Esempio di configurazione di ASA con WebVPN e Single Sign-On con ASDM e NTLMv1

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) in modo che passi automaticamente le credenziali di accesso dell'utente WebVPN, nonché l'autenticazione secondaria, ai server che richiedono una convalida di accesso aggiuntiva in Windows Active Directory con NT LAN Manager versione 1 (NTLMv1). Questa funzionalità è nota come Single Sign-On (SSO). Fornisce ai collegamenti configurati per uno specifico gruppo WebVPN la possibilità di trasmettere queste informazioni di autenticazione utente, eliminando in tal modo più richieste di autenticazione. Questa funzione può essere utilizzata anche a livello di configurazione globale o utente.

Prerequisiti

Requisiti

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

- Verificare che le autorizzazioni NTLMv1 e Windows per gli utenti VPN di destinazione siano configurate. Per ulteriori informazioni sui diritti di accesso al dominio di Windows, consultare la documentazione di Microsoft.

Componenti usati

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

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Microsoft Internet Information Services (IIS)

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.

Configurazione

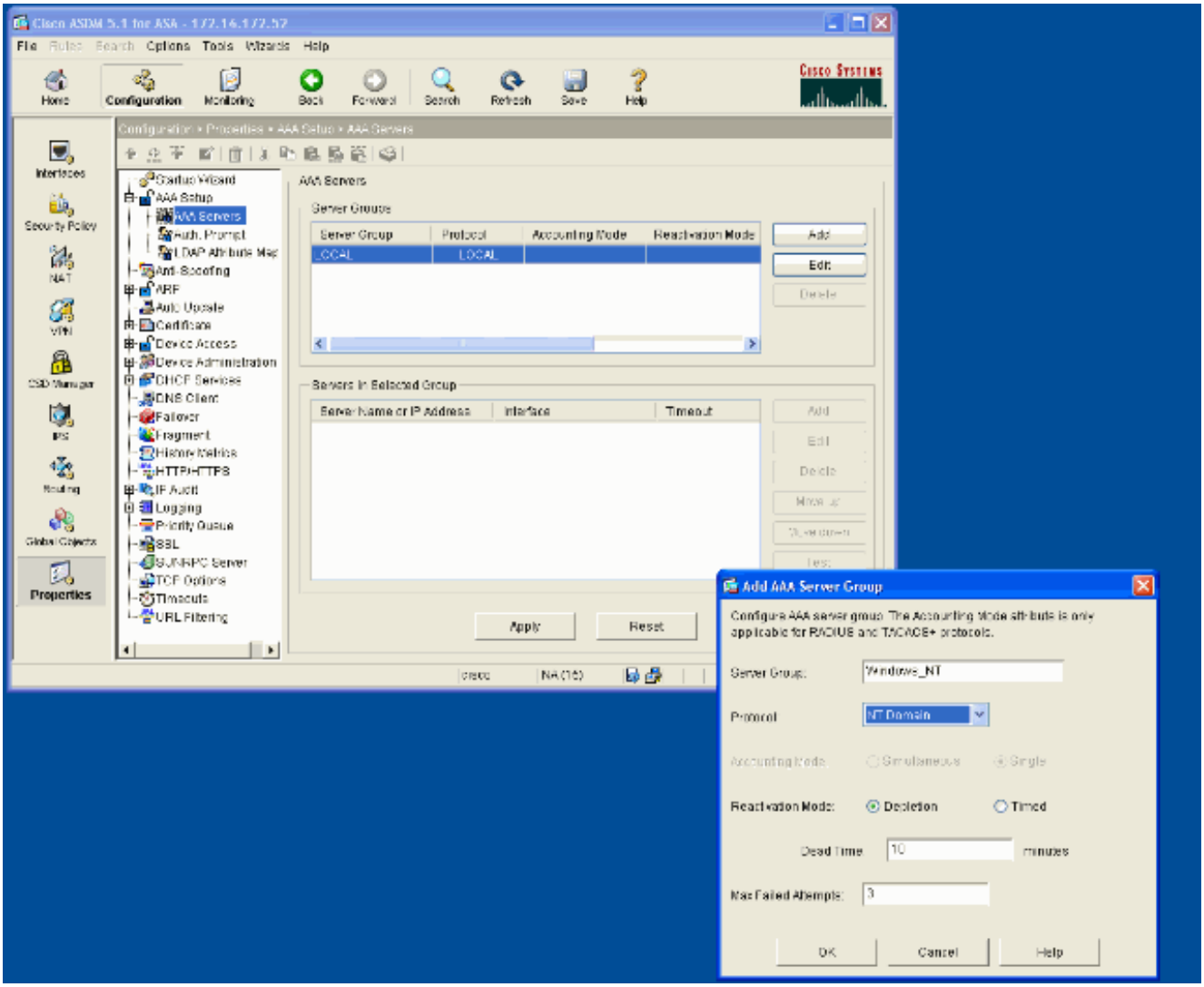
In questa sezione vengono presentate le informazioni necessarie per configurare l'ASA come server WebVPN con SSO.

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

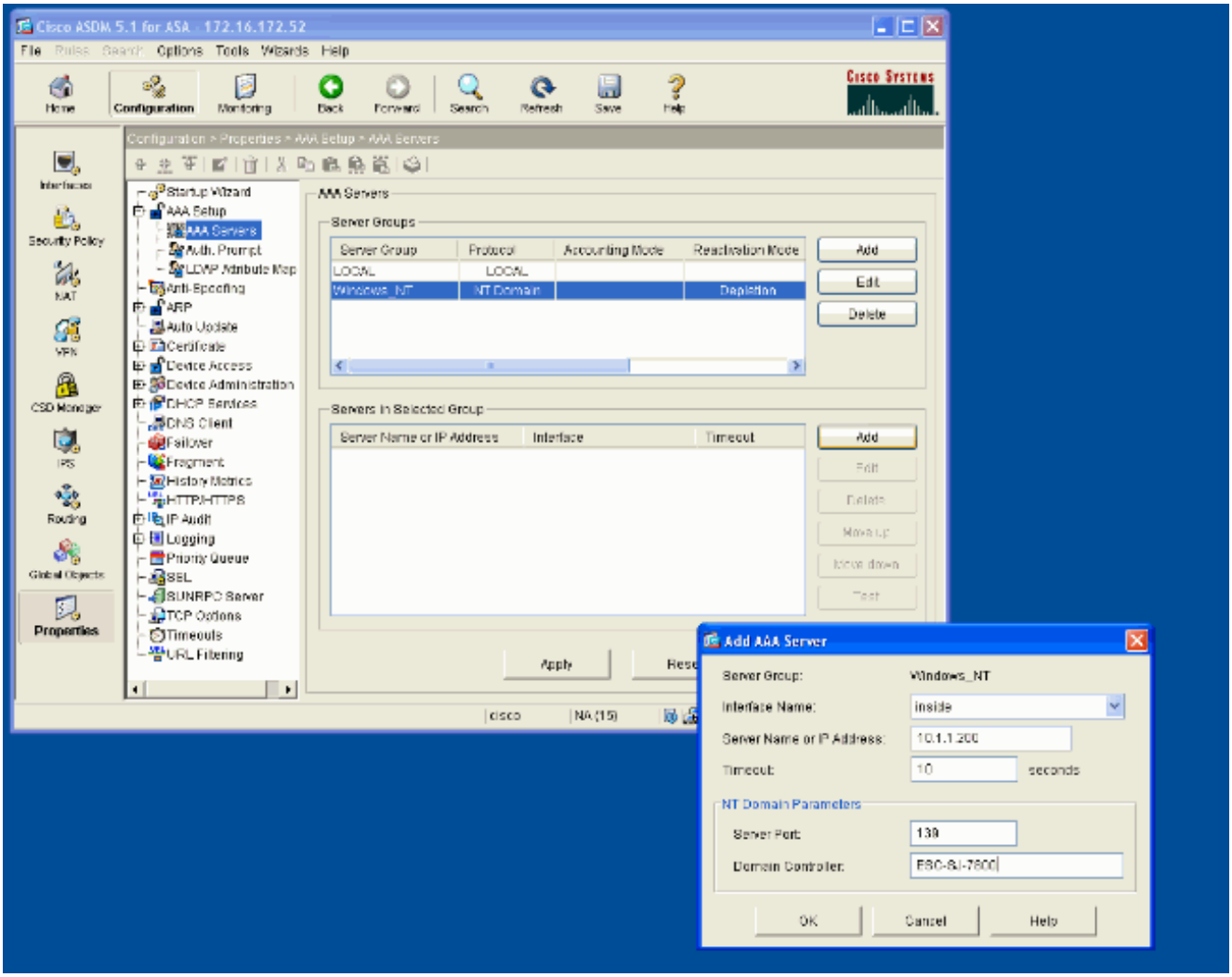
Aggiungere un server AAA per l'autenticazione del dominio Windows

Completare la procedura descritta di seguito per configurare l'appliance ASA in modo che utilizzi un controller di dominio per l'autenticazione.

