ASA 7.2(2): Esempio di configurazione su Memory Stick del client VPN SSL (SVC) per VPN Internet pubblica

Sommario

Introduzione

In questo documento viene descritto come configurare un'appliance ASA (Adaptive Security Appliance) 7.2.2 per eseguire una VPN SSL su un stick. Questa configurazione è valida in un caso specifico in cui l'ASA non consente il tunneling di split e gli utenti si connettono direttamente all'ASA prima di essere autorizzati a connettersi a Internet.

Nota: nell'ASA versione 7.2.2, la parola chiave *intra-interface* del comando **same-security-traffic-allow** configuration mode permette a tutto il traffico di entrare e uscire dalla stessa interfaccia (non solo dal traffico IPsec).

Prerequisiti

Requisiti

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

- Hub ASA Security Appliance deve eseguire la versione 7.2.2
- Cisco SSL VPN Client (SVC) 1.x**Nota:** scaricare il pacchetto SSL VPN Client (sslclient-win*.pkg) da Cisco Software Download (solo utenti registrati). Copiare lo SVC sulla memoria

flash dell'appliance ASA. Per stabilire la connessione VPN SSL con l'appliance ASA, l'SVC deve essere scaricato sui computer degli utenti remoti. Per ulteriori informazioni, consultare la sezione Installazione del software SVC nella *guida alla configurazione della riga di comando di Cisco Security Appliance, versione 7.2*.

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
- PC con Windows 2000 Professional o Windows XP
- 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 l'utente soddisfa i requisiti di accesso e autenticazione e l'appliance di sicurezza identifica l'utente come utente che richiede l'SVC, l'appliance di sicurezza scarica l'SVC sul computer remoto. Se l'appliance di sicurezza identifica che l'utente ha la possibilità di utilizzare l'SVC, l'appliance di sicurezza scarica l'SVC sul computer remoto presentando un collegamento nella schermata utente per saltare l'installazione dell'SVC.

Dopo il download, l'SVC si installa e si configura automaticamente, quindi l'SVC rimane o si disinstalla automaticamente dal computer remoto (a seconda della configurazione) al termine della connessione.

Configurazione

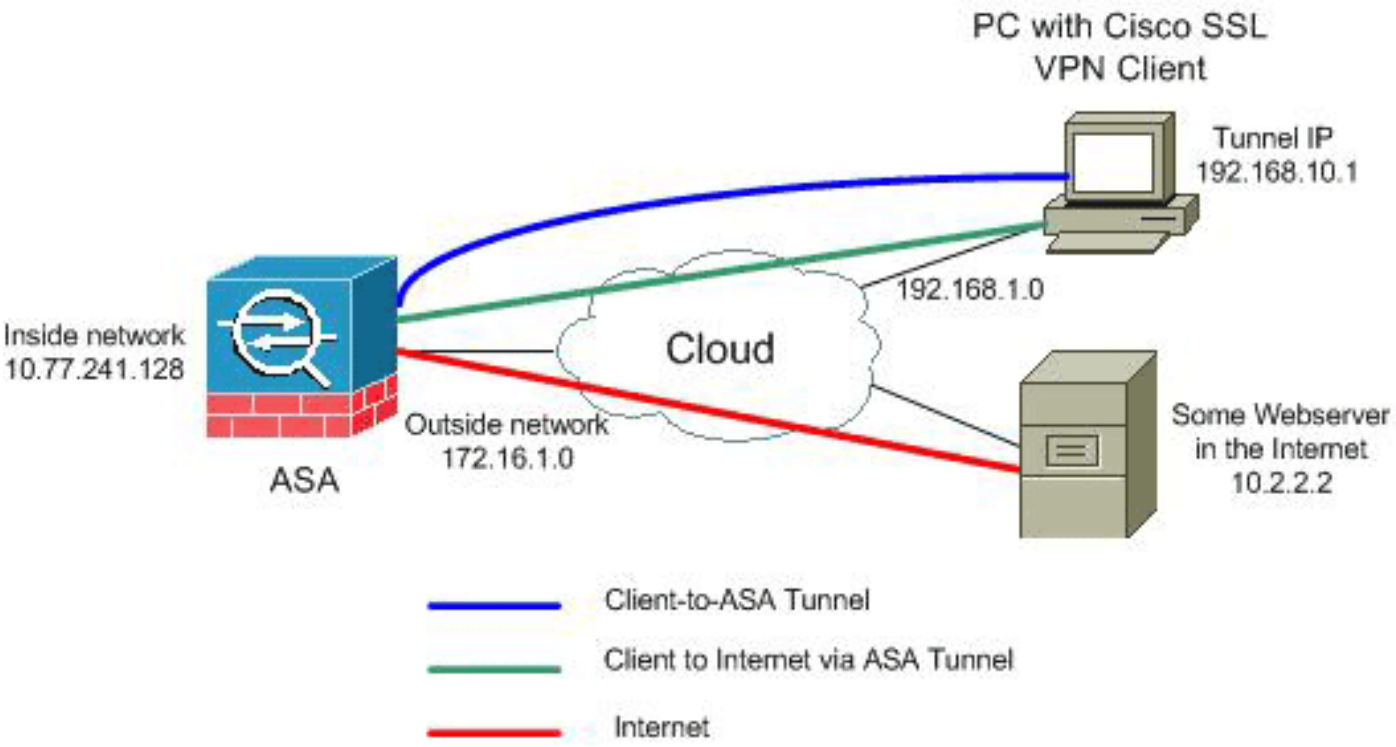
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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 7.2(2) con ASDM 5.2(2)

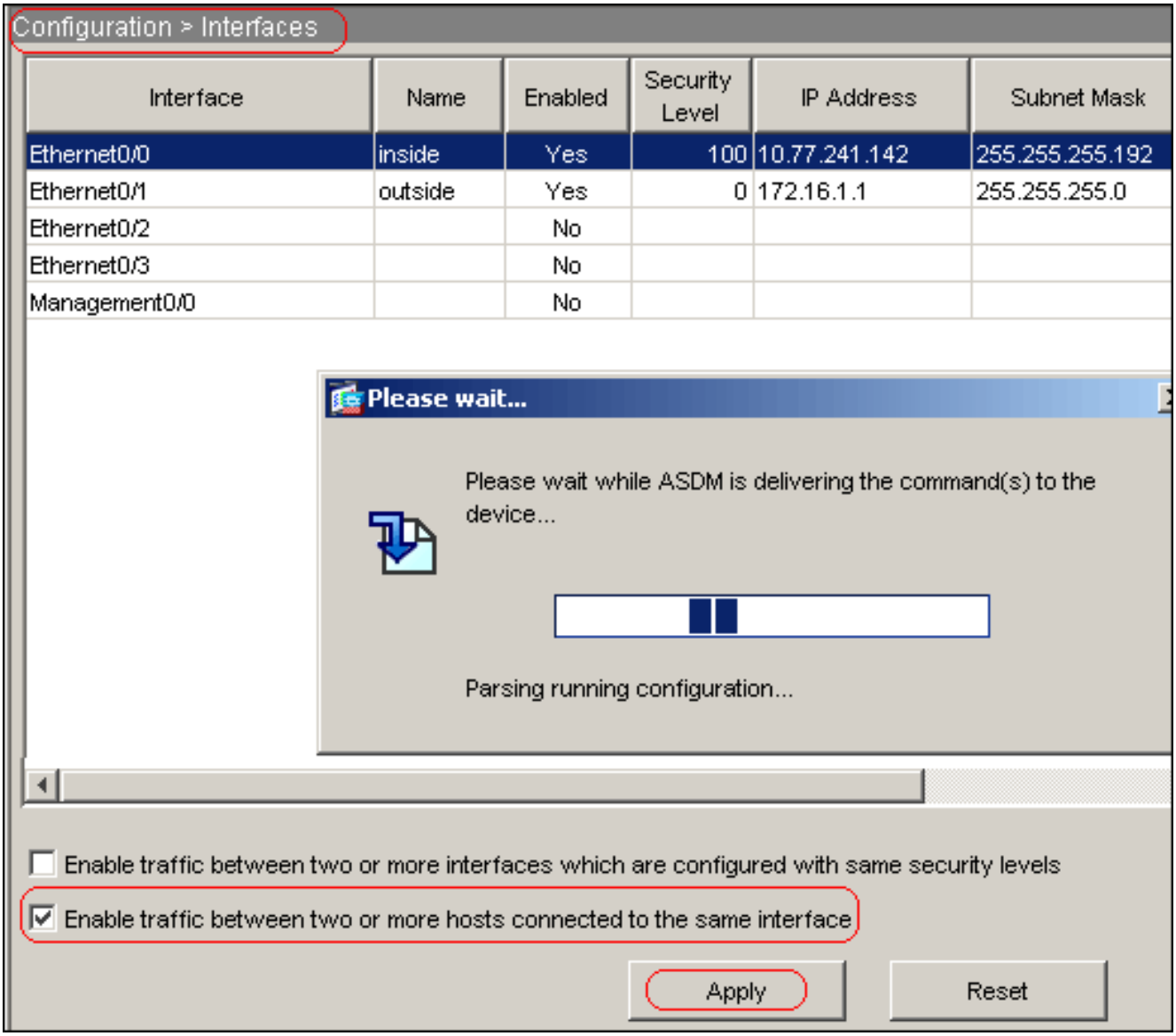
In questo documento si presume che le configurazioni di base, ad esempio la configurazione dell'interfaccia, siano già state create e funzionino correttamente.

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.

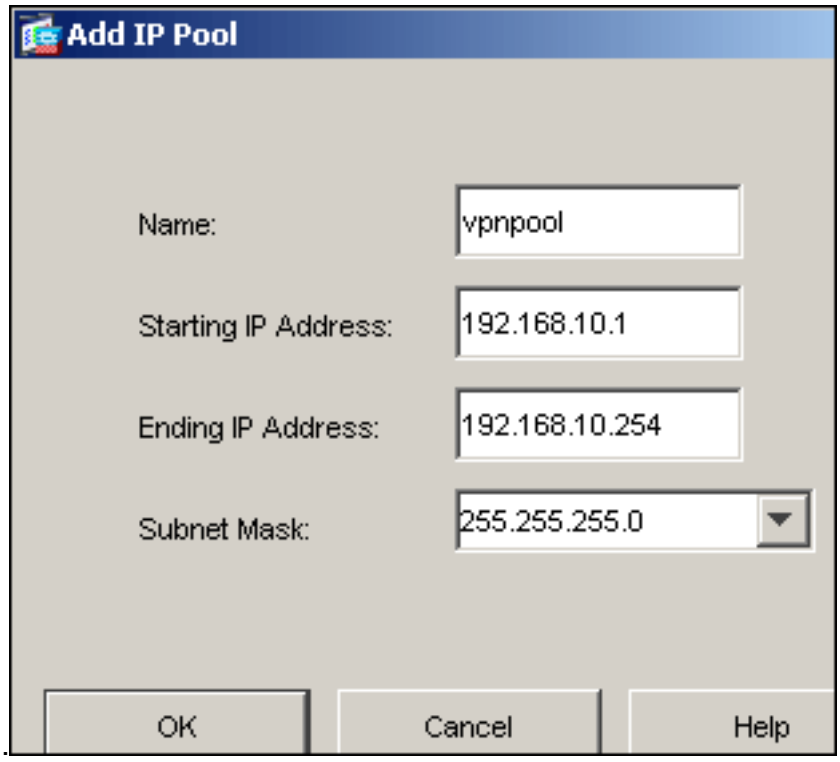
Per configurare la VPN SSL su uno stick nell'appliance ASA, completare la procedura seguente:

1. Scegliere **Configurazione > Interfacce** e selezionare la casella di controllo **Abilita traffico tra due o più host connessi alla stessa interfaccia** per consentire al traffico VPN SSL di entrare e uscire dalla stessa interfaccia.
2. Fare clic su **Apply**
   (Applica).



