Esempio di configurazione di una VPN SSL thin-client (WebVPN) su un'appliance ASA con ASDM

Sommario

Introduzione

La tecnologia VPN SSL thin-client consente l'accesso sicuro per alcune applicazioni che dispongono di porte statiche, ad esempio Telnet(23), SSH(22), POP3(110), IMAP4(143) e SMTP(25). È possibile utilizzare la VPN SSL thin client come applicazione basata su utente, applicazione basata su regole o entrambe. In altri termini, è possibile configurare l'accesso in base all'utente oppure creare Criteri di gruppo in cui aggiungere uno o più utenti.

- **VPN SSL senza client (WebVPN)**: fornisce un client remoto che richiede un browser Web abilitato per SSL per accedere ai server Web HTTP o HTTPS su una rete LAN aziendale. Inoltre, la VPN SSL senza client fornisce l'accesso per l'esplorazione dei file di Windows tramite il protocollo CIFS (Common Internet File System). Outlook Web Access (OWA) è un

esempio di accesso HTTP.Per ulteriori informazioni sulla VPN SSL senza client, consultare l'esempio di configurazione di WebVPN (ClientSSL VPN) sull'appliance ASA.

- **Thin-Client SSL VPN (Port Forwarding)**: fornisce un client remoto che scarica una piccola applet basata su Java e consente l'accesso sicuro per le applicazioni TCP (Transmission Control Protocol) che utilizzano numeri di porta statici. Esempi di accesso protetto sono il protocollo POP3 (Post Office Protocol), il protocollo SMTP (Simple Mail Transfer Protocol), il protocollo IMAP (Internet Message Access Protocol), il protocollo ssh (Secure Shell) e Telnet. Poiché i file nel computer locale vengono modificati, per utilizzare questo metodo è necessario disporre dei privilegi di amministrazione locali. Questo metodo di VPN SSL non funziona con le applicazioni che utilizzano assegnazioni dinamiche delle porte, ad esempio alcune applicazioni FTP (File Transfer Protocol).**Nota:** UDP (User Datagram Protocol) non è supportato.
- **SSL VPN Client (modalità tunnel)**: scarica un client di piccole dimensioni sulla workstation remota e consente l'accesso sicuro alle risorse su una rete aziendale interna. È possibile scaricare in modo permanente il client VPN SSL (SVC) in una workstation remota oppure rimuovere il client dopo la chiusura della sessione protetta.Per ulteriori informazioni sul client VPN SSL, fare riferimento all'esempio di configurazione di SSL VPN Client (SVC) sull'appliance ASA con ASDM.

In questo documento viene illustrata una configurazione semplice della VPN SSL thin-client su appliance ASA (Adaptive Security Appliance). La configurazione consente all'utente di connettersi in modo sicuro a un router situato all'interno dell'appliance ASA. La configurazione descritta in questo documento è supportata per ASA versione 7.x e successive.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti per le stazioni client remote:

- browser abilitato per SSL
- SUN Java JRE versione 1.4 o successiva
- Cookie abilitati
- Blocchi popup disattivati
- Privilegi amministrativi locali (non richiesti, ma consigliati)

Nota: l'ultima versione di SUN Java JRE è disponibile come download gratuito dal sito Web Java.

Componenti usati

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

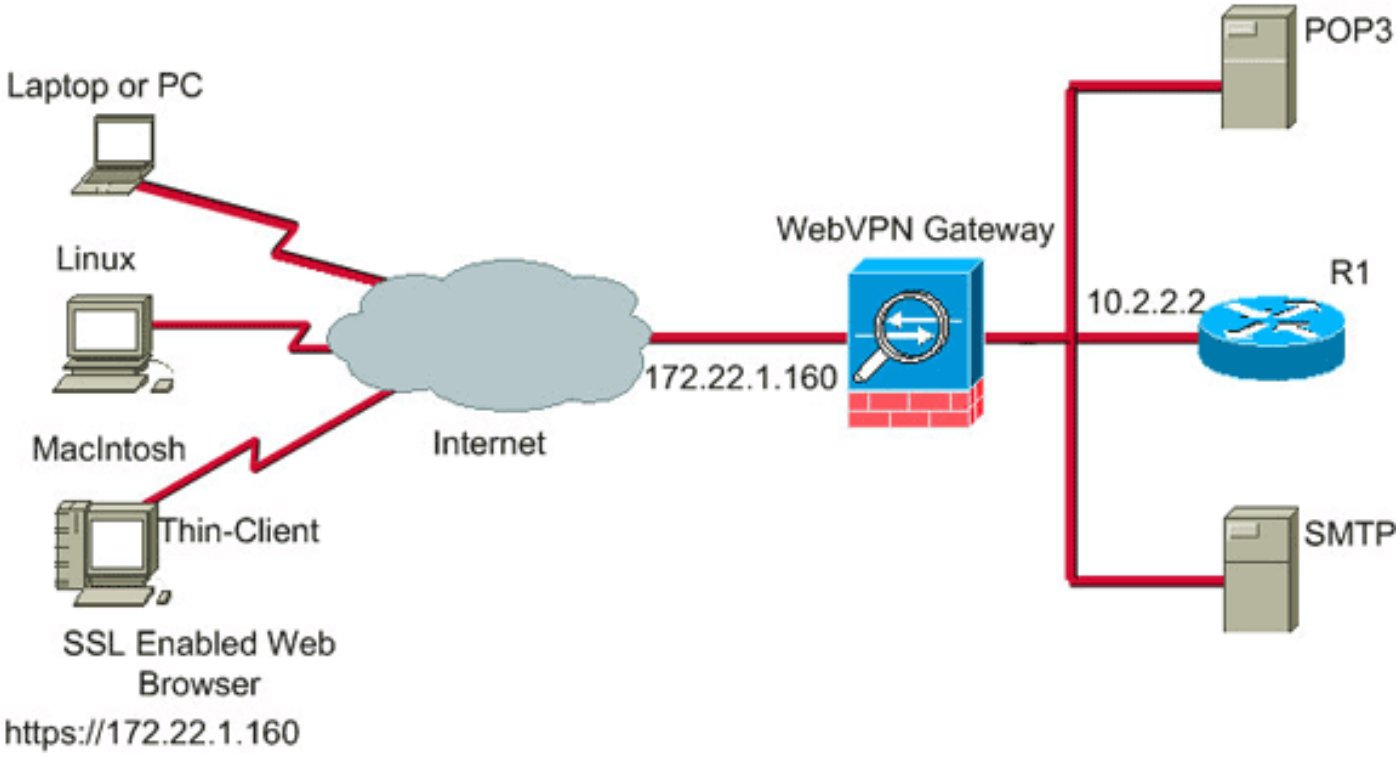
- Cisco Adaptive Security Appliance serie 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Nota:** per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.
- Software Cisco Adaptive Security Appliance versione 7.2(1)
- Client remoto Microsoft Windows XP Professional (SP 2)

Le informazioni discusse in questo documento fanno parte di un ambiente di emulazione. Tutti i dispositivi utilizzati nel documento sono stati ripristinati alla configurazione predefinita. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi. Tutti gli indirizzi IP utilizzati in questa configurazione sono stati selezionati dagli indirizzi RFC 1918 di un ambiente lab; questi indirizzi IP non possono essere instradati su Internet e sono solo a scopo di prova.

Esempio di rete

Nel documento viene usata la configurazione di rete descritta in questa sezione.

Quando un client remoto avvia una sessione con l'ASA, scarica una piccola applet Java sulla workstation. Al client viene presentato un elenco di risorse preconfigurate.



Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Per avviare una sessione, il client remoto apre un browser SSL all'interfaccia esterna dell'ASA. Dopo aver stabilito la sessione, l'utente può usare i parametri configurati sull'appliance ASA per richiamare qualsiasi accesso Telnet o alle applicazioni. L'appliance ASA invia tramite proxy la connessione protetta e consente all'utente di accedere al dispositivo.

Nota: Gli elenchi degli accessi in entrata non sono necessari per queste connessioni perché l'ASA è già a conoscenza del significato di una sessione legale.

Configurazione VPN SSL thin client con ASDM

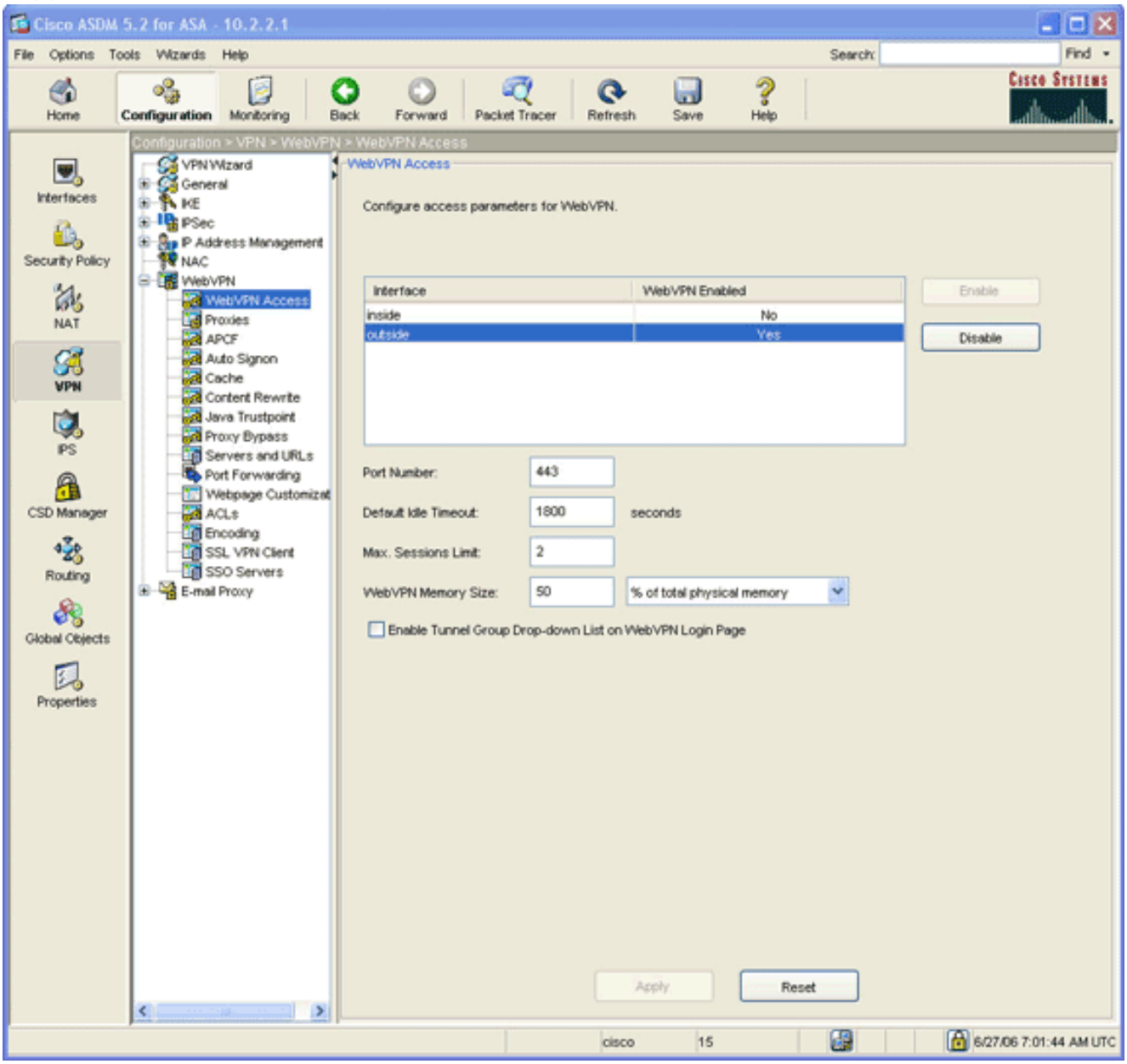
Per configurare la VPN SSL thin-client sull'appliance ASA, attenersi alla seguente procedura:

1. Abilitare WebVPN sull'appliance ASA
2. Configura caratteristiche inoltro porta
3. Creare un criterio di gruppo e collegarlo all'elenco di inoltro porte (creato nel passaggio 2)
4. Creare un gruppo di tunnel e collegarlo ai Criteri di gruppo (creato al passaggio 3)
5. Creare un utente e aggiungerlo ai Criteri di gruppo (creato al passaggio 3)

Passaggio 1. Abilitare WebVPN sull'appliance ASA

Per abilitare WebVPN sull'appliance ASA, attenersi alla seguente procedura:

1. Nell'applicazione ASDM, fare clic su **Configurazione**, quindi su **VPN**.
2. Espandere **WebVPN** e scegliere **Accesso WebVPN**.

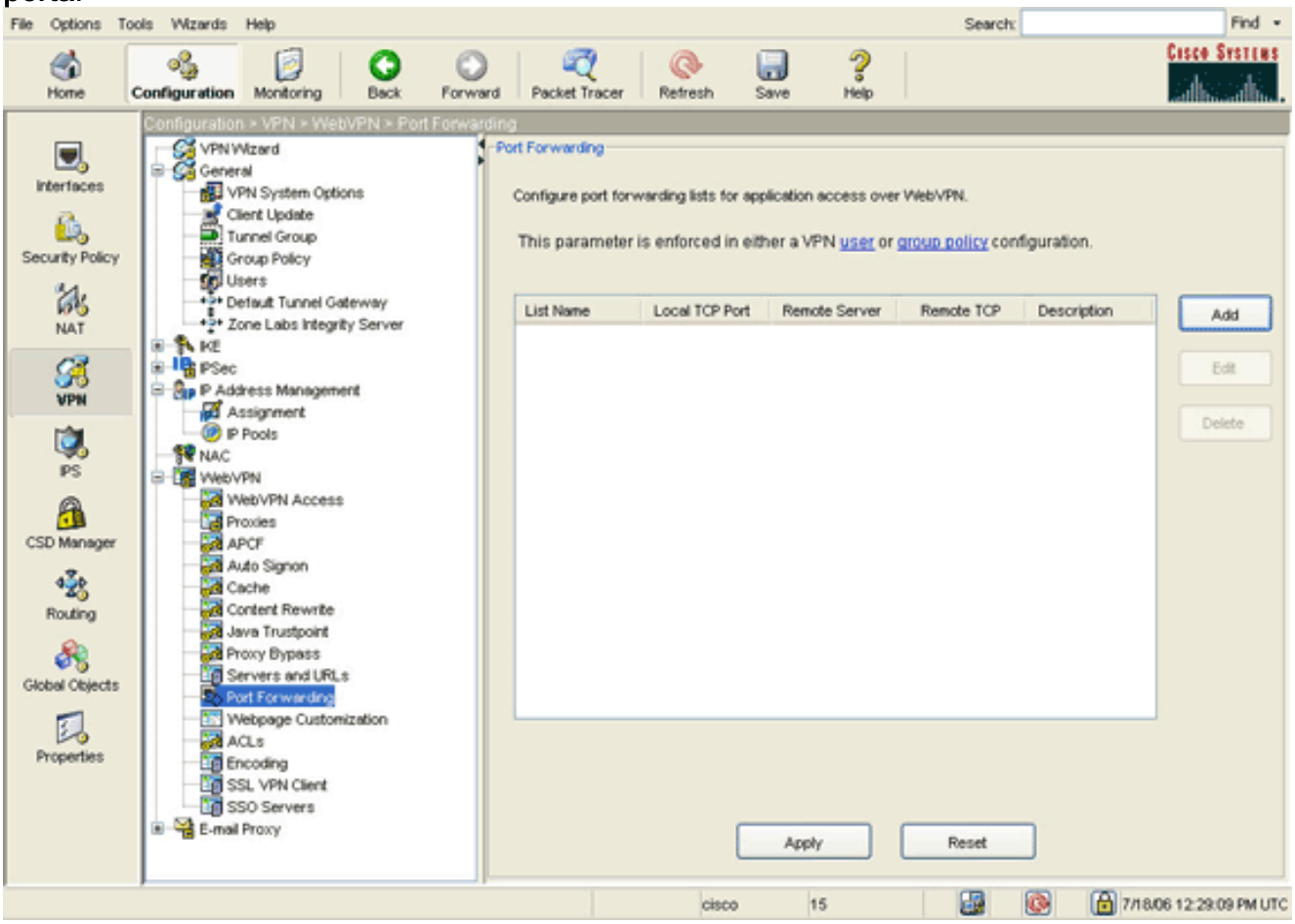


3. Evidenziare l'interfaccia e fare clic su **Attiva**.
4. Fare clic su **Applica**, su **Salva** e quindi su **Sì** per accettare le modifiche.

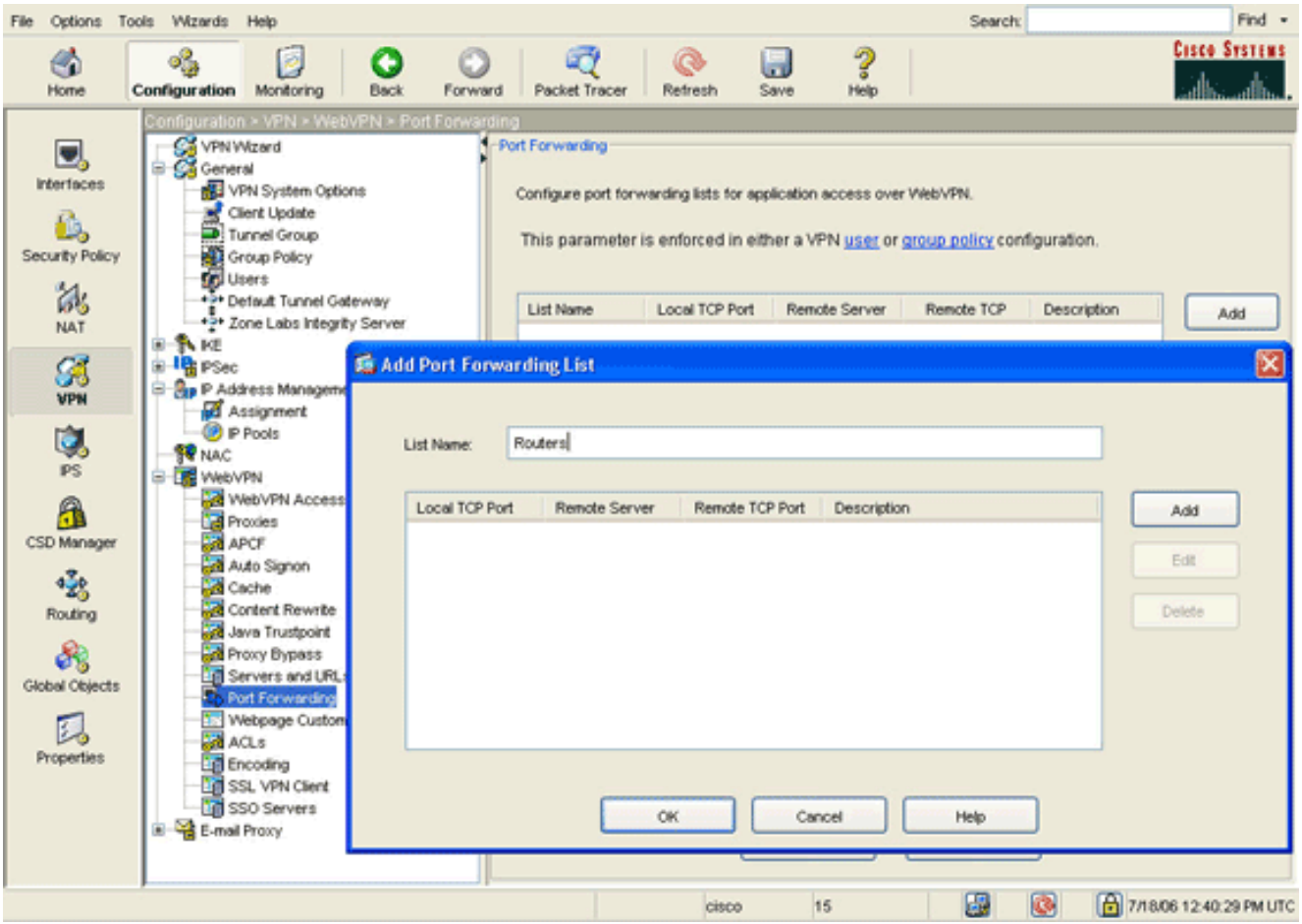
Passaggio 2. Configurazione delle caratteristiche di inoltro porta