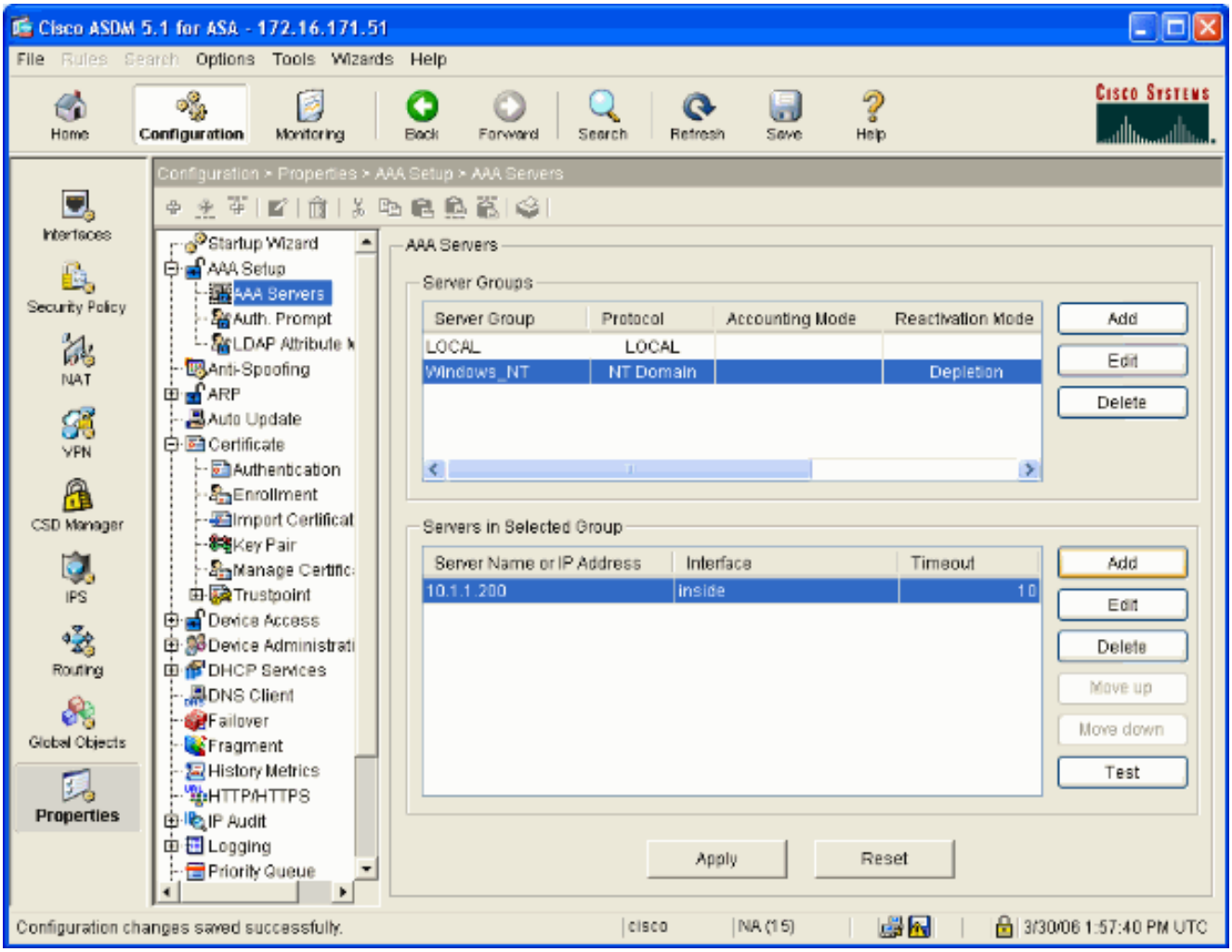
1. Selezionare **Configurazione > Proprietà > Impostazione AAA > Server AAA** e fare clic su **Aggiungi**. Fornire un nome per il gruppo di server, ad esempio Windows_NT, e scegliere **Dominio NT** come
protocollo.



2. Aggiungere un server Windows.Selezionare il gruppo appena creato e fare clic su **Aggiungi**. Selezionare l'interfaccia in cui si trova il server e immettere l'indirizzo IP e il nome del controller di dominio. Assicurarsi che il nome del controller di dominio sia scritto in maiuscolo. Al termine, fare clic su
OK.



Questa finestra mostra la configurazione AAA completata:

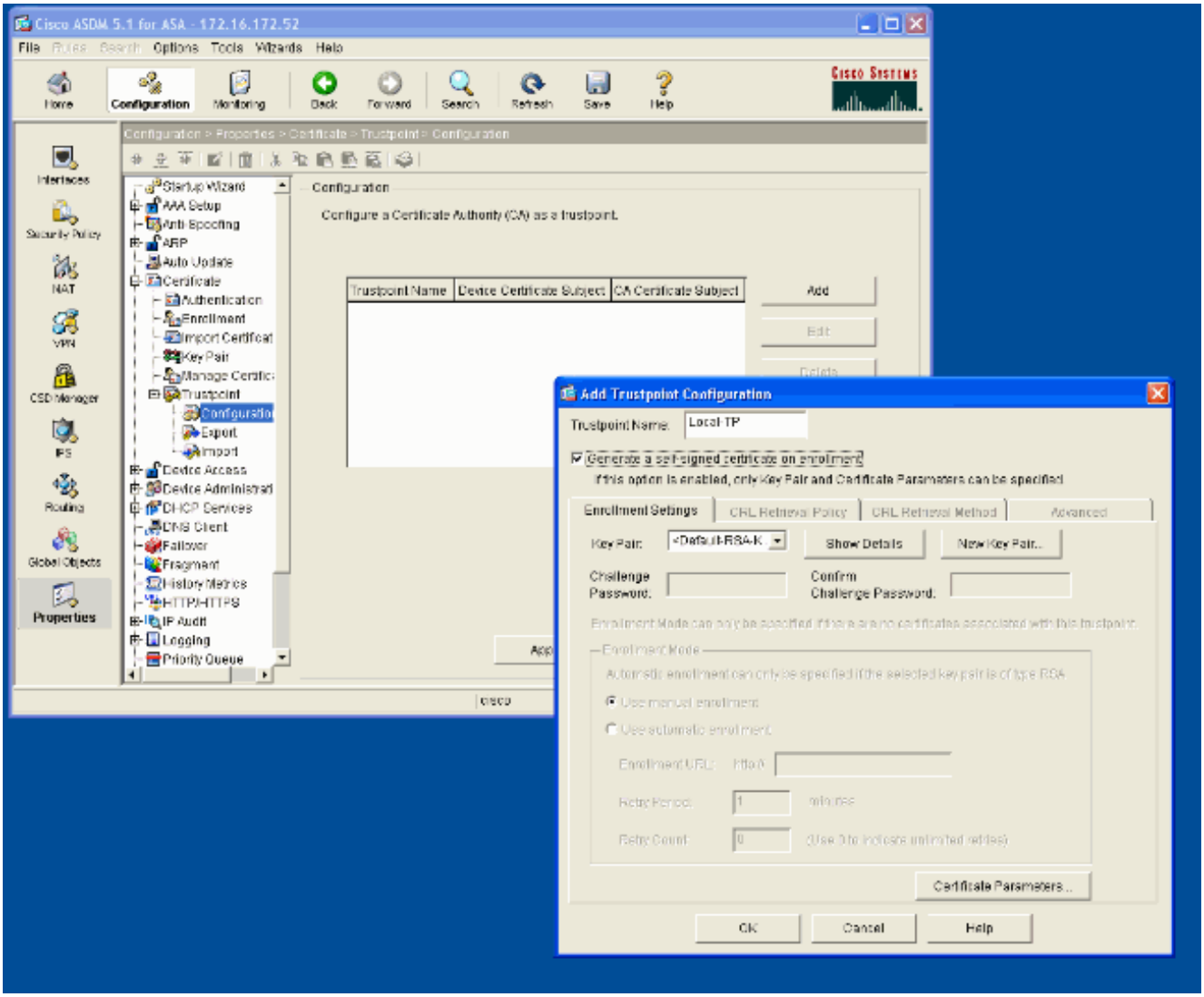


Creare un certificato autofirmato

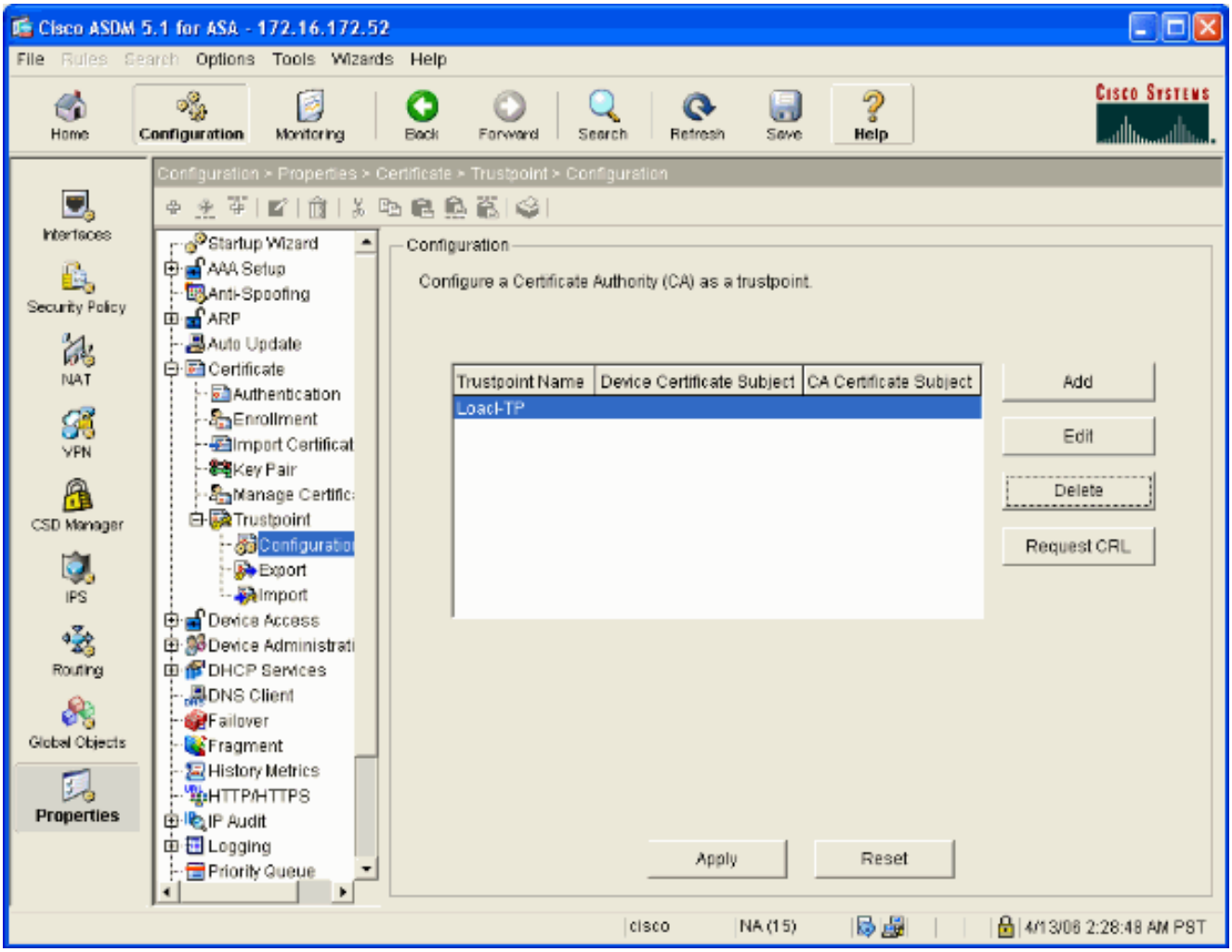
Completare la procedura seguente per configurare l'appliance ASA per l'utilizzo di un certificato autofirmato.