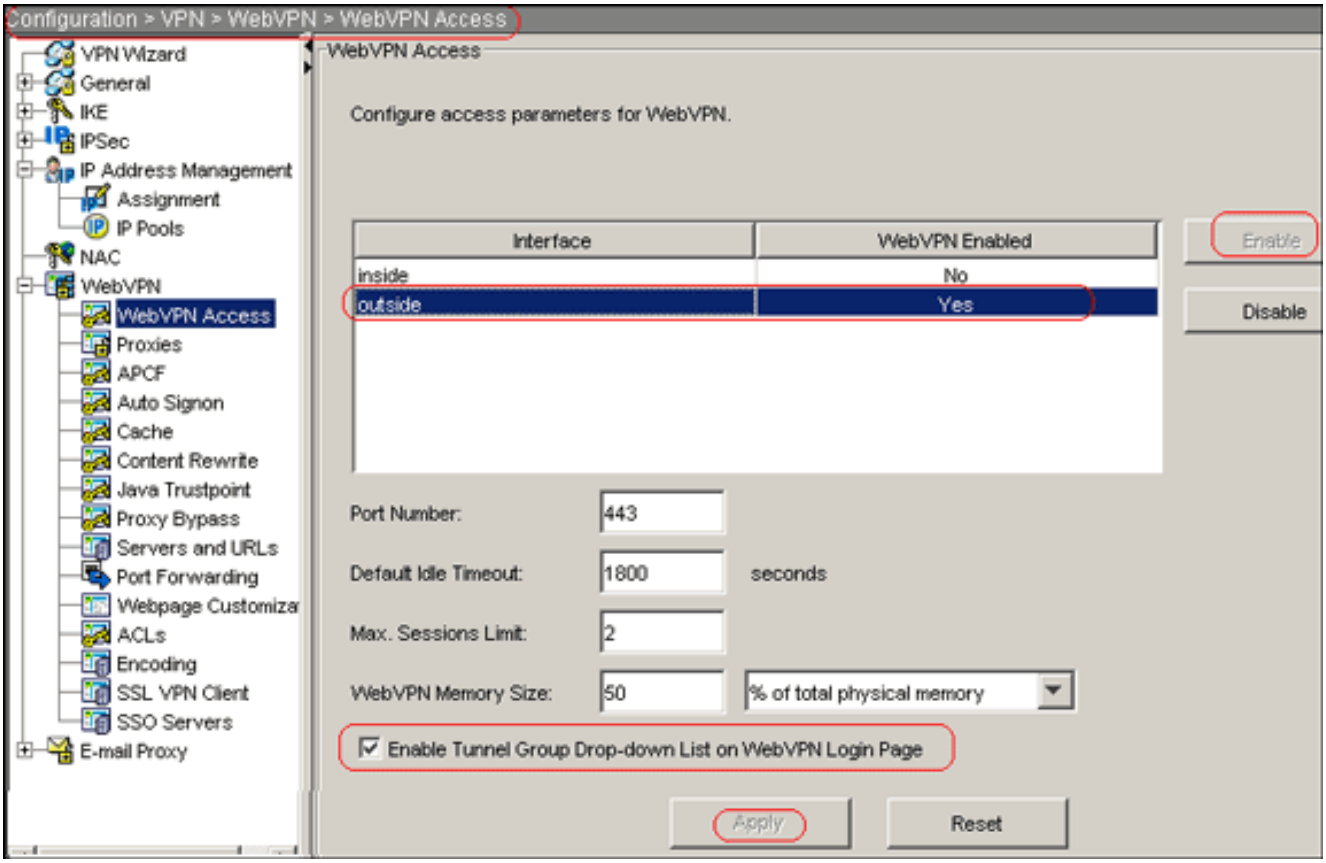
Nota: di seguito è riportato il comando di configurazione CLI equivalente:

3. Per creare un pool di indirizzi IP denominato *vpnpool*, scegliere **Configurazione > VPN > Gestione indirizzi IP > Pool di indirizzi IP >**

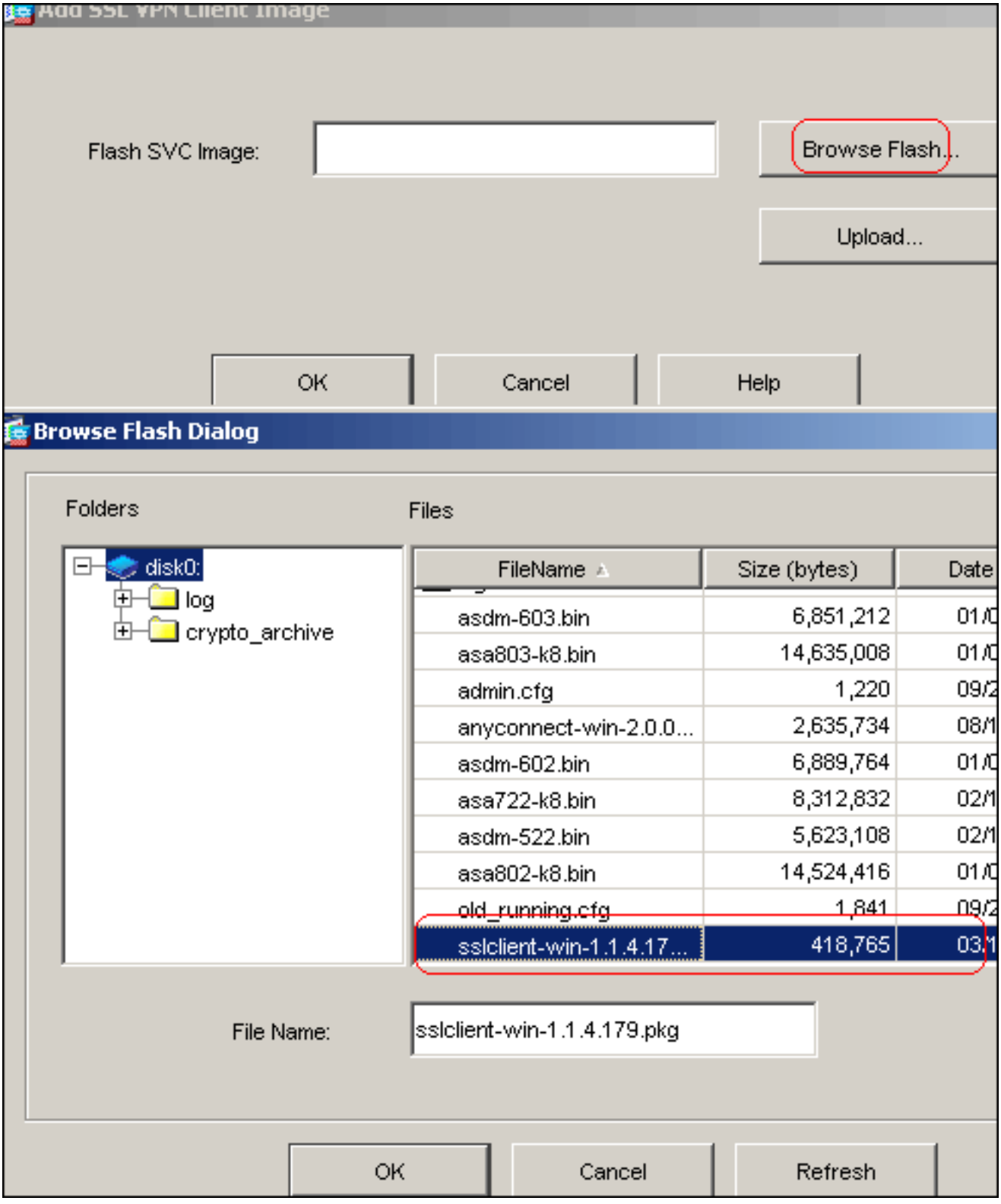


Aggiungi.

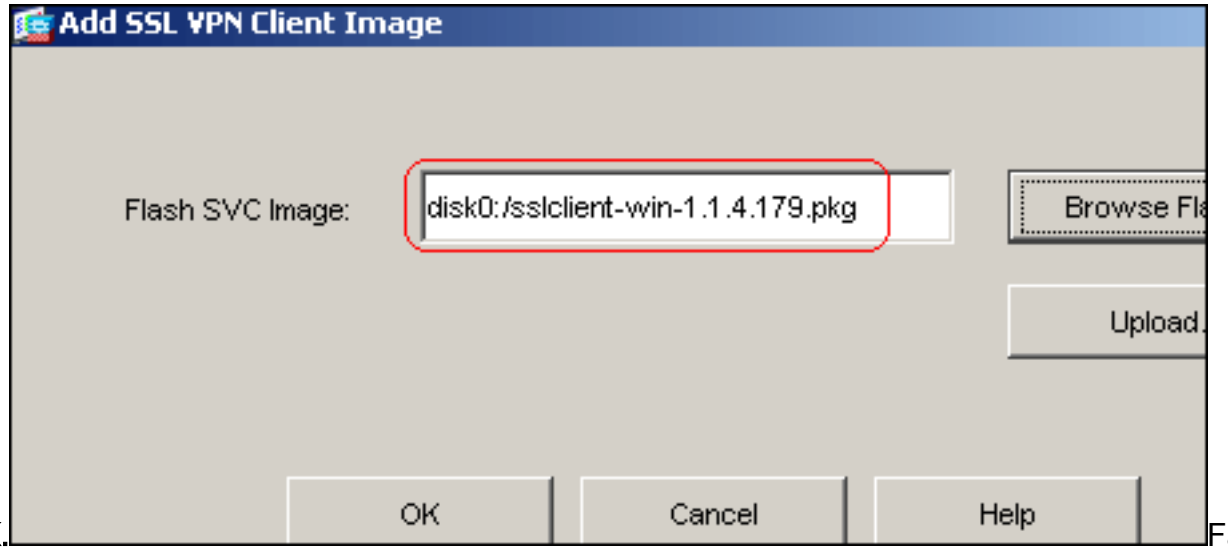
4. Fare clic su **Apply** (Applica).**Nota:** di seguito è riportato il comando di configurazione CLI equivalente:
5. Abilita WebVPN:Scegliere **Configurazione > VPN > WebVPN > Accesso WebVPN**, quindi selezionare l'interfaccia esterna.Fare clic su **Attiva**.Selezionare la casella di controllo **Abilita elenco a discesa gruppi tunnel nella pagina di accesso WebVPN** per consentire agli utenti di scegliere i rispettivi gruppi dalla pagina di accesso.