Per configurare le caratteristiche di inoltro delle porte, attenersi alla seguente procedura:

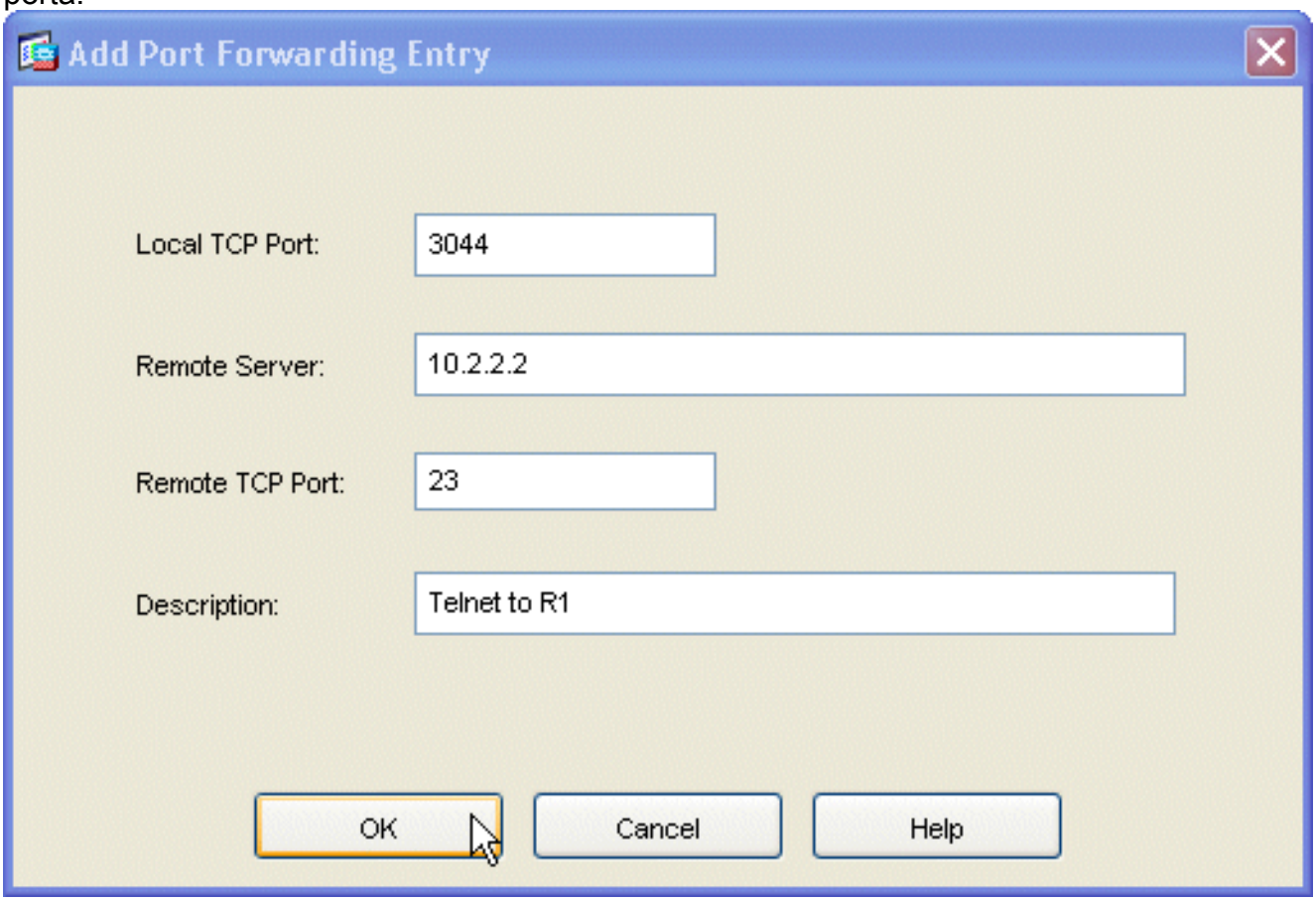
1. Espandere **WebVPN** e scegliere **Inoltro porta**.



2. Fare clic sul pulsante **Aggiungi**.



3. Nella finestra di dialogo Aggiungi elenco inoltro porte, immettere un nome di elenco e fare clic su **Aggiungi**.Verrà visualizzata la finestra di dialogo Aggiungi voce di inoltro porta.



4. Nella finestra di dialogo Aggiungi voce di inoltro porta, immettere le seguenti opzioni:Nel campo Porta TCP locale, immettere un numero di porta o accettare il valore predefinito.Il

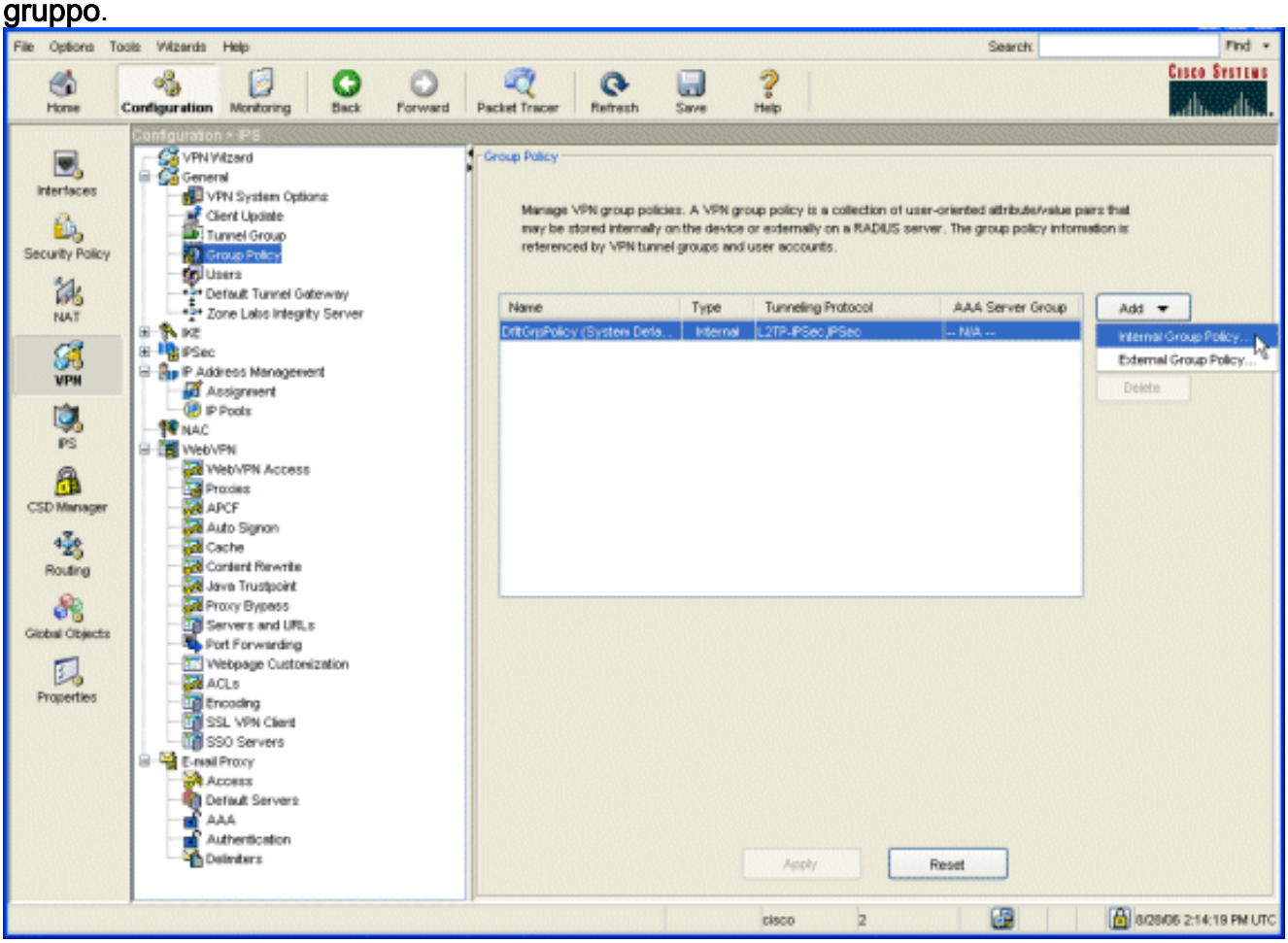
valore immesso può essere un numero compreso tra 1024 e 65535.Nel campo Server remoto immettere un indirizzo IP.In questo esempio viene utilizzato l'indirizzo del router.Nel campo Porta TCP remota, immettere un numero di porta.In questo esempio viene utilizzata la porta 23.Nel campo Descrizione, immettere una descrizione e fare clic su **OK**.

