ASA 7.1/7.2: Allow Split Tunneling for SVC on the ASA Configuration Example

Contents

Introduction

This document provides step-by-step instructions on how to allow Secure Socket Layer (SSL) VPN Clients (SVC) access to the Internet while they are tunneled into a Cisco Adaptive Security Appliance (ASA). This configuration allows SVC secure access to corporate resources through SSL and gives unsecured access to the Internet with the use of split tunneling.

The ability to transmit both secured and unsecured traffic on the same interface is known as split tunneling. Split tunneling requires that you specify exactly which traffic is secured and what the destination of that traffic is, so that only the specified traffic enters the tunnel, while the rest is transmitted unencrypted across the public network (Internet).

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Local administrative privileges on all remote workstations
- Java and ActiveX controls on the remote workstation
- Port 443(SSL) is not blocked anywhere along the connection path

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series Adaptive Security Appliance (ASA) that runs software version 7.2(2)
- Cisco SSL VPN Client version for Windows 1.1.4.179**Note:** Download the SSL VPN Client package (sslclient-win*.pkg) from the Cisco Software Download (registered customers only) . Copy the SVC to the flash memory of the ASA, which is to be downloaded to the remote user computers in order to establish the SSL VPN connection with ASA. Refer to Installing the SVC Software section of ASA configuration guide for more information.
- PC that runs Windows 2000 professional SP4 or Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM) version 5.2(2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The SSL VPN Client (SVC) is a VPN tunneling technology that gives remote users the benefits of an IPsec VPN client without the need for network administrators to install and configure IPsec VPN clients on remote computers. The SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the security appliance.

In order to establish an SVC session, the remote user enters the IP address of a WebVPN interface of the security appliance in the browser, and the browser connects to that interface and displays the WebVPN login screen. If you satisfy the login and authentication, and the security appliance identifies you as requiring the SVC, the security appliance downloads the SVC to the remote computer. If the security appliance identifies you with the option to use the SVC, the security appliance downloads the SVC to the remote computer while it presents a link on the window to skip the SVC installation.

After you download, the SVC installs and configures itself, and then the SVC either remains or uninstalls itself, which depends on the configuration, from the remote computer when the connection terminates.

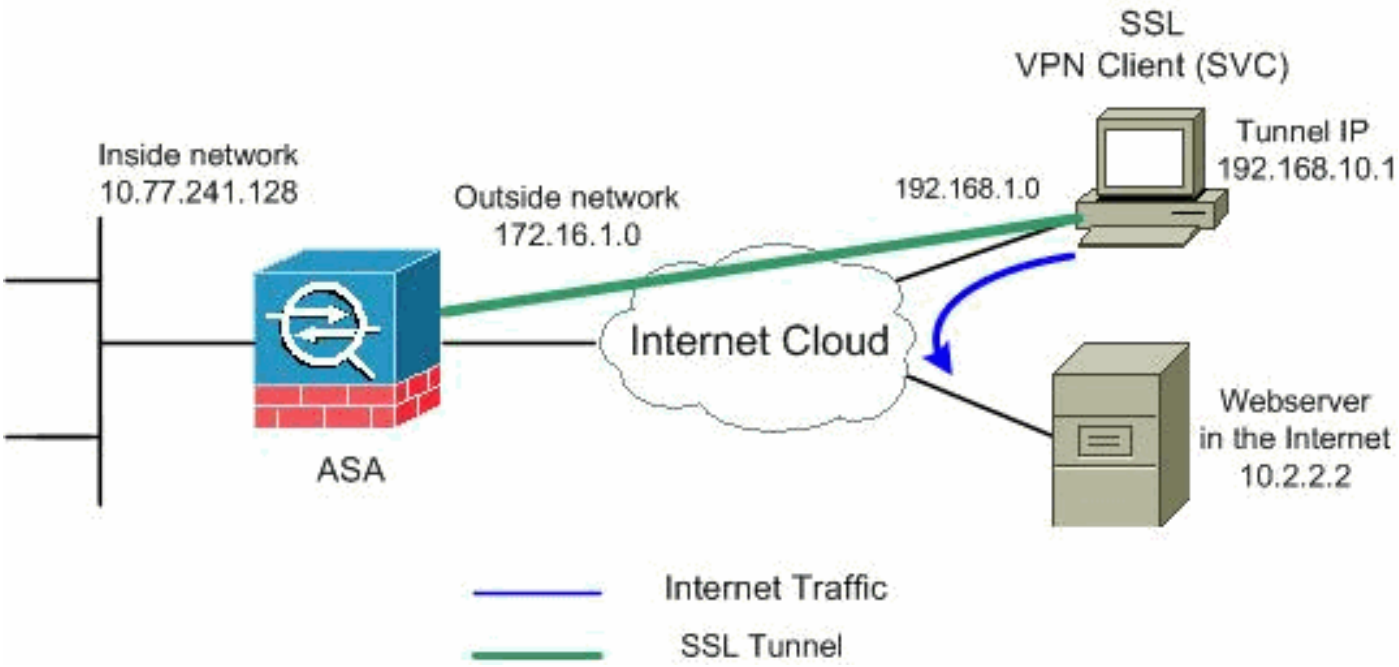
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

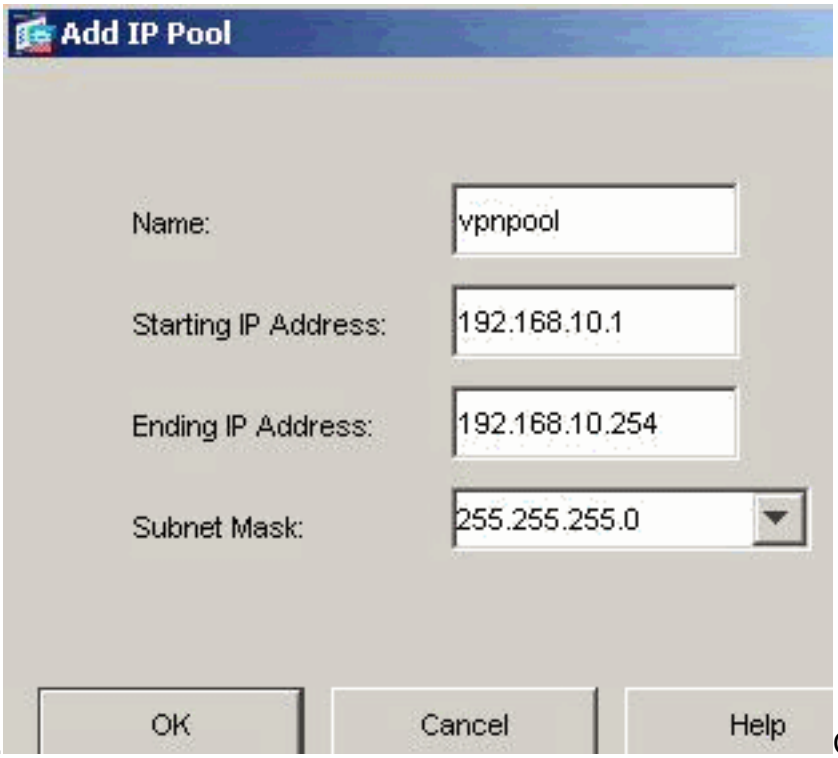


Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses that have been used in a lab environment.

ASA Configurations Using ASDM 5.2(2)

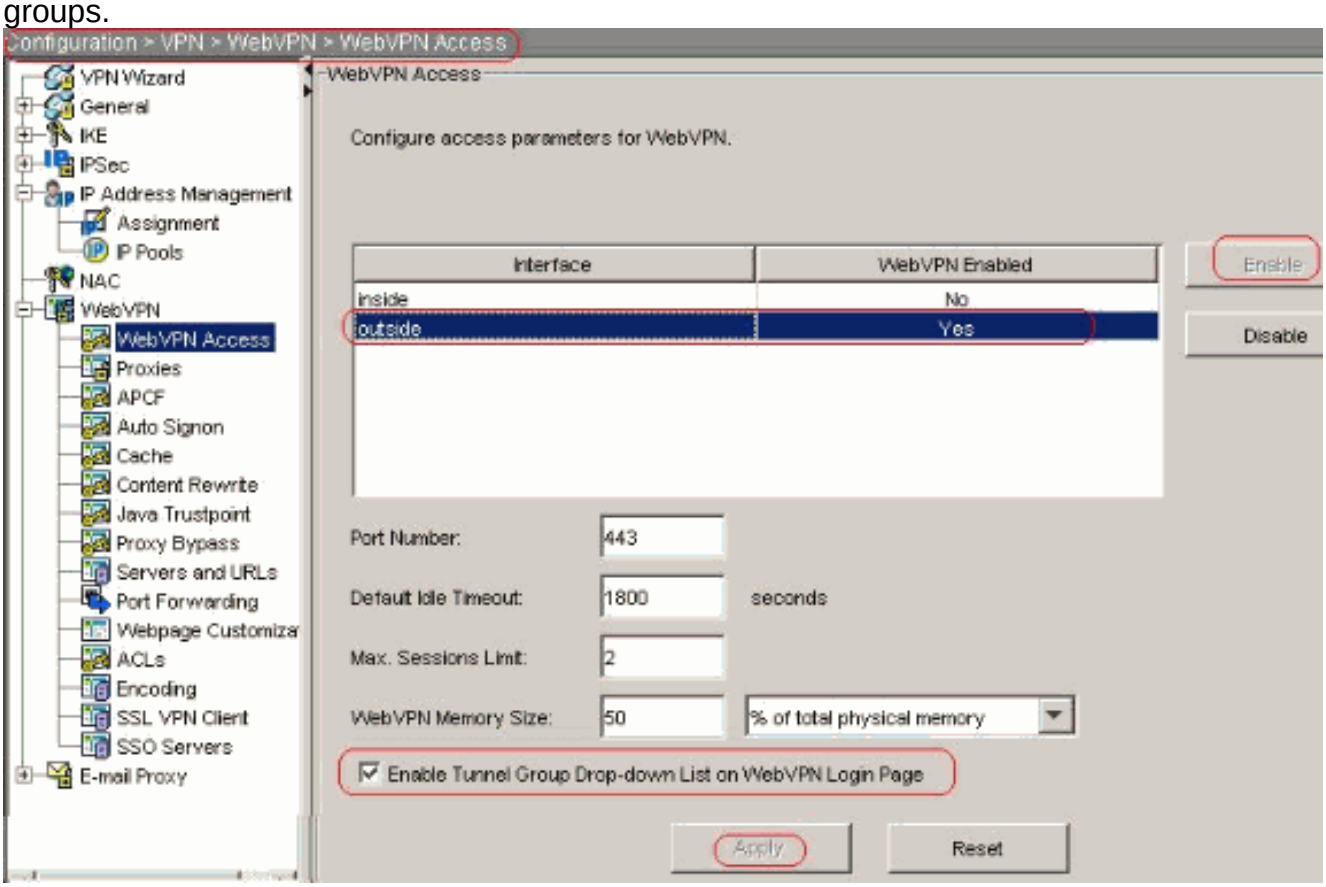
Complete these steps in order to configure the SSL VPN on ASA with Split Tunneling as shown:

1. The document assumes the basic configuration such as interface configuration and so forth are already made and work properly.**Note:** Refer to Allowing HTTPS Access for ASDM in order to allow the ASA to be configured by the ASDM.**Note:** WebVPN and ASDM cannot be enabled on the same ASA interface unless you change the port numbers. Refer to ASDM and WebVPN Enabled on the Same Interface of ASA for more information.
2. Choose **Configuration > VPN > IP Address Management > IP Pools** in order to create an IP address pool: **vpnpool** for VPN

