Пример конфигурации бесклиентной SSL VPN (WebVPN) на Cisco IOS с SDM

Содержание

Введение

Clientless SSL VPN (WebVPN) предоставляет пользователю возможность безопасного доступа к ресурсам корпоративной LAN из любой точки с помощью веб-браузера с поддержкой SSL. Сначала пользователь проходит аутентификацию на шлюзе WebVPN, который затем предоставляет пользователю доступ к предварительно настроенным ресурсам сети. Шлюзы WebVPN можно настроить на маршрутизаторах Cisco IOS®, устройствах адаптивной безопасности Cisco (ASA), концентраторах Cisco VPN 3000 и модуле служб Cisco WebVPN для маршрутизаторов Catalyst 6500 и 7600.

Технологию SSL VPN можно настроить на устройствах Cisco в трех основных режимах: Clientless SSL VPN — бесклиентный, Thin-Client SSL VPN (переадресация портов) — с тонким клиентом и SSL VPN Client (туннельный режим SVC) — с обычным клиентом. В этом документе показана настройка WebVPN на маршрутизаторах Cisco IOS.

Примечание: Не делайте для изменения или IP domain name или имени хоста

маршрутизатора, поскольку это инициирует регенерацию подписанного сертификата и отвергнет настроенную точку доверия. Восстановление самозаверенного сертификата приводит к ошибкам подключения, если маршрутизатор был настроен для WebVPN. WebVPN привязывает имя доверенной точки SSL к конфигурации шлюза WebVPN. Поэтому при выпуске нового самозаверенного сертификата новое имя доверенной точки не соответствует конфигурации WebVPN и пользователи не могут установить соединение.

Примечание: Если вы выполняете **команду ip https-secure server** на маршрутизаторе WebVPN, который использует персистентный подписанный сертификат, новый ключ RSA генерируется, и сертификат становится недопустимым. Создается новая доверенная точка, что приводит к разрыву SSL WebVPN. **Если маршрутизатор, использующий постоянный самозаверенный сертификат, перезагрузить после выполнения команды ip https-secure server, возникнет та же проблема.**

Дополнительные сведения о тонком клиенте SSL VPN см. в разделе Пример конфигурации тонкого клиента SSL VPN (WebVPN) IOS с SDM.

Дополнительные сведения о клиенте SSL VPN см. в разделе Пример конфигурации клиента SSL VPN (SVC) на IOS с SDM.

SSL VPN работает на следующих платформах маршрутизаторов Cisco:

- Маршрутизаторы Cisco серий 870, 1811, 1841, 2801, 2811, 2821 и 2851
- Маршрутизаторы Cisco 3725, 3745, 3825, 3845, 7200 и 7301

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Расширенный образ ПО Cisco IOS версии 12.4(6)T или более поздних версий
- Одна из платформ маршрутизаторов Cisco, перечисленных в разделе Введение

Используемые компоненты

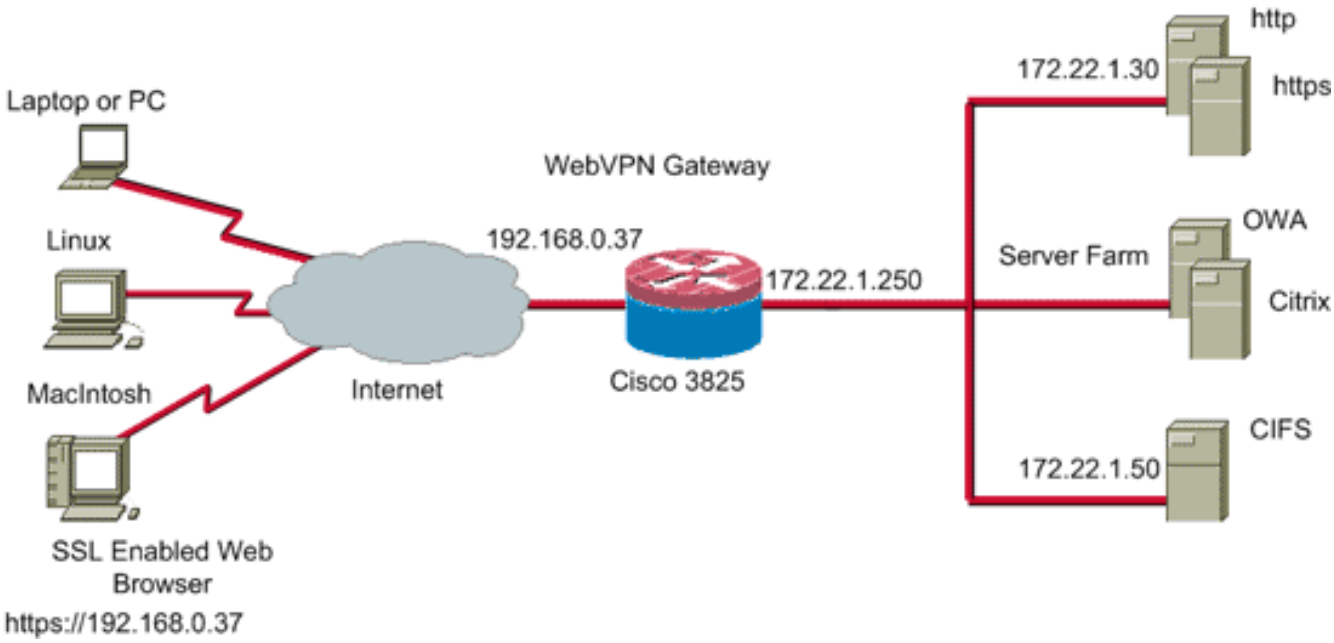
Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор Cisco 3825
- Образ ПО Advanced Enterprise — ПО Cisco IOS версии 12.4(9)T
- Cisco Router and Security Device Manager (SDM), версия 2.3.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования. IP-адреса, используемые в этом примере, взяты из адресов RFC 1918, которые являются частными и не могут использоваться в Интернете.

Схема сети

В настоящем документе используется следующая схема сети:



Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Предварительные действия

Прежде чем начать, выполните следующие действия:

1. Настройте имя узла и доменное имя.
2. Настройте маршрутизатор для SDM. Некоторые маршрутизаторы Cisco поставляются с предустановленной копией SDM.Если Cisco SDM не установлен на маршрутизаторе, можно загрузить бесплатную копию со страницы Загрузка ПО (только для зарегистрированных пользователей) . Для этого необходима учетная запись CCO и контракт на обслуживание. Дополнительные сведения об установке и настройке SDM см. в разделе Cisco Router and Security Device Manager.
3. Установите на маршрутизаторе правильную дату, время и часовой пояс.

Настройка WebVPN на Cisco IOS

С одним устройством может быть связано несколько шлюзов WebVPN. Каждый шлюз WebVPN связан только с одним IP-адресом на маршрутизаторе. Для определенного шлюза WebVPN можно создать больше одного контекста WebVPN. Чтобы идентифицировать отдельные контексты, снабдите каждый из них уникальным именем. Одна группа политик может быть связана только с одним контекстом WebVPN. Группа политик описывает, какие ресурсы доступны в определенном контексте WebVPN.

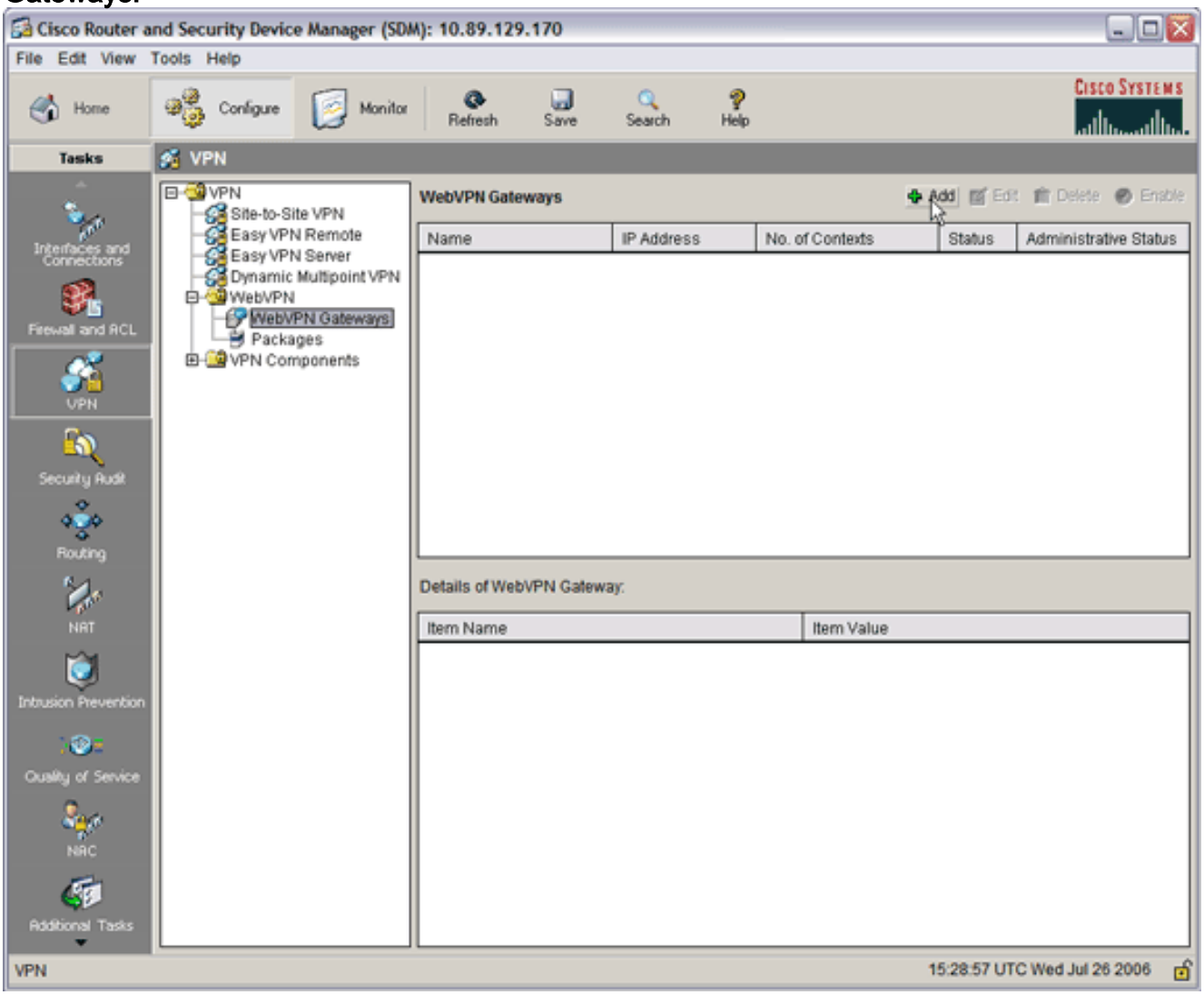
Чтобы настроить WebVPN на Cisco IOS, выполните следующие действия:

1. Настройка шлюза WebVPN
2. Настройка ресурсов, разрешенных для группы политик
3. Настройка группы политик WebVPN и выбор ресурсов
4. Настройка WebVPN-контекста
5. Настройка базы данных пользователей и метода аутентификации

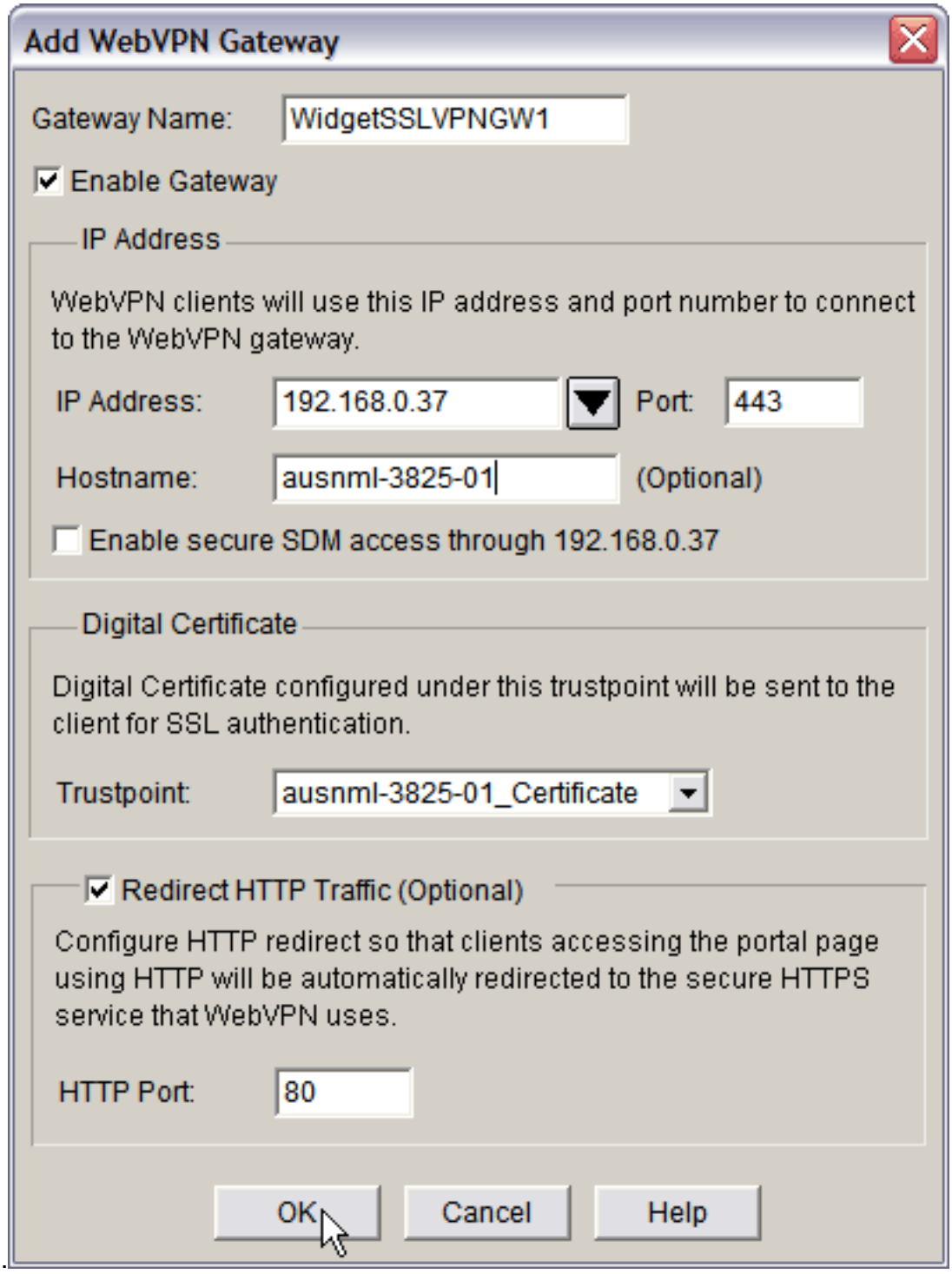
Шаг 1. Настройка шлюза WebVPN

Чтобы настроить шлюз WebVPN, выполните следующие действия:

1. **В приложении SDM нажмите Configure и VPN.**
2. **Разверните WebVPN и выберите WebVPN Gateways.**



3. **Нажмите Add.**Появляется диалоговое окно «Add WebVPN Gateway» (Добавление шлюза



WebVPN).

4. **Введите данные в поля "Gateway Name" (Имя шлюза)) и "IP Address" (IP-адрес) и установите флажок Enable Gateway.**
5. **Установите флажок Redirect HTTP Traffic и нажмите OK.**
6. **Нажмите Save и Yes, чтобы принять изменения.**

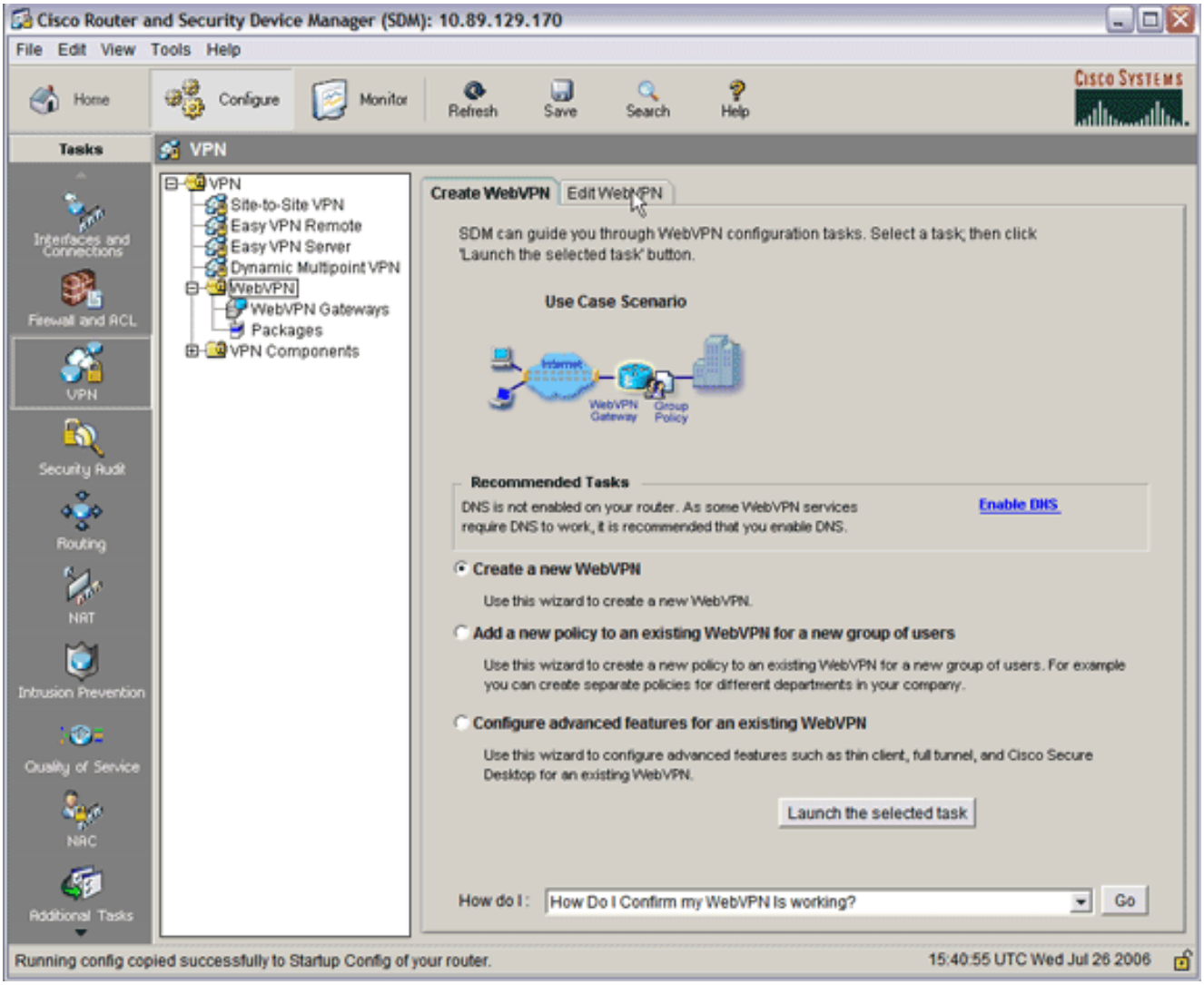
Шаг 2. Настройка ресурсов, разрешенных для группы политик

Чтобы упростить добавление ресурсов в группу политик, можно настроить ресурсы до создания группы политик.

