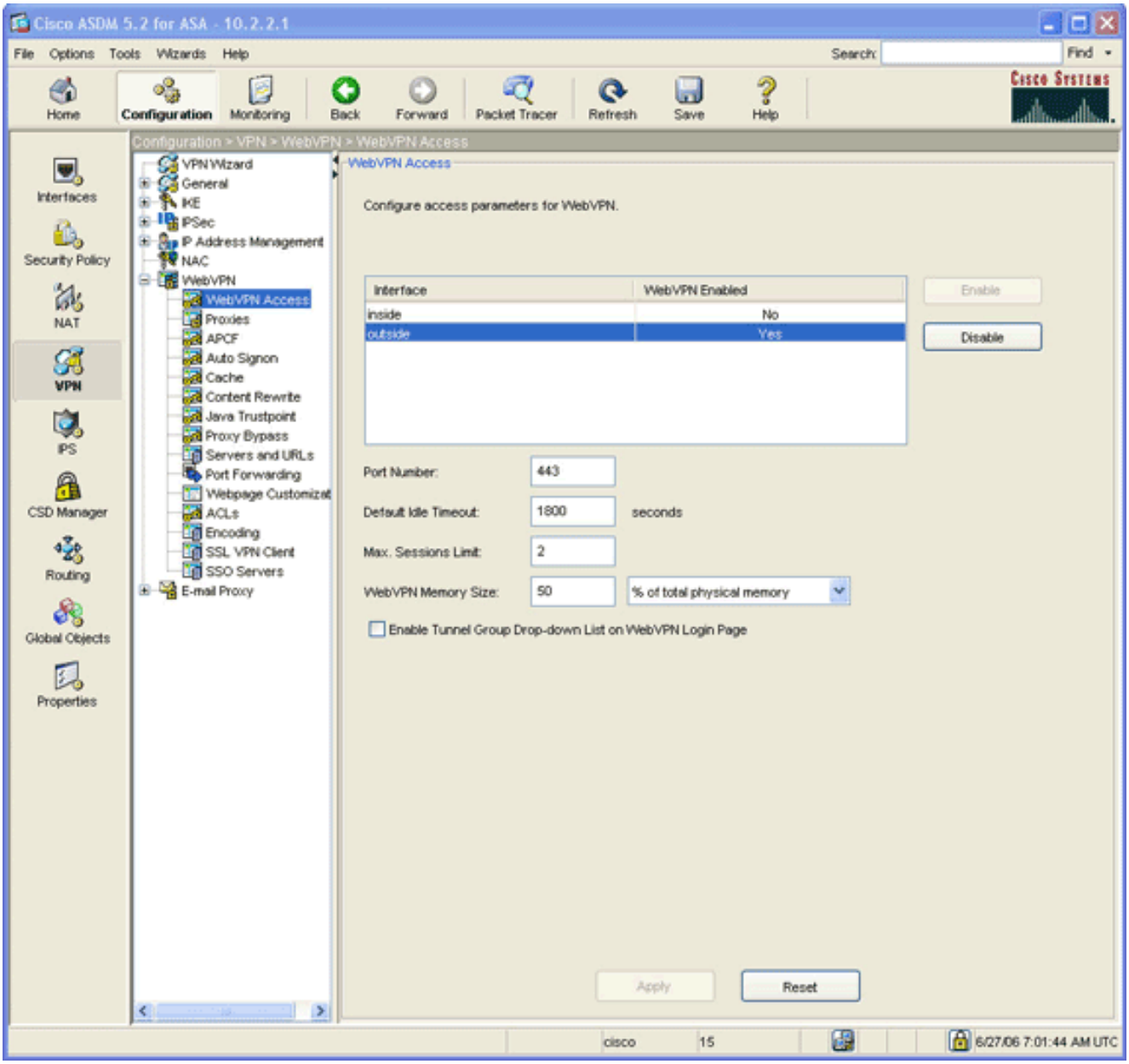
Для настройки тонкого клиента SSL VPN на устройстве ASA выполните следующие действия:

1. Включение WebVPN на ASA
2. Настройка характеристик переадресации портов
3. Создание групповой политики и связывание ее со списком переадресации портов (созданным на шаге 2)
4. Создание группы туннелирования и связывание ее с групповой политикой (созданной на шаге 3)
5. Создание пользователя и добавление его в групповую политику (созданную на шаге 3)

Шаг 1. Включение WebVPN на ASA

Чтобы включить доступ WebVPN на устройстве ASA, выполните следующие действия:

1. **В приложении ASDM выберите Configuration (Настройка), затем выберите VPN.**
2. **Разверните WebVPN и выберите WebVPN Access (Доступ к WebVPN).**

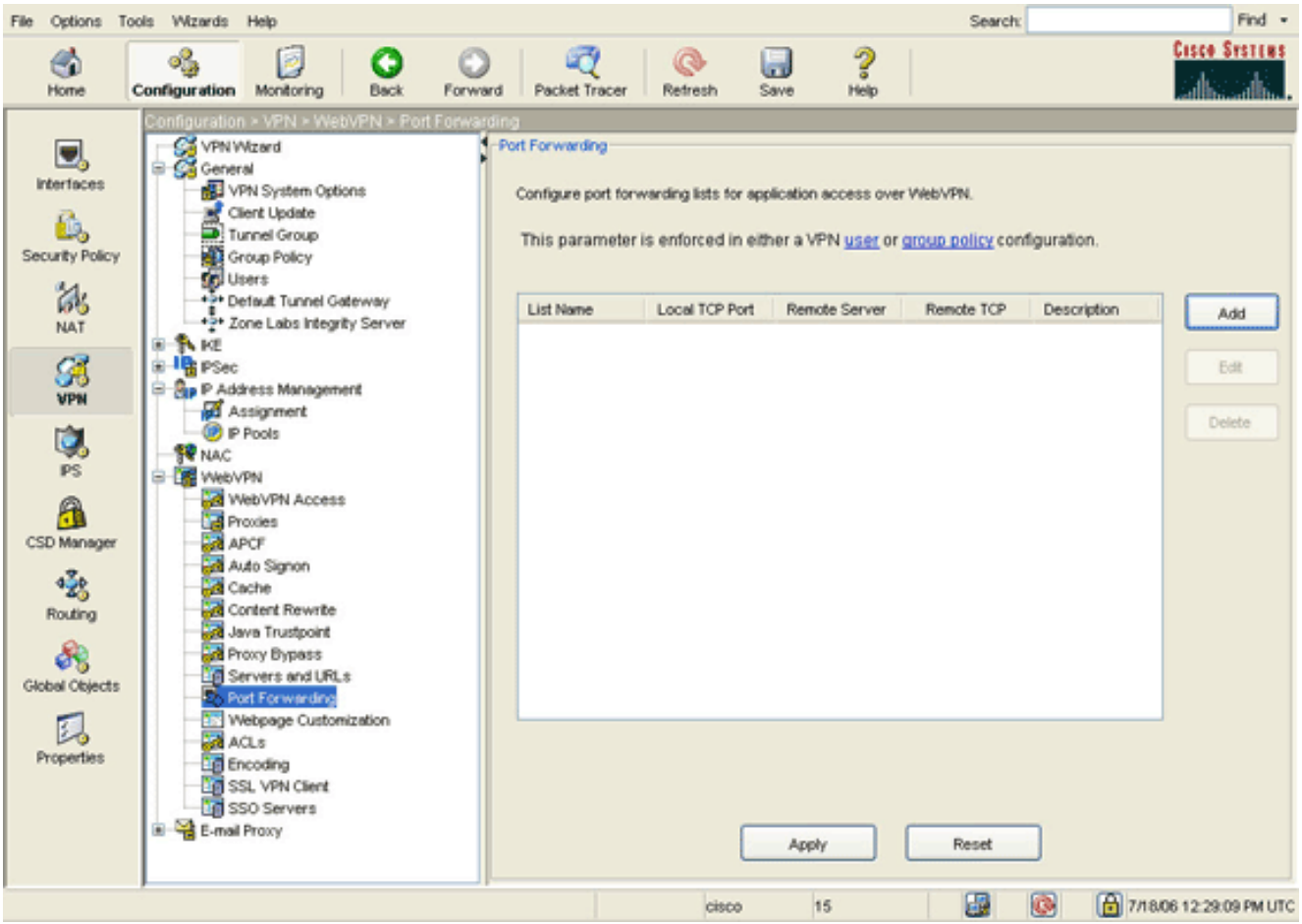


3. **Выделите интерфейс и щелкните Enable (Включить).**
4. **Выберите Apply (Применить), выберите Save (Сохранить) затем ответьте Yes (Да), чтобы подтвердить изменения.**