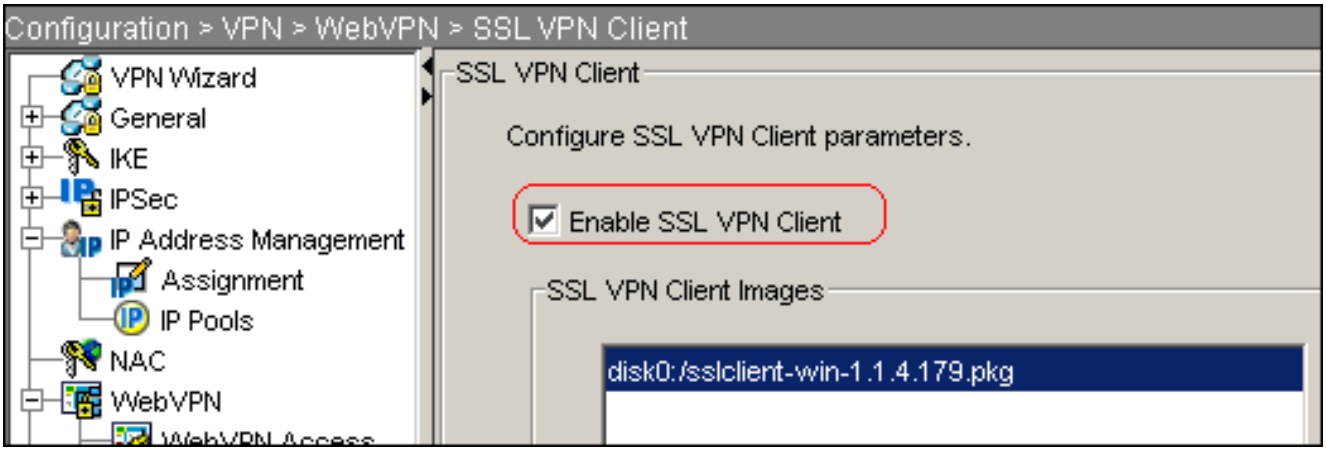
Fare clic su **Apply** (Applica).Per aggiungere l'immagine SSL VPN Client dalla memoria flash dell'ASA, scegliere **Configurazione > VPN > WebVPN > SSL VPN Client > Aggiungi**.


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
asa803-k8.bin 14,635,008
admin.cfg 1,220
anyconnect-win-2.0.0... 2,635,734
asdm-602.bin 6,889,764
asa722-k8.bin 8,312,832
asdm-522.bin 5,623,108
asa802-k8.bin 14,524,416
old_running.cfg 1,841
sslclient-win-1.1.4.17... 418,765
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

Fare clic su

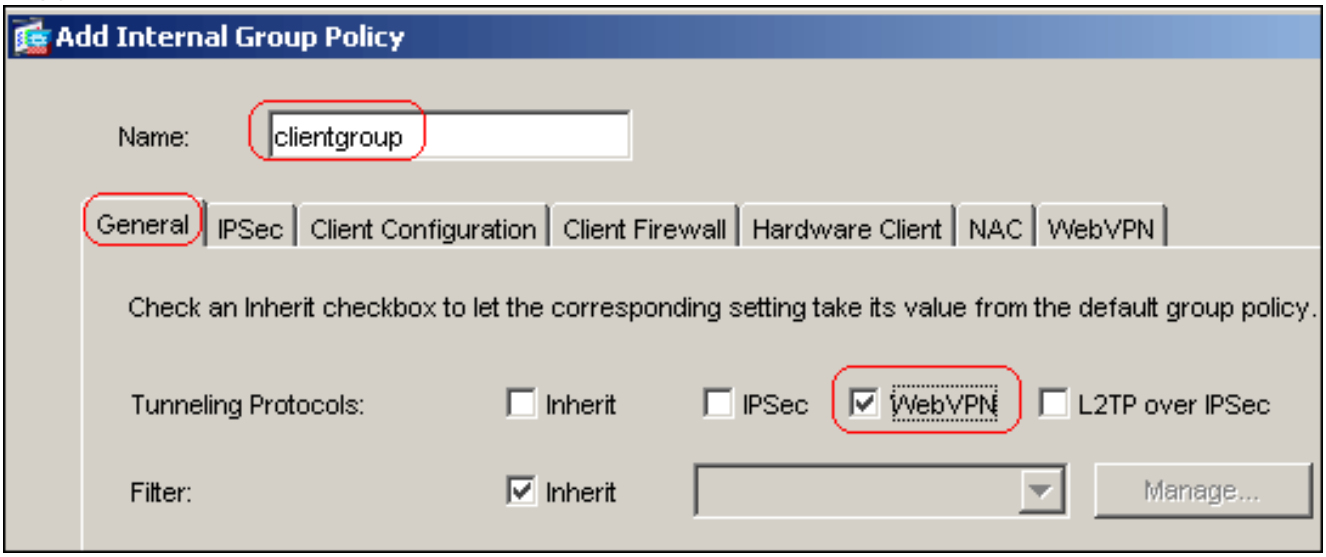


OK.Fare clic su **OK**.Selezionare la casella di controllo **SSL VPN Client**.



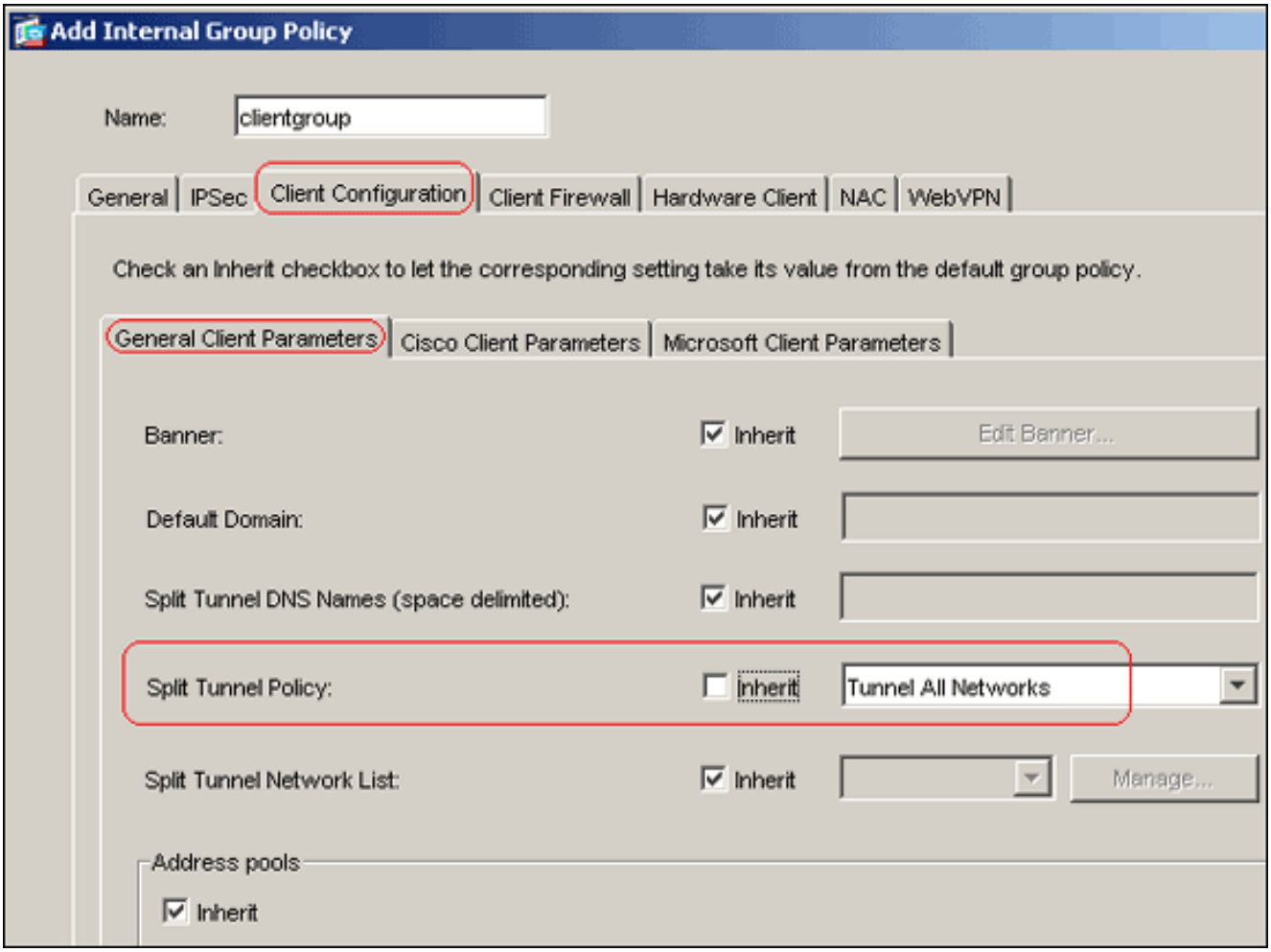
Nota: di seguito sono riportati i comandi di configurazione CLI equivalenti:

6. Configurare i Criteri di gruppo:Per creare un criterio di gruppo interno denominato *gruppo client,* scegliere **Configurazione > VPN > Generale > Criteri di gruppo > Aggiungi (Criteri di gruppo interni)**.Per abilitare WebVPN come protocollo di tunneling, fare clic sulla scheda **Generale** e selezionare la casella di controllo **WebVPN**.

