ASA 7.1/7.2: Esempio di configurazione dell'appliance ASA che consente il tunneling ripartito per SVC

Sommario

Introduzione

In questo documento viene spiegato dettagliatamente come consentire ai client VPN (SVC) Secure Socket Layer (SSL) di accedere a Internet mentre sono tunneling in una appliance Cisco Adaptive Security (ASA). Questa configurazione consente a SVC di accedere in modo sicuro alle risorse aziendali tramite SSL e fornisce accesso non protetto a Internet tramite l'utilizzo del tunneling ripartito.

La capacità di trasmettere il traffico protetto e non protetto sulla stessa interfaccia è nota come tunneling suddiviso. Il tunneling ripartito richiede che si specifichi esattamente quale traffico è protetto e quale sia la destinazione di tale traffico, in modo che solo il traffico specificato entri nel tunnel, mentre il resto viene trasmesso in modo non crittografato attraverso la rete pubblica (Internet).

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Privilegi amministrativi locali su tutte le workstation remote
- Controlli Java e ActiveX sulla workstation remota
- La porta 443 (SSL) non è bloccata in alcun punto del percorso di connessione

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 7.2(2)
- Cisco SSL VPN Client versione per Windows 1.1.4.179**Nota:** scaricare il pacchetto SSL VPN Client (sslclient-win*.pkg) da Cisco Software Download (solo utenti registrati). Copiare lo SVC sulla memoria flash dell'ASA, che deve essere scaricata sui computer degli utenti remoti per stabilire la connessione VPN SSL con ASA. Per ulteriori informazioni, consultare la sezione Installazione del software SVC nella guida alla configurazione dell'ASA.
- PC con Windows 2000 Professional SP4 o Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM) versione 5.2(2)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

SSL VPN Client (SVC) è una tecnologia di tunneling VPN che offre agli utenti remoti i vantaggi di un client VPN IPsec senza la necessità per gli amministratori di rete di installare e configurare client VPN IPsec in computer remoti. SVC utilizza la crittografia SSL già presente nel computer remoto, nonché l'accesso e l'autenticazione WebVPN dell'appliance di sicurezza.

Per stabilire una sessione SVC, l'utente remoto immette nel browser l'indirizzo IP di un'interfaccia WebVPN dell'accessorio di protezione e il browser si connette a tale interfaccia e visualizza la schermata di accesso di WebVPN. Se il login e l'autenticazione sono soddisfacenti e l'appliance di sicurezza identifica l'utente come dispositivo che richiede l'SVC, l'appliance di sicurezza scarica l'SVC sul computer remoto. Se l'accessorio di protezione consente di utilizzare l'SVC, l'accessorio di protezione scaricherà l'SVC sul computer remoto mentre nella finestra viene visualizzato un collegamento che consente di ignorare l'installazione dell'SVC.

Una volta scaricato, l'SVC viene installato e configurato automaticamente e quindi rimane o si disinstalla automaticamente dal computer remoto, a seconda della configurazione, al termine della connessione.

Configurazione

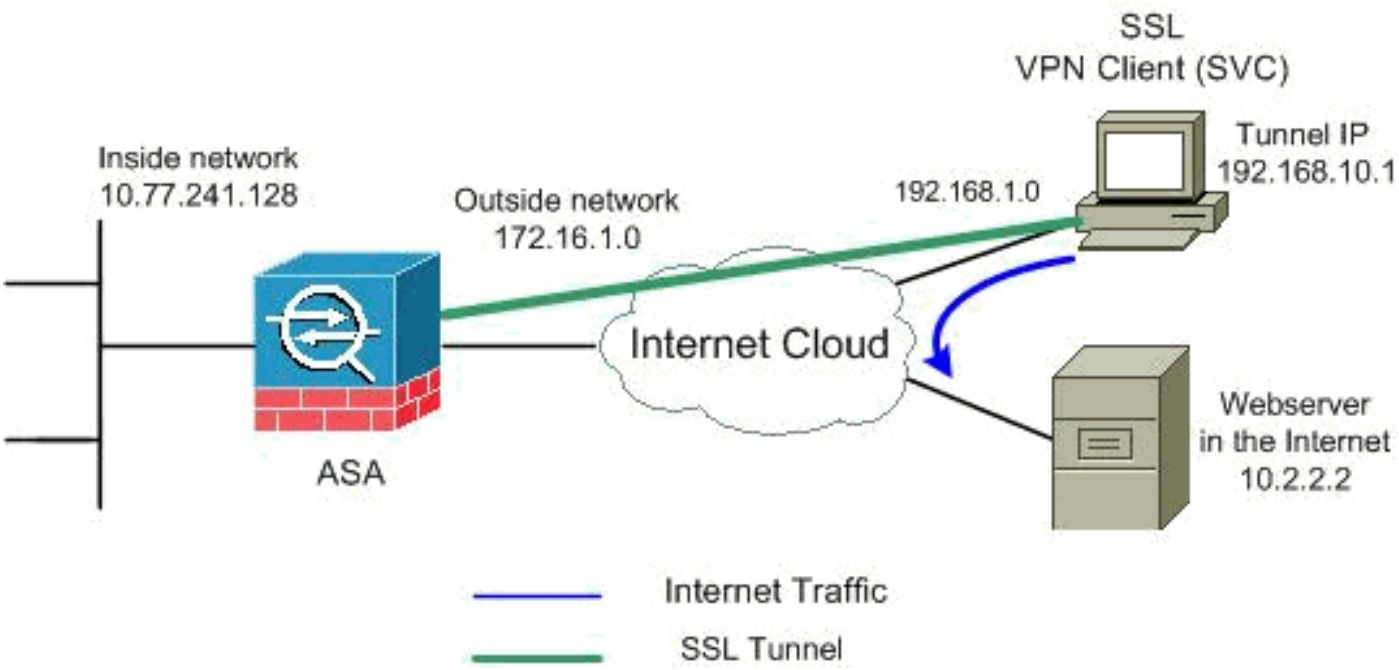
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità

descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:

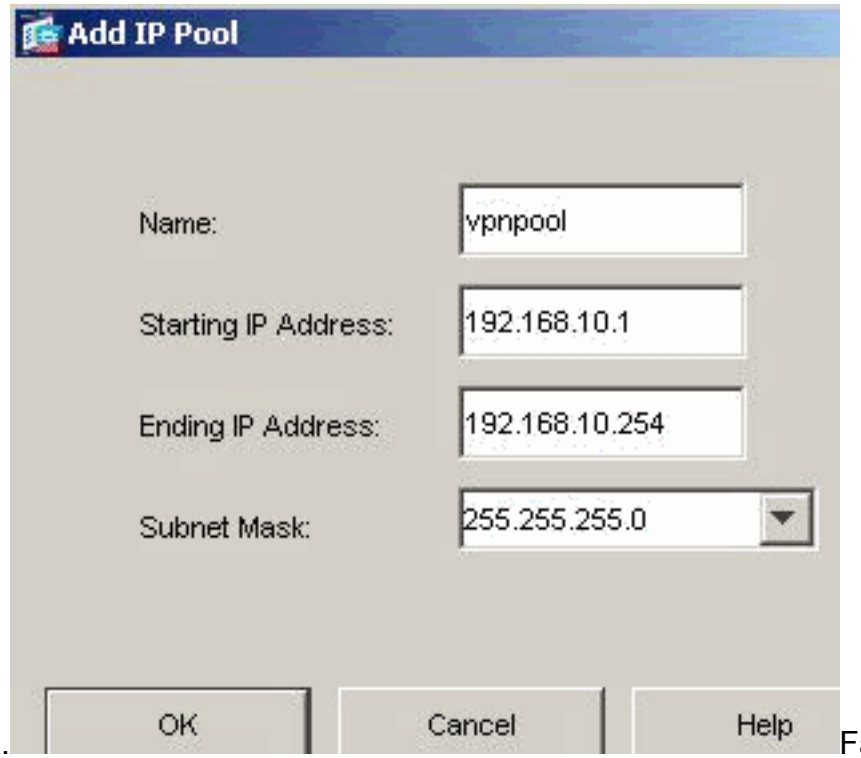


Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazioni ASA con ASDM 5.2(2)

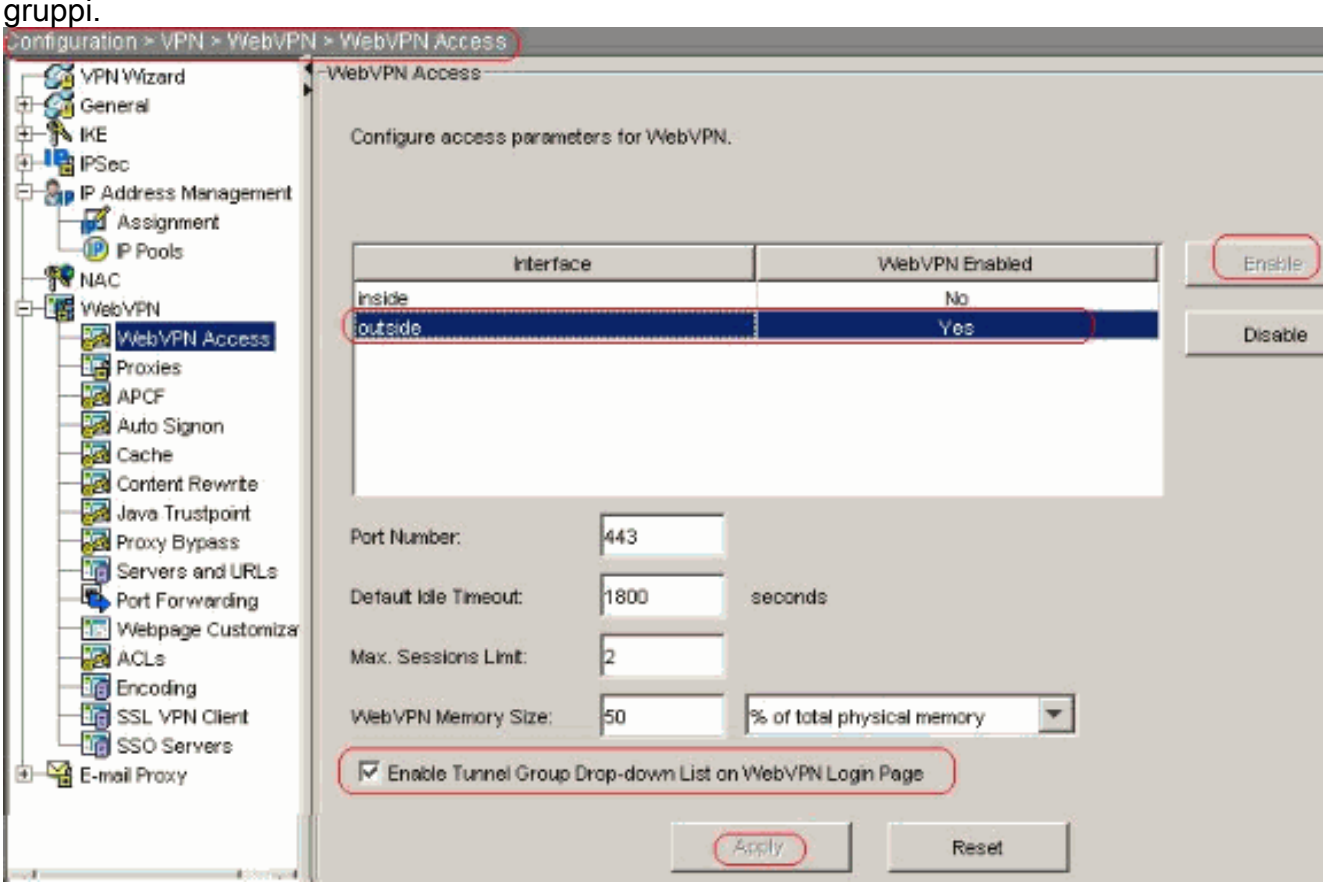
Completare questa procedura per configurare la VPN SSL sull'appliance ASA con tunneling ripartito come mostrato:

1. Nel documento si presume che la configurazione di base, ad esempio la configurazione dell'interfaccia, sia già stata creata e funzioni correttamente.**Nota:** per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.**Nota:** WebVPN e ASDM non possono essere abilitati sulla stessa interfaccia ASA a meno che non si modifichino i numeri di porta. Per ulteriori informazioni, fare riferimento a ASDM e WebVPN abilitati sulla stessa interfaccia dell'ASA.
2. Per creare un pool di indirizzi IP, scegliere **Configurazione > VPN > Gestione indirizzi IP > Pool** di indirizzi IP: **vpnpool** per client

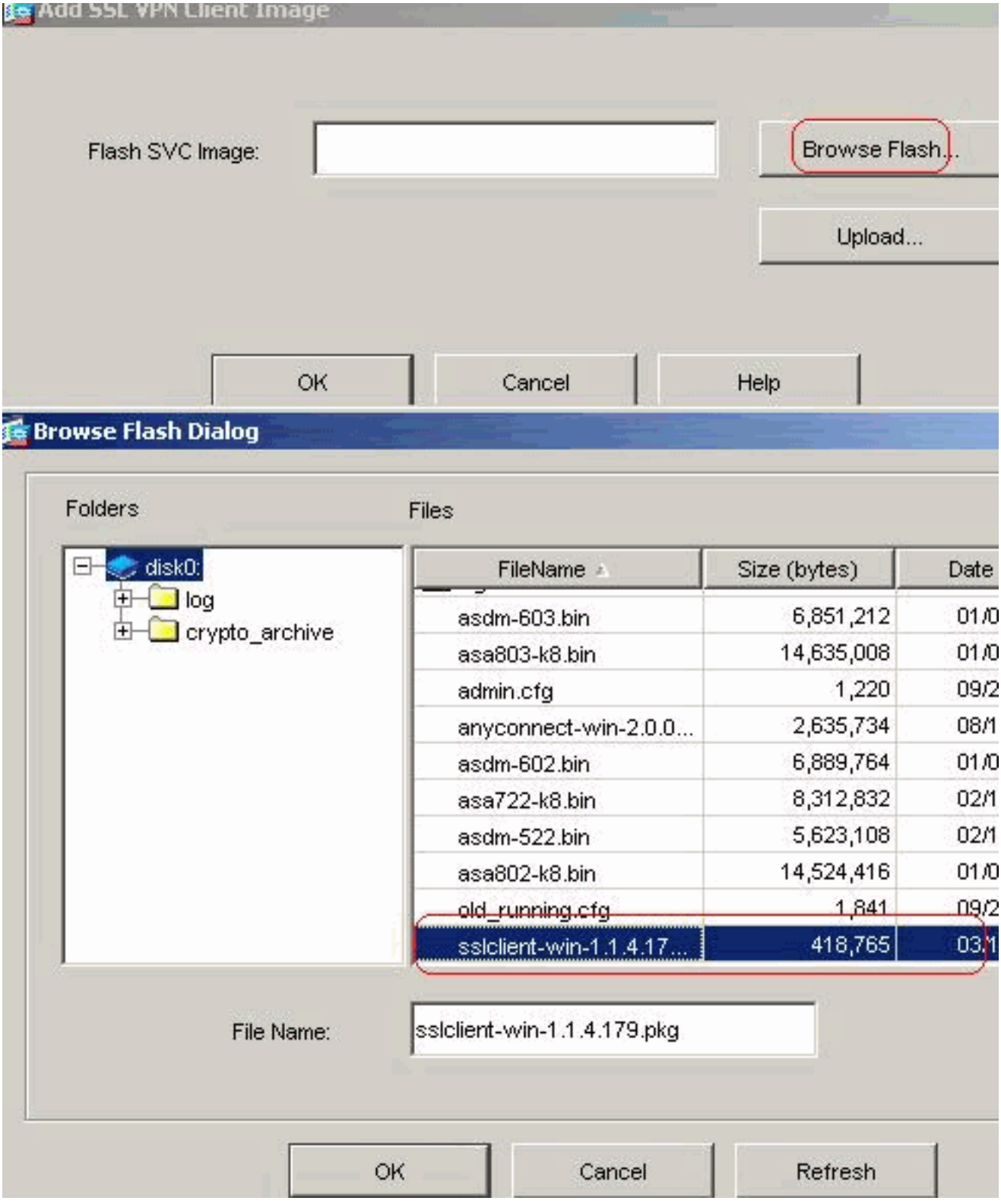


VPN. Fare clic su **Apply** (Applica).

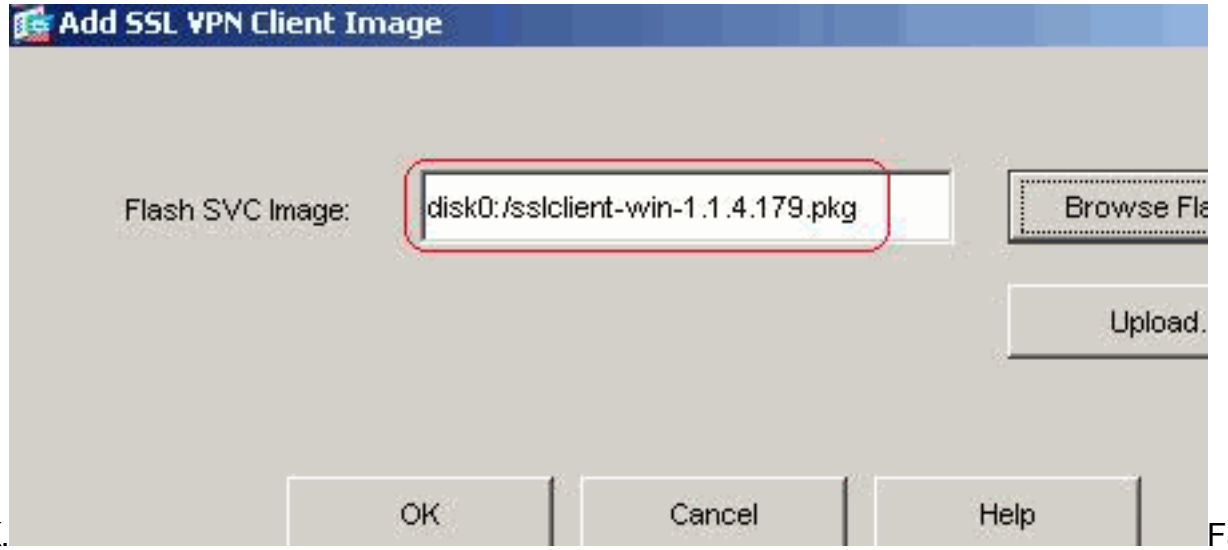
3. **Abilita WebVPN**Scegliere **Configurazione > VPN > WebVPN > Accesso WebVPN** ed evidenziare l'interfaccia esterna con il mouse e fare clic su **Abilita**. Selezionare la casella di controllo **Abilita elenco a discesa gruppi tunnel nella pagina di accesso WebVPN** per abilitare la visualizzazione dell'elenco a discesa nella pagina di accesso per gli utenti, per scegliere i rispettivi
gruppi.



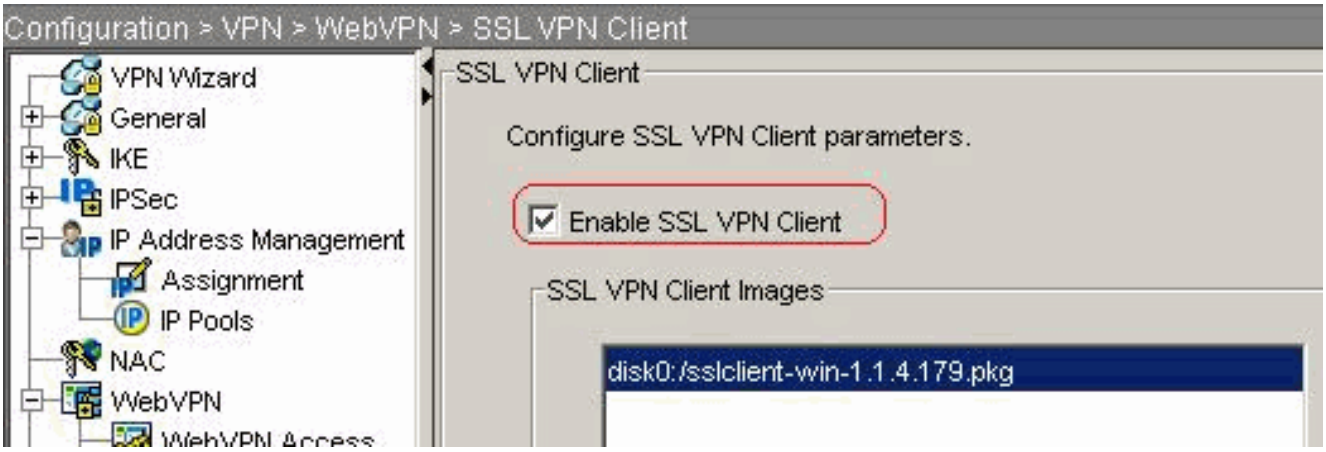
Fare clic su **Apply** (Applica).Scegliere **Configurazione > VPN > WebVPN > SSL VPN Client > Aggiungi** per aggiungere l'immagine del client VPN SSL dalla memoria flash dell'ASA, come mostrato.


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

Fare clic su

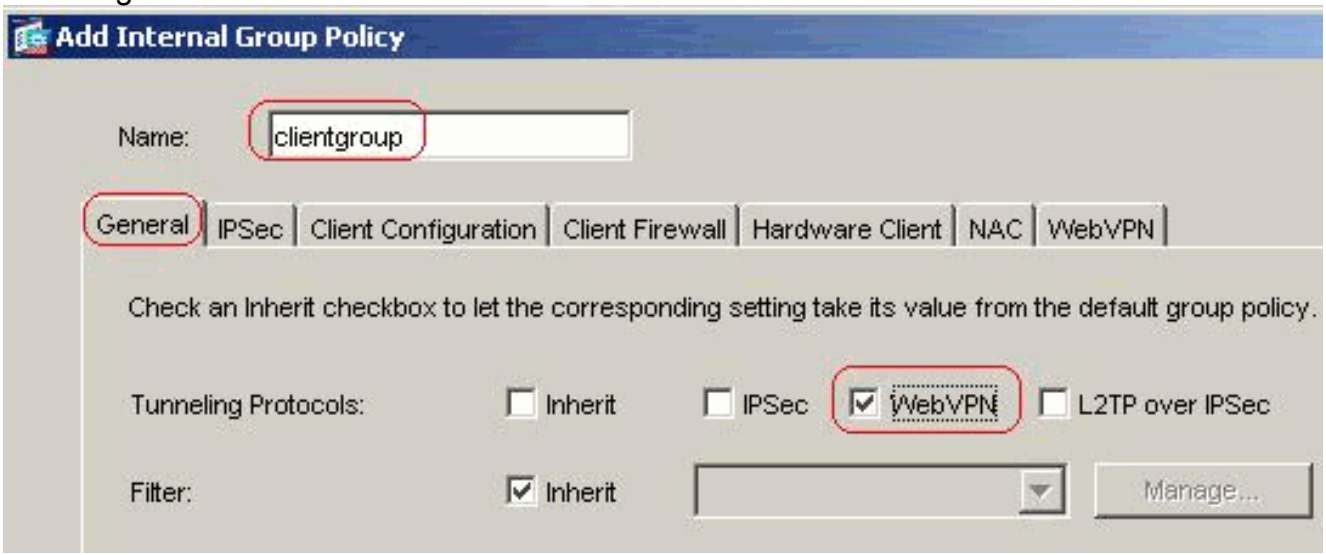


OK.Fare clic su **OK**.Selezionare la casella di controllo **SSL VPN Client**.



