ASA 7.1/7.2: Разрешите раздельное туннелирование для SVC на примере конфигурации ASA

Содержание

Введение

Этот документ предоставляет пошаговые инструкции о том, как позволить Клиентам VPN Протокола SSL (SVC) доступ к Интернету, в то время как они туннелированы в устройство адаптивной защиты Cisco (ASA). Эта конфигурация позволяет безопасный доступ SVC корпоративным ресурсам через SSL и предоставляет необеспеченный доступ к Интернету с использованием разделенного туннелирования.

Возможность передавать через один интерфейс как защищенный трафик, так и открытый называется разделенным туннелированием. Раздельное туннелирование требует точного указания, какой трафик является защищённым и откуда он происходит, таким образом только указанный трафик попадает в туннель, в то время как другой передается в незашифрованном виде через публичную сеть (Интернет).

Предварительные условия

Требования

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

- Локальные администраторские привилегии на всех удаленных рабочих станциях
- Java и элементы управления ActiveX на удаленной рабочей станции
- Порт 443 (SSL) не заблокирован нигде вдоль пути подключения

Используемые компоненты

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

- Устройство адаптивной защиты (ASA) серии 5500 Cisco, которое работает под управлением ПО версии 7.2 (2)
- Версия Cisco SSL VPN Client для Windows 1.1.4.179**Примечание:** Загрузите пакет VPN-клиента SSL (SVC) (sslclient-win*.pkg) от Загрузки Программного обеспечения Cisco (только зарегистрированные клиенты). Скопируйте SVC к флэш-памяти ASA, который должен быть загружен к компьютерам удаленного пользователя для установления VPN-подключения на базе SSL с ASA. См. Установку Раздела программного обеспечения SVC руководства по конфигурации ASA для получения дополнительной информации.
- ПК, который выполняет SP4 профессионала Windows 2000 или Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM) версия 5.2 (2)

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.

Общие сведения

Клиент SSL VPN (SVC) является технологией туннелирования VPN, которая приносит удаленным пользователям пользу VPN-клиента IPSec без потребности в администраторах сети, чтобы установить и настроить VPN-клиентов IPSec на удаленных компьютерах. SVC использует шифрование SSL, которое уже присутствует на удаленном компьютере, а также входе в систему WebVPN и аутентификации устройства безопасности.

Для установления сеанса SVC удаленный пользователь вводит IP-адрес интерфейса WebVPN устройства безопасности в браузере и подключения браузера к тому интерфейсу и отображает экран входа в систему WebVPN. Если вы удовлетворяете вход в систему и аутентификацию, и устройство безопасности определяет вас как требование SVC, устройство безопасности загружает SVC к удаленному компьютеру. Если устройство безопасности определяет вас с опцией для использования SVC, устройство безопасности загружает SVC к удаленному компьютеру, в то время как это представляет ссылку на окне для пропуска установки SVC.

После загрузки SVC устанавливает и настраивает себя, и затем SVC или остается или деинсталлирует себя, который зависит от конфигурации от удаленного компьютера, когда завершается соединение.

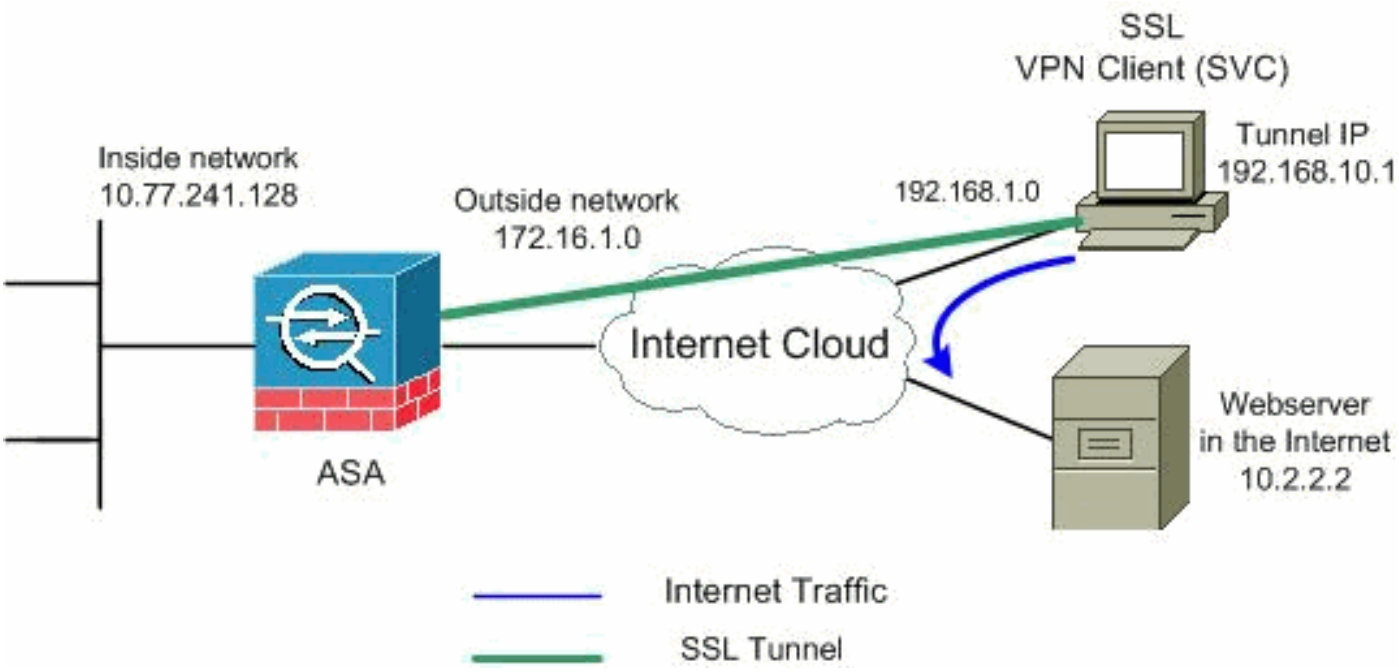
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

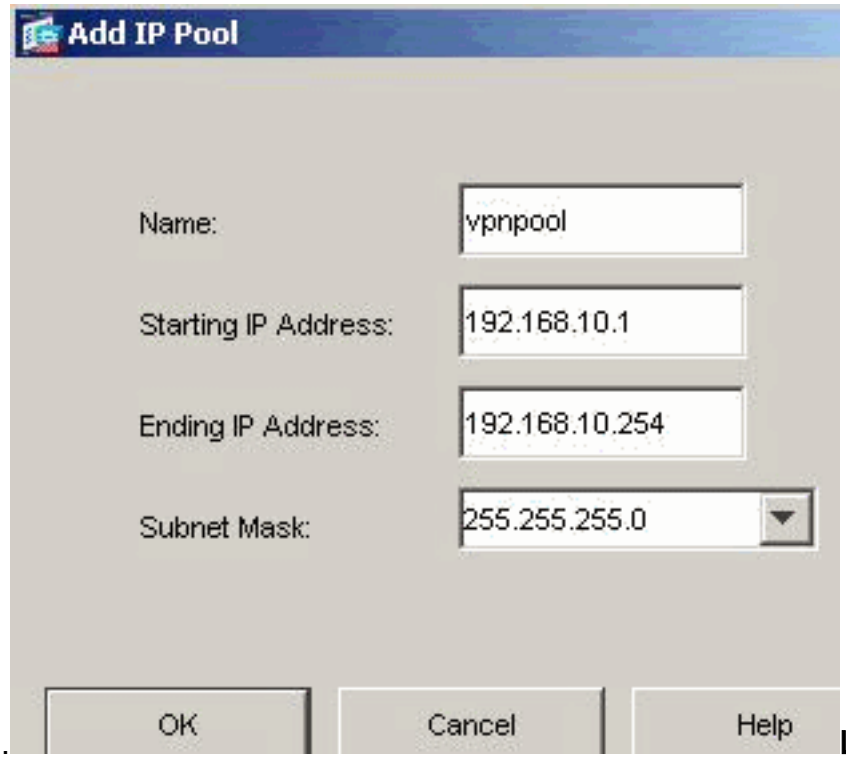


Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Конфигурации ASA Использование ASDM 5.2 (2)

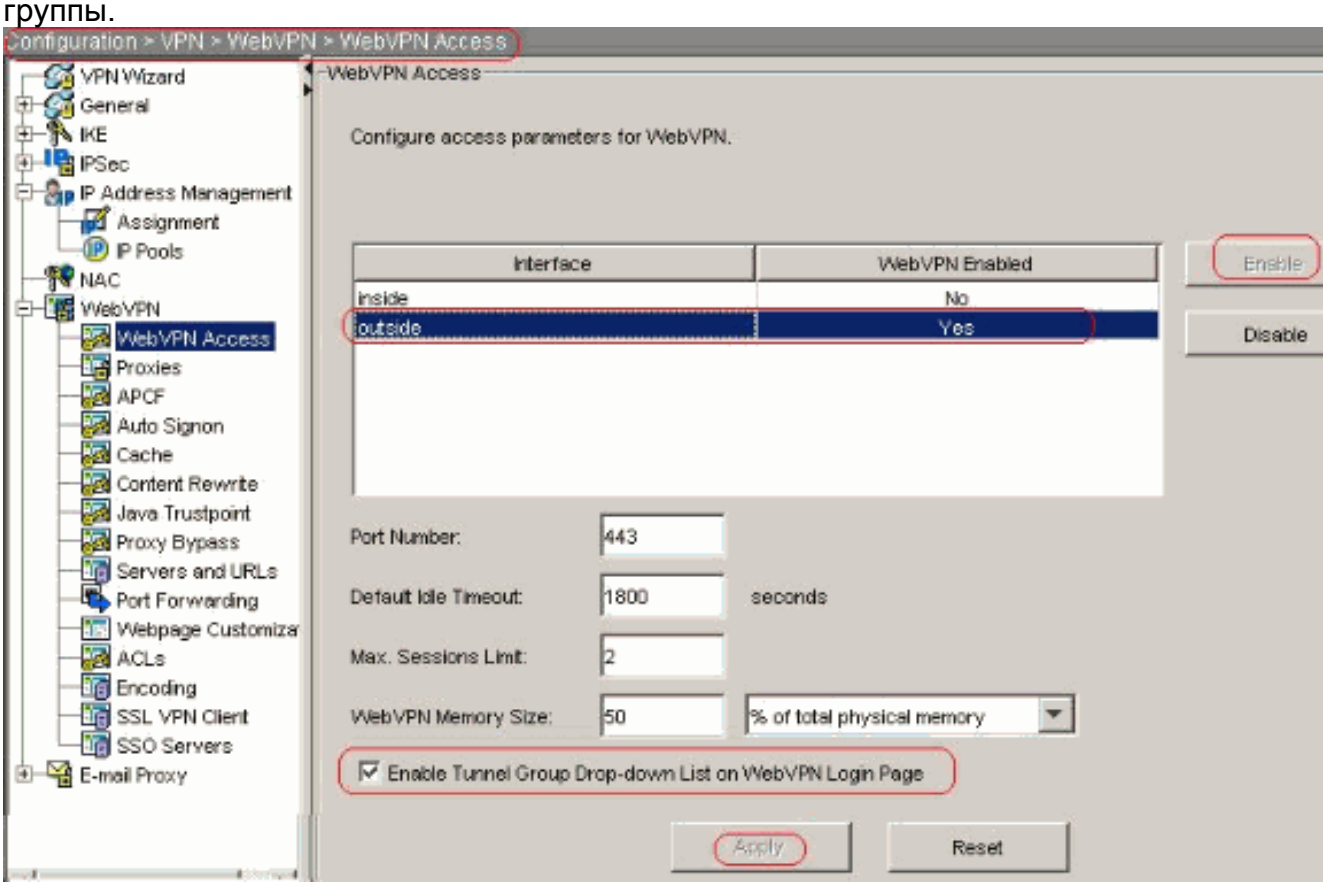
Выполните эти шаги для настройки VPN SSL на ASA с Разделенным туннелированием как показано:

1. Документ предполагает, что базовая конфигурация, такая как конфигурация интерфейса и т.д уже сделана и работает должным образом.**Примечание:** Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.**Примечание:** Нельзя включать WebVPN и ASDM на одном и том же интерфейсе ASA, если не изменены номера портов. Для получения дополнительных сведений обратитесь к документу Включение ASDM и WebVPN на одном и том же интерфейсе ASA.
2. Выберите **Configuration> VPN> IP Address Management> IP Pools** для создания пула IP-адреса: **vpnpool** для клиентов

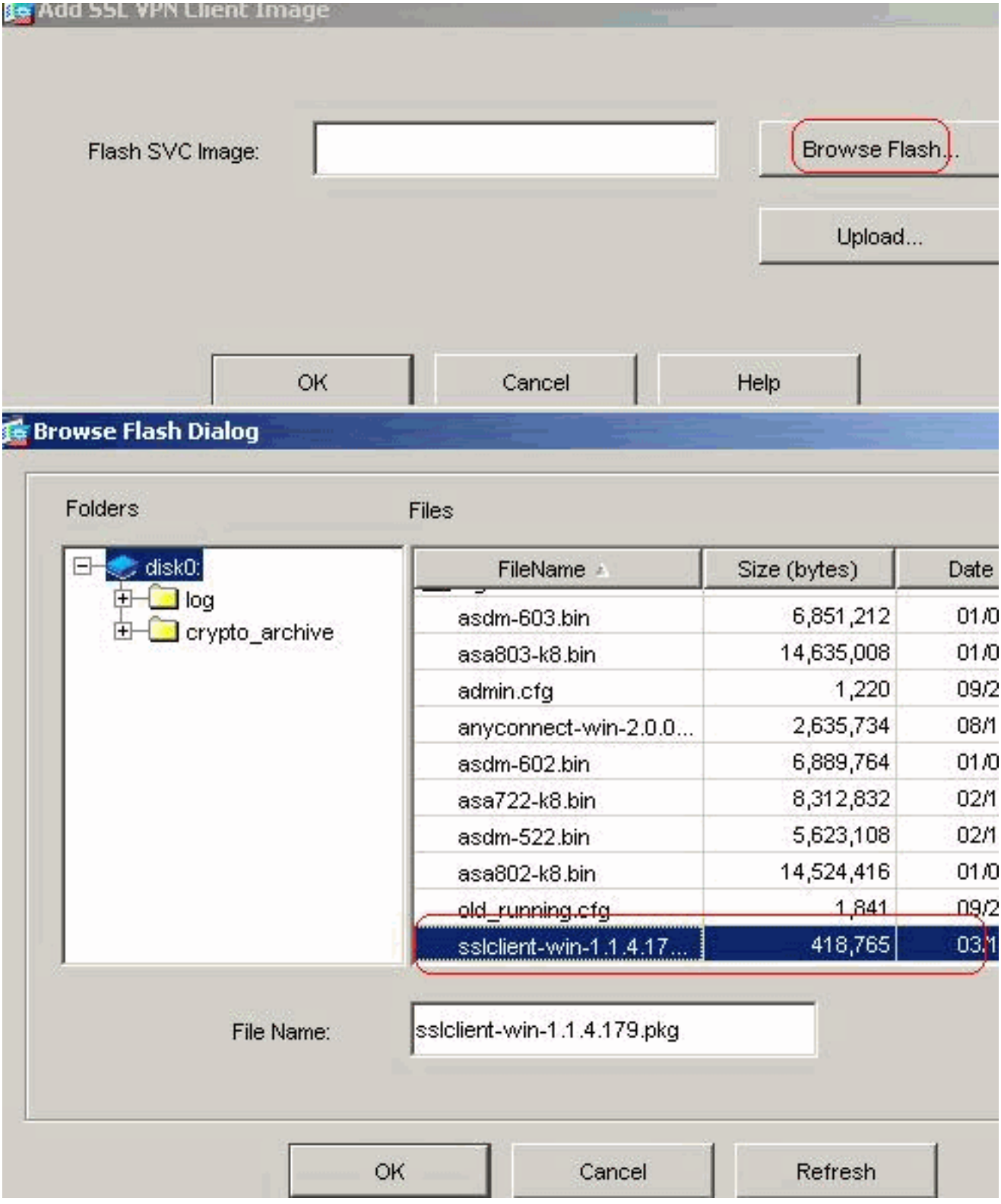


VPN. **Щелкните "Применить".**

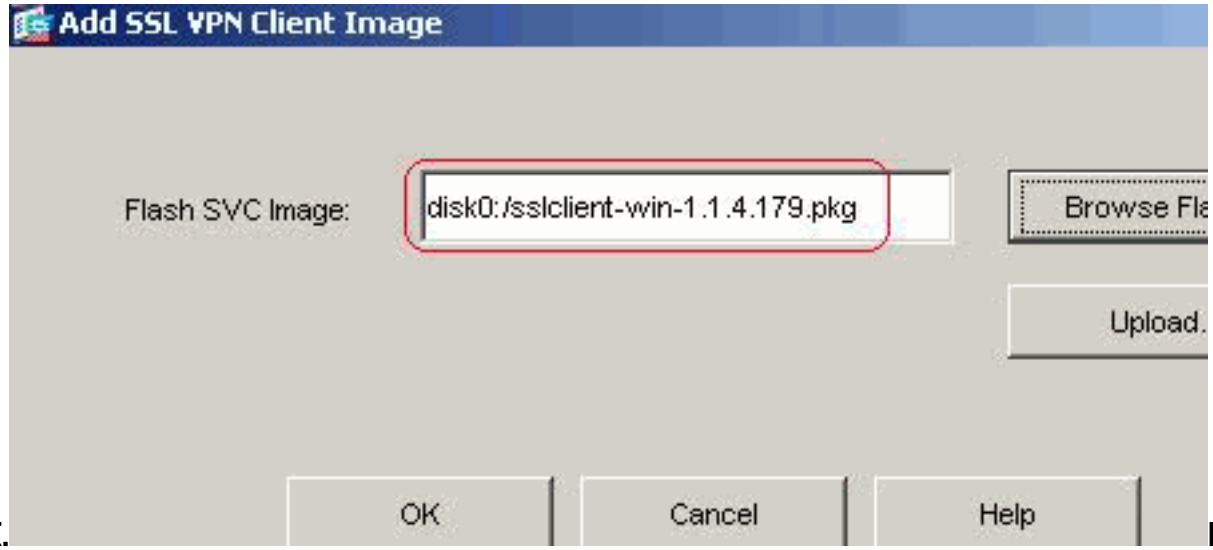
3. **Включенный WebVPN**Выберите **Configuration> VPN> WebVPN> WebVPN Access** и выделите внешний интерфейс с мышью и нажмите **Enable**. Проверка **Включает Выпадающий список Туннельной группы на** флажке **WebVPN Login Page** для включения выпадающего, кажется, в странице входа для пользователей, выбирают их соответствующие
группы.



Щелкните "Применить".Выберите **Configuration> VPN> WebVPN> SSL VPN Client> Add** для добавления образа VPN-клиента SSL (SVC) от флэш-памяти ASA как показано.



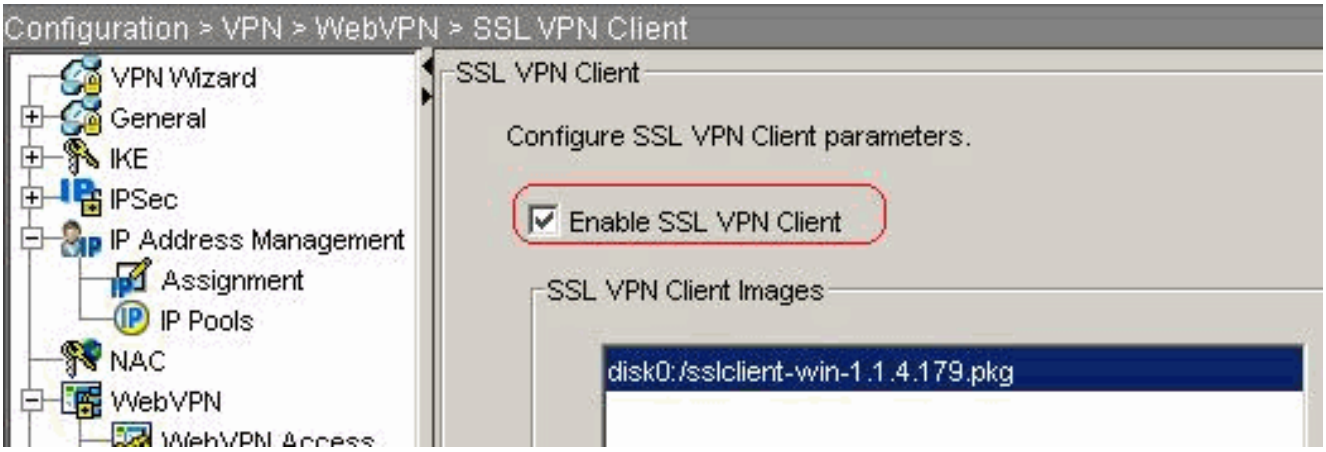
Нажмите кнопку



OK. **Наж**

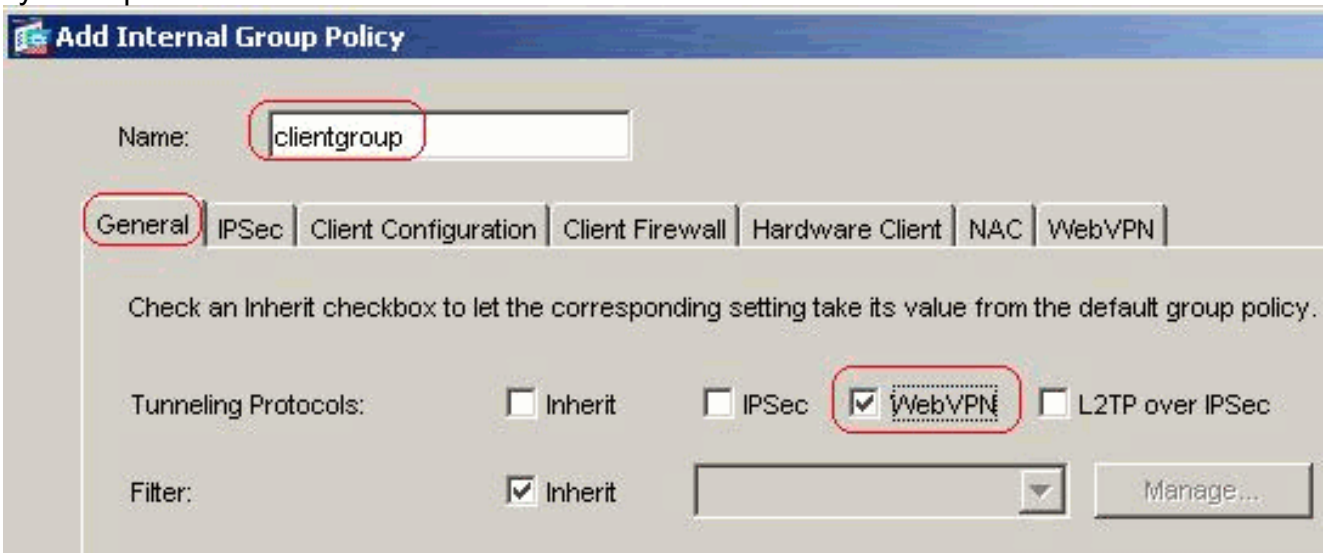
мите кнопку OK.Нажмите флажок **SSL VPN**

Client.