5. Fare clic su **OK**, quindi su **Applica**.
6. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

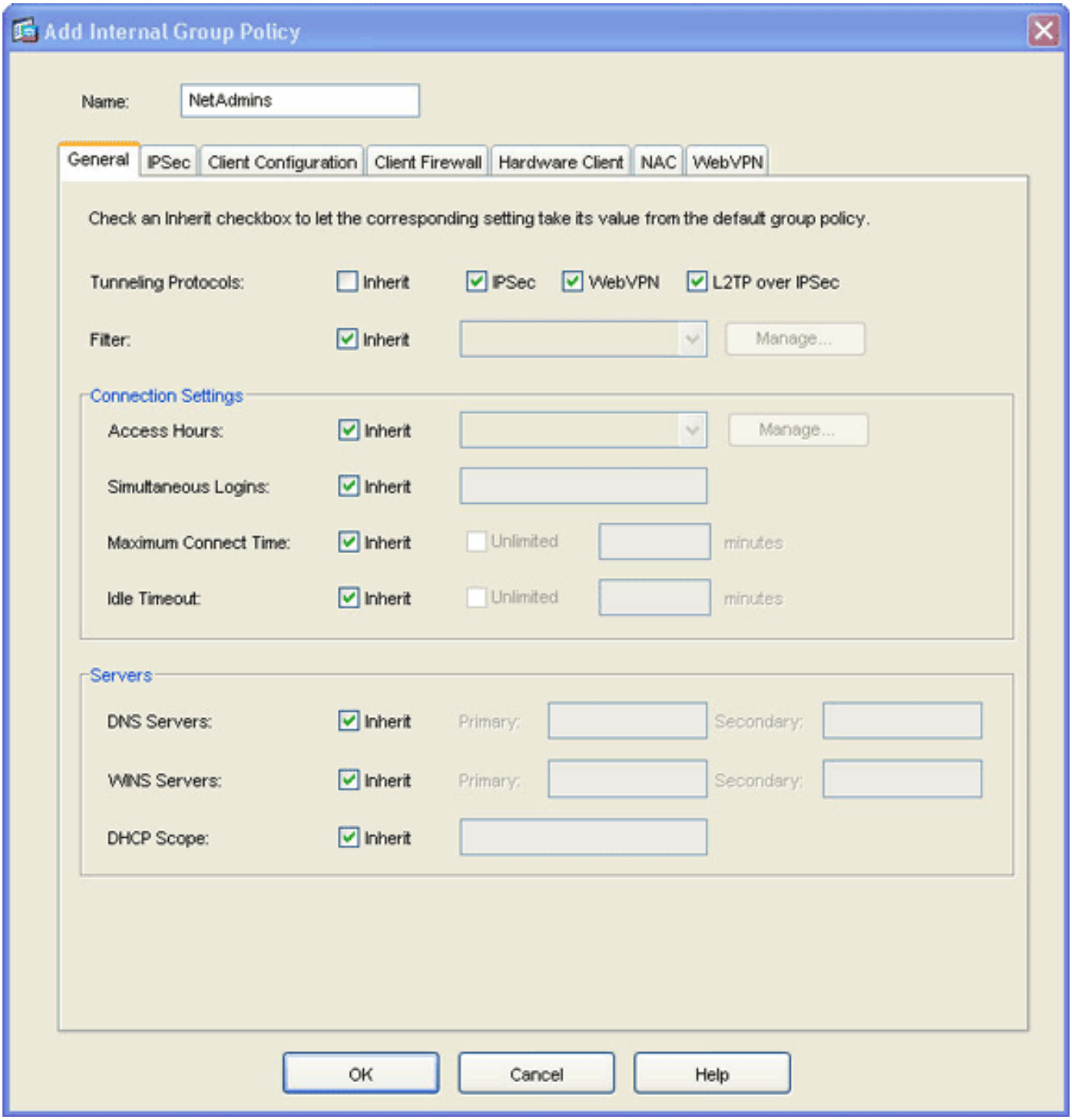
Passaggio 3. Creare un criterio di gruppo e collegarlo all'elenco di inoltro porte

Per creare un criterio di gruppo e collegarlo all'elenco di inoltro porte, eseguire la procedura seguente:

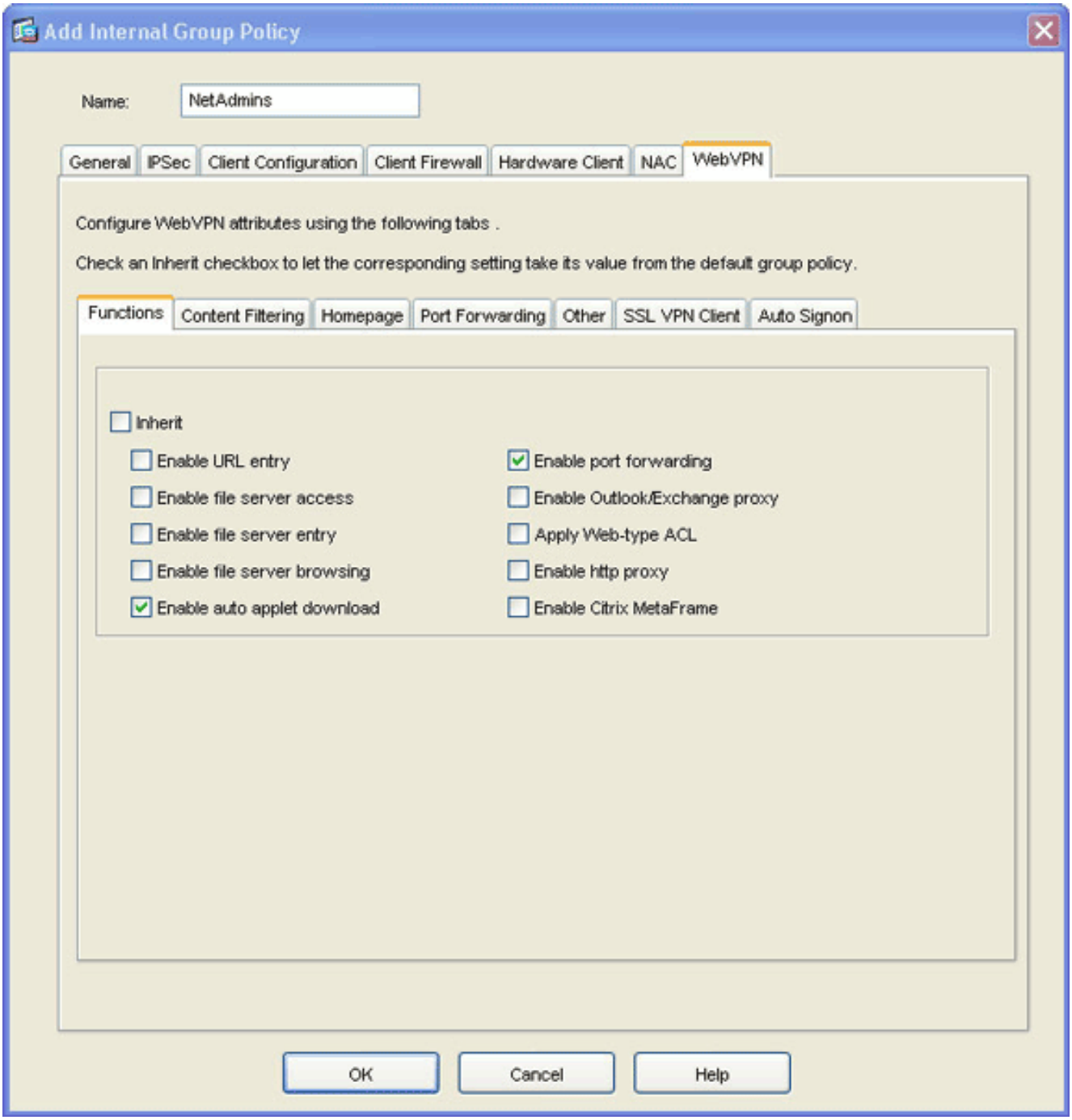
1. Espandere **Generale** e scegliere **Criteri di gruppo**.



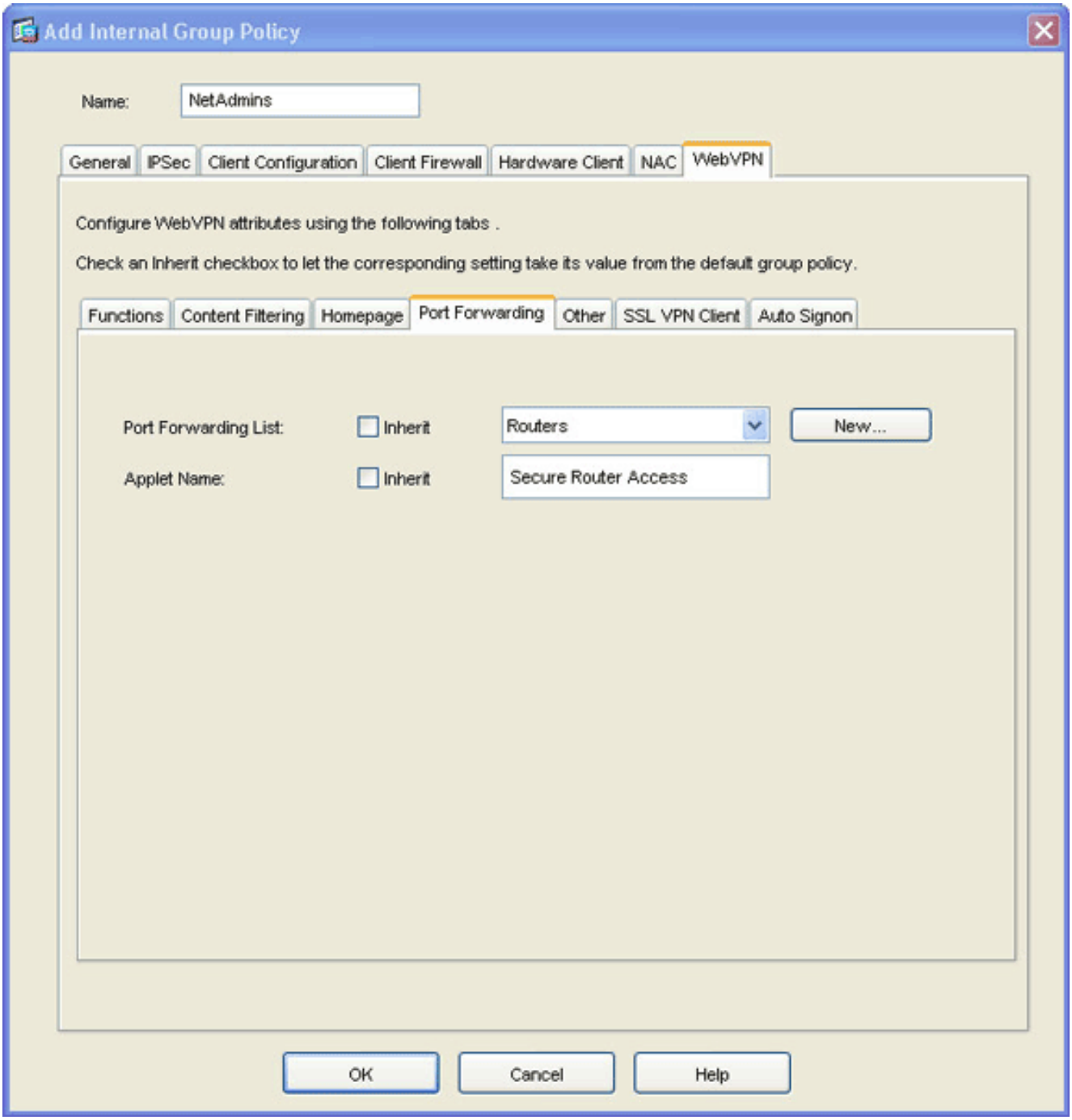
2. Fare clic su **Aggiungi** e scegliere **Criteri di gruppo interni**.Verrà visualizzata la finestra di dialogo Aggiungi Criteri di gruppo interni.