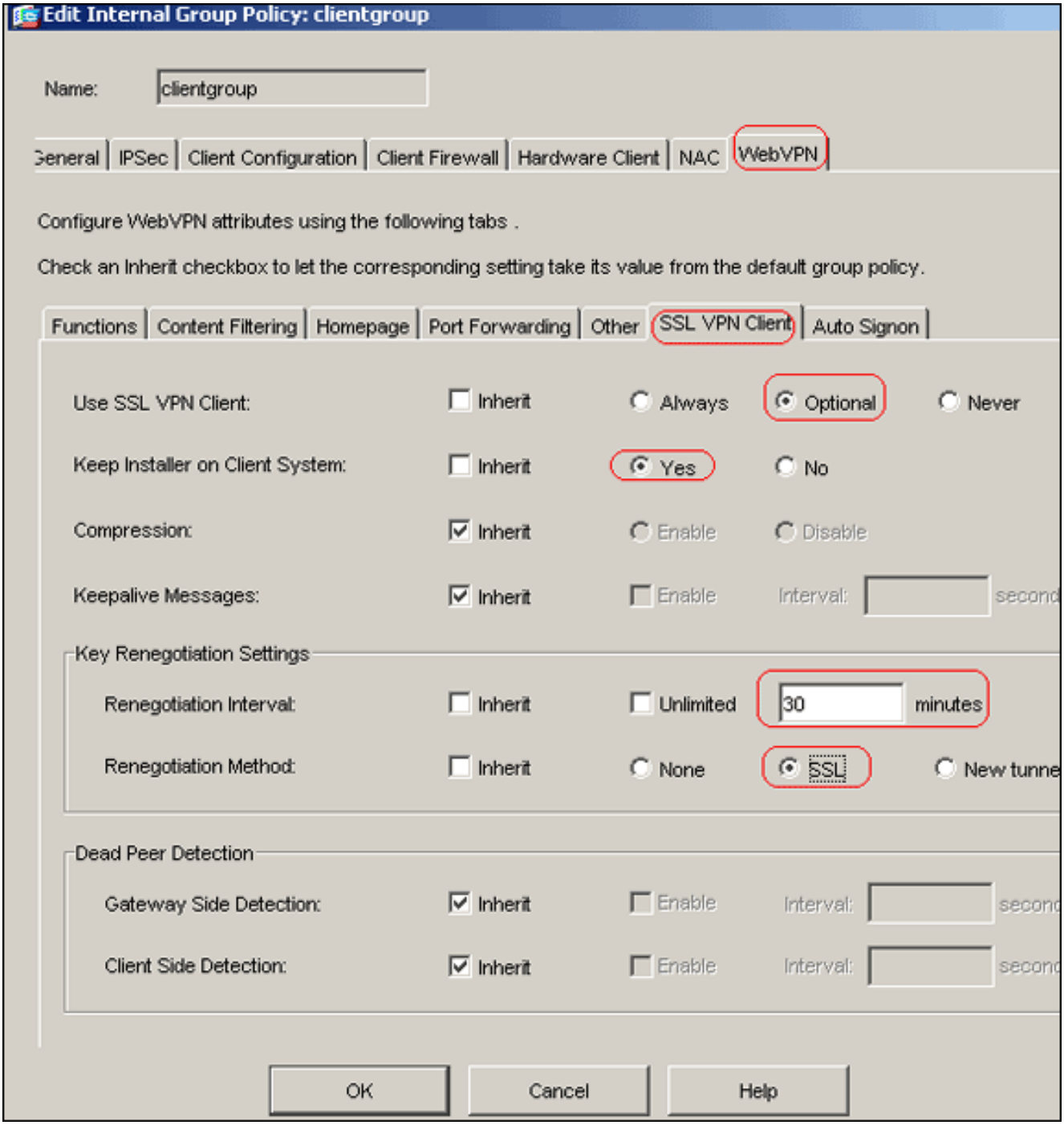


Fare clic sulla scheda **Configurazione client** e quindi sulla scheda **Parametri generali client**.Selezionare **Tunnel All Networks** (Tutte le reti del tunnel) dall'elenco a discesa Split Tunnel Policy (Criterio tunnel diviso) per consentire a tutti i pacchetti di viaggiare dal PC

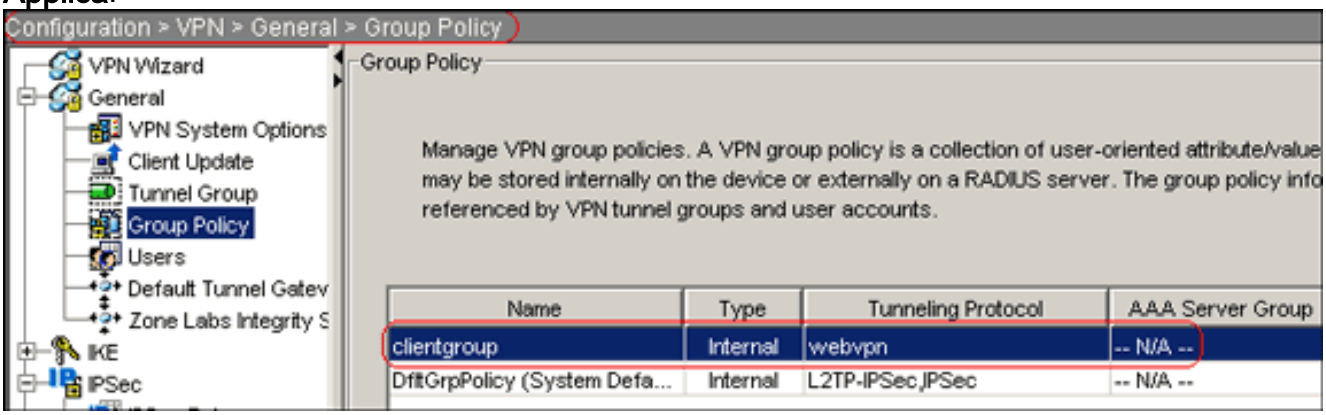
remoto attraverso un tunnel
sicuro.



Fare clic sulla scheda **WebVPN > SSL VPN Client** e scegliere le opzioni seguenti: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 scaricare o meno l'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 opzione consente al software SVC di rimanere sul computer client. Pertanto, ogni volta che si effettua una connessione, l'ASA non deve scaricare il software SVC sul client. 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.**Nota:** la protezione viene migliorata impostando limiti sulla durata di validità di una chiave.Per l'opzione Metodo rinegoziazione, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **SSL**.**Nota: la** rinegoziazione può utilizzare il tunnel SSL corrente o un nuovo tunnel creato appositamente per la rinegoziazione.Gli attributi del client VPN SSL devono essere configurati come mostrato in questa
immagine:



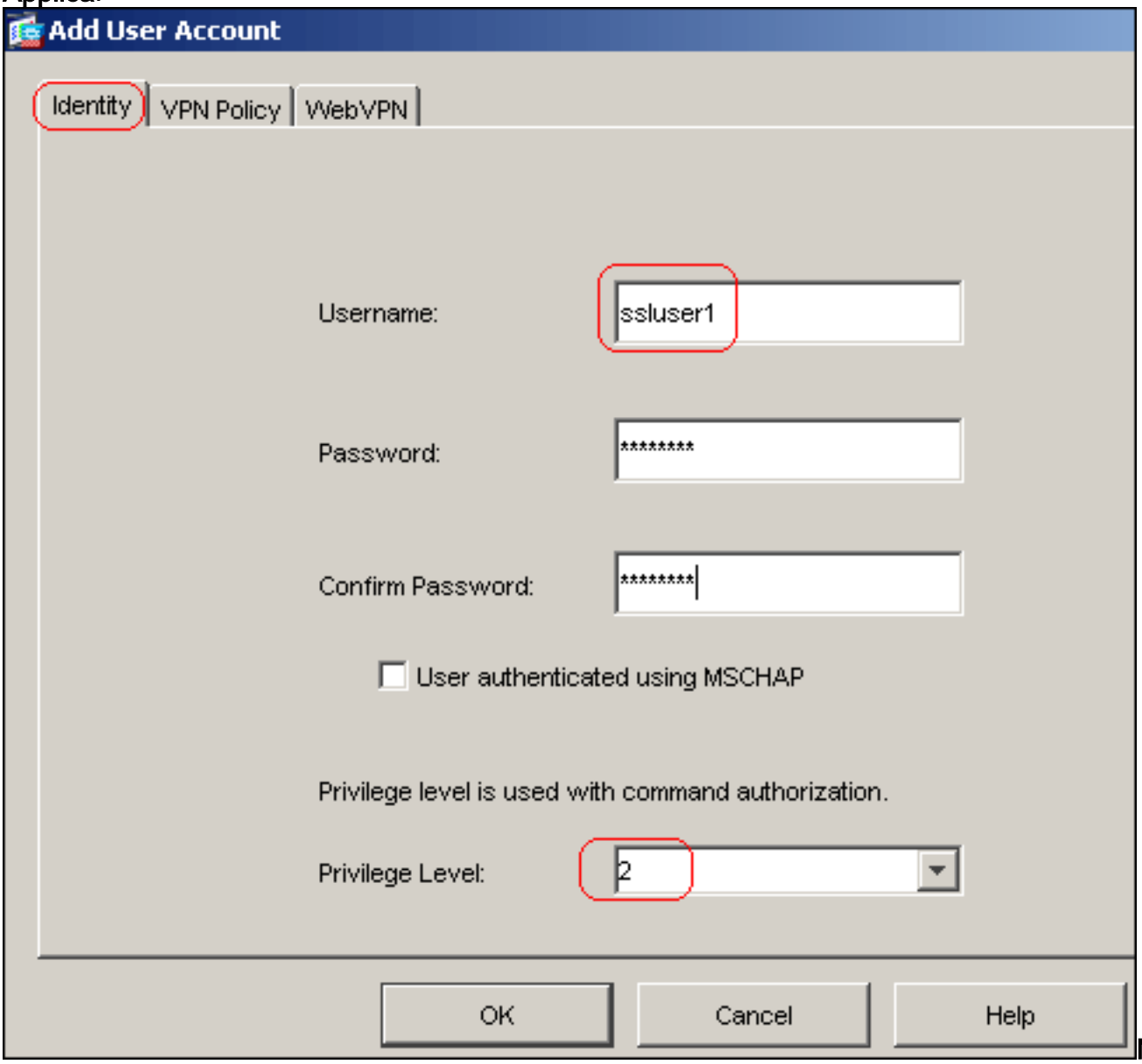
Fare clic su **OK**, quindi su **Applica**.



Nota: di seguito sono riportati i comandi di configurazione CLI equivalenti:

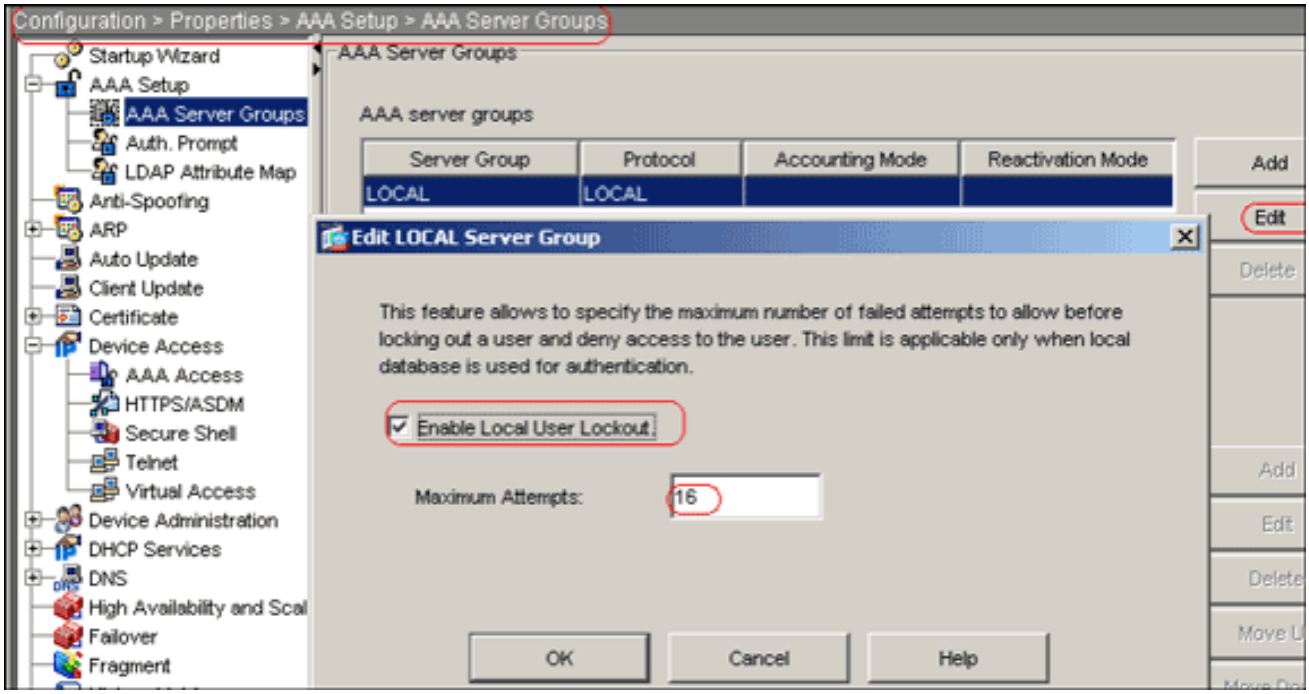
7. Per creare un nuovo account utente *ssluser1*, scegliere **Configurazione > VPN > Generale > Utenti > Aggiungi**.

