Пример настройки ASA с WebVPN и единым входом при использовании ASDM NTLMv1

Содержание

Введение

В этом документе описана настройка устройств адаптивной защиты Cisco (ASA) для автоматической передачи параметров входа в систему WebVPN с реквизитами вторичной аутентификации серверам, требующим выполнения дополнительных проверок при входе в систему посредством Windows Active Directory с использованием пакета протоколов NT LAN Manager версии 1 (NTLMv1). Эта функция называется единым входом в систему (Single Sign-On, SSO). Соединениям, настроенным для определенной группы WebVPN, она позволяет передавать данные аутентификации пользователя, избегая многократного запроса аутентификации. Эта функция может также использоваться на глобальном или пользовательском уровне конфигурации.

Предварительные условия

Требования

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

- Убедитесь в том, что настроены NTLMv1 и разрешения Windows для пользователей целевой сети VPN. Обратитесь к документации Microsoft за дополнительными сведениями о полномочиях доступа в домен Windows.

Используемые компоненты

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

- Cisco ASA 7.1 (1)
- Менеджер устройств адаптивной защиты Cisco (ASDM) версии 5.1(2)
- Службы Microsoft Internet Information Services (IIS)

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.

Условные обозначения

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

Настройка

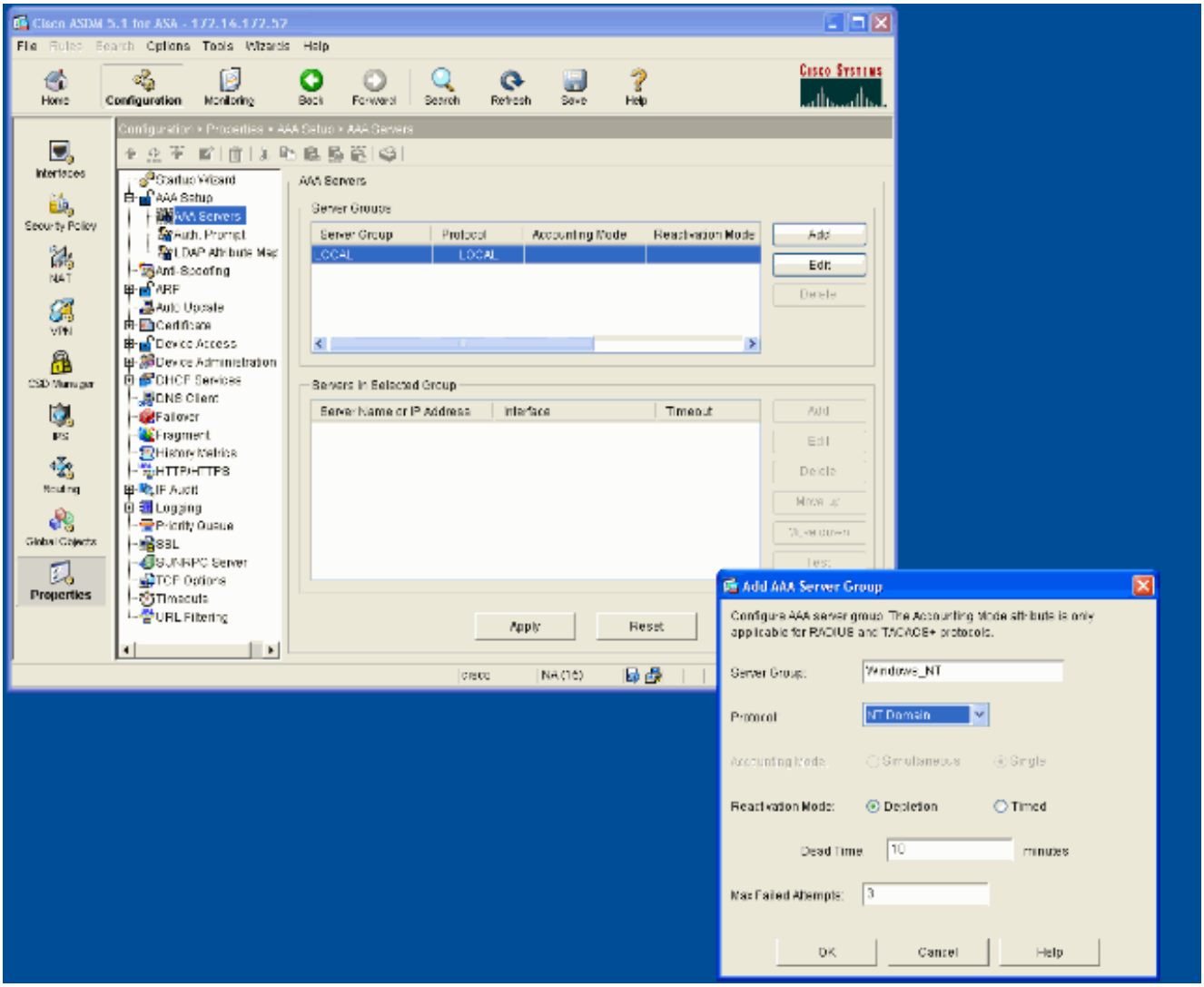
В этом разделе представлены сведения о настройке устройства ASA в качестве сервера WebVPN с функцией SSO.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

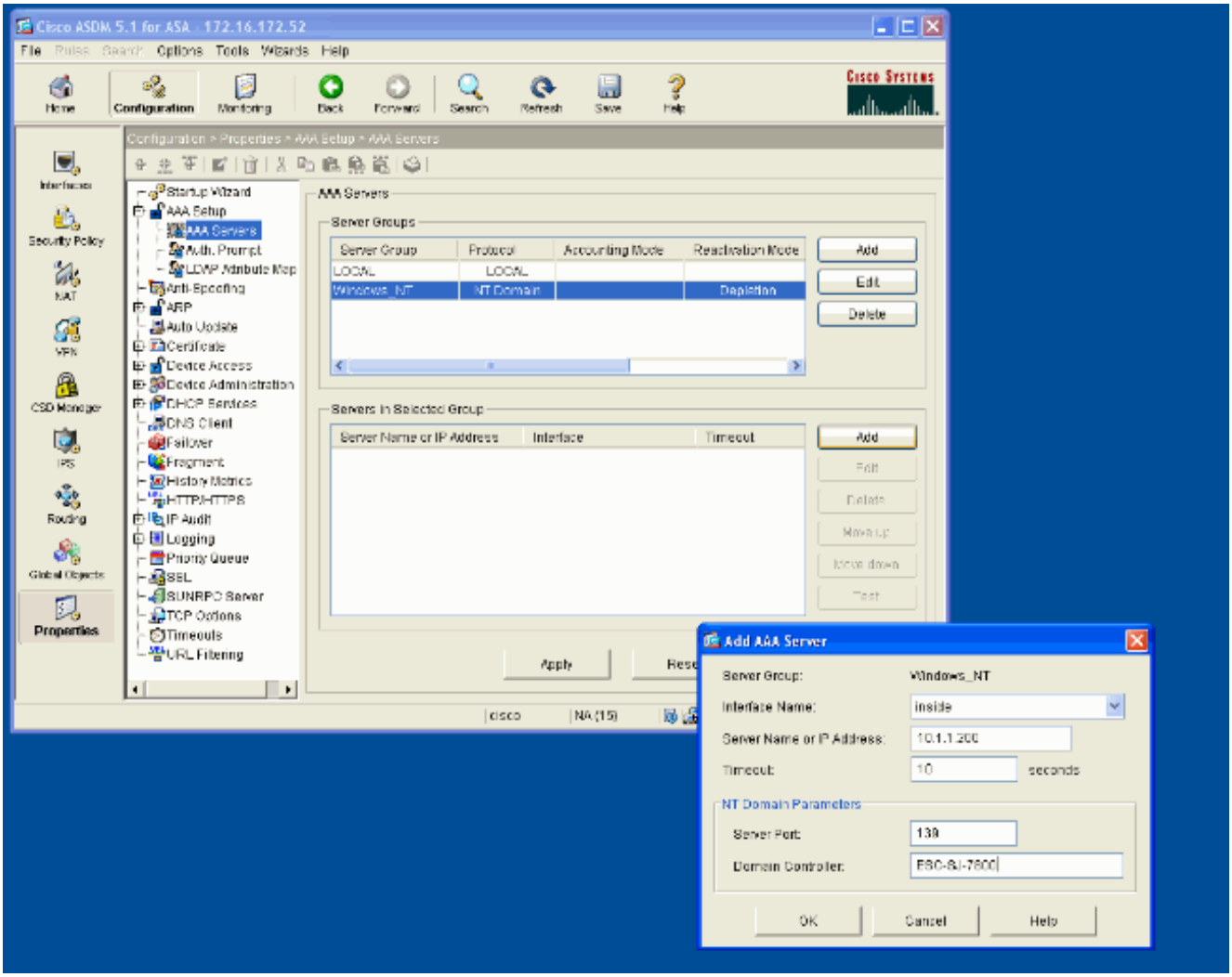
Добавление сервера AAA для аутентификации в домене Windows

Чтобы настроить устройство ASA для использования контроллера домена при выполнении аутентификации, выполните следующие шаги.