3. Immettere un nome o accettare il nome del criterio di gruppo predefinito.
4. Deselezionare la casella di controllo **Eredita** protocolli di tunneling e selezionare la casella di controllo **WebVPN**.
5. Fare clic sulla scheda **WebVPN** nella parte superiore della finestra di dialogo e quindi sulla scheda **Funzioni**.
6. Deselezionare la casella di controllo **Eredita** e selezionare le caselle di controllo **Abilita download automatico applet** e **Abilita inoltro porta**, come mostrato nell'immagine:



7. Anche all'interno della scheda WebVPN, fare clic sulla scheda **Port Forwarding** e deselezionare la casella di controllo **Eredita** elenco inoltro porte.



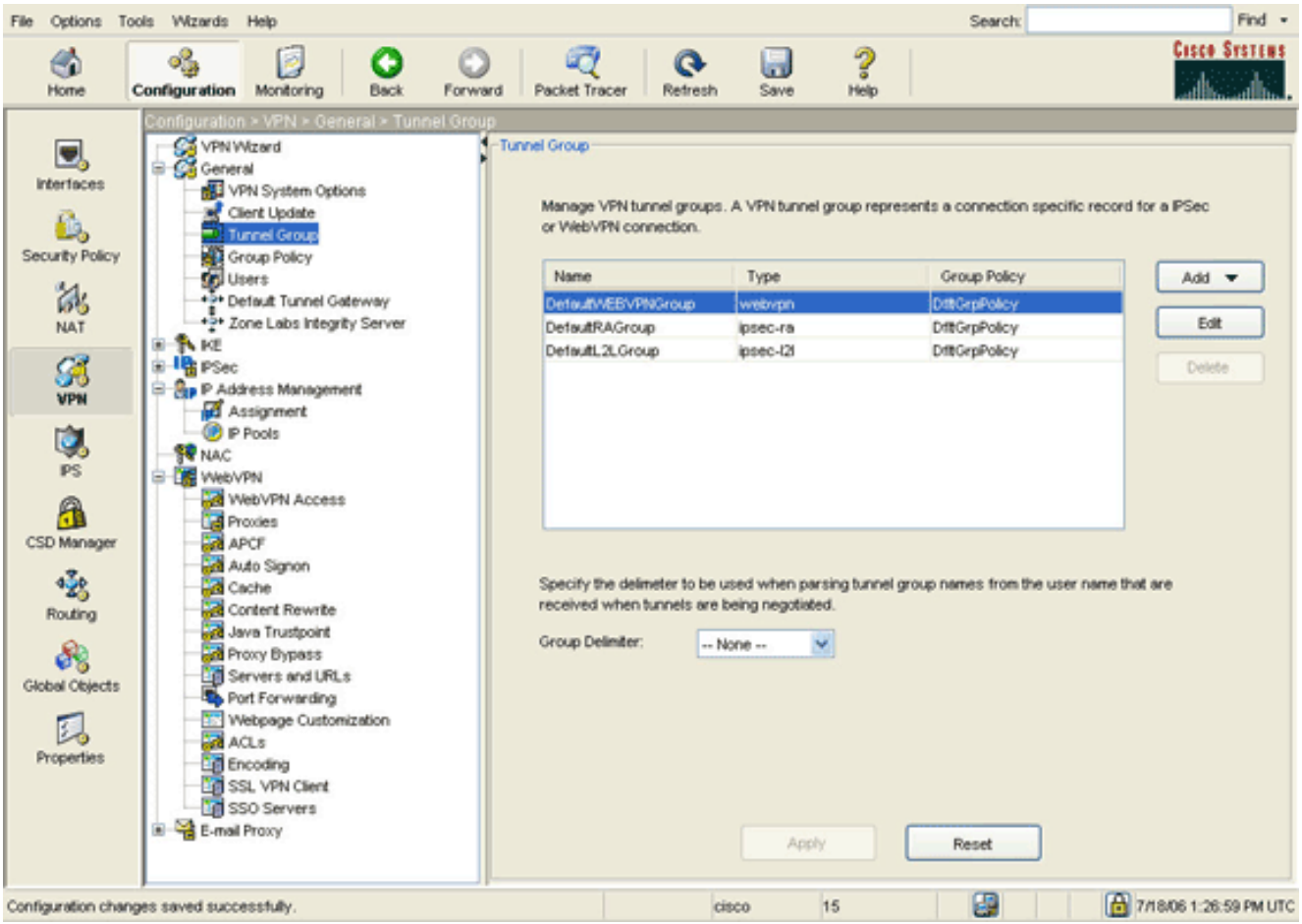
8. Fare clic sulla freccia a discesa **Elenco inoltro porte** e scegliere l'elenco di inoltro porte creato nel passaggio 2.
9. Deselezionare la casella di controllo **Eredita** nome applet e modificare il nome nel campo di testo.Il client visualizza il nome dell'applet alla connessione.
10. Fare clic su **OK**, quindi su **Applica**.
11. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

Passaggio 4. Creare un gruppo di tunnel e collegarlo ai Criteri di gruppo

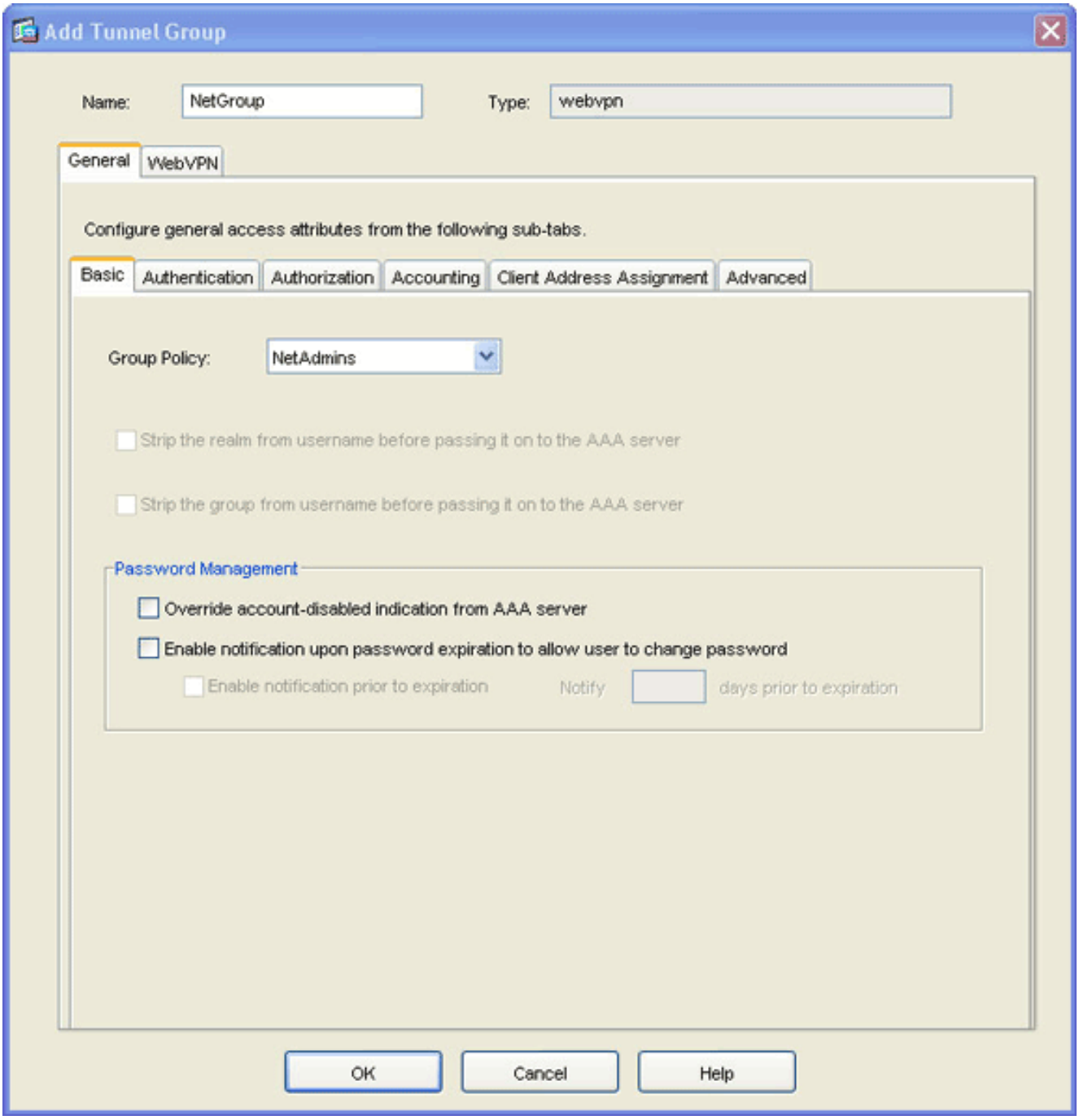
Èpossibile modificare il gruppo di tunnel *DefaultWebVPNGroup* predefinito o creare un nuovo gruppo di tunnel.

Per creare un nuovo gruppo di tunnel, attenersi alla seguente procedura:

1. Espandere **Generale** e scegliere **Gruppo tunnel**.



2. Fare clic su **Add** (Aggiungi), quindi selezionare **WebVPN Access** (Accesso VPN Web).Verrà visualizzata la finestra di dialogo Aggiungi gruppo di tunnel.