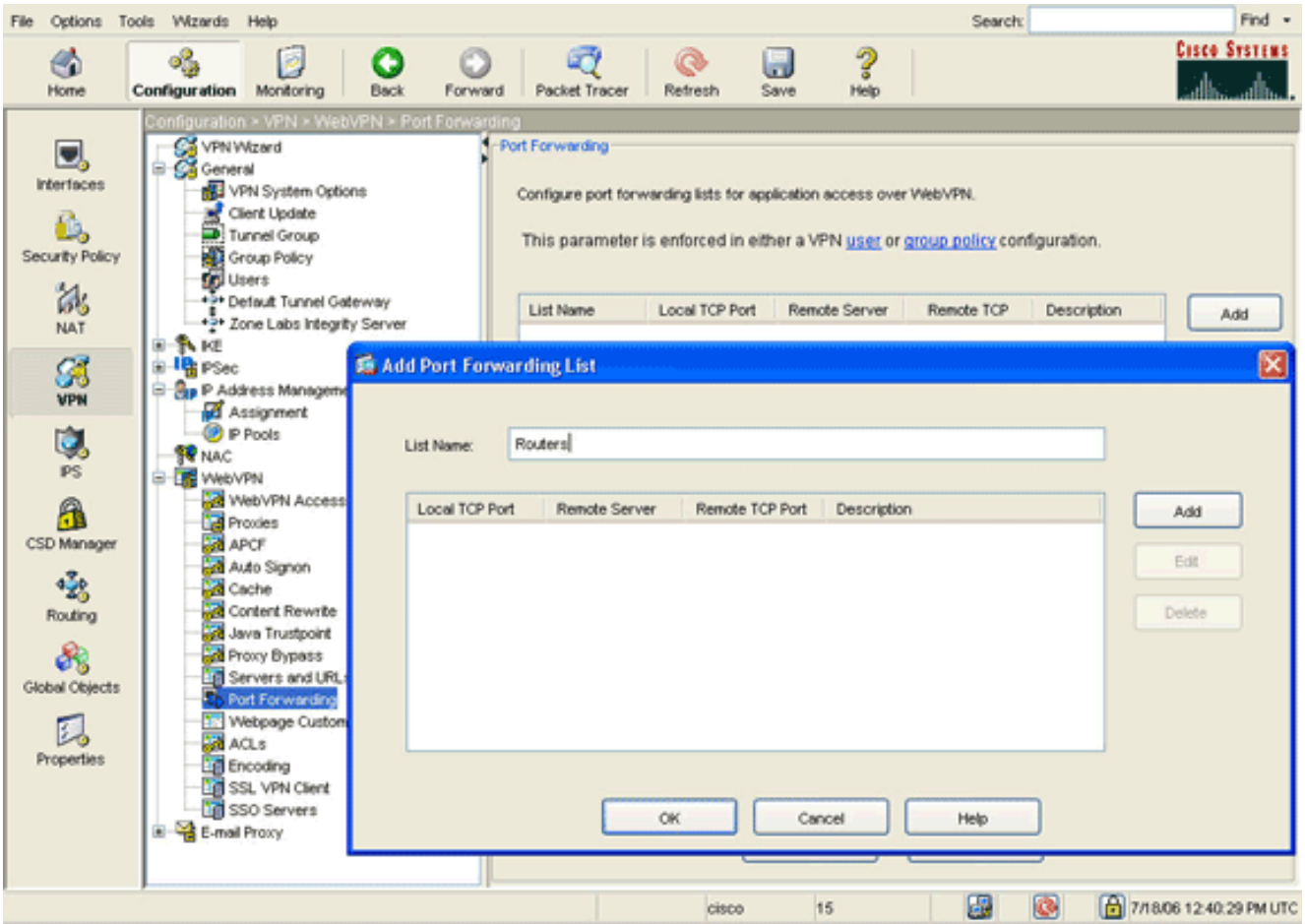
Шаг 2. Настройка характеристик переадресации портов

Для настройки характеристик переадресации портов выполните следующие шаги:

1. **Разверните WebVPN и выберите Port Forwarding (Переадресация портов).**

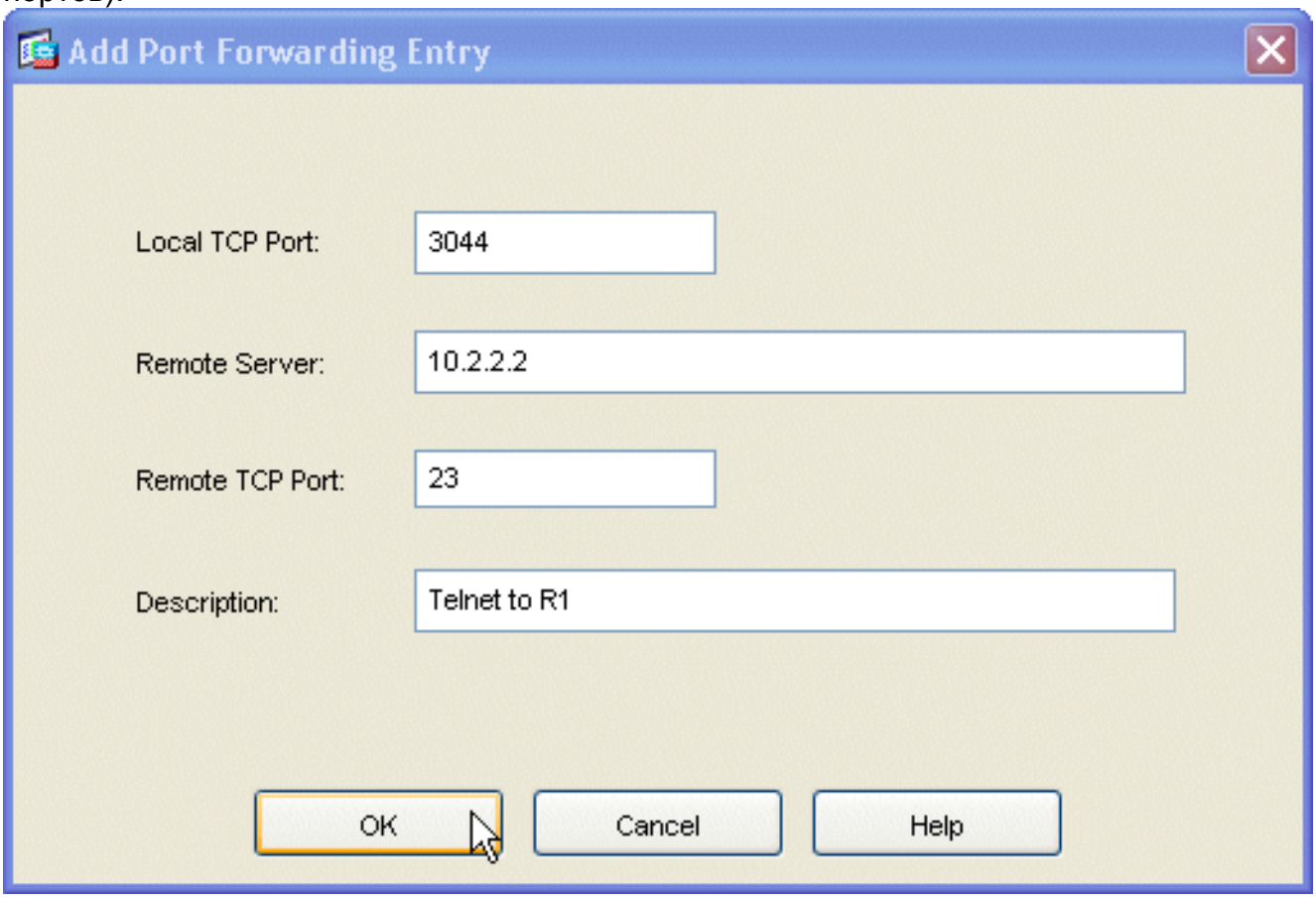


2. Нажмите кнопку Add.



3. **В диалоговом окне Add Port Forwarding List (Добавление списка переадресации портов) введите имя списка и нажмите кнопку Add (Добавить).**Появится диалоговое окно Add

Port Forwarding (Добавление переадресации портов).