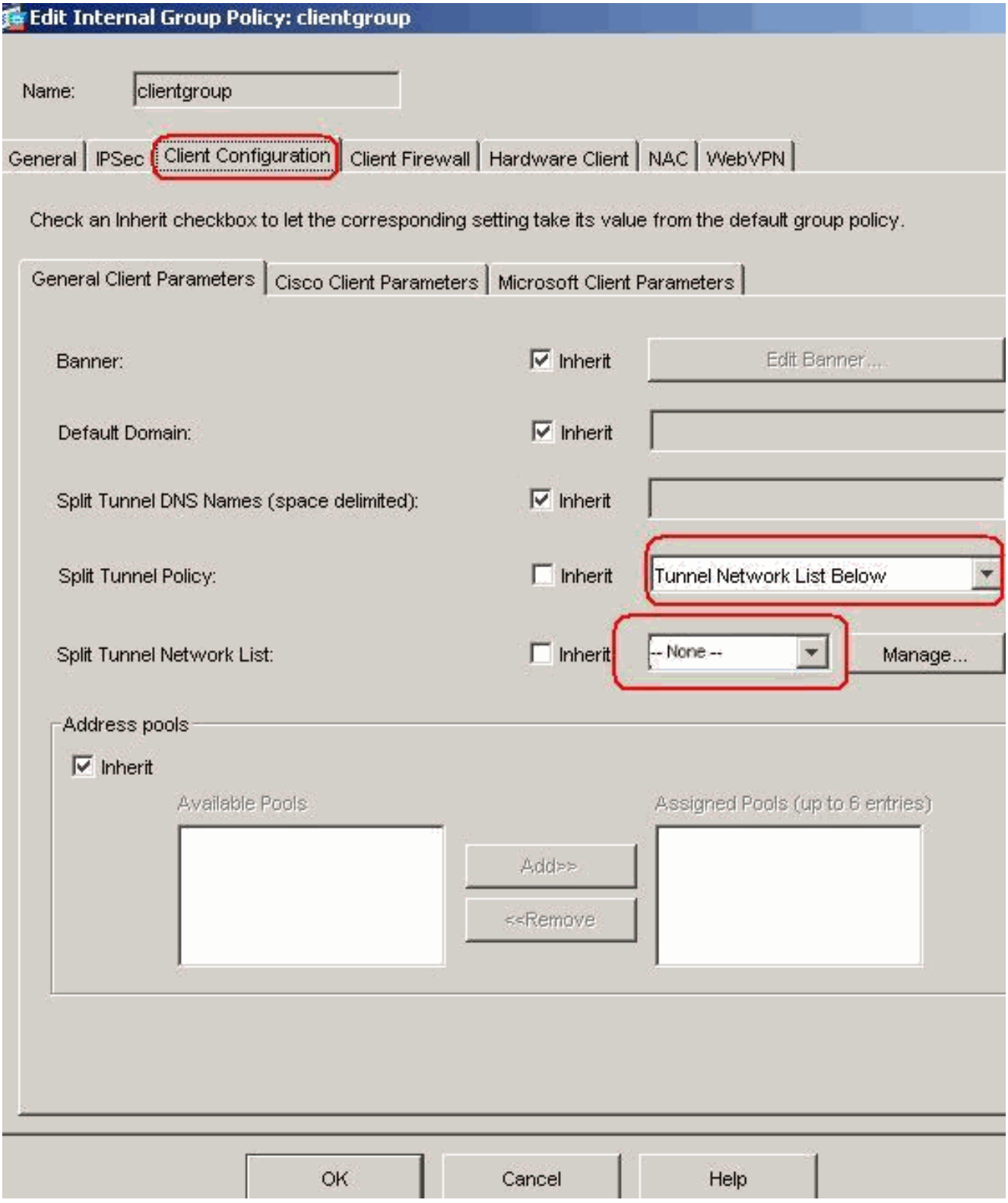
Щелкните "Применить".Эквивалентная конфигурация в интерфейсе командной строки:

4. **Настройка групповой политики**Выберите **Configuration> VPN> General> Group Policy> Add (Internal Group Policy)** для создания внутренней групповой политики **clientgroup**. Под **Общим** выберите **флажок WebVPN** для включения WebVPN как протокола туннелирования.

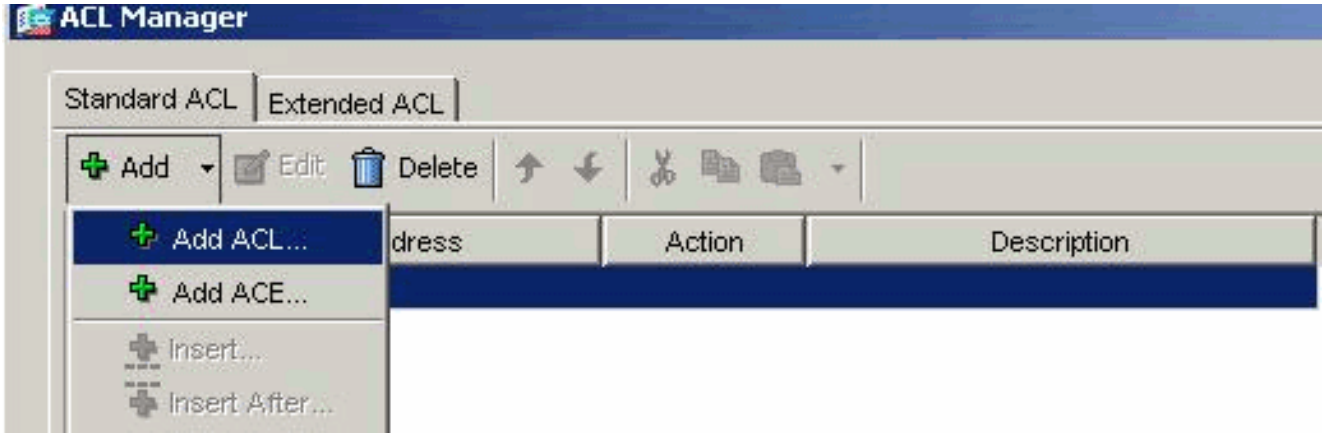


Во вкладке **Client Configuration> General Client Parameters** снимите **Наследовать** флажок для Политики раздельных туннелей и выберите **Tunnel Network List Below** из выпадающего списка.**Снимите флажок Наследование для списка сетей с разделенными туннелями, затем нажмите кнопку Контроль, чтобы запустить диспетчер**

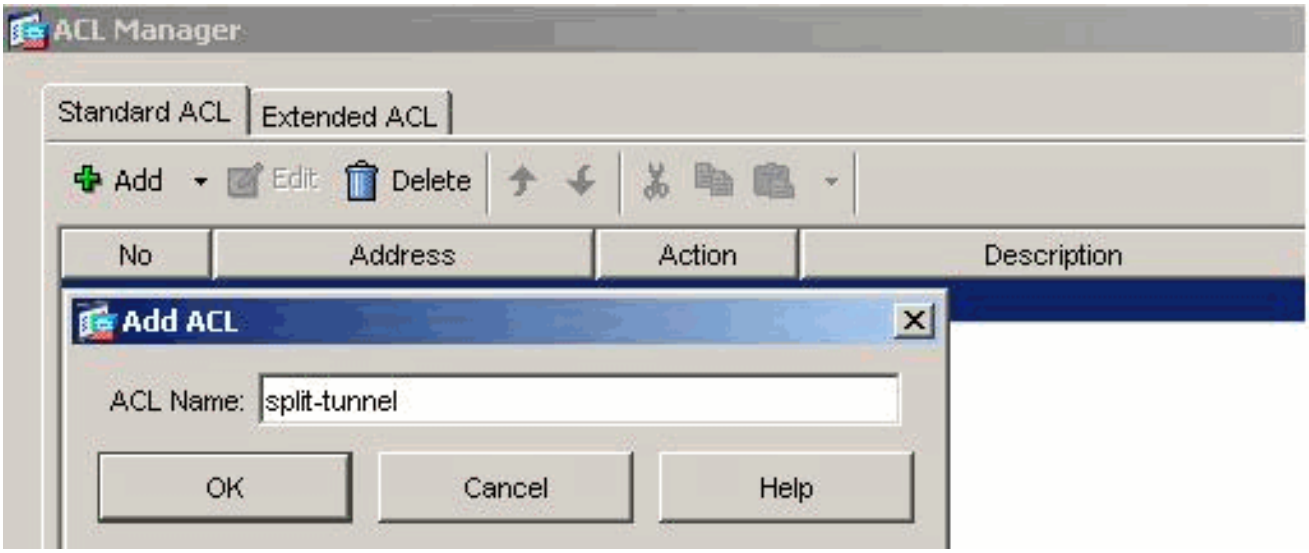
ACL.



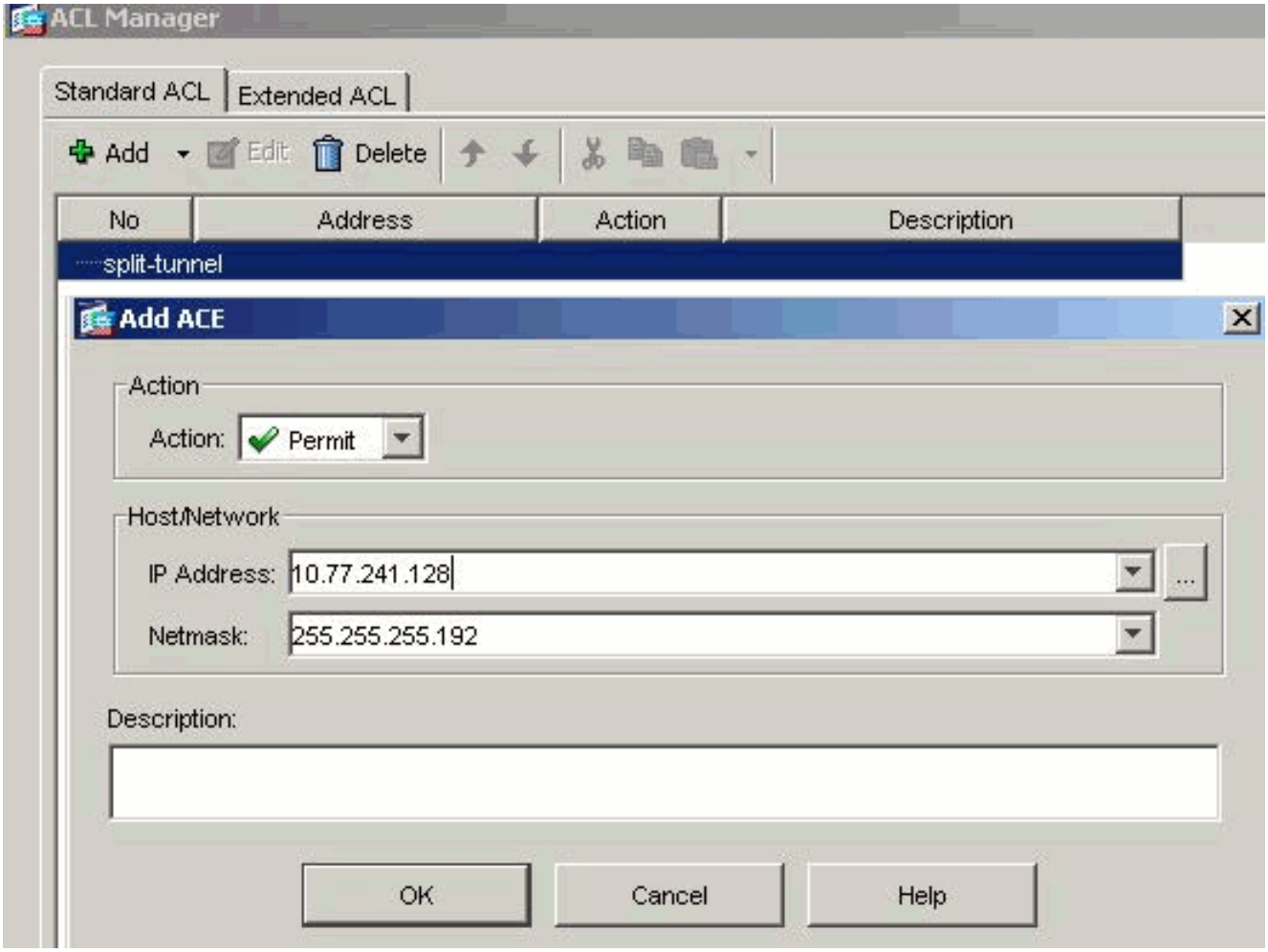
В данном диспетчере выберите Добавить > Добавить список ACL..., чтобы создать новый список контроля
доступа.