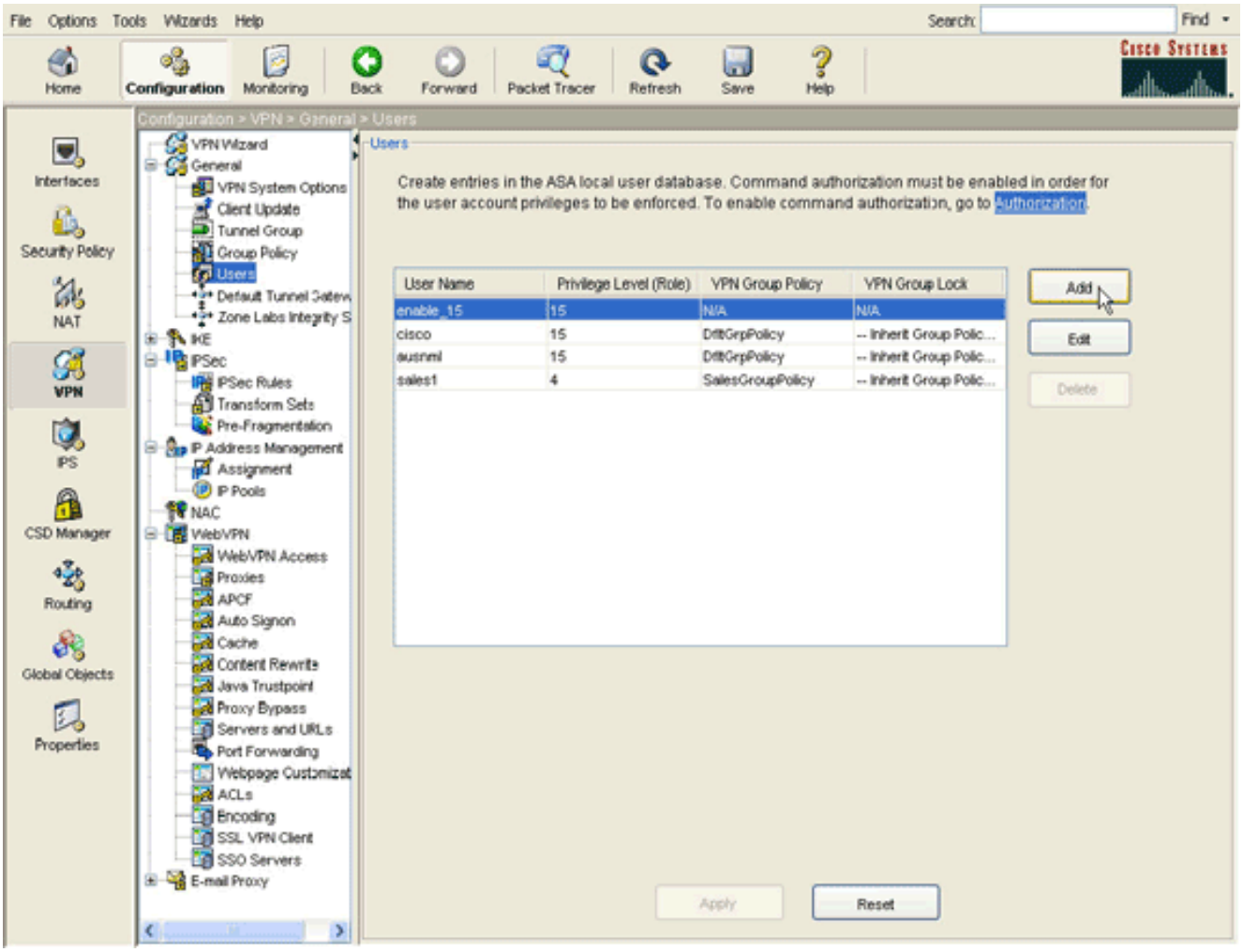


3. Immettere un nome nel campo Nome.
4. Fare clic sulla freccia a discesa **Criteri di gruppo** e scegliere il criterio di gruppo creato nel passaggio 3.
5. Fare clic su **OK**, quindi su **Applica**.
6. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.Le caratteristiche di inoltro a livello di gruppo di tunnel, criteri di gruppo e porta sono ora collegate.

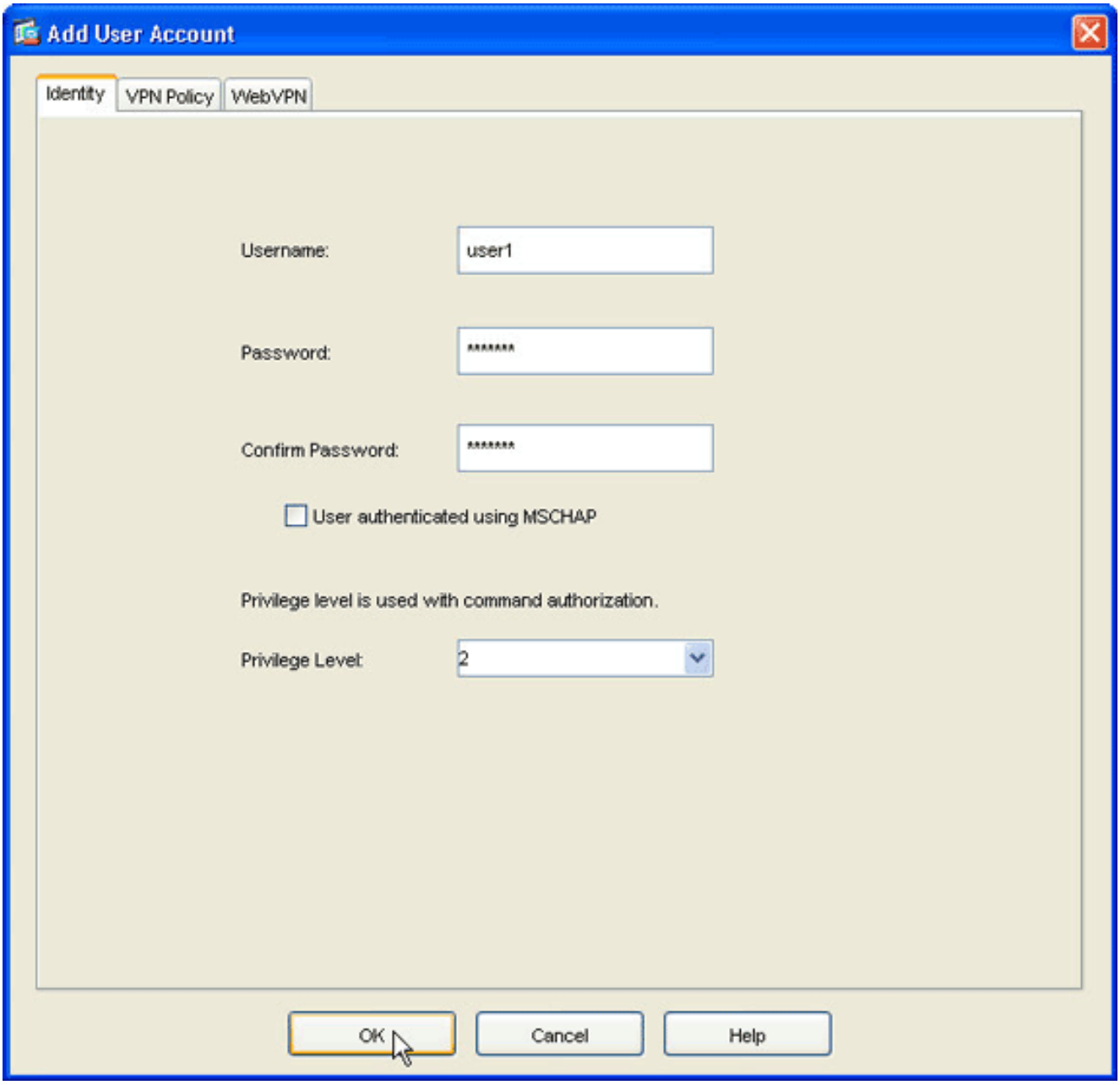
Passaggio 5. Creare un utente e aggiungerlo ai Criteri di gruppo

Per creare un utente e aggiungerlo ai Criteri di gruppo, eseguire la procedura seguente:

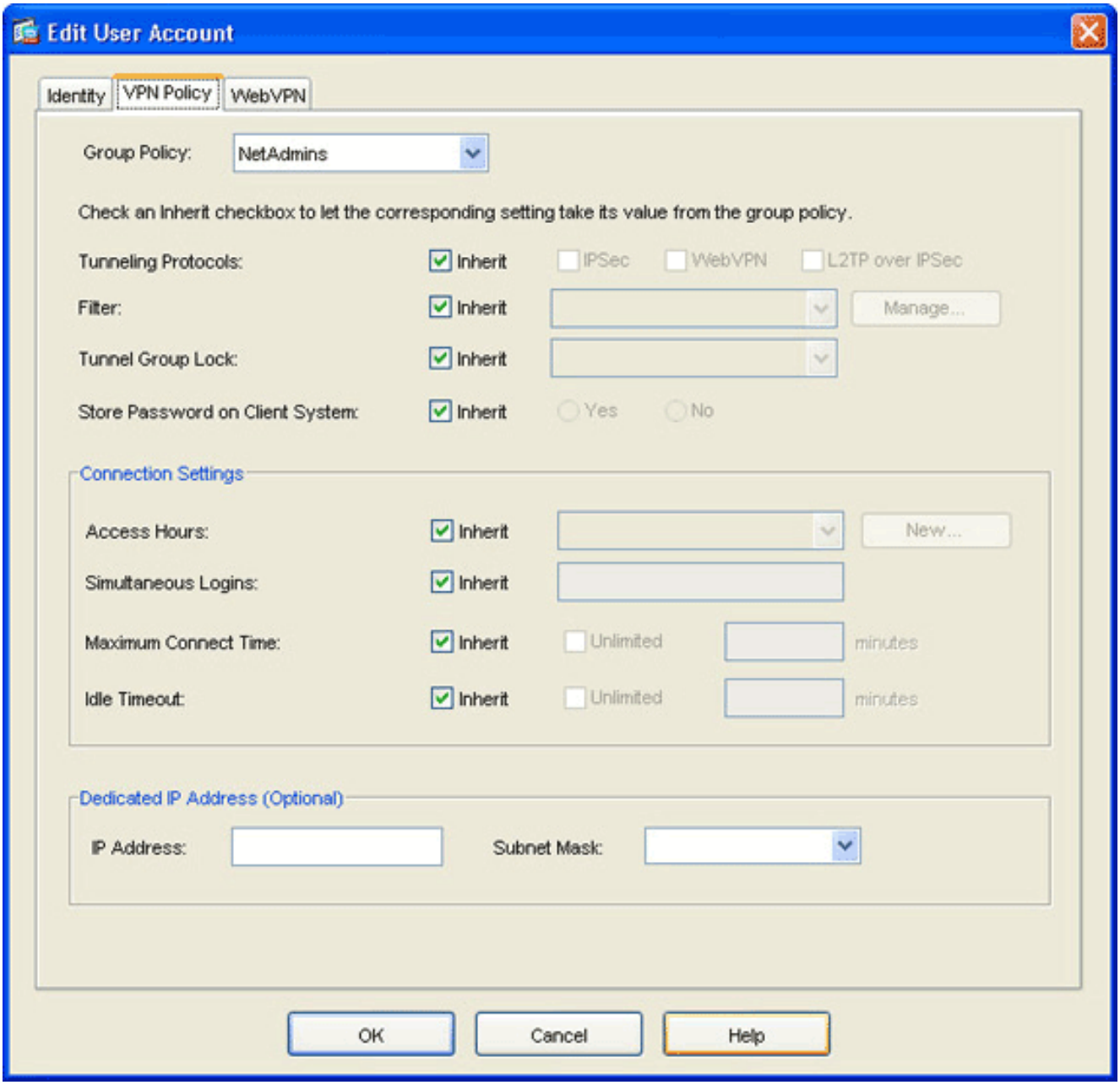
1. Espandere **Generale** e scegliere **Utenti**.