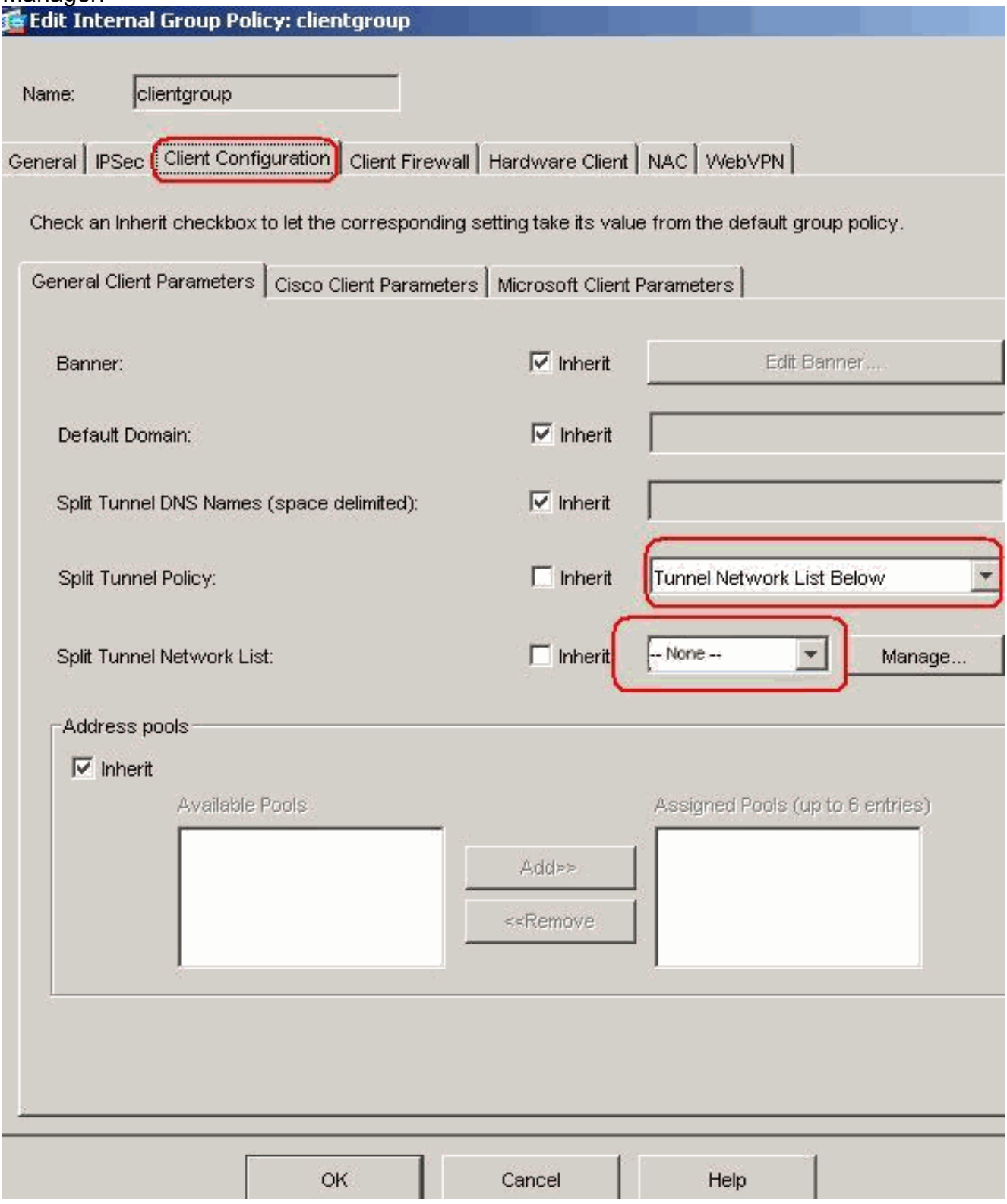
Fare clic su **Apply** (Applica).**Configurazione CLI equivalente:**

4. **Configura Criteri di gruppo**Per creare un **gruppo client di** Criteri di gruppo interno, scegliere **Configurazione > VPN > Generale > Criteri di gruppo > Aggiungi (Criteri di gruppo interni)**. In **Generale**, scegliere la casella di controllo **WebVPN** per abilitare WebVPN come protocollo di tunneling.

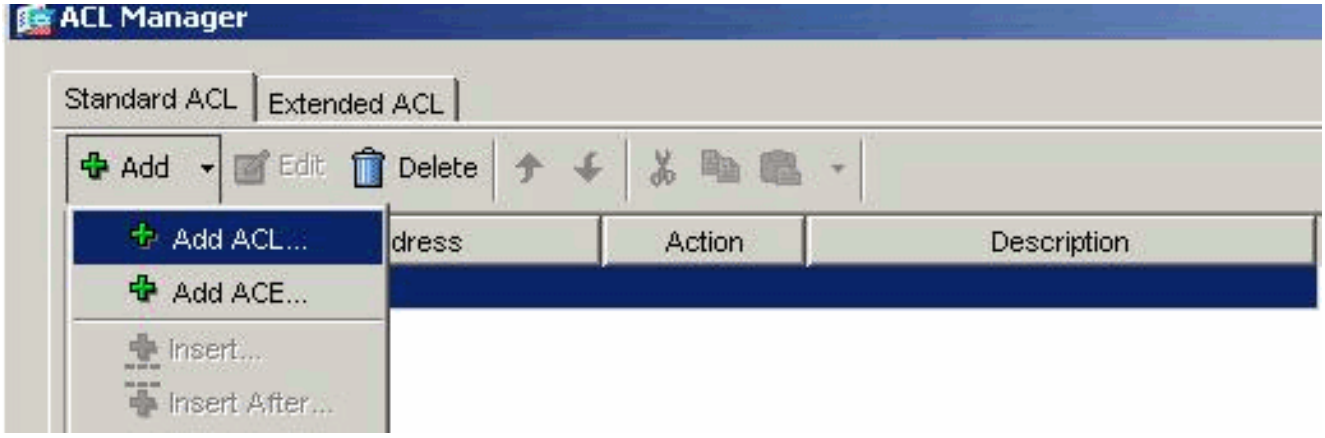


Nella scheda **Configurazione client >Parametri generali del client**, deselezionare la casella **Eredita** per Criterio tunnel diviso e scegliere **Elenco reti tunnel sotto** dall'elenco a discesa.Deselezionare la casella **Inherit** (Eredita) per **Split Tunnel Network List** (Elenco reti tunnel suddiviso) e fare clic su **Manage** (Gestisci) per avviare ACL

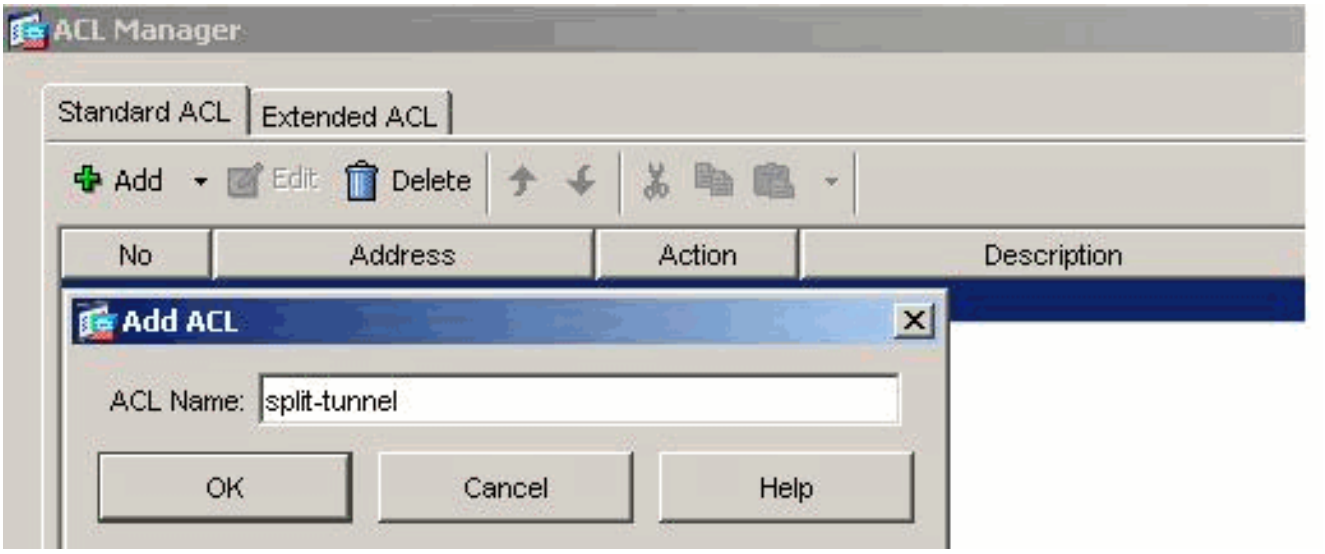
Manager.



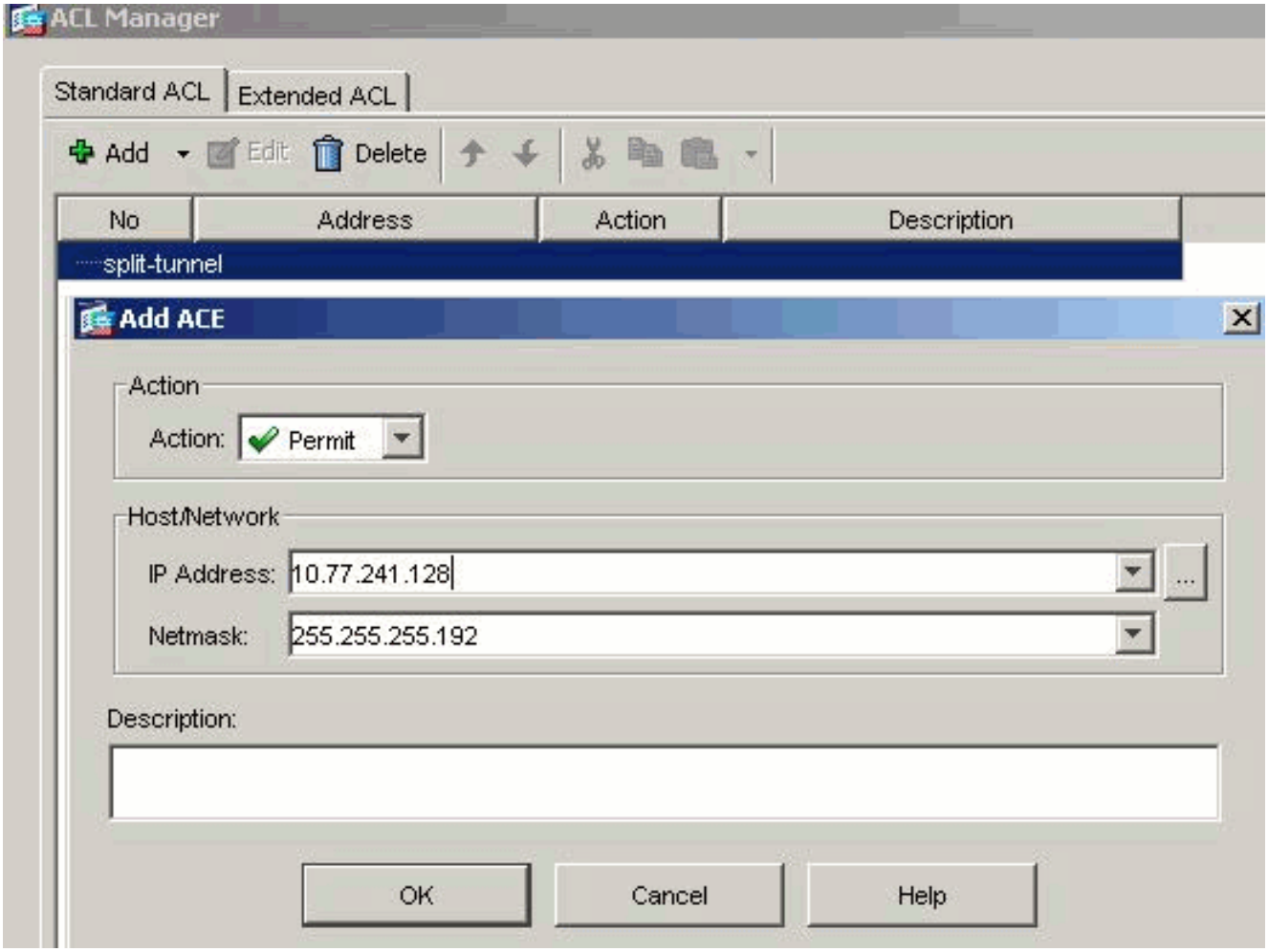
In Gestione ACL, selezionare **Add > Add ACL...** (Aggiungi ACL) per creare un nuovo elenco degli
accessi.