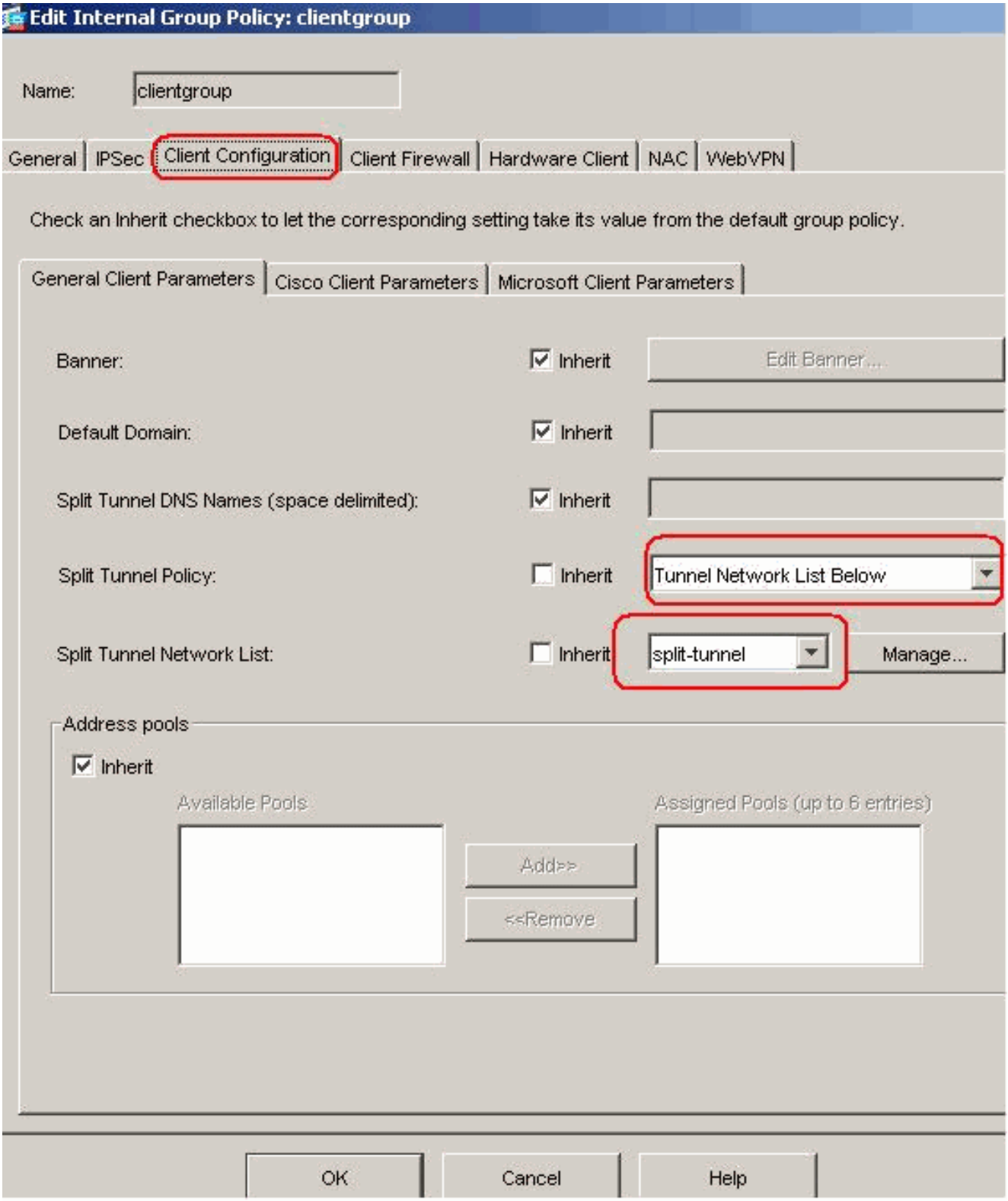
Укажите имя ACL и нажмите кнопку OK.



После создания списка ACL выберите Add > Add ACE, чтобы добавить элемент контроля доступа (ACE).Задайте запись ACE, соответствующую локальной сети, расположенной за модулем ASA. В этом случае сеть является 10.77.241.128/26, и выберите **Permit**.**Нажмите кнопку OK, чтобы завершить работу с приложением ACL Manager.**

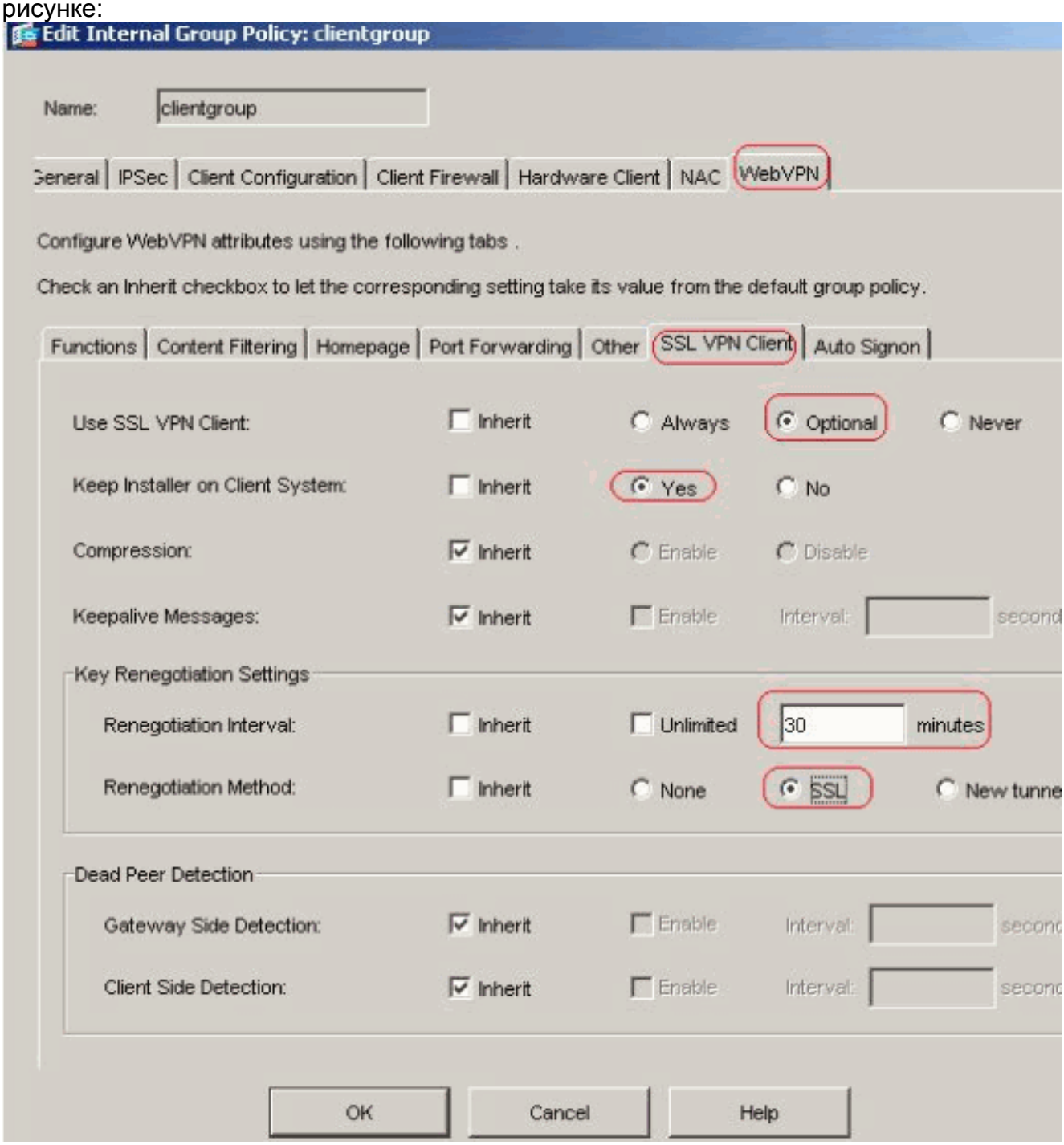


Убедитесь, что только что созданный ACL выбран для списка сетей с разделенными туннелями.**Нажмите кнопку OK, чтобы вернуться к настройке групповой политики.**

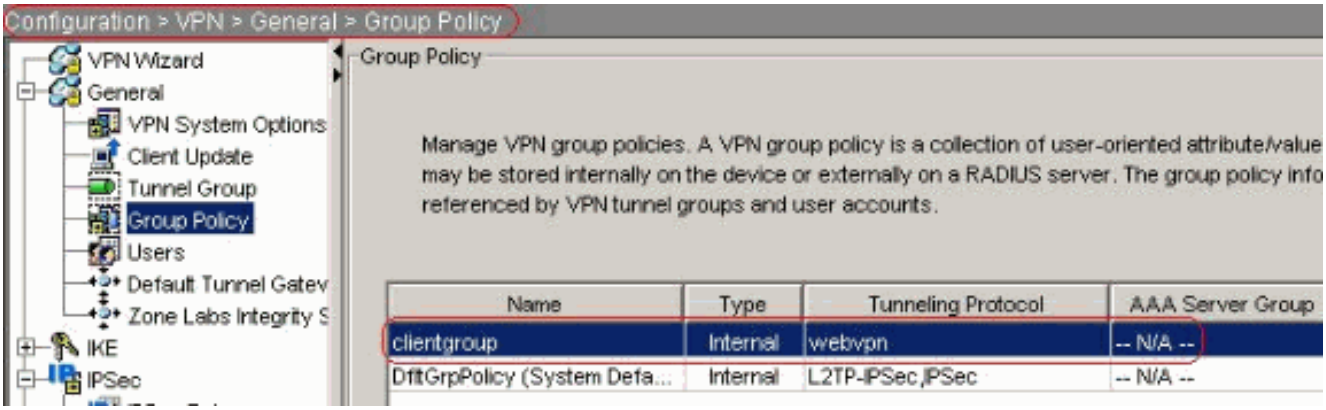


В главной странице нажмите **Apply** и затем **Передайте** (при необходимости) для передачи команд к ASA.**В разделе "Use SSL VPN Client" снимите флажок Inherit и установите переключатель в положение Optional.**Этот выбор позволяет удаленному клиенту выбирать, нажать ли вкладку **WebVPN> SSLVPN Client** и выбрать эти опции:Не делайте для загрузки SVC. Выбор Always гарантирует, что SVC будет загружаться на удаленную рабочую станцию во время каждого подключения SSL VPN.**В разделе "Keep Installer on Client System" снимите флажок Inherit и установите переключатель в положение Yes.**Это позволит ПО SVC оставаться на клиентской машине. Таким образом, модулю ASA не потребуется загружать ПО SVC на клиент во время каждого установления соединения. Такой выбор оптимален для удаленных пользователей, которые часто обращаются к корпоративной сети.**В разделе "Renegotiation Interval"**

снимите флажки Inherit и Unlimited, после чего укажите время до смены ключа в минутах.Безопасность улучшена при установлении пределов для промежутка времени, что ключ допустим.**В разделе "Renegotiation Method" снимите флажок Inherit и установите переключатель в положение SSL.** При повторном согласовании может использоваться имеющийся туннель SSL или новый туннель, созданный специально для повторного согласования.Атрибуты SSL VPN Client должны быть настроены, как показано на
рисунке:

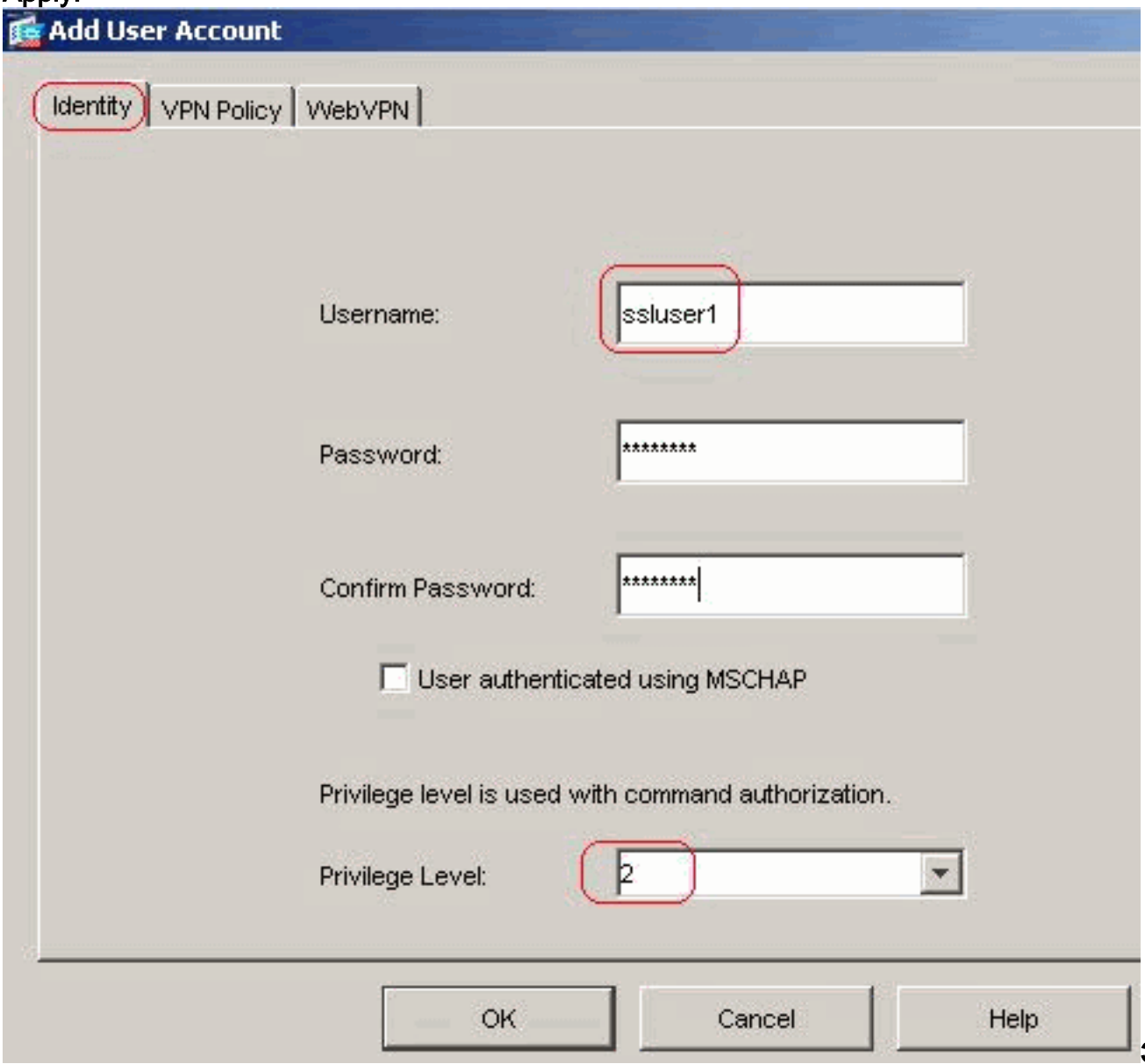


Нажмите кнопку OK, а затем Apply.



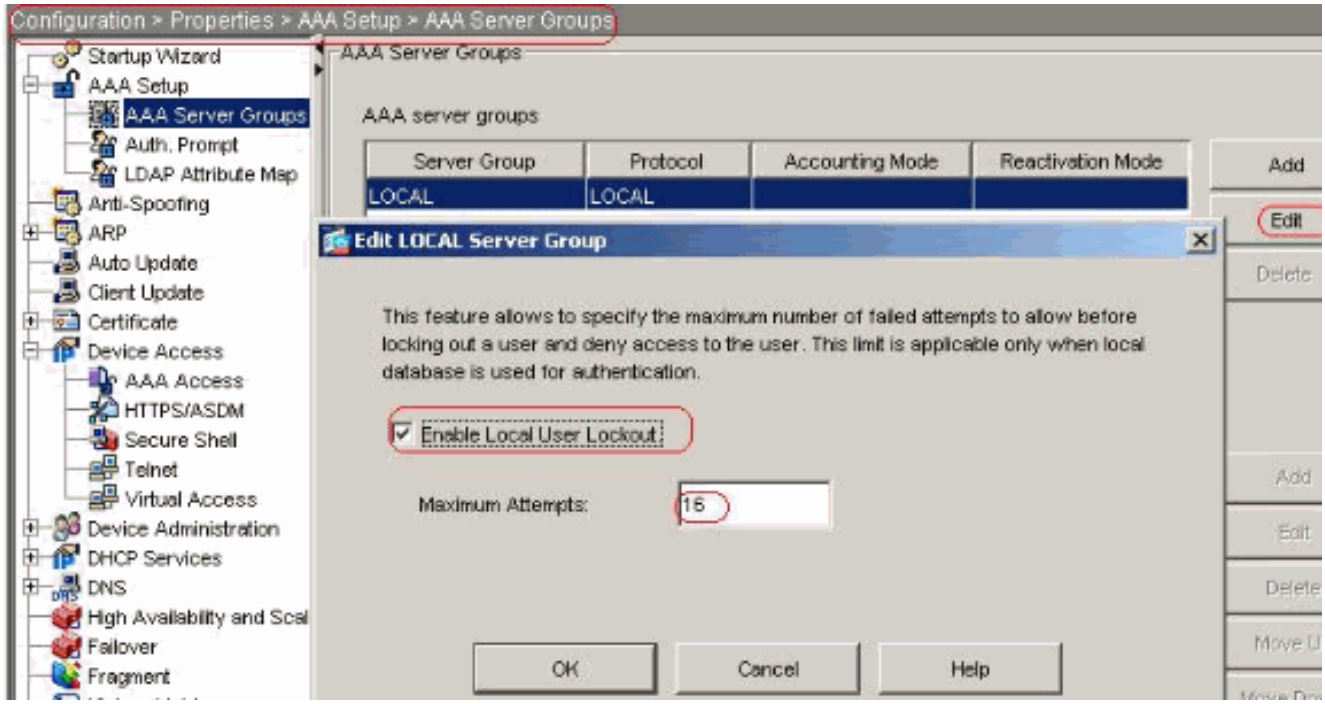
Эквивалентная конфигурация в интерфейсе командной строки:

5. Выберите **Configuration> VPN>,> Users General> Добавляет** для создания учетной записи нового пользователя **ssluser1**. **Нажмите кнопку OK, а затем Apply.**



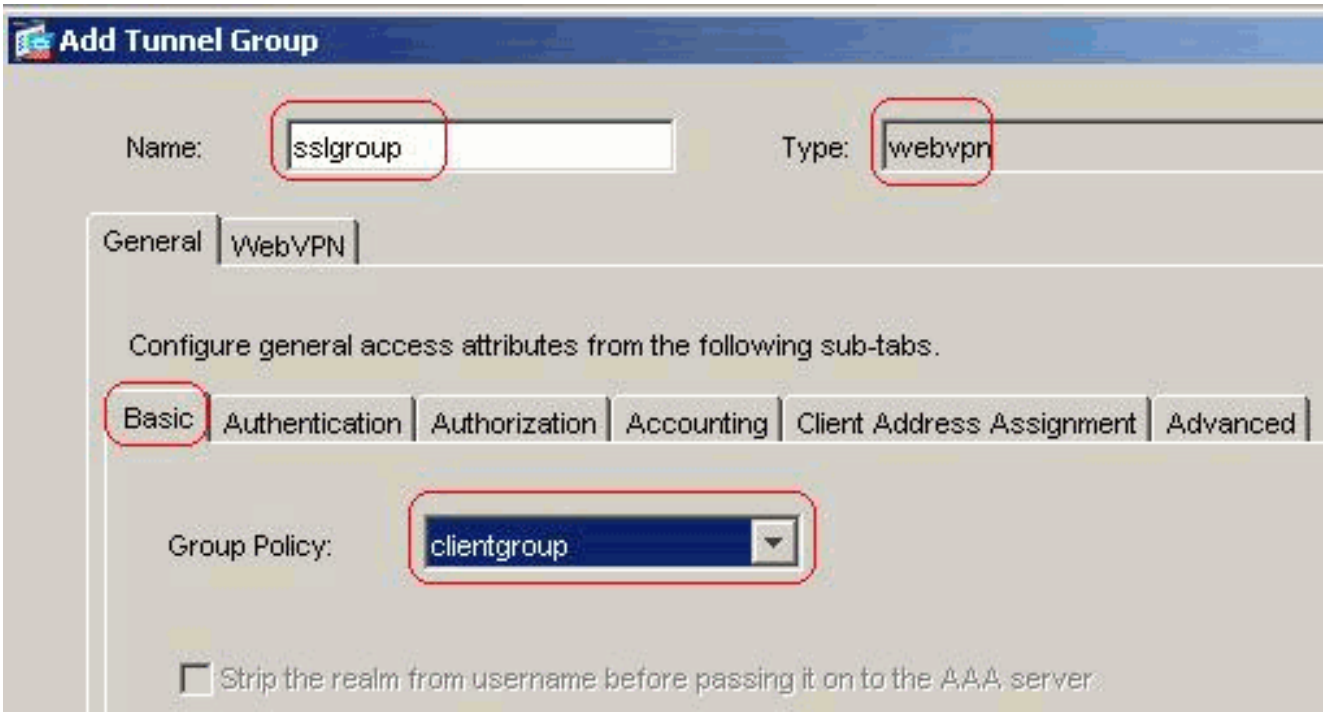
Эквивалентная конфигурация в интерфейсе командной строки:

6. Выберите **Configuration> Properties> AAA Setup> AAA Servers Groups> Edit**, чтобы модифицировать **ЛОКАЛЬНУЮ** группу серверов по умолчанию и выбрать флажок **Enable Local User Lockout** с максимальным значением попыток как **16**.