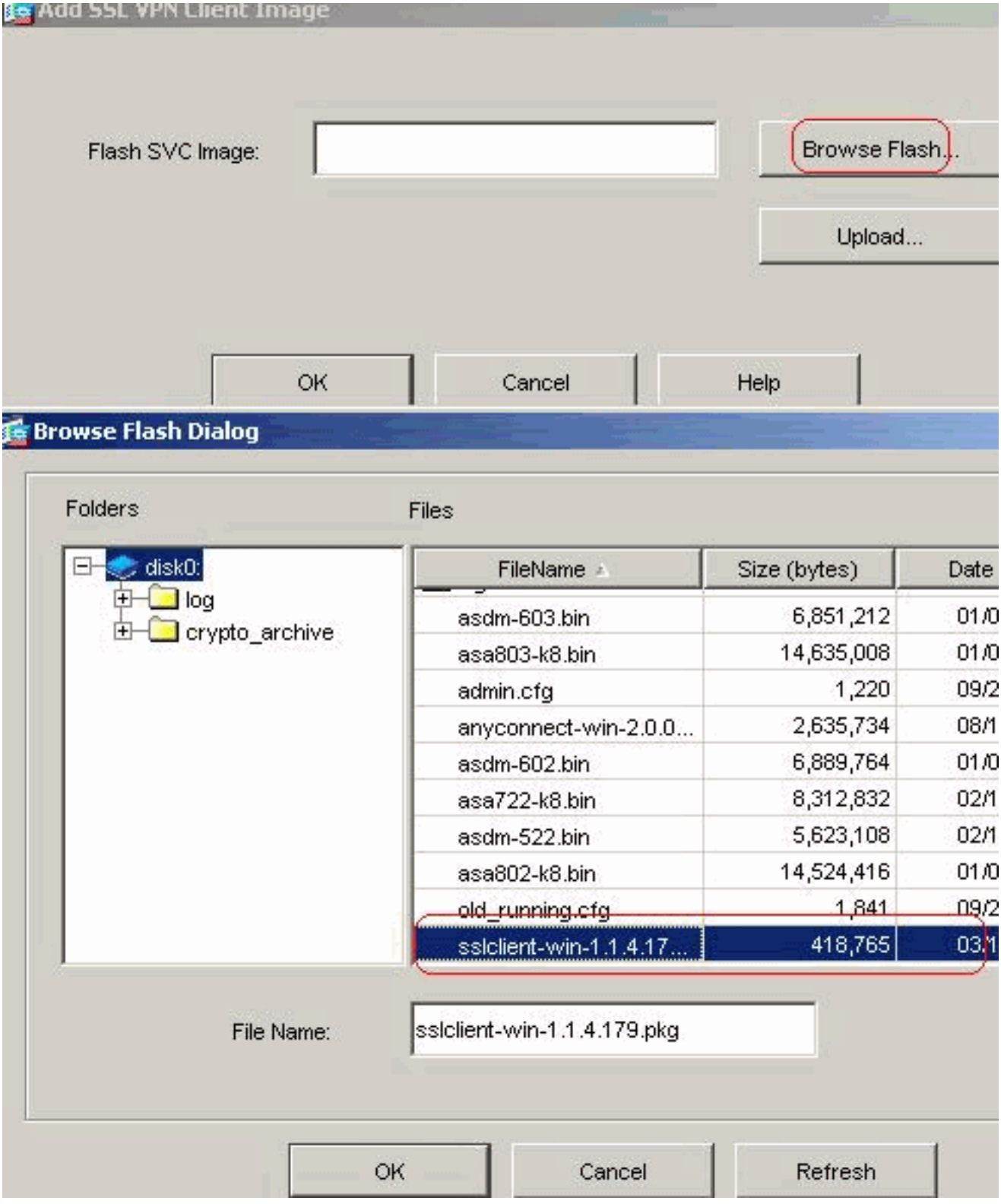


clients. Click **Apply**.

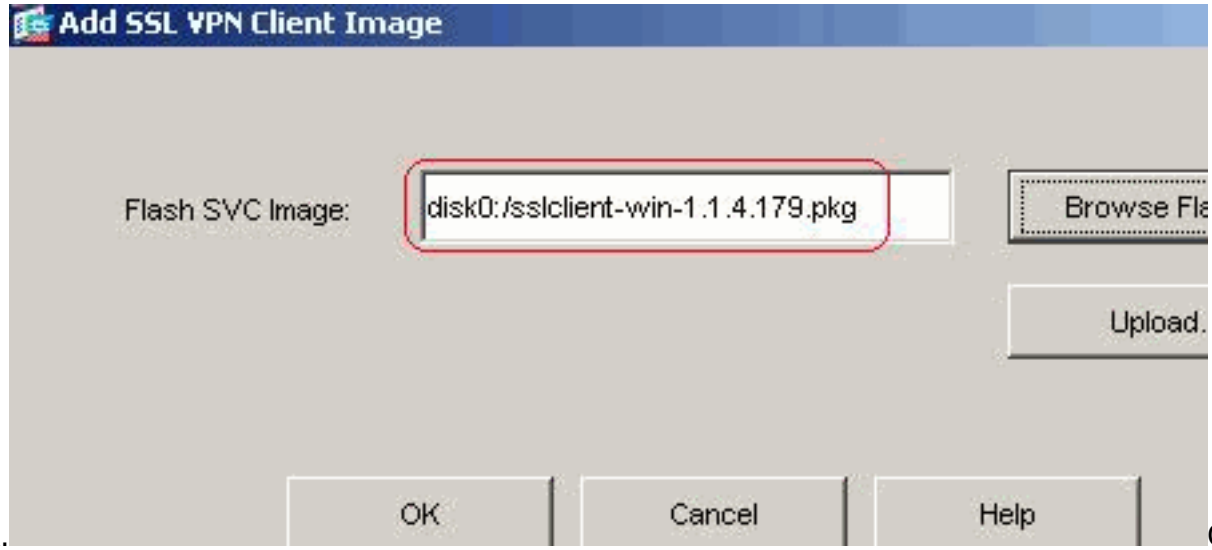
3. **Enable WebVPN**Choose **Configuration > VPN > WebVPN > WebVPN Access** and highlight the outside interface with mouse and click **Enable**. Check **Enable Tunnel Group Drop-down List on WebVPN Login Page** check box in order to enable the drop down appear in the login page for users, to choose their respective groups.



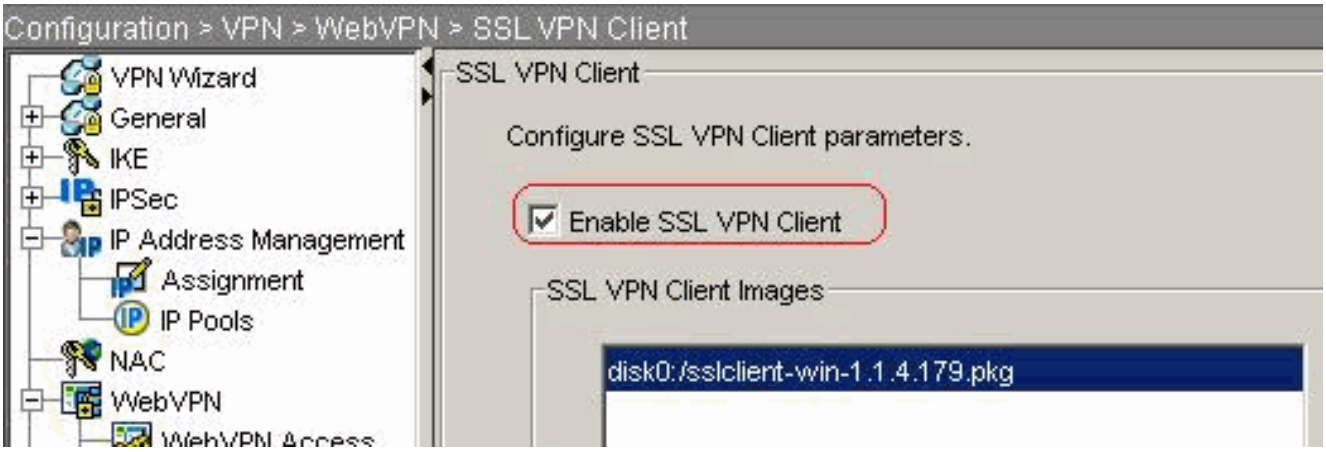
Click **Apply**.Choose **Configuration > VPN > WebVPN > SSL VPN Client > Add** in order to add the SSL VPN client image from the flash memory of ASA as shown.


Add SSL VPN Client Image
Flash SVC Image:
Browse Flash...
Upload...
OK
Cancel
Help
Browse Flash Dialog
Folders
Files
disk0:
log
crypto_archive
FileName
Size (bytes)
Date
asdm-603.bin
6,851,212
01/0
asa803-k8.bin
14,635,008
01/0
admin.cfg
1,220
09/2
anyconnect-win-2.0.0...
2,635,734
08/1
asdm-602.bin
6,889,764
01/0
asa722-k8.bin
8,312,832
02/1
asdm-522.bin
5,623,108
02/1
asa802-k8.bin
14,524,416
01/0
old_running.cfg
1,841
09/2
sslclient-win-1.1.4.17...
418,765
03/1
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

Click

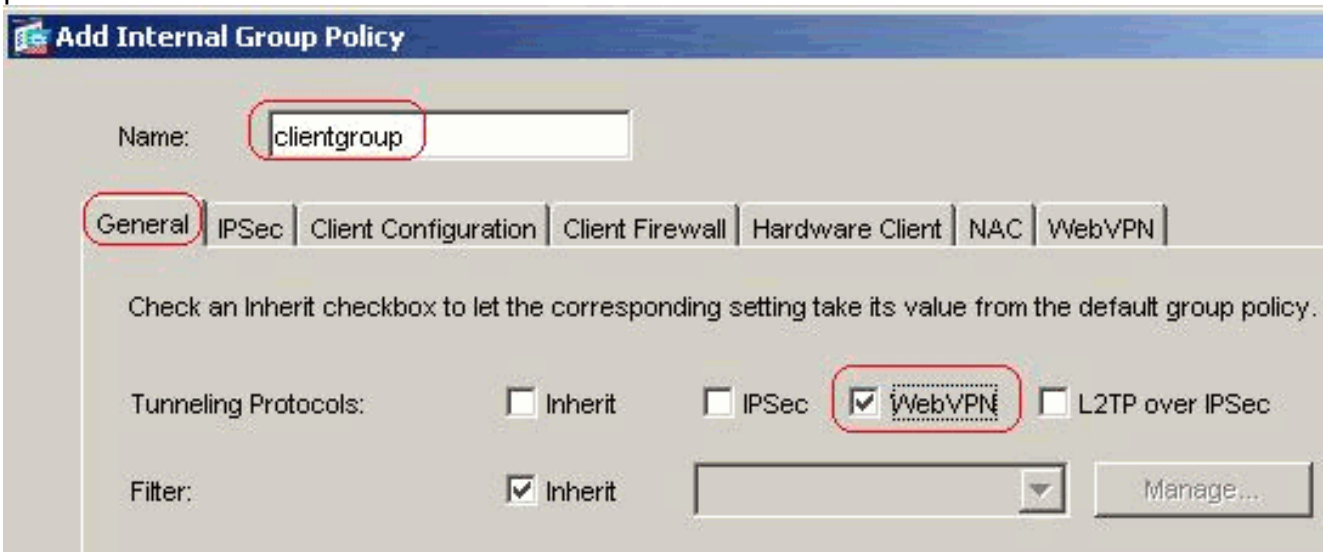


OK.Click **OK**.Click **SSL VPN Client** check box.