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



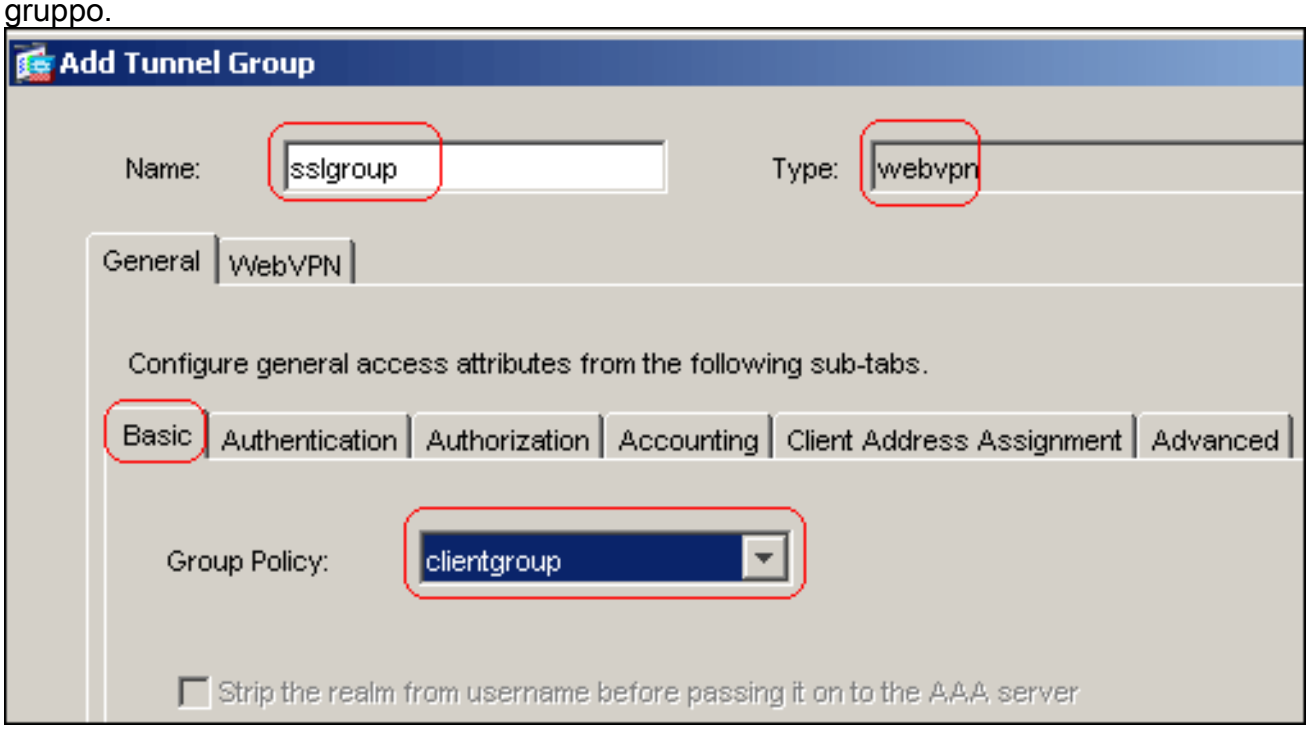
Nota: di seguito è riportato il comando CLI equivalente:

9. Scegliere **Configurazione > Proprietà > Impostazione AAA > Gruppi di server AAA > Modifica**.
10. Selezionare il gruppo di server predefinito *LOCAL*, quindi fare clic su **Modifica**.
11. Nella finestra di dialogo Modifica gruppo di server LOCALE selezionare la casella di controllo **Attiva blocco utente locale** e immettere 16 nella casella di testo Numero massimo di tentativi.
12. Fare clic su **OK**.

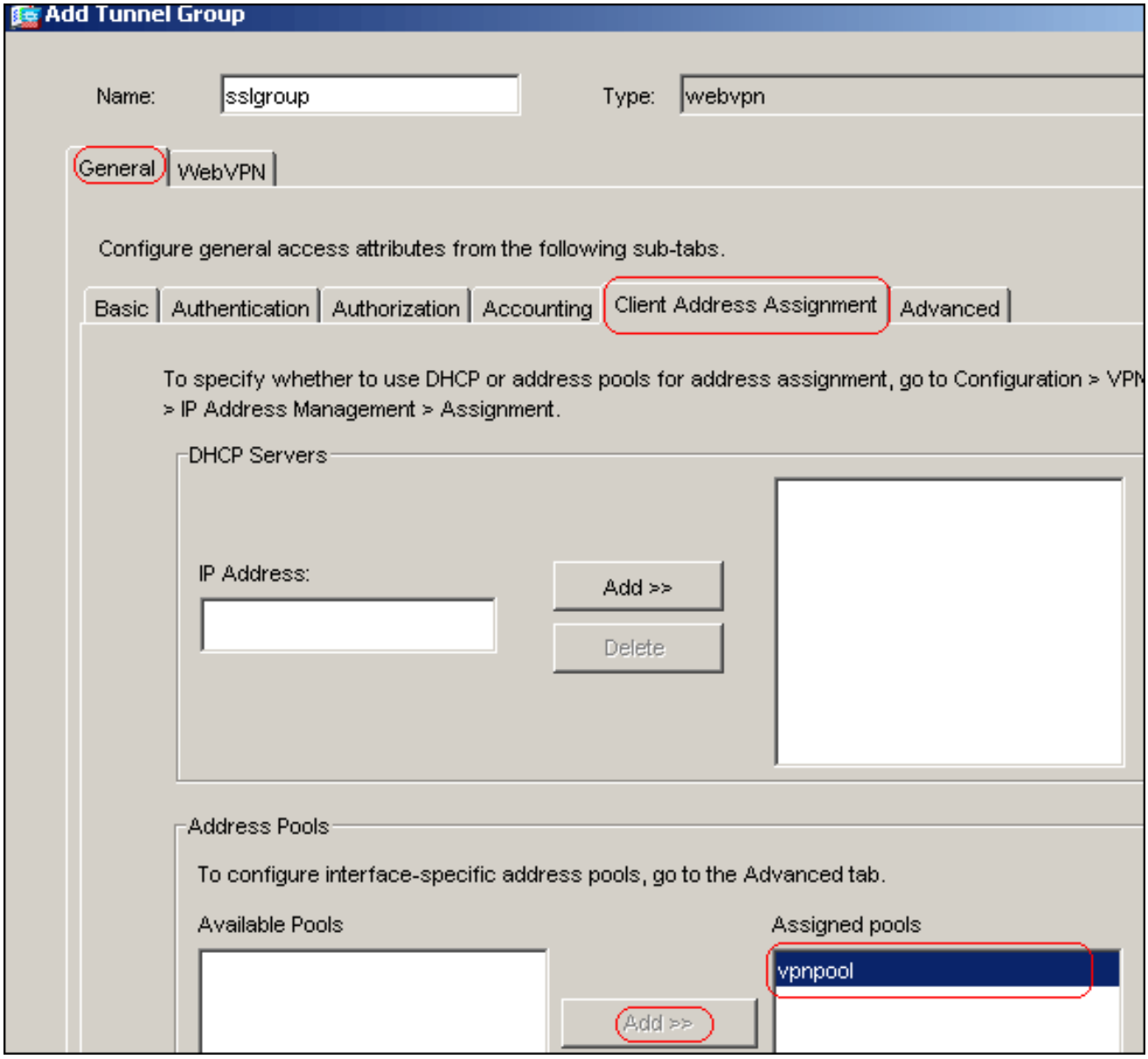


Nota: di seguito è riportato il comando CLI equivalente:

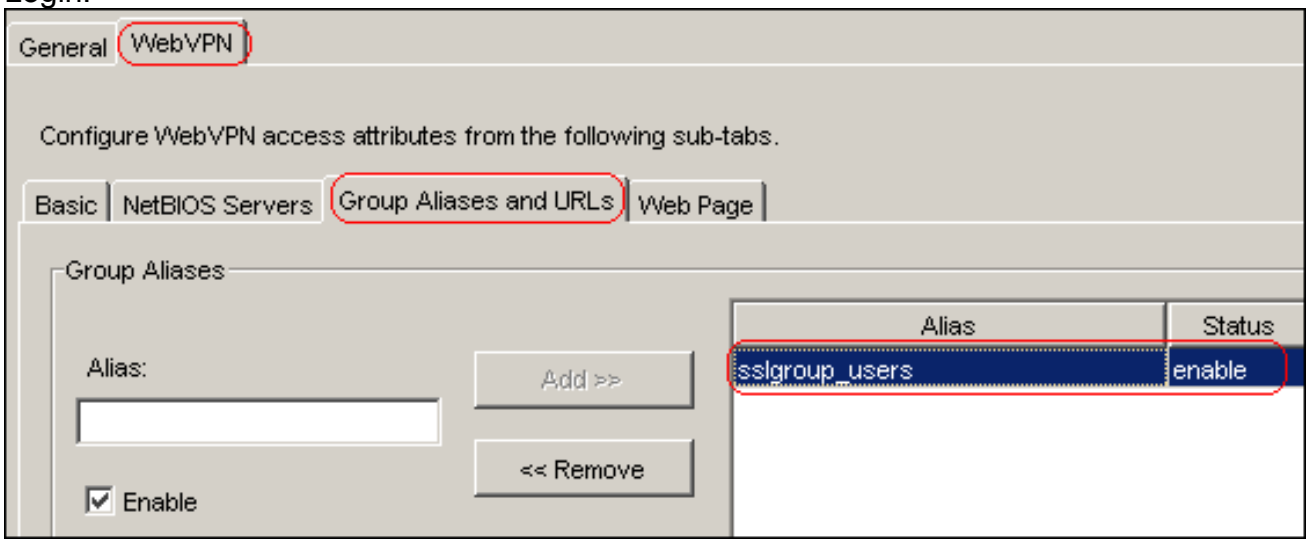
13. Configurare il gruppo di tunnel:Scegliere **Configurazione > VPN > Generale > Gruppo di tunnel > Aggiungi (accesso WebVPN)** per creare un nuovo gruppo di tunnel denominato *sslgroup*.Fare clic sulla scheda **Generale** e quindi sulla scheda **Generale**.Selezionare **clientgroup** dall'elenco a discesa Criteri di gruppo.



