ASA 8.x: Esempio di configurazione dell'appliance ASA che consente il tunneling ripartito per il client VPN AnyConnect

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Premesse
Configurazione
Esempio di rete
Configurazione ASA con ASDM 6.0(2)
Configurazione ASA CLI
Stabilire la connessione VPN SSL con SVC
Verifica
Risoluzione dei problemi
Informazioni correlate

Introduzione

Questo documento offre istruzioni dettagliate su come consentire ai client VPN Cisco AnyConnect di accedere a Internet mentre sono tunneling in una Cisco Adaptive Security Appliance (ASA) 8.0.2. Questa configurazione consente al client di accedere in modo sicuro alle risorse aziendali tramite SSL e allo stesso tempo di accedere a Internet in modo non protetto con il tunneling suddiviso.

Prerequisiti

Requisiti

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

- ASA Security Appliance deve eseguire la versione 8.x
- Cisco AnyConnect VPN Client 2.x**Nota:** scaricare il pacchetto AnyConnect VPN Client (anyconnect-win*.pkg) da Cisco Software Download (solo utenti registrati). Copiare il client VPN AnyConnect nella memoria flash dell'ASA, da scaricare sui computer degli utenti remoti per stabilire la connessione VPN SSL con l'ASA. Per ulteriori informazioni, consultare la sezione Installazione del client AnyConnect della guida alla configurazione delle appliance

ASA.

Componenti usati

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

- Cisco serie 5500 ASA con software versione 8.0(2)
- Cisco AnyConnect SSL VPN Client versione per Windows 2.0.0343
- PC con Microsoft Vista, Windows XP SP2 o Windows 2000 Professional SP4 e Microsoft Installer versione 3.1
- Cisco Adaptive Security Device Manager (ASDM) versione 6.0(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

Il client VPN Cisco AnyConnect fornisce connessioni SSL sicure all'appliance di sicurezza per gli utenti remoti. Senza un client installato in precedenza, gli utenti remoti immettono l'indirizzo IP nel browser di un'interfaccia configurata per accettare connessioni VPN SSL. A meno che l'appliance di sicurezza non sia configurata per reindirizzare le richieste http:// a https://, gli utenti devono immettere l'URL nel formato https://<indirizzo>.

Dopo aver immesso l'URL, il browser si connette all'interfaccia e visualizza la schermata di accesso. Se l'utente soddisfa i requisiti di accesso e autenticazione e l'appliance di sicurezza identifica l'utente come utente che richiede il client, scarica il client corrispondente al sistema operativo del computer remoto. Al termine del download, il client si installa e si configura, stabilisce una connessione SSL protetta e rimane o si disinstalla (a seconda della configurazione dell'appliance di sicurezza) quando la connessione viene interrotta.

Nel caso di un client installato in precedenza, quando l'utente esegue l'autenticazione, l'appliance di sicurezza esamina la revisione del client e lo aggiorna in base alle esigenze.

Quando il client negozia una connessione VPN SSL con l'appliance di sicurezza, si connette utilizzando TLS (Transport Layer Security) e, facoltativamente, DTLS (Datagram Transport Layer Security). DTLS evita i problemi di latenza e larghezza di banda associati ad alcune connessioni SSL e migliora le prestazioni delle applicazioni in tempo reale che sono sensibili ai ritardi dei pacchetti.

Il client AnyConnect può essere scaricato dall'appliance di sicurezza o installato manualmente sul PC remoto dall'amministratore di sistema. Per ulteriori informazioni su come installare manualmente il client, consultare la Cisco AnyConnect VPN Client Administrator Guide.

L'accessorio di protezione scarica il client in base agli attributi dei criteri di gruppo o del nome utente dell'utente che stabilisce la connessione. È possibile configurare l'appliance di sicurezza in modo che il client venga scaricato automaticamente oppure in modo che venga richiesto all'utente remoto se scaricare il client. Nel secondo caso, se l'utente non risponde, è possibile configurare l'appliance di sicurezza in modo che scarichi il client dopo un periodo di timeout o presenti la pagina di accesso.

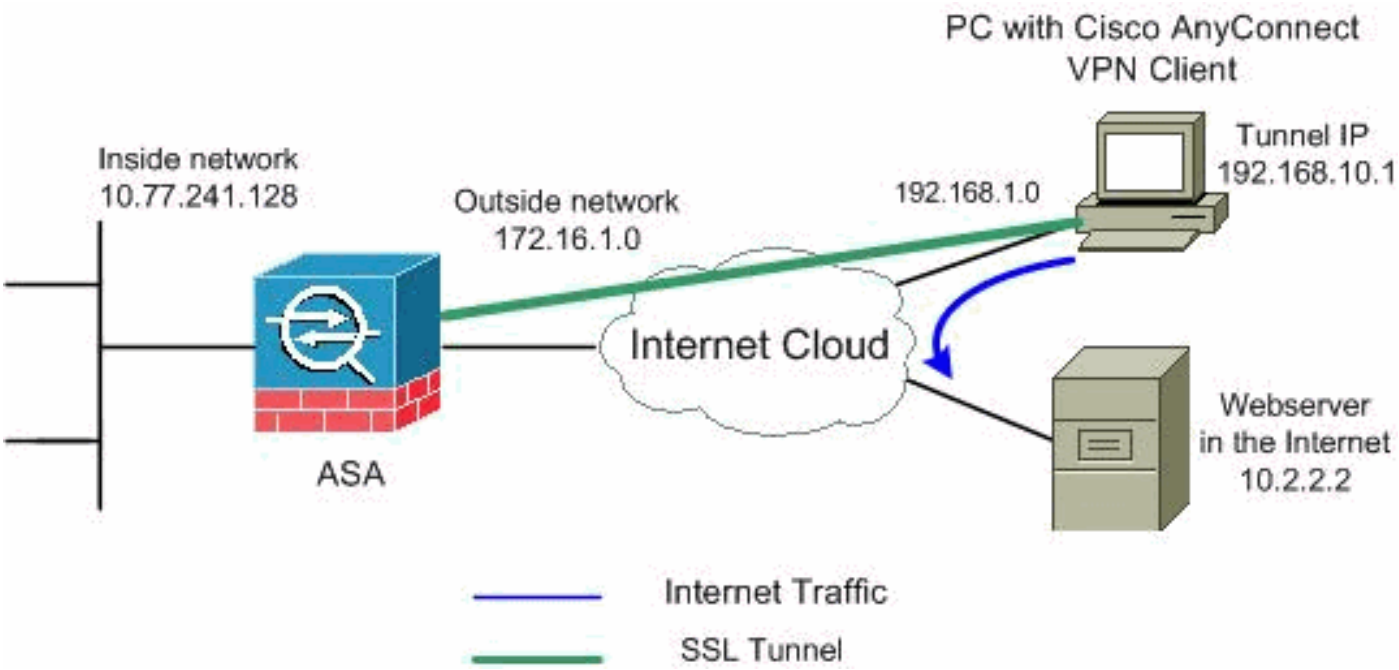
Configurazione

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.

Configurazione ASA con ASDM 6.0(2)

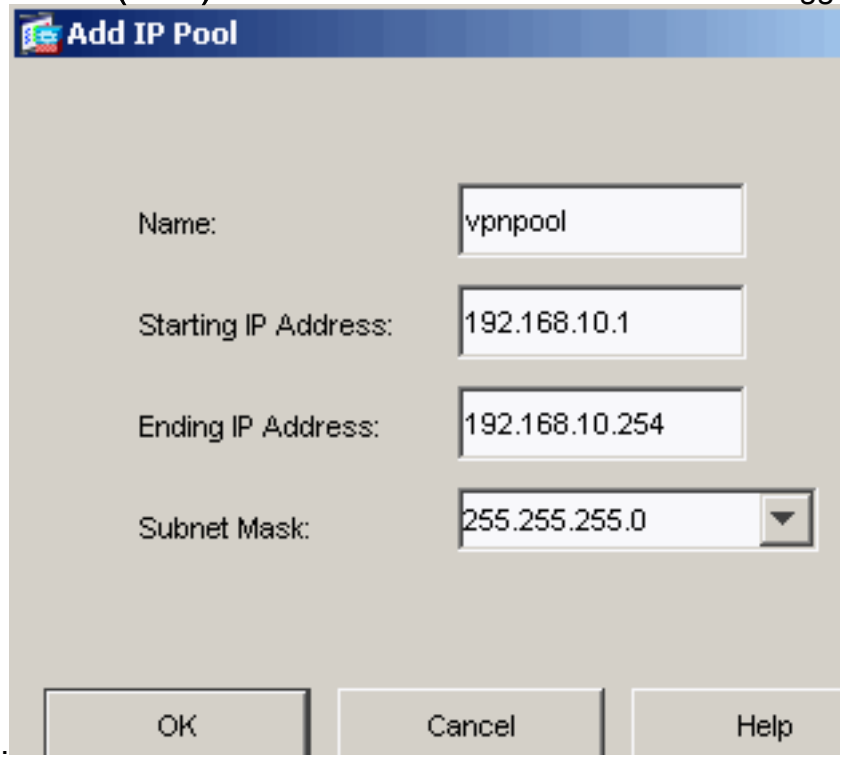
in questo documento si presume che la configurazione di base, ad esempio la configurazione dell'interfaccia, sia già stata creata e funzioni correttamente.