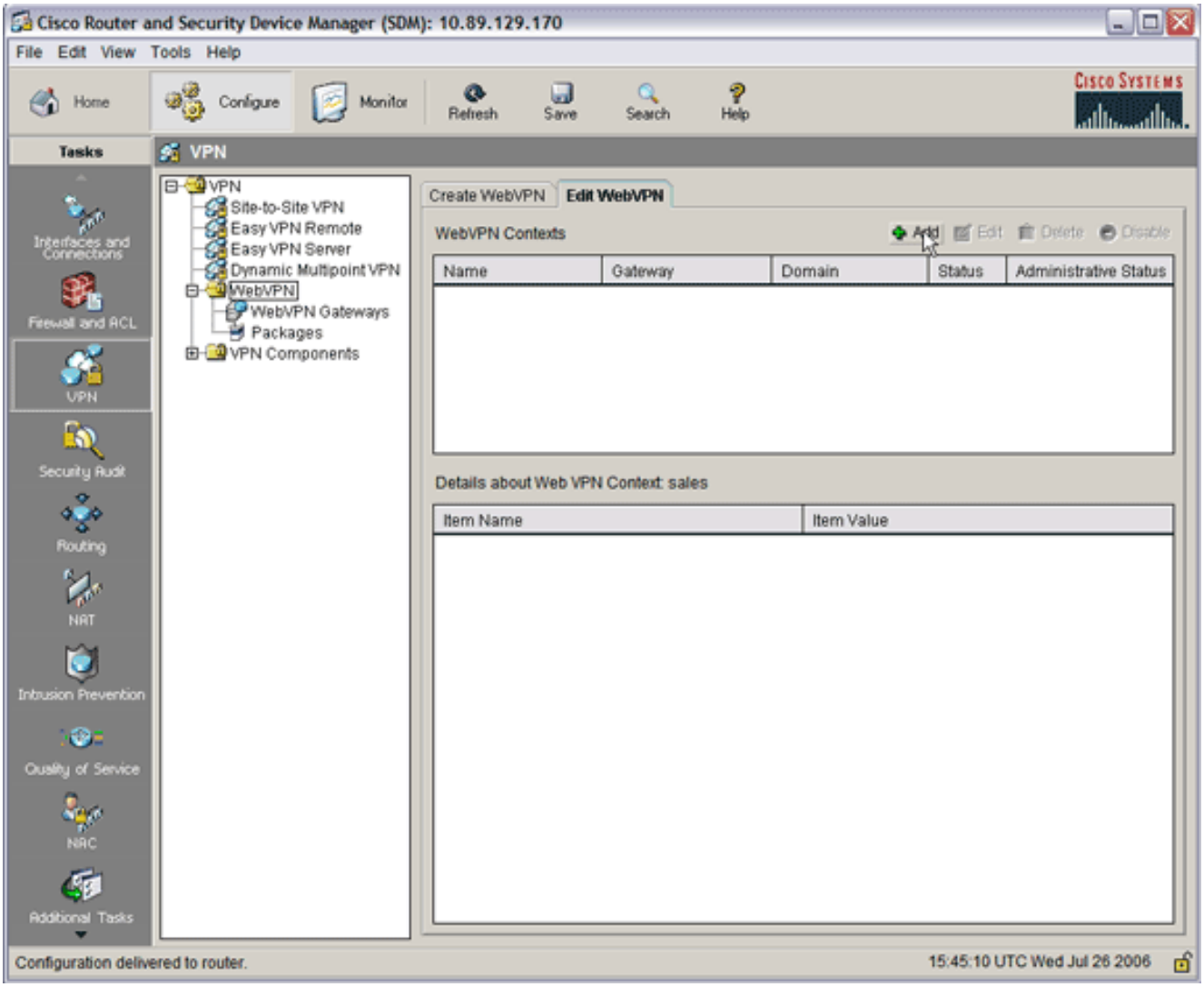
Чтобы настроить ресурсы, разрешенные для группы политик, выполните следующие действия:

1. **Нажмите Configure и**

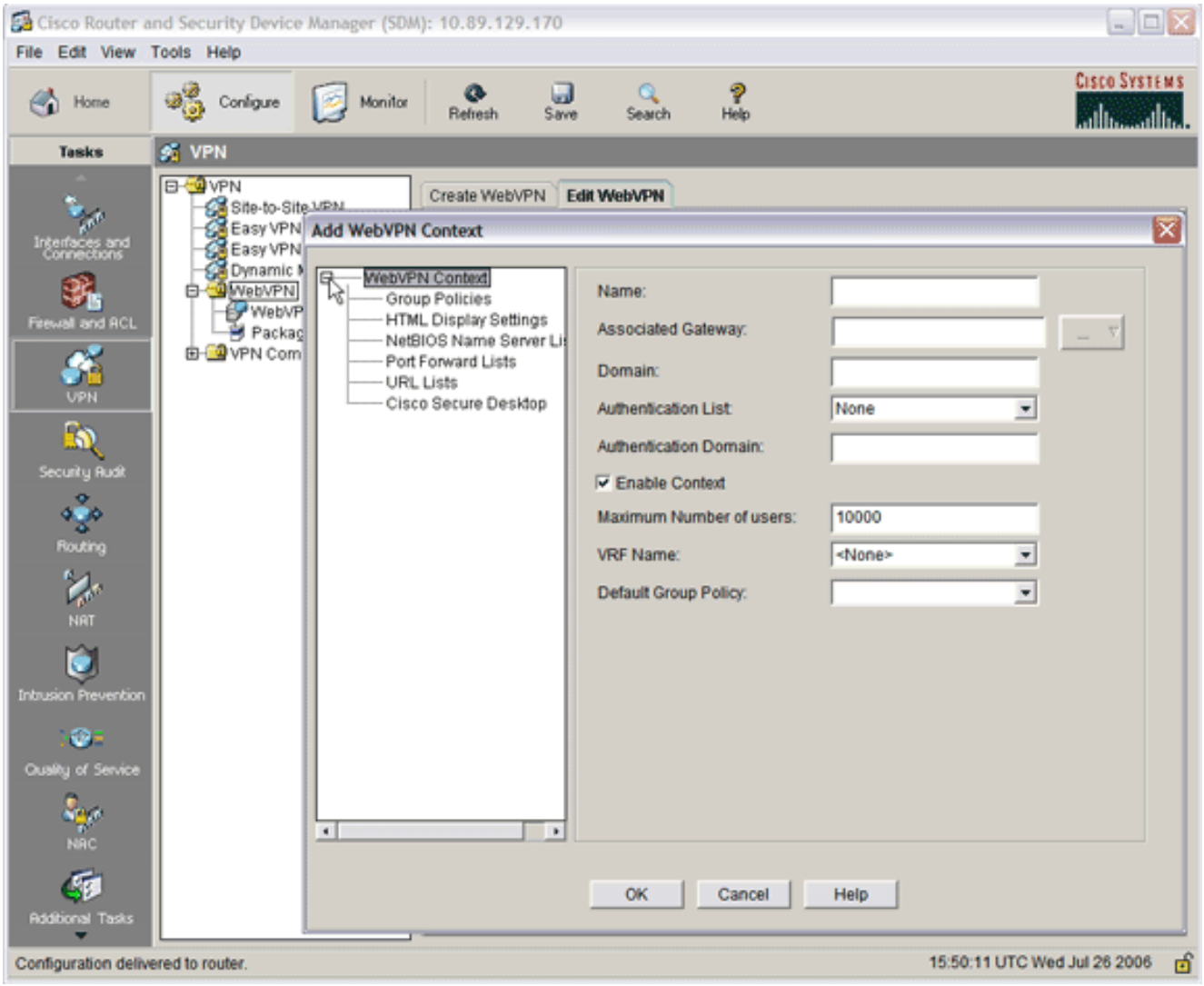
VPN.



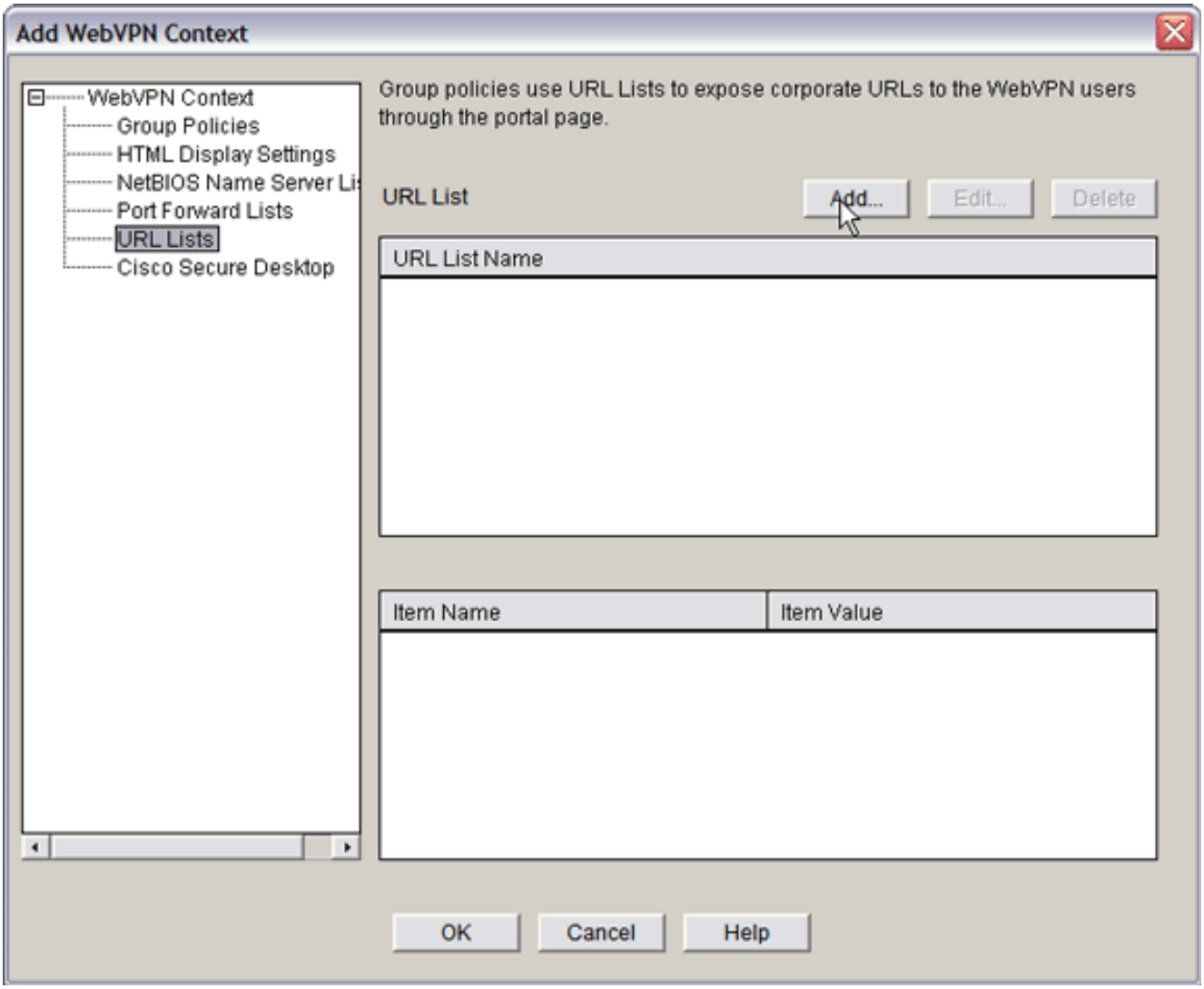
2. **Выберите WebVPN и щелкните вкладку Edit WebVPN.Примечание: WebVPN** позволяет вам настраивать доступ для HTTP, HTTPS, просмотра файлов Windows через Протокол CIFS и
Citrix.