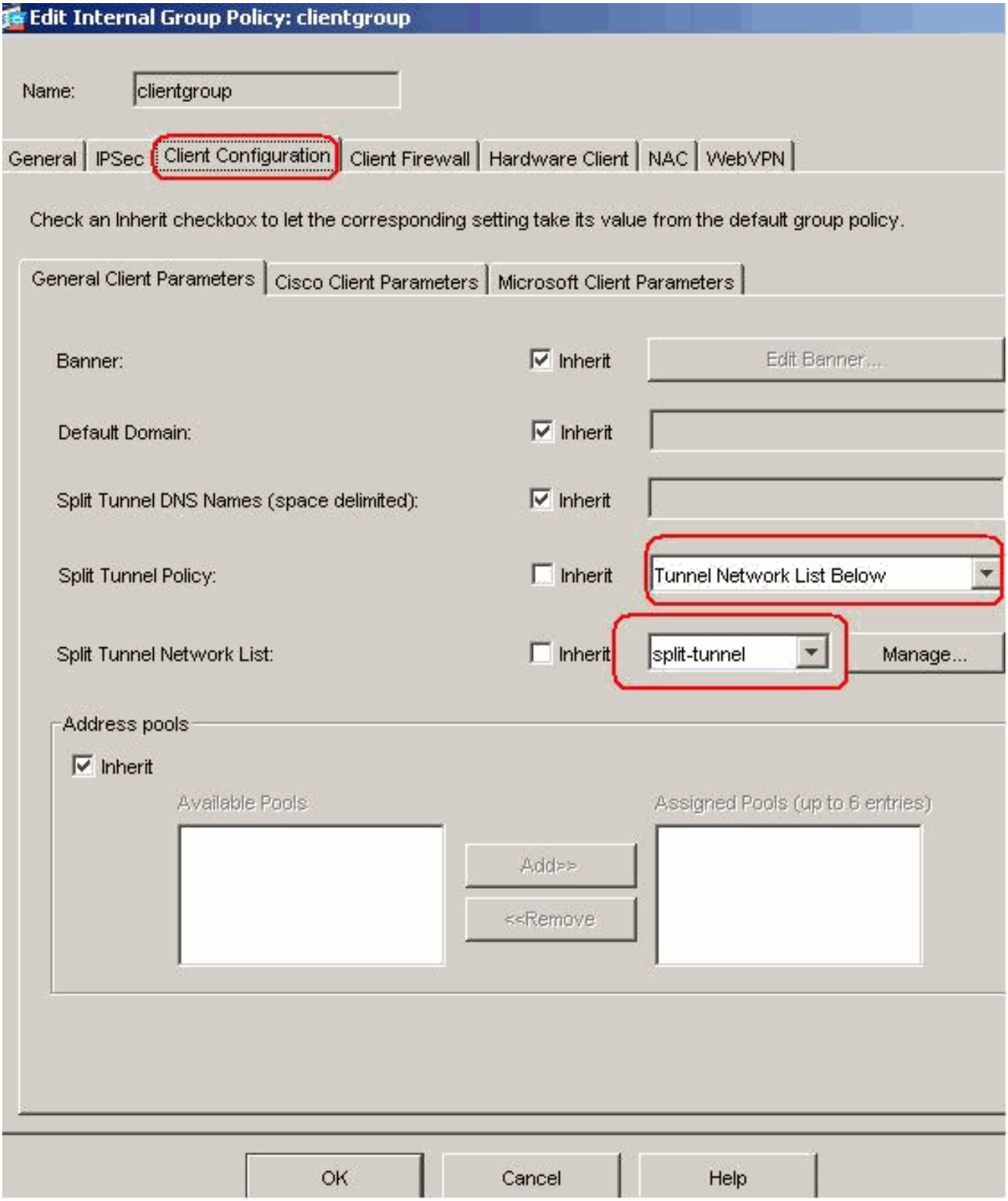
Specificare un nome per l'ACL e fare clic su
OK.



Una volta creato il nome dell'ACL, scegliere **Aggiungi > Aggiungi ACE** per aggiungere una voce di controllo di accesso (ACE, Access Control Entry).Definire l'ACE che corrisponde alla LAN dietro l'ASA. In questo caso, la rete è 10.77.241.128/26 e selezionare **Permit** (Autorizza).Per uscire da Gestione ACL, fare clic su
OK.

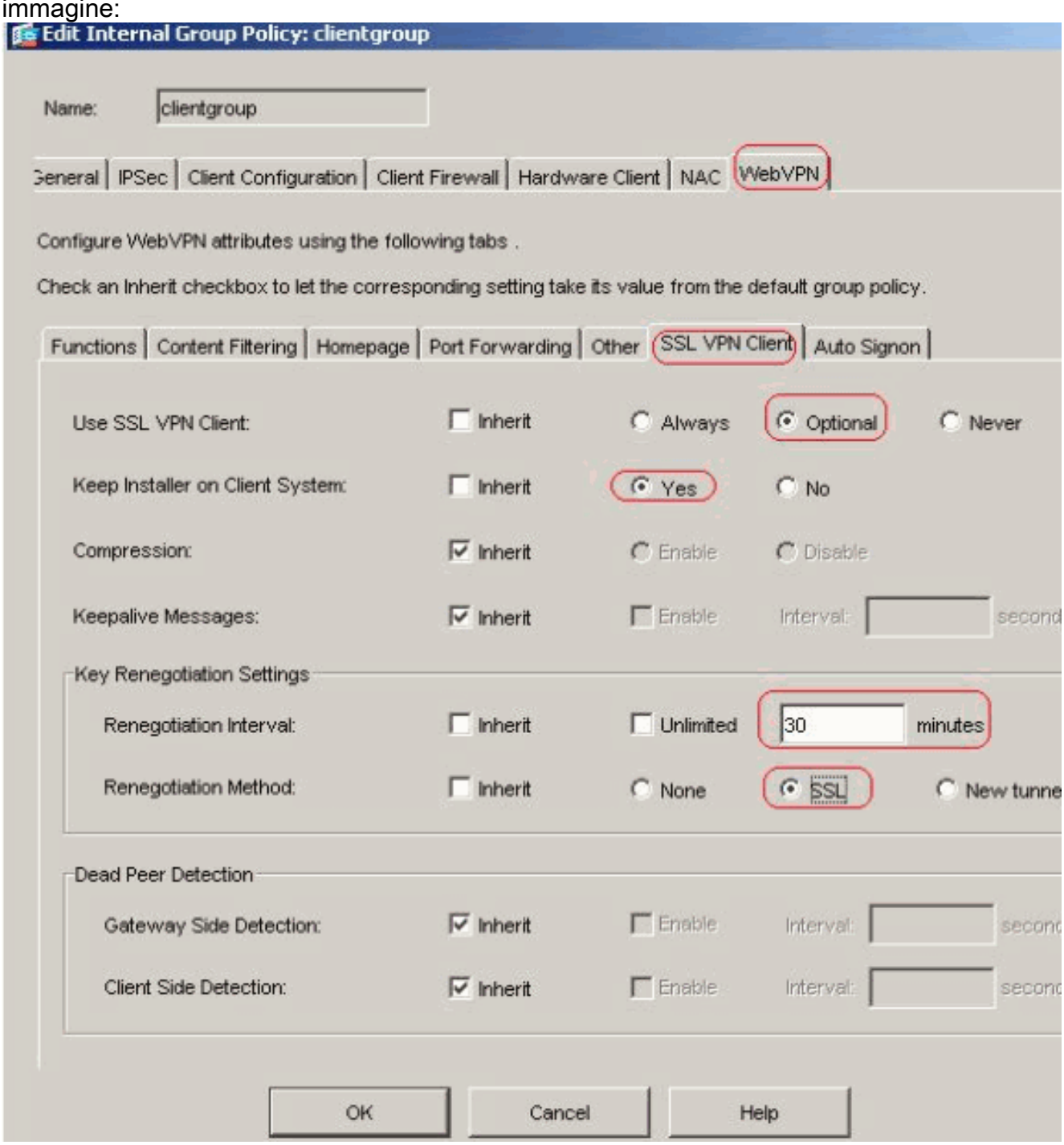


Accertarsi quindi che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel suddiviso.Per tornare alla configurazione di Criteri di gruppo, fare clic su **OK**.

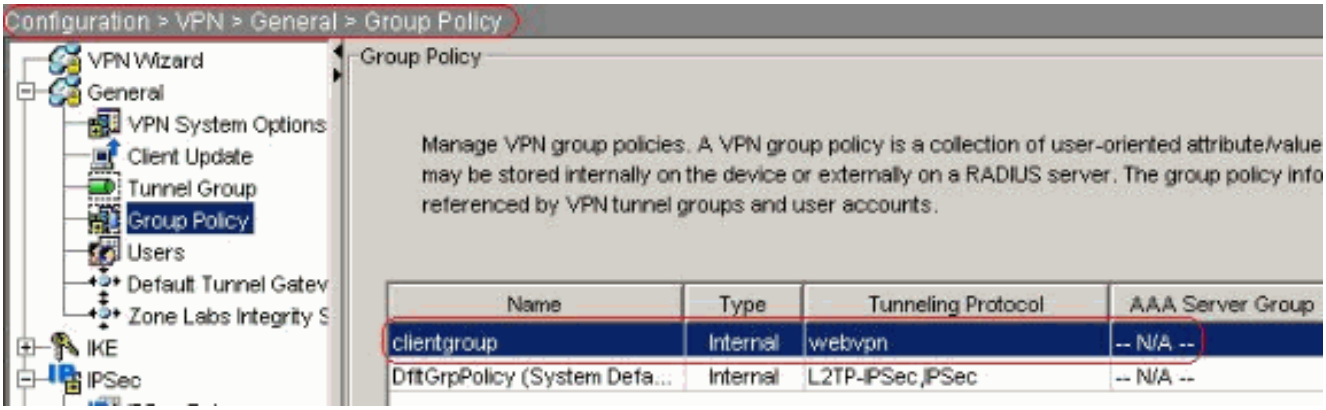


Nella pagina principale, fare clic su **Apply**, quindi su **Send** (se necessario) per inviare i comandi all'appliance ASA.Per l'opzione Usa client VPN SSL, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **Facoltativo**.Questa opzione consente al client remoto di scegliere se fare clic sulla scheda **WebVPN > SSL Client** e di scegliere le opzioni seguenti:Non scaricare SVC. L'opzione Always (Sempre) garantisce che l'SVC venga scaricato sulla workstation remota durante ogni connessione VPN SSL.Per l'opzione Mantieni programma di installazione sul sistema client, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **Sì**.Questa azione consente al software SVC di rimanere sul computer client; di conseguenza, non è necessario che l'ASA scarichi il software SVC sul client ogni volta che viene stabilita una connessione. Questa opzione è ideale per gli utenti remoti che spesso accedono alla rete aziendale.Per l'opzione Intervallo

rinegoziazione, deselezionare la casella di controllo **Eredita**, deselezionare la casella di controllo **Illimitato** e immettere il numero di minuti che devono trascorrere prima della reimpostazione della chiave.La protezione viene migliorata quando si impostano i limiti di validità di una chiave.Per l'opzione Metodo rinegoziazione, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **SSL**. La rinegoziazione può utilizzare il tunnel SSL corrente o un nuovo tunnel creato espressamente per la rinegoziazione.Gli attributi del client VPN SSL devono essere configurati come mostrato in questa immagine:

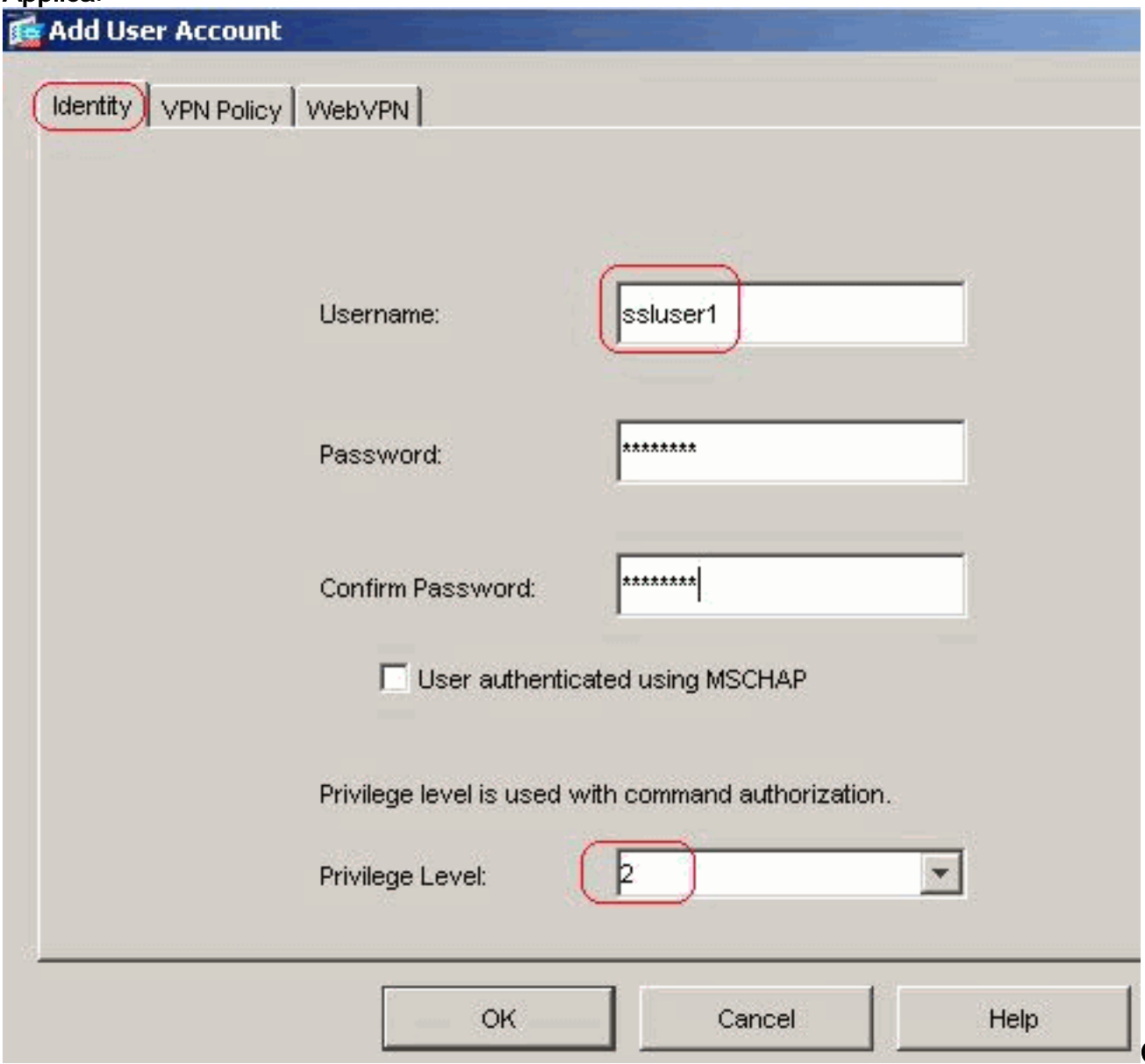


Fare clic su **OK**, quindi su **Applica**.



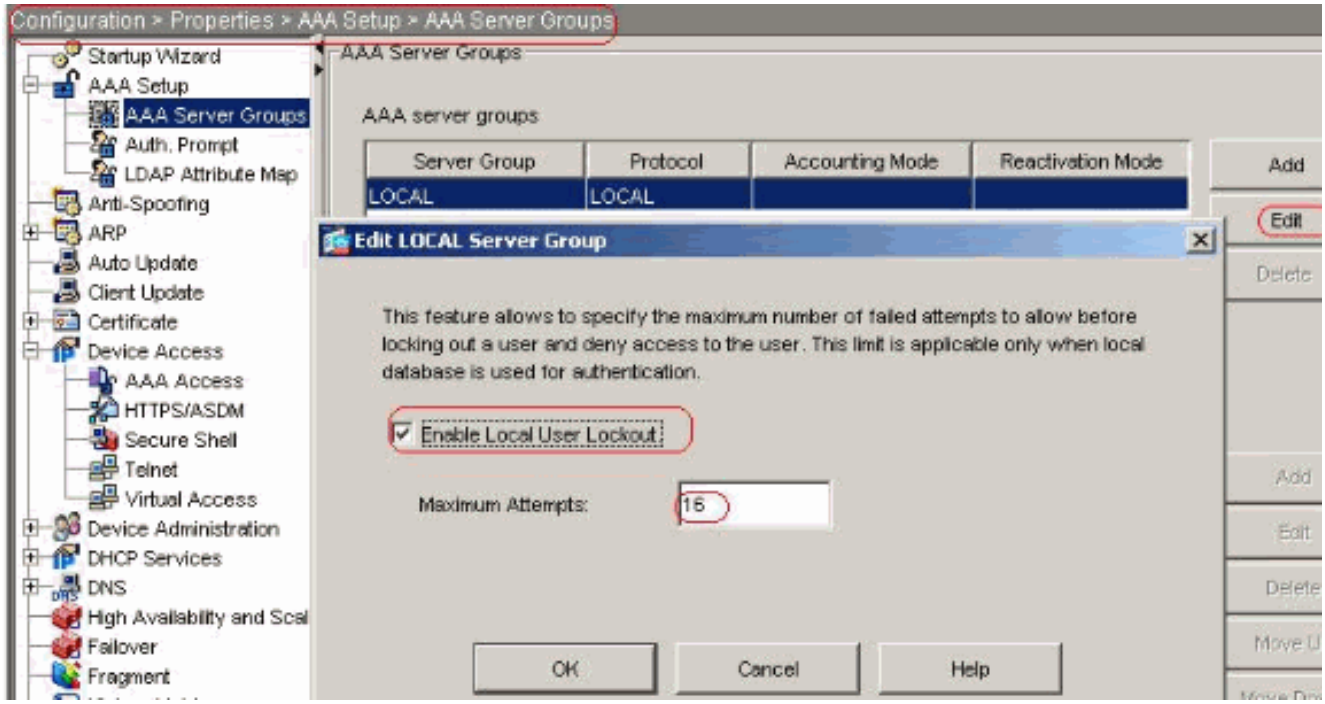
Configurazione CLI equivalente:

5. Per creare un nuovo account utente **ssluser1,** scegliere **Configurazione > VPN > Generale > Utenti > Aggiungi**. Fare clic su **OK** e quindi su **Applica**.



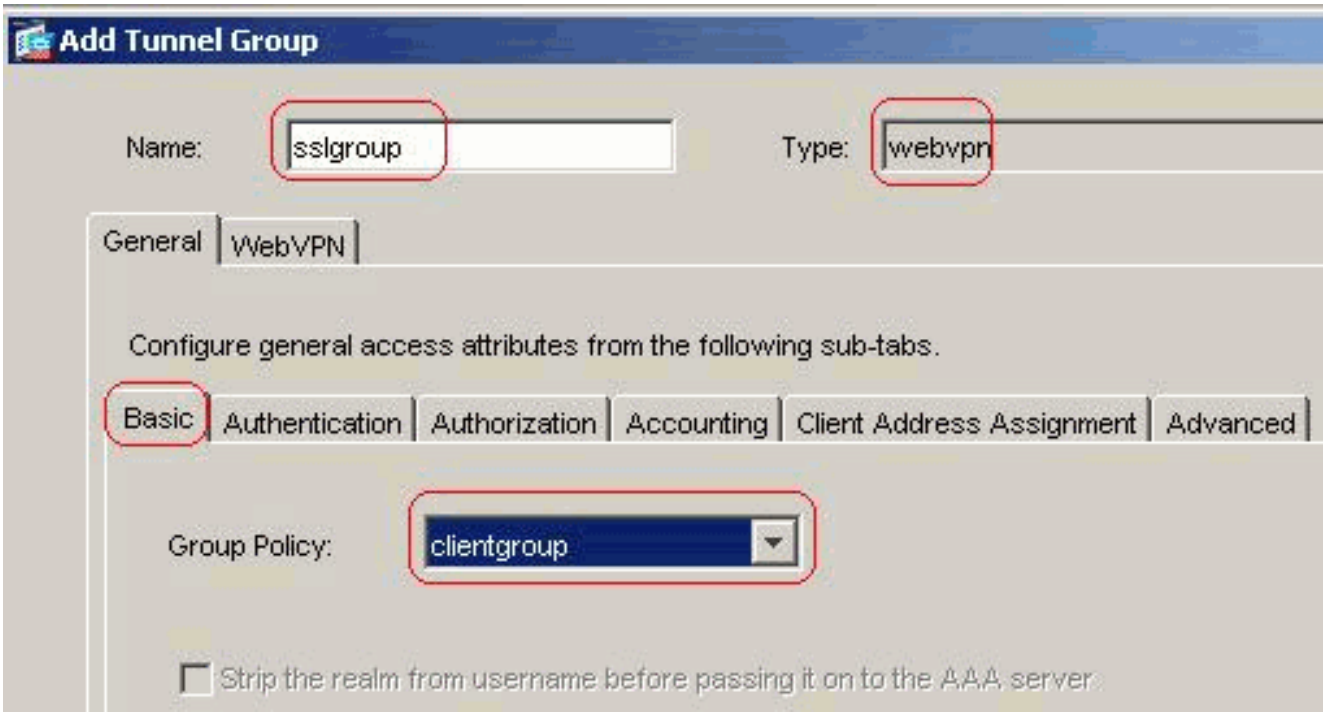
Configurazione CLI equivalente:

6. Scegliere **Configurazione > Proprietà > Impostazione AAA > Gruppi di server AAA > Modifica** per modificare il gruppo di server predefinito **LOCAL** e selezionare la casella di controllo **Abilita blocco utente locale** con un valore di tentativi massimo pari a **16**.