Nota: in questo esempio viene utilizzato un certificato autofirmato per semplificare la gestione. Per ulteriori opzioni di registrazione dei certificati, ad esempio la registrazione a un'Autorità di certificazione esterna, vedere Configurazione dei certificati.

1. Selezionare **Configurazione > Proprietà > Certificato > Trustpoint > Configurazione** e fare clic su **Aggiungi**.
2. Nella finestra che viene visualizzata, immettere un nome di trust, ad esempio Local-TP, e selezionare **Generate a self-signed certificate on enrollment (Genera certificato autofirmato all'iscrizione)**. È possibile lasciare invariate le altre opzioni con le relative impostazioni predefinite. Al termine, fare clic su
OK.



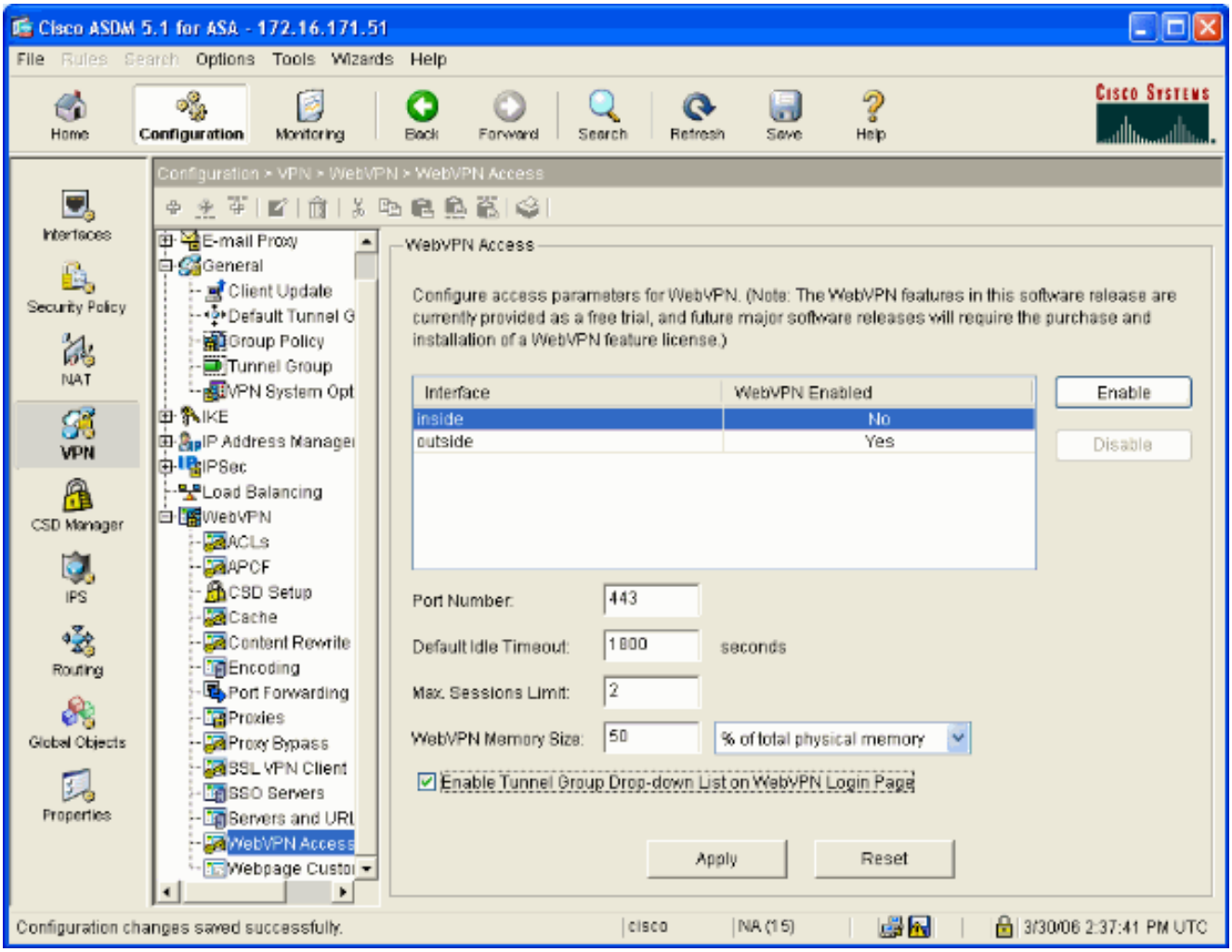
In questa finestra viene visualizzata la configurazione di Trustpoint completata:



Abilita WebVPN sull'interfaccia esterna

Completare questa procedura per consentire agli utenti esterni alla rete di connettersi utilizzando WebVPN.

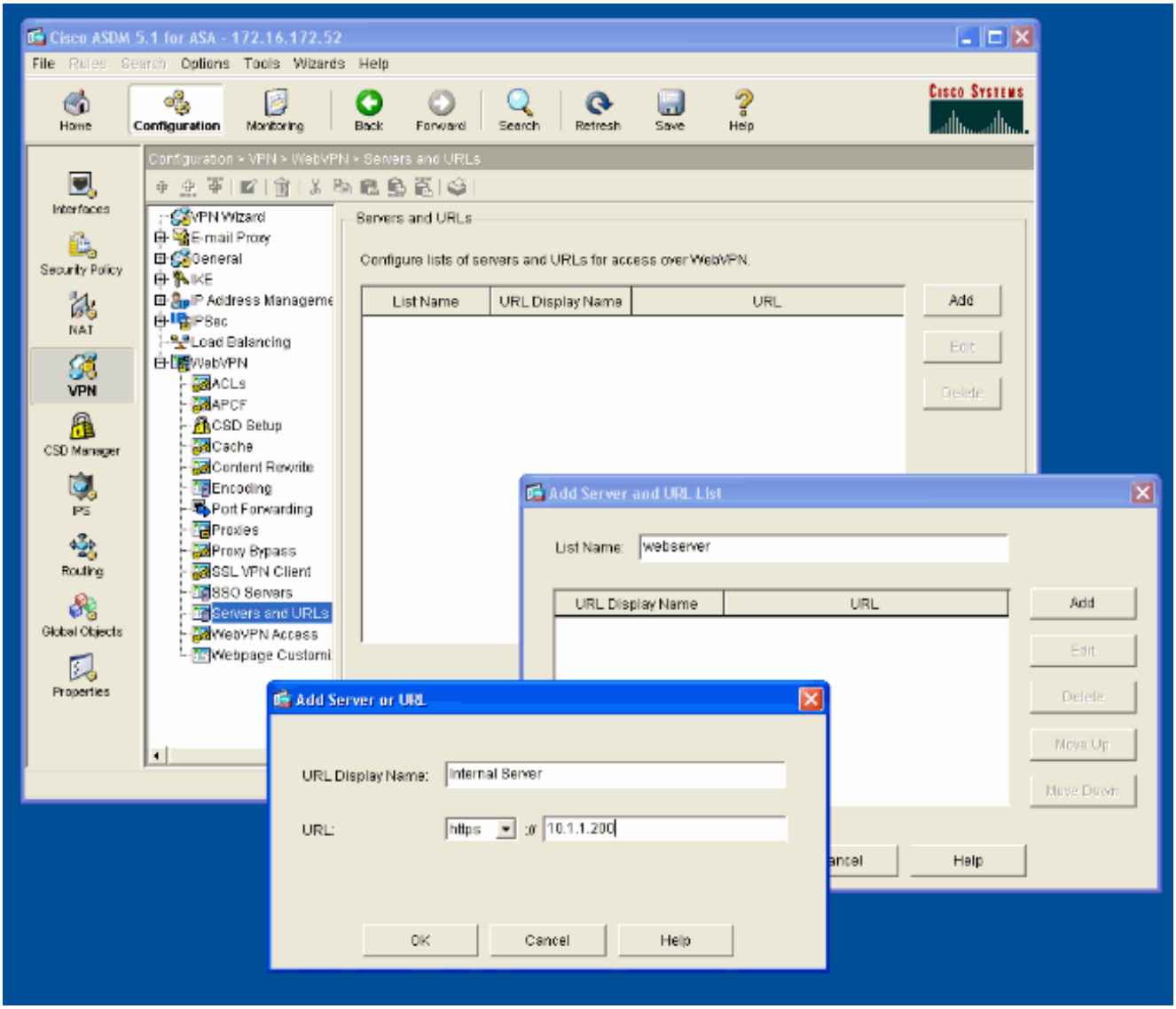
1. Selezionare **Configurazione > VPN > WebVPN > Accesso WebVPN**.
2. Selezionare l'interfaccia desiderata, fare clic su **Abilita** e selezionare **Abilita elenco a discesa Gruppo tunnel nella pagina di accesso a WebVPN.Nota:** se si utilizza la stessa interfaccia per l'accesso WebVPN e ASDM, è necessario modificare la porta predefinita per l'accesso ASDM dalla porta 80 a una nuova porta, ad esempio 8080. Questa operazione viene eseguita in **Configurazione > Proprietà > Accesso dispositivo > HTTPS/ASDM.Nota:** è possibile reindirizzare automaticamente un utente alla porta 443 nel caso in cui un utente passi a **http://<indirizzo_ip>** anziché a **https://<indirizzo_ip>**. Selezionare **Configurazione > Proprietà > HTTP/HTTPS**, scegliere l'interfaccia desiderata, fare clic su **Modifica** e selezionare **Reindirizza HTTP a HTTPS**.