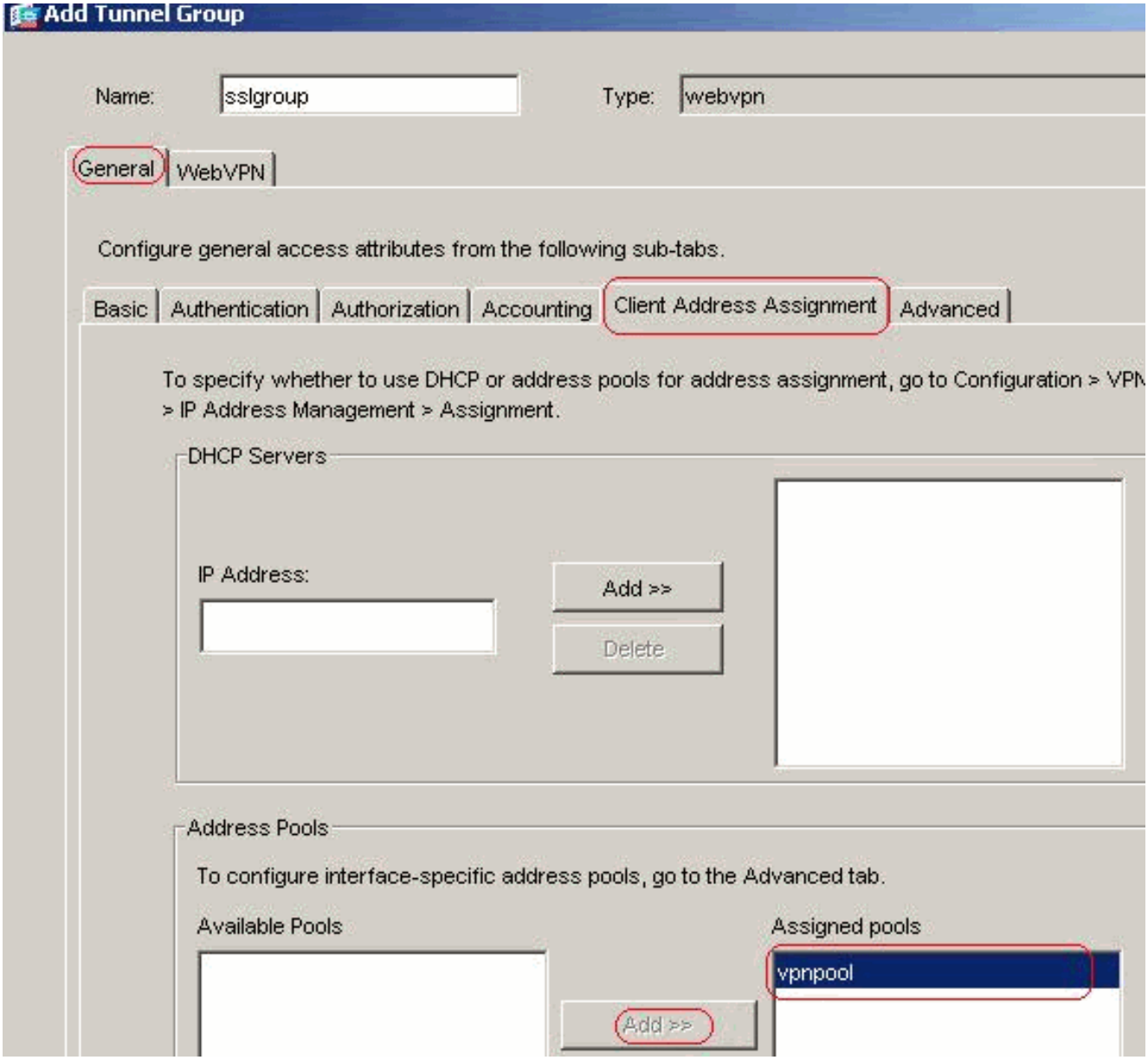


Эквивалентная конфигурация в интерфейсе командной строки:

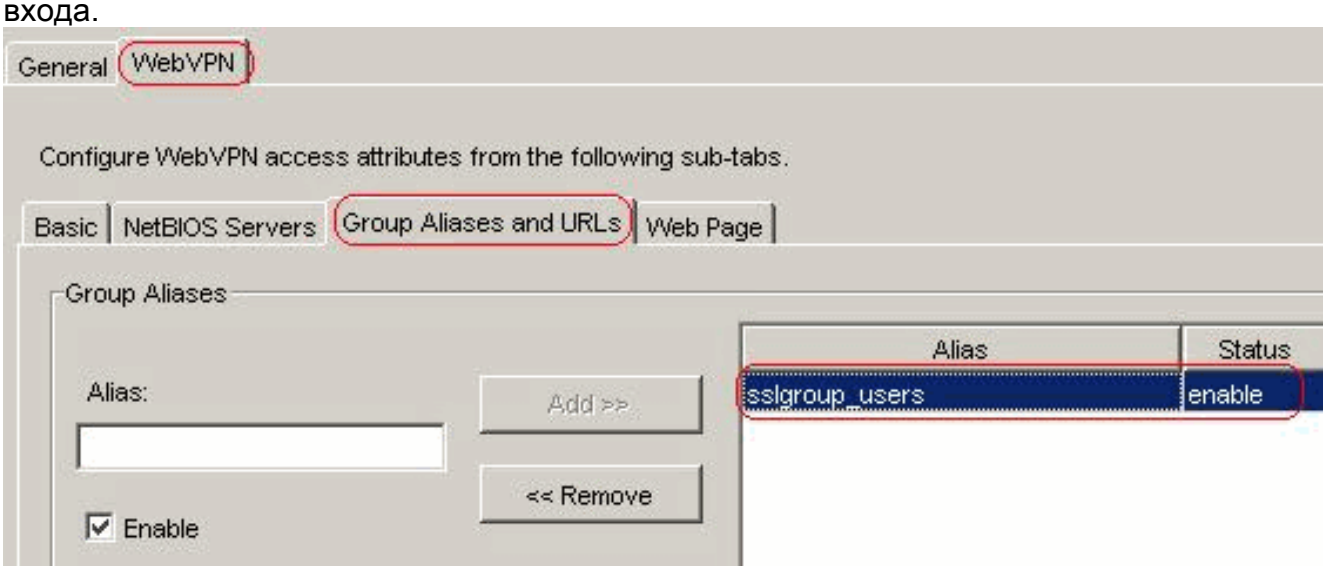
7. **Настройка группы туннелирования**Выберите **Configuration> VPN> General> Tunnel Group> Add (доступ WebVPN)** для создания нового **sslgroup** туннельной группы.Во вкладке **General> Basic** выберите Group Policy в качестве **clientgroup** от выпадающего списка.



В целом> клиентская вкладка **присвоение адреса**, под Пулами адресов, **нажмите Add>>** для присвоения пула доступного адреса
vpnpool.

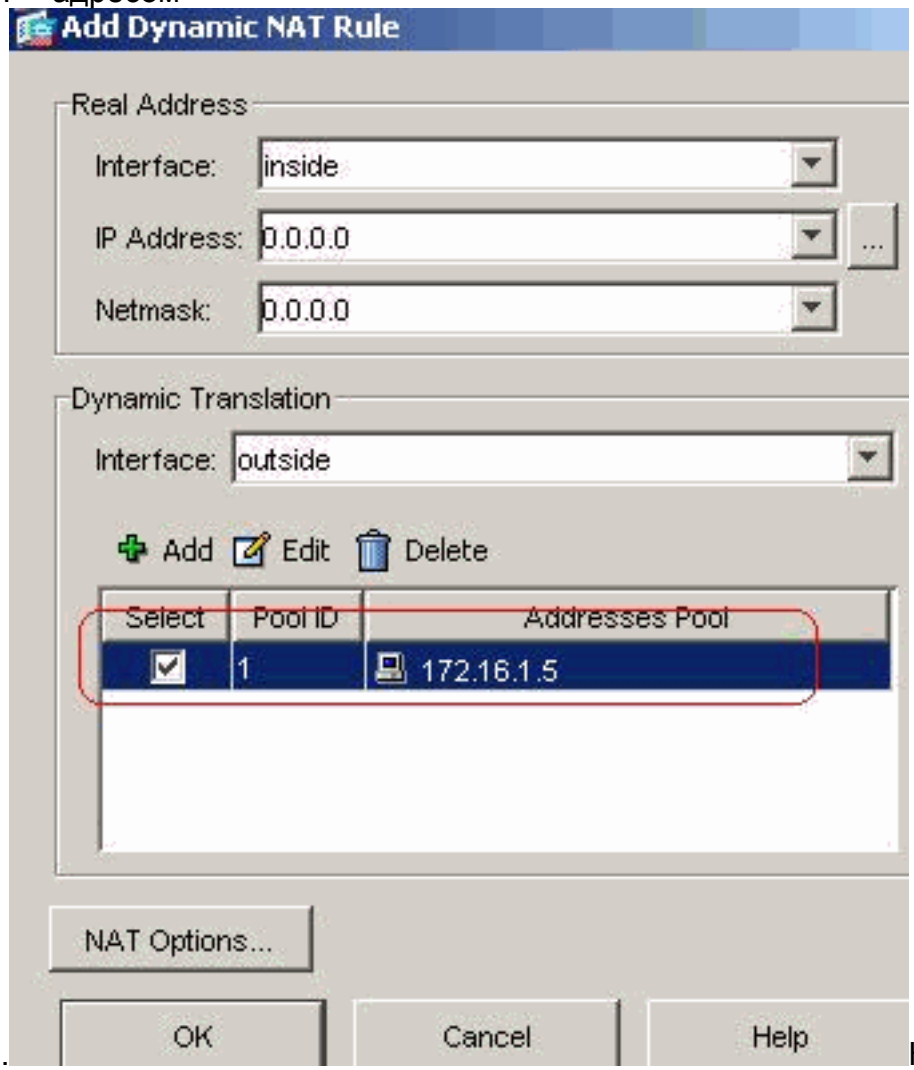


Во вкладке **WebVPN> Group Aliases и URL** введите имя псевдонима в коробке параметра и **нажмите Add>>**, чтобы заставить его появиться в списке имен групп в странице
входа.



Нажмите кнопку OK, а затем Apply.Эквивалентная конфигурация в интерфейсе командной строки:

8. **Настройка NAT**Выберите **Configuration> NAT> Add> Add Dynamic NAT Rule** для трафика, который прибывает из внутренней сети, которая может быть преобразована с внешним IP - адресом



172.16.1.5. Нажмите **OK** и нажмите **Apply** в главной странице.**Эквивалентная конфигурация в интерфейсе командной строки:**

9. Настройте туземное освобождение для ответного трафика из сети клиенту VPN.`ciscoasa(config)#`**`access-list nonat permit ip 10.77.241.0 192.168.10.0`** `ciscoasa(config)#`**`access-list nonat permit ip 192.168.10.0 10.77.241.0`** `ciscoasa(config)#`**`nat (inside) 0 access-list nonat`**

ASA 7.2 (2) конфигурация Использование CLI

Cisco ASA 7.2 (2)
`ciscoasa#`**`show running-config`** `: Saved : ASA Version 7.2(2) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside security-level 100 ip address 10.77.241.142 255.255.255.192 ! interface Ethernet0/1 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0 ! interface Ethernet0/2 shutdown no nameif no security-level no ip address ! interface Ethernet0/3 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 access-list split-tunnel standard permit 10.77.241.128 255.255.255.192` *`!--- ACL for Split`*

