Esempio di configurazione di SSL VPN Client (SVC) su IOS con SDM

Sommario

Introduzione

Il client VPN SSL (SVC) fornisce un tunnel completo per comunicazioni sicure con la rete interna aziendale. È possibile configurare l'accesso in base all'utente oppure creare contesti WebVPN diversi in cui inserire uno o più utenti.

La tecnologia SSL VPN o WebVPN è supportata sulle seguenti piattaforme di router IOS:

- 870, 1811, 1841, 2801, 2811, 2821, 2851
- 3725, 3745, 3825, 3845, 7200 e 7301

Èpossibile configurare la tecnologia VPN SSL nelle seguenti modalità:

- **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, fare riferimento a Esempio di configurazione di Cisco IOS con SDM (WebVPN).

- **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. Punti di presenza (POP3), SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), ssh (Secure Shell) e Telnet sono esempi di accesso protetto. 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).Per ulteriori informazioni sulla VPN SSL thin-client, consultare l'esempio di configurazione di IOS per la VPN SSL thin-client (WebVPN) con SDM.**Nota:** UDP (User Datagram Protocol) non è supportato.
- **SSL VPN Client (SVC Full Tunnel Mode)**: scarica un client di piccole dimensioni sulla workstation remota e consente l'accesso sicuro alle risorse su una rete aziendale interna. È possibile scaricare SVC su una workstation remota in modo permanente oppure rimuovere il client una volta chiusa la sessione protetta.

In questo documento viene illustrata la configurazione di un router Cisco IOS per l'utilizzo da parte di un client VPN SSL.

Prerequisiti

Requisiti

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

- Microsoft Windows 2000 o XP
- Browser Web con SUN JRE 1.4 o versione successiva o un browser controllato da ActiveX
- Privilegi amministrativi locali sul client
- Uno dei router elencati nell'introduzione con un'immagine di sicurezza avanzata (12.4(6)T o versioni successive)
- Cisco Security Device Manager (SDM) versione 2.3Se il software Cisco SDM non è già caricato sul router, è possibile ottenerne una copia gratuita dal sito Download software (solo utenti registrati). Devi avere un account CCO con un contratto di assistenza. Per informazioni dettagliate sull'installazione e la configurazione dell'SDM, consultare il documento Cisco Router and Security Device Manager.
- Un certificato digitale sul routerPer soddisfare questo requisito, è possibile utilizzare un certificato autofirmato permanente o un'Autorità di certificazione (CA) esterna. Per ulteriori informazioni sui certificati autofirmati permanenti, vedere Certificati autofirmati permanenti.