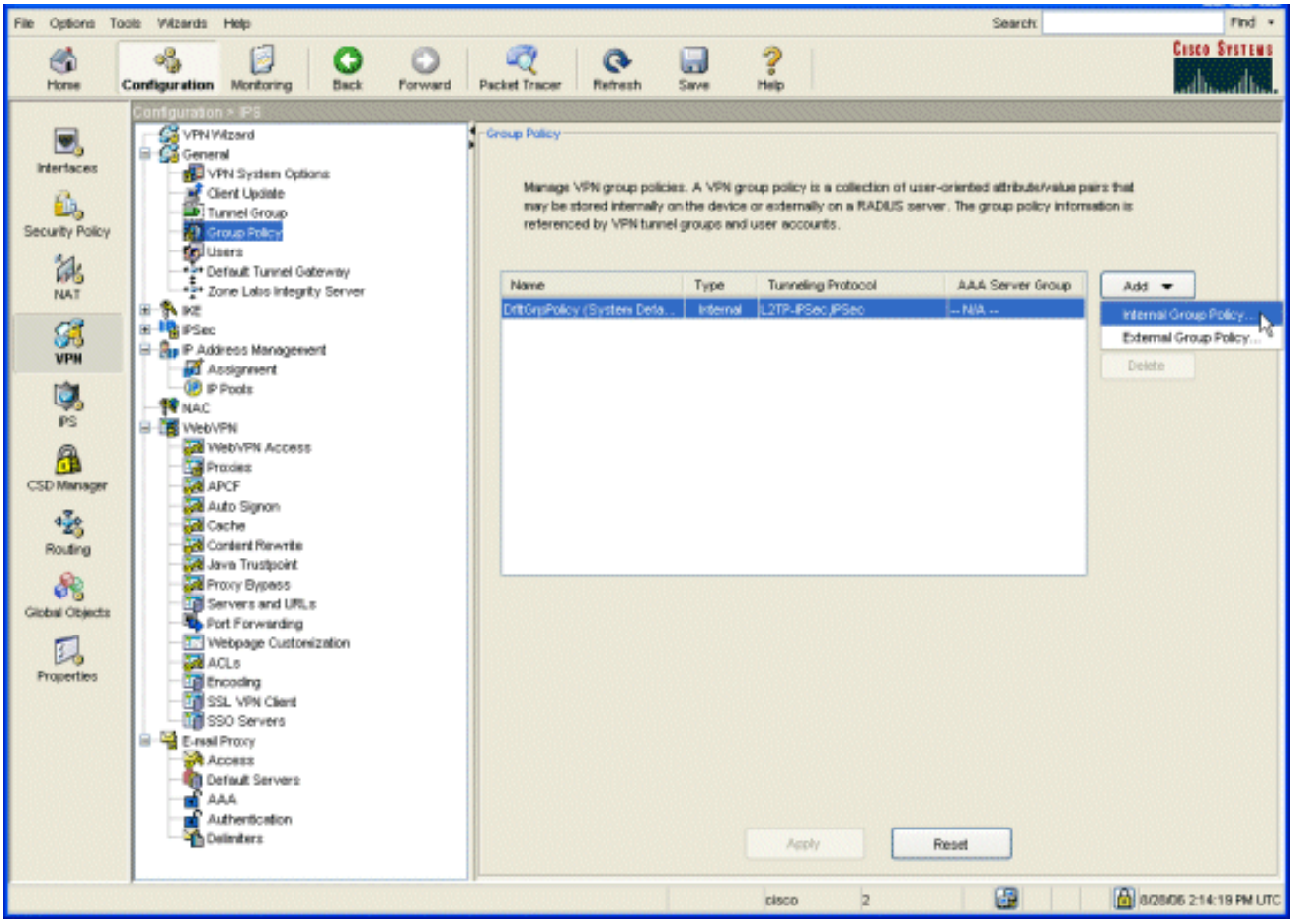


4. В диалоговом окне Add Port Forwarding Entry (Добавление записи переадресации портов) введите следующие параметры:В поле Local TCP Port (Локальный TCP-порт) введите номер порта или примите значение по умолчанию.Введенное значение может быть любым числом от 1024 до 65535.В поле Remote Server (Удаленный сервер) введите IP-адрес.В этом используется адрес маршрутизатора.В поле Remote TCP Port (Удаленный TCP-порт) введите номер порта.В этом примере используется порт 23.**В поле Description (Описание) введите описание и нажмите кнопку OK.**
5. **Нажмите кнопку OK, а затем нажмите Apply.**
6. **Нажмите Save и Yes, чтобы принять изменения.**

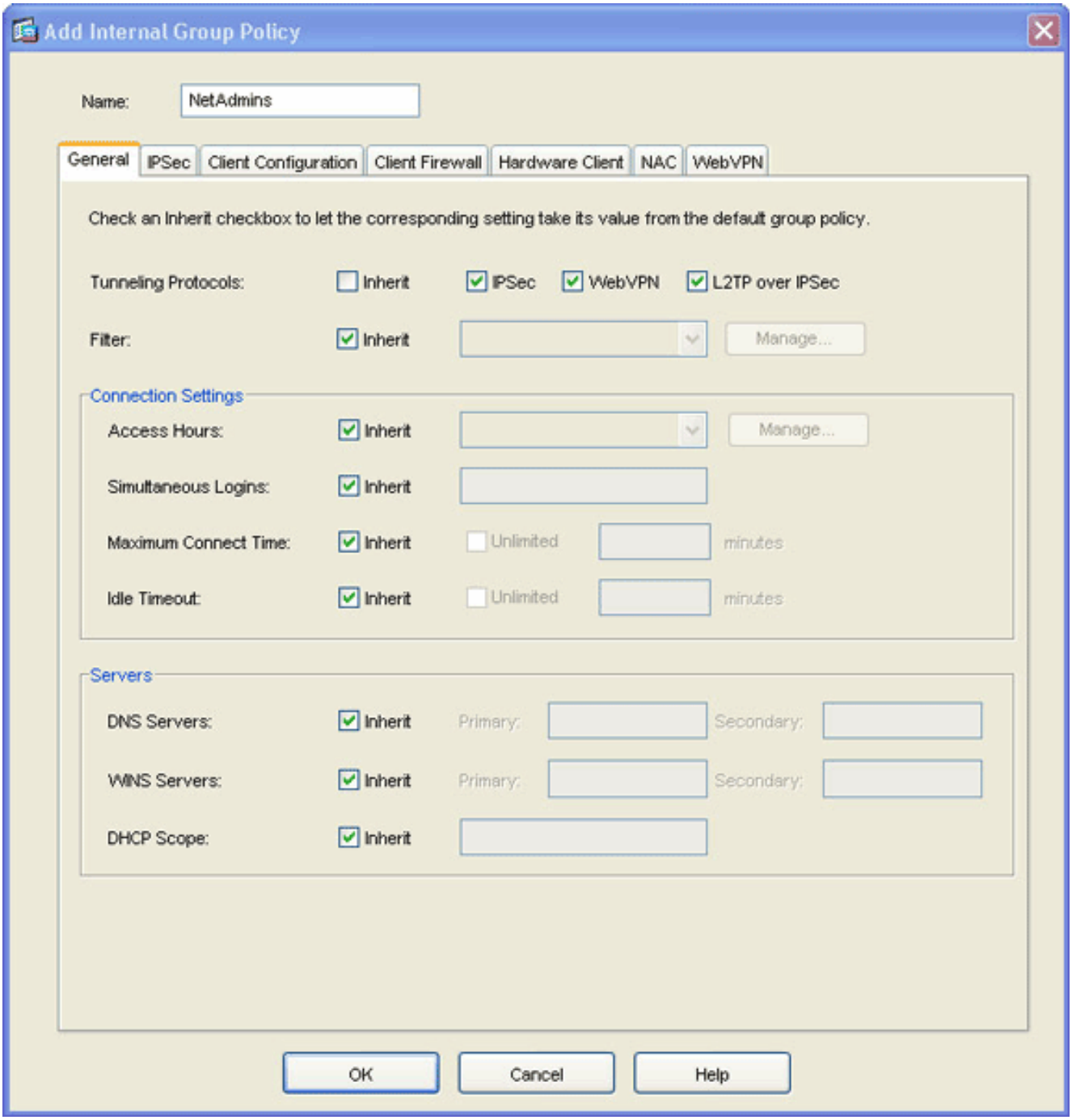
Шаг 3. Создайте Групповую политику и Ссылку это к Списку Переадресации портов

Для создания групповой политики и связывания ее со списком переадресации портов выполните следующие шаги:

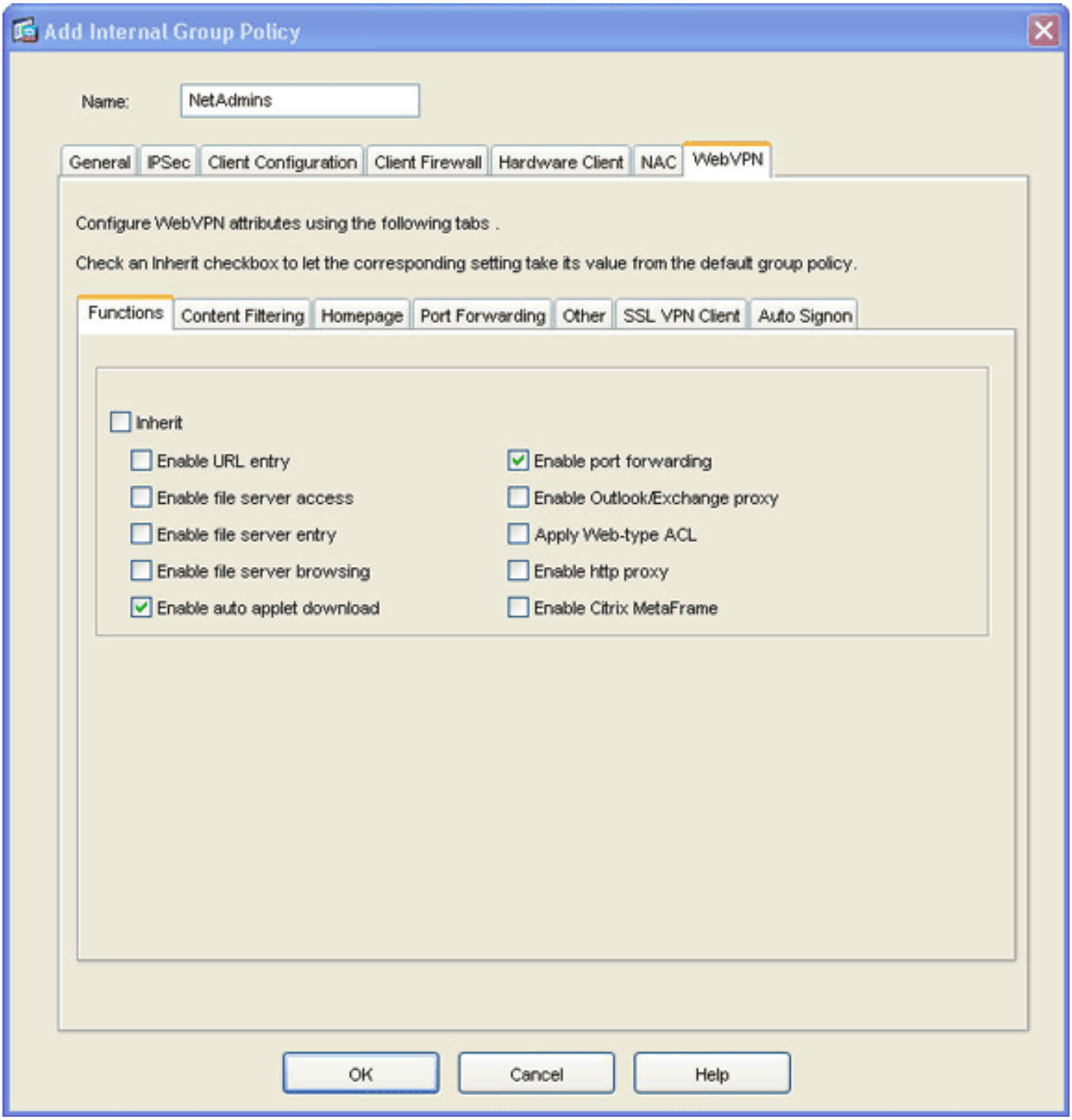
1. **Разверните раздел General (Общее) и выберите Group Policy (Групповая политика).**