Fare clic sulla scheda **Assegnazione indirizzo client** e quindi su **Aggiungi** per assegnare il pool di indirizzi disponibile *vpnpool*.



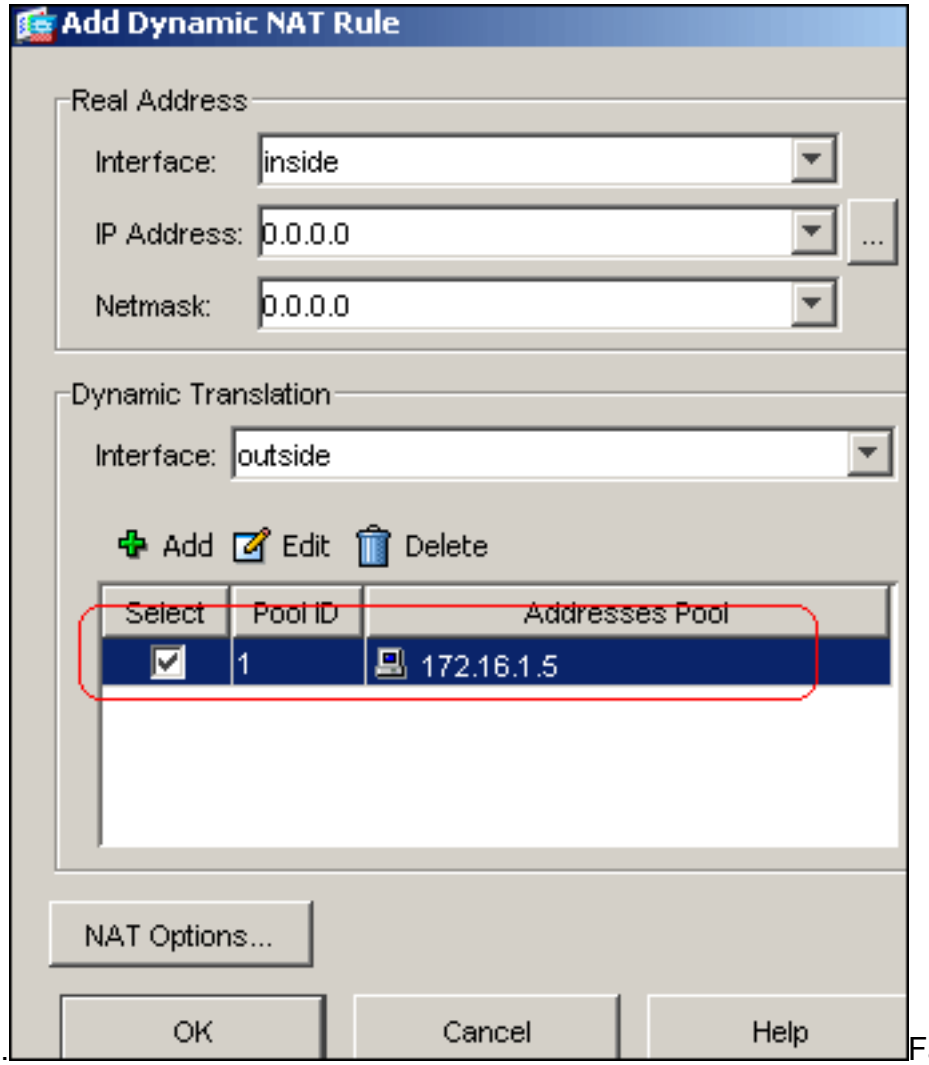
Fare clic sulla scheda **WebVPN** e quindi sulla scheda **Raggruppa alias e URL**.Digitare il nome dell'alias nella casella del parametro e fare clic su **Add** (Aggiungi) per aggiungerlo all'elenco dei nomi dei gruppi nella pagina
Login.



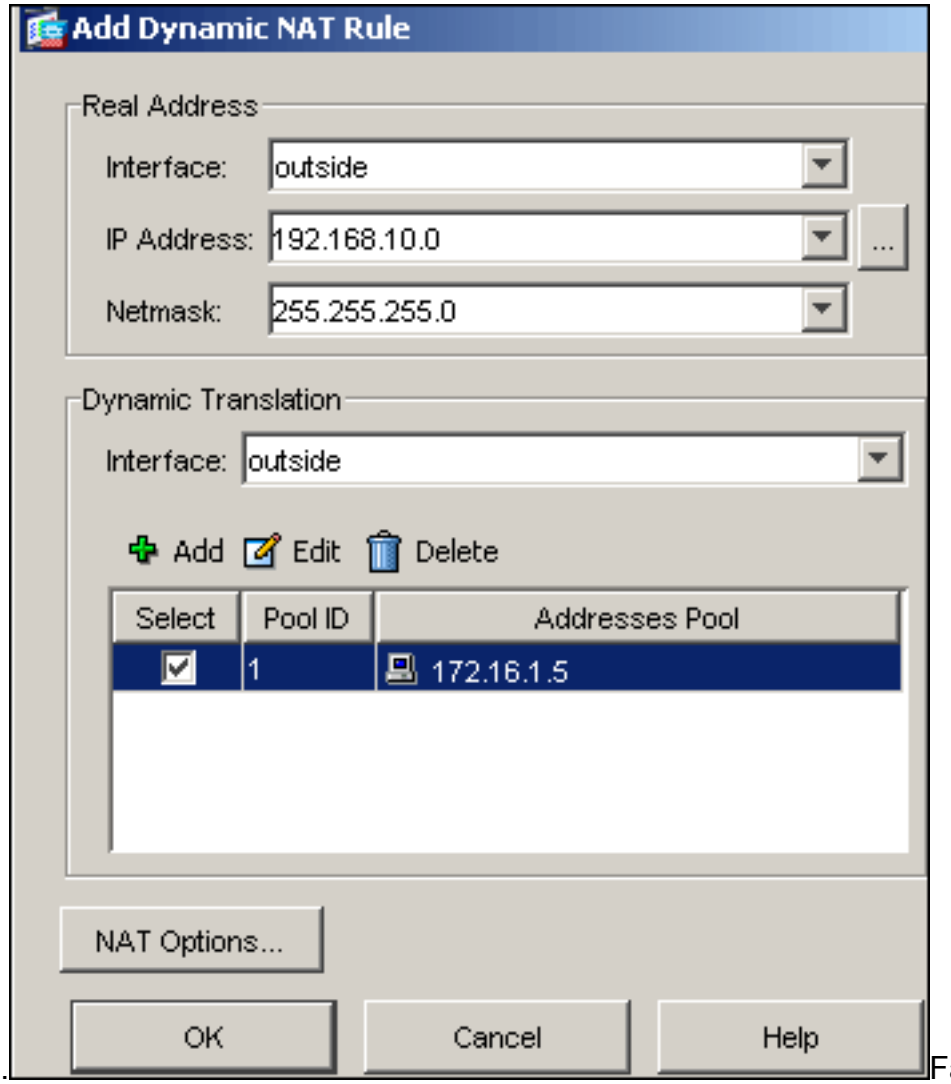
Fare clic su **OK**, quindi su **Applica**.**Nota:** di seguito sono riportati i comandi di configurazione CLI equivalenti:

14. Configurare NAT:Scegliere **Configurazione > NAT > Aggiungi > Aggiungi regola NAT**

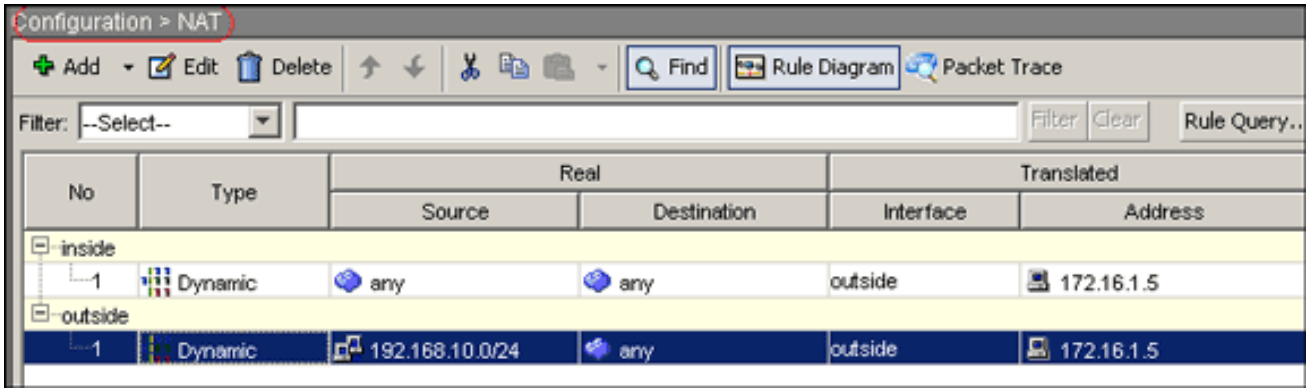
dinamica per consentire la conversione del traffico proveniente dalla rete interna con l'uso dell'indirizzo IP esterno



172.16.1.5. Fare clic su **OK**.Scegliere **Configurazione > NAT > Aggiungi > Aggiungi regola NAT dinamica** per consentire la conversione del traffico proveniente dalla rete esterna 192.168.10.0 con l'uso dell'indirizzo IP esterno



172.16.1.5. Fare clic su **OK**.



Fare clic su **Apply** (Applica).**Nota:** di seguito sono riportati i comandi di configurazione CLI equivalenti:

Configurazione CLI di ASA 7.2(2)

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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter
!--- and exit the same interface. access-list 100
extended permit icmp any any 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) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !---
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