Componenti usati

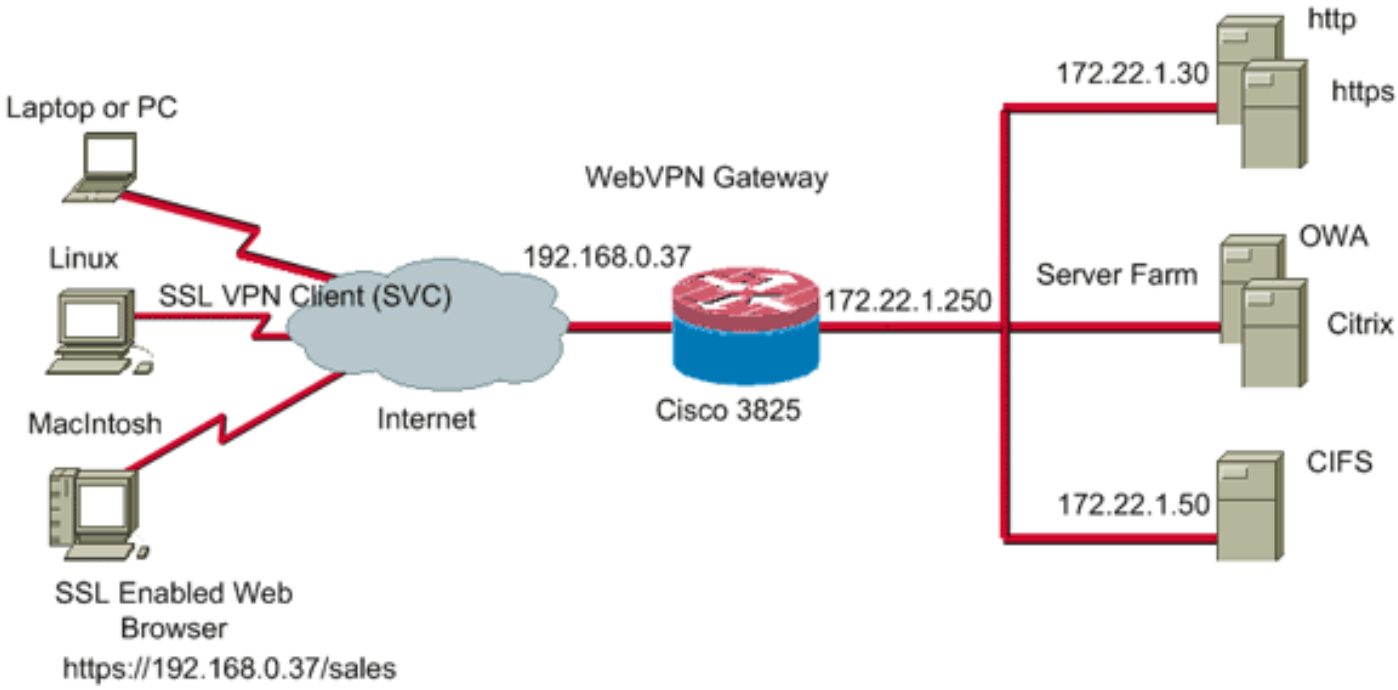
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router Cisco IOS serie 3825 con 12.4(9)T
- Security Device Manager (SDM) versione 2.3.1

Nota: 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.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Task di preconfigurazione

1. Configurare il router per SDM (facoltativo).I router con la licenza del bundle di sicurezza appropriata hanno già caricato l'applicazione SDM nella memoria flash. Per ottenere e configurare il software, consultare il documento sul download e l'installazione del router Cisco e sulla gestione dei dispositivi di sicurezza (SDM).
2. Scaricare una copia dell'SVC sul PC di gestione.Èpossibile ottenere una copia del file del pacchetto SVC da Software Download: Cisco SSL VPN Client (solo utenti registrati). È necessario disporre di un account CCO valido con un contratto di assistenza.
3. Impostare la data, l'ora e il fuso orario corretti, quindi configurare un certificato digitale sul router.

Convenzioni

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

Premesse

L'SVC viene inizialmente caricato sul router gateway WebVPN. Ogni volta che il client si connette, una copia dell'SVC viene scaricata dinamicamente sul PC. Per modificare questo comportamento, configurare il router in modo che il software rimanga permanentemente sul computer client.

Configurazione di SVC su IOS

In questa sezione vengono illustrati i passaggi necessari per configurare le funzionalità descritte più avanti nel documento. In questa configurazione di esempio viene utilizzata la procedura guidata SDM per abilitare il funzionamento del SVC sul router IOS.