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

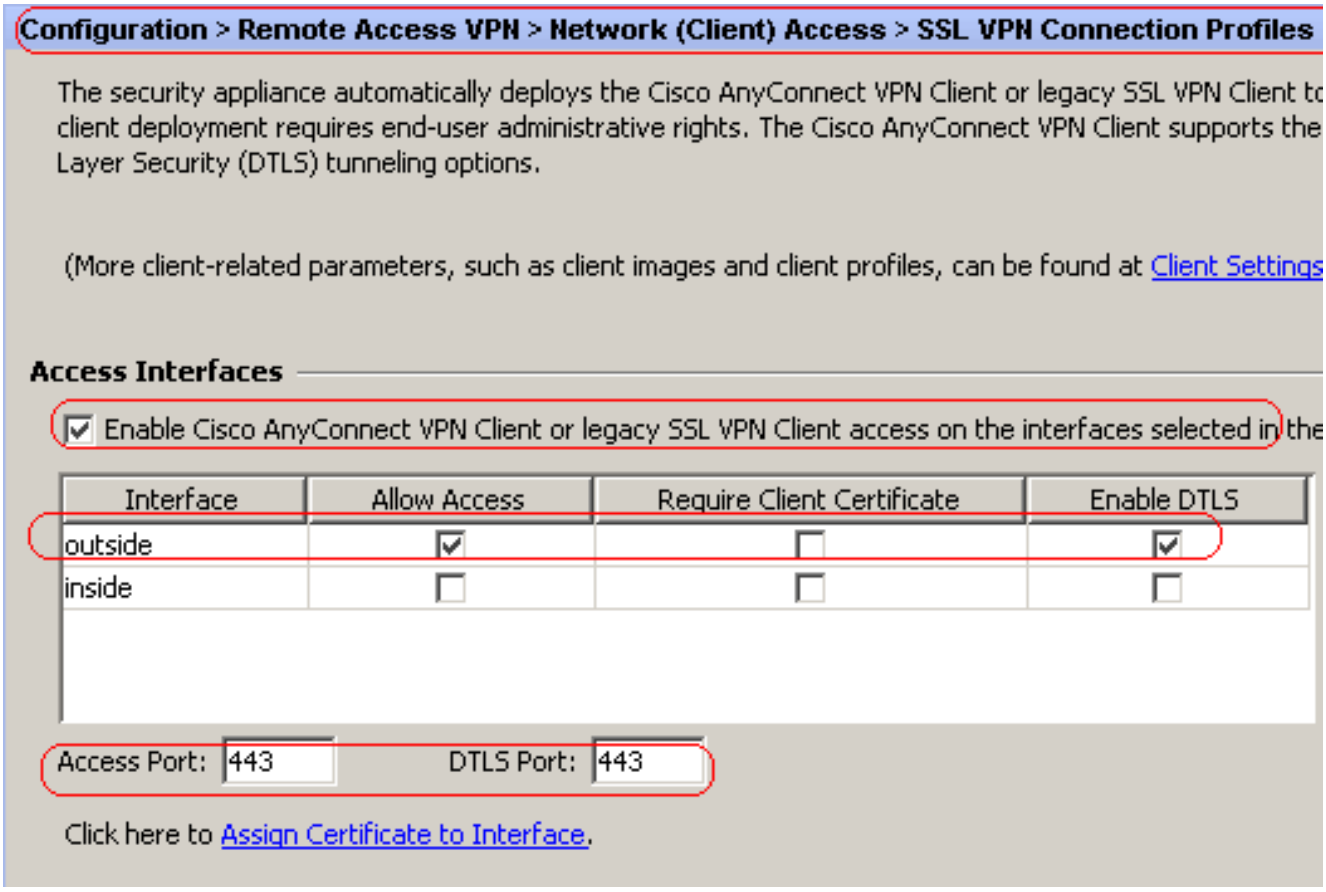
Nota: WebVPN e ASDM non possono essere abilitati sulla stessa interfaccia ASA a meno che non si modifichino i numeri di porta. Per ulteriori informazioni, fare riferimento a ASDM e WebVPN abilitati sulla stessa interfaccia dell'ASA.

Per configurare la VPN SSL sull'appliance ASA con tunneling suddiviso, completare la procedura seguente:

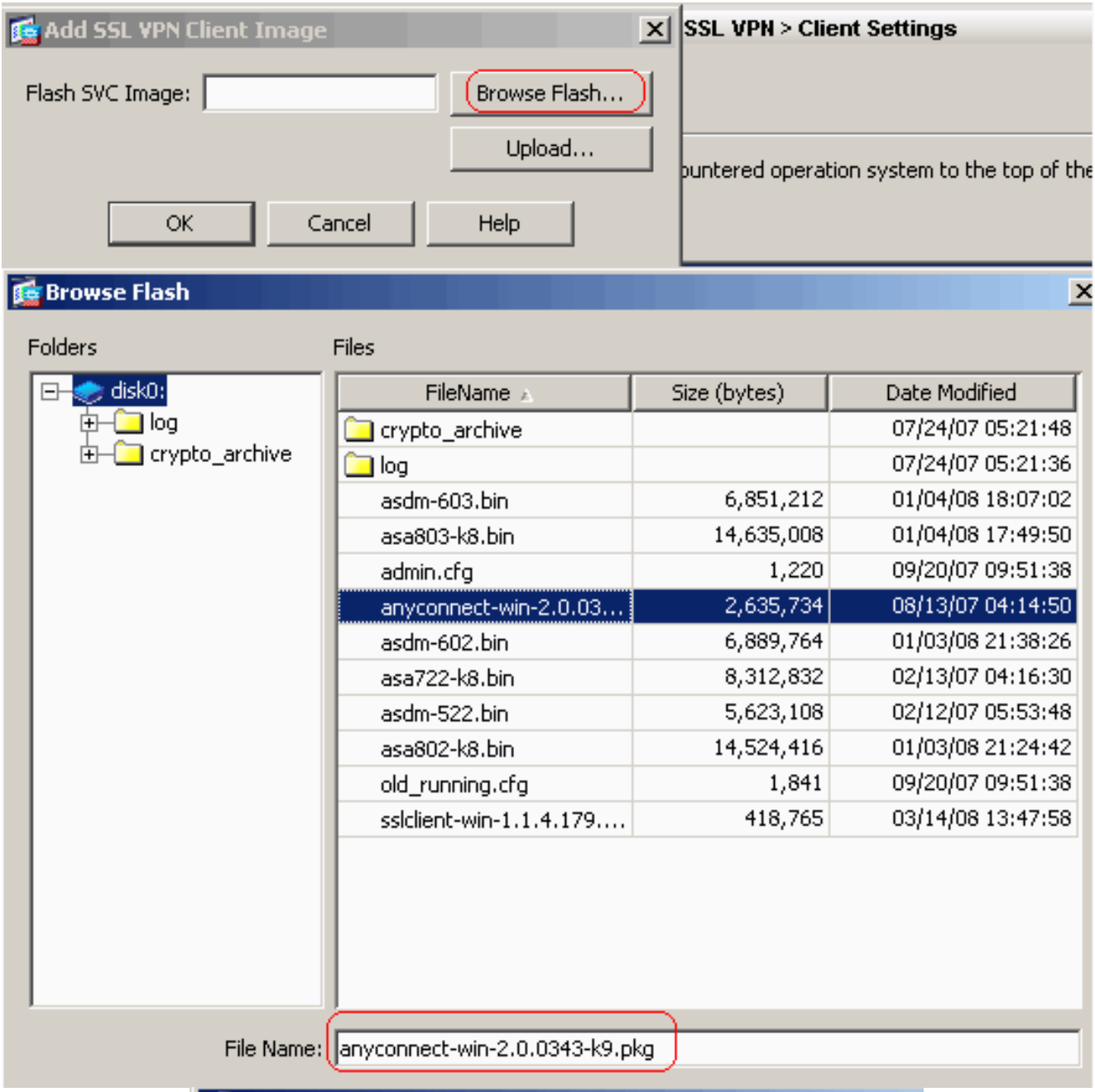
1. Per creare un pool di indirizzi IP, scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Gestione indirizzi > Pool di indirizzi** > Aggiungi **vpnpool**.

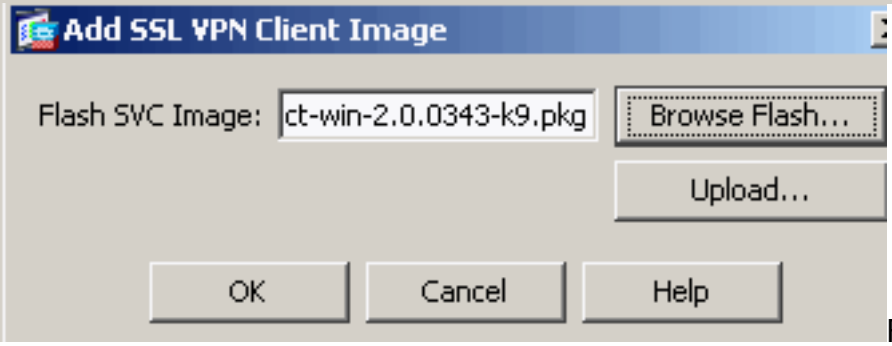


2. Fare clic su **Apply** (Applica).**Configurazione CLI equivalente:**
3. Abilita WebVPN.Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione VPN SSL** e in **Interfacce di accesso**, fare clic sulle caselle di controllo **Consenti accesso** e **Abilita DTLS** per l'interfaccia esterna. Inoltre, selezionare la casella di controllo **Abilita accesso client VPN Cisco AnyConnect o client VPN SSL legacy sull'interfaccia selezionata nella tabella seguente** per abilitare VPN SSL sull'interfaccia esterna.

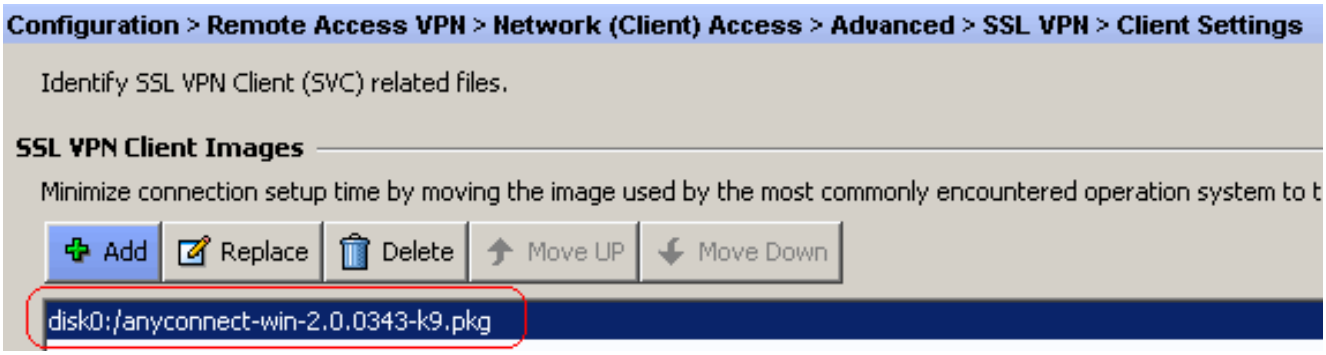


Fare clic su **Apply** (Applica).Per aggiungere l'immagine del client VPN Cisco AnyConnect dalla memoria flash dell'ASA, scegliere **Configurazione > VPN** ad **accesso remoto > Accesso** di **rete (client) > Avanzate > VPN SSL > Impostazioni client > Aggiungi**, come mostrato.