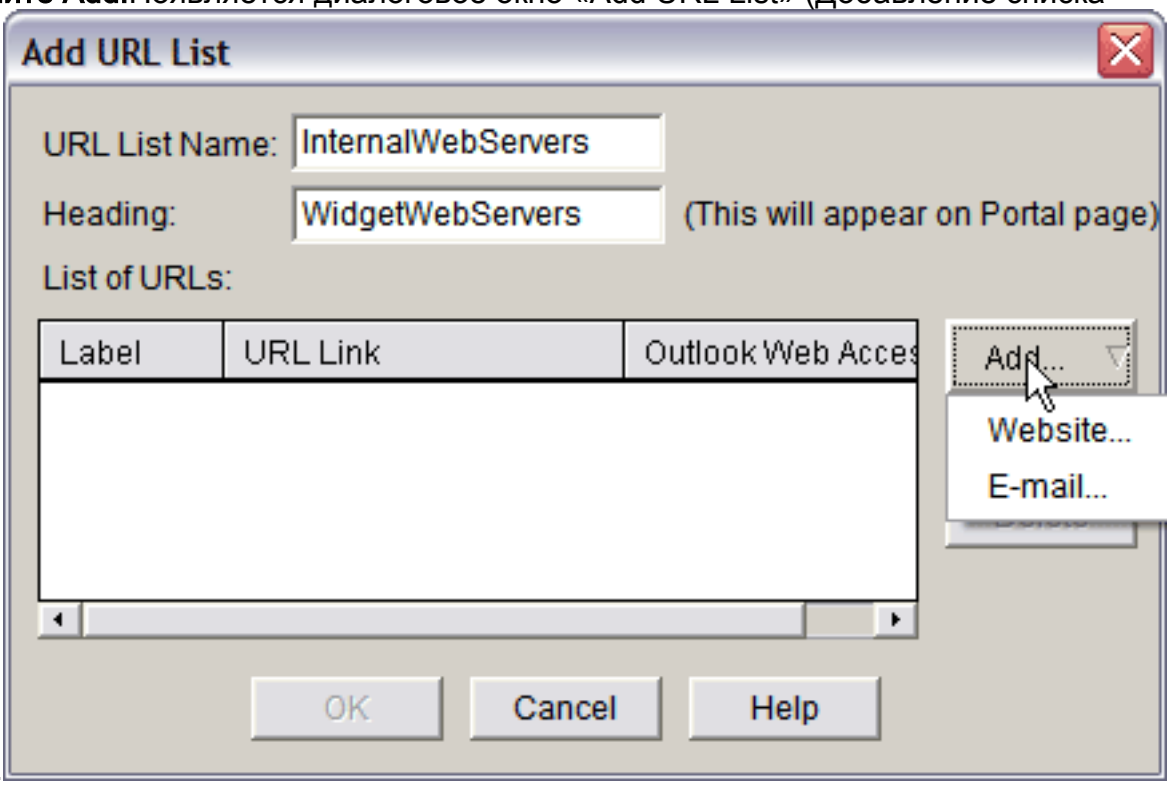
3. **Нажмите Add.**Появляется диалоговое окно «Add WebVPN Context» (Добавление контекста
WebVPN).



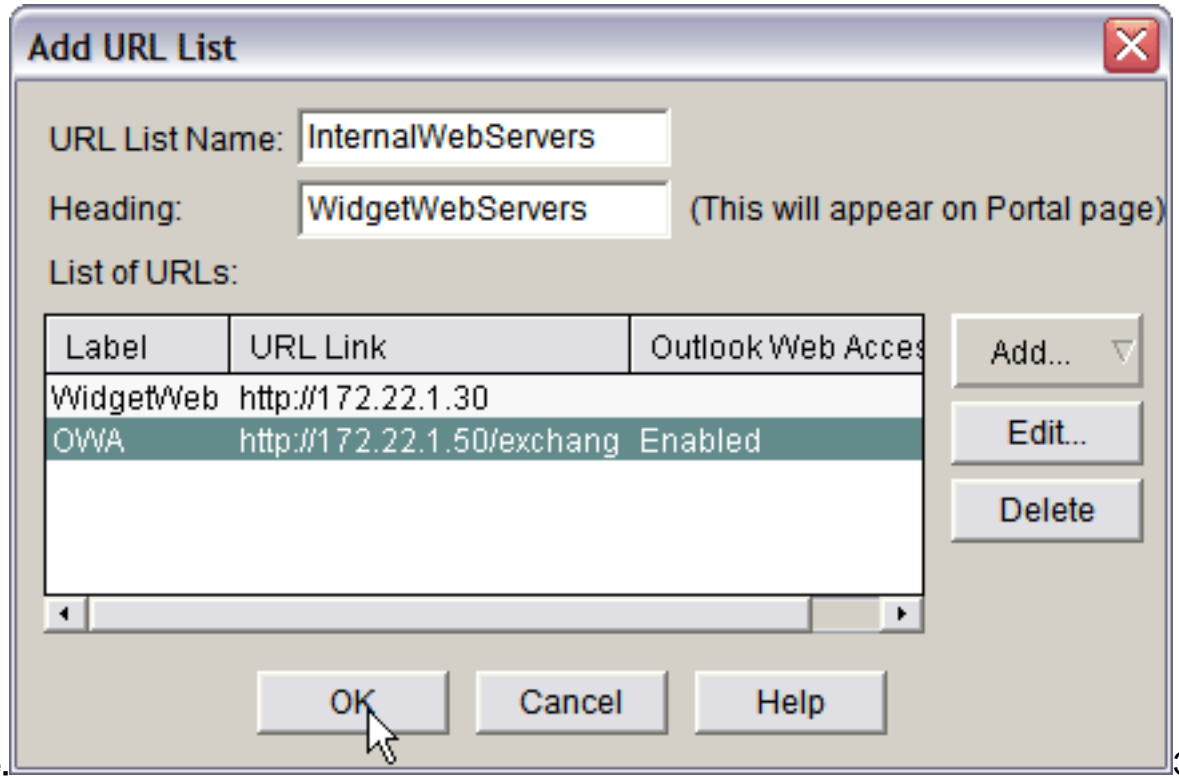
4. Разверните WebVPN Context и выберите URL Lists.



5. **Нажмите Add.**Появляется диалоговое окно «Add URL List» (Добавление списка URL).