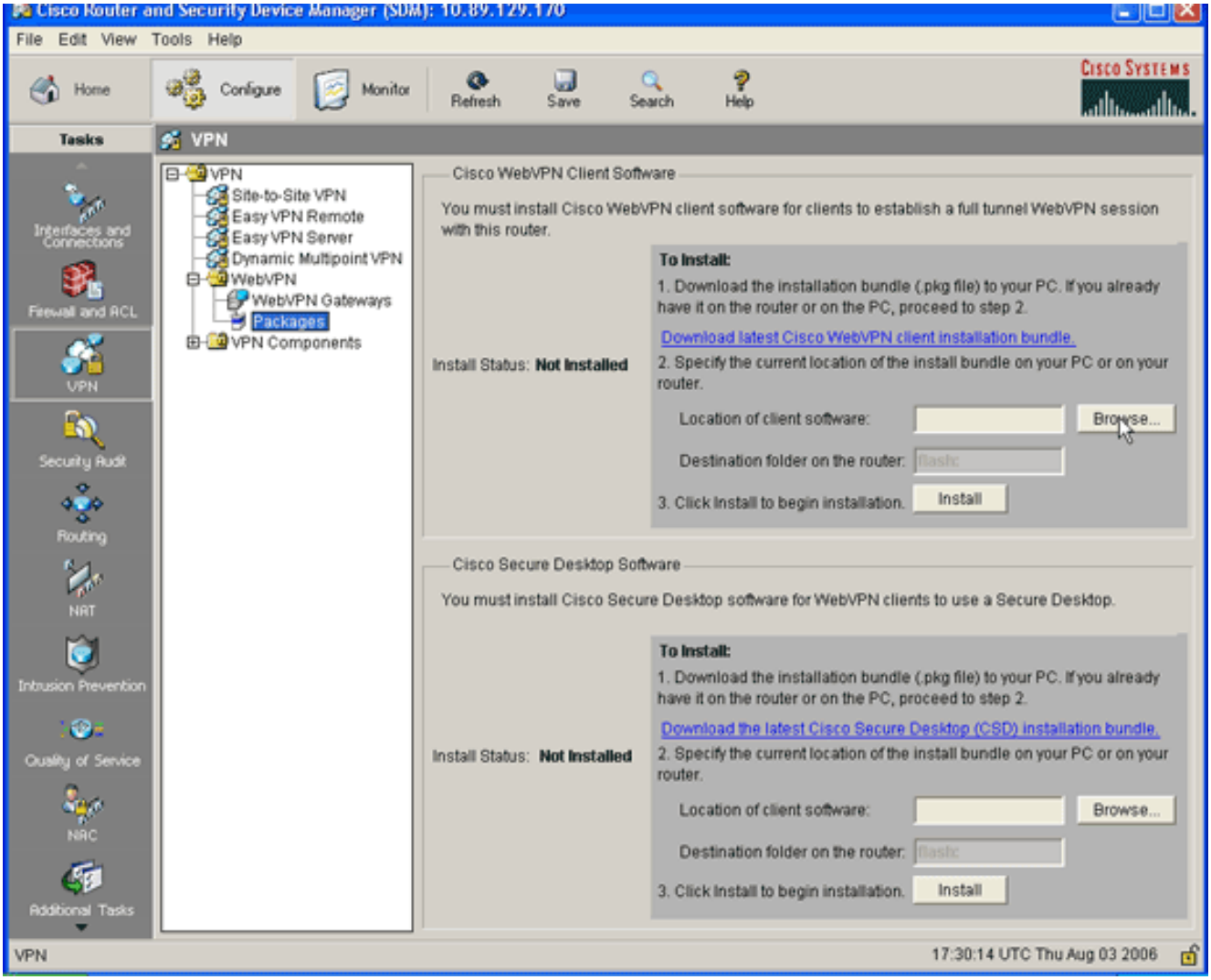
Completare questa procedura per configurare SVC sul router IOS:

1. Installare e abilitare il software SVC sul router IOS
2. Configurare un contesto WebVPN e un gateway WebVPN con la procedura guidata SDM
3. Configurare il database utenti per gli utenti SVC
4. Configurare le risorse da esporre agli utenti