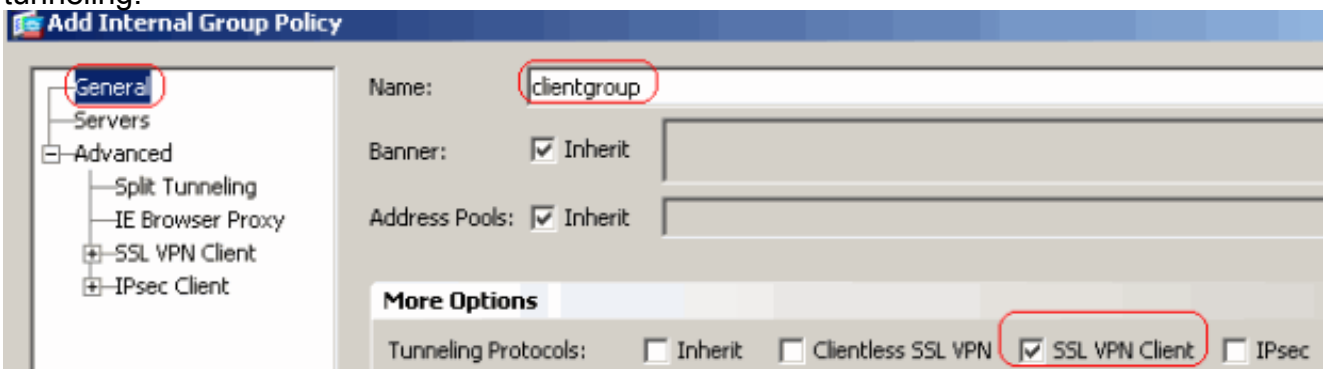


Fare clic su **OK**. Fare clic su **Add**.

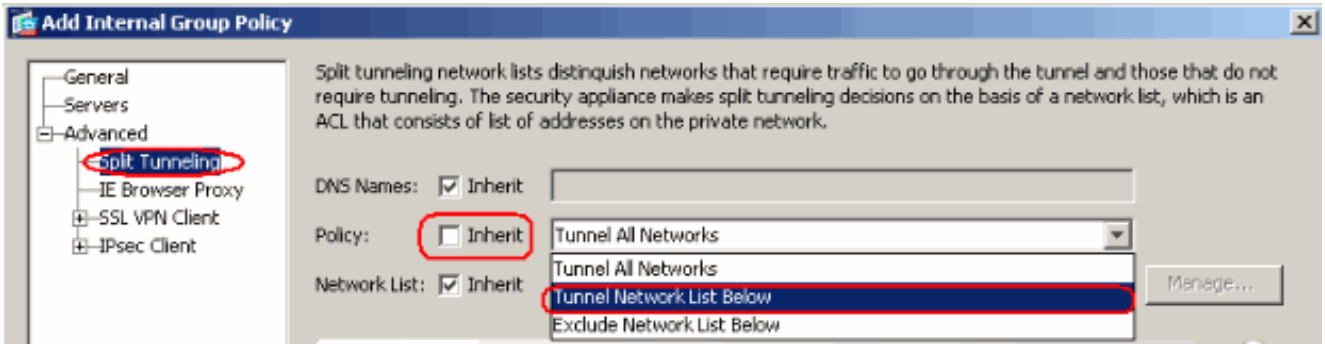


Configurazione CLI equivalente:

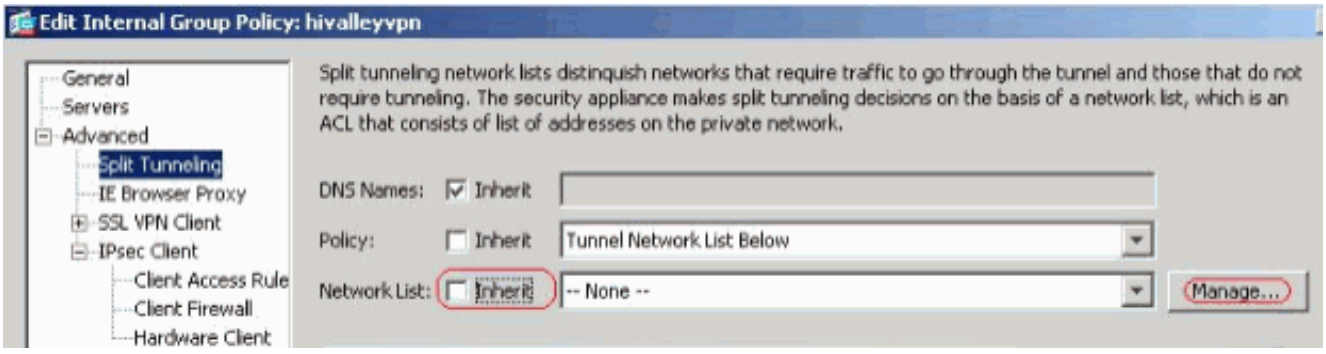
4. Configurare Criteri di gruppo.Per creare un gruppo di **client di** Criteri di gruppo interno, scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client)** > Criteri di gruppo. Nella scheda **Generale**, selezionare la casella di controllo **SSL VPN Client** per abilitare WebVPN come protocollo di tunneling.



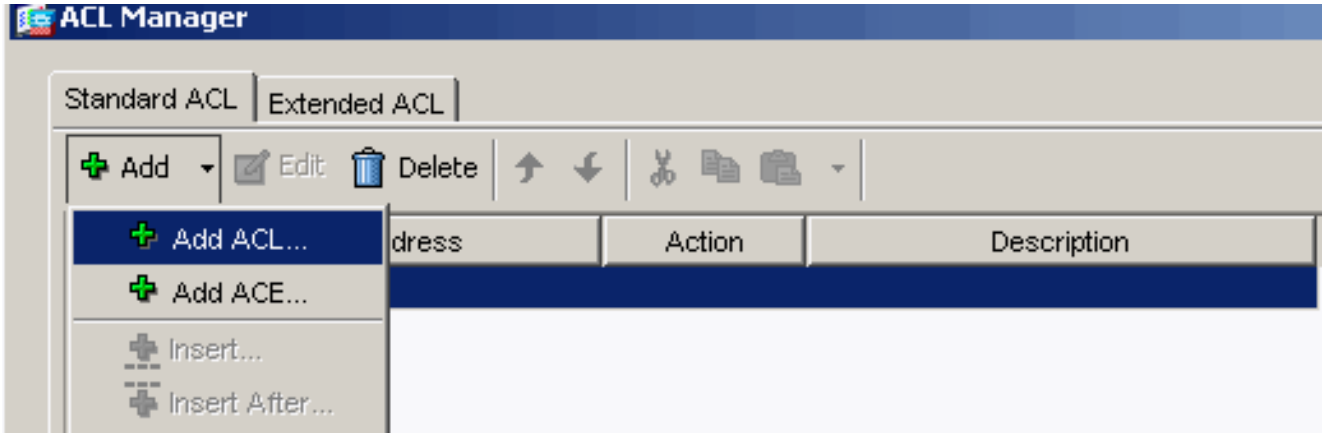
Nella scheda **Avanzate > Tunneling ripartito**, deselezionare la casella di controllo **Eredita** per Criterio tunnel ripartito e scegliere **Elenco reti tunnel sotto** dall'elenco a discesa.



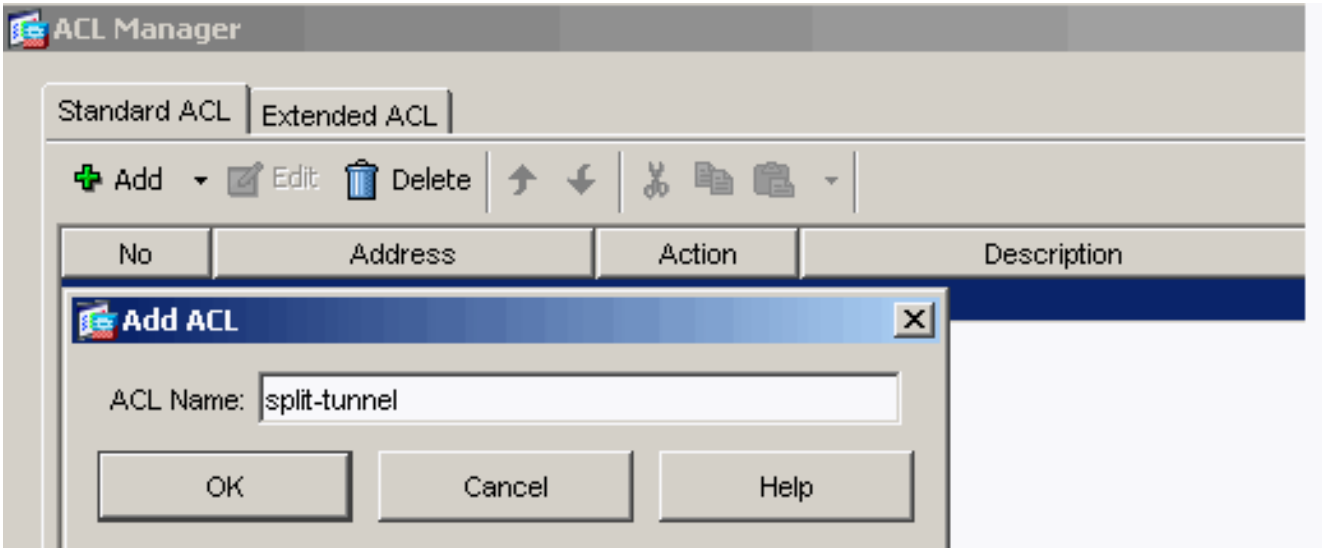
Deselezionare la casella di controllo **Eredita** per **Elenco reti tunnel** e fare clic su **Gestisci** per avviare Gestione ACL.