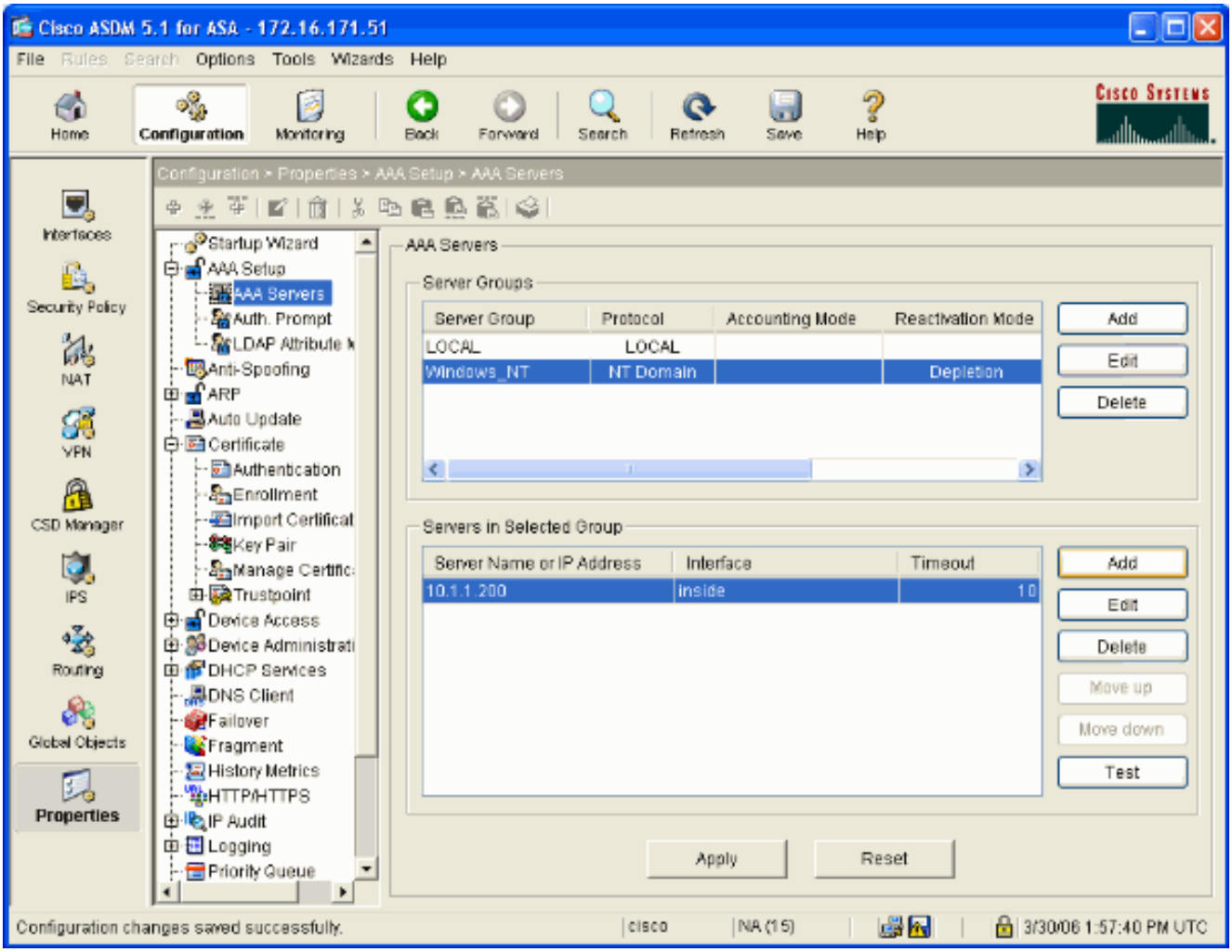
1. **Выберите Configuration > Properties > AAA Setup > AAA Servers (Конфигурация > Свойства > Настройка AAA > Серверы AAA) и нажмите кнопку Add (Добавить). Укажите имя группы серверов, например Windows_NT, и в качестве протокола выберите NT Domain (Домен NT).**



2. Добавьте сервер Windows.**Выберите вновь созданную группу и нажмите кнопку Add (Добавить).** Выберите интерфейс, на котором действует сервер, и введите IP-адрес и имя контроллера домена. Убедитесь в том, что имя контроллера домена вводится полностью заглавными буквами. **Закончив все действия, нажмите кнопку OK.**



В этом окне показана готовая конфигурация AAA:

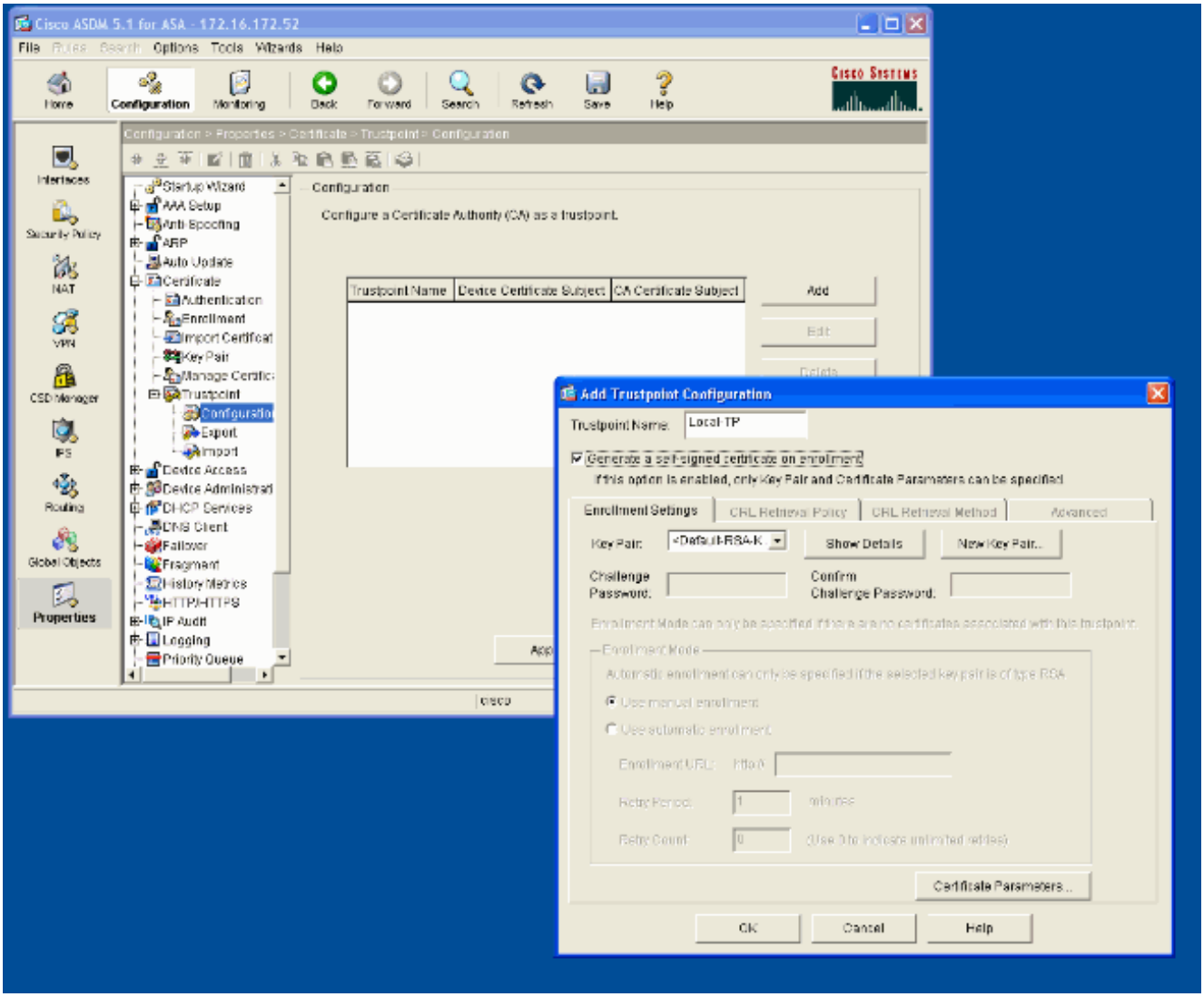


Создание самостоятельно подписанного сертификата

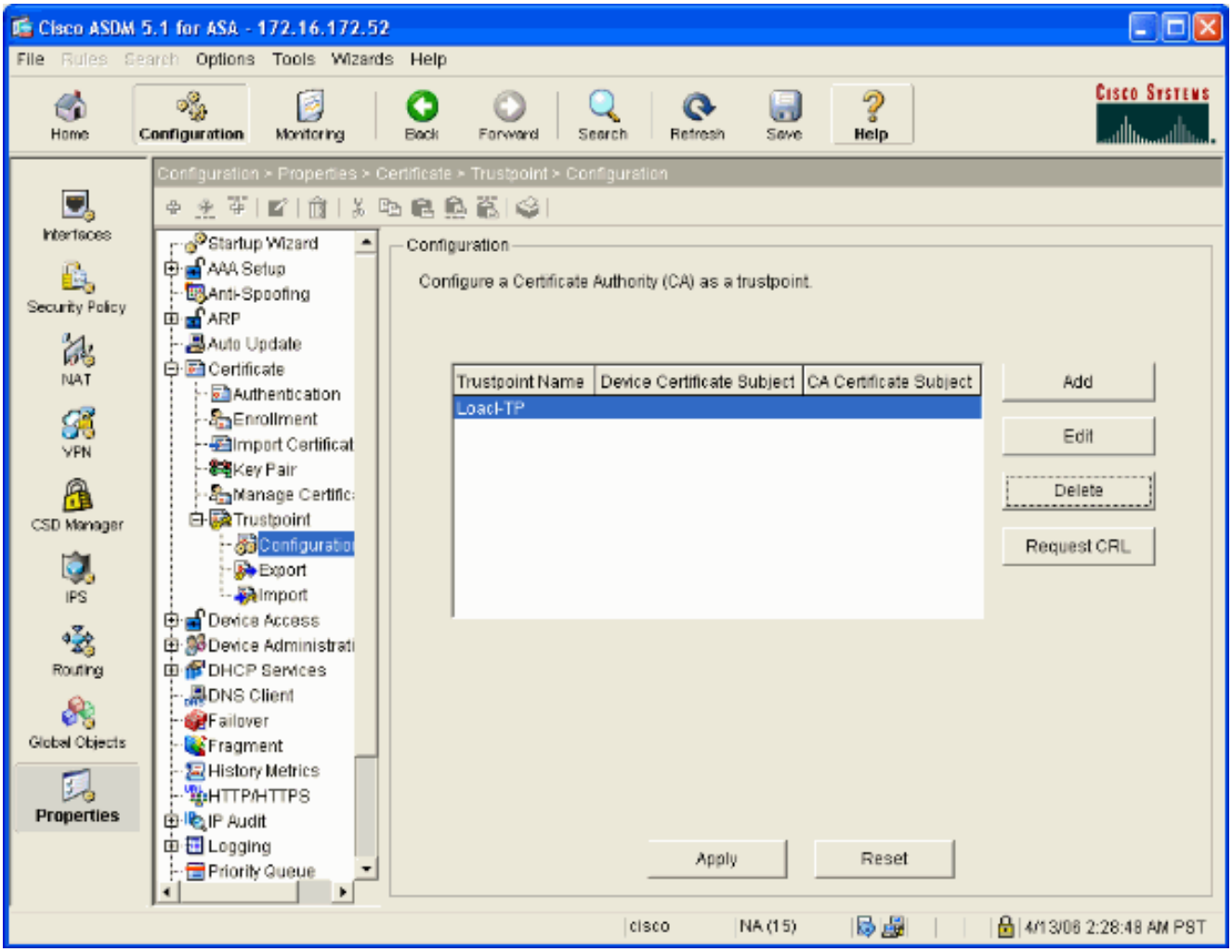
Чтобы настроить устройство ASA для использования самостоятельно подписанного сертификата, выполните следующие шаги.