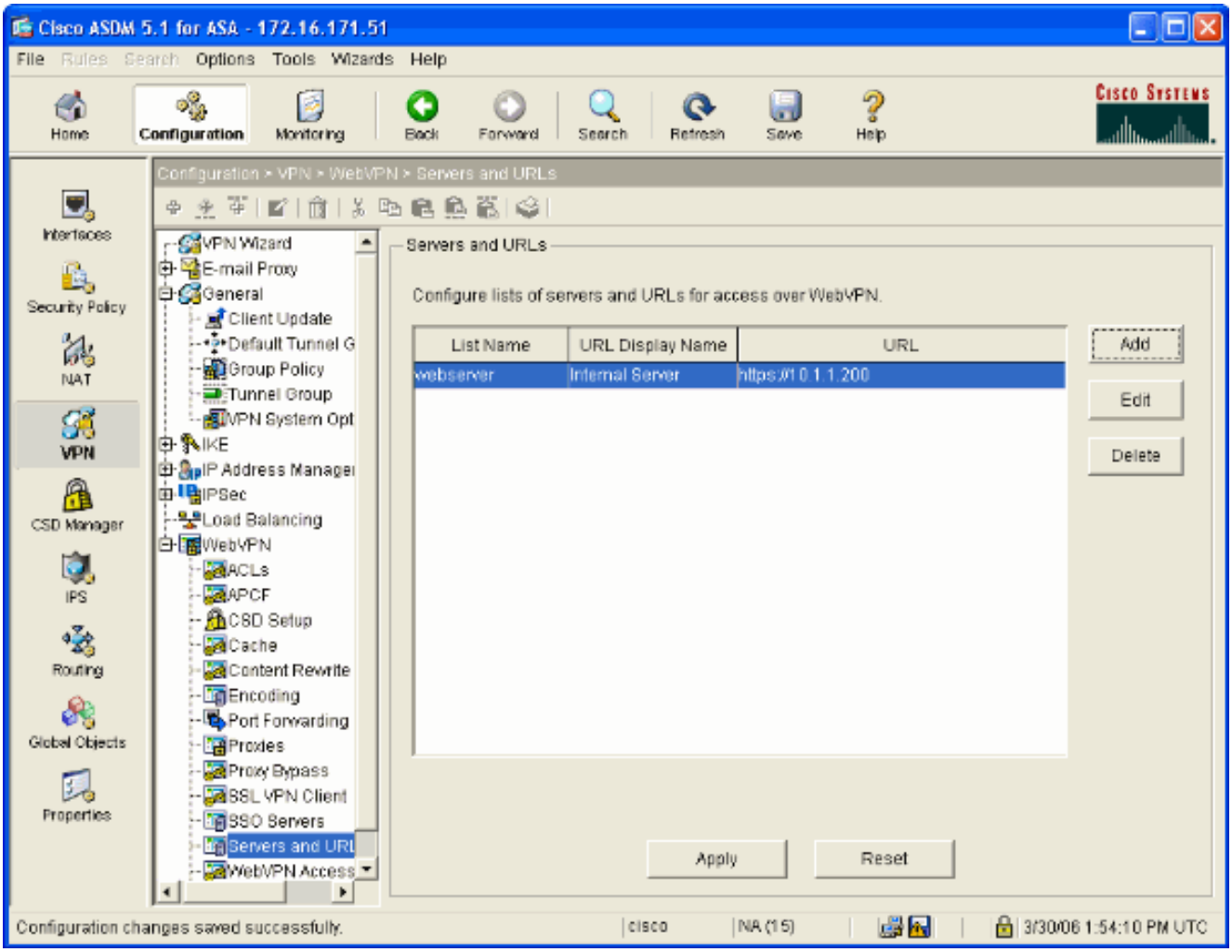
Configurare un elenco di URL per i server interni

Completare questi passaggi per creare un elenco contenente i server per i quali si desidera concedere l'accesso agli utenti WebVPN.

1. Selezionare **Configurazione > VPN > WebVPN > Server e URL** e fare clic su **Aggiungi**.
2. Immettere un nome per l'elenco di URL. Questo nome non è visibile agli utenti finali. Fare clic su **Add**.
3. Immettere il nome visualizzato dell'URL da visualizzare agli utenti. Immettere le informazioni sull'URL del server. Questo dovrebbe essere il modo in cui si accede normalmente al server.



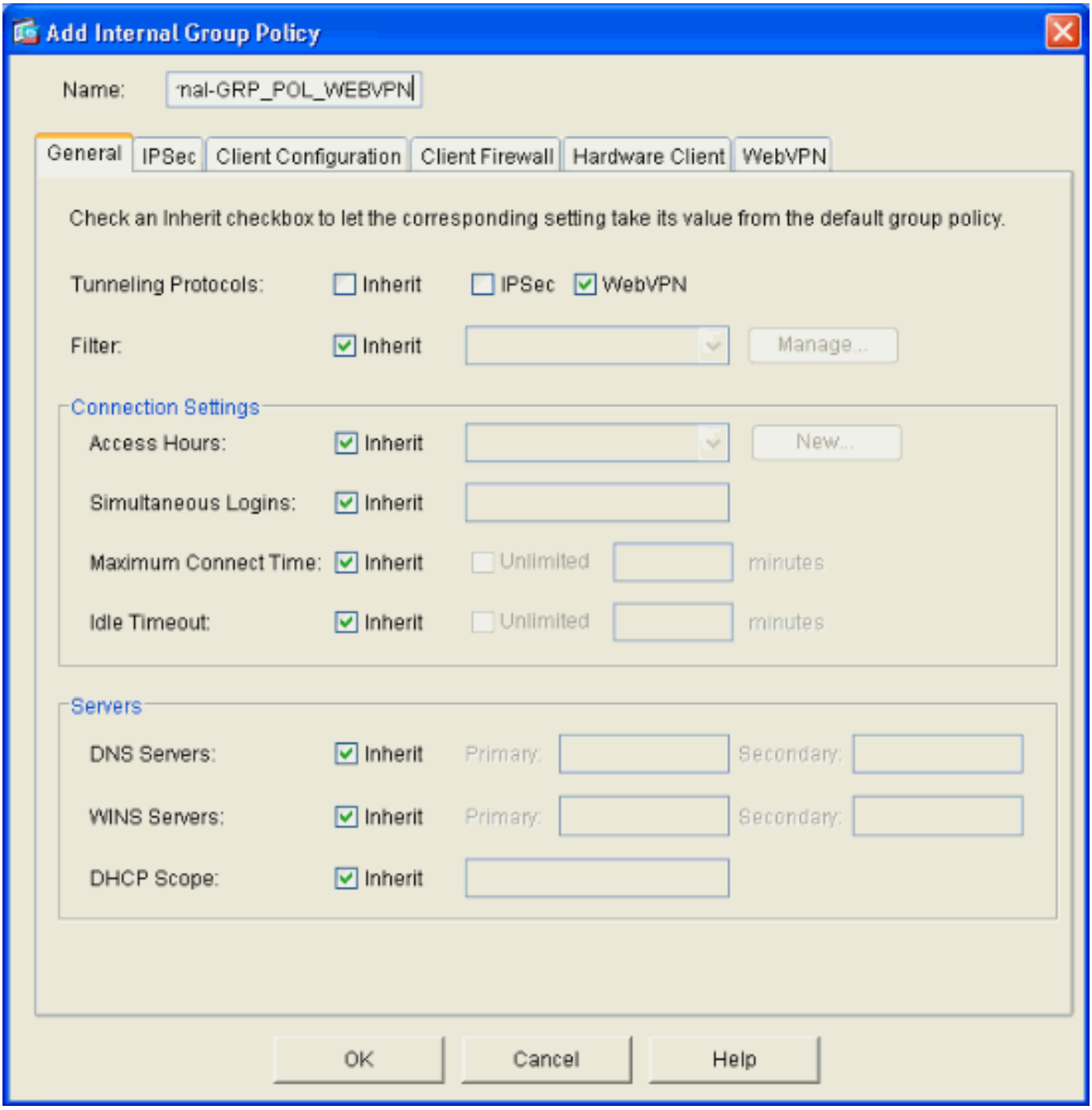
4. Fare clic su **OK**, **OK** e quindi su **Applica**.