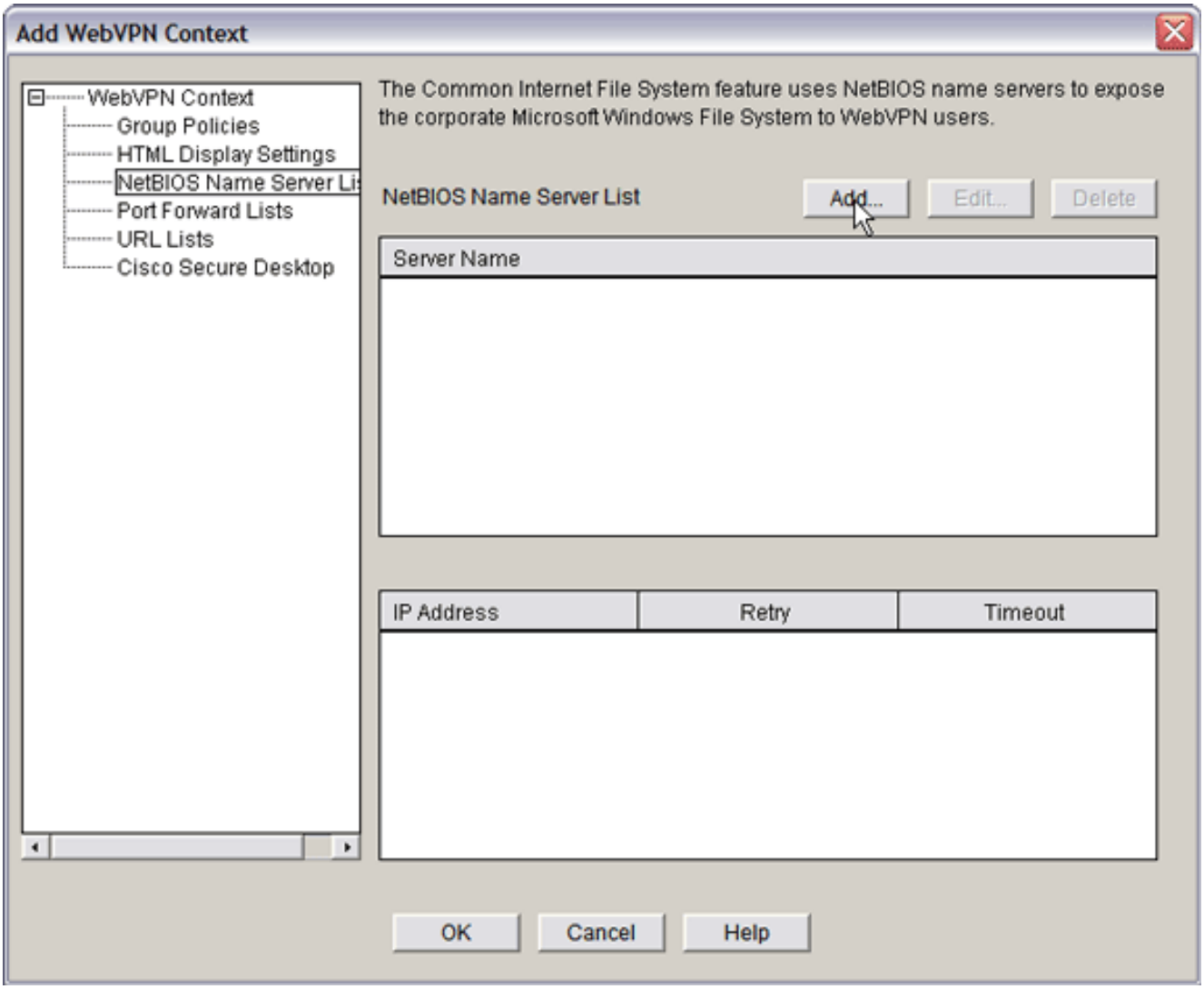


6. Введите данные в поля "URL List Name" (Имя списка URL) и "Heading" (Заголовок).
7. **Нажмите Add и выберите**

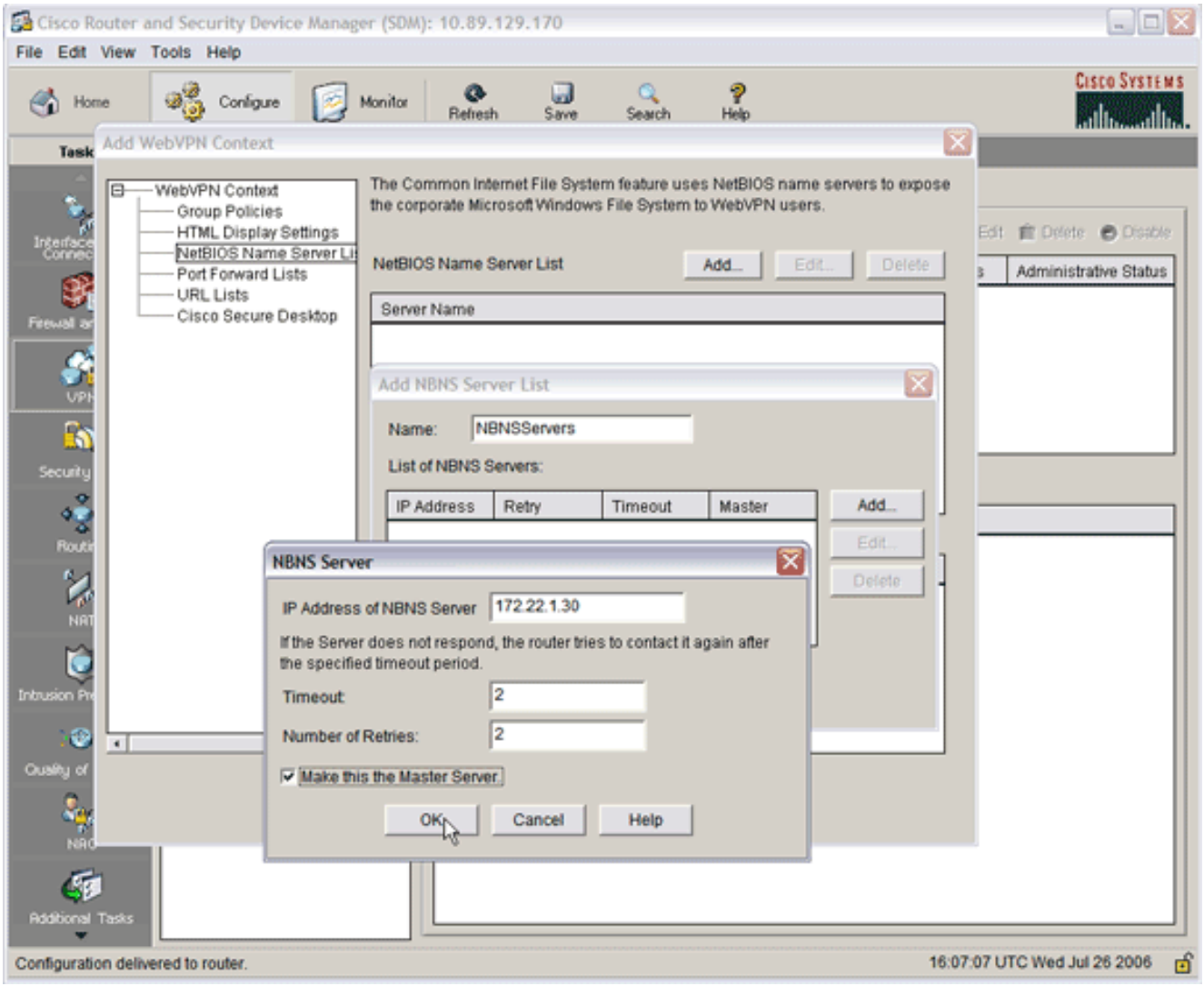


Website. Этот список содержит все веб-серверы HTTP и HTTPS, которые вы хотите сделать доступными для данного WebVPN-соединения.

8. **Чтобы добавить доступ для Outlook Web Access (OWA), нажмите Add, выберите E-mail и нажмите OK после заполнения всех необходимых полей.**
9. Чтобы разрешить доступ к файлам Windows через протокол CIFS, можно назначить сервер службы имен NetBIOS (NBNS) и настроить соответствующие ресурсы в домене Windows.**Из списка "WebVPN Context" (Контекст WebVPN) выберите NetBIOS Name Server Lists.**



Нажмите Add.Появляется диалоговое окно «Add NBNS Server List» (Добавление списка серверов NBNS).**Введите имя списка и нажмите Add.**Появляется диалоговое окно «NBNS Server» (Сервер
NBNS).

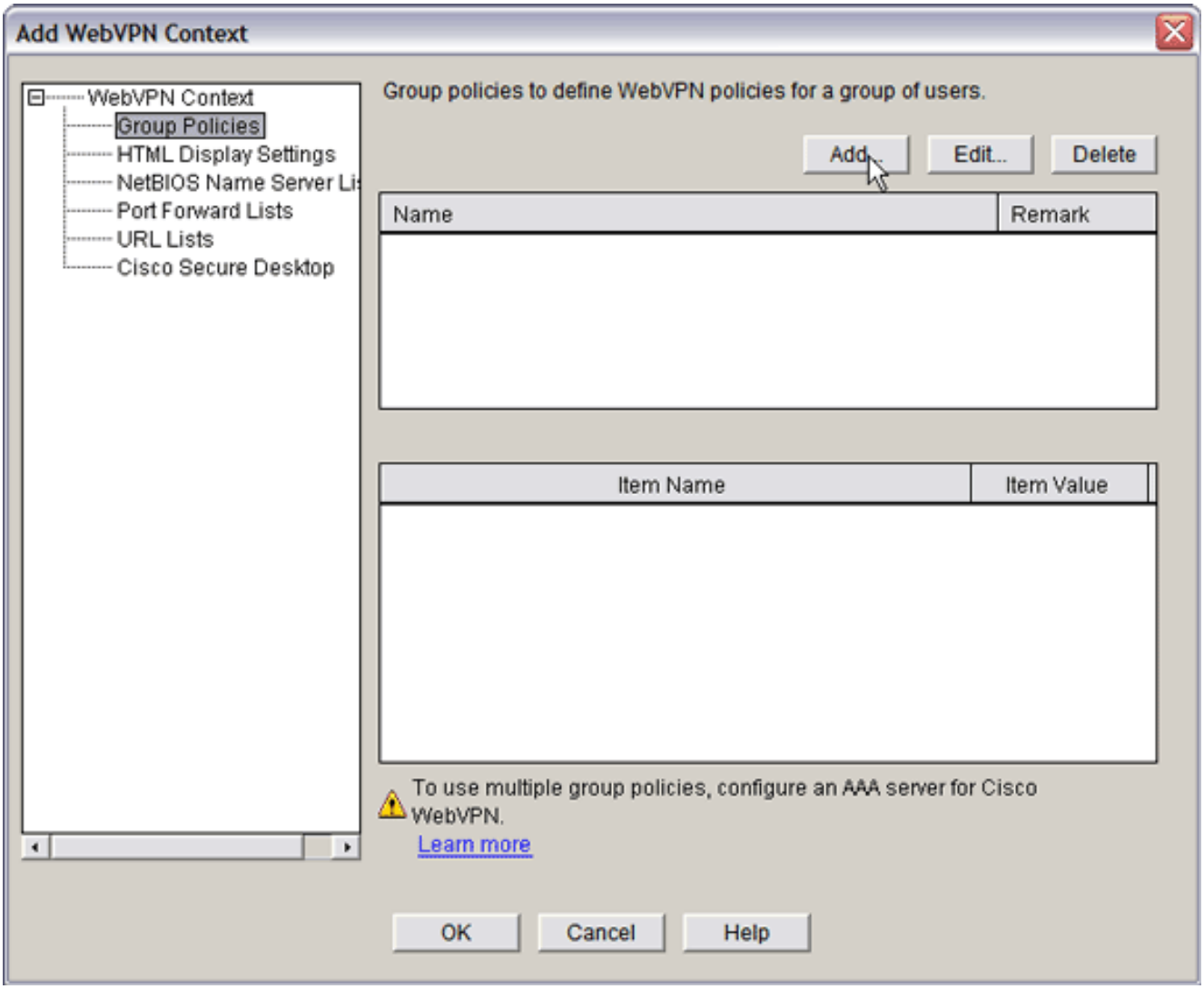


Если применимо, установите флажок Make This the Master Server.Нажмите OK и OK.