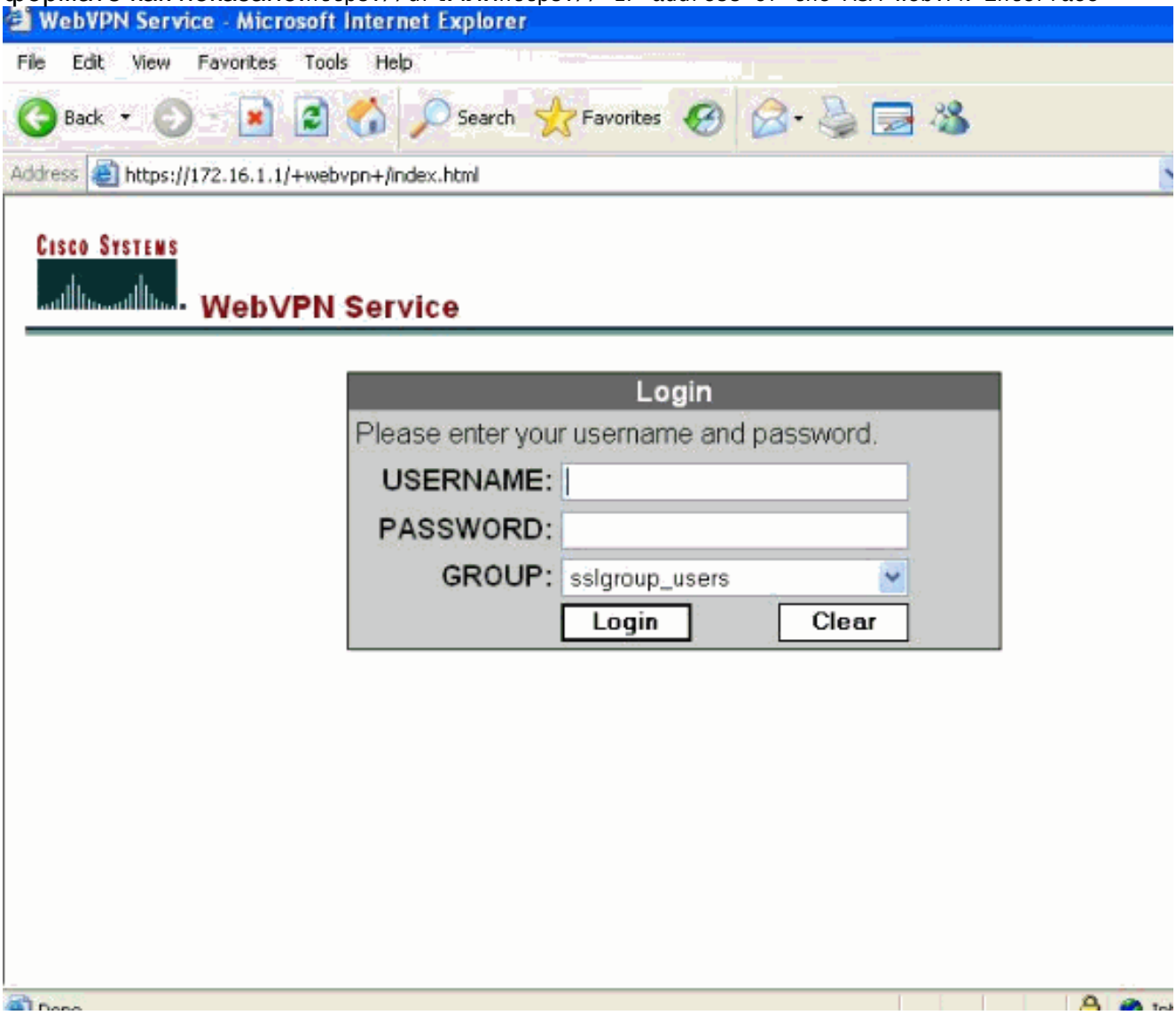
```
Tunnel network list for encryption. access-list nonat
permit ip 10.77.241.0 192.168.10.0 access-list nonat
permit ip 192.168.10.0 10.77.241.0 !--- ACL to define
the traffic to be exempted from NAT. pager lines 24 mtu
inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 !--- The address pool for
the SSL VPN Clients no failover icmp unreachable rate-
limit 1 burst-size 1 asdm image disk0:/asdm-522.bin no
asdm history enable arp timeout 14400 global (outside) 1
172.16.1.5 !--- The global address for Internet access
used by VPN Clients. !--- Note: Uses an RFC 1918 range
for lab setup. !--- Apply an address from your public
range provided by your ISP. nat (inside) 0 access-list
nonat !--- The traffic permitted in "nonat" ACL is
exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0
access-group 100 in interface outside route outside
0.0.0.0 0.0.0.0 172.16.1.2 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 mgcp-pat 0:05:0 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02: timeout uauth 0:05:00 absolute group-policy
clientgroup internal !--- Create an internal group
policy "clientgroup". group-policy clientgroup
attributes vpn-tunnel-protocol webvpn !--- Enable webvpn
as tunneling protocol. split-tunnel-policy
tunnelspecified split-tunnel-network-list value split-
tunnel !--- Encrypt the traffic specified in the split
tunnel ACL only. webvpn svc required !--- Activate the
SVC under webvpn mode. svc keep-installer installed !---
When the security appliance and the SVC perform a rekey,
!--- they renegotiate the crypto keys and initialization
vectors, !--- and increase the security of the
connection. svc rekey time 30 !--- Command that
specifies the number of minutes !--- from the start of
the session until the rekey takes place, !--- from 1 to
10080 (1 week). svc rekey method ssl !--- Command that
specifies that SSL renegotiation !--- takes place during
SVC rekey. username ssluser1 password ZRhW85jZqEaVd5P.
encrypted !--- Create an user account "ssluser1". aaa
local authentication attempts max-fail 16 !--- Enable
the AAA local authentication. http server enable http
0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart tunnel-group
sslgroup type webvpn !--- Create a tunnel group
"sslgroup" with type as WebVPN. tunnel-group sslgroup
general-attributes address-pool vpnpool !--- Associate
the address pool vpnpool created. default-group-policy
clientgroup !--- Associate the group policy
"clientgroup" created. tunnel-group sslgroup webvpn-
attributes group-alias sslgroup_users enable !---
Configure the group alias as sslgroup-users. 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 WebVPN on the outside
interface. svc image disk0:/sslclient-win-1.1.4.179.pkg
```

```
1 !--- Assign an order to the SVC image. svc enable !---
Enable the security appliance to download !--- SVC
images to remote computers. tunnel-group-list enable !--
- Enable the display of the tunnel-group list !--- on
the WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

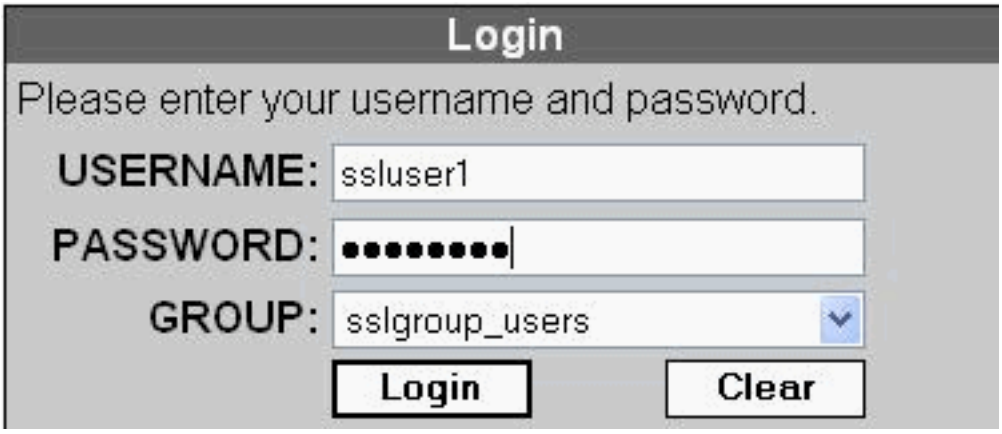
Установление соединение SSL VPN с SVC

Выполните эти шаги, чтобы установить VPN-подключение к ASA по протоколу SSL.

1. Введите URL или IP-адрес интерфейса WebVPN ASA в вашем web-браузере в формате как показано.`https://url`Или`https://<IP address of the ASA WebVPN interface>`



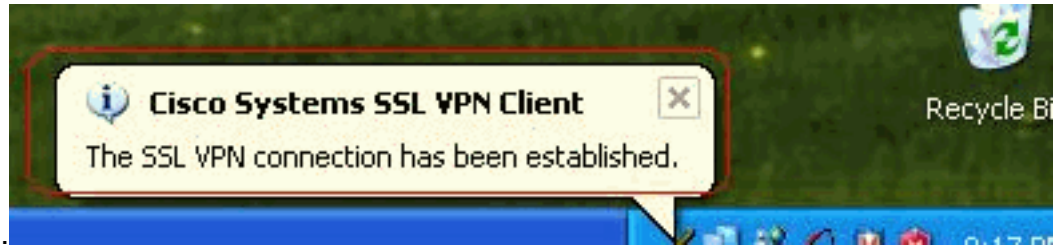
2. Введите свое имя пользователя и пароль и затем выберите свою соответствующую группу из выпадающего списка как

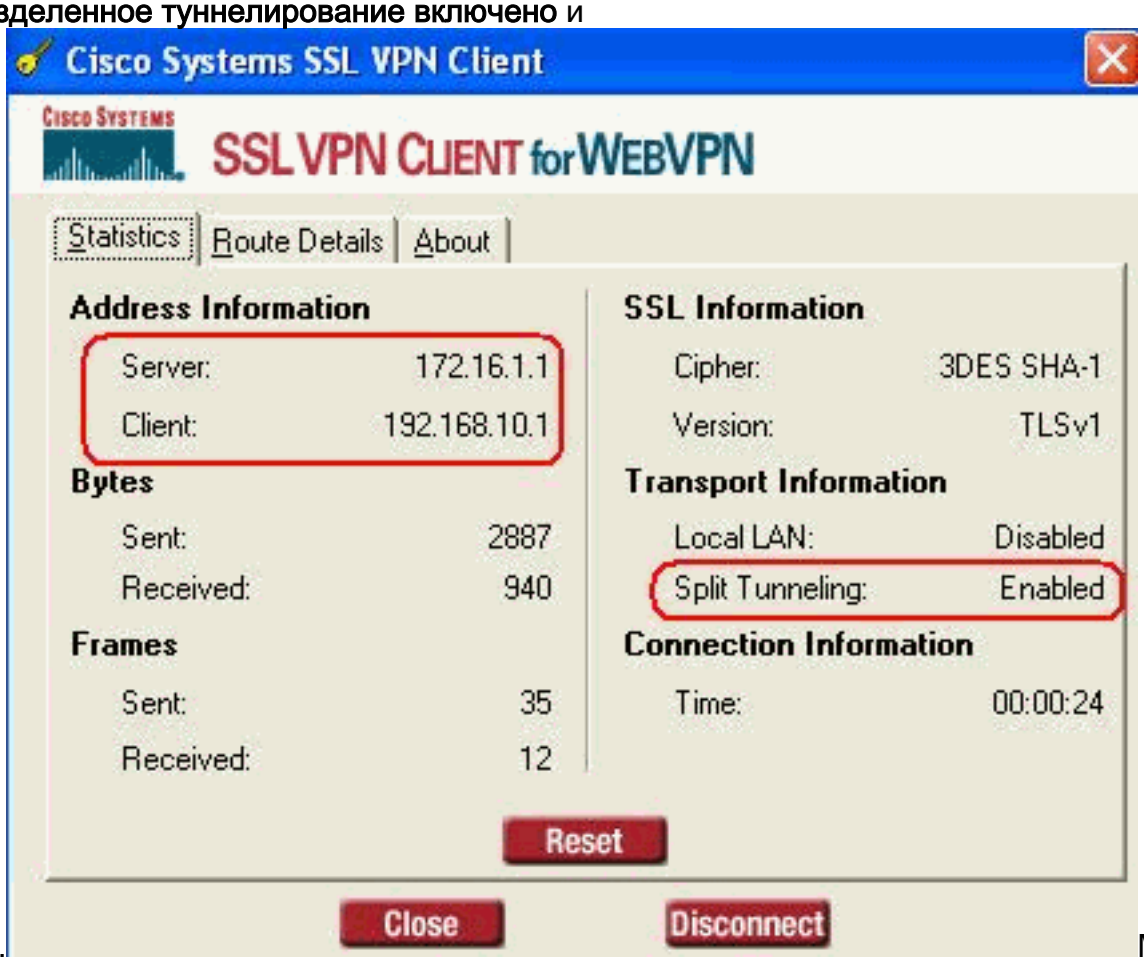
показано. 

3. Программное обеспечение ActiveX должно быть установлено в вашем компьютере перед загрузкой SVC. 

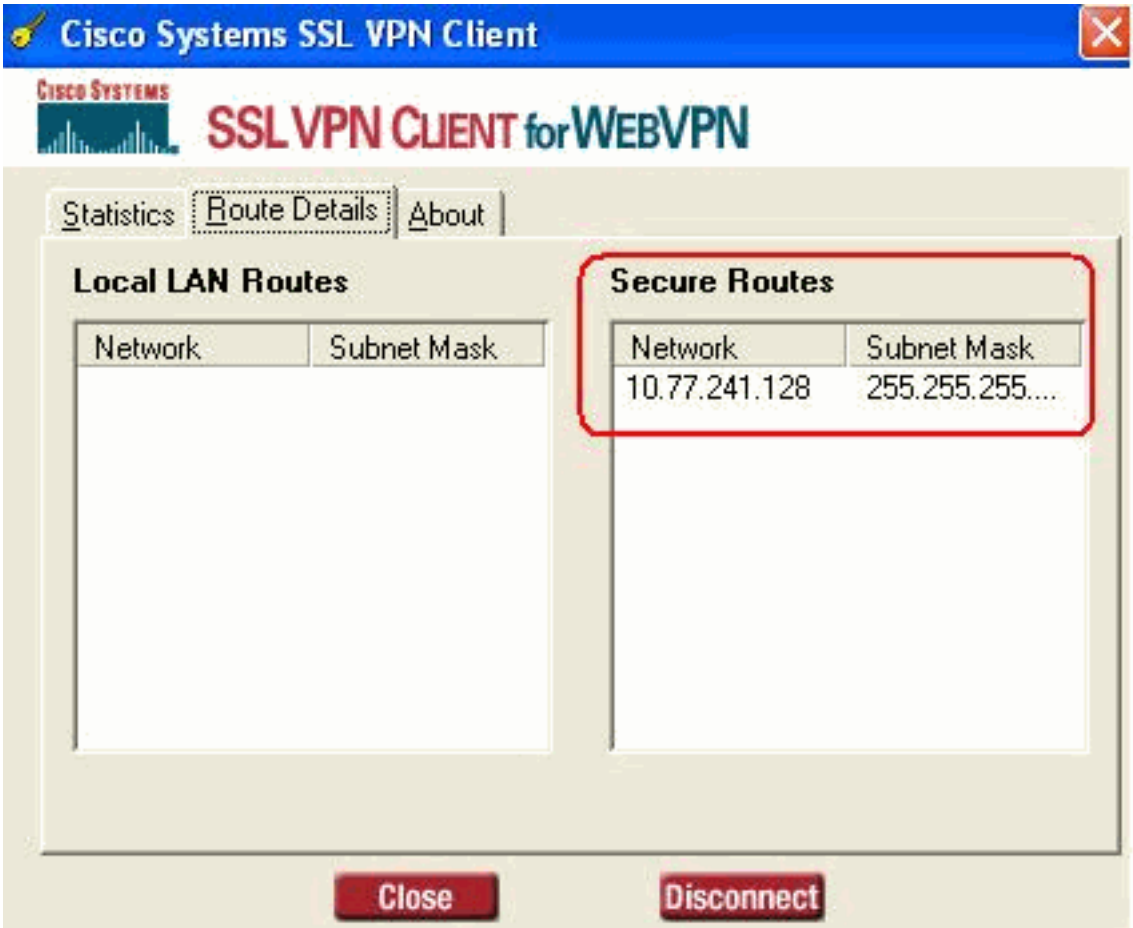
4. Эти окна появляются, прежде чем VPN-подключение на базе SSL установлено. 

5. Можно получить эти окна, как только установлено

соединение. 

6. Нажмите желтый ключ, который появляется в панели задач вашего компьютера. Эти окна появляются, который дает информацию о подключении SSL. Например, **192.168.10.1** назначенный IP - адрес для IP-адреса клиента и сервера, 172.16.1.1, **Разделенное туннелирование включено** и 

т.д. Можно также проверить защищенную сеть, которая должна быть зашифрована SSL, список сети загружен от списка доступа разделения туннеля, настроенного в ASA.В то время как весь другой трафик не зашифрован и не передан через туннель, в данном примере VPN-клиент SSL (SVC) защищает доступ к 10.77.241.128/24.

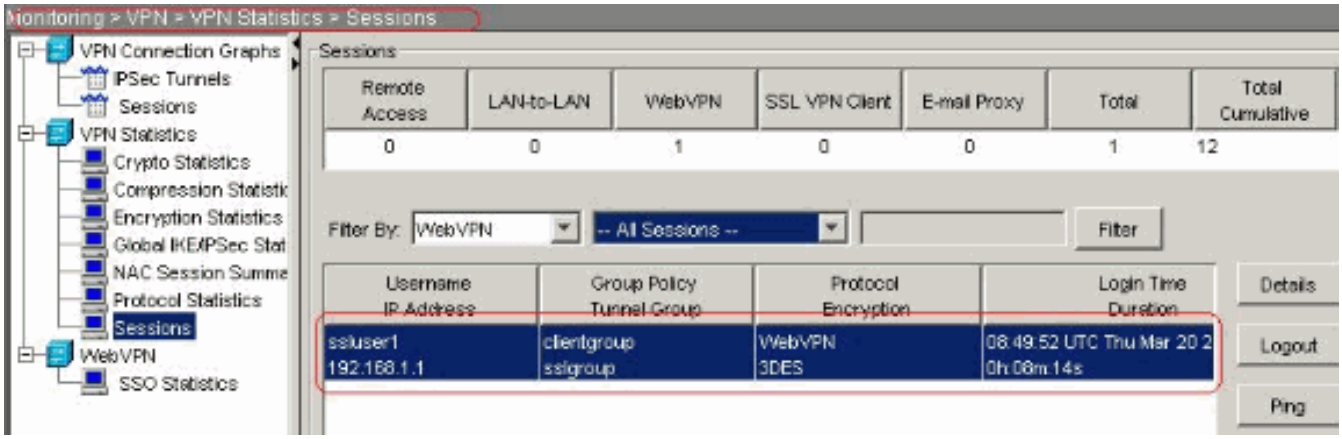


Проверка

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.

- show webvpn svc — отображает образы SVC, записанные во флэш-памяти ASA.`ciscoasa#show webvpn svc 1. disk0:/sslclient-win-1.1.4.179.pkg 1 CISCO STC win2k+ 1.0.0 1,1,4,179 Fri 01/18/2008 15:19:49.43 1 SSL VPN Client(s) installed`
- show vpn-sessiondb svc — отображает информацию о текущих SSL-подключениях.`ciscoasa#show vpn-sessiondb svc Session Type: SVC Username : ssluser1 Index : 1 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 Protocol : SVC Encryption : 3DES Hashing : SHA1 Bytes Tx : 131813 Bytes Rx : 5082 Client Type : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Client Ver : Cisco Systems SSL VPN Client 1, 1, 4, 179 Group Policy : clientgroup Tunnel Group : sslgroup Login Time : 12:38:47 UTC Mon Mar 17 2008 Duration : 0h:00m:53s Filter Name :`
- show webvpn group-alias — отображает псевдонимы, назначенные разным группам.`ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup_users enabled`
- В ASDM выберите Monitoring> VPN> VPN Statistics> Sessions для знания о текущих сеансах WebVPN в ASA.



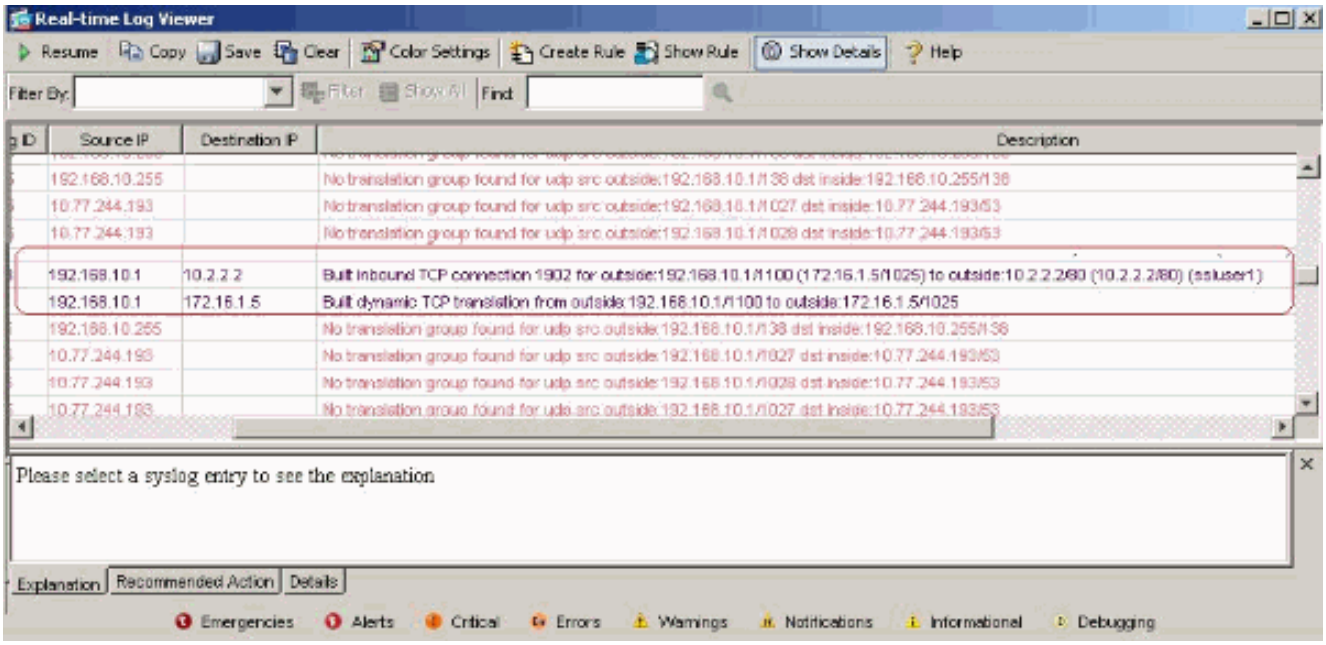
Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

1. команда vpn-sessiondb logoff name<username> используется для прекращения сеанса SSL VPN для определенного пользователя.`ciscoasa#vpn-sessiondb logoff name ssluser1 Called vpn_remove_uauIth: success! webvpn_svc_np_tear_down: no ACL NFO: Number of sessions with name "ssluser1" logged off : 1` Также можно использовать команду vpn-sessiondb logoff svc, чтобы прекратить все SVC-сеансы.
2. Примечание: Если ПК переходит к резерву, или будьте в спящем режиме режим, то VPN-подключение на базе SSL может быть завершено.
   `webvpn_rx_data_cstp webvpn_rx_data_cstp: got message SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc) Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL ciscoasa#show vpn-sessiondb svc INFO: There are presently no active sessions`
3. Команда debug webvpn svc <1-255> предоставляет все события webvpn в реальном времени для установления сеанса.`Ciscoasa#debug webvpn svc 7 ATTR_CISCO_AV_PAIR: got SVC ACL: -1 webvpn_rx_data_tunnel_connect CSTP state = HEADER_PROCESSING http_parse_cstp_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn_cstp_parse_request_field() ...input: 'Host: 172.16.1.1' Processing CSTP header line: 'Host: 172.16.1.1' webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco Systems`