2. Fare clic sul pulsante **Aggiungi**.Verrà visualizzata la finestra di dialogo Aggiungi account utente.



3. Immettere i valori per il nome utente, la password e le informazioni sui privilegi e quindi fare clic sulla scheda **Criteri VPN**.



4. Fare clic sulla freccia a discesa **Criteri di gruppo** e scegliere il criterio di gruppo creato nel passaggio 3.Questo utente eredita le caratteristiche e i criteri WebVPN dei Criteri di gruppo selezionati.
5. Fare clic su **OK**, quindi su **Applica**.
6. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

Configurazione VPN SSL thin client tramite CLI

ASA
ASA Version 7.2(1) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside

```
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Output truncated  port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
!--- Configure the set of applications that WebVPN
users !--- can access over forwarded TCP ports group-
policy NetAdmins internal
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
!--- Configure group policy attributes webvpn
  functions port-forward auto-download
!--- Configure group policies for WebVPN   port-forward
value portforward
!--- Configure port-forward to enable WebVPN
application access !--- for the new group policy  port-
forward-name value Secure Router Access
!--- Configure the display name that identifies TCP
port !--- forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
 vpn-group-policy NetAdmins
!--- Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
 default-group-policy NetAdmins
!--- Create a new tunnel group and link it to the group
policy 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 Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context
```

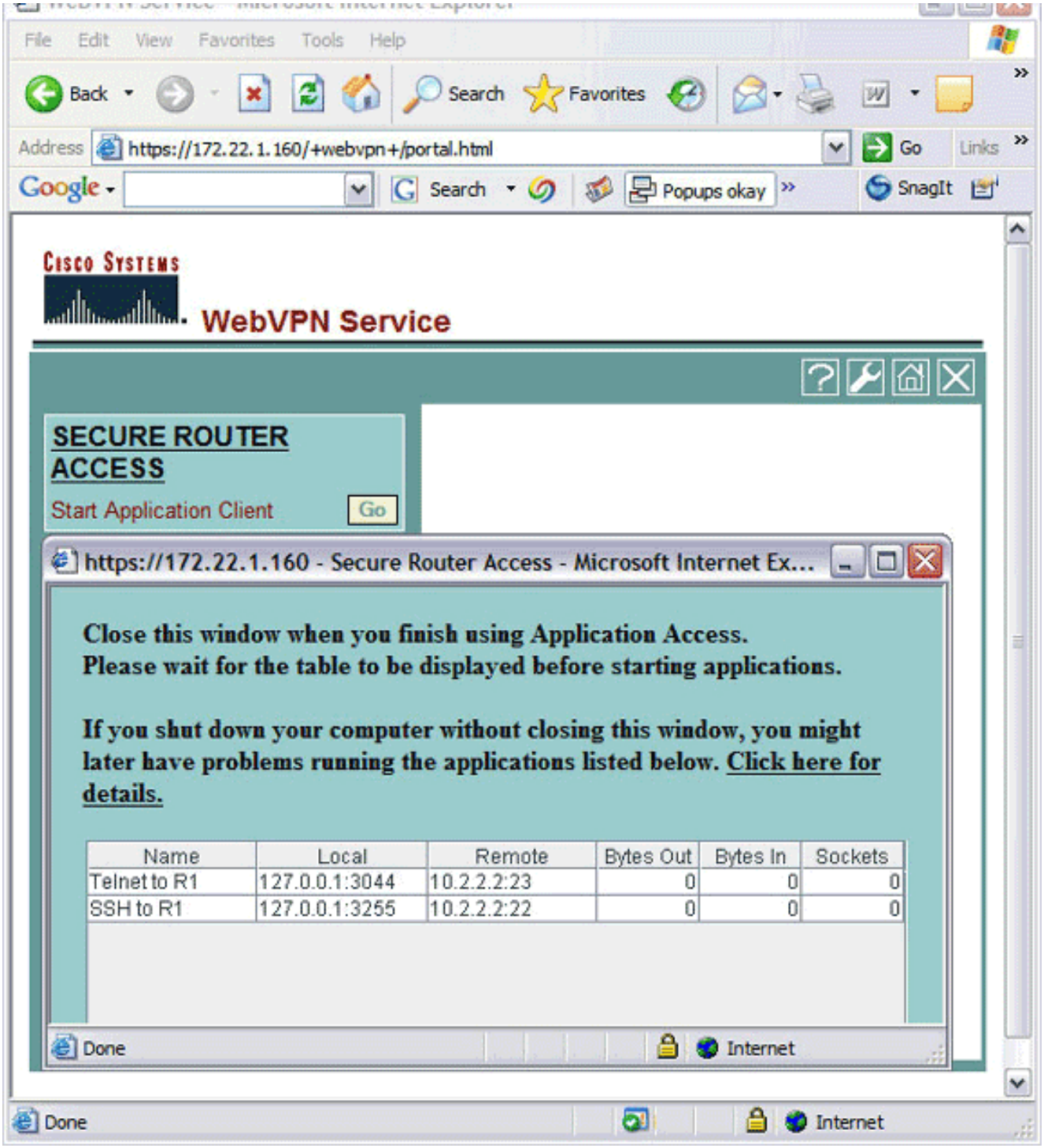
Verifica

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

Procedura

In questa procedura viene descritto come determinare la validità della configurazione e come verificarla.

1. Da una workstation client, immettere **https://*outside_ASA_IP Address***; dove *outside_ASA_IPAddress* è l'URL SSL dell'appliance ASA.Una volta accettato il certificato digitale e autenticato l'utente, viene visualizzata la pagina Web Servizio WebVPN.

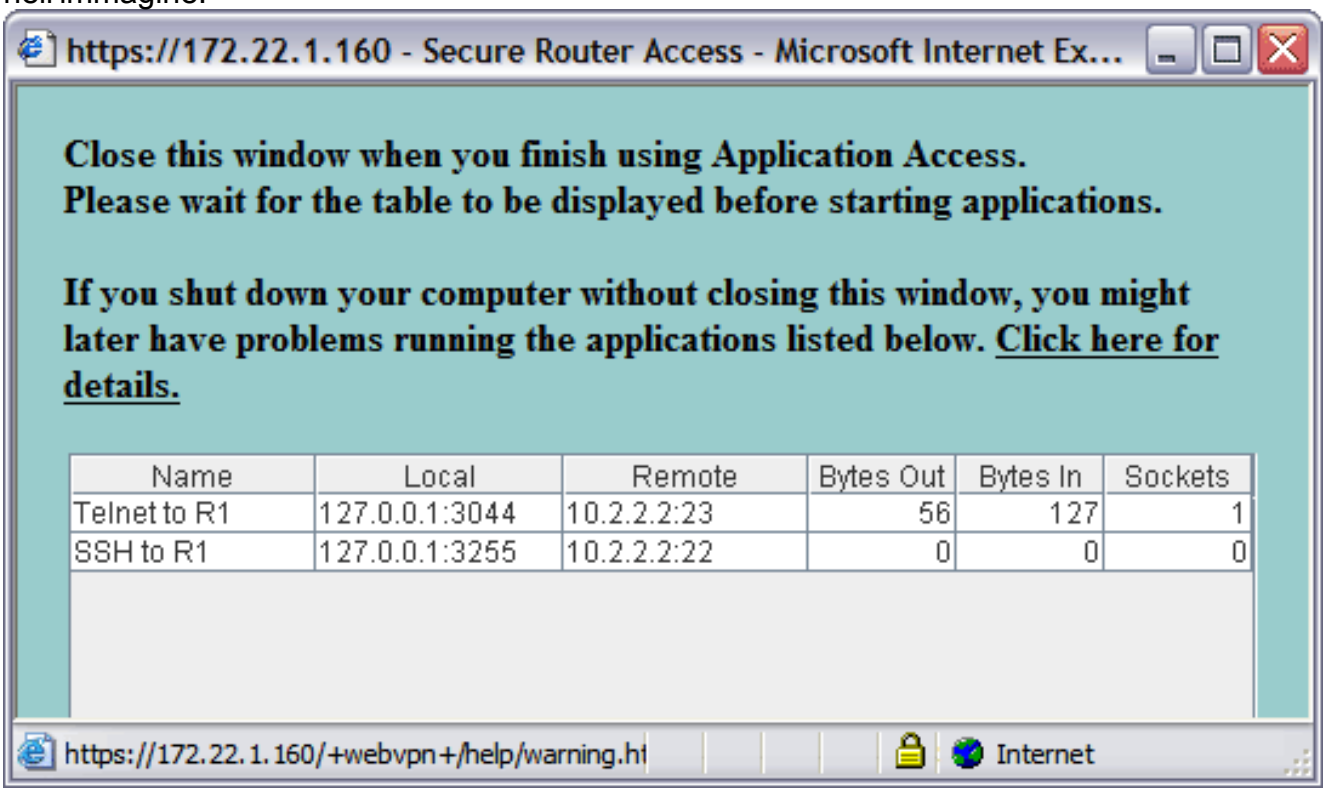


Le informazioni sull'indirizzo e sulla porta necessarie per accedere all'applicazione vengono visualizzate nella colonna locale. Nelle colonne Byte in uscita e Byte in ingresso non viene visualizzata alcuna attività perché l'applicazione non è stata richiamata in questo momento.