Примечание: В данном примере подписанный сертификат используется для простоты. Другие варианты зачисления сертификатов, например, зачисление посредством внешнего центра сертификации, описаны в документе Настройка сертификатов.

1. **Выберите Configuration > Properties > Certificate > Trustpoint > Configuration (Конфигурация > Свойства > Сертификат > Доверенная точка > Конфигурация) и нажмите кнопку Add (Добавить).**
2. **В появившемся окне введите имя доверенной точки (например, Local-TP) и выберите Generate a self-signed certificate on enrollment (Сформировать самостоятельно подписанный сертификат по зачислению).** Другие параметры можно оставить со значениями по умолчанию. **Закончив все действия, нажмите кнопку OK.**



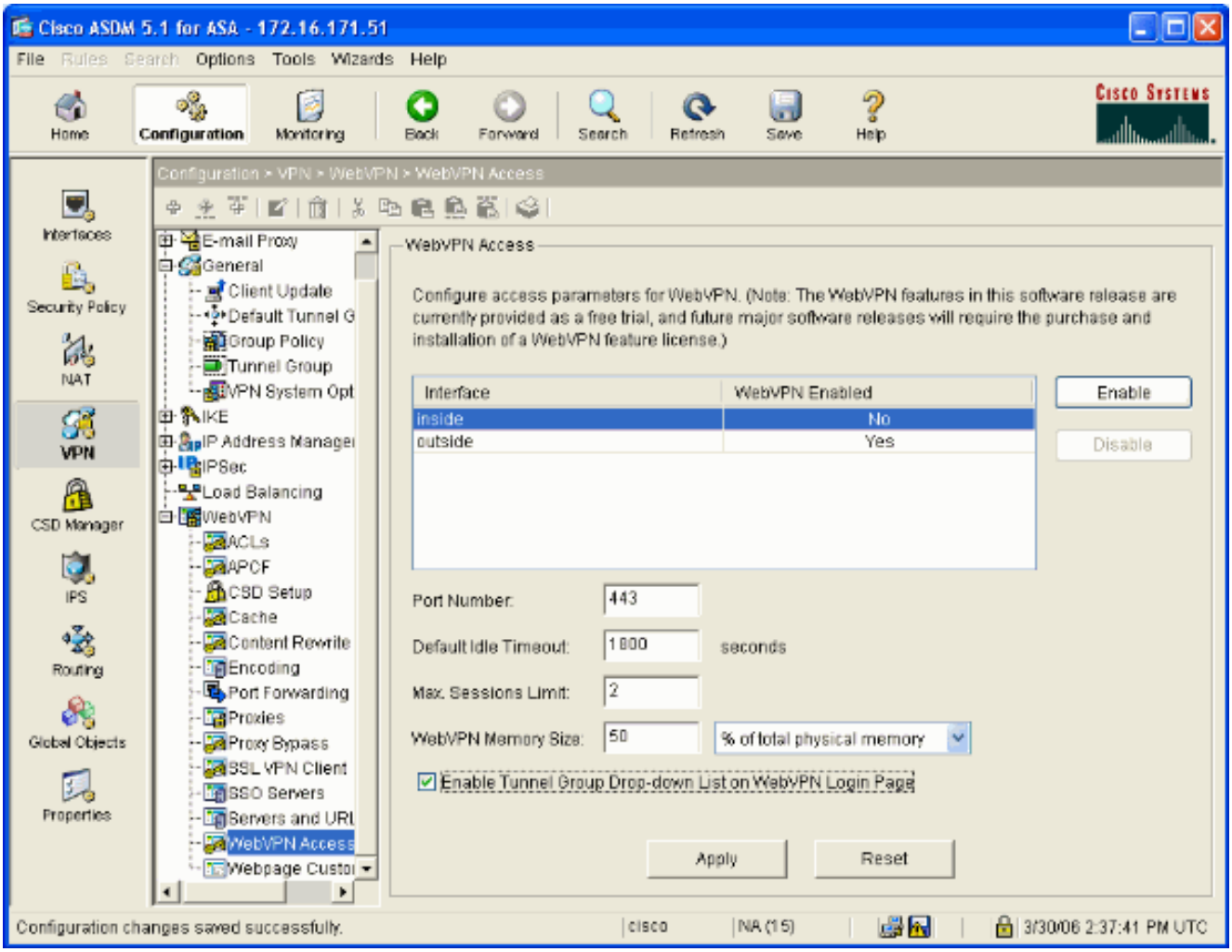
В этом окне показана готовая конфигурация доверенной точки:



Включение WebVPN на внешнем интерфейсе

Чтобы разрешить пользователям вне сети подключаться с использованием WebVPN, выполните следующие шаги.

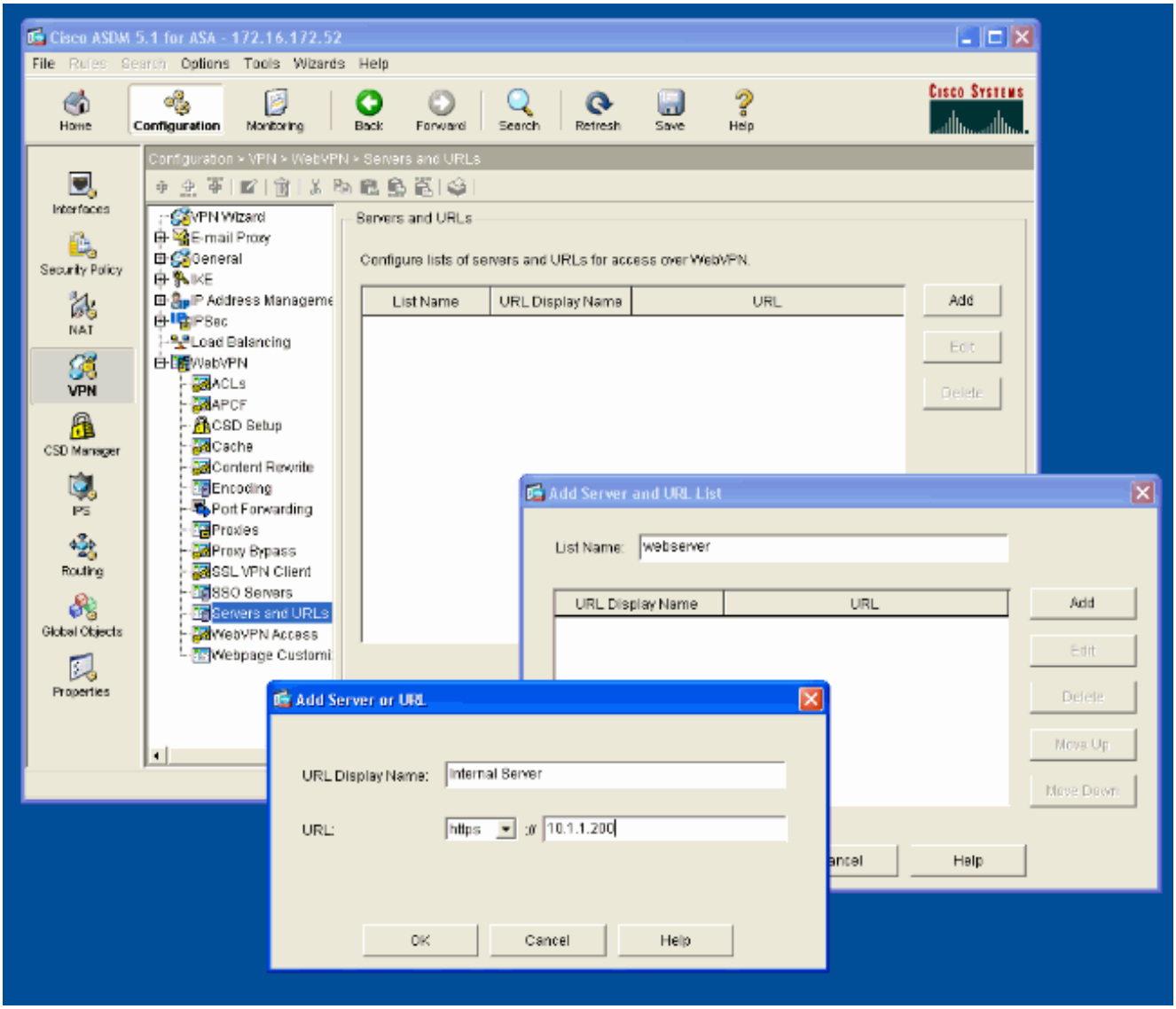
1. **Выберите Configuration > VPN > WebVPN > WebVPN Access (Конфигурация > VPN > WebVPN > Доступ WebVPN).**
2. **Выберите требуемый интерфейс, щелкните Enable (Активировать) и отметьте флажок Enable Tunnel Group Drop-down List on WebVPN Login Page (Разрешить раскрывающийся список групп туннелирования на странице входа WebVPN).Примечание:** Если тот же интерфейс используется для WebVPN и доступа ASDM, необходимо изменить порт по умолчанию для доступа ASDM от порта 80 до нового порта такой как 8080. Это сделано под **Конфигурацией> Свойства> Доступ к устройству> HTTPS/ASDM.Примечание:** Можно автоматически перенаправить пользователя к порту 443, если пользователь перешел к **http://<ip_address>** вместо **https://<ip_address>. Выберите Configuration > Properties > HTTP/HTTPS (Конфигурация > Свойства > HTTP/HTTPS), укажите требуемый интерфейс, нажмите кнопку Edit (Редактировать) и выберите Redirect HTTP to HTTPS (Переадресовывать HTTP на HTTPS).**