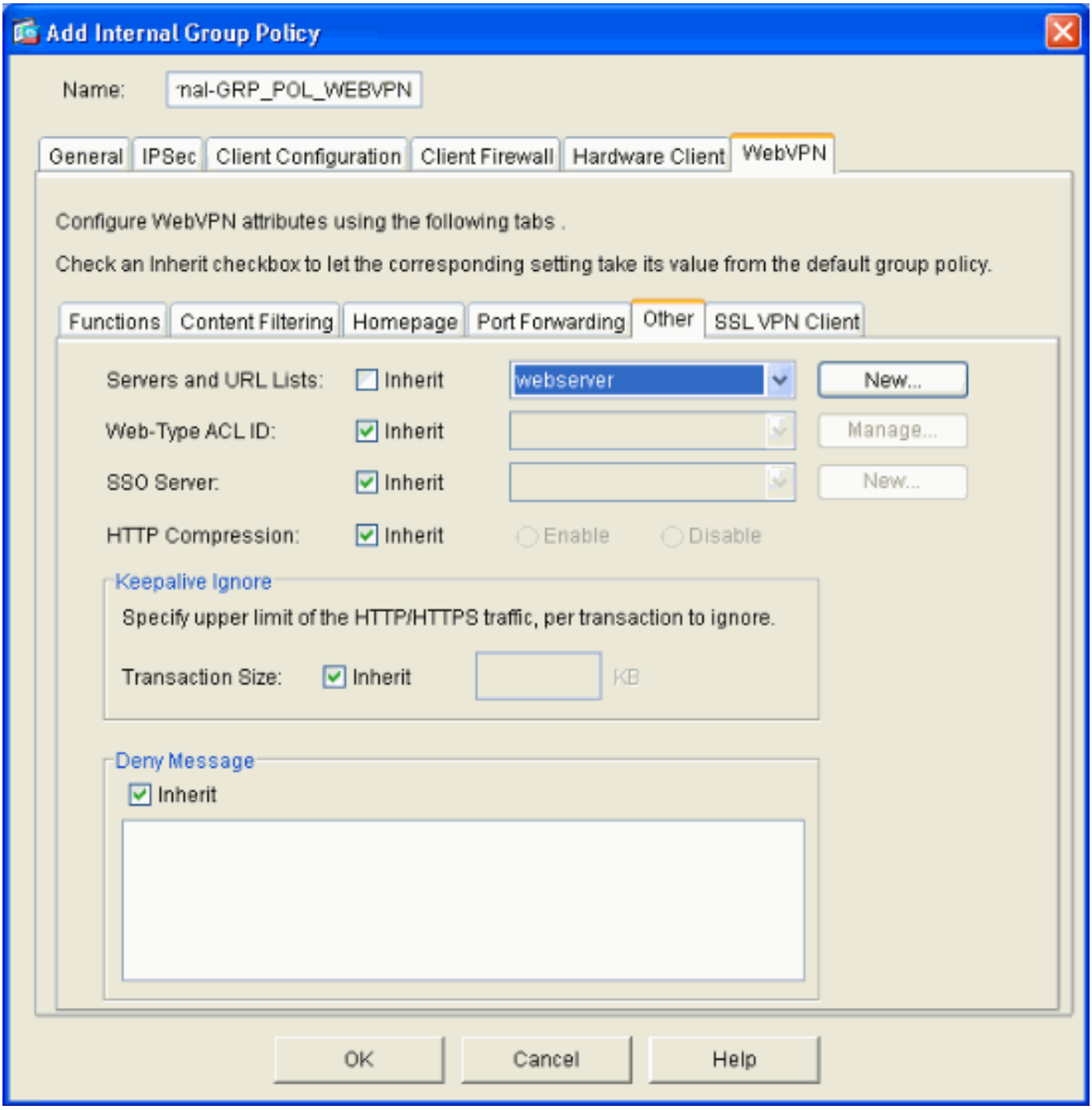
Configurare Criteri di gruppo interni

Completare la procedura seguente per configurare un criterio di gruppo per gli utenti WebVPN.

1. Selezionare **Configurazione > VPN > Generale > Criteri di gruppo**, fare clic su **Aggiungi** e selezionare **Criteri di gruppo interni**.
2. Nella scheda Generale specificare un nome di criterio, ad esempio Gruppo interno_POL_WEBVPN. Quindi, deselezionare **Inherit** (Eredita) accanto a Tunneling Protocol (Protocolli di tunneling) e selezionare **WebVPN** (VPN Web).



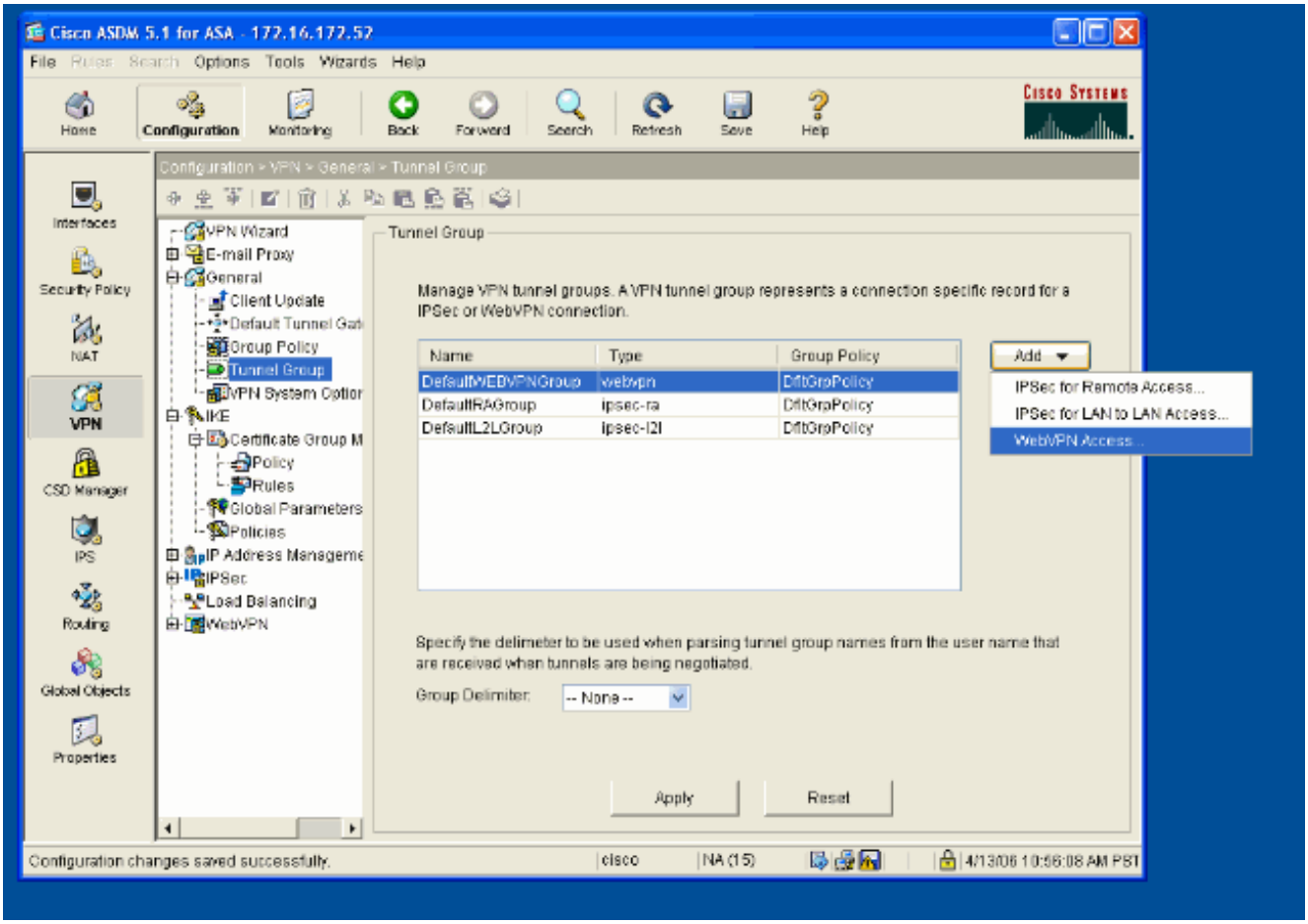
3. Nella scheda WebVPN selezionare la scheda secondaria **Altro**. Deselezionare **Inherit** (Eredita) accanto a Server ed elenchi URL, quindi selezionare l'elenco di URL configurato dall'elenco a discesa. Al termine, fare clic su **OK**.