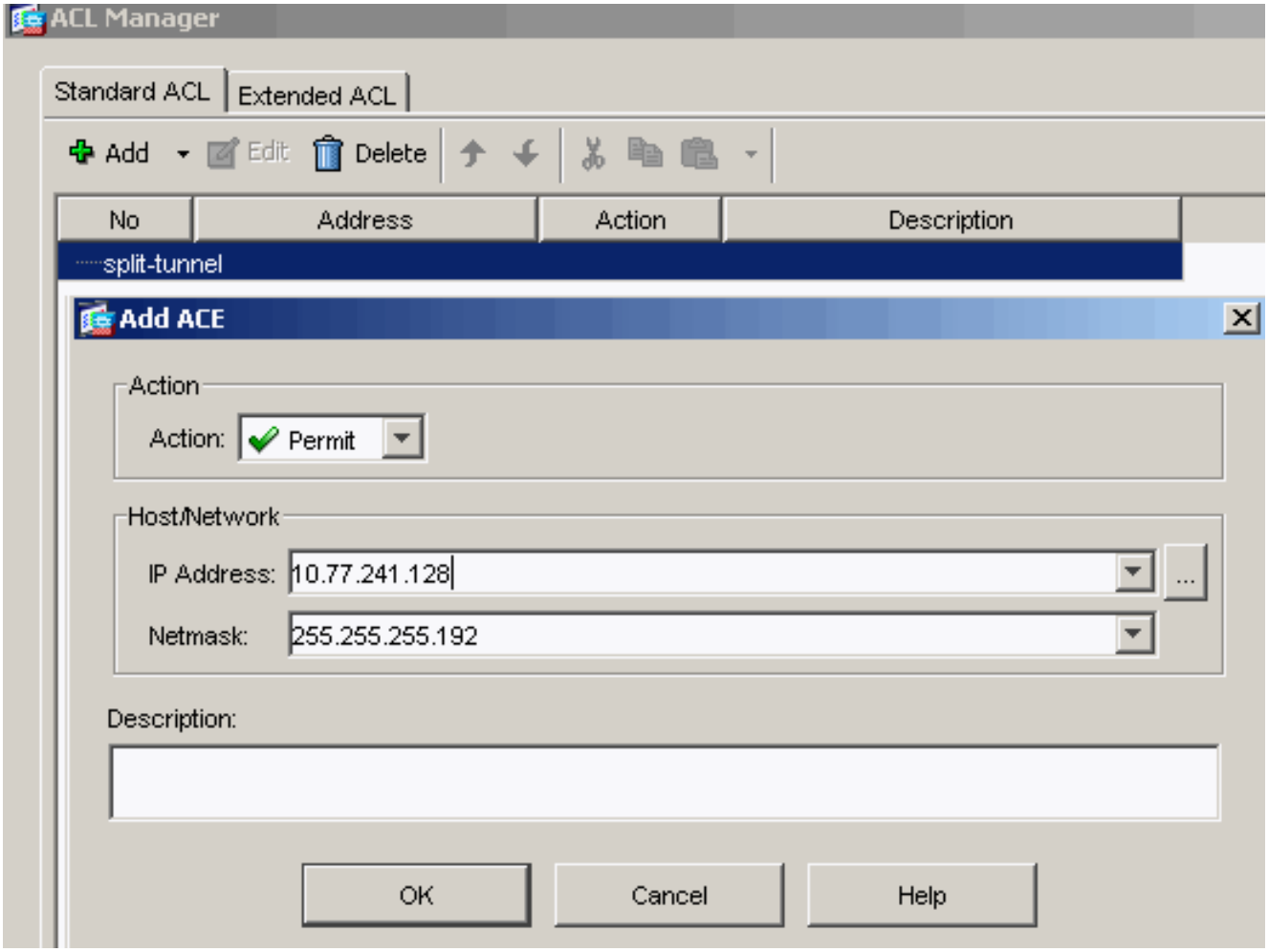
In Gestione ACL, selezionare **Add > Add ACL...** (Aggiungi ACL) per creare un nuovo elenco degli accessi.



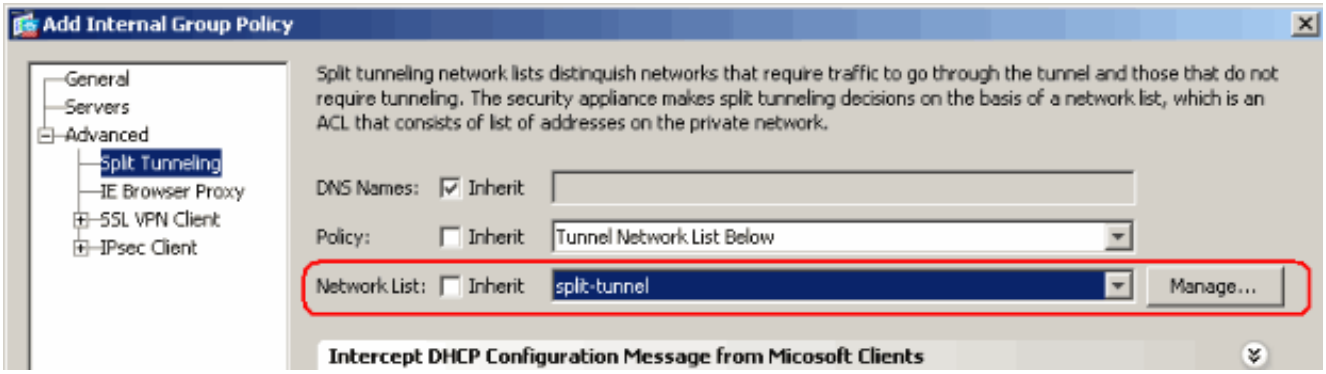
Specificare un nome per l'ACL e fare clic su
OK.



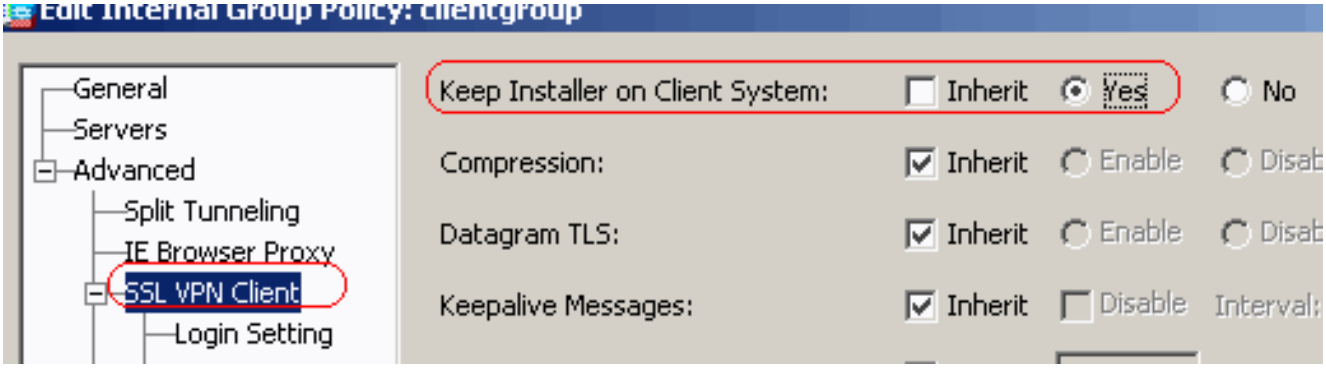
Una volta creato il nome dell'ACL, scegliere **Aggiungi > Aggiungi ACE** per aggiungere una voce di controllo di accesso (ACE, Access Control Entry).Definire l'ACE che corrisponde alla LAN dietro l'ASA. In questo caso, la rete è 10.77.241.128/26 e selezionare **Permit** come azione.Per uscire da Gestione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



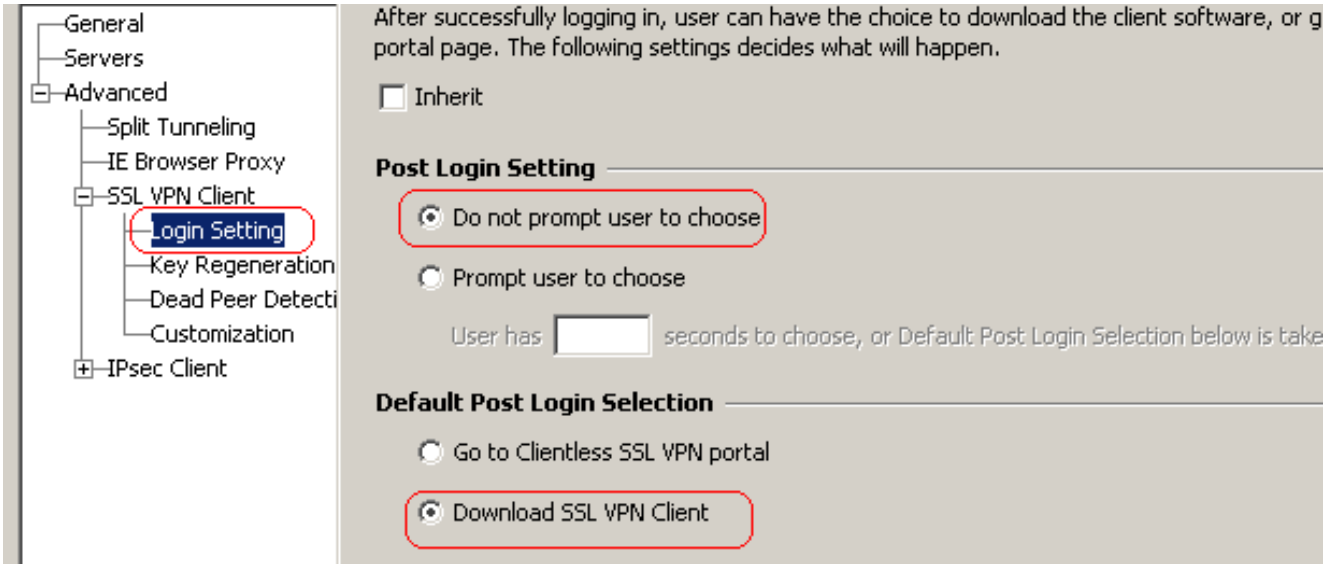
Verificare che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel separato. Per tornare alla configurazione di Criteri di gruppo, fare clic su **OK**.