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
```

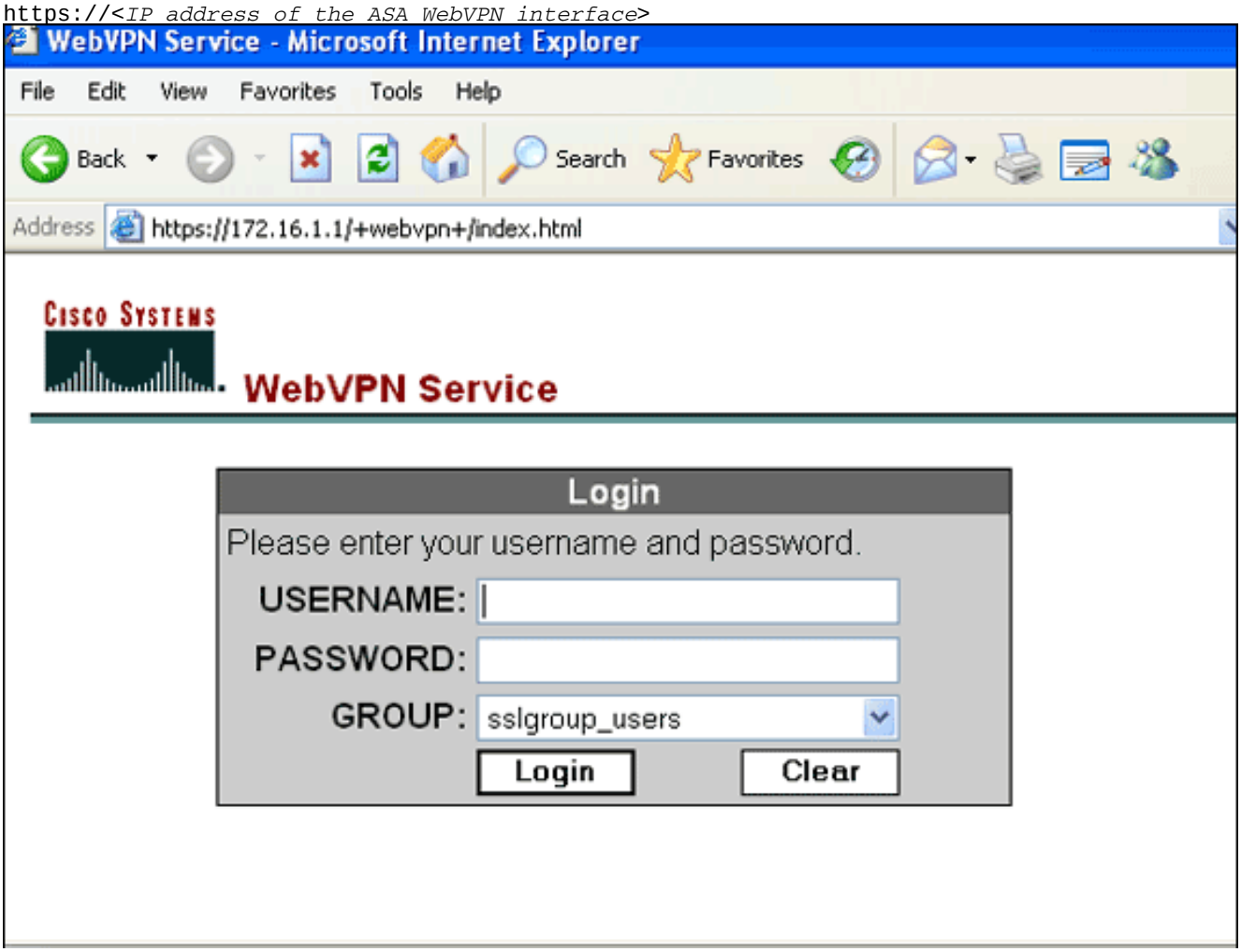
```
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup."
group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN
Clients. 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, increasing 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#
```

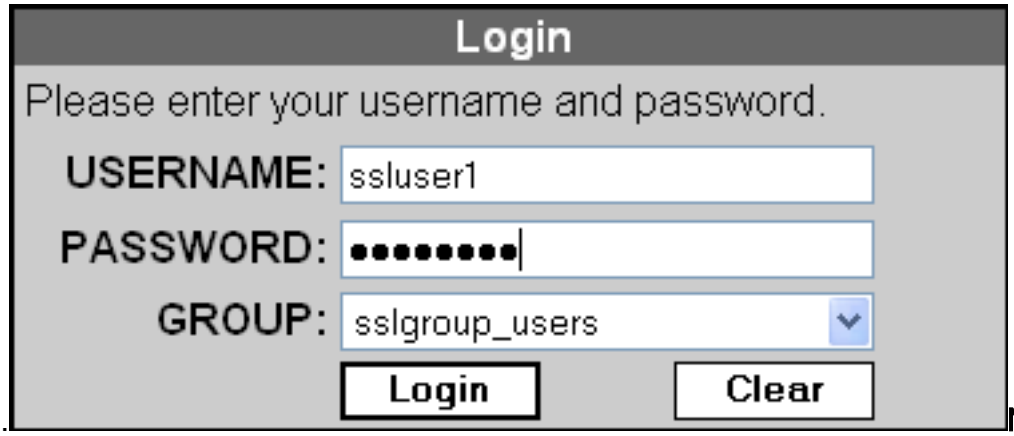
Stabilire la connessione VPN SSL con SVC

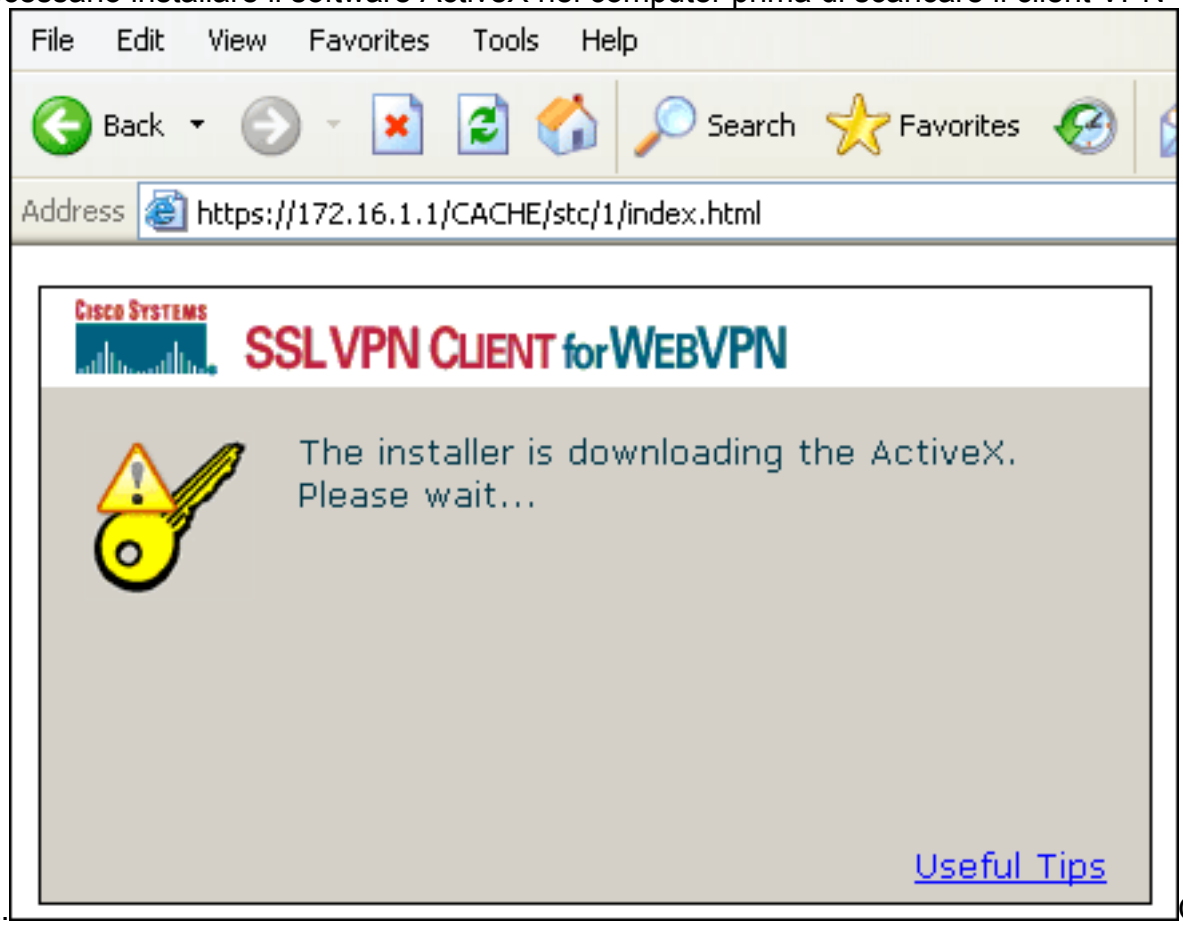
Completare questa procedura per stabilire una connessione VPN SSL con ASA.

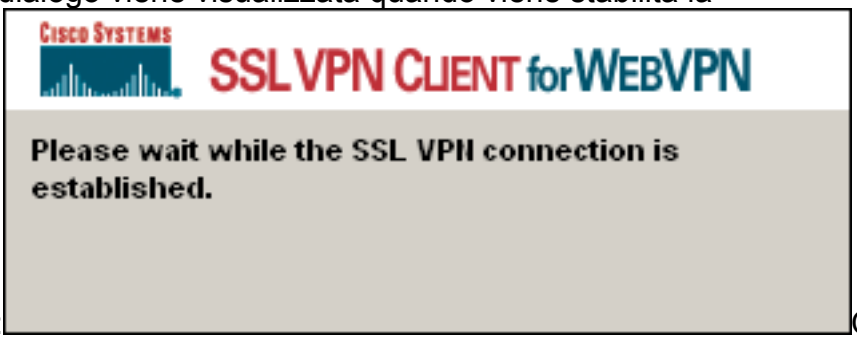
1. Nel campo Address (Indirizzo) del browser Web, immettere l'URL o l'indirizzo IP dell'interfaccia WebVPN dell'appliance ASA.Ad esempio:
   `https://<IP address of the ASA WebVPN interface>`

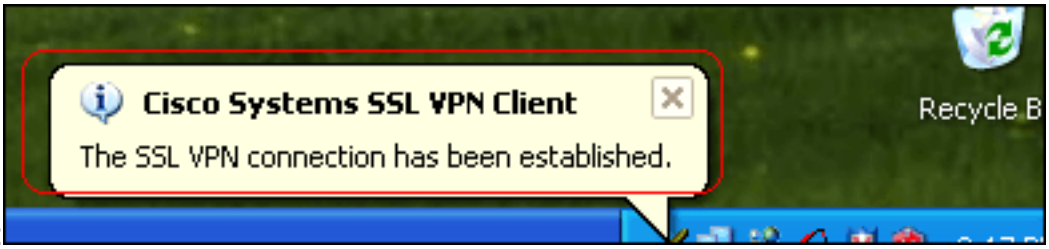


2. Immettere il nome utente e la password, quindi scegliere il gruppo desiderato dall'elenco a

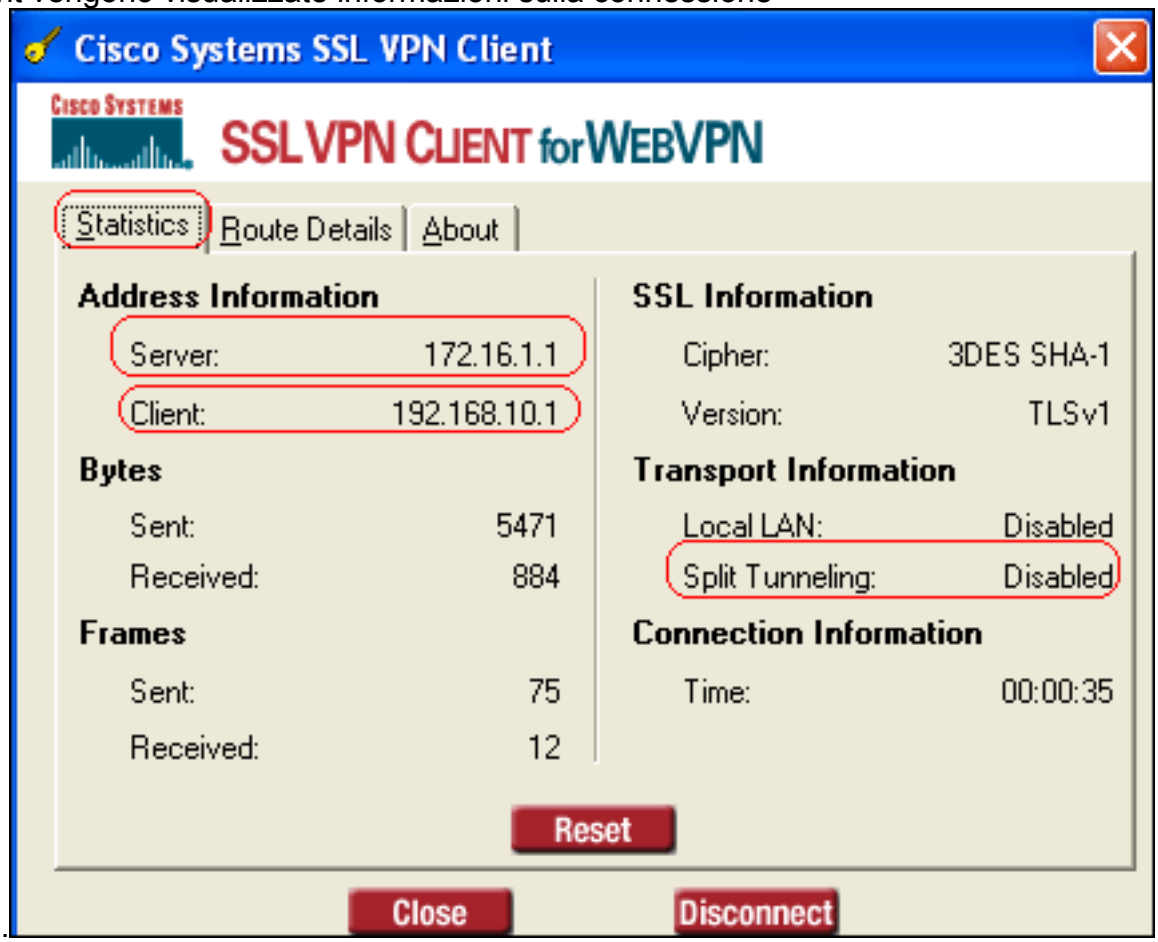
discesa Gruppo. 

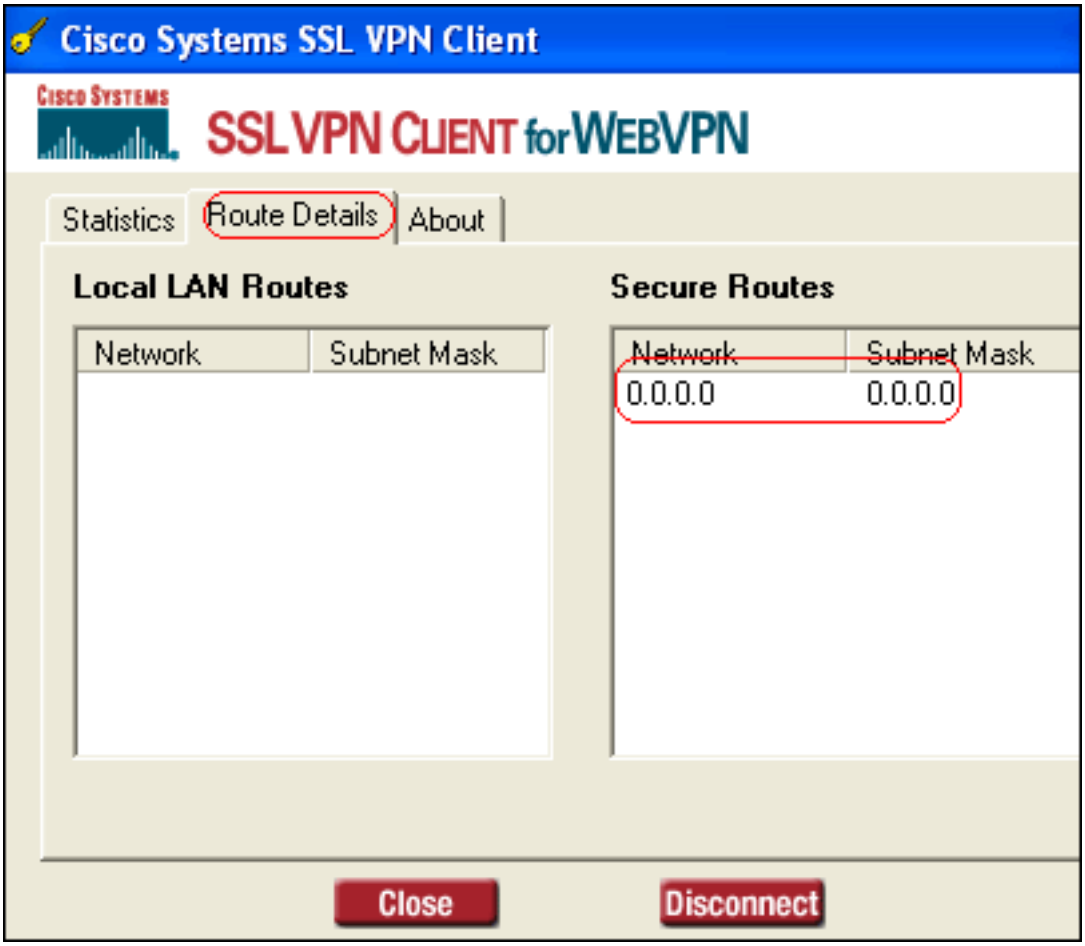
Nota: è necessario installare il software ActiveX nel computer prima di scaricare il client VPN SSL. 

Questa finestra di dialogo viene visualizzata quando viene stabilita la connessione: 

Questo messaggio viene visualizzato una volta stabilita la connessione: 

3. Una volta stabilita la connessione, fare doppio clic sull'icona con il tasto giallo visualizzata nella barra delle applicazioni del computer.Nella finestra di dialogo Cisco Systems SSL VPN Client vengono visualizzate informazioni sulla connessione SSL.





Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

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.

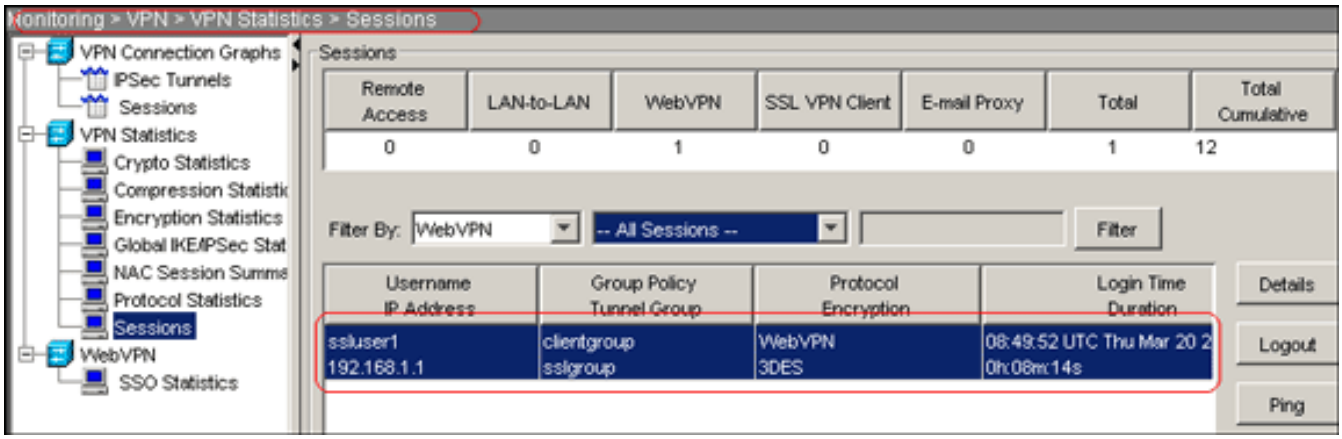
```
ciscoasa#show vpn-sessiondb svc