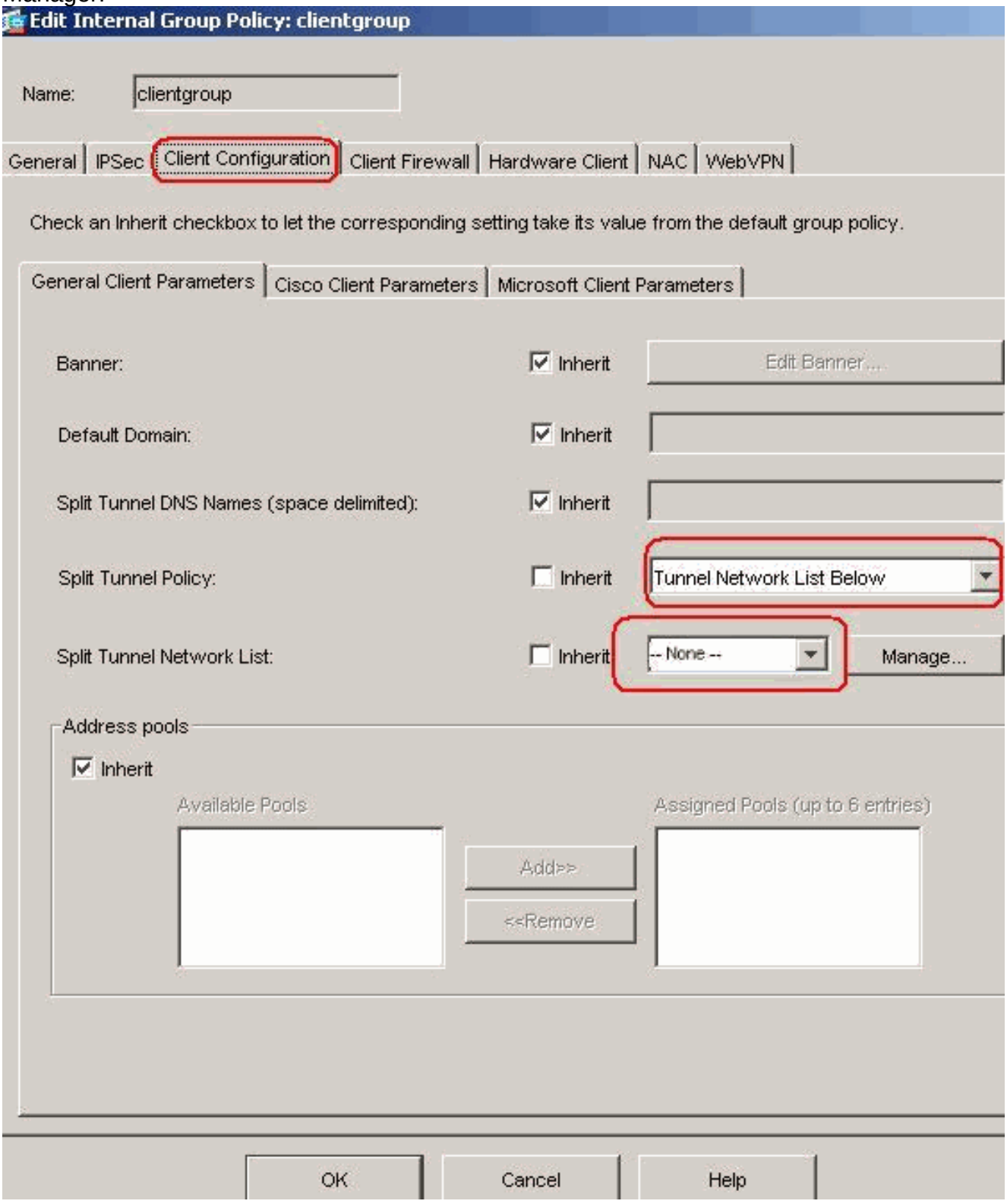
Click **Apply**.**Equivalent CLI Configuration:**

4. **Configure Group Policy**Choose **Configuration > VPN > General > Group Policy > Add (Internal Group Policy)** in order to create an internal group policy **clientgroup**. Under **General**, choose the **WebVPN** check box in order to enable the WebVPN as tunneling protocol.

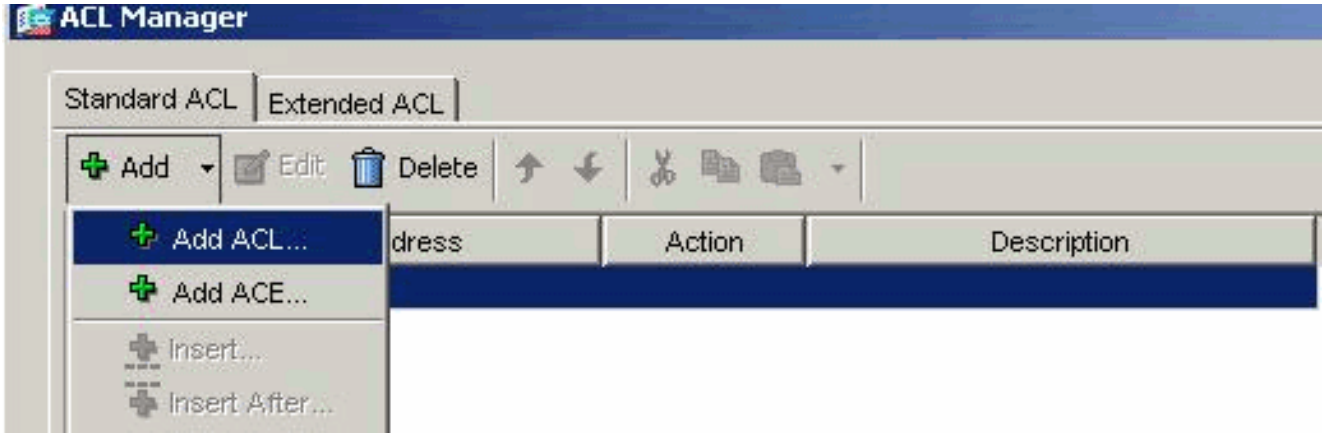


In the **Client Configuration > General Client Parameters** tab, uncheck the **Inherit** box for Split Tunnel Policy and choose **Tunnel Network List Below** from the drop-down list.Uncheck the **Inherit** box for **Split Tunnel Network List** and then click **Manage** in order to launch the ACL

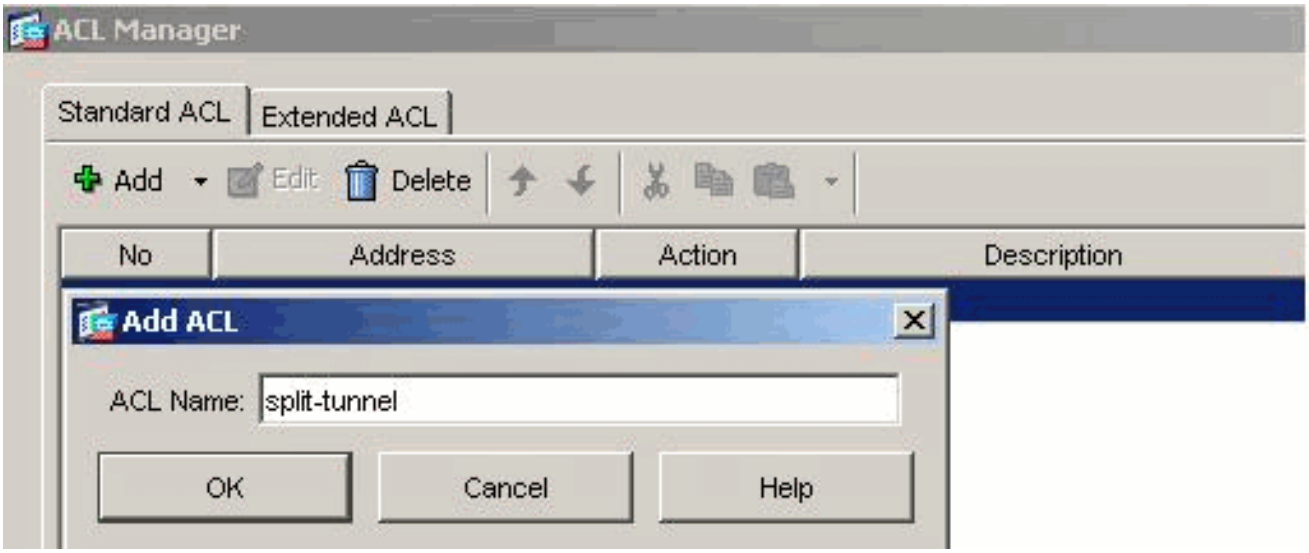
Manager.



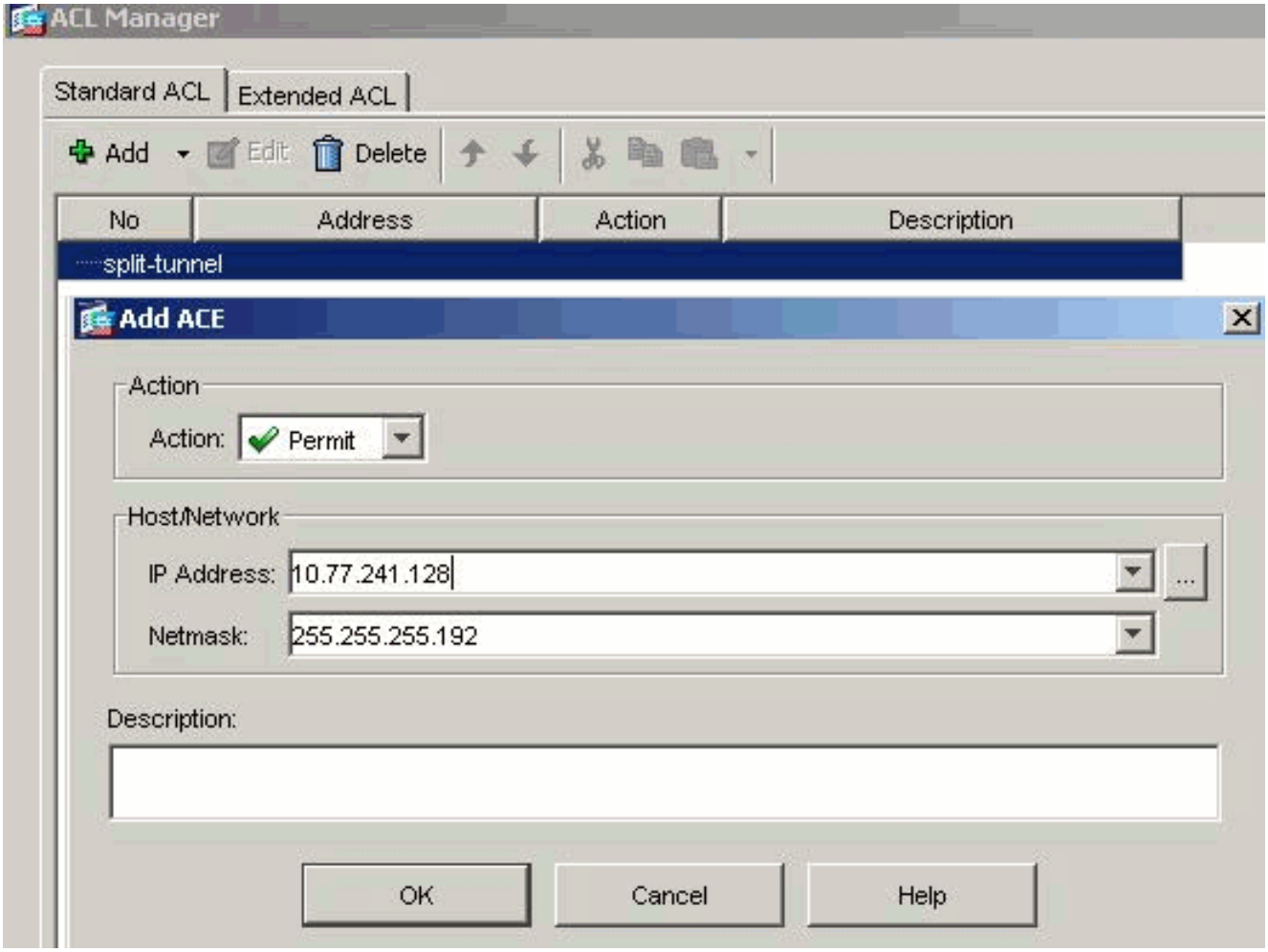
Within the ACL Manager, choose **Add > Add ACL...** in order to create a new access list.