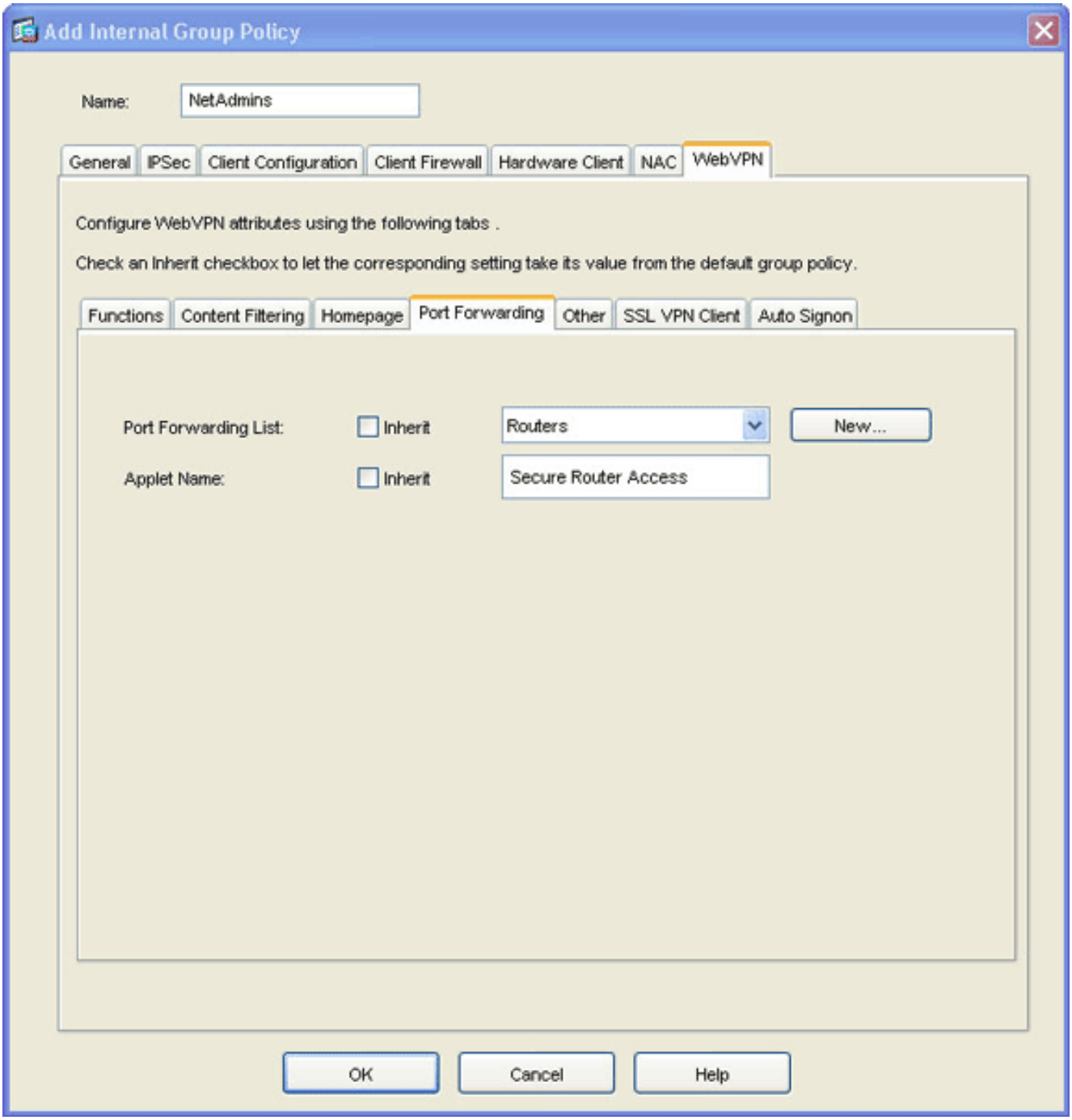
2. **Нажмите кнопку Add (Добавить) и выберите Internal Group Policy (Внутренняя групповая политика).**Откроется диалоговое окно Add Internal Group Policy (Добавление внутренней групповой
политики).



3. Введите имя групповой политики или подтвердите имя, предложенное по умолчанию.
4. **Снимите флажок Inherit (Наследовать) для протоколов туннелирования и отметьте флажок WebVPN.**
5. **Откройте вкладку WebVPN вверху диалогового окна и выберите вкладкуFunctions (Функции).**
6. **Снимите флажок Inherit (Наследовать) и отметьте флажки Enable auto applet download (Разрешить автоматическую загрузку апплета) и Enable port forwarding (Разрешить переадресацию портов), как показано на рисунке:**



7. Также на вкладке WebVPN выберите вкладку Port Forwarding (Переадресация портов) и снимите флажок Inherit (Наследовать) у списка переадресации портов.



8. **Щелкните стрелку раскрывающегося списка Port Forwarding List (Список переадресации портов) и выберите список переадресации портов, созданный на шаге 2.**
9. **Снимите флажок Inherit (Наследовать) у имени апплета и измените имя в текстовом поле.**Клиент отображает имя апплета при подключении.
10. **Нажмите кнопку OK, а затем нажмите Apply.**
11. **Нажмите Save и Yes, чтобы принять изменения.**

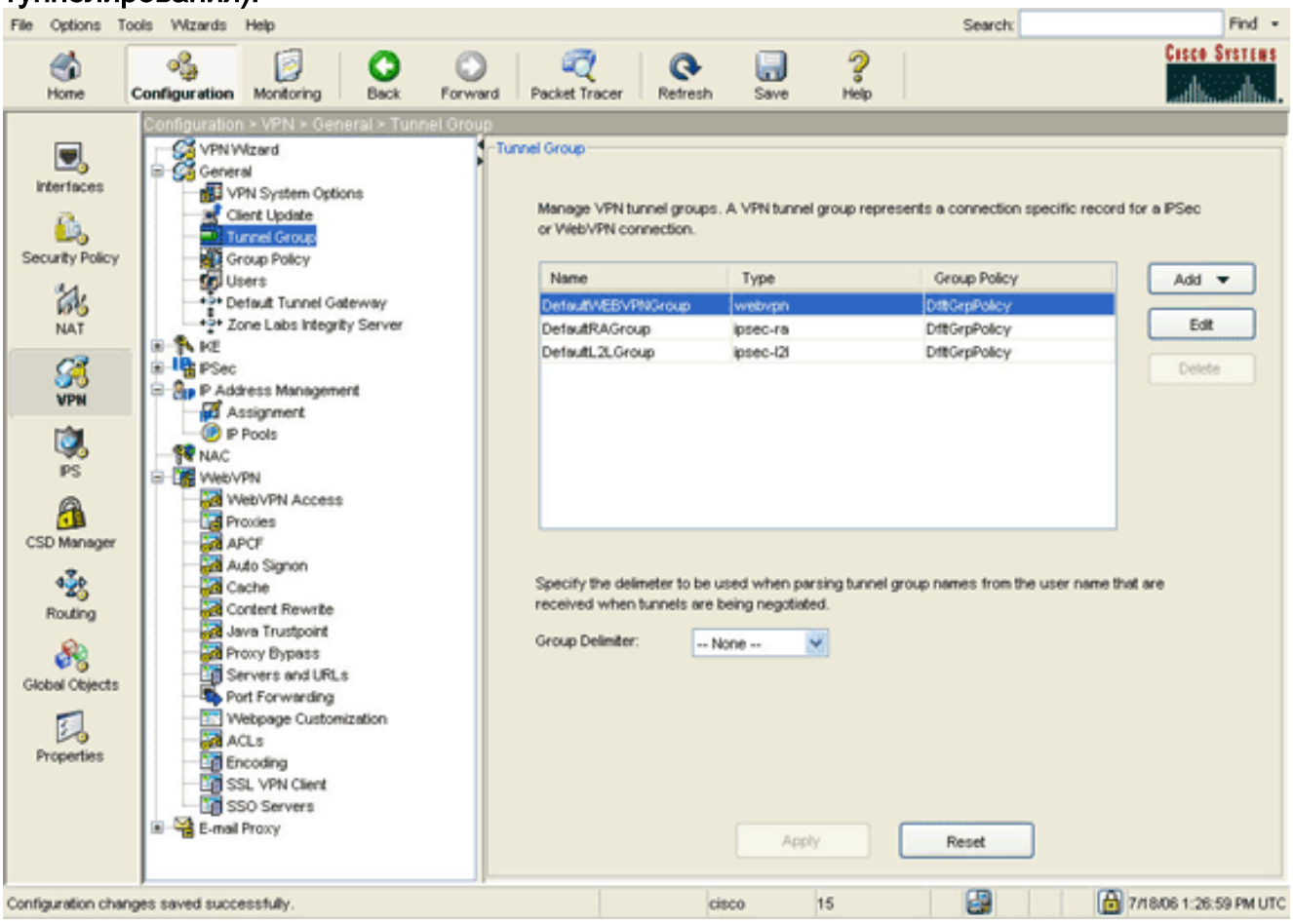
Шаг 4. . Создайте Туннельную группу и Ссылку это к Групповой политике

Можно отредактировать группу туннелирования DefaultWebVPNGroup по умолчанию или создать новую группу туннелирования.