```
SSL VPN Client 1, 1, 4, 179' Processing CSTP header line: 'User-Agent: Cisco Systems SSL
VPN Client 1, 1, 4, 179' Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header
line: 'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb' Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Accept-
Encoding: deflate;q=1.0' Processing CSTP header line: 'X-CSTP-Accept-Encoding:
deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'Cookie:
webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486 D5BC554D2' Processing CSTP
header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2' Found WebVPN cookie:
'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1 486D5BC554D2' WebVPN Cookie:
'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B C554D2' Validating
address: 0.0.0.0 CSTP state = WAIT_FOR_ADDRESS webvpn_cstp_accept_address:
192.168.10.1/0.0.0.0 CSTP state = HAVE_ADDRESS No subnetmask... must calculate it SVC: NP
setup webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth
success! SVC: adding to sessmgmt SVC: Sending response CSTP state = CONNECTED
```

4. **В ASDM последовательно выберите Monitoring > Logging > Real-time Log Viewer > View, чтобы увидеть все события в реальном времени.** Они пример показывают об информации о сеанса между SVC 192.168.10.1 и веб-сервером 10.2.2.2 в Интернете через ASA
172.16.1.5.



Дополнительные сведения

- Поддержка продуктов устройства адаптивной безопасности серии 5500 Cisco
- ASA/PIX: Пример конфигурации устройства ASA, разрешающей раздельное туннелирование для VPN-клиентов
- Пример конфигурации маршрутизатора, разрешающего VPN-клиентам подключаться к узлам по протоколу IPsec и к сети Интернет, с использованием раздельного туннелирования
- Пример настройки PIX/ASA 7.x и VPN-клиента для сети VPN, организованной в общедоступной части Интернета и имеющей один внешний интерфейс
- Пример настройки SSL клиента VPN (SVC) на ASA с ASDM
- Cisco Systems – техническая поддержка и документация