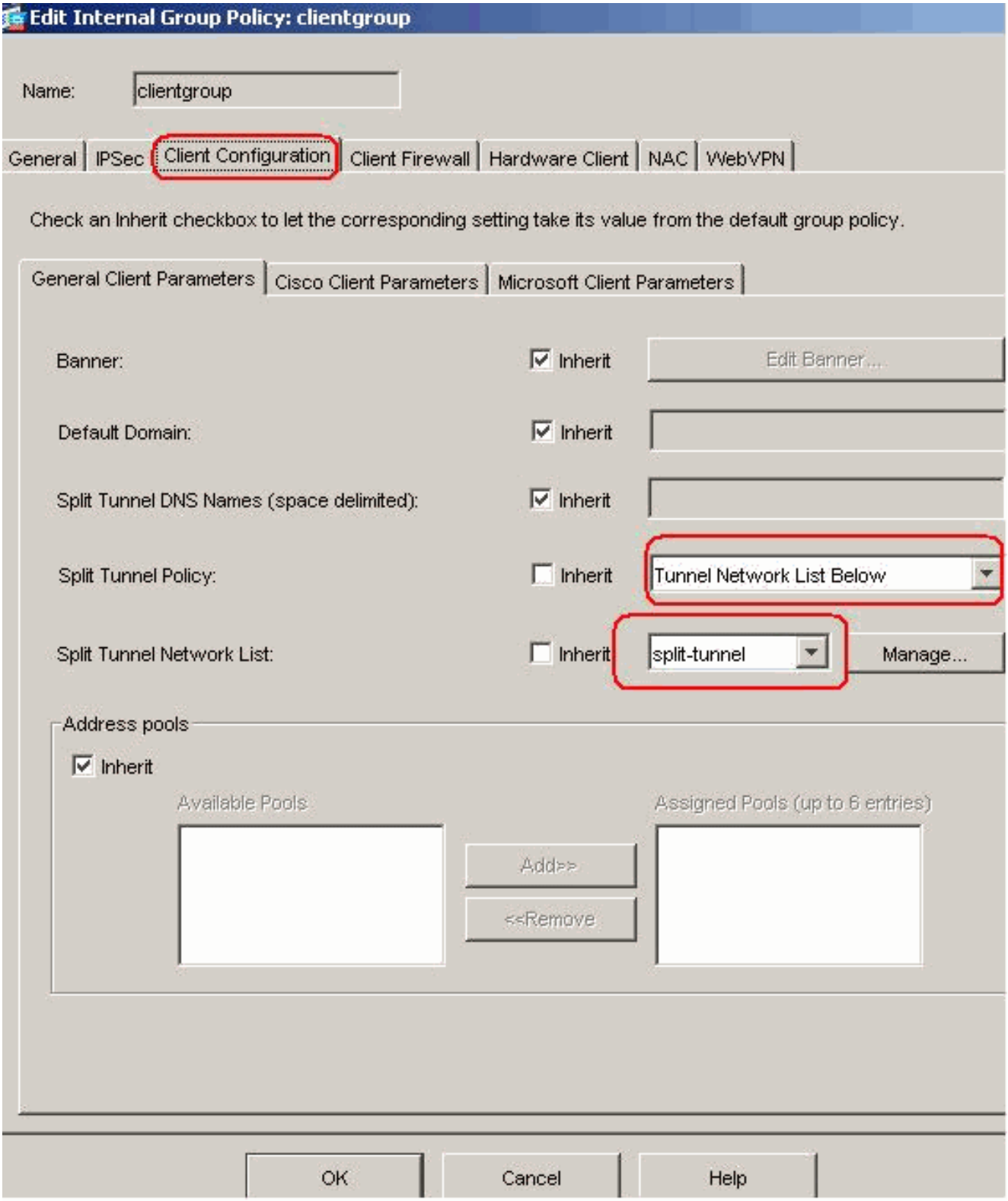
Provide a name for the ACL and click **OK**.



Once the ACL name is created, choose **Add > Add ACE** in order to add an Access Control Entry (ACE).Define the ACE that corresponds to the LAN behind the ASA. In this case, the network is 10.77.241.128/26 and choose **Permit**.Click **OK** in order to exit the ACL Manager.

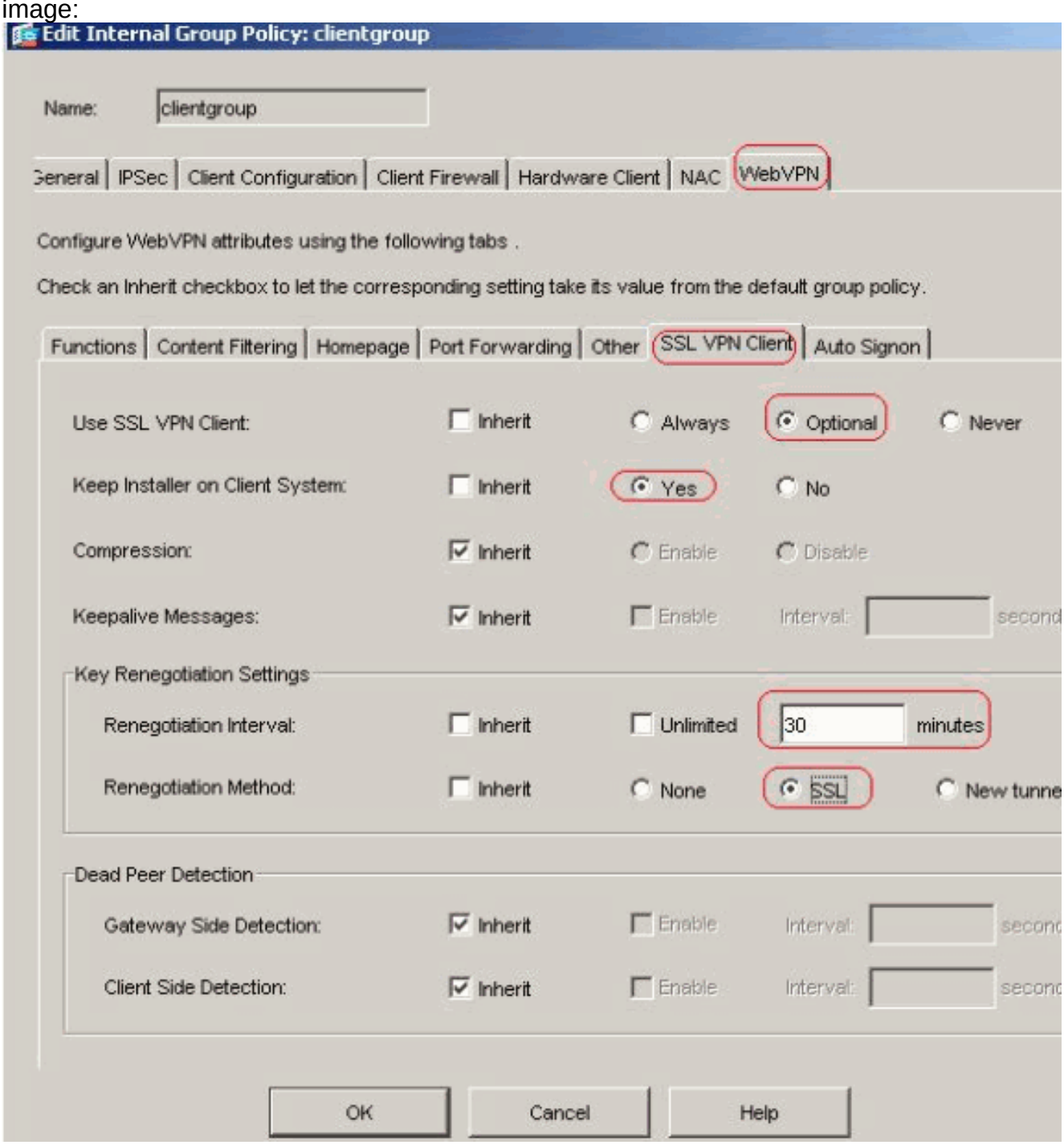


Be sure that the ACL you just created is selected for Split Tunnel Network List.Click **OK** in order to return to the Group Policy
configuration.

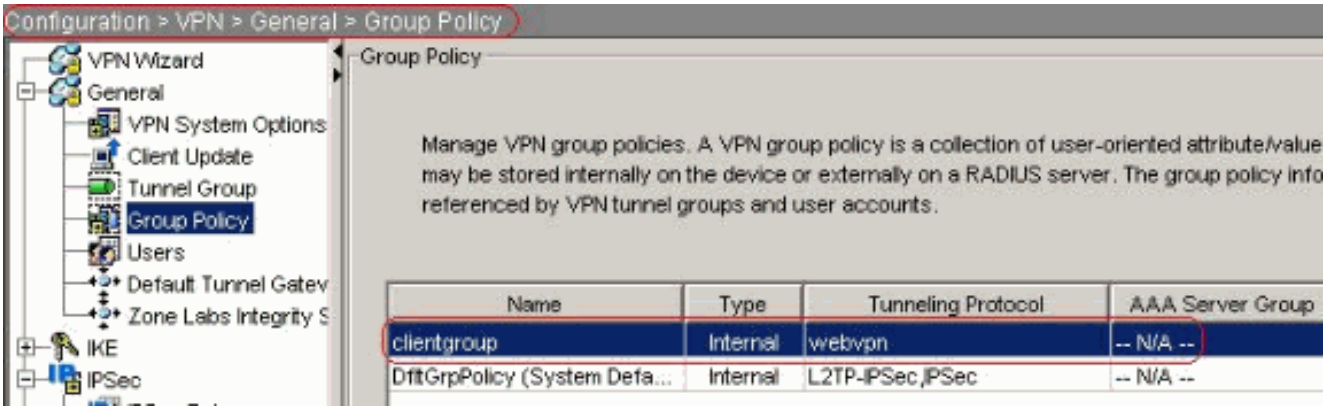


In the main page, click **Apply** and then **Send** (if required) in order to send the commands to the ASA.For the Use SSL VPN Client option, uncheck the **Inherit** check box and click the **Optional** radio button.This choice allows the remote client to choose whether to click the **WebVPN > SSLVPN Client** tab, and choose these options:Do not to download the SVC. The Always choice ensures that the SVC is downloaded to the remote workstation during each SSL VPN connection.For the Keep Installer on Client System option, uncheck the **Inherit** check box, and click the **Yes** radio button.This action allows the SVC software to remain on the client machine; therefore, the ASA is not required to download the SVC software to the client each time a connection is made. This option is a good choice for remote users who often access the corporate network.For the Renegotiation Interval option, uncheck the **Inherit** box, uncheck the **Unlimited** check box, and enter the number of minutes until

rekey.Security is enhanced when you set the limits on the length of time that a key is valid.For the Renegotiation Method option, uncheck the **Inherit** check box, and click the **SSL** radio button. Renegotiation can use the present SSL tunnel or a new tunnel created expressly for renegotiation.Your SSL VPN Client attributes should be configured as shown in this
image:

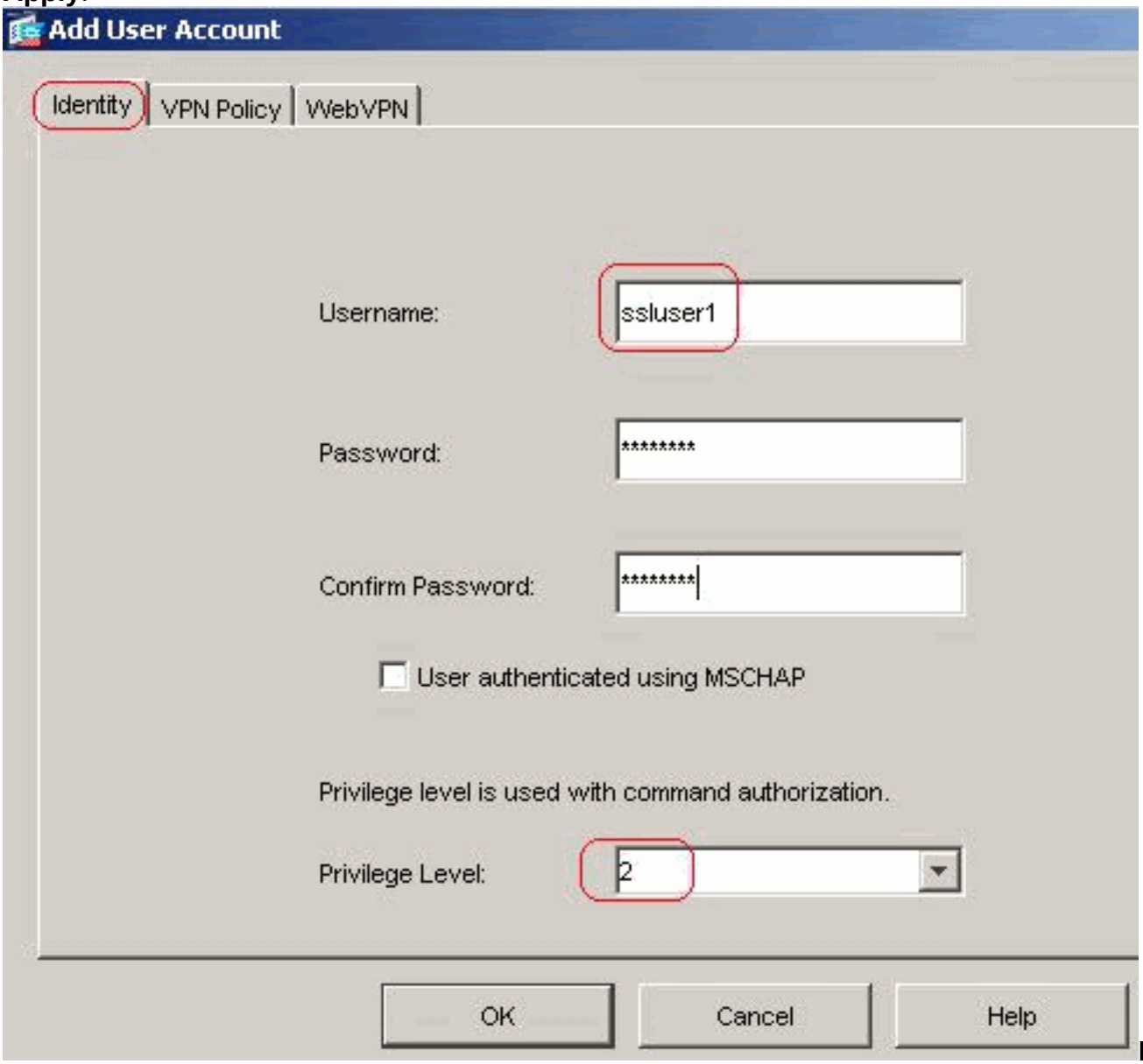


Click **OK** and then
Apply.



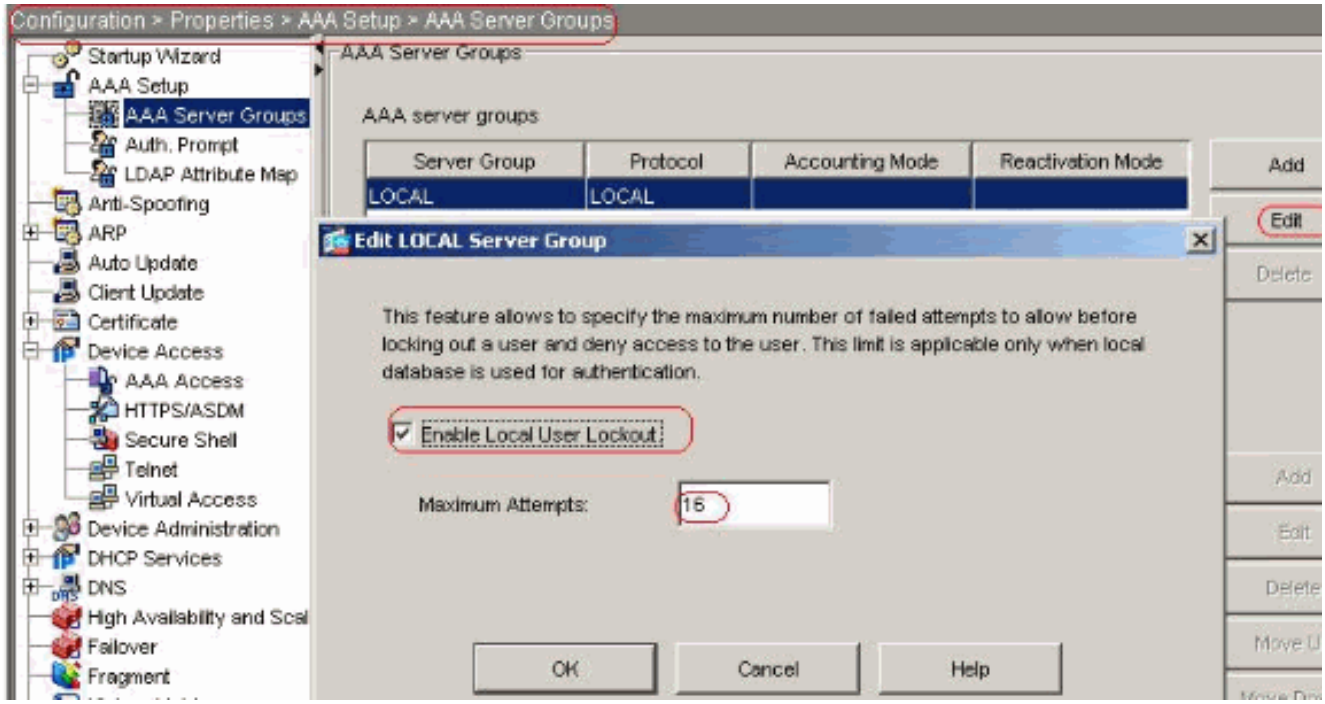
Equivalent CLI Configuration:

5. Choose **Configuration > VPN > General > Users > Add** in order to create a new user account **ssluser1**. Click **OK** and then **Apply**.



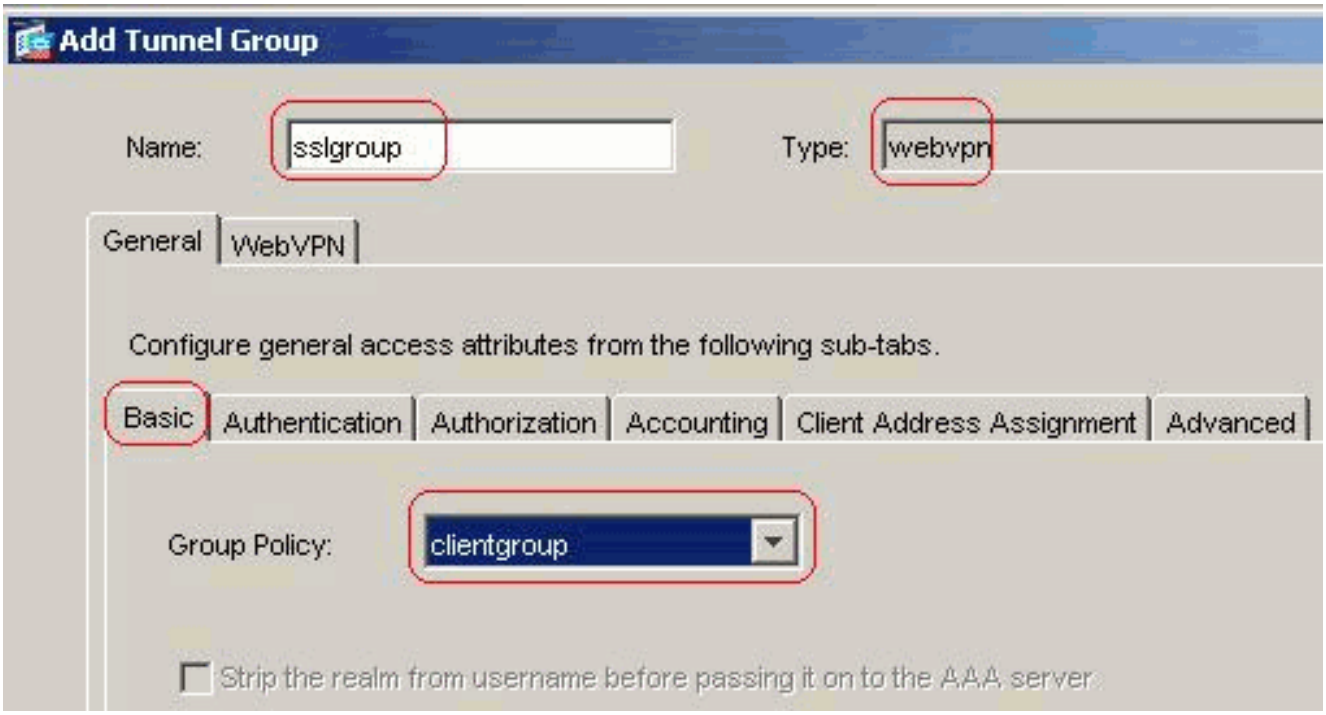
Equivalent CLI Configuration:

6. Choose **Configuration > Properties > AAA Setup > AAA Servers Groups > Edit** in order to modify the default server group **LOCAL** and choose the **Enable Local User Lockout** check box with maximum attempts value as **16**.