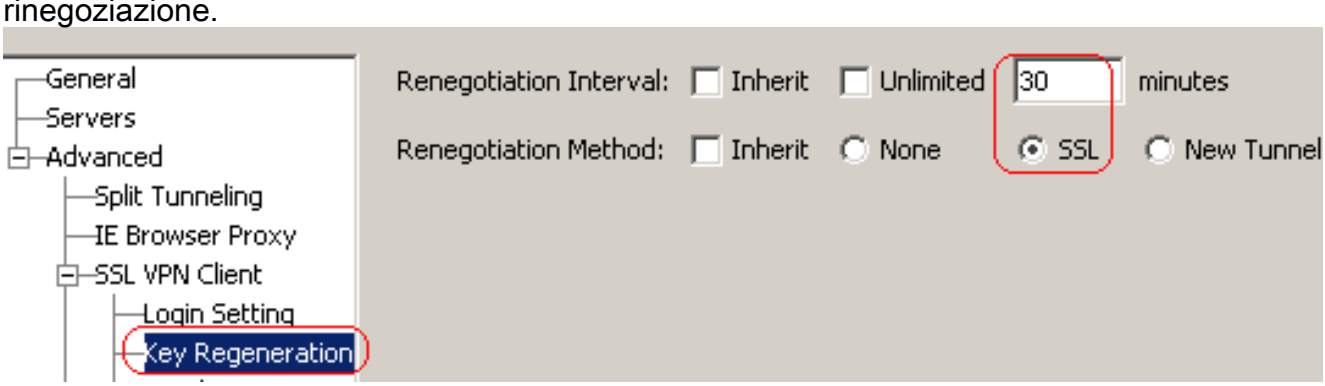
Nella pagina principale, fare clic su **Apply**, quindi su Send (se necessario) per inviare i comandi all'appliance ASA.Configurare le impostazioni della **VPN SSL** in modalità Criteri di gruppo.Per l'opzione Mantieni programma di installazione sul sistema client, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **Sì**.Questa azione consente al software SVC di rimanere sul computer client. 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.



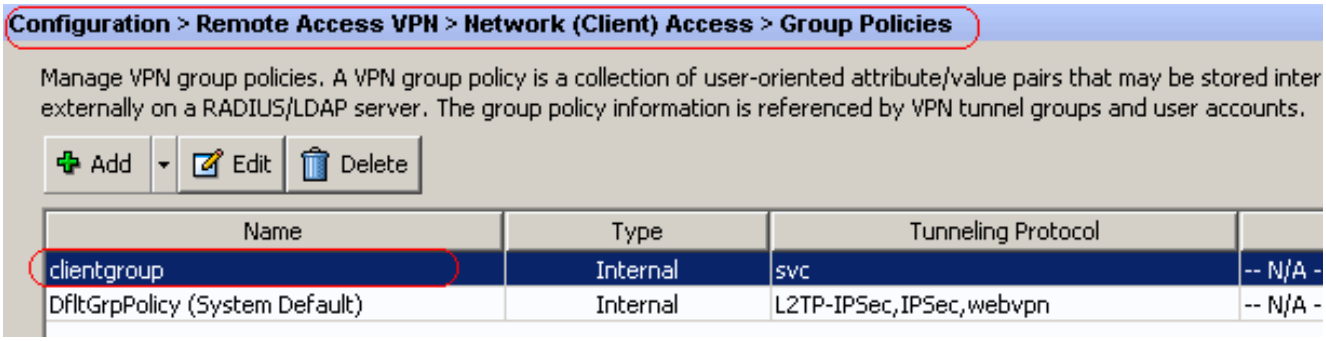
Fare clic su **Login Setting** (Impostazione accesso) per impostare **Post Login Setting** (Impostazione post accesso) e **Default Post Login Selection** (Selezione predefinita post accesso), come
mostrato.



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 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**.La rinegoziazione può utilizzare il tunnel SSL corrente o un nuovo tunnel creato espressamente per la
rinegoziazione.

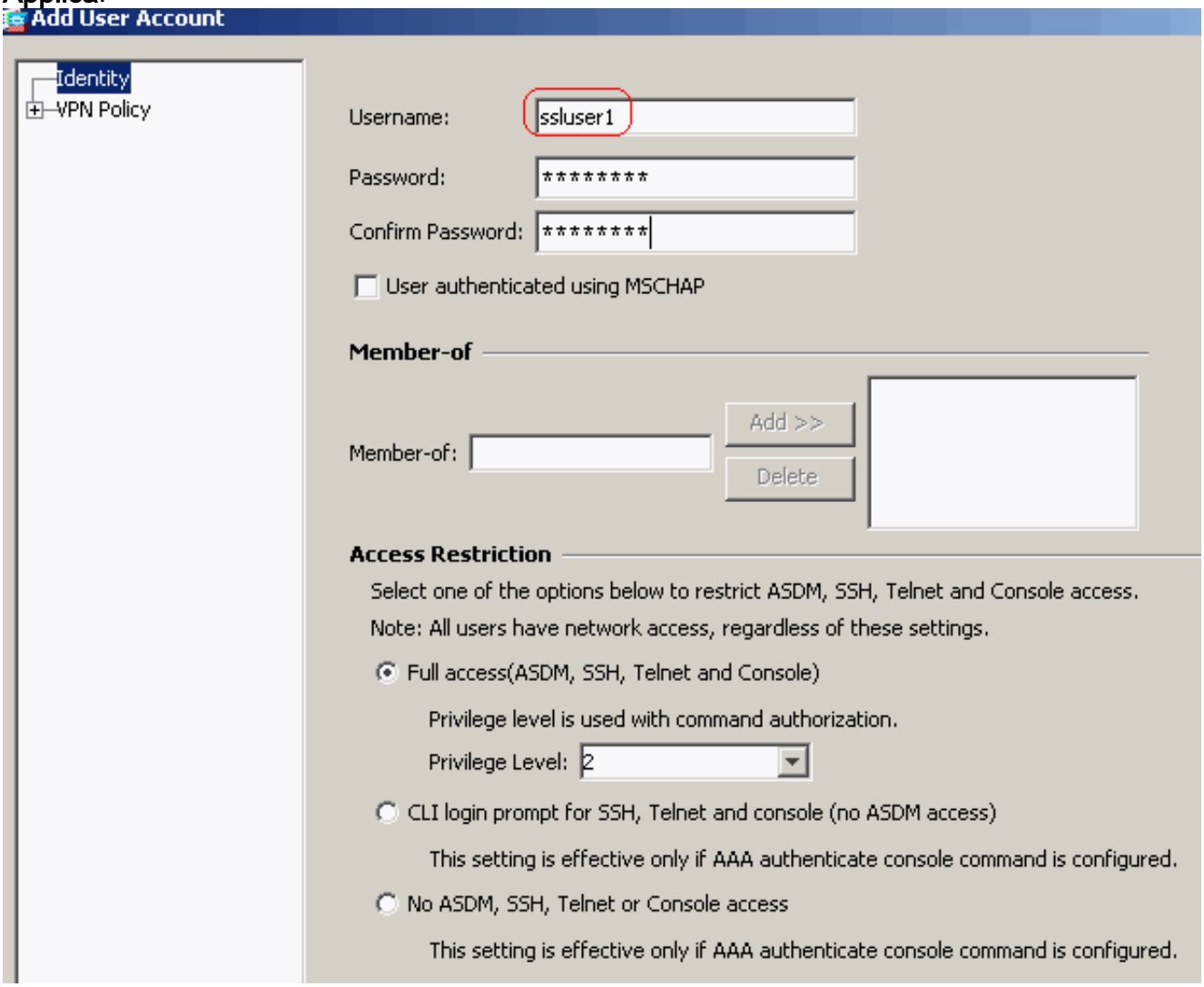


Fare clic su **OK**, quindi su
Applica.