2. Utilizzare il prompt di DOS o un'altra applicazione Telnet per avviare una sessione Telnet.
3. Al prompt dei comandi, immettere **telnet 127.0.0.1 3044**.**Nota:** questo comando fornisce un esempio di come ottenere l'accesso alla porta locale visualizzata nell'immagine della pagina Web del servizio WebVPN in questo documento. *Il comando non include i due punti (:).* Digitare il comando come descritto in questo documento.L'ASA riceve il comando sulla sessione protetta e, poiché memorizza una mappa delle informazioni, sa immediatamente come aprire la sessione Telnet protetta sul dispositivo mappato.

Dopo aver immesso il nome utente e la password, l'accesso al dispositivo è completato.

4. Per verificare l'accesso al dispositivo, controllare le colonne Byte in uscita e Byte in ingresso come mostrato nell'immagine:



Comandi

Diversi comandi **show** sono associati a WebVPN. È possibile eseguire questi comandi dall'interfaccia della riga di comando (CLI) per visualizzare le statistiche e altre informazioni. Per informazioni dettagliate sui comandi **show**, consultare il documento sulla verifica della configurazione di WebVPN.

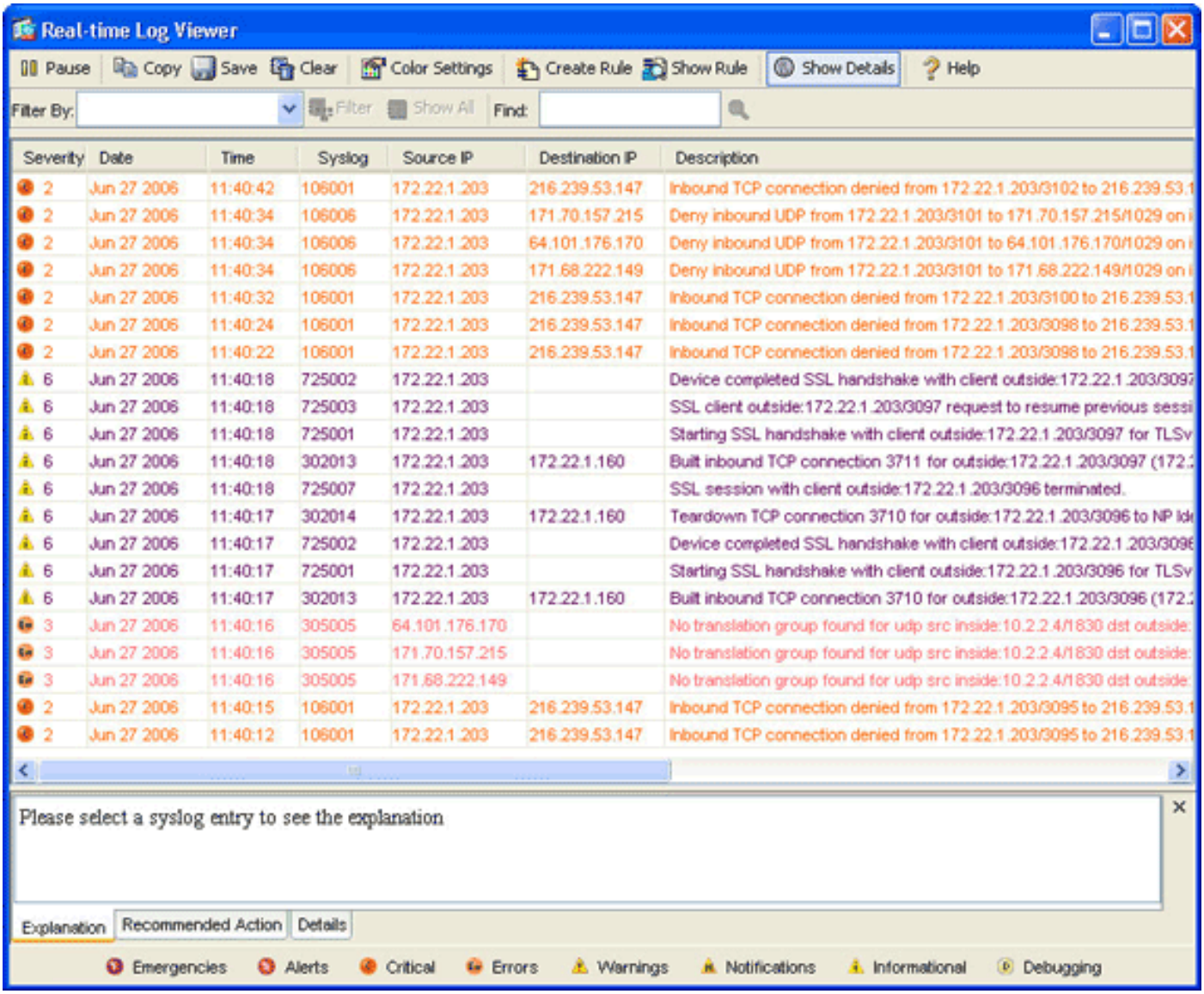
Nota: lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Il processo di handshake SSL è completato?

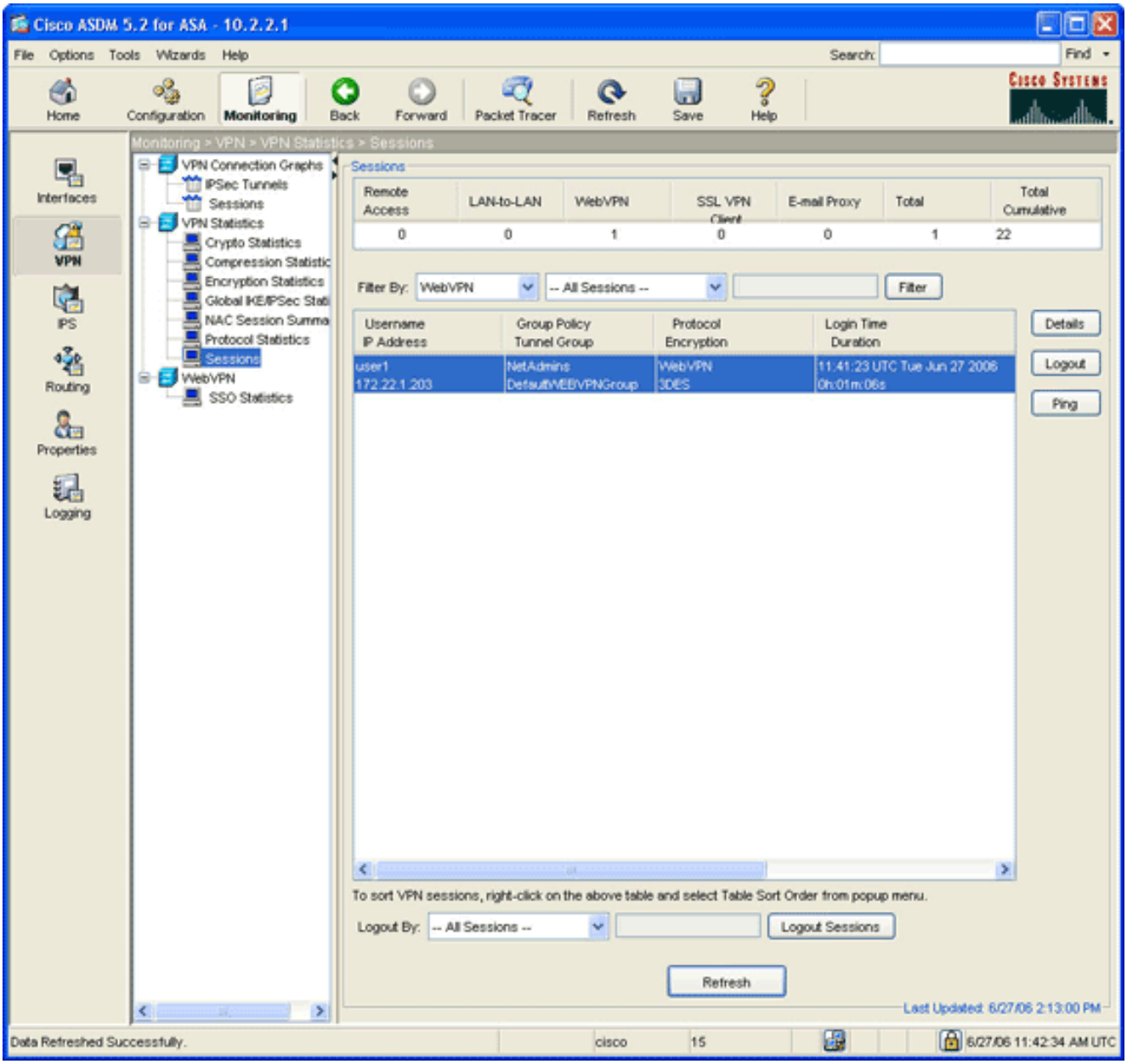
Dopo aver effettuato la connessione all'ASA, verificare che il log in tempo reale mostri il completamento dell'handshake SSL.



Il protocollo SSL VPN Thin-Client è operativo?

Per verificare il corretto funzionamento di SSL VPN Thin-Client, attenersi alla seguente procedura:

1. Fare clic su **Monitoraggio** e quindi su **VPN**.
2. Espandere **Statistiche VPN** e fare clic su **Sessioni**.La sessione SSL VPN Thin-Client dovrebbe essere visualizzata nell'elenco delle sessioni. Assicurarsi di filtrare in base a WebVPN, come mostrato
nell'immagine:



Comandi

Diversi comandi **debug** sono associati a WebVPN. Per informazioni dettagliate su questi comandi, consultare il documento sull'uso dei comandi di debug di WebVPN.

Nota: l'uso dei comandi di **debug** può avere un impatto negativo sul dispositivo Cisco. Prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Informazioni correlate

- Esempio di configurazione di una VPN SSL senza client (WebVPN) su ASA
- Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM
- Cisco ASA serie 5500 Adaptive Security Appliance
- Esempio di configurazione di ASA con WebVPN e Single Sign-On con ASDM e NTLMv1
- Documentazione e supporto tecnico – Cisco Systems