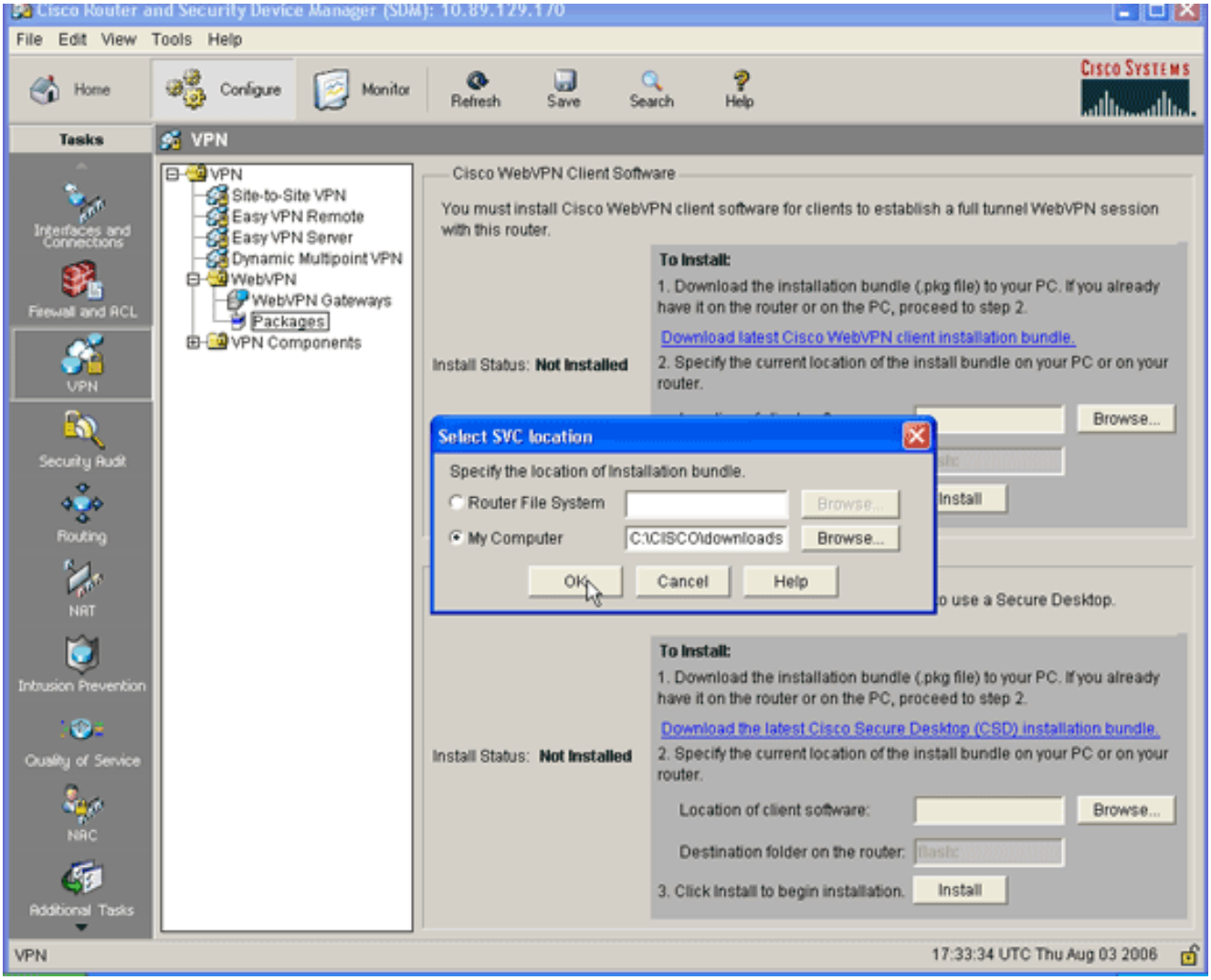
Passaggio 1. Installare e abilitare il software SVC sul router IOS

Per installare e abilitare il software SVC sul router IOS, completare i seguenti passaggi:

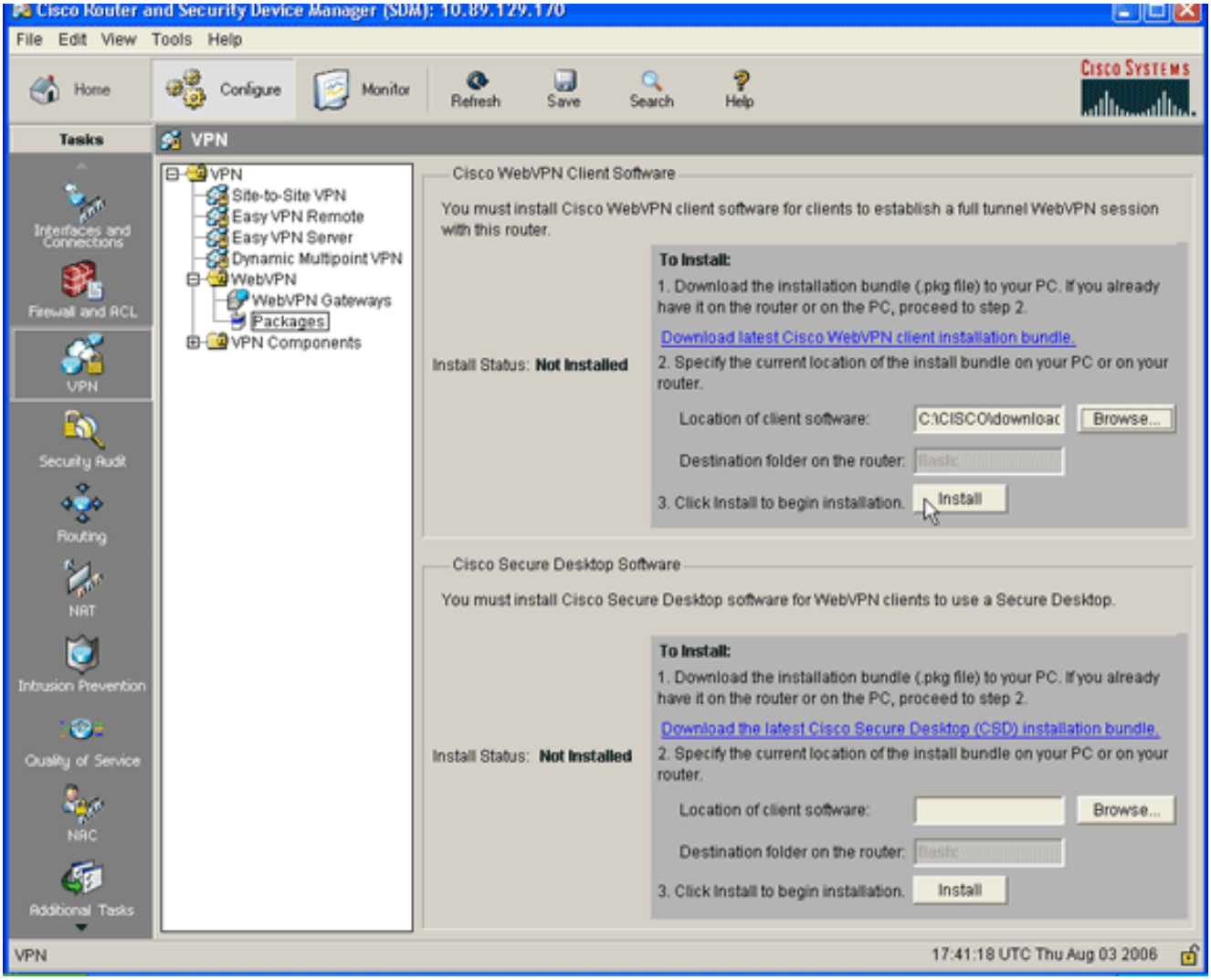
1. Aprire l'applicazione SDM, fare clic su **Configura** e quindi su **VPN**.
2. Espandere **WebVPN** e scegliere **Pacchetti**.