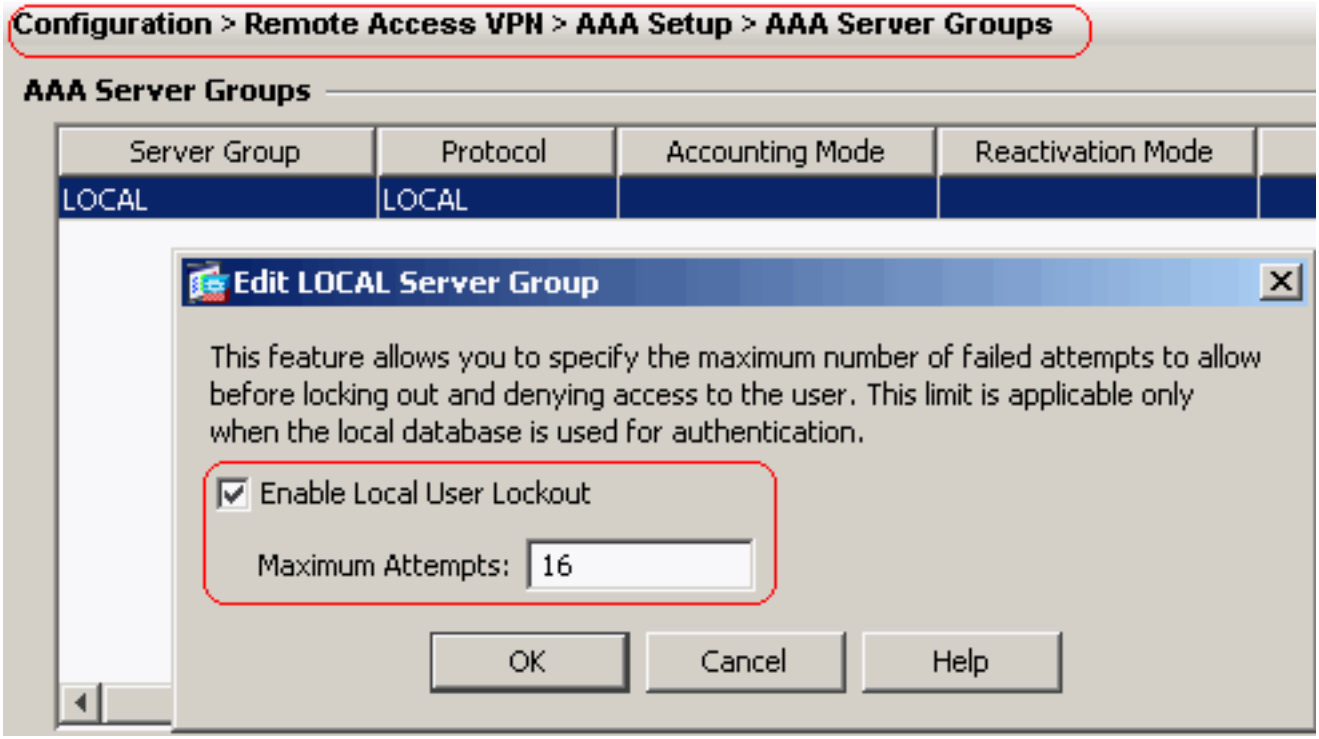
Configurazione CLI equivalente:

5. Per creare un nuovo account utente **ssluser1,** scegliere **Configurazione > VPN ad accesso remoto > Impostazione AAA > Utenti locali > Aggiungi**. Fare clic su **OK** e quindi su **Applica**.

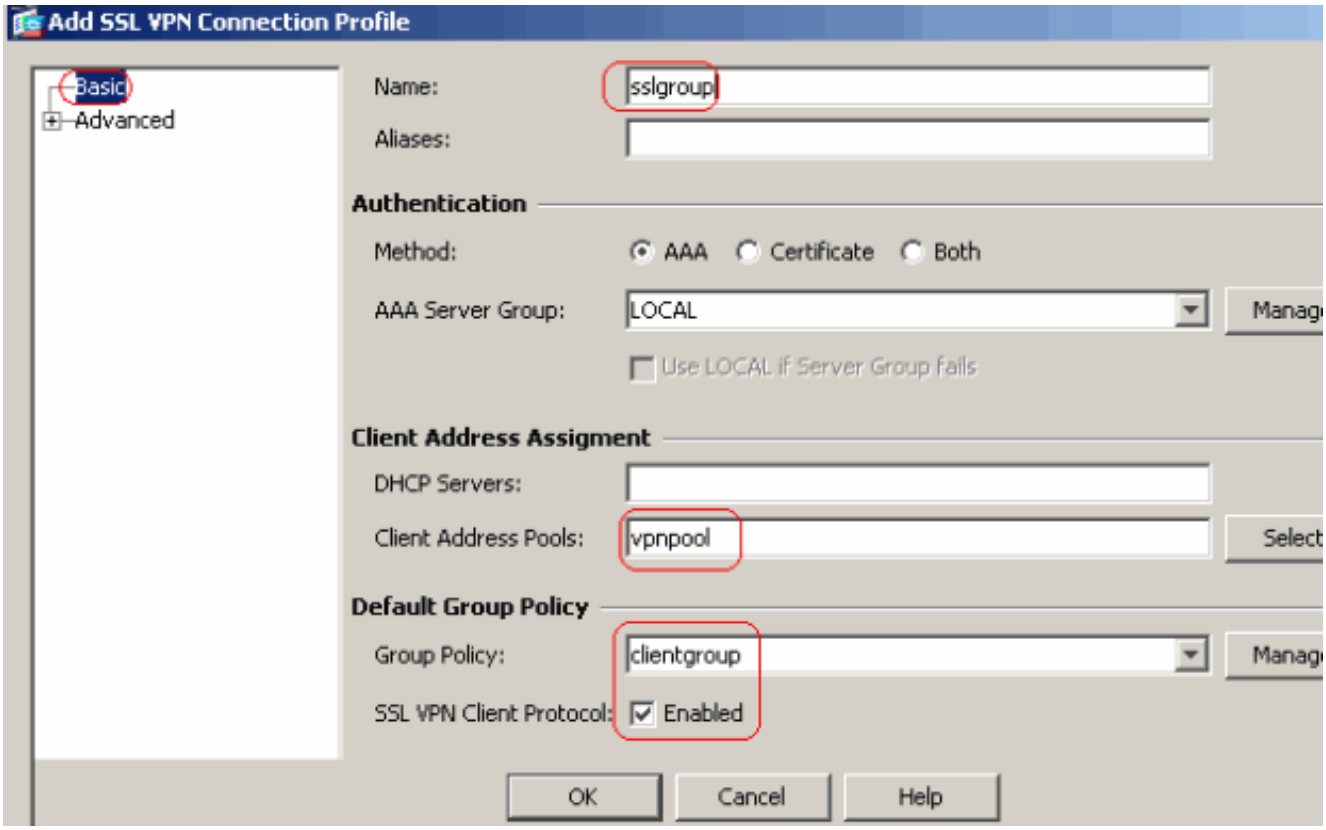


Configurazione CLI equivalente:

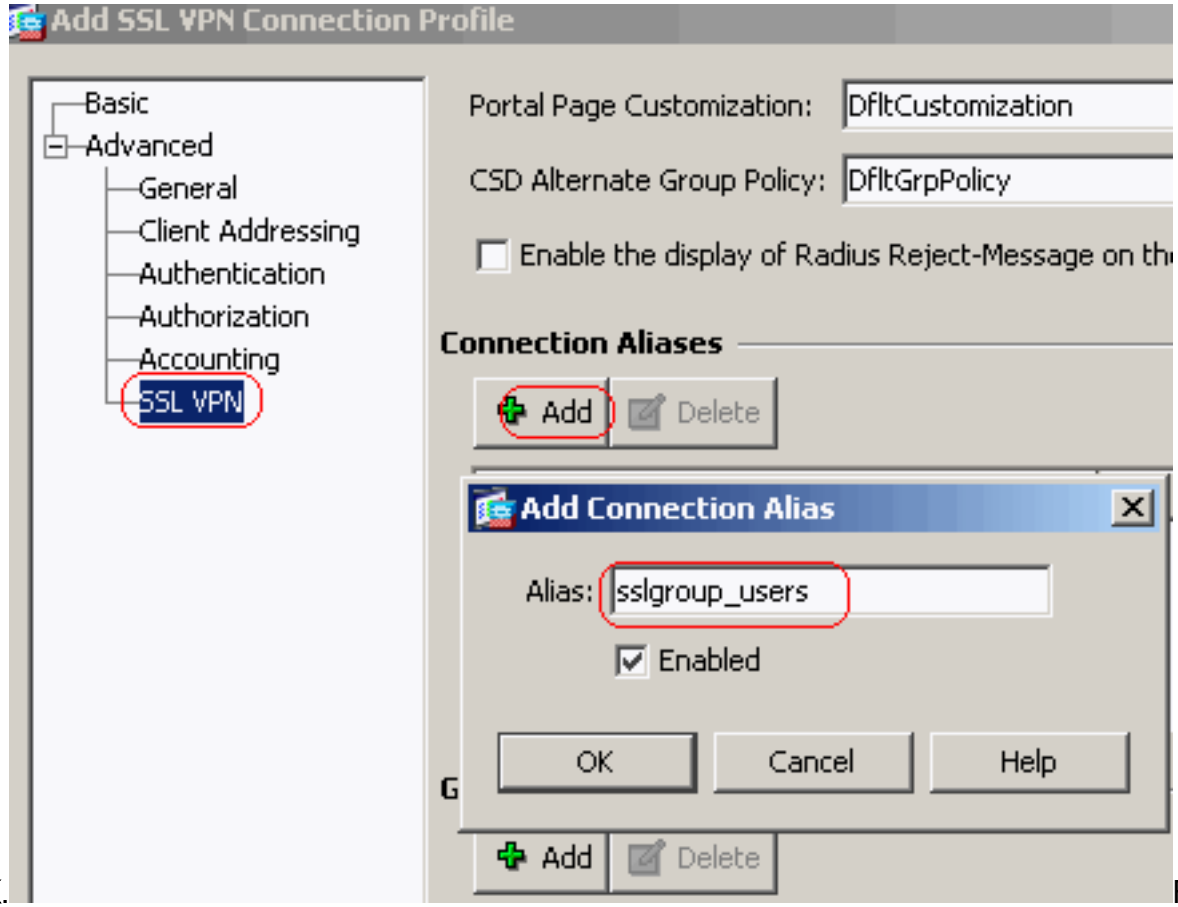
6. Scegliere **Configurazione > VPN ad accesso remoto > Impostazione AAA > Gruppi di server AAA > Modifica** per modificare il gruppo di server predefinito LOCAL selezionando la casella di controllo **Abilita blocco utente locale** con un valore massimo di tentativi pari a **16**.



7. Fare clic su **OK**, quindi su **Applica**.**Configurazione CLI equivalente:**
8. Configurare il gruppo di tunnel.Per creare un nuovo **gruppo di** tunnel, scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione VPN SSL > Aggiungi**.Nella scheda **Base** è possibile eseguire l'elenco delle configurazioni come illustrato di seguito.Assegnare al gruppo di tunnel il nome **sslgroup**.In Assegnazione indirizzo client scegliere il pool di indirizzi **vpnpool** dall'elenco a discesa.In Criteri di gruppo predefiniti scegliere il **gruppo client** di Criteri di gruppo dall'elenco a discesa.