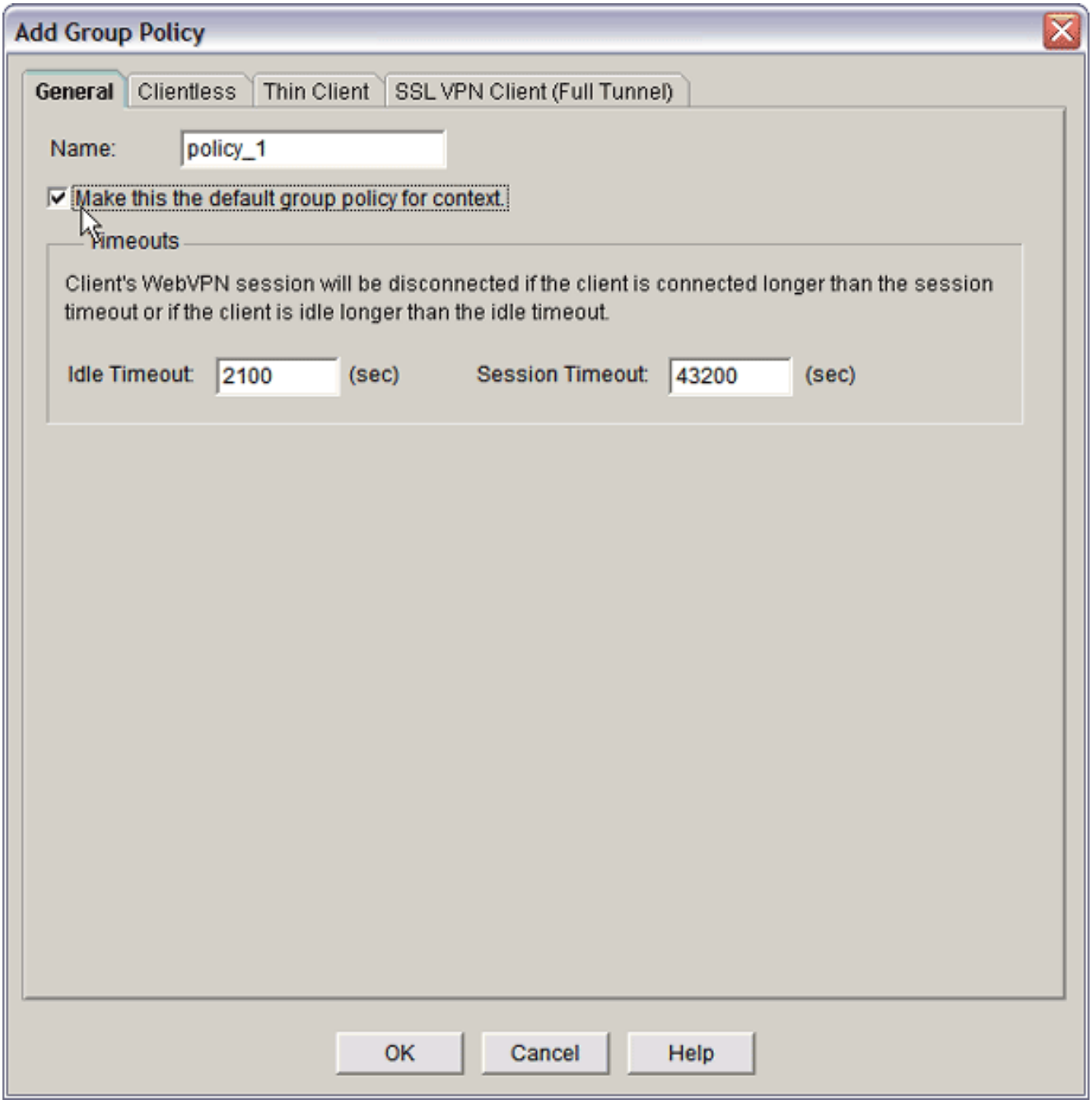
Шаг 3. Настройка группы политик WebVPN и выбор ресурсов

Чтобы настроить группу политик WebVPN и выбрать ресурсы, выполните следующие действия:

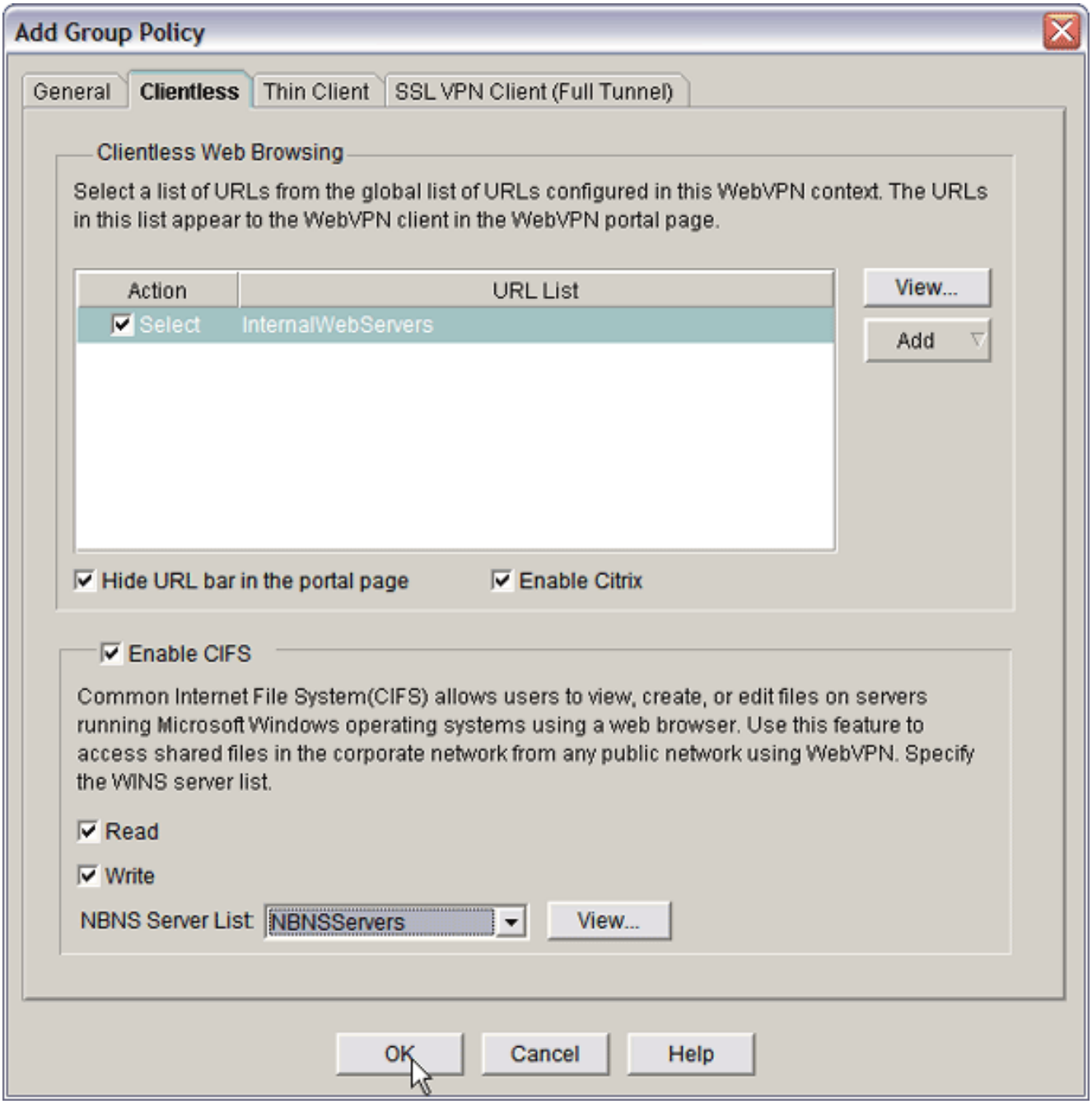
1. **Нажмите Configure и VPN.**
2. **Разверните WebVPN и выберите WebVPN Context.**



3. **Выберите Group Policies и нажмите Add.**Отобразится диалоговое окно "Add Group Policy" (Добавление групповой политики).



4. Введите имя новой политики и установите флажок Make this the default group policy for context.
5. Щелкните вкладку Clientless, расположенную в верхней части диалогового окна.