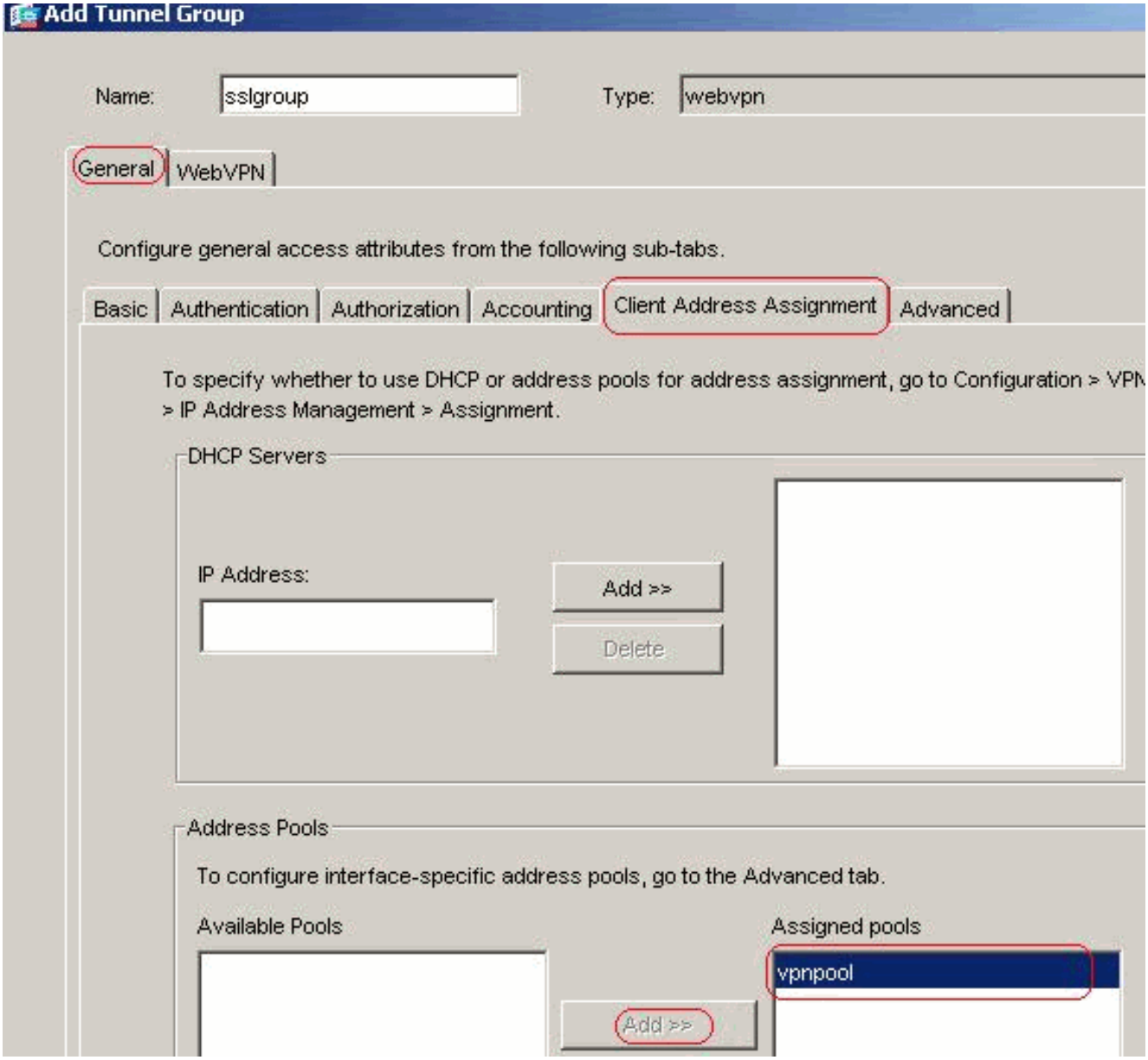


Configurazione CLI equivalente:

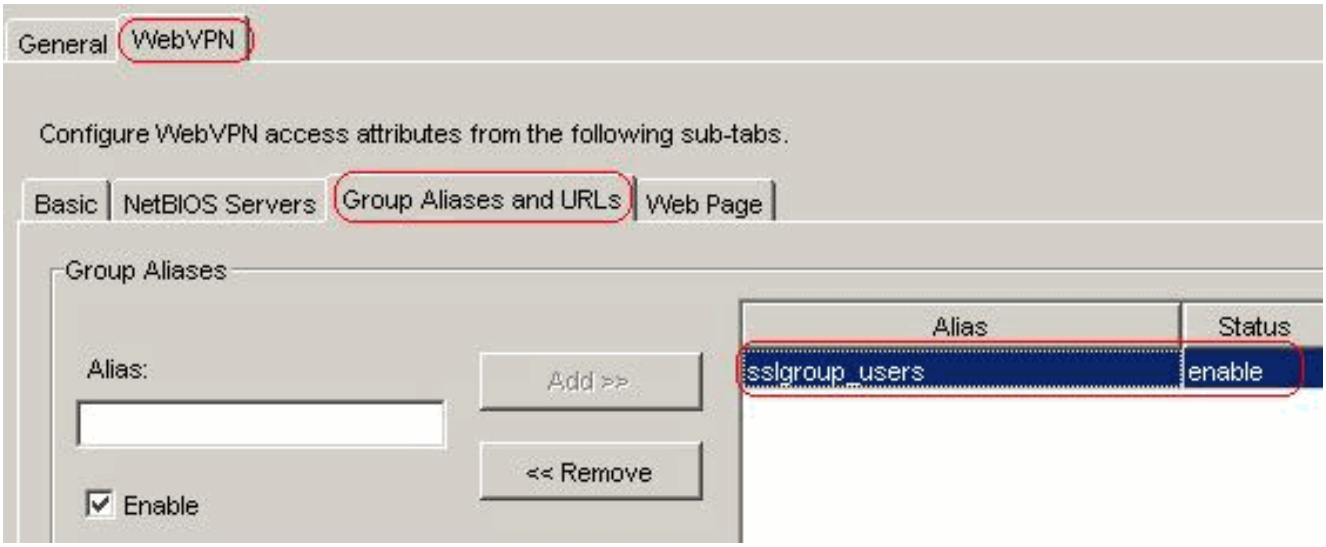
7. **Configura gruppo di tunnel**Scegliere **Configurazione > VPN > Generale > Gruppo di tunnel > Aggiungi (accesso WebVPN)** per creare un nuovo **gruppo di** tunnel.Nella scheda **Generale > Generale** scegliere Criteri di gruppo come **gruppo client** dall'elenco a discesa.



In **Generale >** scheda **Assegnazione indirizzi client**, in Pool di indirizzi, fare clic su **Aggiungi >>** per assegnare il pool di indirizzi disponibile **vpnpool**.

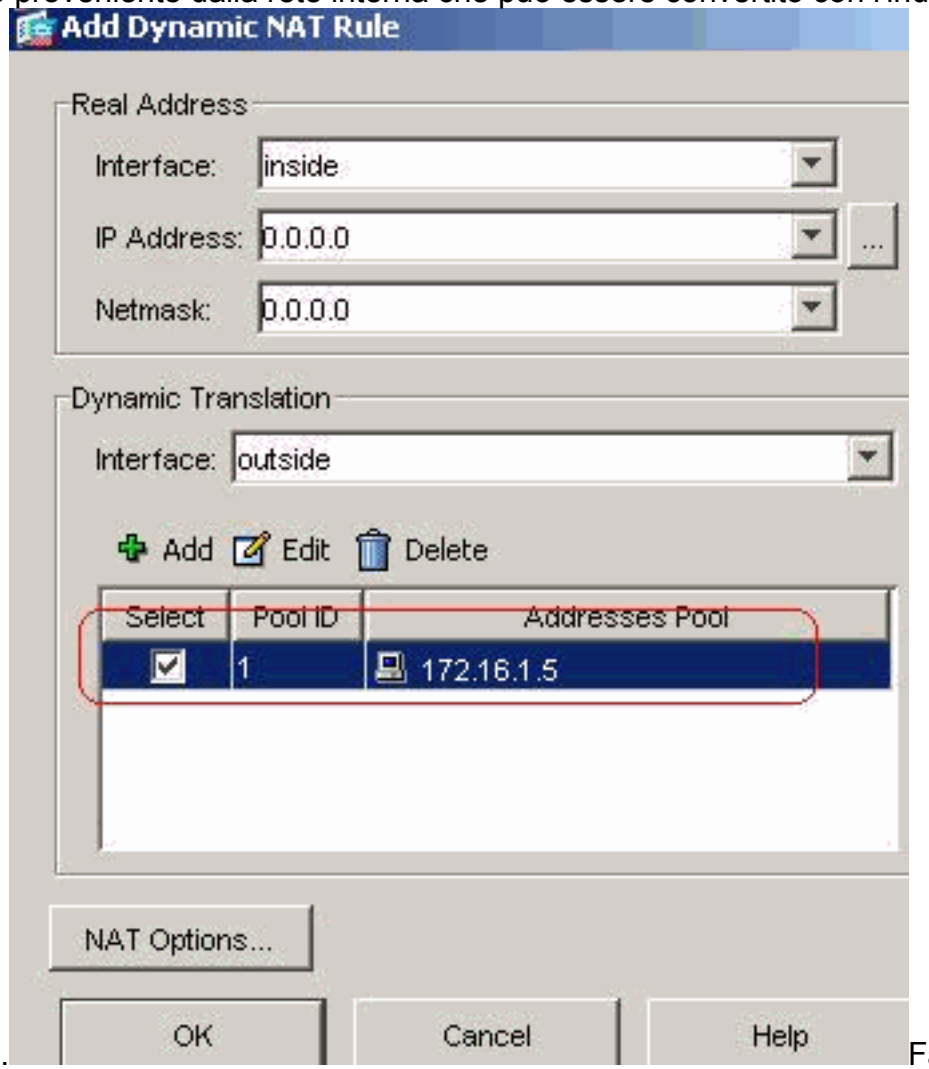


Nella scheda **WebVPN > Alias gruppo e URL**, digitare il nome dell'alias nella casella del parametro e fare clic su **Aggiungi >>** per visualizzarlo nell'elenco dei nomi dei gruppi nella pagina di
accesso.



Fare clic su **OK**, quindi su **Applica**.**Configurazione CLI equivalente:**

8. **Configurazione NAT**Scegliere **Configurazione > NAT > Aggiungi > Aggiungi regola NAT**

dinamica per il traffico proveniente dalla rete interna che può essere convertito con l'indirizzo IP esterno 172.16.1.5. 