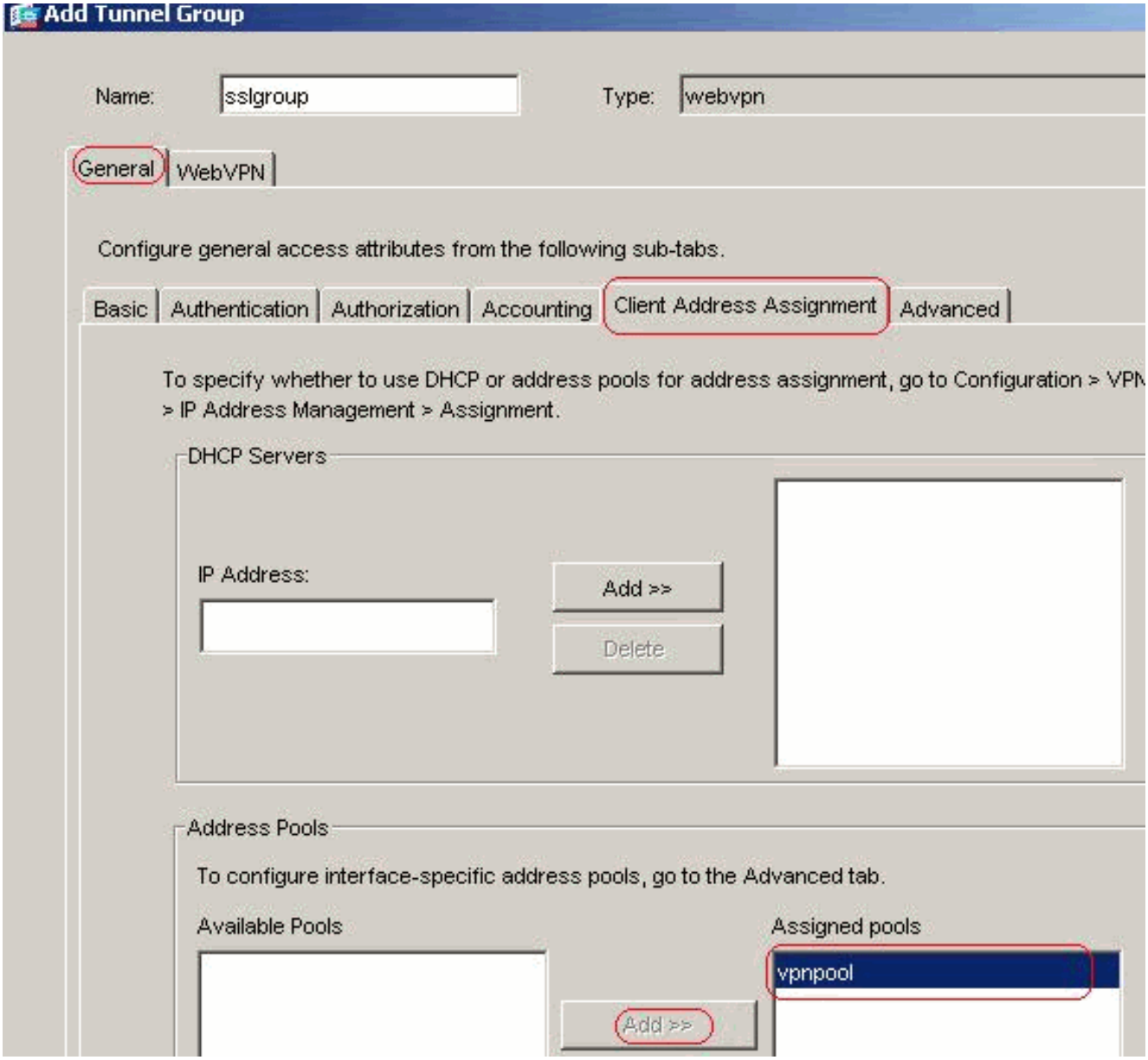


Equivalent CLI Configuration:

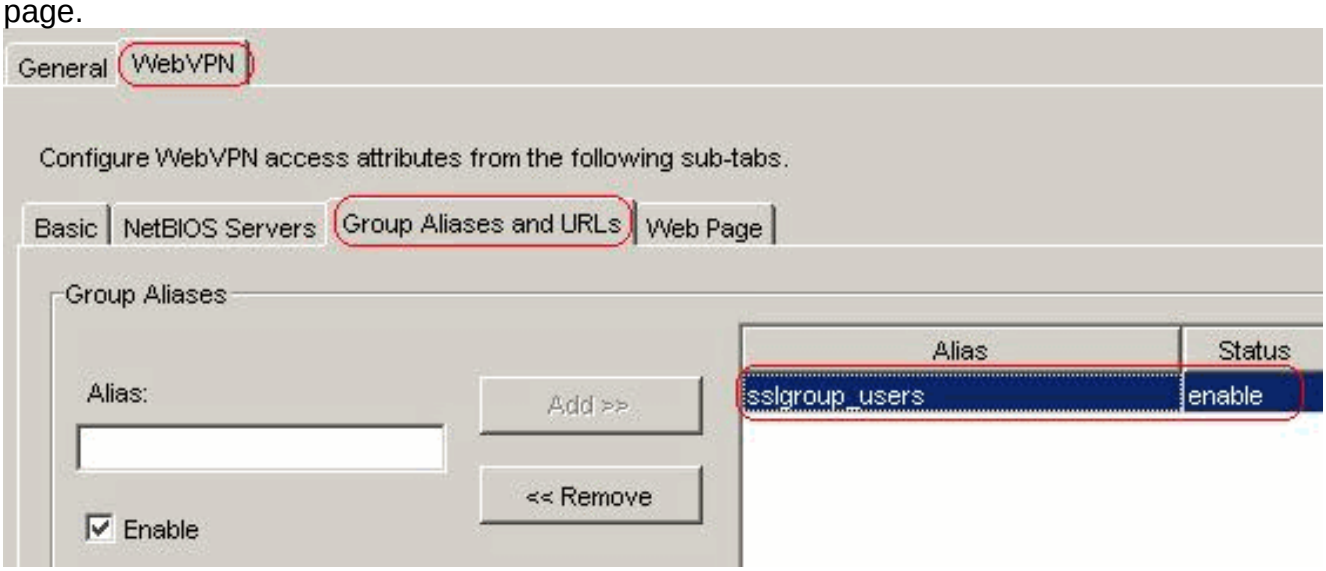
7. **Configure Tunnel Group**Choose **Configuration > VPN > General > Tunnel Group > Add (WebVPN access)** in order to create a new tunnel group **sslgroup**.In the **General > Basic** tab, choose the Group Policy as **clientgroup** from the drop-down list.



In **General > Client Address Assignment** tab, under Address Pools, click **Add >>** in order to assign the available address pool **vpnpool**.

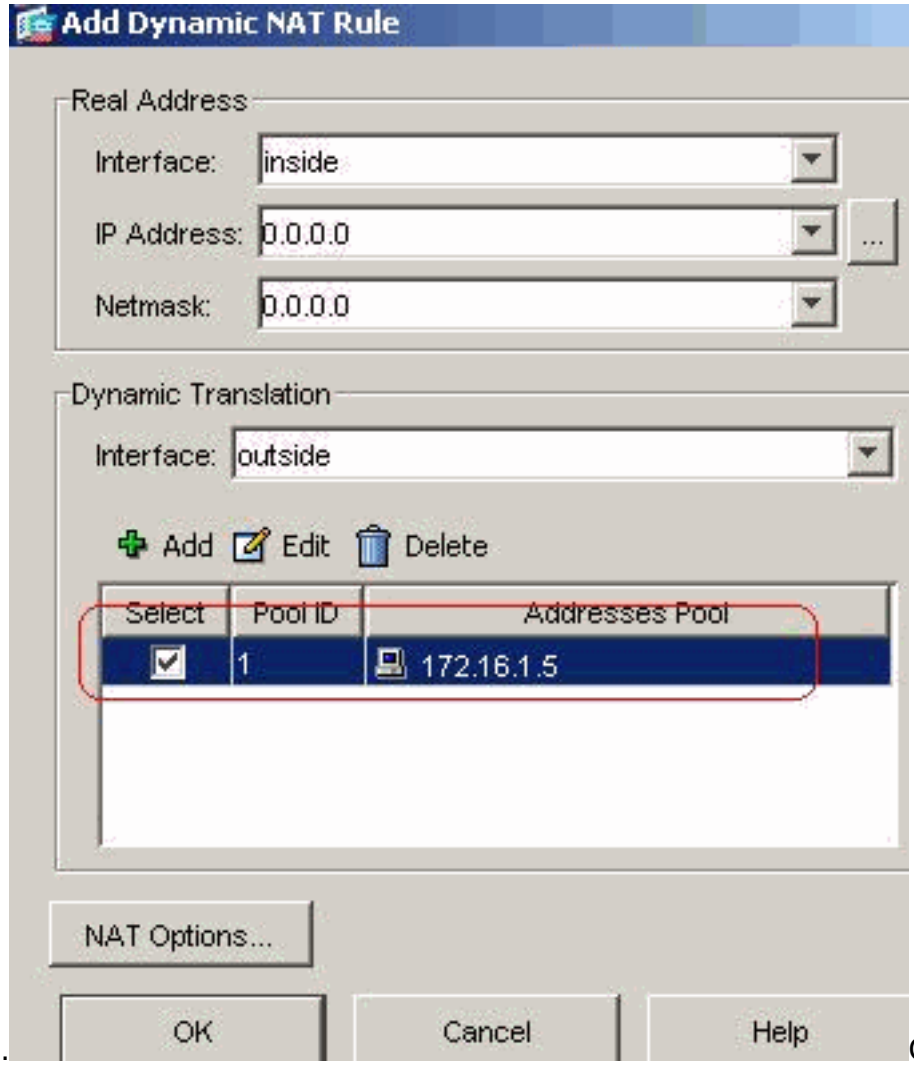


In the **WebVPN > Group Aliases and URLs** tab, type the alias name in the parameter box and click **Add >>** in order to make it appear in the list of group names in the login page.