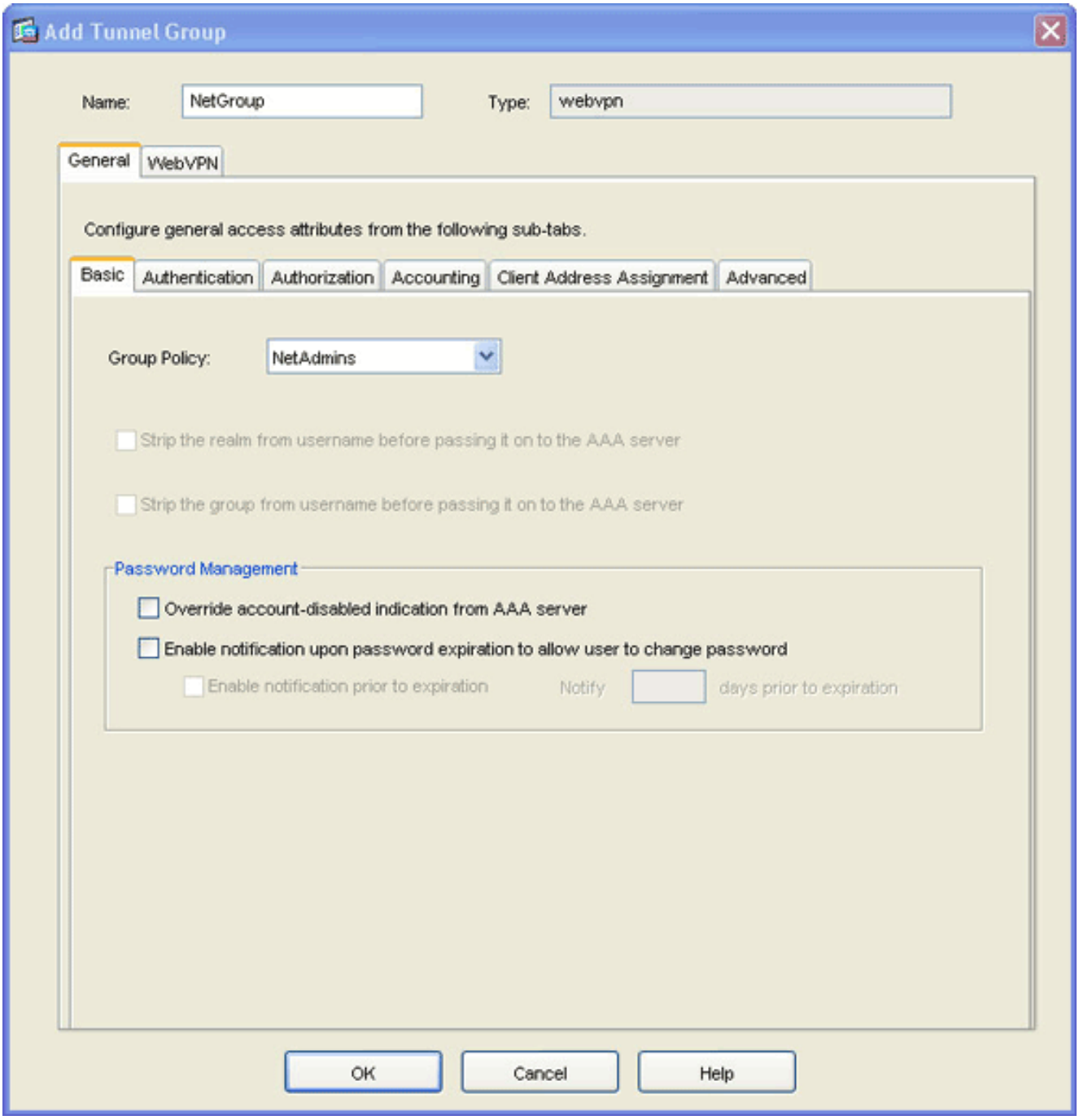
Для создания новой группы туннелирования выполните следующие действия:

1. **Разверните раздел General (Общее) и выберите Tunnel Group (Группа**

туннелирования).



2. **Нажмите кнопку Add (Добавить) и выберите WebVPN Access (Доступ WebVPN).**Появится диалоговое окно Add Tunnel Group (Добавление группы туннелирования).

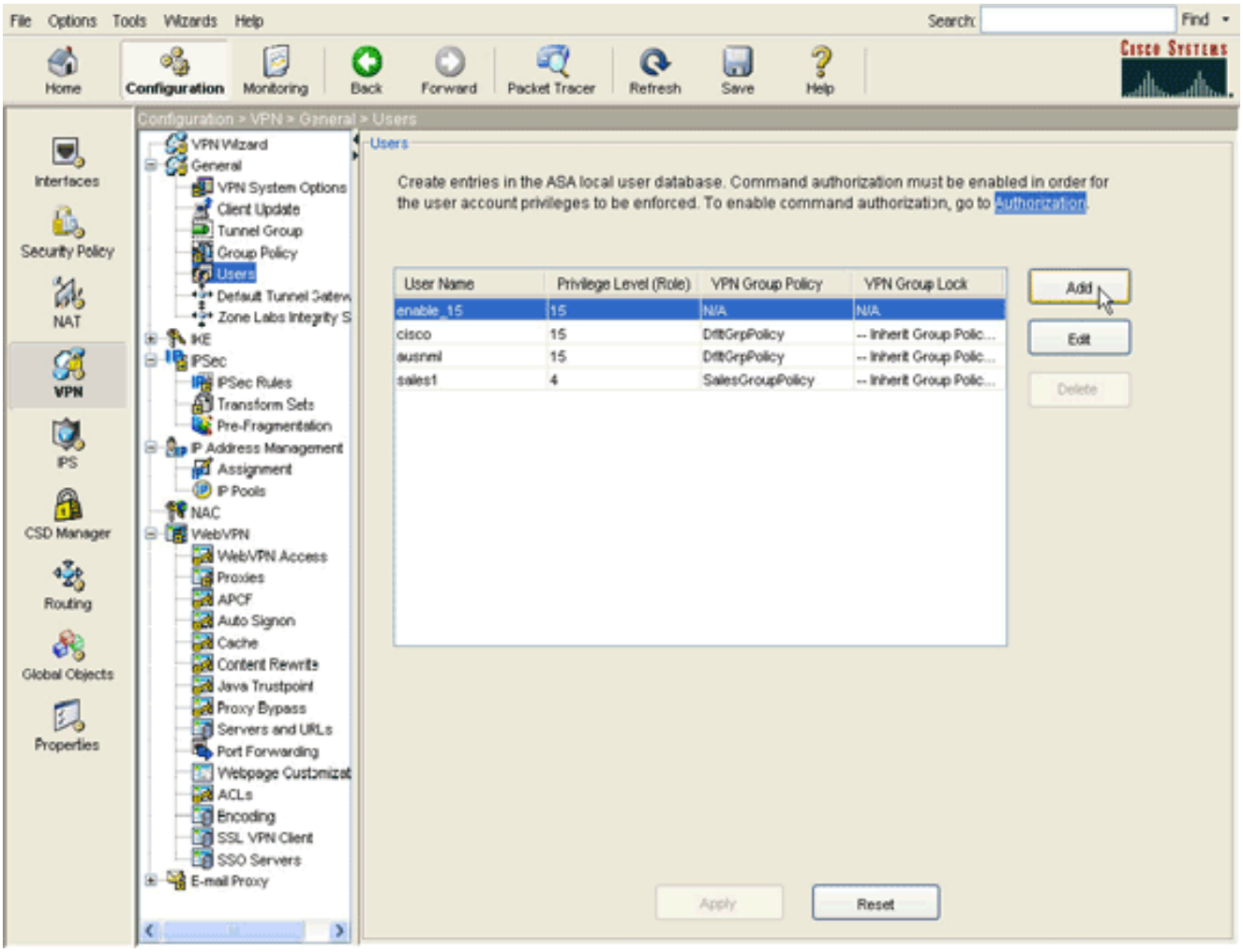


3. Введите имя в поле Name (Имя).
4. **Щелкните стрелку раскрывающегося списка Group Policy (Групповая политика) и выберите групповую политику, созданную на шаге 3.**
5. **Нажмите кнопку OK, а затем нажмите Apply.**
6. **Нажмите Save и Yes, чтобы принять изменения.**Группа туннелирования, групповая политика и характеристики переадресации портов теперь связаны.