Fare clic su **OK**, quindi su **Applica** nella pagina principale.**Configurazione CLI equivalente:**

9. Configurare l'esenzione nat per il traffico di ritorno dalla rete interna al client 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
```

Configurazione di ASA 7.2(2) con 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-
```

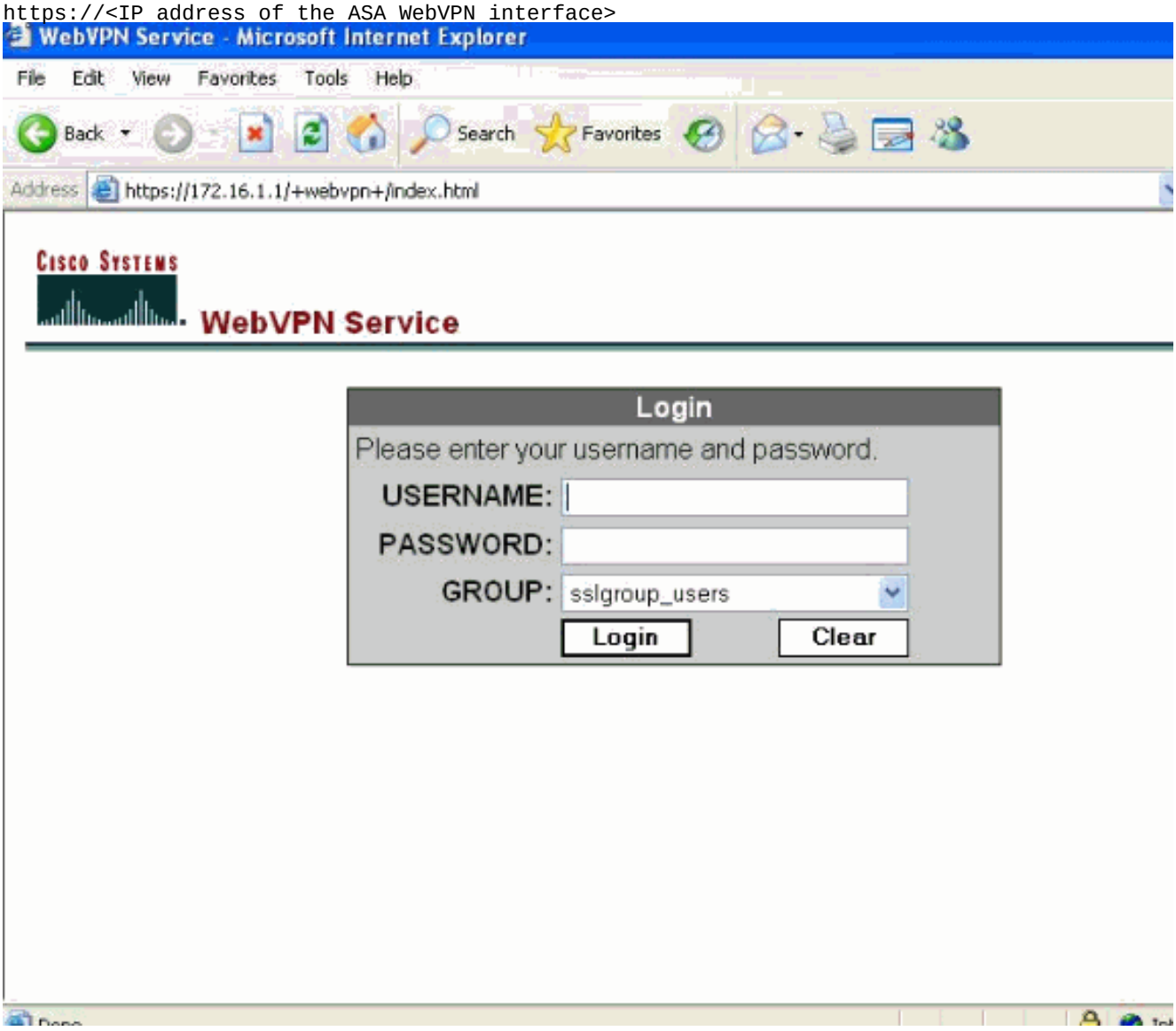
```
policy tunnelspecified
 split-tunnel-network-list value split-tunnel

!--- 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#
```

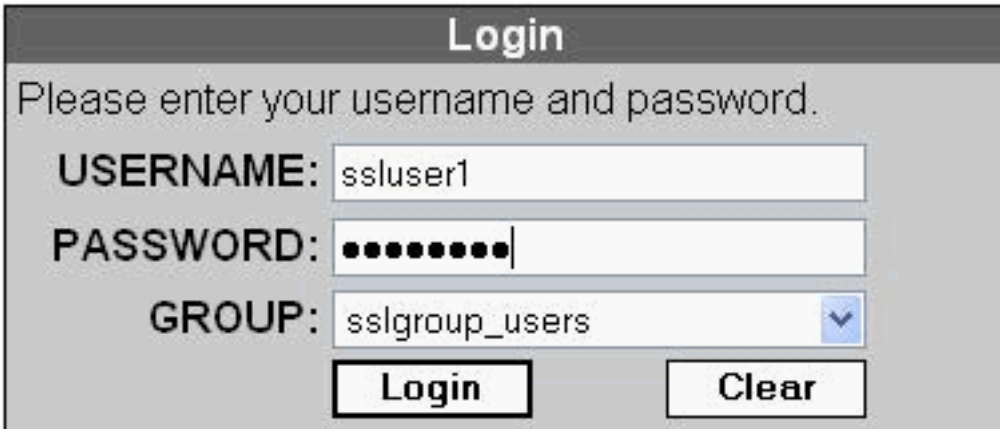
Stabilire la connessione VPN SSL con SVC

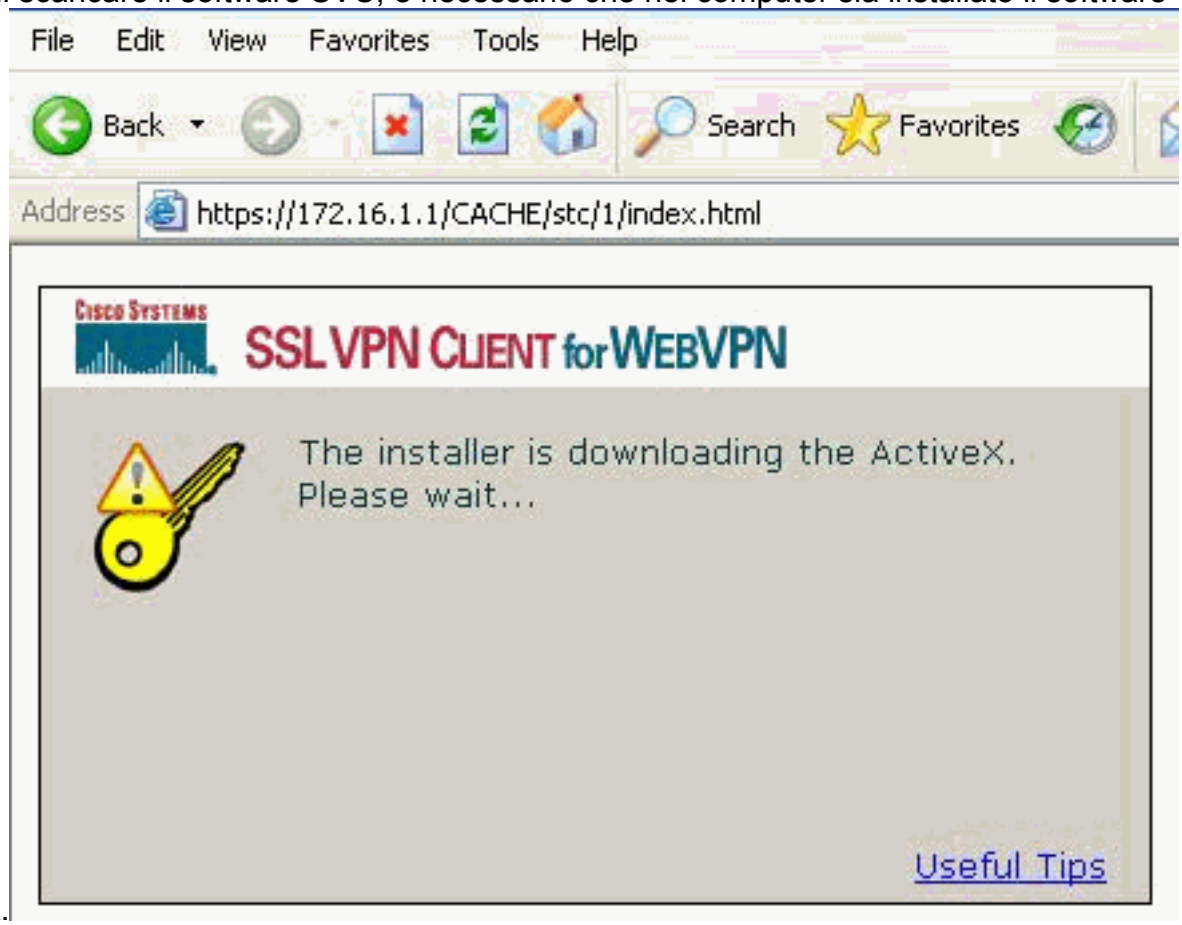
Completare questa procedura per stabilire una connessione VPN SSL con ASA.

1. Digitare l'URL o l'indirizzo IP dell'interfaccia WebVPN dell'ASA nel browser Web nel formato mostrato.
   `https://url`
   O
   `https://<IP address of the ASA WebVPN interface>`



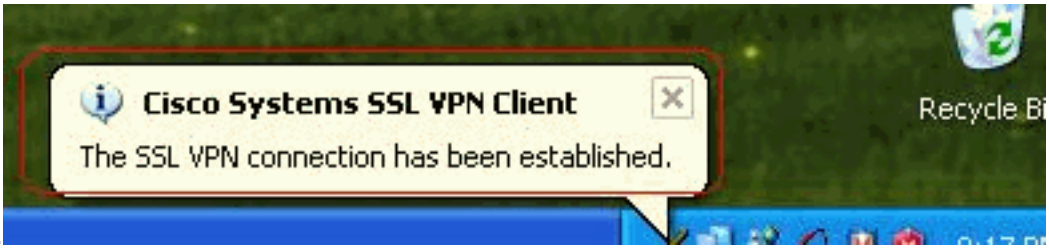
2. Immettere il nome utente e la password, quindi scegliere il gruppo desiderato dall'elenco a discesa come

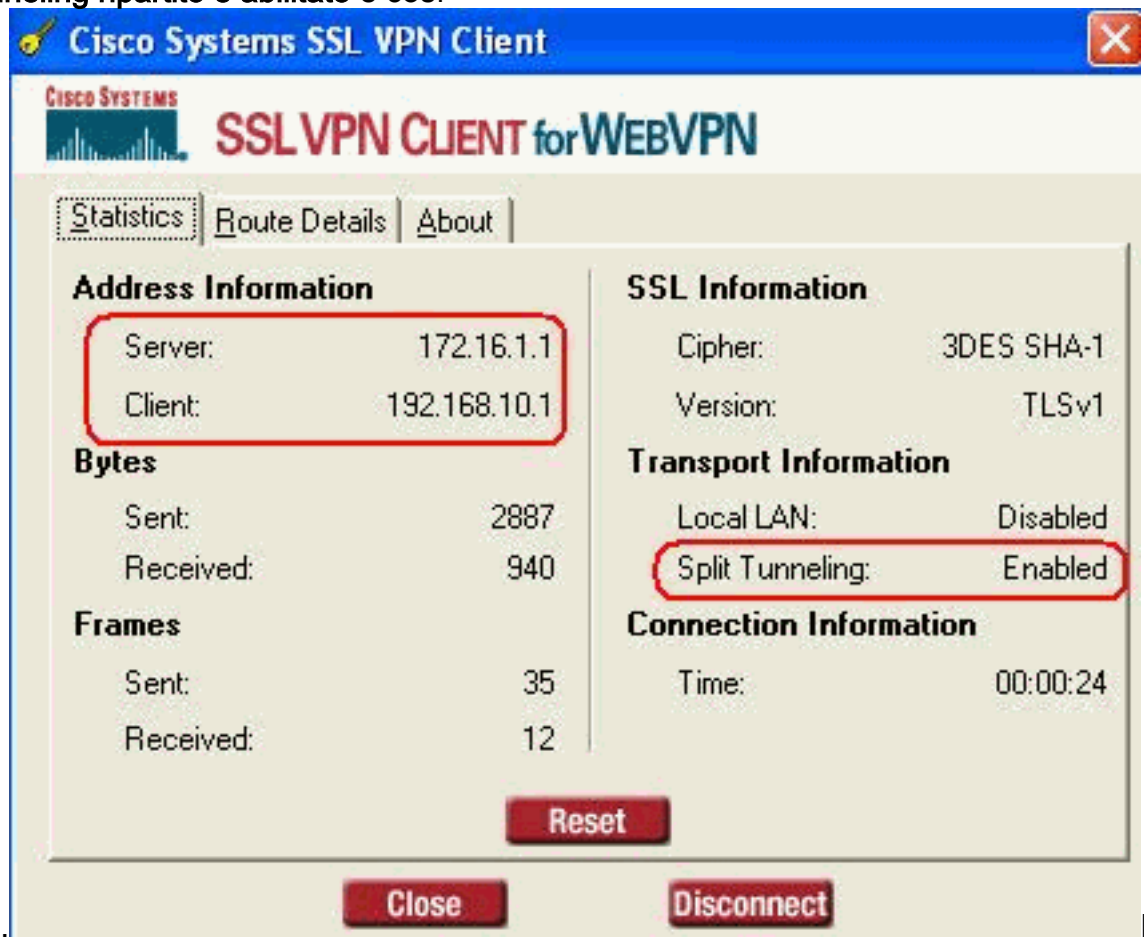
mostrato. 