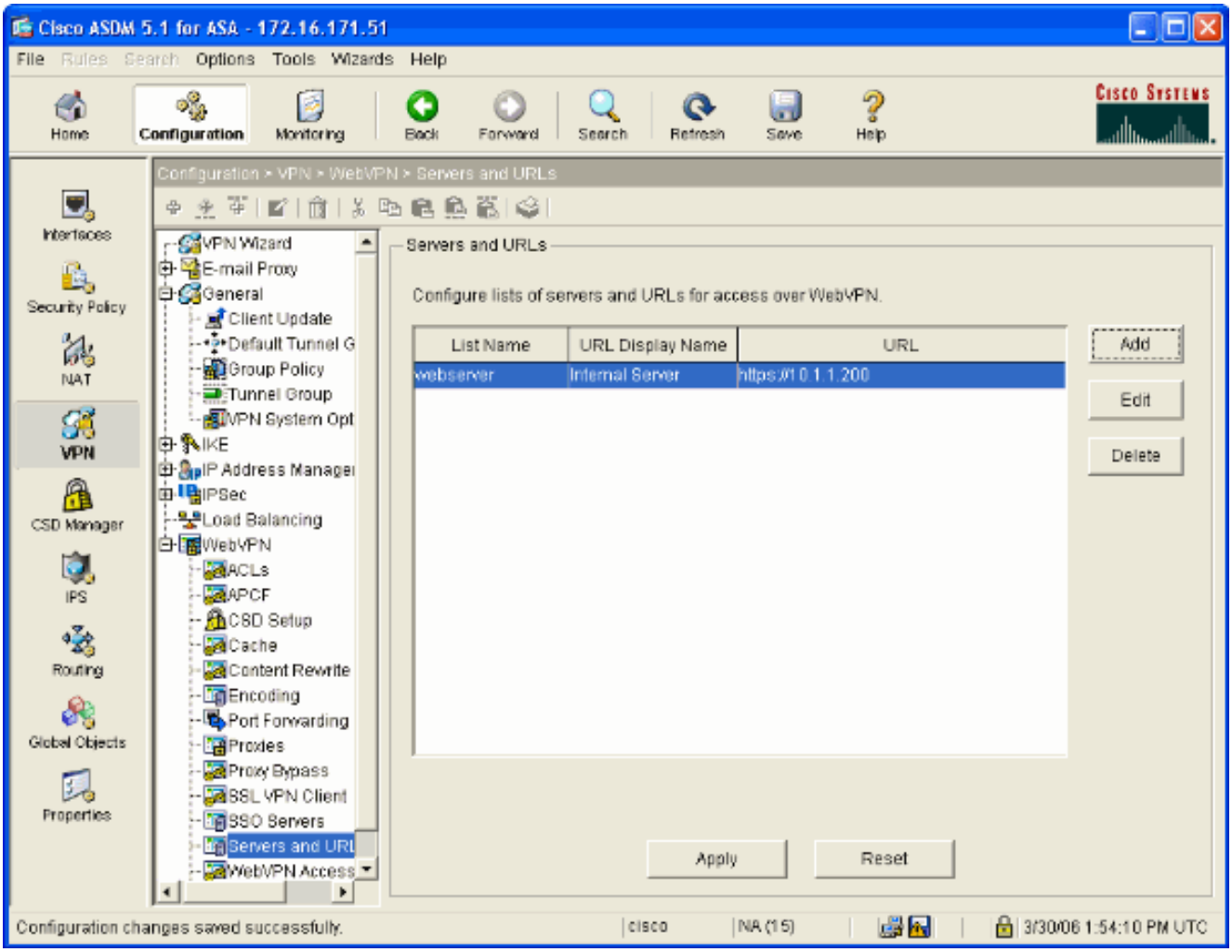
Настройка списка URL-адресов для внутренних серверов

Для создания списка серверов, доступ к которым предоставляется пользователям WebVPN, выполните следующие действия.

1. **Выберите Configuration > VPN > WebVPN > Servers and URLs (Конфигурация > VPN > WebVPN > Серверы и URL-адреса) и нажмите кнопку Add (Добавить).**
2. Введите имя списка URL-адресов. Это имя не будет показываться конечным пользователям. **Нажмите Add.**
3. В поле URL Display Name введите отображаемое имя, которое будет показываться пользователям. Введите параметры URL-адреса сервера. Их нужно вводить в том виде, в котором они обычно используются для доступа к серверу.



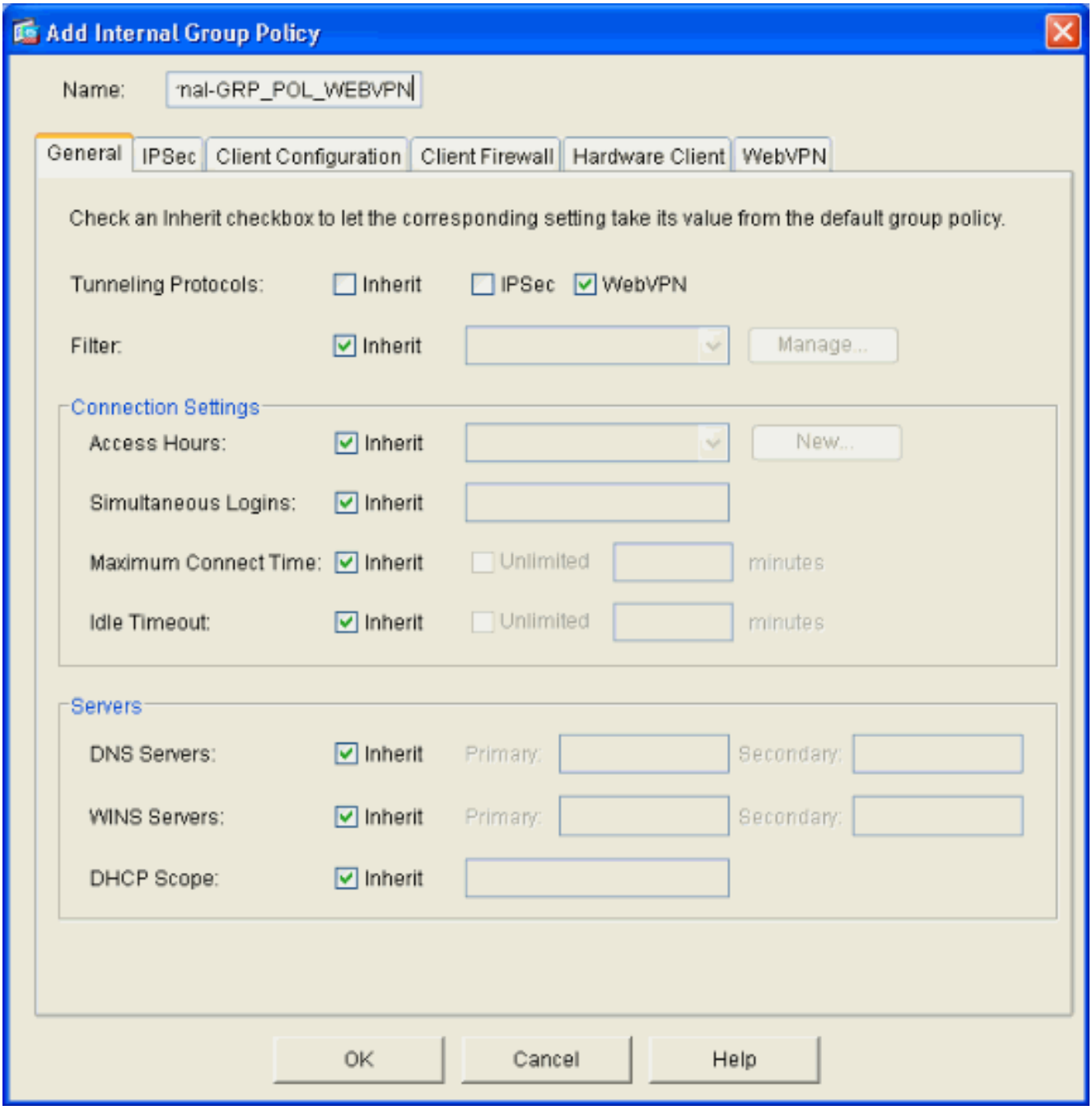
4. Нажмите OK, затем снова OK и Apply (Применить).