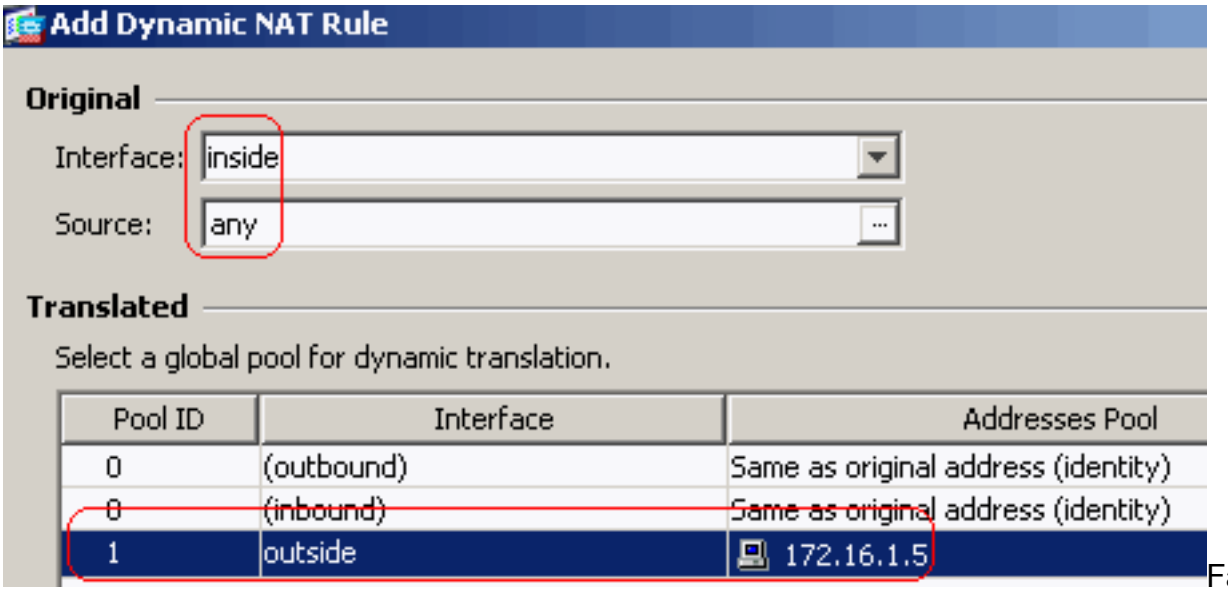


Nella scheda **SSL VPN > Alias connessione**, specificare il nome alias del gruppo come **sslgroup_users** e fare clic su

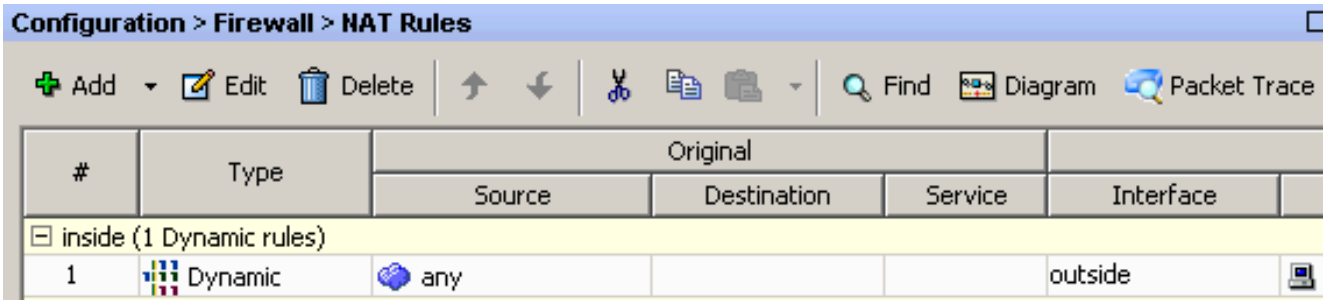


OK. Fare clic su **OK**, quindi su **Applica**.**Configurazione CLI equivalente:**

9. Configurare NAT.Scegliere **Configurazione > Firewall > Regole NAT > Aggiungi regola NAT dinamica in** modo che il traffico proveniente dalla rete interna possa essere convertito con l'indirizzo IP esterno
172.16.1.5.



Fare clic su **OK**.Fare clic su
OK.



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

10. 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 ASA CLI

Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
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
boot system disk0:/asa802-k8.bin
```

```
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
 domain-name default.domain.invalid
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 logging enable logging asdm informational
mtu inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN
Clients no failover icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.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


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 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
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
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
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
```

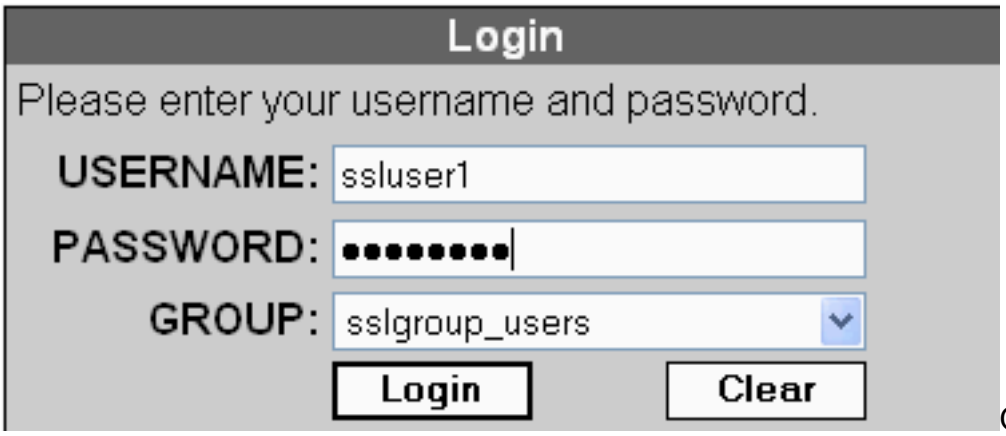
```
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
webvpn
 enable outside

!--- Enable WebVPN on the outside interface  svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client
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 group-policy clientgroup internal

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

!--- Specify SSL as a permitted VPN 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 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. svc ask none default svc

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as
remote access 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 prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#
```

Stabilire la connessione VPN SSL con SVC

Per stabilire una connessione VPN SSL con ASA, completare la procedura seguente:

1. Immettere 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. Inoltre, scegliere il proprio gruppo dall'elenco a discesa come mostrato. 

   Questa finestra viene visualizzata prima della connessione VPN

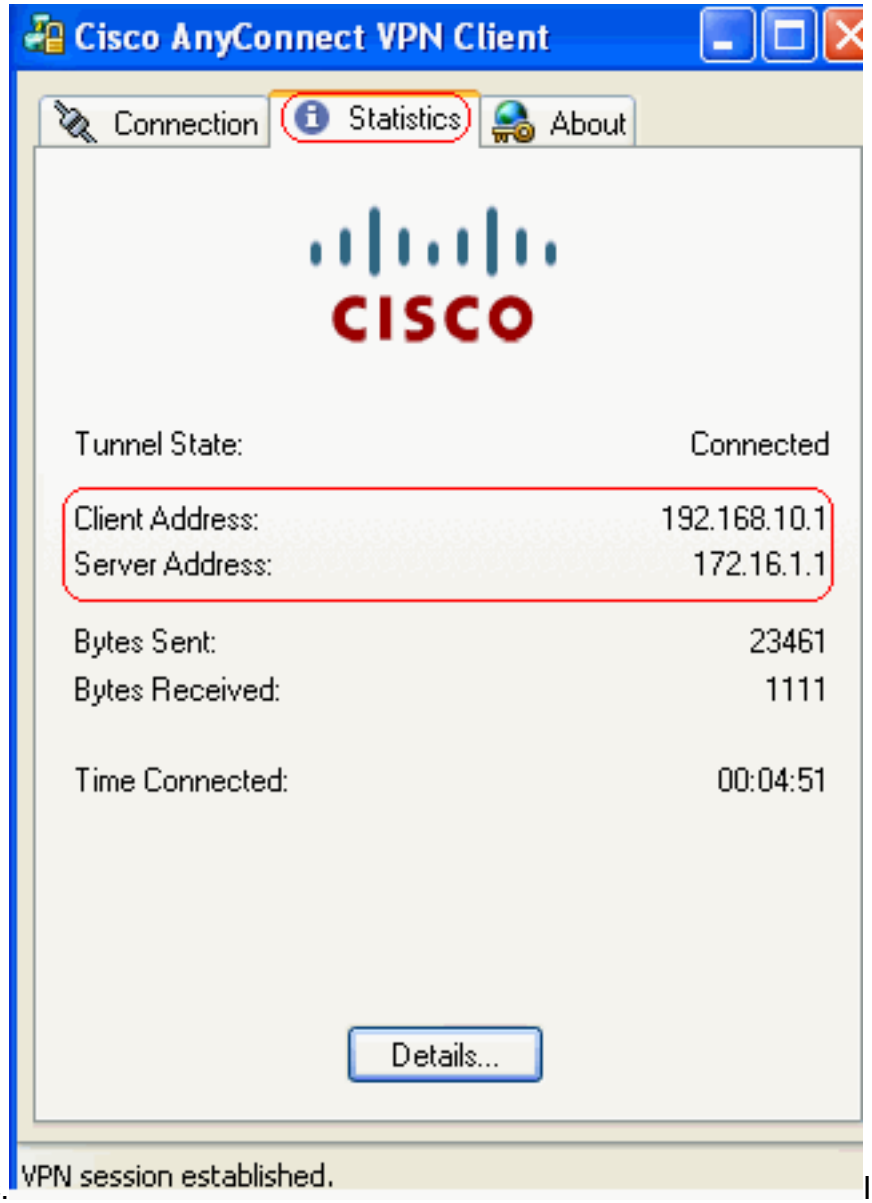
SSL.

Nota: il software ActiveX deve essere installato sul computer prima di scaricare SVC.Questa finestra viene visualizzata una volta stabilita la connessione.

3. Fare clic sul blocco visualizzato nella barra delle applicazioni del

computer. 

Viene visualizzata questa finestra che fornisce informazioni sulla connessione SSL. Ad esempio, **192.168.10.1** è l'indirizzo IP assegnato dall'ASA,



ecc. In questa finestra vengono visualizzate le informazioni sulla versione del client VPN Cisco

AnyConnect.

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:/anyconnect-win-2.0.0343-k9.pkg 1
  CISCO STC win2k+
  2,0,0343
  Mon 04/23/2007  4:16:34.63

1 SSL VPN Client(s) installed
```