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 visualizzare le informazioni sulle sessioni WebVPN correnti nell'appliance ASA.



Risoluzione dei problemi

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

- **vpn-sessiondb logoff name <*username*>**: consente di disconnettersi dalla sessione VPN SSL per il nome utente specificato.

```
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.**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
```

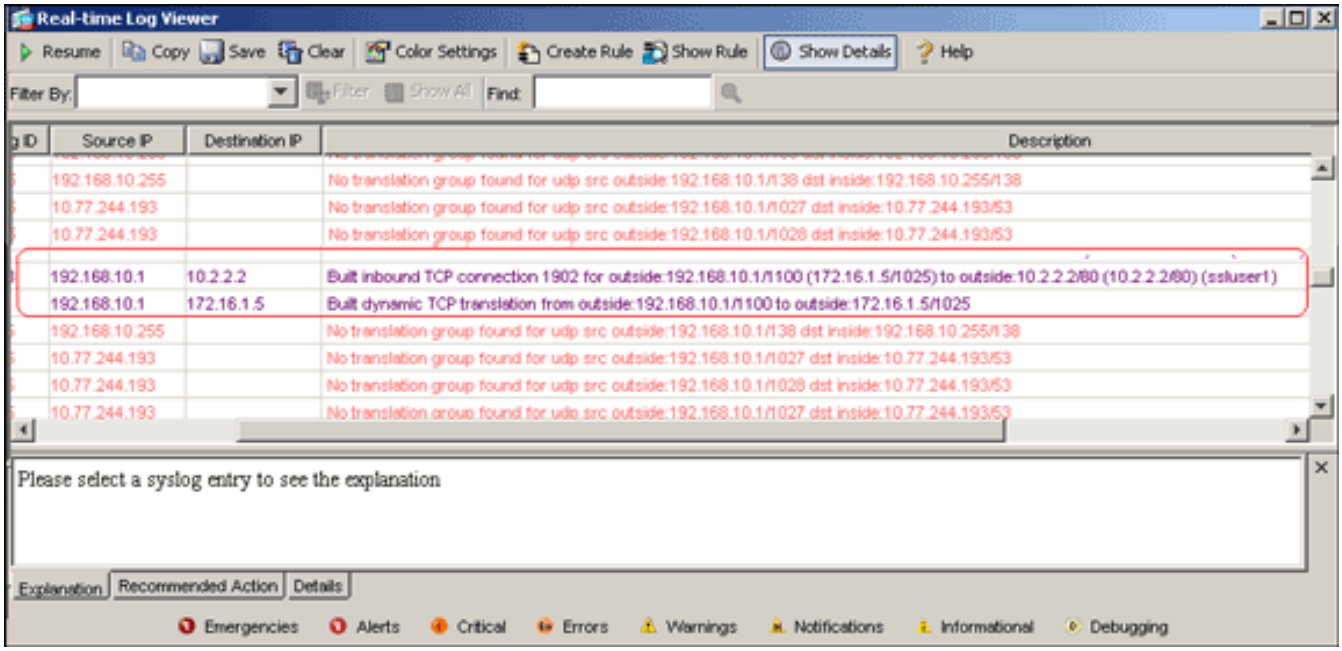
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

- **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
```

- In ASDM, scegliere **Monitoraggio > Log > Visualizzatore log in tempo reale > Visualizza** per visualizzare gli eventi in tempo reale. Gli esempi mostrano 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 - Pagina di supporto
- 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