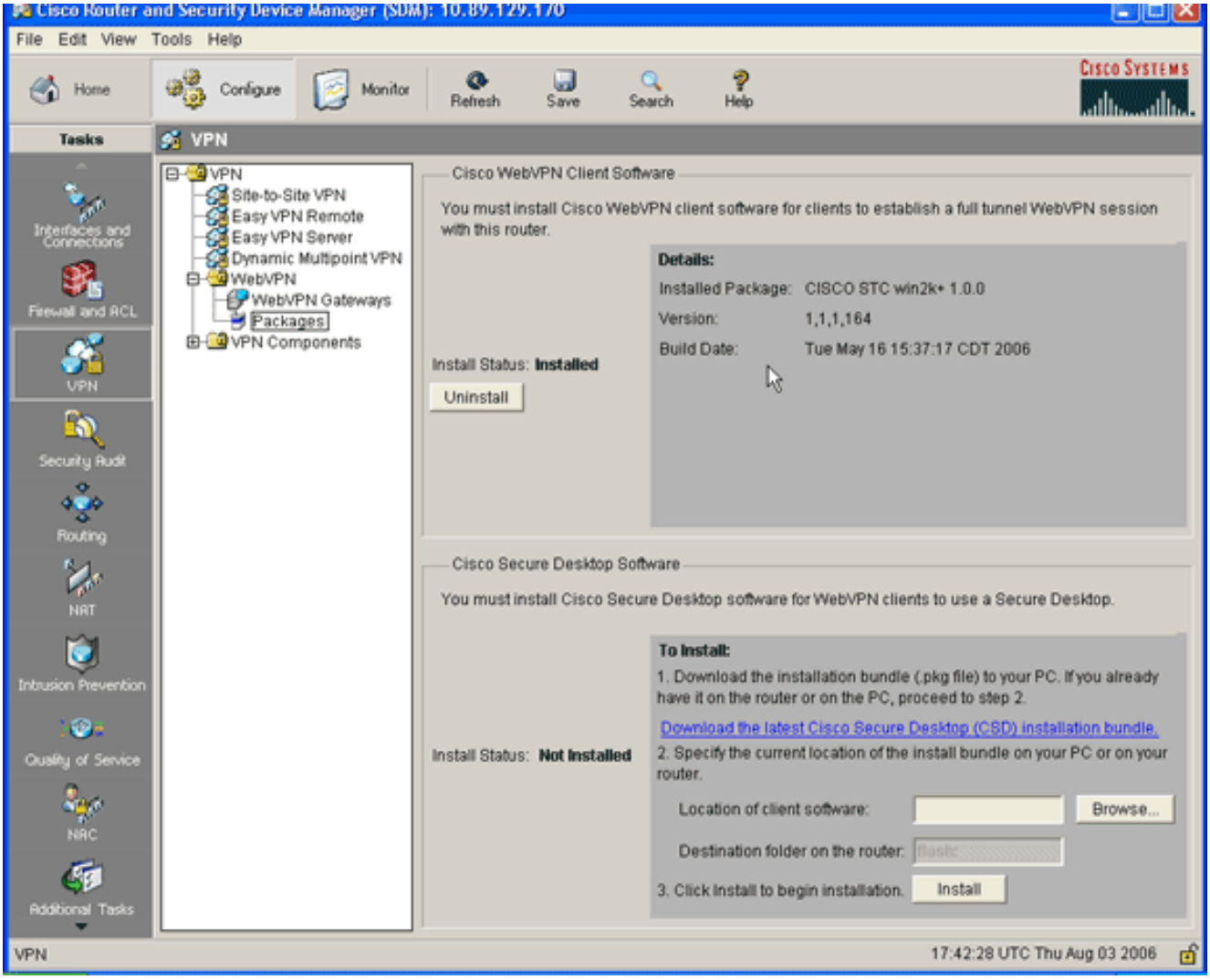
3. Nell'area Cisco WebVPN Client Software, fare clic sul pulsante **Sfoglia**.Verrà visualizzata la finestra di dialogo Seleziona percorso
SVC.



4. Fare clic sul pulsante di scelta **Risorse del computer** e quindi su **Sfoglia** per individuare il pacchetto SVC nel PC di gestione.
5. Fare clic su **OK**, quindi sul pulsante **Installa**.