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

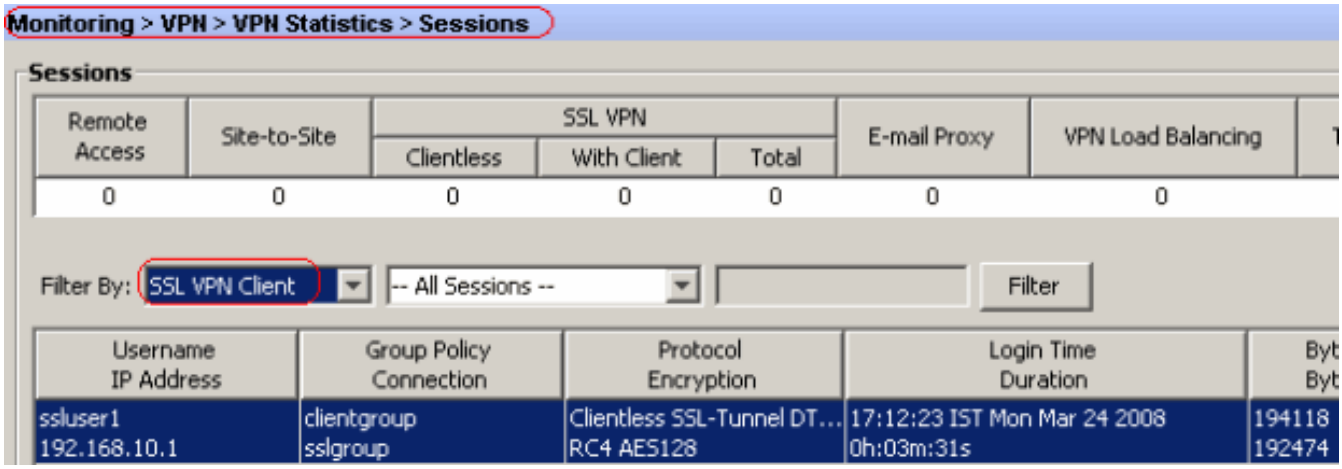
```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1                Index        : 12
```

```
Assigned IP  : 192.168.10.1          Public IP    : 192.168.1.1
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128            Hashing      : SHA1
Bytes Tx     : 194118                Bytes Rx     : 197448
Group Policy : clientgroup           Tunnel Group : sslgroup
Login Time   : 17:12:23 IST Mon Mar 24 2008
Duration     : 0h:12m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```

- **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
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1

ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)
```

   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, e
tc)
Called vpn_remove_uauth: success!
```

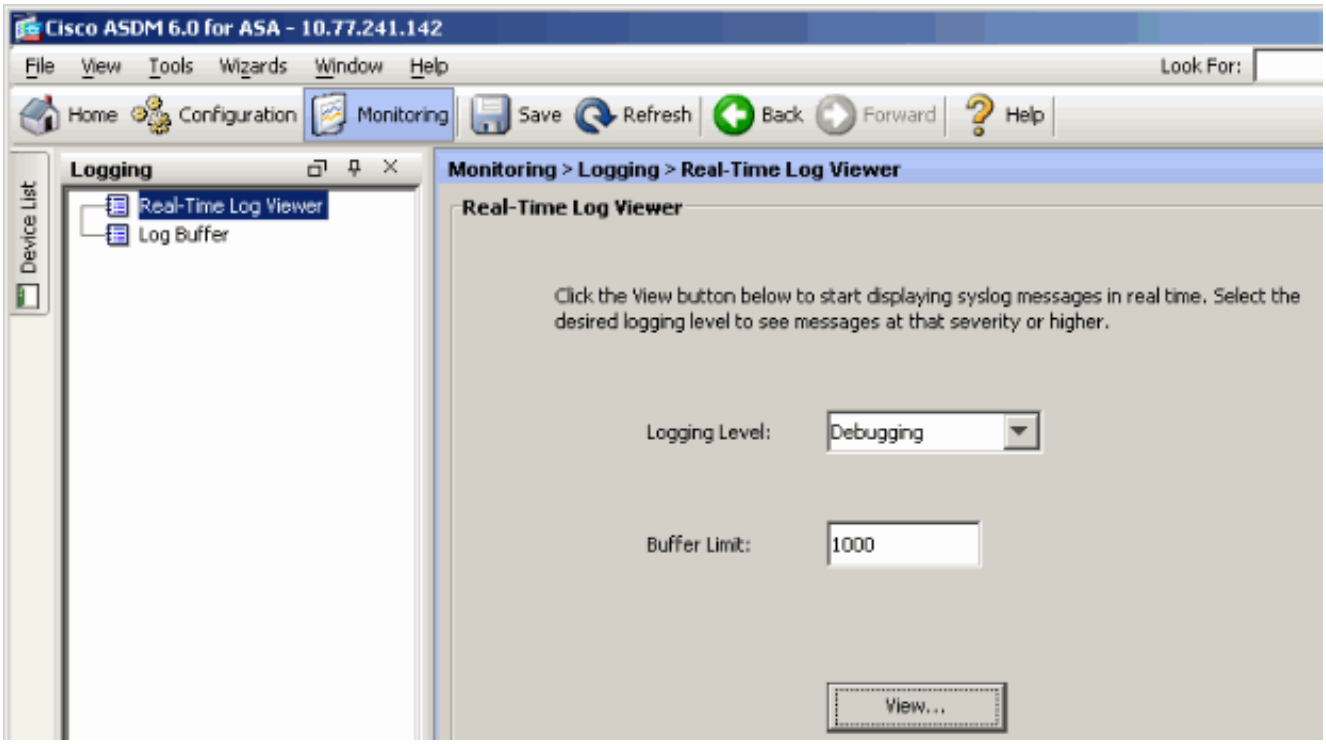
```
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xA000)



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.

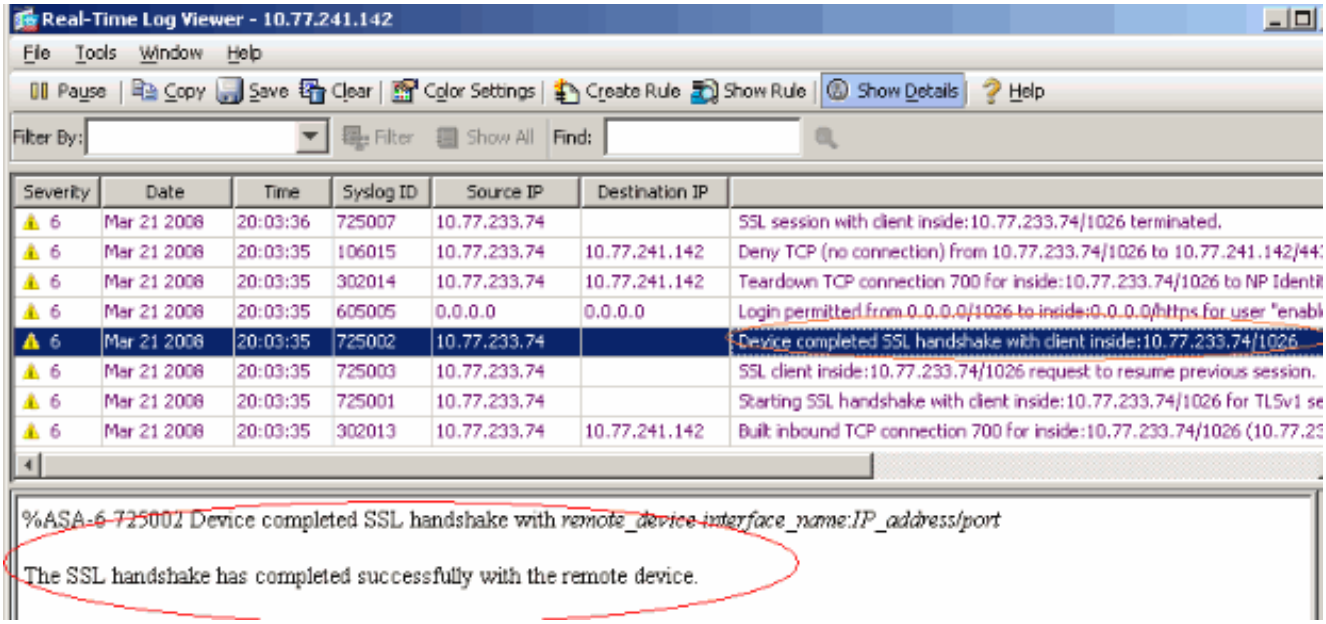
```
Ciscoasa#debug webvpn svc 7

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 AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343
'
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B
7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
625B92C1338D631B08B7D75F4EDEF26'
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
5F4EDEF26'
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: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
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
np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

4. In ASDM, scegliere **Monitoraggio > Log > Visualizzatore log in tempo reale > Visualizza** per visualizzare gli eventi in tempo
reale.



Nell'esempio viene mostrato come stabilire una sessione SSL con il dispositivo headend.



Informazioni correlate

- Cisco serie 5500 Adaptive Security Appliance - Pagina di supporto
- Note sulla versione per AnyConnect VPN Client, versione 2.0
- 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