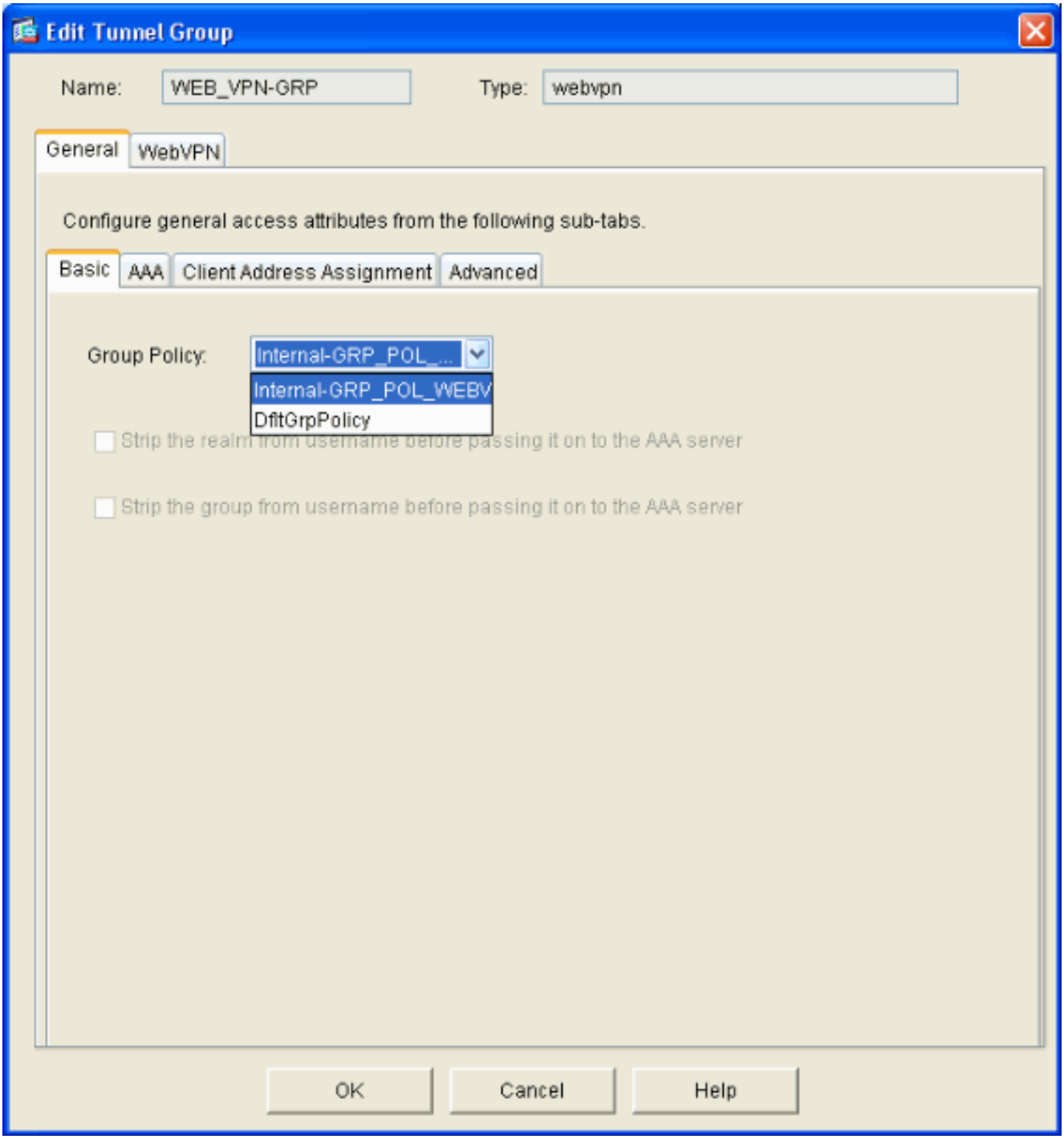
Configurare un gruppo di tunnel

Completare questa procedura per configurare un gruppo di tunnel per gli utenti WebVPN.

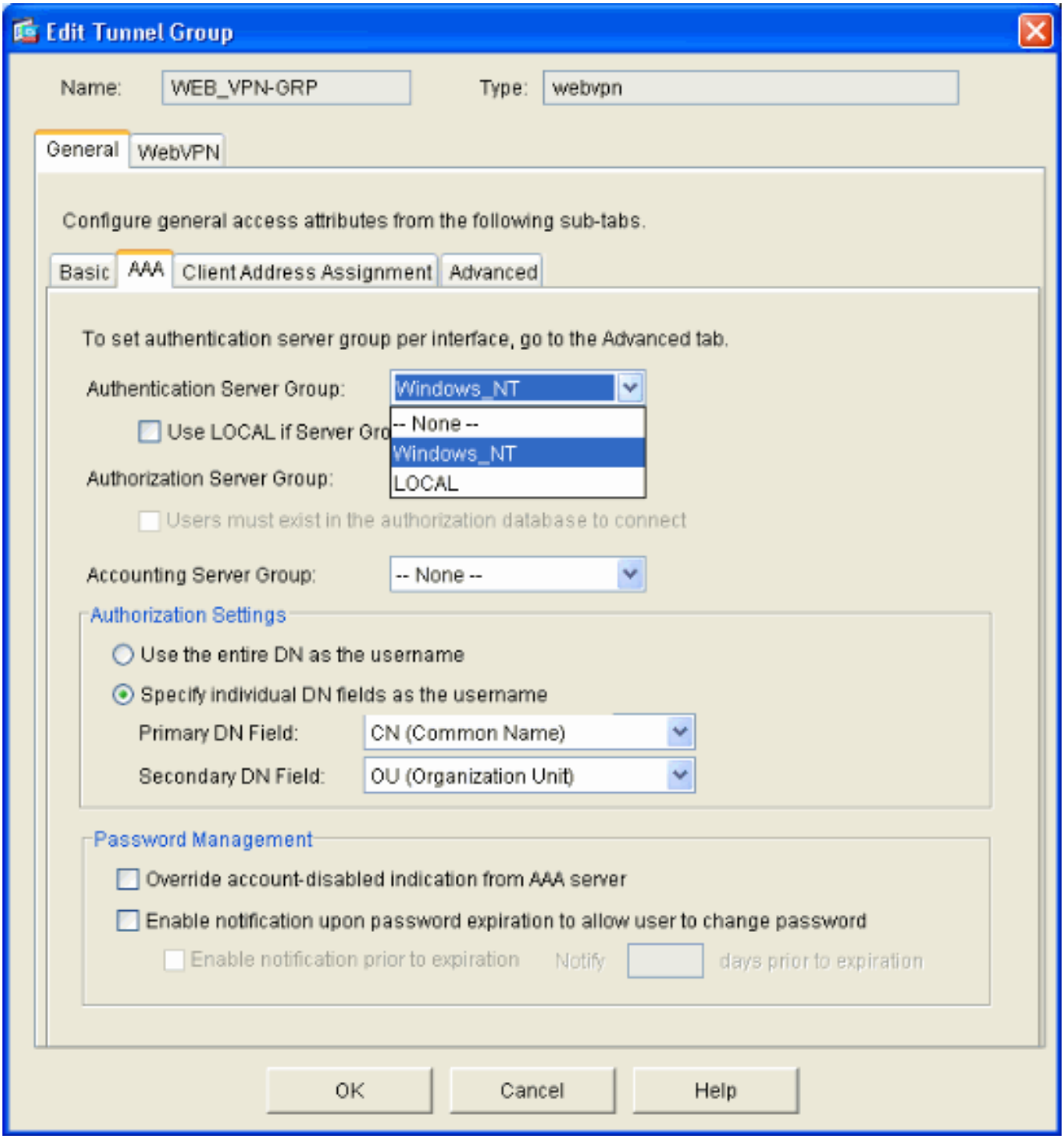
1. Selezionare **Configurazione > VPN > Generale > Gruppo tunnel**, fare clic su **Aggiungi** e selezionare **Accesso WebVPN...**



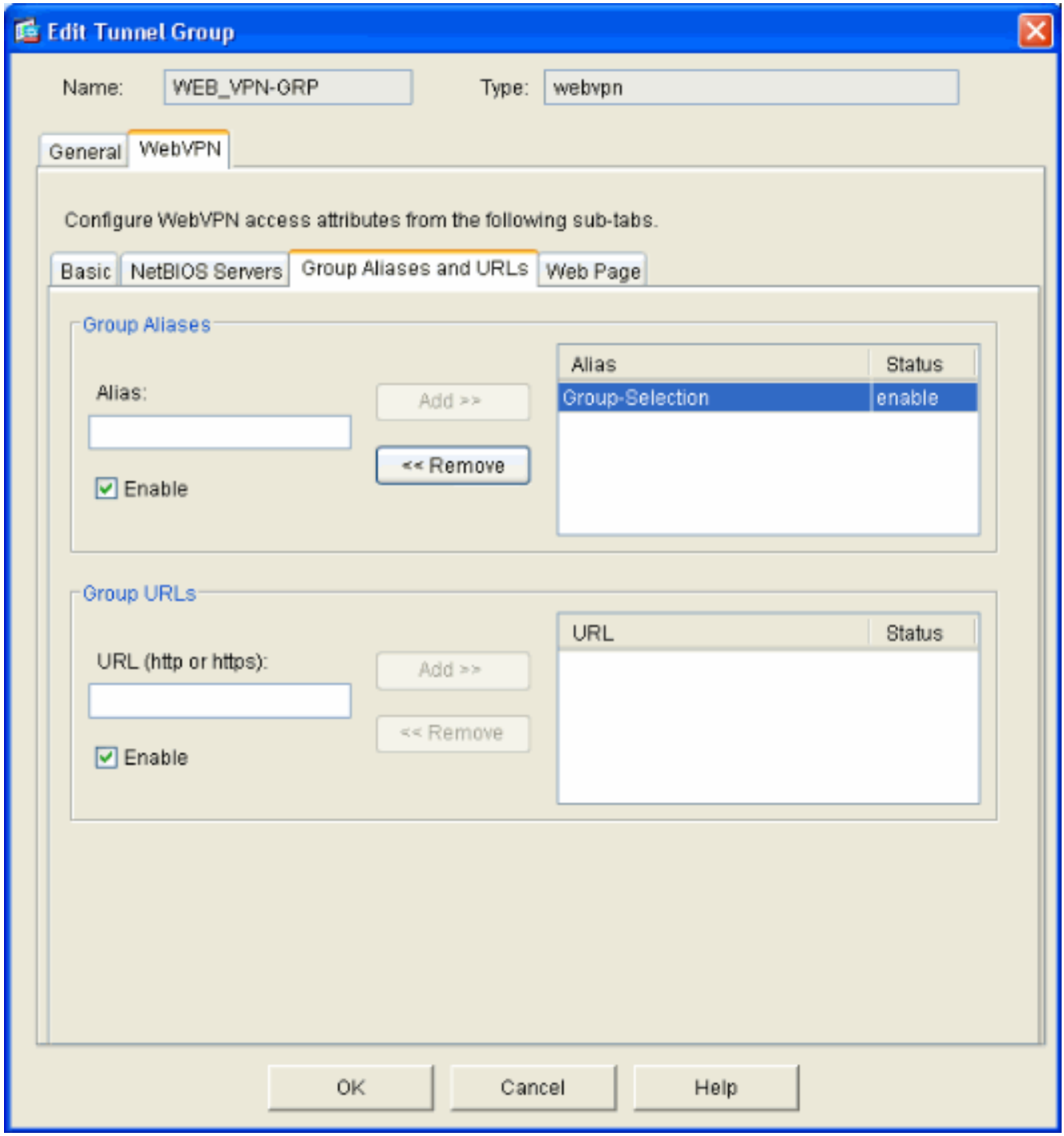
2. Immettere un nome per il gruppo di tunnel, ad esempio WEB_VPN-GRP. Nella scheda Base selezionare i Criteri di gruppo creati e verificare che il tipo di gruppo sia **webvpn**.