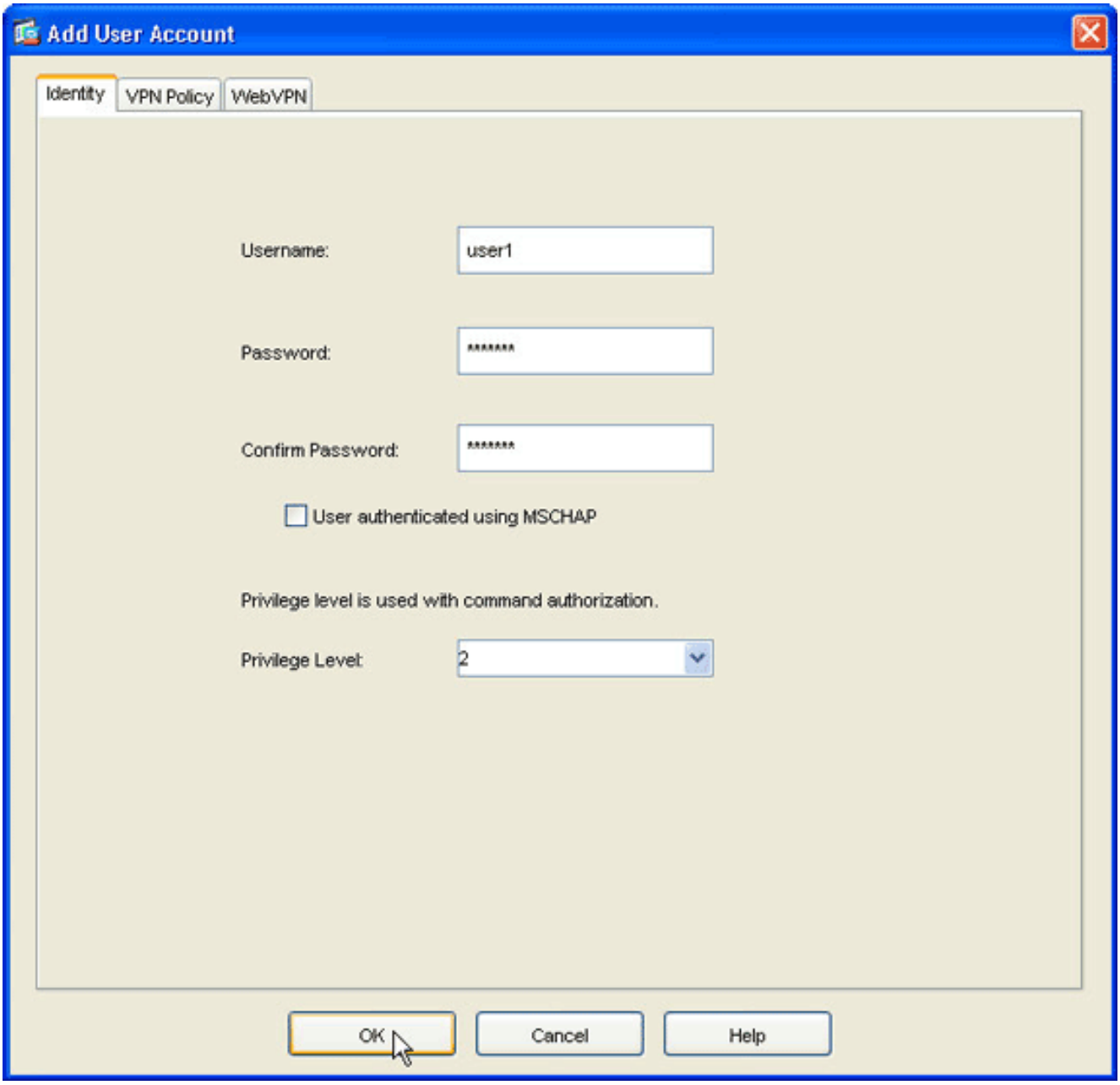
Шаг 5. . Создайте пользователя и добавьте что пользователь к групповой политике

Для создания пользователя и добавления его в групповую политику выполните следующие шаги:

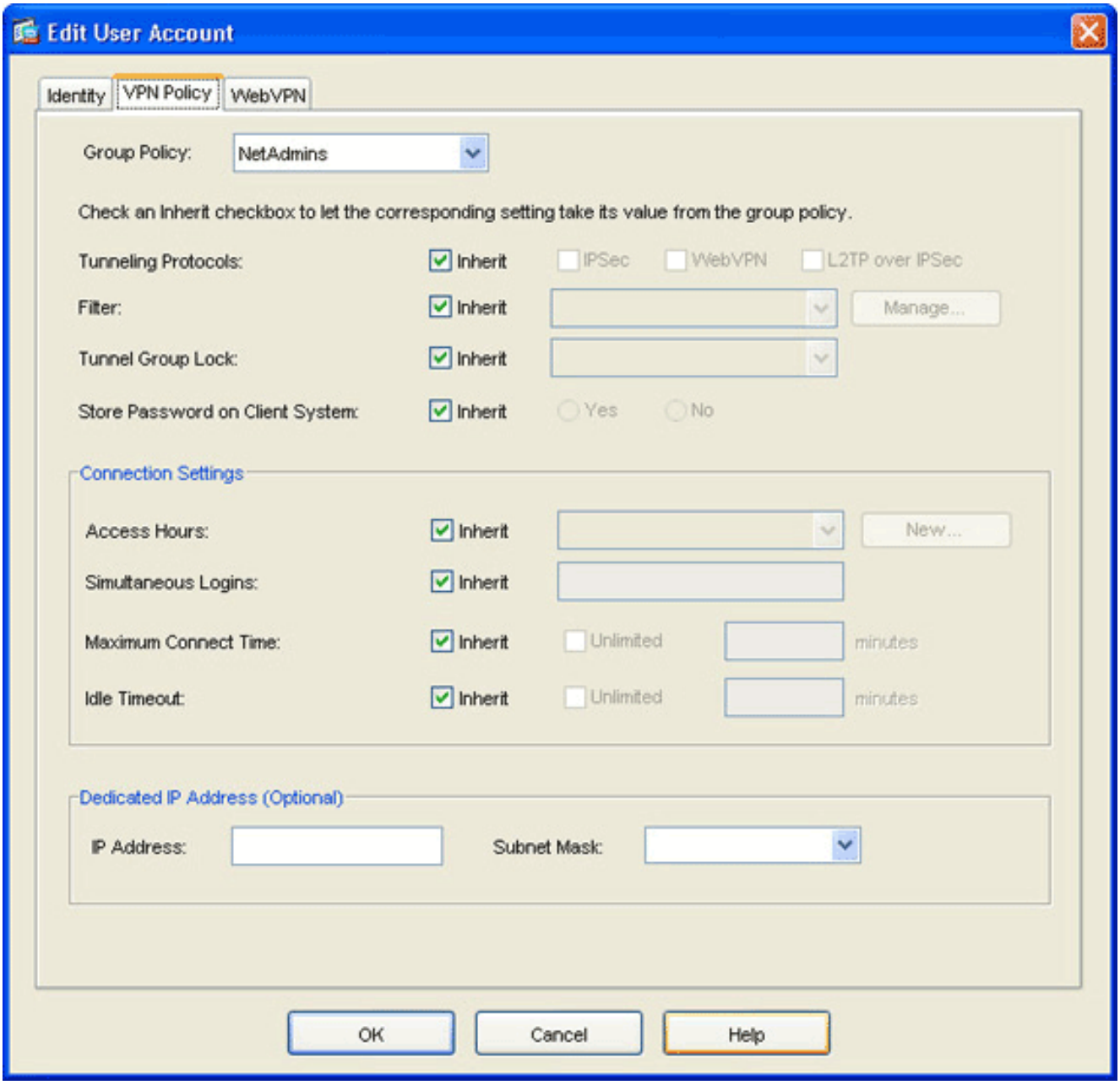
1. **Разверните раздел General (Общее) и выберите Users (Пользователи).**



2. **Нажмите кнопку Add.**Появляется диалоговое окно «Add User Account» (Добавление учетной записи пользователя).



3. Введите значения имени пользователя, пароля и сведения о полномочиях, затем выберите вкладкуVPN Policy (Политика VPN).