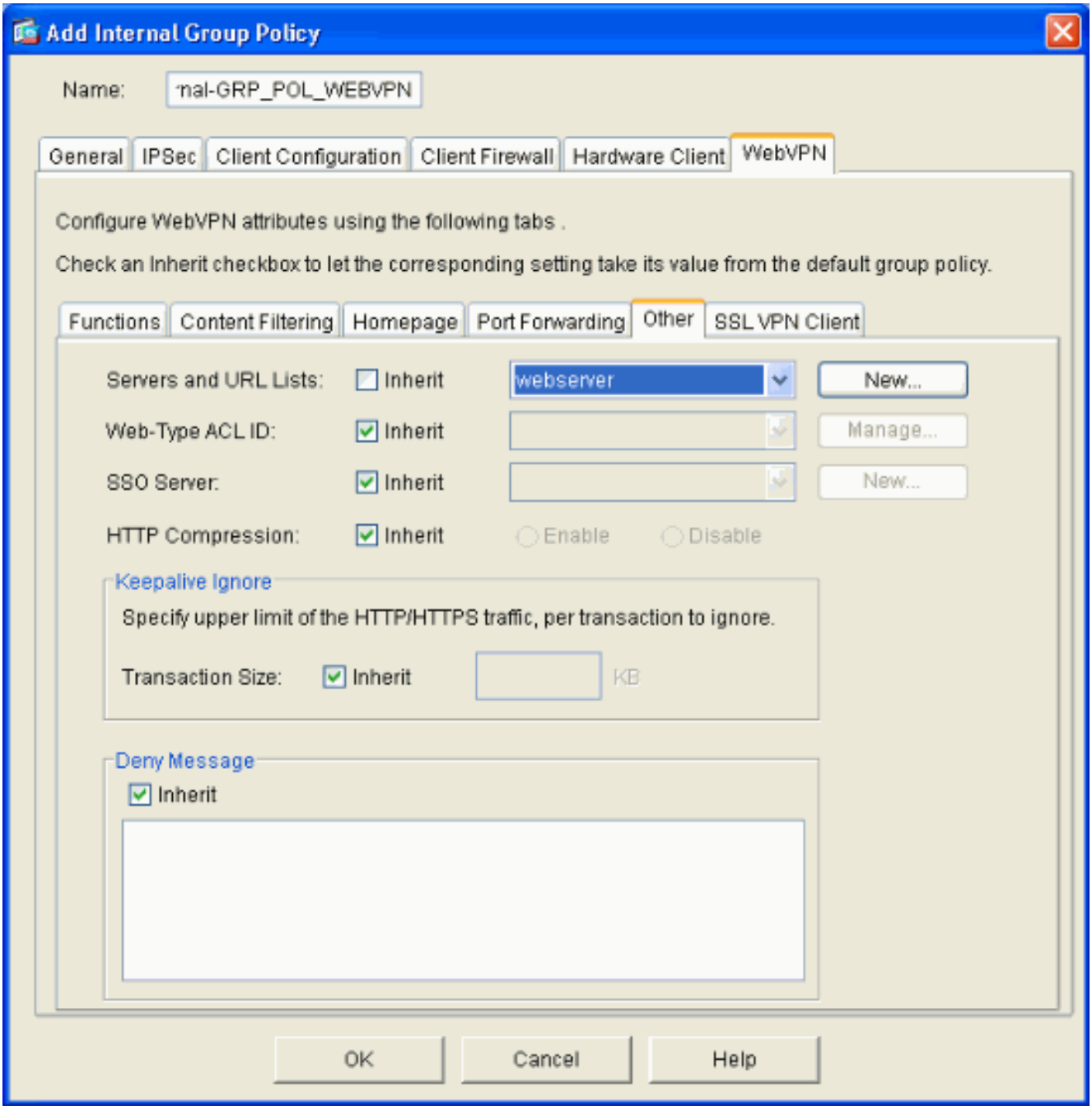
Настройка внутренней групповой политики

Чтобы настроить групповую политику для пользователей WebVPN, выполните следующие шаги.

1. **Выберите Configuration > VPN > General > Group Policy (Конфигурация > VPN > Общее > Групповая политика), нажмите кнопку Add (Добавить) и выберите Internal Group Policy (Внутренняя групповая политика).**
2. На вкладке General (Общее) определите имя политики, например Internal-Group_POL_WEBVPN. **Затем снимите флажок Inherit (Наследовать) рядом с полем Tunneling Protocols (Протоколы туннелирования) и отметьте WebVPN.**



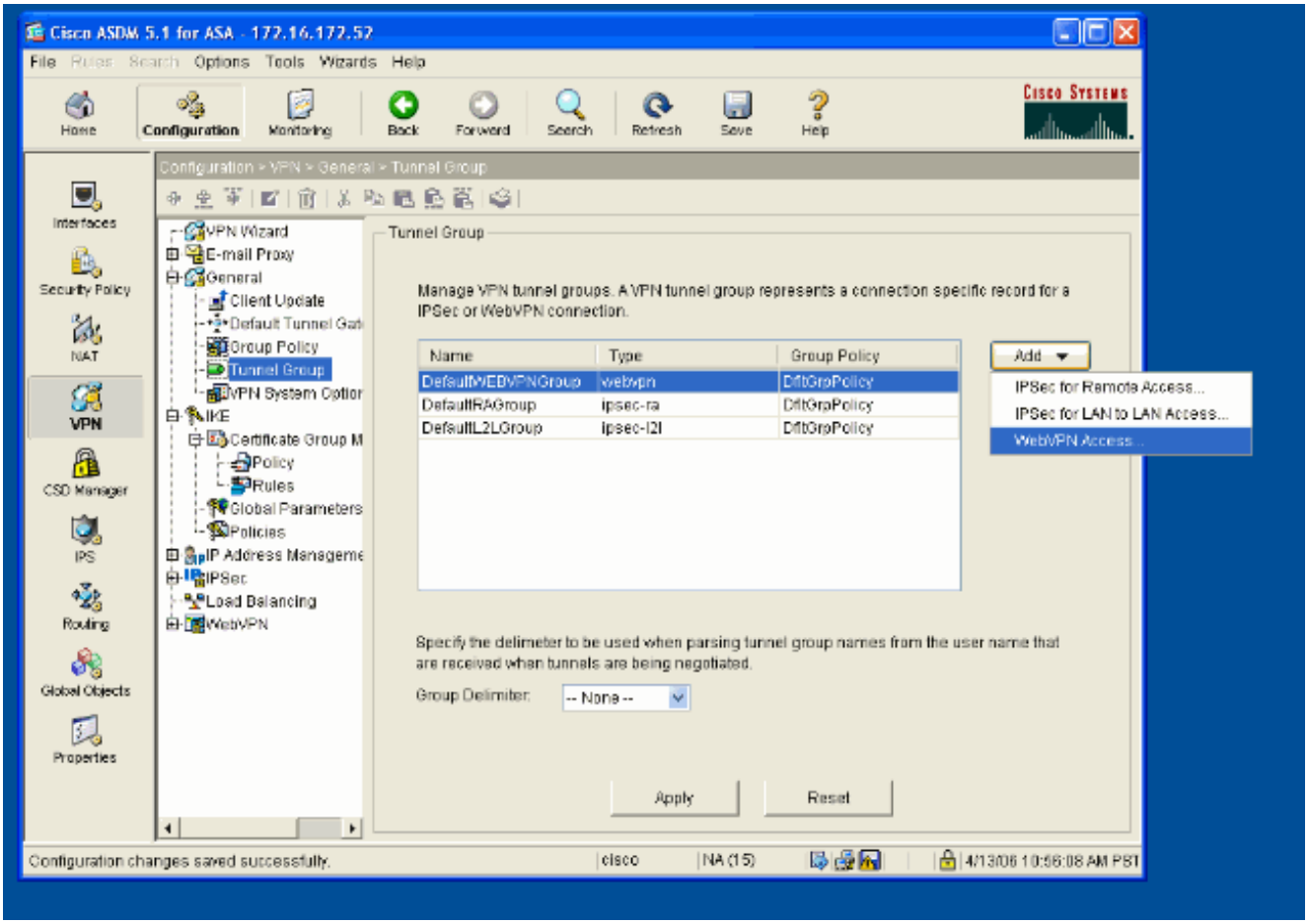
3. На вкладке WebVPN выберите подвкладку Other (Прочее). Снимите флажок Inherit (Наследовать) рядом со списками серверов и URL-адресов, затем выберите настроенный список URL-адресов из раскрывающегося списка. Закончив все действия, нажмите кнопку
OK.