Click **OK** and then **Apply**.**Equivalent CLI Configuration:**

8. **Configure NAT**Choose **Configuration > NAT > Add > Add Dynamic NAT Rule** for the traffic that comes from the inside network that can be translated with outside IP address



172.16.1.5. Click **OK** and click **Apply** in main page.**Equivalent CLI Configuration:**

9. Configure the nat-exemption for the return-traffic from inside network to the VPN client.`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) Configuration Using 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
```

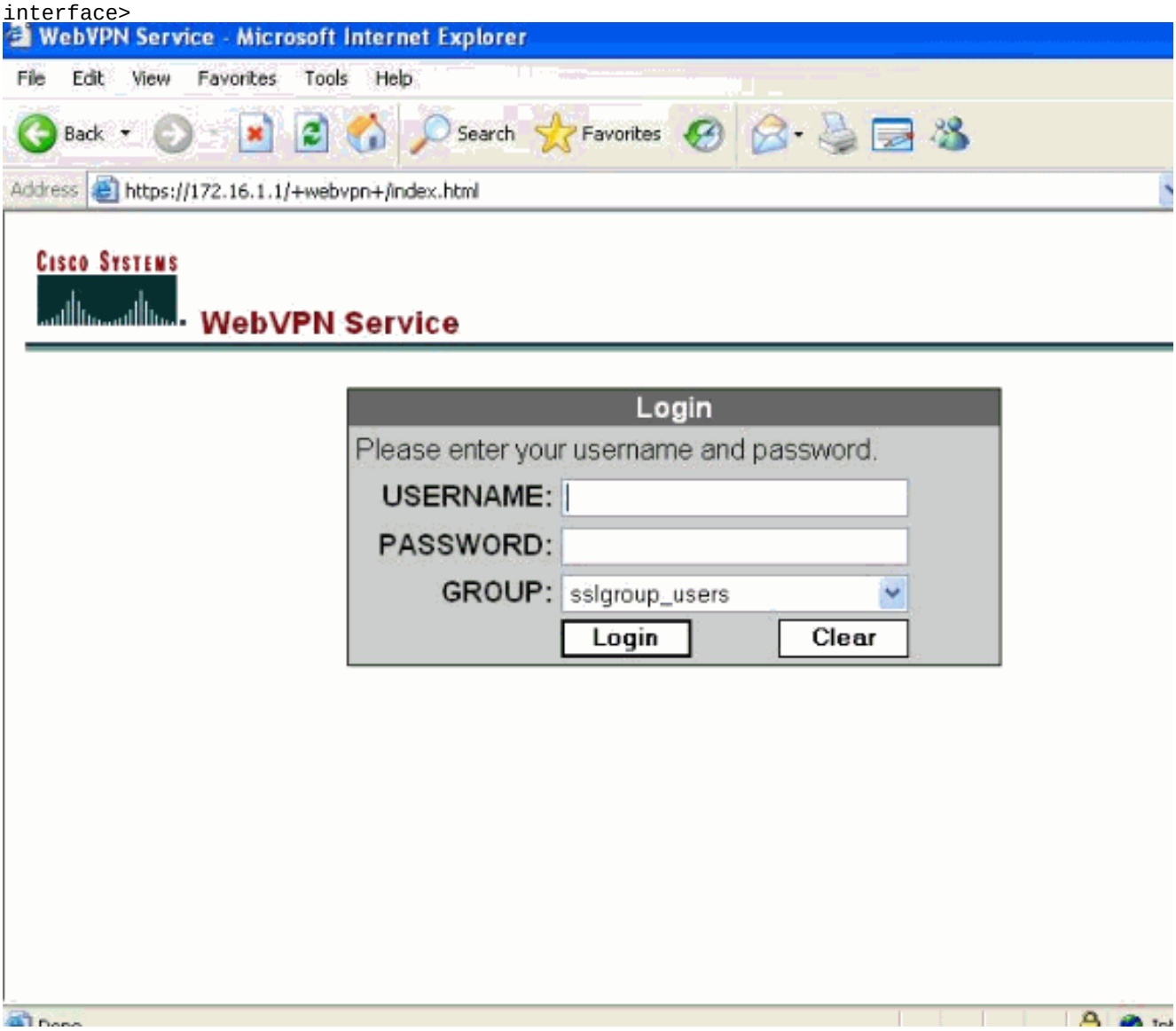
```
the SSL VPN Clients no failover icmp unreachable rate-
limit 1 burst-size 1 asdm image disk0:/asdm-522.bin no
asdm history enable arp timeout 14400 global (outside) 1
172.16.1.5 !--- The global address for Internet access
used by VPN Clients. !--- Note: Uses an RFC 1918 range
for lab setup. !--- 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#
```

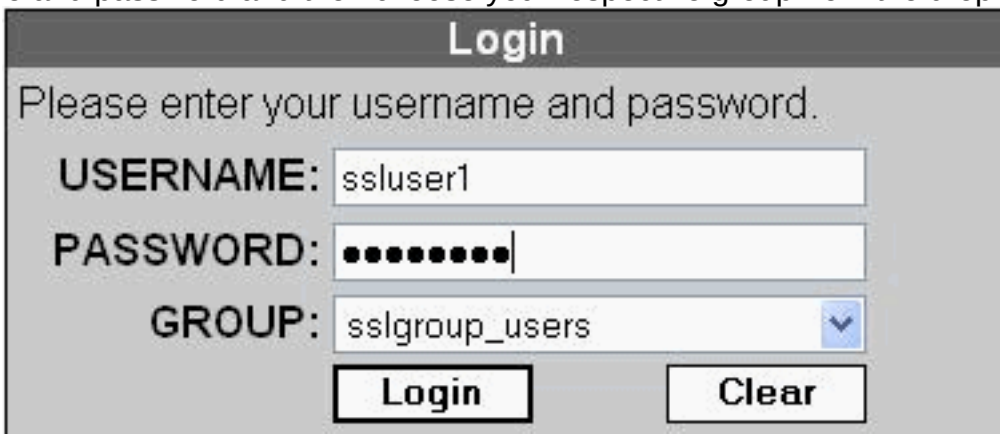
Establish the SSL VPN Connection with SVC

Complete these steps in order to establish a SSL VPN connection with ASA.

1. Type the URL or IP address of the WebVPN interface of the ASA in your web browser in the format as shown.`https://url`OR`https://<IP address of the ASA WebVPN interface>`



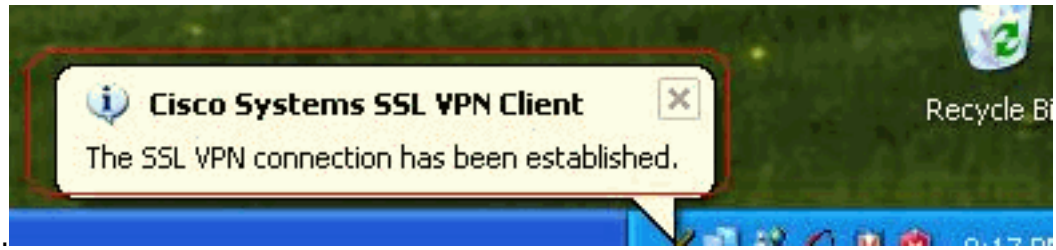
2. Enter your username and password and then choose your respective group from the drop down list as shown.



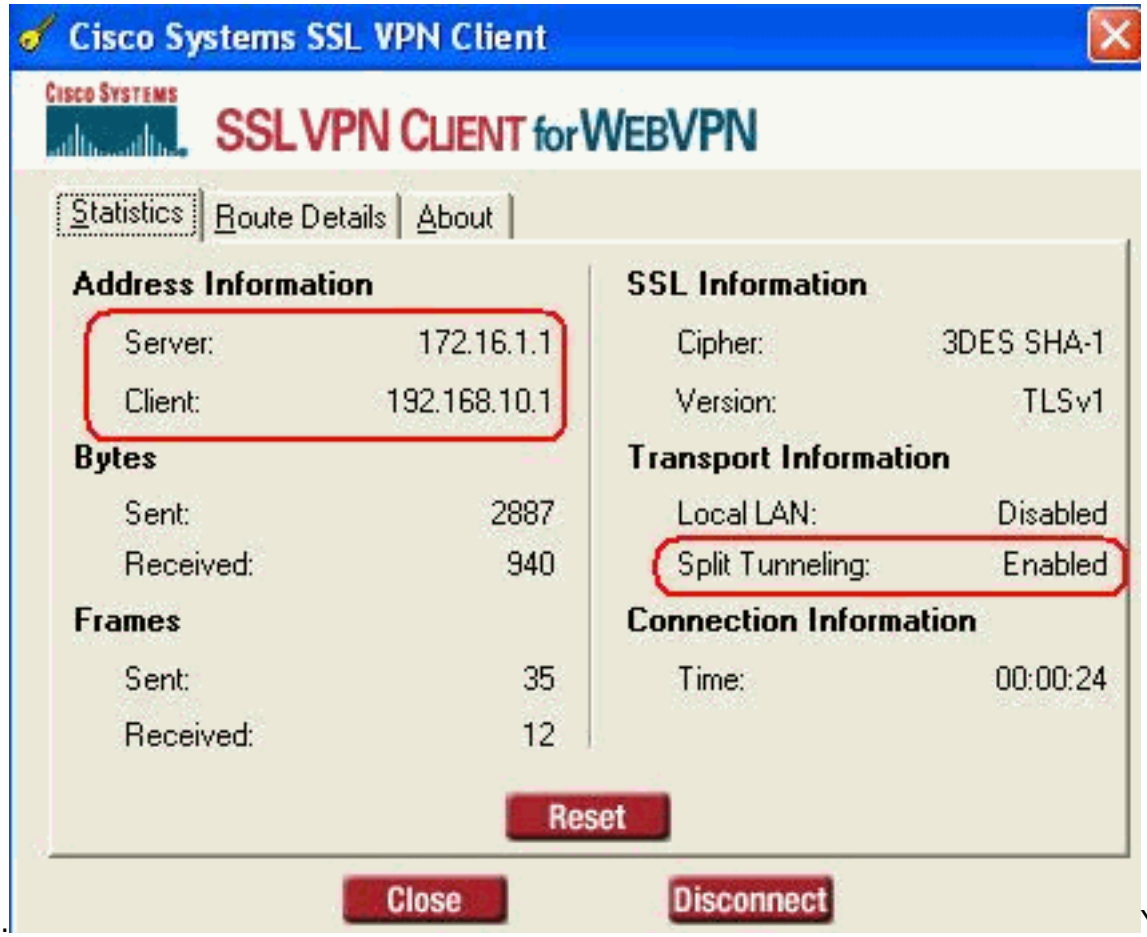
3. ActiveX software must be installed in your computer before download the

SVC. 

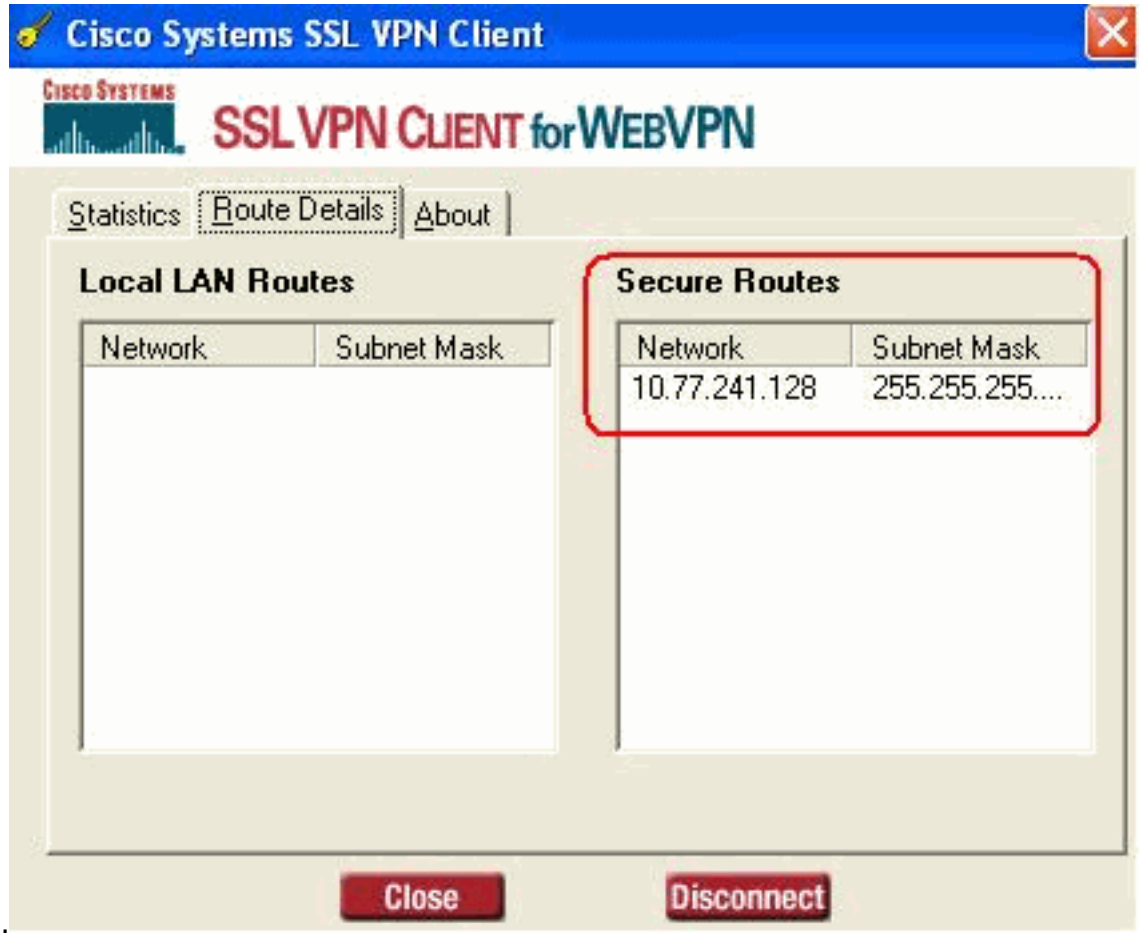
4. These windows appear before the SSL VPN connection is established. 

5. You can get these windows once the connection is established. 

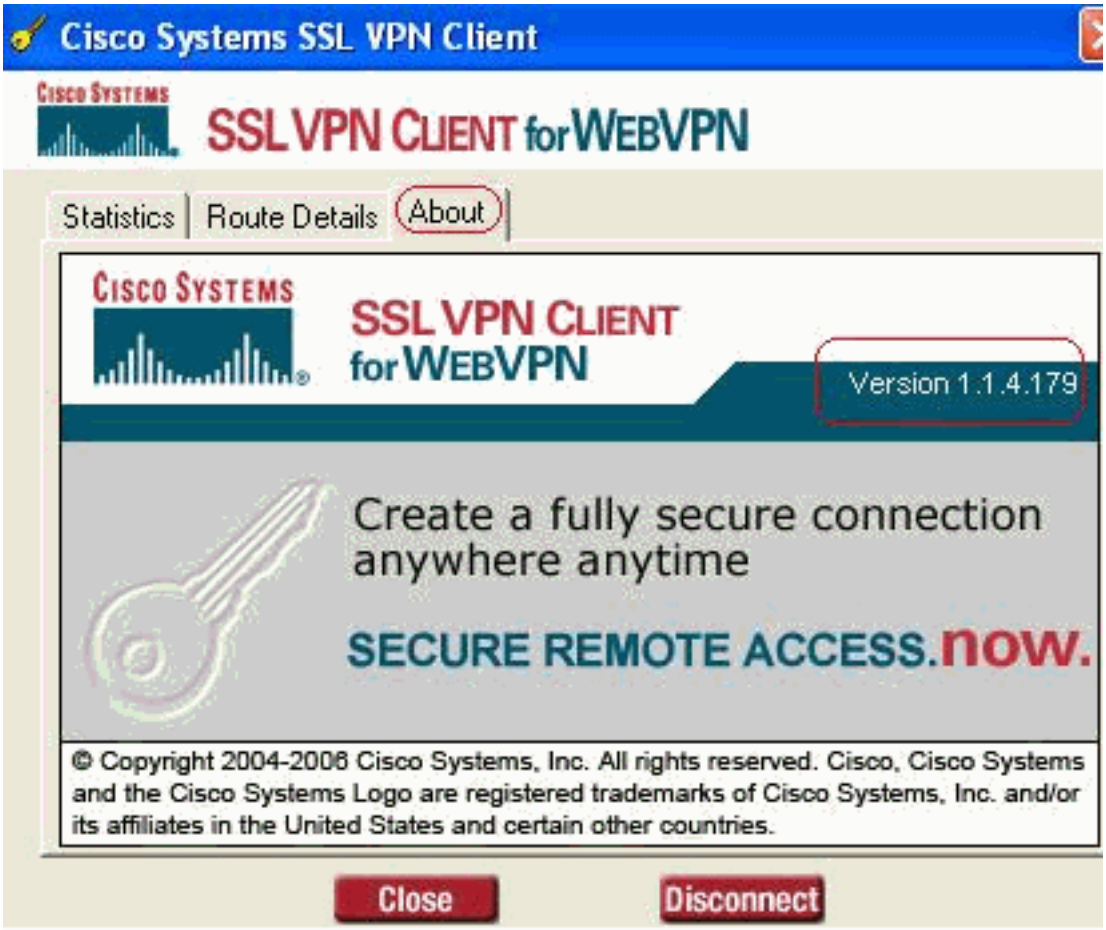
6. Click the yellow key which appears in the task bar of your computer. These windows appears which gives information about the SSL connection. For example, **192.168.10.1** is the assigned IP for client and server IP address is 172.16.1.1, **Split tunneling is enabled**, and



so forth. You can also check the secured network which is to be encrypted by SSL, the network list is downloaded from split-tunnel access list configured in ASA.In this example, the SSL VPN Client secures access to 10.77.241.128/24 while all other traffic is not encrypted and not sent across the