4. **Щелкните стрелку раскрывающегося списка Group Policy (Групповая политика) и выберите групповую политику, созданную на шаге 3.**Пользователь наследует характеристики WebVPN и политики выбранной групповой политики.
5. **Нажмите кнопку OK, а затем нажмите Apply.**
6. **Для подтверждения изменения выберите Save (Сохранить) и затем Yes (Да).**

Настройка тонкого клиента SSL VPN посредством интерфейса командной строки

ASA
ASA Version 7.2(1) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside

```
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Output truncated port-forward portforward 3044
10.2.2.2 telnet Telnet to R1 !--- Configure the set of
applications that WebVPN users !--- can access over
forwarded TCP ports group-policy NetAdmins internal !--
- Create a new group policy for enabling WebVPN access
group-policy NetAdmins attributes vpn-tunnel-protocol
IPSec l2tp-ipsec webvpn !--- Configure group policy
attributes webvpn functions port-forward auto-download
!--- Configure group policies for WebVPN port-forward
value portforward !--- Configure port-forward to enable
WebVPN application access !--- for the new group policy
port-forward-name value Secure Router Access !---
Configure the display name that identifies TCP port !--
- forwarding to end users username user1 password
tJsDL6po9m1UFs.h encrypted username user1 attributes
vpn-group-policy NetAdmins !--- Create and add User(s)
to the new group policy http server enable http 0.0.0.0
0.0.0.0 DMZ no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart tunnel-group NetGroup type
webvpn tunnel-group NetGroup general-attributes
default-group-policy NetAdmins !--- Create a new tunnel
group and link it to the group policy telnet timeout 5
ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp
inspect sip inspect xdmcp ! service-policy
global_policy global webvpn enable outside !--- Enable
Web VPN on Outside interface port-forward portforward
3044 10.2.2.2 telnet Telnet to R1 prompt hostname
context
```

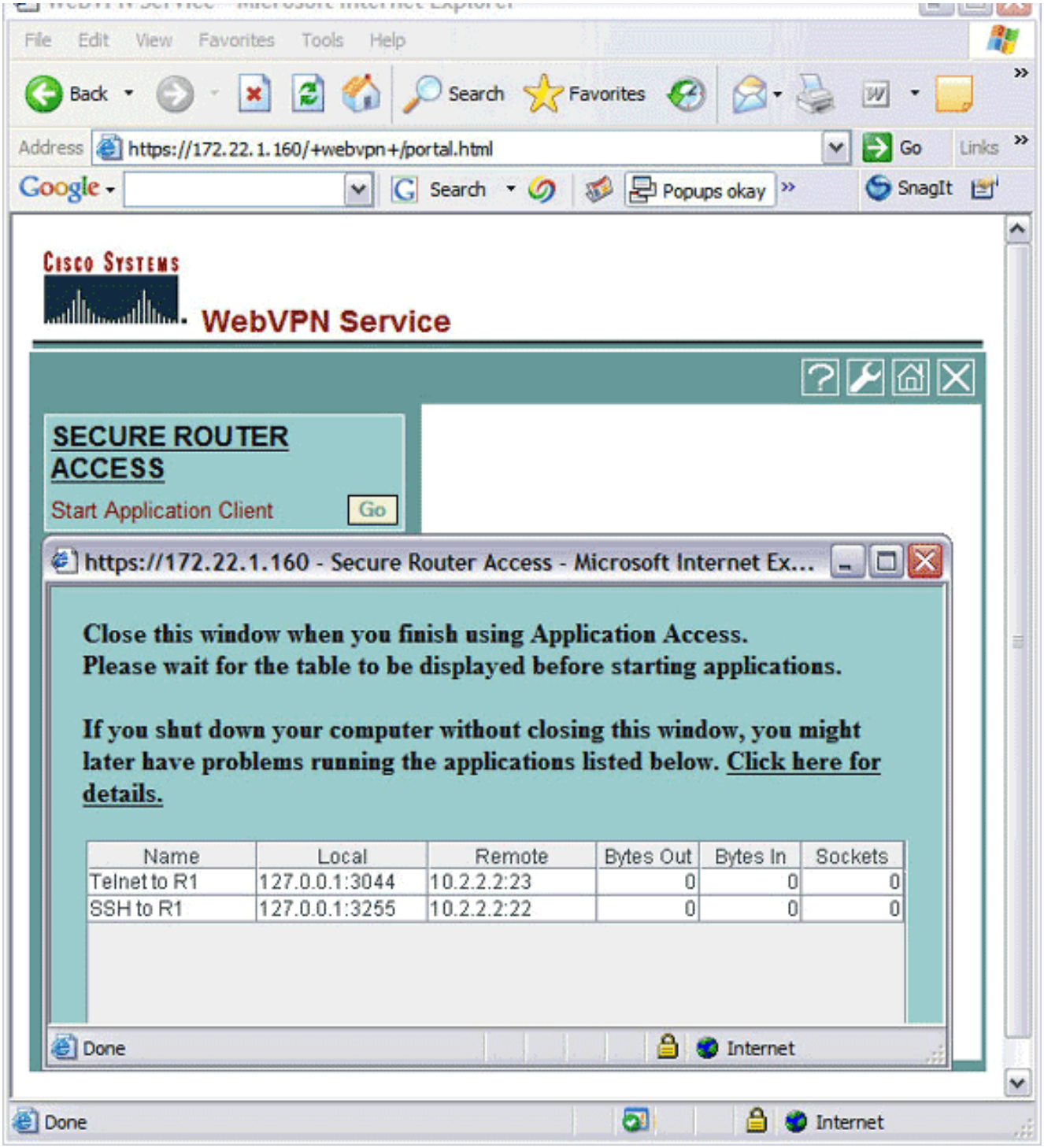
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Процедура

Ниже приведен порядок действий для проверки действительности конфигурации и испытания конфигурации.

1. *С рабочей станции клиента введите https://внешний_IP-адрес_ASA, где внешний_IP-адрес_ASA— URL-адрес устройства ASA для доступа с шифрованием SSL.*После принятия электронного сертификата и прохождения аутентификации пользователя открывается web-страница WebVPN Services (Службы WebVPN).

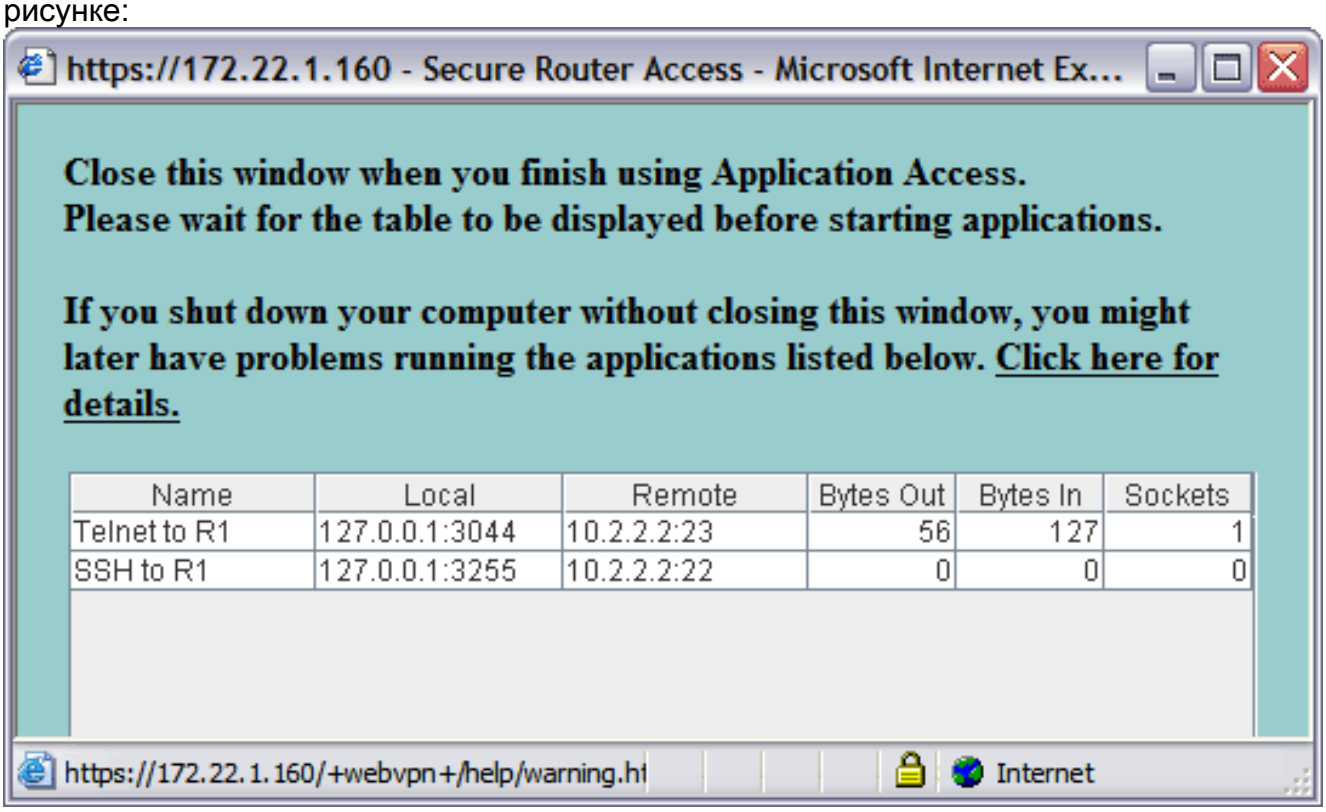


В столбце локальных параметров указываются адрес и параметры портов для доступа к приложению. Столбцы Bytes Out (Отправлено байт) и Bytes In (Получено байт) сообщают об отсутствии каких-либо действий, поскольку приложение еще не запущено.

2. Для запуска сеанса Telnet используйте приглашение DOS или другое приложение Telnet.
3. **В командной строке введите: telnet 127.0.0.1 3044.Примечание:** Эта команда предоставляет пример того, как получить доступ к локальному порту, отображенному в образе веб-страницы Сервиса WebVPN в этом документе. *Двоеточие (:) не является частью команды:).* Вводят команду так, как описано в этом документе.Устройство ASA получает команду по защищенному сеансу, а поскольку оно хранит информацию в виде привязок, оно сразу узнает о необходимости открытия защищенного сеанса Telnet с привязанным
устройством.

После ввода имени пользователя и пароля получение доступа к устройству завершается.