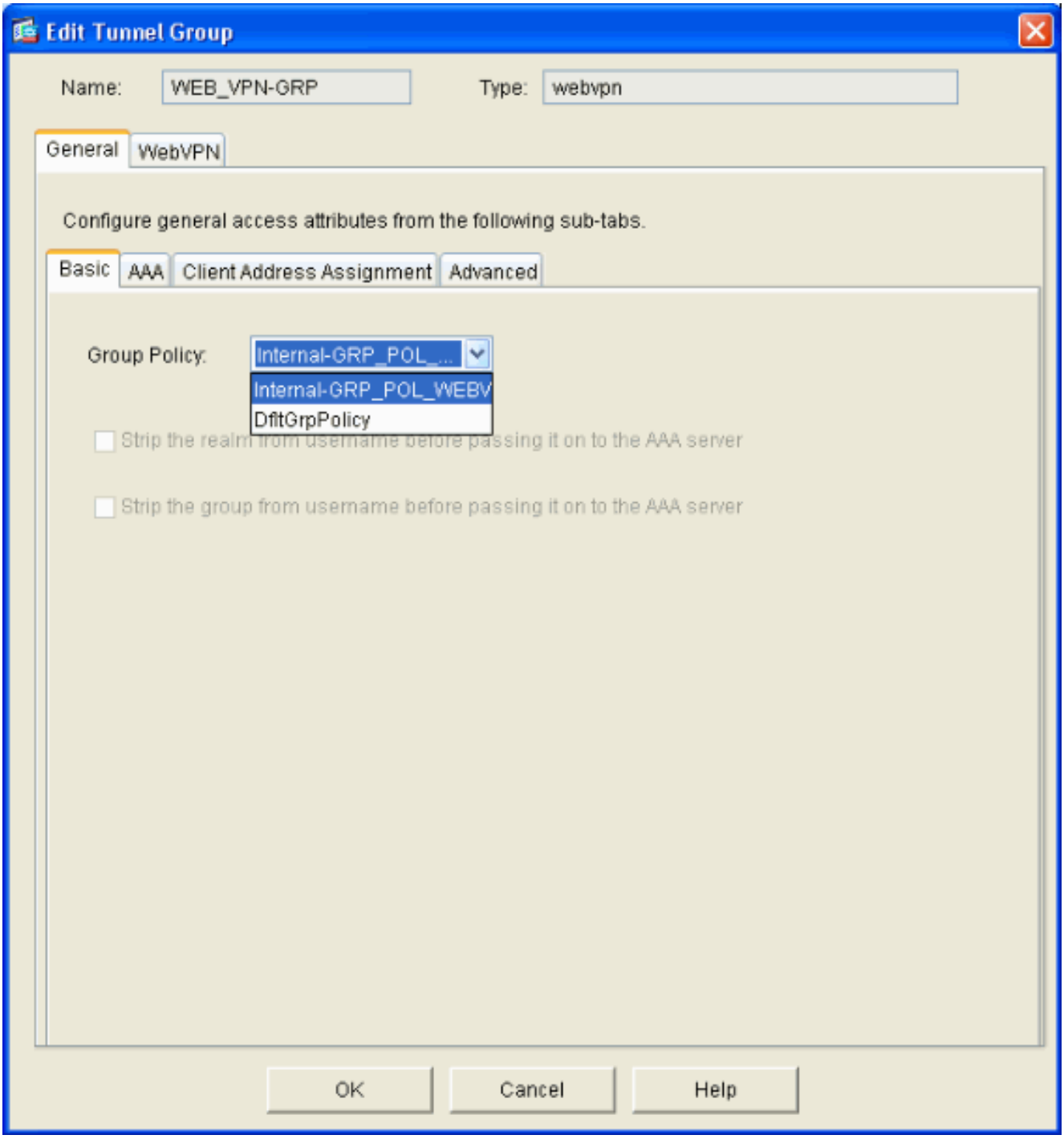
Настройка группы туннелирования

Чтобы настроить группу туннелирования для пользователей WebVPN, выполните следующие шаги.

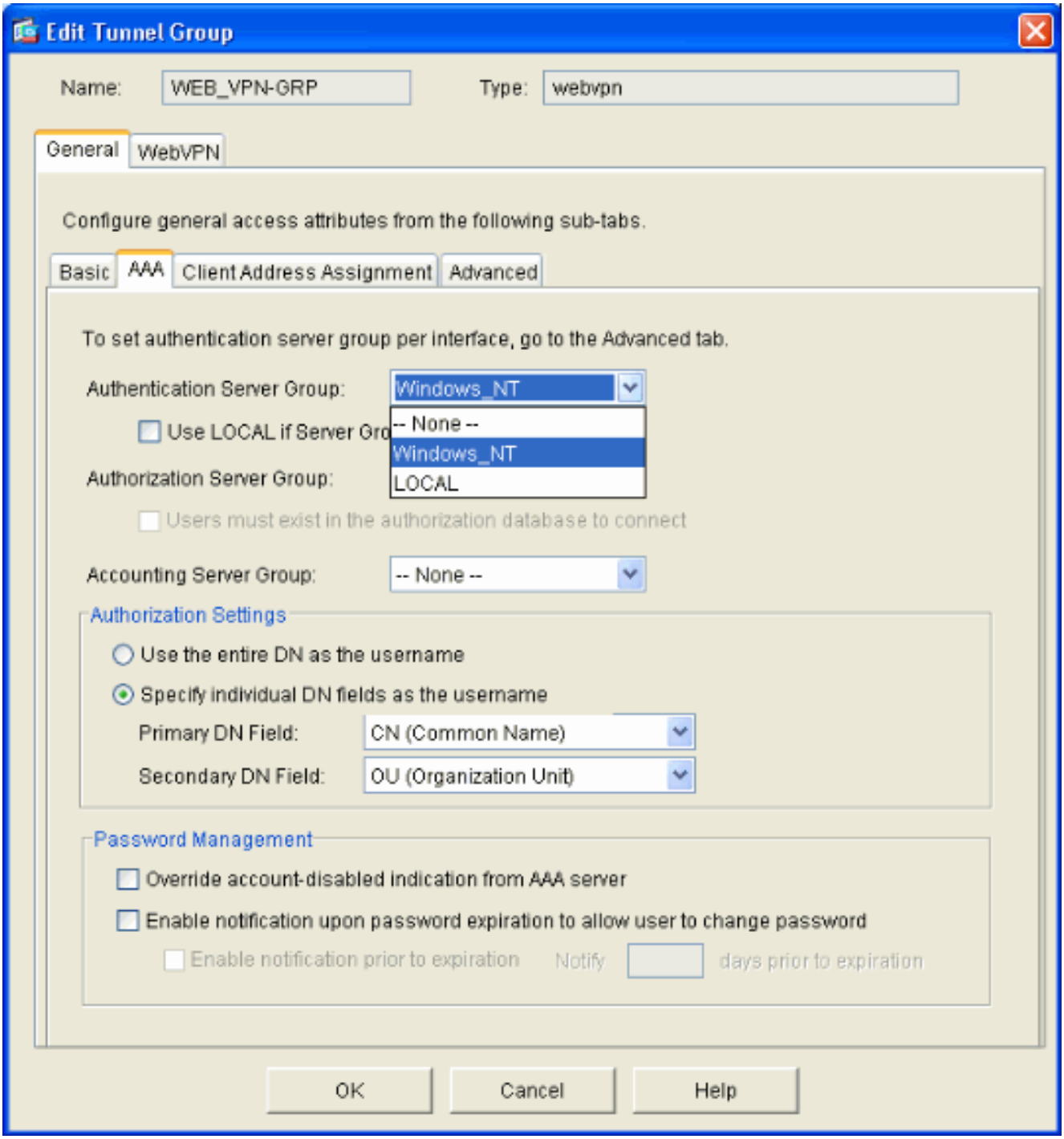
1. **Выберите Configuration > VPN > General > Tunnel Group (Конфигурация > VPN > Общее > Группа туннелирования), нажмите кнопку Add (Добавить), затем выберите WebVPN Access... (Доступ WebVPN…)...**



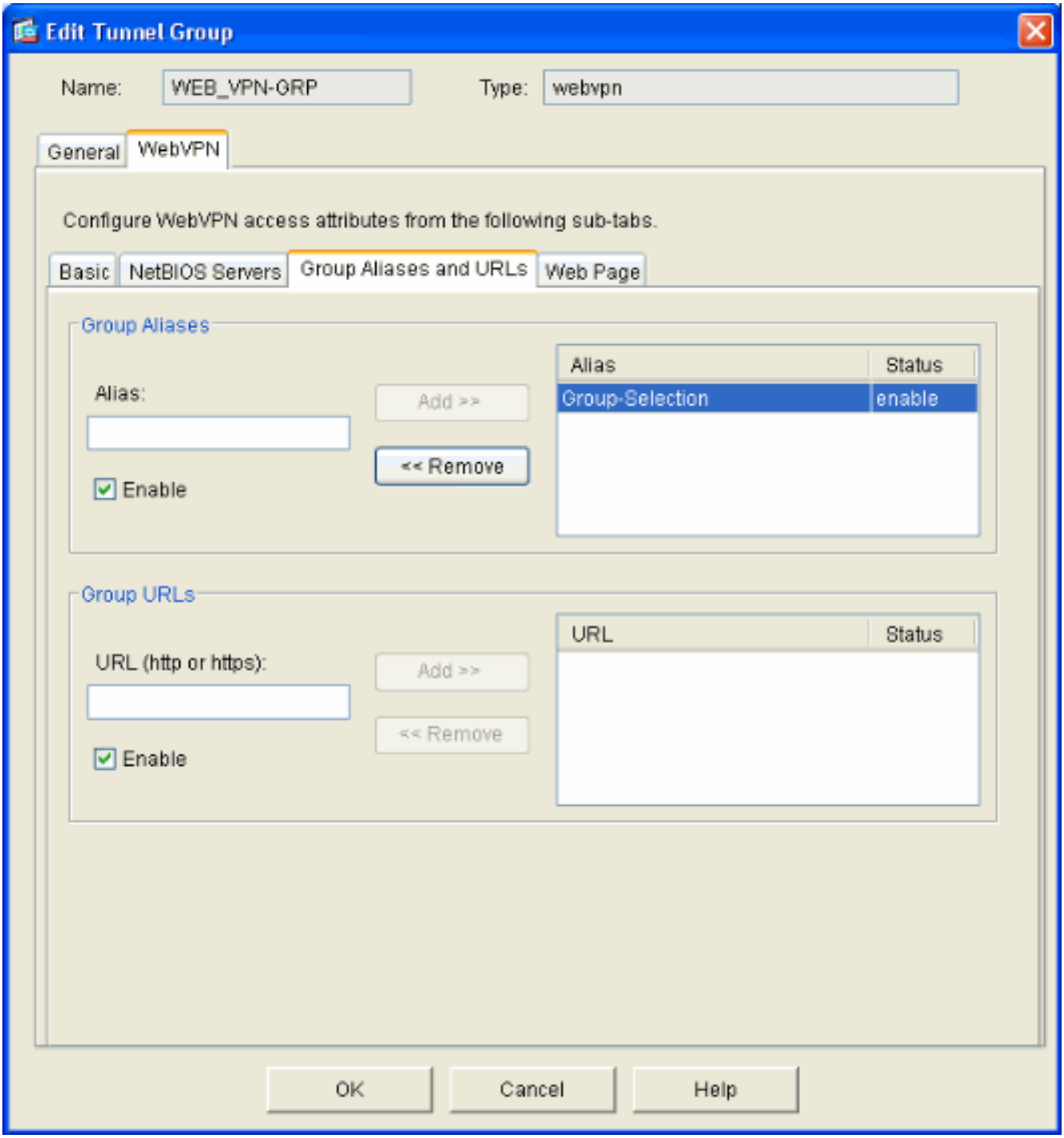
2. Введите имя группы туннелирования, например WEB_VPN-GRP. **На вкладке Basic (Основные настройки) выберите созданную групповую политику и убедитесь в том, что тип группы**
—webvpn.