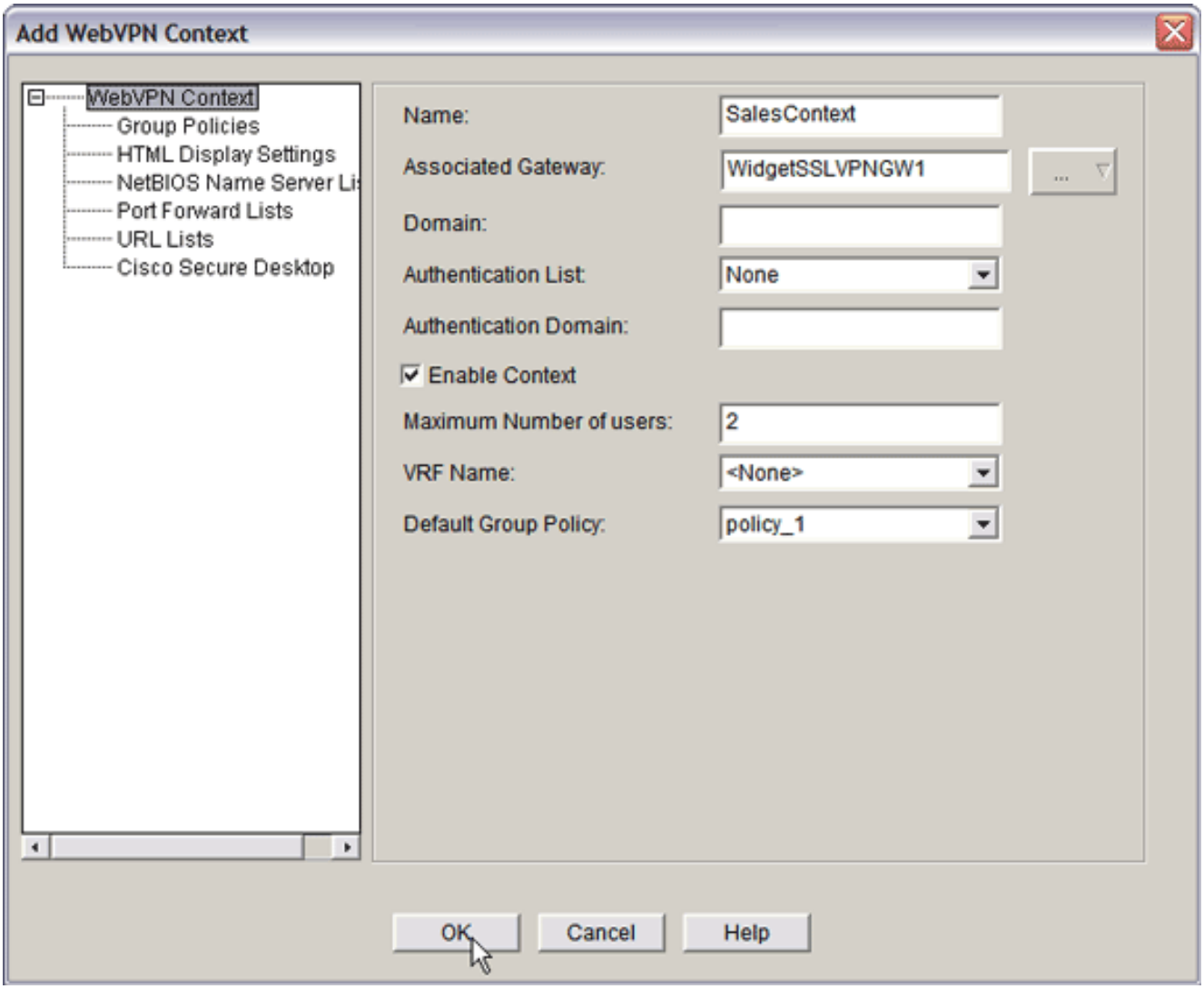


6. **Установите флажок Select для желаемого списка URL.**
7. **Если пользователи используют клиенты Citrix, которым необходим доступ к серверам Citrix, установите флажок Enable Citrix.**
8. **Установите флажки Enable CIFS, Read и Write.**
9. **Щелкните выпадающий список NBNS Server List и выберите список серверов NBNS, созданный для доступа к файлам Windows на Шаге 2.**
10. **Нажмите кнопку OK.**

Шаг 4. . Настройка WebVPN-контекста

Чтобы связать шлюз WebVPN, групповую политику и ресурсы, необходимо настроить контекст WebVPN. Чтобы настроить контекст WebVPN, выполните следующие действия:

1. **Выберите WebVPN Context и введите имя контекста.**



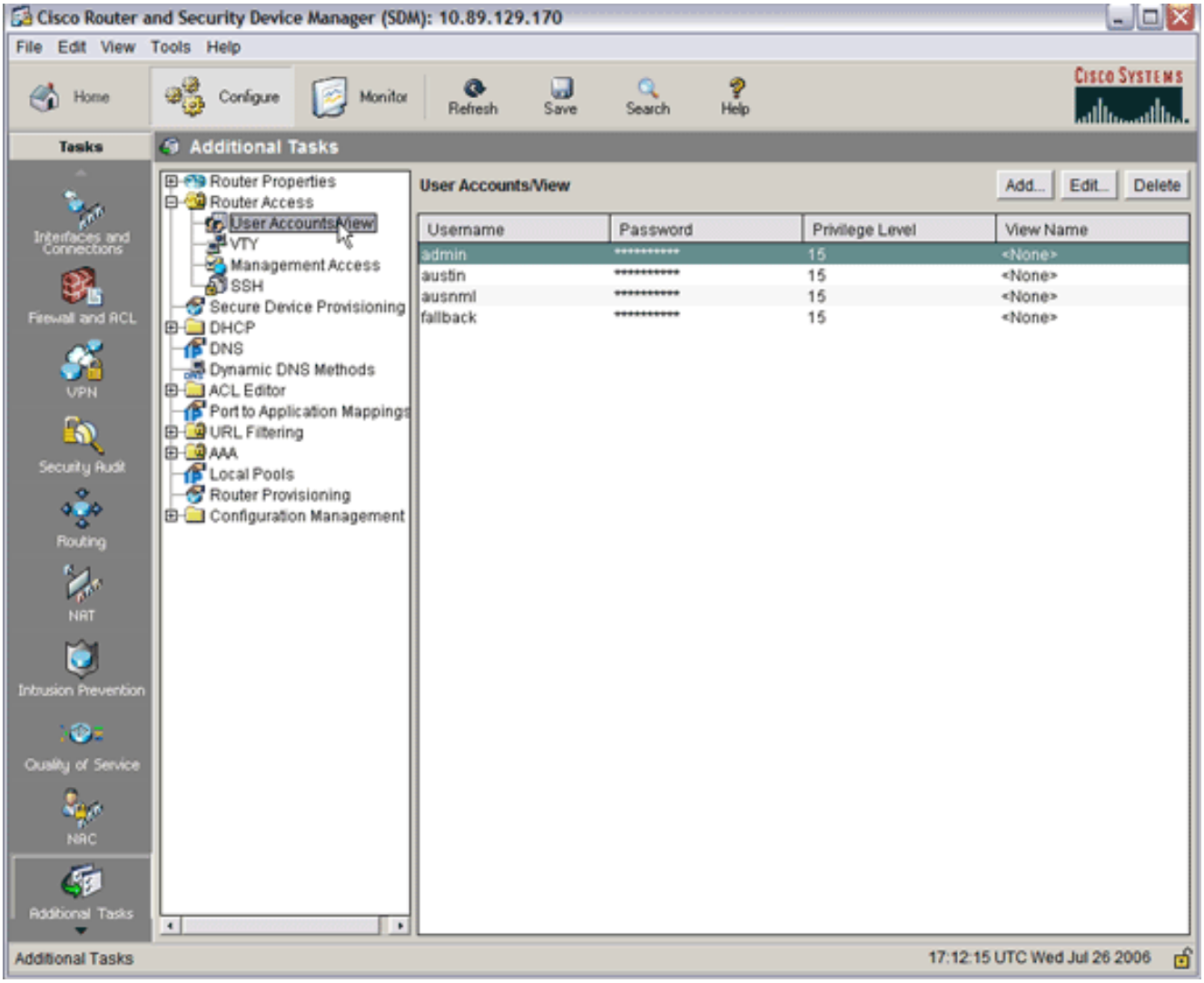
2. Щелкните выпадающий список "Associated Gateway" (Связанный шлюз) и выберите связанный шлюз.
3. Если необходимо создать больше одного контекста, введите уникальное имя в поле "Domain", чтобы идентифицировать контекст. ***Если оставить поле "Domain" пустым, пользователи должны обращаться к WebVPN через https://IPAddress.*** *Если задано доменное имя (например, Sales), пользователи должны подключаться через https://IPAddress/Sales.*
4. **Установите флажок Enable Context.**
5. В поле "Maximum Number of Users" (Максимальное число пользователей) введите максимальное количество пользователей, разрешенное лицензией устройства.
6. **Щелкните выпадающий список Default Group policy и выберите групповую политику для связи с данным контекстом.**
7. **Нажмите OK и OK.**