4. Для проверки доступа к устройству обратитесь к значениям столбцов Bytes Out (Отправлено байт) и Bytes In (Получено байт), как показано на рисунке:



Команды

Некоторые команды show связаны с WebVPN. Эти команды можно выполнить в интерфейсе командной строки (CLI) для отображения статистики и другой информации. **Дополнительные сведения о командах show см. в разделе Проверка конфигурации WebVPN.**

Примечание: Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать**

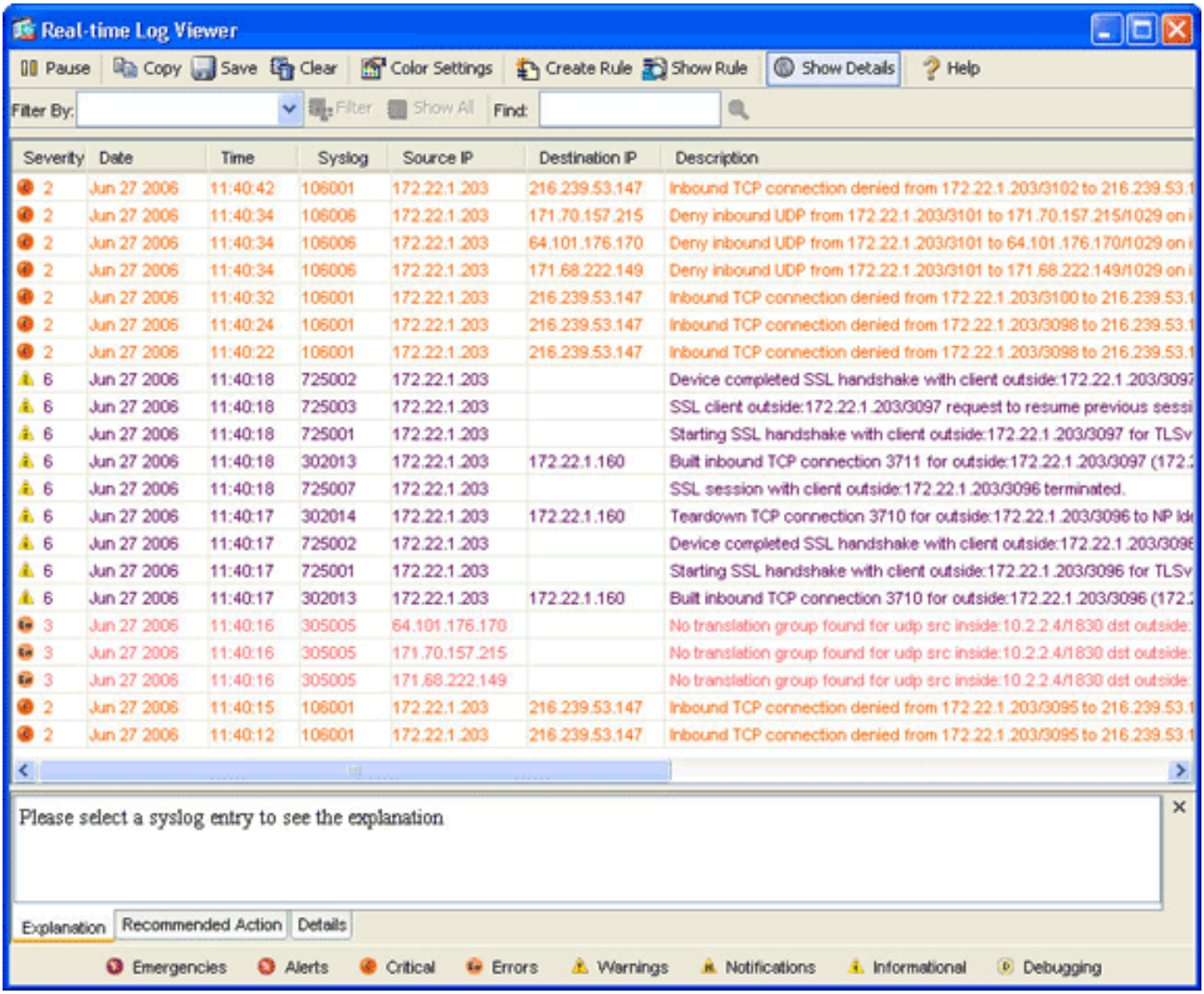
выходные данные команд show.

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Завершается ли процесс согласования SSL?

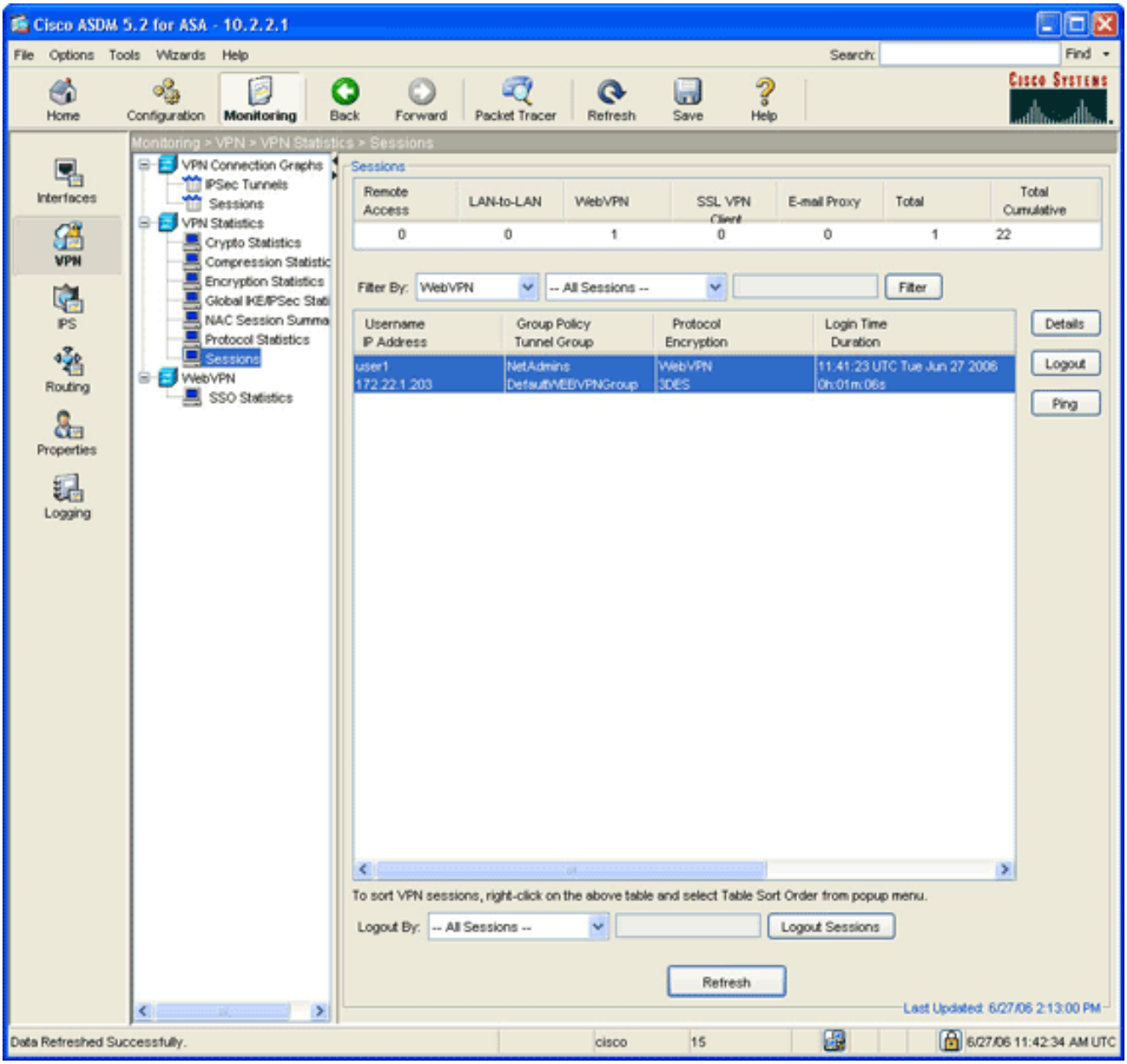
После подключения к устройству ASA проверьте, сообщает ли журнал реального времени о завершении согласования SSL.



Работоспособен ли тонкий клиент SSL VPN?

Для проверки работоспособности тонкого клиента SSL VPN выполните следующие шаги:

1. **Выберите Monitoring (Контроль), затем выберите VPN.**
2. **Разверните раздел VPN Statistics и выберите Sessions (Сеансы).**Сеанс тонкого клиента SSL VPN должен появиться в списке сеансов. Убедитесь, что действует фильтр по соединениям WebVPN, как показано на
рисунке:



Команды

Некоторые команды debug связаны с WebVPN. Дополнительную информацию о данных командах см. в документе Использование команд WebVPN debug.

Примечание: Использование команд debug может неблагоприятно сказаться на производительности модуля Cisco. Перед использованием команд debug ознакомьтесь с документом Важные сведения о командах debug.

Дополнительные сведения

- Пример конфигурации бесклиентного SSL VPN (WebVPN) на ASA
- Пример настройки SSL клиента VPN (SVC) на ASA с ASDM
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Пример настройки ASA с WebVPN и единым входом при использовании ASDM NTLMv1
- Cisco Systems – техническая поддержка и документация