3. Перейдите на вкладку AAA.В разделе Authentication Server Group (Группы серверов аутентификации) выберите настроенную группу, чтобы разрешить аутентификацию NTLMv1 на контроллере домена.**Дополнительно: Чтобы разрешить использование локальной (LOCAL) базы данных пользователей в случае, если настроенная группа AAA перестанет действовать, отметьте флажок Use LOCAL if Server Group Fails (Использовать LOCAL при сбое серверной группы).** Эта мера может помочь при последующем устранении
неполадок.



4. **Перейдите на вкладку WebVPN и откройте подвкладку Group Aliases and URLs (Псевдонимы и URL-адреса группы).**
5. **В списке Group Aliases (Псевдонимы группы) введите псевдоним и нажмите кнопку Add (Добавить).** Псевдоним добавится в раскрывающийся список, который будет показываться пользователям WebVPN при входе в систему.



6. **Нажмите кнопку OK, а затем Apply.**

Настройка автоматической регистрации для сервера

Чтобы включить для внутренних серверов режим единого входа в систему (SSO), перейдите в командную строку.

Примечание: Этот шаг не может быть выполнен в ASDM и должен быть выполнен с помощью командной строки. Дополнительную информацию см. в разделе Доступ к интерфейсу командной строки.

В команде auto-signon укажите сетевой ресурс, например, сервер, к которому пользователям нужно предоставить доступ. Здесь настраивается один IP-адрес сервера, но можно задать и диапазон адресов, например 10.1.1.0 /24. Для получения дополнительной информации обратитесь к описанию команды auto-signon.

```
ASA>enable ASA#configure terminal ASA(config)#webvpn ASA(config-webpvn)#auto-signon allow ip
10.1.1.200 255.255.255.255 auth-type ntlm ASA(config-webvpn)#quit ASA(config)#exit ASA#write
memory
```

В этом примере выходных данных команда auto-signon настраивается для WebVPN глобально. Эта команда может также использоваться в режиме настройки группы WebVPN или режиме настройки имени пользователя WebVPN. При использовании в режиме настройки группы WebVPN эта команда действует строго для определенной группы. Аналогичным образом в режиме настройки имени пользователя WebVPN команда действует только для конкретного пользователя. Для получения дополнительной информации обратитесь к описанию команды auto-signon.

Итоговая конфигурация ASA

В данном документе используется следующая конфигурация:

Устройство ASA версии 7.1(1)

```
ASA#show running-config : Saved : ASA Version 7.1(1) !
terminal width 200 hostname ASA domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface GigabitEthernet0/0 nameif outside security-
level 0 ip address 172.16.171.51 255.255.255.0 !
interface GigabitEthernet0/1 nameif inside security-
level 100 ip address 10.1.1.1 255.255.255.0 ! interface
GigabitEthernet0/2 shutdown no nameif no security-level
no ip address ! interface GigabitEthernet0/3 shutdown no
nameif no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
cisco.com pager lines 24 mtu inside 1500 mtu outside
1500 no failover asdm image disk0:/asdm512.bin no asdm
history enable arp timeout 14400 route outside 0.0.0.0
0.0.0.0 172.16.171.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute !---
AAA server configuration aaa-server Windows_NT protocol
nt aaa-server Windows_NT host 10.1.1.200 nt-auth-domain-
controller ESC-SJ-7800 !--- Internal group policy
configuration group-policy Internal-GRP_POL_WEBVPN
internal group-policy Internal-GRP_POL_WEBVPN attributes
vpn-tunnel-protocol webvpn webvpn url-list value
webserver username cisco password Q/odgwmtmVIw4Dcm
encrypted privilege 15 aaa authentication http console
LOCAL aaa authentication ssh console LOCAL aaa
authentication enable console LOCAL http server enable
8181 http 0.0.0.0 0.0.0.0 outside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !---
Trustpoint/certificate configuration crypto ca
trustpoint Local-TP enrollment self crl configure crypto
ca certificate chain Local-TP certificate 31 308201b0
30820119 a0030201 02020131 300d0609 2a864886 f70d0101
04050030 1e311c30 1a06092a 864886f7 0d010902 160d4153
412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334
3930345a 170d3136 30333237 31333439 30345a30 1e311c30
1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e
636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d
00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a
```

```
1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434
561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404
9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17
68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3
776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06
092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544
59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d
3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b
af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de
775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a
f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c
quit !--- Tunnel group configuration tunnel-group
WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP
general-attributes authentication-server-group
Windows_NT default-group-policy Internal-GRP_POL_WEBVPN
tunnel-group WEB_VPN-GRP webvpn-attributes group-alias
Group-Selection enable telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
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 Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6 : end
```

Проверка

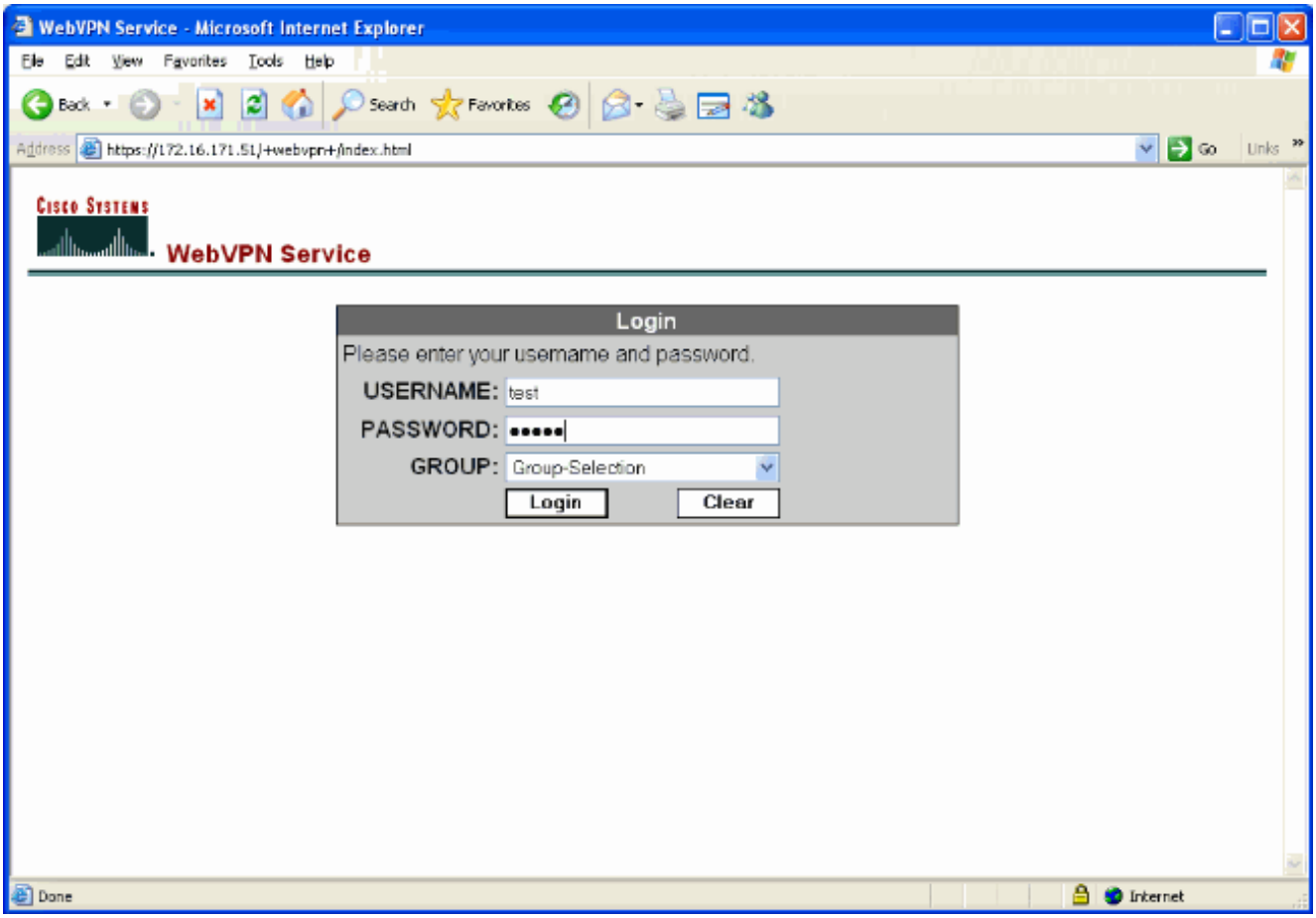
Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