3. Selezionare la scheda AAA.In Gruppo server di autenticazione scegliere il gruppo configurato per abilitare l'autenticazione NTLMv1 con il controller di dominio.**Facoltativo:** Selezionare **Utilizza LOCAL se il gruppo di server non riesce** a abilitare l'uso del database locale nel caso in cui si verifichi un errore nel gruppo AAA configurato. Ciò consente di risolvere i problemi in un secondo momento.



4. Andare alla scheda WebVPN e quindi alla scheda secondaria **Alias e URL gruppo**.
5. Immettere un alias in Alias gruppo e fare clic su **Aggiungi**. Questo alias viene visualizzato nell'elenco a discesa visualizzato agli utenti WebVPN al momento dell'accesso.



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

Configurare la firma automatica per un server

Passare alla riga di comando per abilitare SSO per i server interni.

Nota: questo passaggio non può essere completato in ASDM e deve essere eseguito dalla riga di comando. Per ulteriori informazioni, fare riferimento a Accesso all'interfaccia della riga di comando.

Utilizzare il comando **auto-signon** per specificare la risorsa di rete, ad esempio un server, a cui si desidera consentire l'accesso agli utenti. In questa configurazione è configurato un singolo indirizzo IP del server, ma è possibile specificare un intervallo di rete, ad esempio **10.1.1.0 /24**. Per ulteriori informazioni, fare riferimento al comando **auto-sign**.

```
ASA>enable
ASA#configure terminal
ASA(config)#webvpn
ASA(config-webpvn)#auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
ASA(config-webvpn)#quit
ASA(config)#exit
ASA#write memory
```

In questo output di esempio, il comando **auto-sign** è configurato globalmente per WebVPN. Questo comando può essere utilizzato anche in modalità di configurazione gruppo WebVPN o nome utente WebVPN. L'utilizzo di questo comando nella modalità di configurazione gruppo WebVPN lo limita a un gruppo particolare. Analogamente, l'utilizzo di questo comando nella modalità di configurazione del nome utente WebVPN lo limita a un singolo utente. Per ulteriori informazioni, fare riferimento al comando auto-sign.

Configurazione finale dell'ASA

Nel documento viene usata questa configurazione:

ASA versione 7.1(1)

```
ASA# show running-config
: Saved
:
ASA Version 7.1(1)
!
terminal width 200
hostname ASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.171.51 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 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
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm512.bin
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 172.16.171.1 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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- AAA server configuration aaa-server Windows_NT
protocol nt aaa-server Windows_NT host 10.1.1.200 nt-
auth-domain-controller ESC-SJ-7800 !--- Internal group
policy configuration group-policy Internal-
GRP_POL_WEBVPN internal group-policy Internal-
GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn
webvpn url-list value webserver username cisco password
Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa
authentication http console LOCAL aaa authentication ssh
console LOCAL aaa authentication enable console LOCAL
http server enable 8181 http 0.0.0.0 0.0.0.0 outside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart !--- Trustpoint/certificate configuration
crypto ca trustpoint Local-TP enrollment self crl
configure crypto ca certificate chain Local-TP
certificate 31 308201b0 30820119 a0030201 02020131
300d0609 2a864886 f70d0101 04050030 1e311c30 1a06092a
864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30
1e170d30 36303333 30313334 3930345a 170d3136 30333237
31333439 30345a30 1e311c30 1a06092a 864886f7 0d010902
160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86
4886f70d 01010105 0003818d 00308189 02818100 e47a29cd
56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4
a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f
30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18
496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc
ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7
4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500
03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15
e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e
1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21
49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16
a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076
294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group
configuration tunnel-group WEB_VPN-GRP type webvpn
tunnel-group WEB_VPN-GRP general-attributes
authentication-server-group Windows_NT default-group-
policy Internal-GRP_POL_WEBVPN tunnel-group WEB_VPN-GRP
webvpn-attributes group-alias Group-Selection enable
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512
```

```
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 Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6
: end
```

Verifica

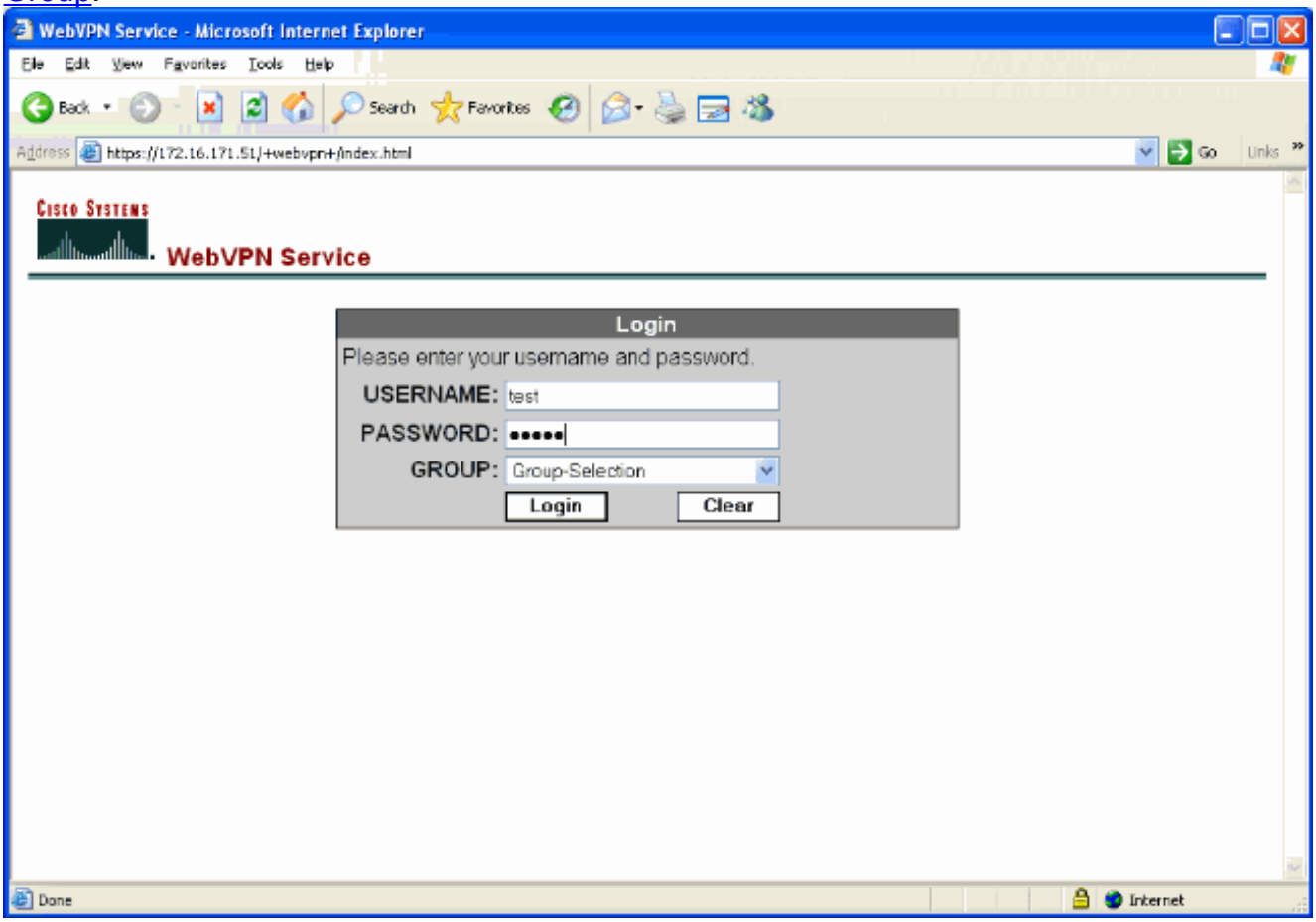
Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