Шаг 5. . Настройка базы данных пользователей и метода аутентификации

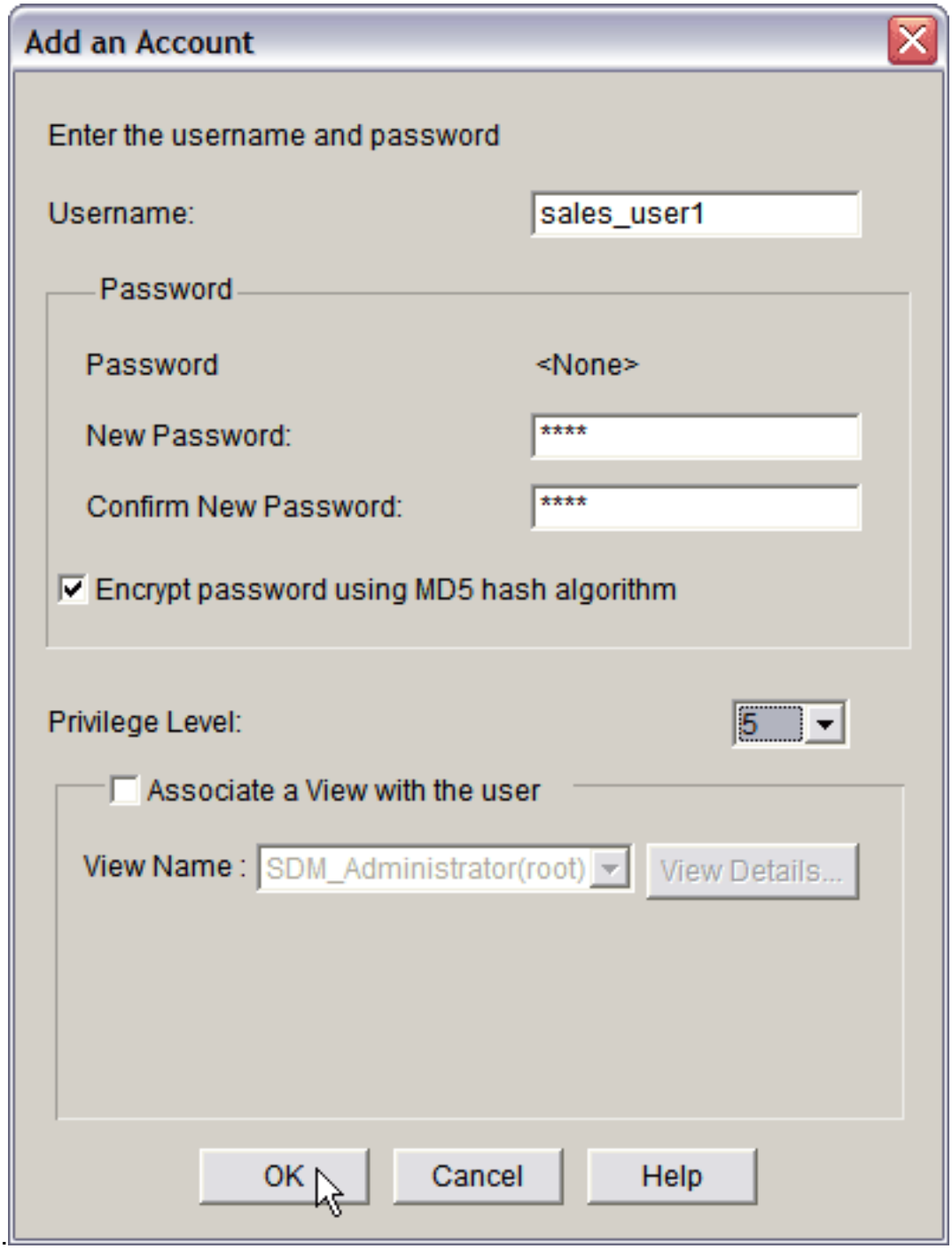
Можно настроить аутентификацию сеансов Clientless SSL VPN (WebVPN) через сервер Radius, сервер Cisco AAA или локальную базу данных. В этом примере используется локальная база данных.

Чтобы настроить базу данных пользователей и метод аутентификации, выполните следующие действия:

1. **Нажмите Configuration и Additional Tasks.**
2. **Разверните Router Access и выберите User Accounts/View.**



3. **Нажмите кнопку Add.**Появляется диалоговое окно «Add an Account» (Добавление



учетной записи).

4. Введите учетную запись пользователя и пароль.
5. **Нажмите OK и OK.**
6. **Нажмите Save и Yes, чтобы принять изменения.**

Результаты

ASDM создает следующие конфигурации командных строк:

ausnml-3825-01
Building configuration... Current configuration : 4190 bytes ! ! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by ausnml ! NVRAM config last updated at 17:22:31 UTC Wed Jul 26 2006 by ausnml

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 29312730 2506092A 864886F7 0D010902
16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63
6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
31303130 30303030 305A3029 31273025 06092A86 4886F70D
01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363
6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B
E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093
C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B
09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3
78307630 0F060355 1D130101 FF040530 030101FF 30230603
551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E
63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D
0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D
4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4
2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6
7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6
5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC
55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920
88A8A55E quit username admin privilege 15 secret 5
$1$jm6N$2xNfhupbAinq3BQZMRzrW0 username ausnml privilege
```

```
15 password 7 15071F5A5D292421 username fallback
privilege 15 password 7 08345818501A0A12 username austin
privilege 15 secret 5 $1$3xFv$W0YUsKDx1adDc.cVQF2Ei0
username sales_user1 privilege 5 secret 5
$1$2/SX$ep4fsCpodeyKaRji2mJkX/ ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http timeout-policy idle 600
life 86400 requests 100 ! control-plane ! line con 0
stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-
timeout 40 0 privilege level 15 password 7
071A351A170A1600 transport input telnet ssh line vty 5
15 exec-timeout 40 0 password 7 001107505D580403
transport input telnet ssh ! scheduler allocate 20000
1000 ! !--- WebVPN Gateway webvpn gateway
WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address
192.168.0.37 port 443 http-redirect port 80 ssl
trustpoint ausnml-3825-01_Certificate inservice ! webvpn
context SalesContext ssl authenticate verify all ! !---
Identify resources for the SSL VPN session url-list
"InternalWebServers" heading "WidgetWebServers" url-text
"WidgetWeb" url-value "http://172.22.1.30" url-text
"OWA" url-value "http://172.22.1.50/exchange" ! nbns-
list NBNSServers nbns-server 172.22.1.30 ! !--- Identify
the policy which controls the resources available policy
group policy_1 url-list "InternalWebServers" nbns-list
"NBNSServers" functions file-access functions file-
browse functions file-entry hide-url-bar citrix enabled
default-group-policy policy_1 gateway WidgetSSLVPNGW1
max-users 2 inservice ! end
```

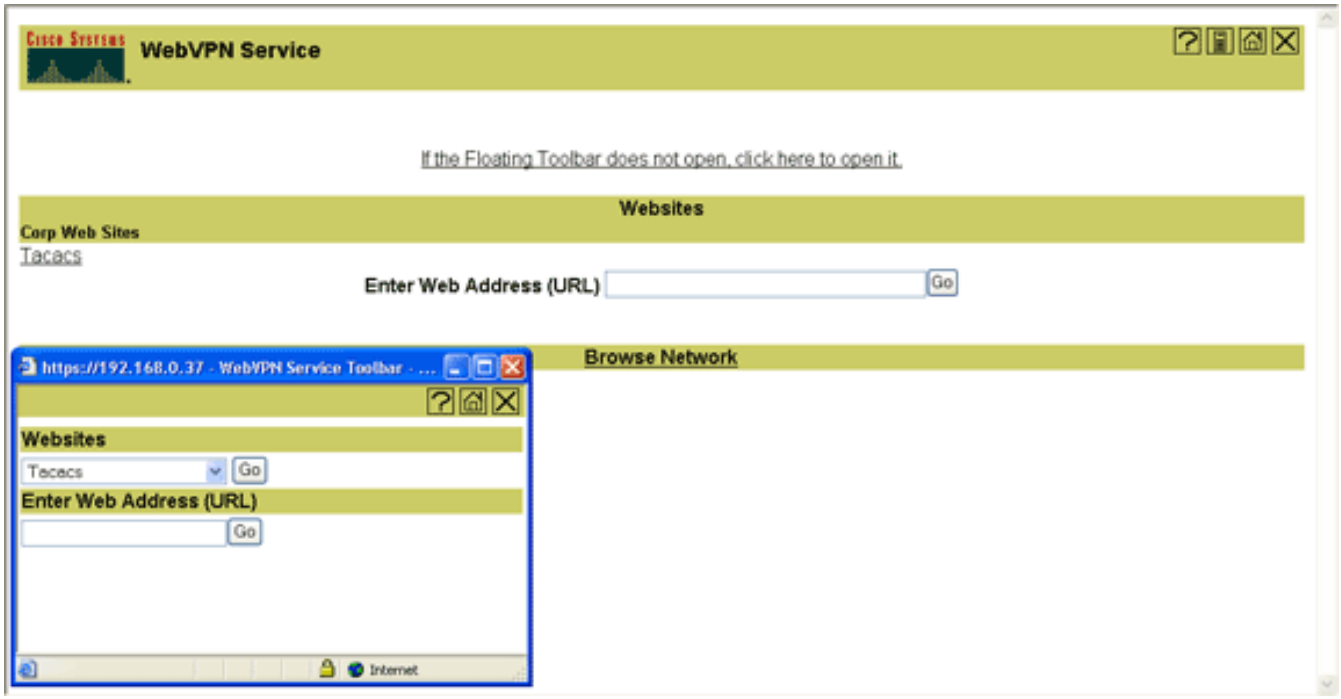
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Процедура

Чтобы убедиться, что конфигурация работает правильно, выполните следующие действия:

- Проверьте конфигурацию с помощью учетной записи пользователя. ***Введите https://WebVPN_Gateway_IP_Address в веб-браузере с поддержкой SSL, где WebVPN_Gateway_IP_Address — IP-адрес службы WebVPN.*** После получения сертификата и ввода имени пользователя и пароля появляется экран, подобный следующему
  изображению.



- Проверьте сеанс SSL VPN. **В приложении SDM нажмите кнопку Monitor и VPN Status. Разверните WebVPN (All Contexts), разверните соответствующий контекст и выберите Users.**
- Проверьте сообщения об ошибках. **В приложении SDM нажмите кнопку Monitor, нажмите Logging и щелкните вкладку Syslog.**
- Просмотрите рабочую конфигурацию устройства. **В приложении SDM нажмите кнопку Configure и Additional Tasks. Разверните Configuration Management и выберите Config Editor.**

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.

Примечание: Не прервите **команду Copy File to Server** или перейдите к другому окну, в то время как копирование происходит. Прерывание этой операции может привести к сохранению на сервере неполного файла.

Примечание: Пользователи могут загрузить и загрузить новые файлы с помощью клиента WebVPN, но пользователю не разрешают перезаписать файлы в Протоколе CIFS на WebVPN с помощью **команды Copy File to Server**. При попытке заменить файл на сервере пользователь получит следующее сообщение:

```
Unable to add the file
```

Процедура

Выполните следующие шаги для устранения неполадки в вашей настройке:

1. Убедитесь, что на клиентах отключена блокировка всплывающих окон.
2. Убедитесь, что на клиентах включены cookies.
3. Убедитесь, что на клиентах используется веб-браузер Netscape, Internet Explorer, Firefox или Mozilla.

Команды

Некоторые команды debug связаны с WebVPN. Дополнительные сведения об этих командах см. в разделе Использование команд отладки WebVPN.

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

- Cisco IOS SSLVPN
- Cisco IOS SSLVPN — вопросы и ответы
- Пример конфигурации тонкого клиента SSL VPN (WebVPN) IOS с помощью SDM
- Пример конфигурации клиента SSL VPN на IOS с помощью SDM
- Cisco Systems – техническая поддержка и документация