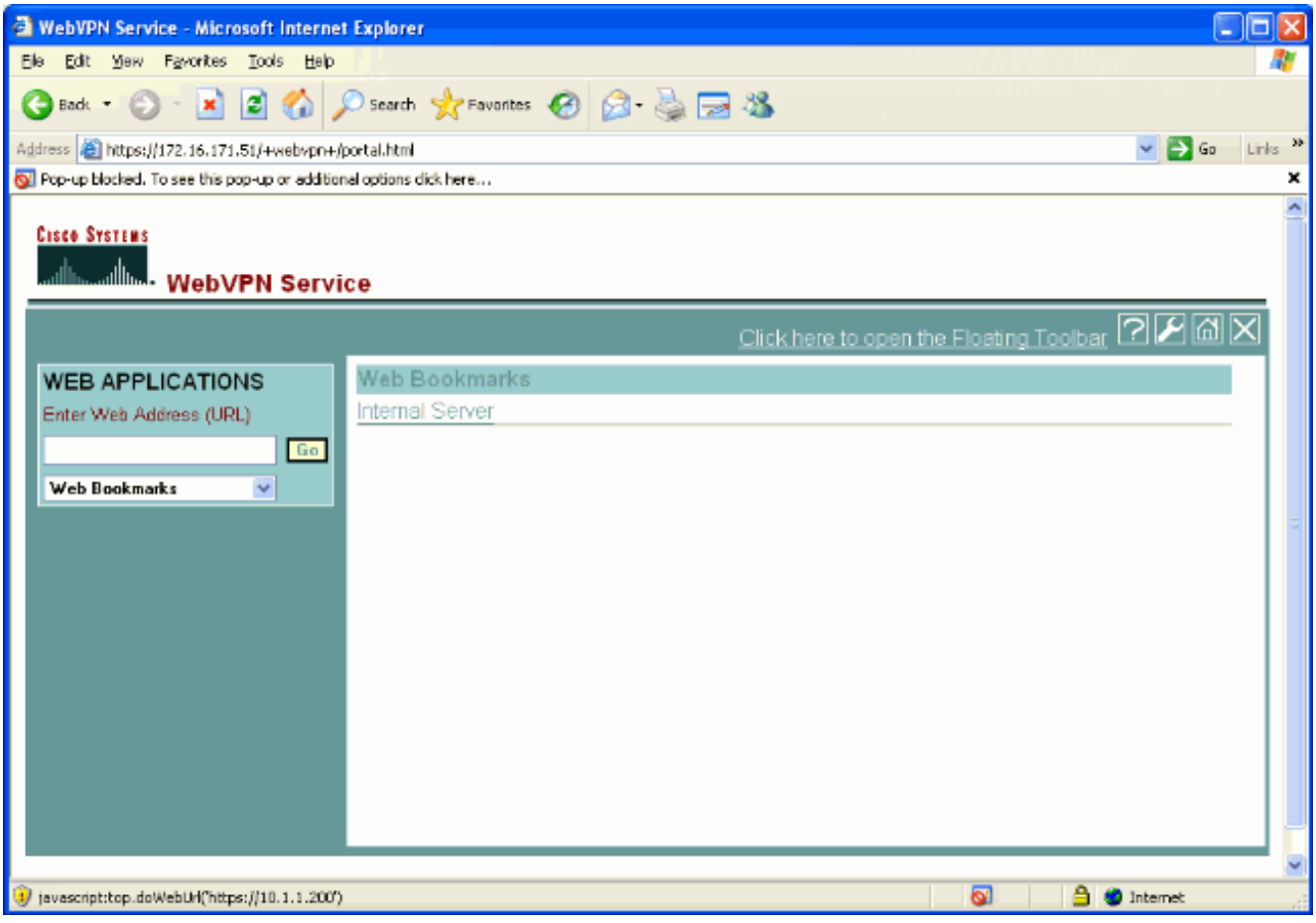
Проверка входа WebVPN

Для проверки конфигурации войдите в систему как пользователь.

1. Попытайтесь войти в устройство ASA, применяя информацию о пользователе из домена NT. Выберите псевдоним группы, настроенный на шаге 5 в разделе Настройка группы туннелирования.

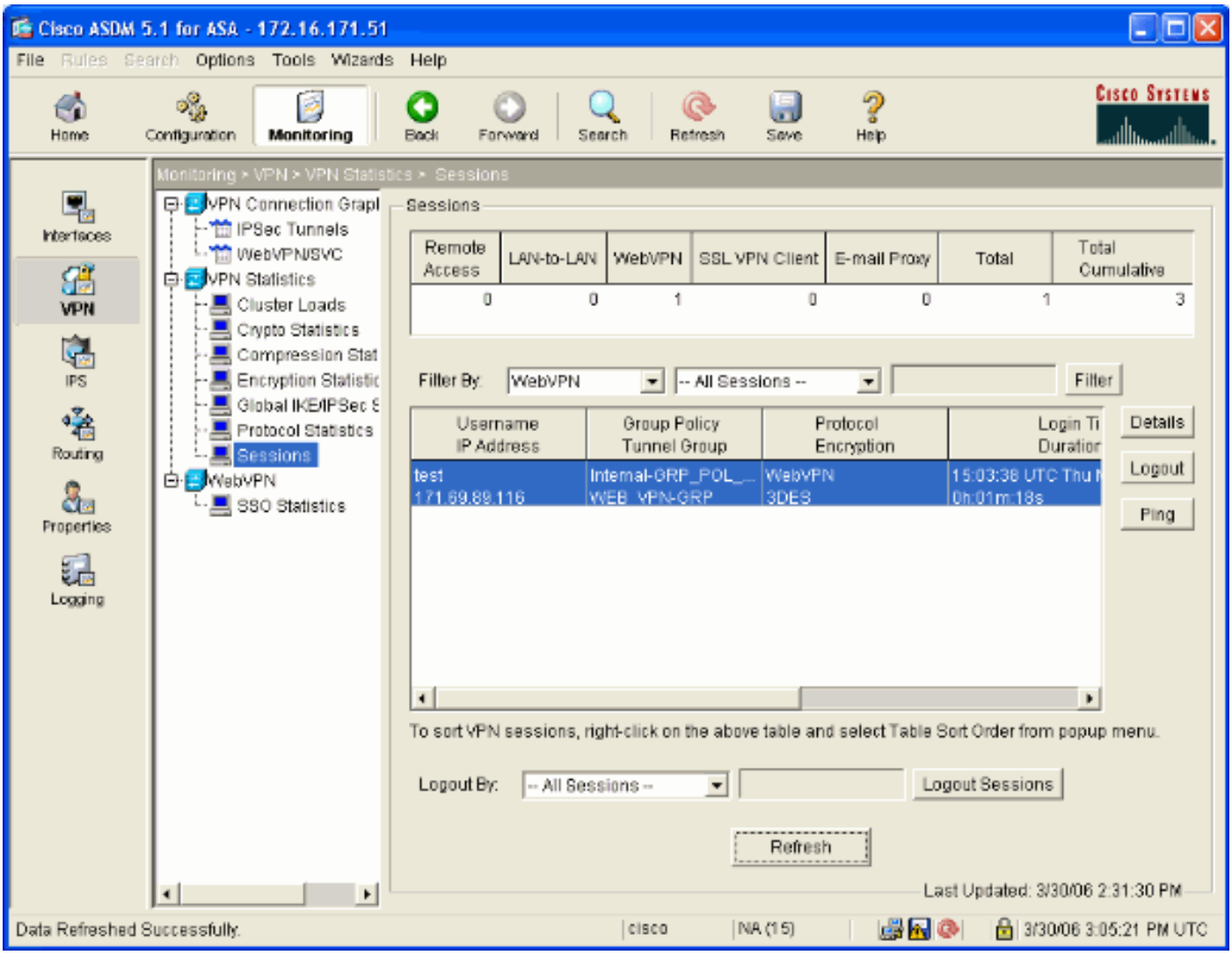


2. Найдите настроенные ссылки, указывающие на внутренние серверы. Чтобы проверить ссылку, щелкните на ней
мышью.



Контроль сеансов

Выберите Monitoring > VPN > VPN Statistics > Sessions (Контроль > VPN > Статистика VPN > Сеансы) и найдите сеанс WebVPN, относящийся к группе, настройка которой выполнялась в этом документе.



Отладка сеанса WebVPN

Следующие выходные данные представляют собой пример успешно проведенного сеанса отладки WebVPN.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

```
ASA#debug webvpn 255 INFO: debug webvpn enabled at level 255 ASA# ASA#
webvpn_portal.c:ewaFormServe_webvpn_login[1570] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286] WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782] !--- Begin AAA WebVPN: calling AAA with
ewsContext (78986968) and nh (78960800)! WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422] WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095] WebVPN: user: (test) authenticated. !--- End
AAA webvpn_auth.c:http_webvpn_auth_accept[2093] webvpn_session.c:http_webvpn_create_session[159]
webvpn_session.c:http_webvpn_find_session[136] WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136] webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202] traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421] webvpn_auth.c:webvpn_auth[286]
```

```
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. !--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

- Если на странице входа WebVPN отсутствует раскрывающийся список Group (Группа), то убедитесь, что выполнен шаг 2 из раздела Включение WebVPN на внешнем интерфейсе и шаг 5 из раздела Настройка группы туннелирования. Если эти шаги не будут выполнены и раскрывающийся список не появится, то аутентификация будет выполняться в группе по умолчанию и с наибольшей вероятностью не пройдет.
- Несмотря на то, что невозможно назначить права доступа пользователю в ASDM или на устройстве ASA, можно ограничить пользователей правами доступа Microsoft Windows на контроллере домена. Добавьте необходимые разрешения группы NT для web-страницы, при доступе к которой пользователь проходит аутентификацию. После входа пользователя в WebVPN с разрешениями группы доступ к указанным страницам соответственно либо предоставляется, либо запрещается. ASA только играет роль промежуточного хоста аутентификации от имени контроллера домена; весь обмен данными здесь идет посредством протоколов NTLMv1.
- Настроить SSO для Sharepoint по WebVPN нельзя, поскольку сервер Sharepoint не поддерживает аутентификацию на основе форм. Как следствие, закладки с отправкой или подключаемая процедура отправки здесь не действуют.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Cisco Systems – техническая поддержка и документация