3. Prima di scaricare il software SVC, è necessario che nel computer sia installato il software ActiveX. 

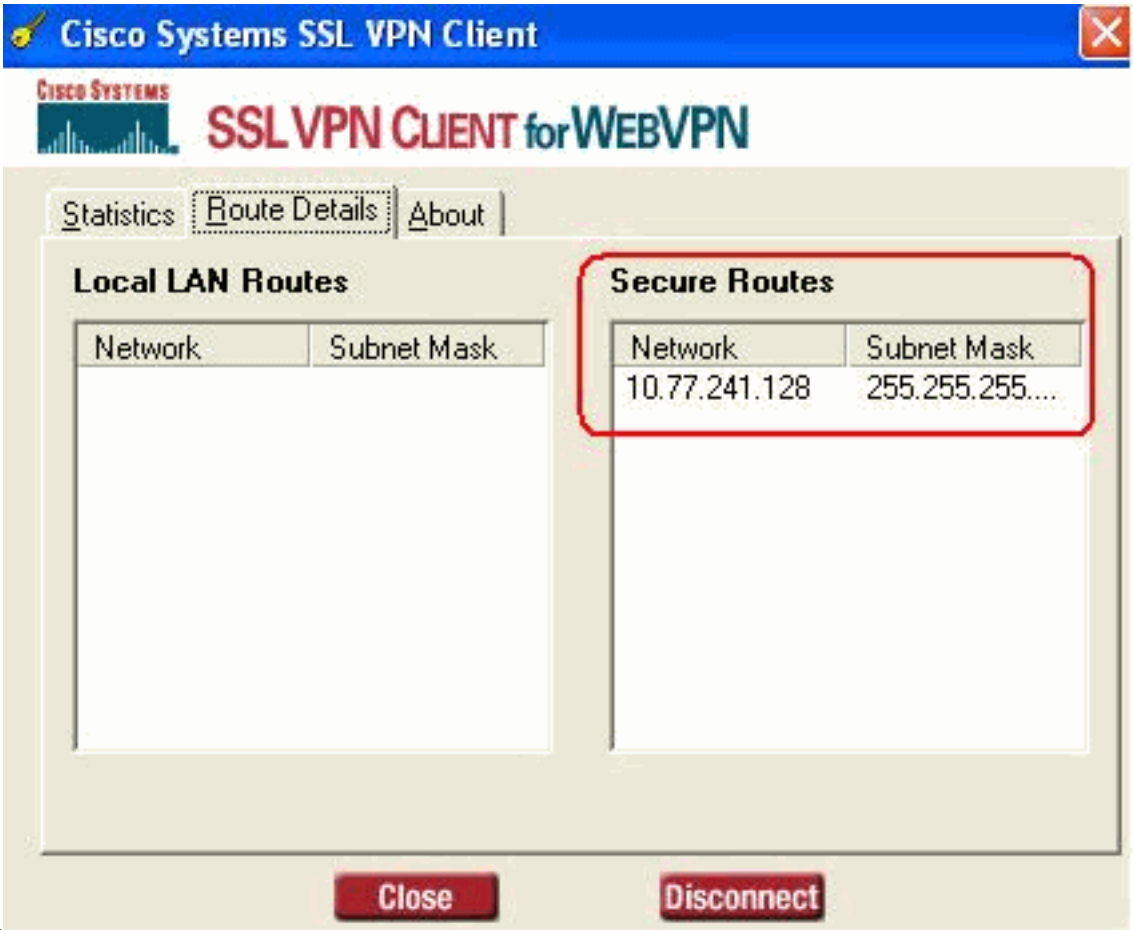
4. Queste finestre vengono visualizzate prima della connessione VPN SSL. 

5. Èpossibile visualizzare queste finestre dopo aver stabilito la

connessione. 

6. Fare clic sul tasto giallo visualizzato nella barra delle applicazioni del computer. Vengono visualizzate queste finestre che forniscono informazioni sulla connessione SSL. Ad esempio, **192.168.10.1** è l'indirizzo IP assegnato per l'indirizzo IP del client e del server è 172.16.1.1, il **tunneling ripartito è abilitato** e così via. 

Inoltre, è possibile controllare la rete protetta che deve essere crittografata con SSL. L'elenco delle reti viene scaricato dall'elenco degli accessi al tunnel separato configurato in ASA.Nell'esempio, il client VPN SSL protegge l'accesso a 10.77.241.128/24, mentre tutto il resto del traffico non viene crittografato e non inviato attraverso il



tunnel.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show webvpn svc**: visualizza le immagini SVC memorizzate nella memoria flash 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
```

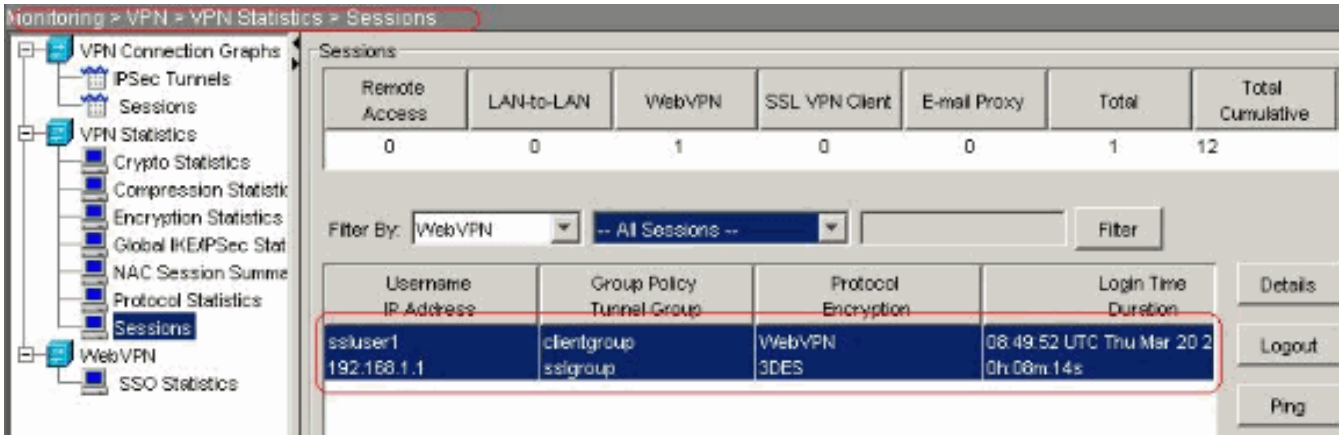
- **show vpn-sessiondb svc**: visualizza le informazioni sulle connessioni SSL correnti.

```
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**: visualizza l'alias configurato per vari gruppi.

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- In ASDM, scegliere **Monitoraggio > VPN > Statistiche VPN > Sessioni** per conoscere le sessioni WebVPN correnti nell'appliance ASA.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

1. **vpn-sessiondb logoff name <nomeutente>**: comando per chiudere la sessione VPN SSL per

il nome utente specifico.

```
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
```

Analogamente, è possibile utilizzare il comando **vpn-sessiondb logoff svc** per terminare tutte le sessioni SVC.

2. **Nota:** se il PC passa alla modalità standby o sospensione, la connessione VPN SSL può essere interrotta.

```
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
```

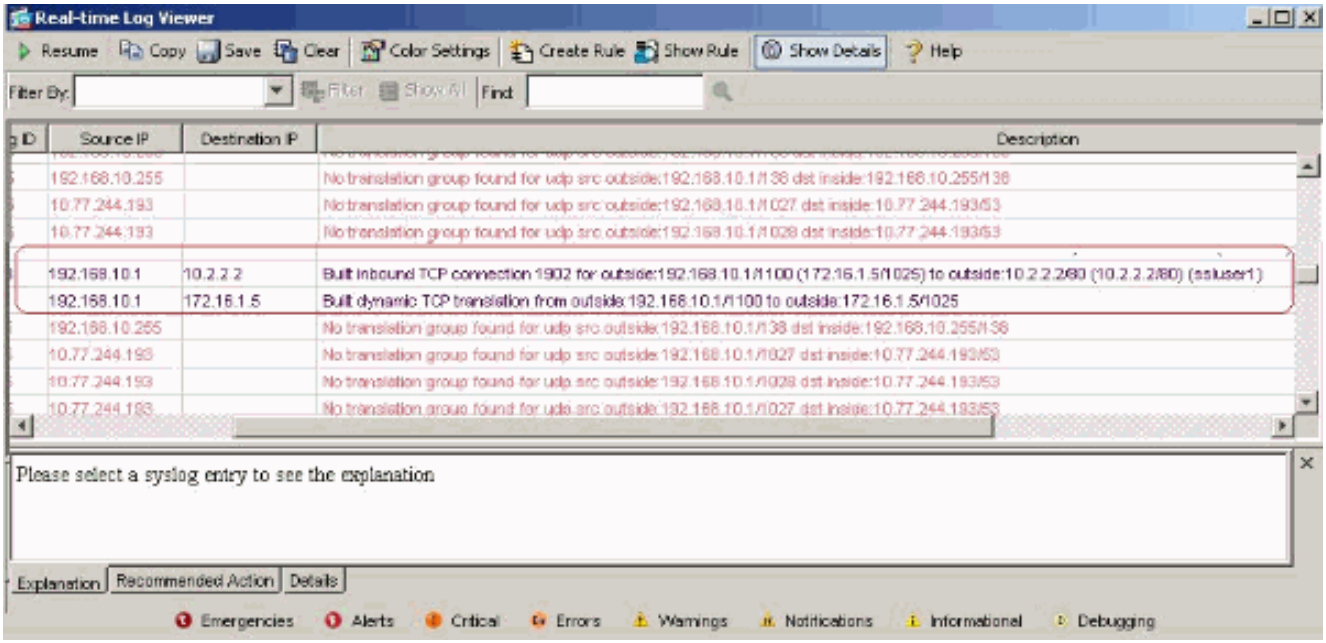
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

3. **Debug webvpn svc <1-255>**: fornisce gli eventi webvpn in tempo reale per stabilire la sessione.

```
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, scegliere **Monitoraggio > Log > Visualizzatore log in tempo reale > Visualizza** per visualizzare gli eventi in tempo reale. Nell'esempio vengono mostrate le informazioni sulla sessione tra SVC 192.168.10.1 e Webserver 10.2.2.2 in Internet tramite ASA 172.16.1.5.



Informazioni correlate

- Cisco serie 5500 Adaptive Security Appliance - Supporto dei prodotti
- ASA/PIX: Esempio di configurazione dell'appliance ASA che consente il tunneling ripartito per i client VPN
- Il router consente ai client VPN di connettersi a IPsec e a Internet utilizzando un esempio di configurazione del tunneling ripartito
- Esempio di configurazione di PIX/ASA 7.x e VPN Client per VPN Internet pubblica su Memory Stick
- Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM
- Documentazione e supporto tecnico – Cisco Systems