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

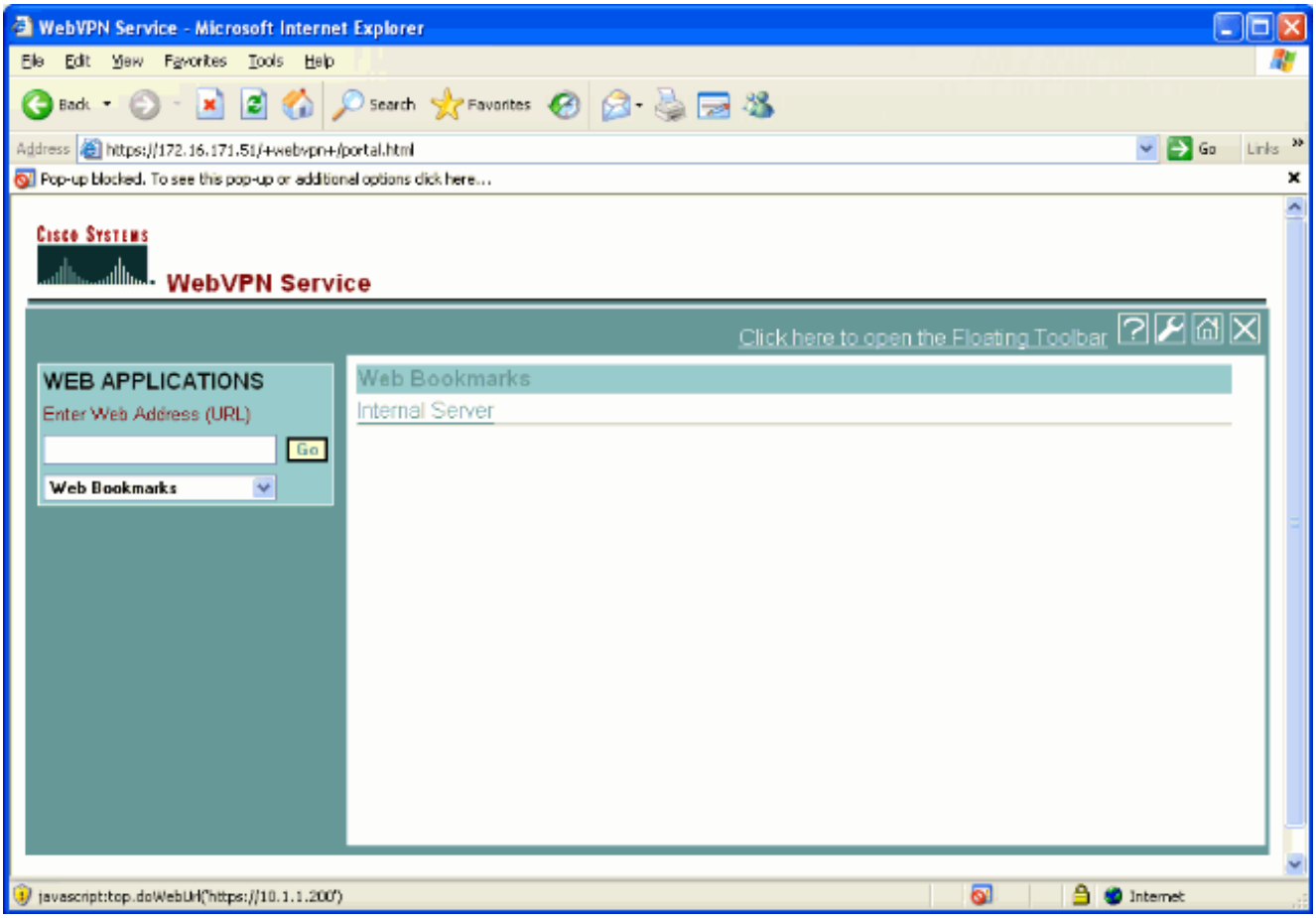
Verifica accesso WebVPN

Eseguire il login come utente per verificare la configurazione.

1. Tentare di accedere all'appliance ASA con le informazioni utente dal dominio NT. Selezionare l'alias del gruppo configurato nel passaggio 5 in Configure a Tunnel Group.

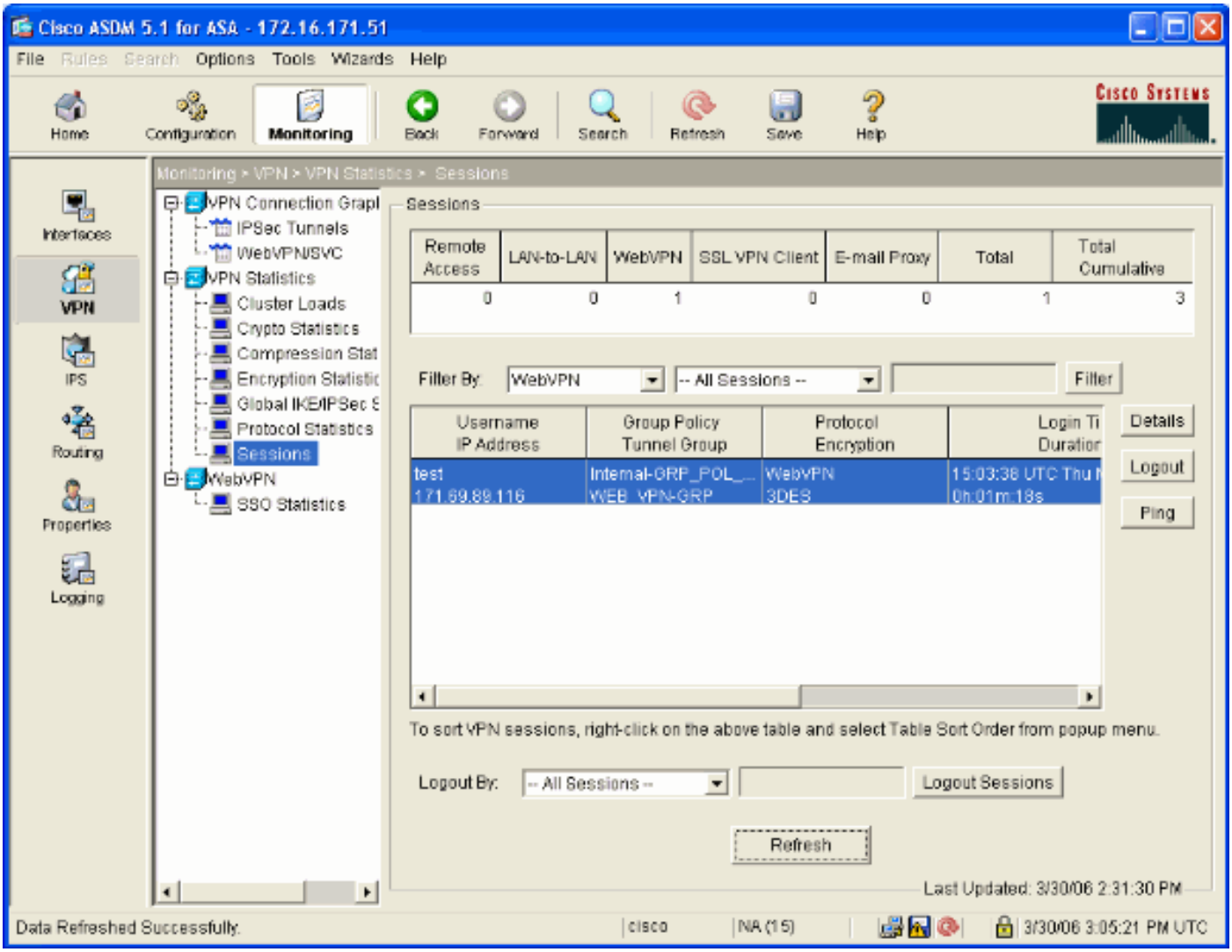


2. Cercare i collegamenti configurati per i server interni. Fai clic sul link per verificare.



Sessioni di monitoraggio

Selezionare **Monitoraggio > VPN > Statistiche VPN > Sessioni** e cercare una sessione WebVPN appartenente al gruppo configurato in questo documento.



Debug di una sessione WebVPN

Questo output è un esempio di debug di una sessione WebVPN riuscita.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

```
ASA#debug webvpn 255
INFO: debug webvpn enabled at level 255
ASA#
ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286]
WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782]
!--- Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started
user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422]
WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095]
WebVPN: user: (test) authenticated.
!--- End AAA webvpn_auth.c:http_webvpn_auth_accept[2093]
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
```

```
WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136]
webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202]
traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421]
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
!--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Risoluzione dei problemi

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

- Se la casella a discesa Gruppo non è presente nella pagina di accesso di WebVPN, accertarsi di aver completato il passaggio 2 in Abilita WebVPN sull'interfaccia esterna e il passaggio 5 in Configura un gruppo di tunnel. Se questi passaggi non vengono completati e l'elenco a discesa risulta mancante, l'autenticazione rientra nel gruppo predefinito e potrebbe non riuscire.
- Sebbene non sia possibile assegnare i diritti di accesso all'utente in ASDM o sull'appliance ASA, è possibile limitare gli utenti con diritti di accesso a Microsoft Windows sul controller di dominio. Aggiungere le autorizzazioni del gruppo NT necessarie per la pagina Web a cui l'utente esegue l'autenticazione. Una volta che l'utente accede a WebVPN con le autorizzazioni del gruppo, l'accesso alle pagine specificate viene concesso o negato di conseguenza. L'appliance ASA opera solo come host di autenticazione proxy per conto del controller di dominio e tutte le comunicazioni presenti sono NTLMv1.
- Impossibile configurare SSO per SharePoint su WebVPN. Il server SharePoint non supporta l'autenticazione basata su moduli. Di conseguenza, i segnalibri con post o la procedura di plug-in post non sono applicabili qui.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Documentazione e supporto tecnico – Cisco Systems