tunnel.

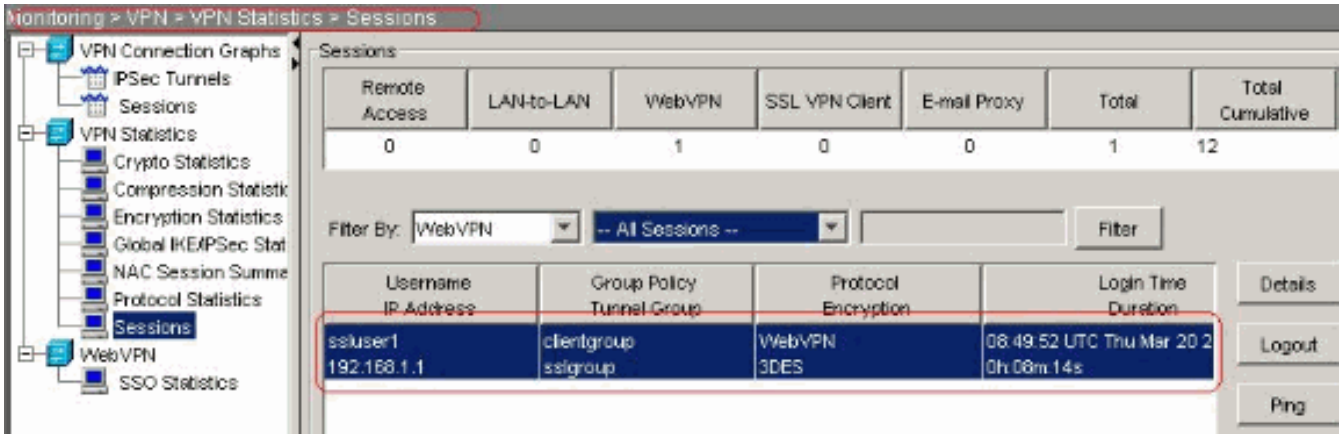


Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

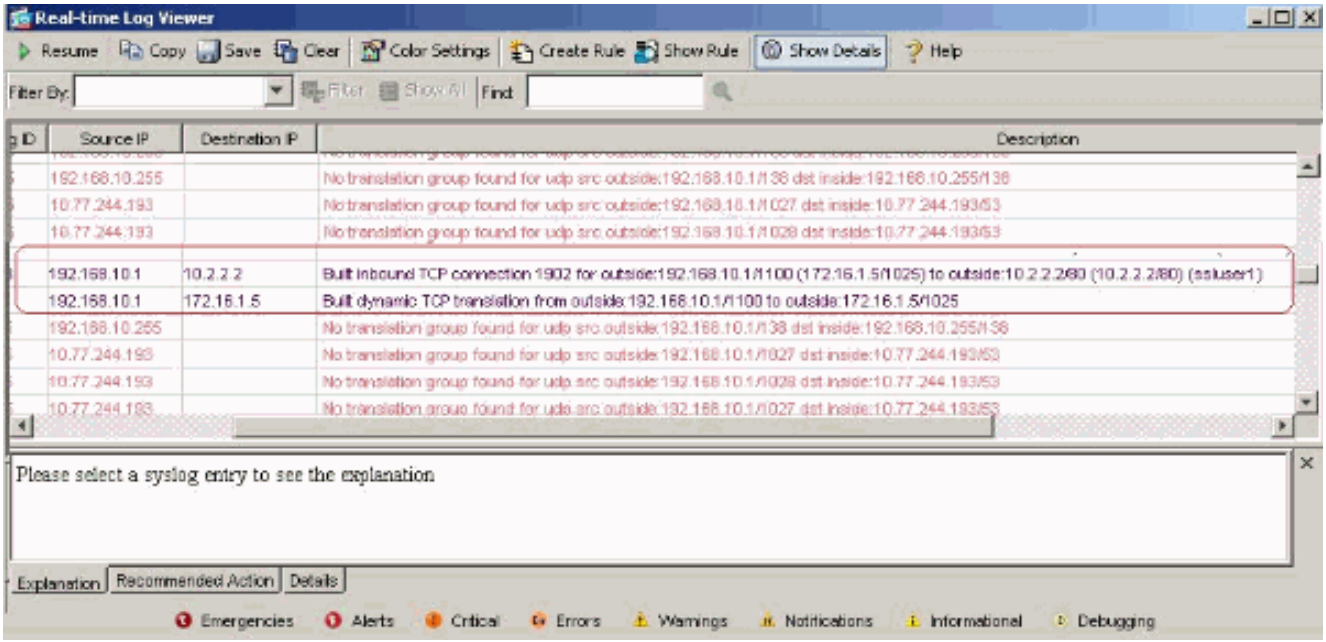
- **show webvpn svc**—Displays the SVC images stored in the ASA flash memory.`ciscoasa#show webvpn svc 1. disk0:/sslclient-win-1.1.4.179.pkg 1 CISCO STC win2k+ 1.0.0 1,1,4,179 Fri 01/18/2008 15:19:49.43 1 SSL VPN Client(s) installed`
- **show vpn-sessiondb svc**—Displays the information about the current SSL connections.`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**—Displays the configured alias for various groups.`ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup_users enabled`
- In ASDM, choose **Monitoring > VPN > VPN Statistics > Sessions** in order to know about the current WebVPN sessions in the ASA.



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

1. **vpn-sessiondb logoff name <username>**—Command to logoff the SSL VPN session for the particular username.`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`** Similarly, you can use the **vpn-sessiondb logoff svc** command in order to terminate all the SVC sessions.
2. **Note:** If the PC goes to standby or hibernate mode, then the SSL VPN connection can be terminated.
   `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. **Debug webvpn svc <1-255>**—Provides the real time webvpn events in order to establish the session.`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. In ASDM, choose **Monitoring > Logging > Real-time Log Viewer > View** in order to see the real time events. These example shows about the session information between the SVC 192.168.10.1 and Webserver 10.2.2.2 in the internet through ASA 172.16.1.5.



Related Information

- Cisco 5500 Series Adaptive Security Appliance Product Support
- ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example
- Router Allows VPN Clients to Connect IPsec and Internet Using Split Tunneling Configuration Example
- PIX/ASA 7.x and VPN Client for Public Internet VPN on a Stick Configuration Example
- SSL VPN Client (SVC) on ASA with ASDM Configuration Example
- Technical Support & Documentation - Cisco Systems