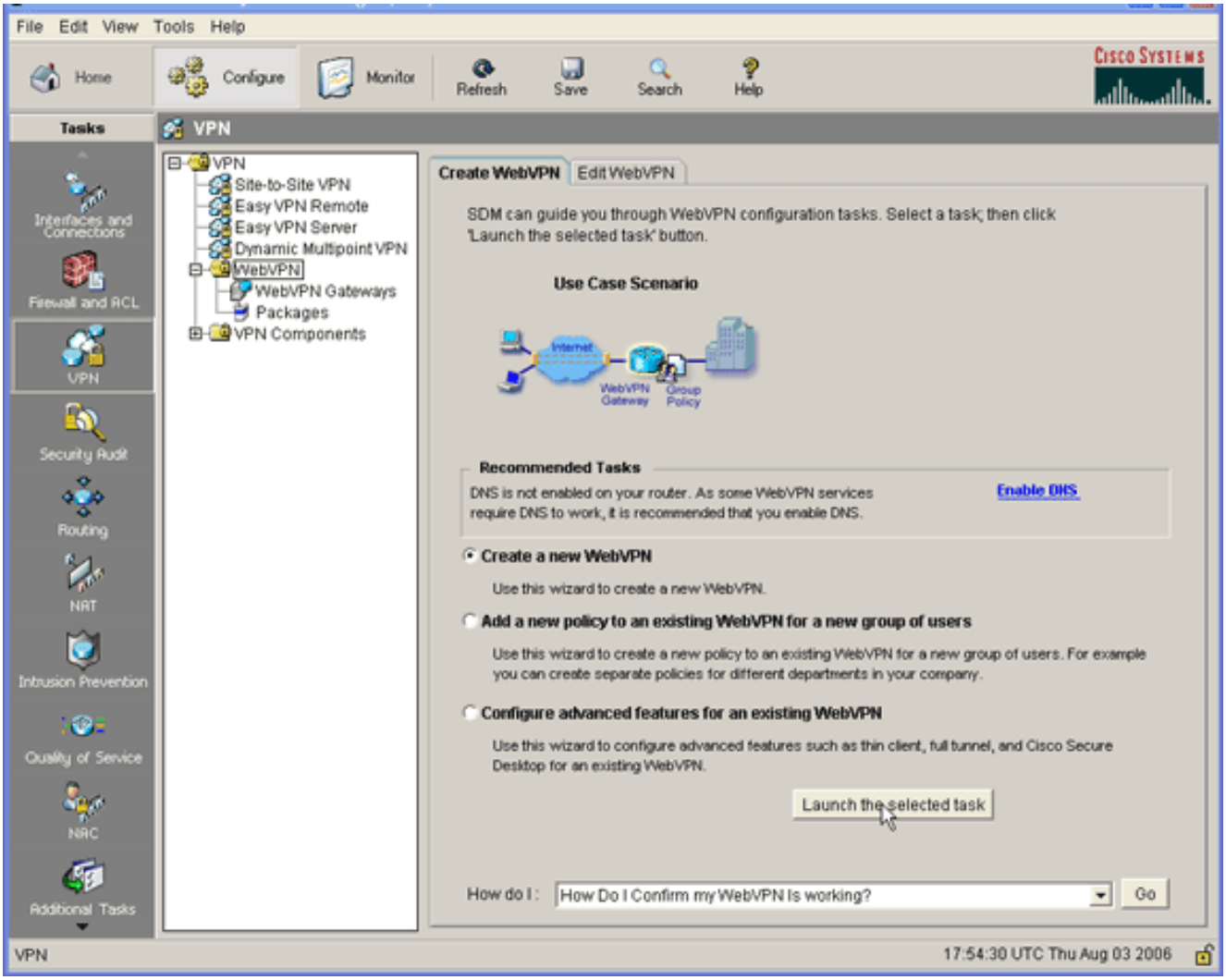
6. Fare clic su **Sì**, quindi su **OK**.L'immagine mostra come il pacchetto SVC è stato installato correttamente:



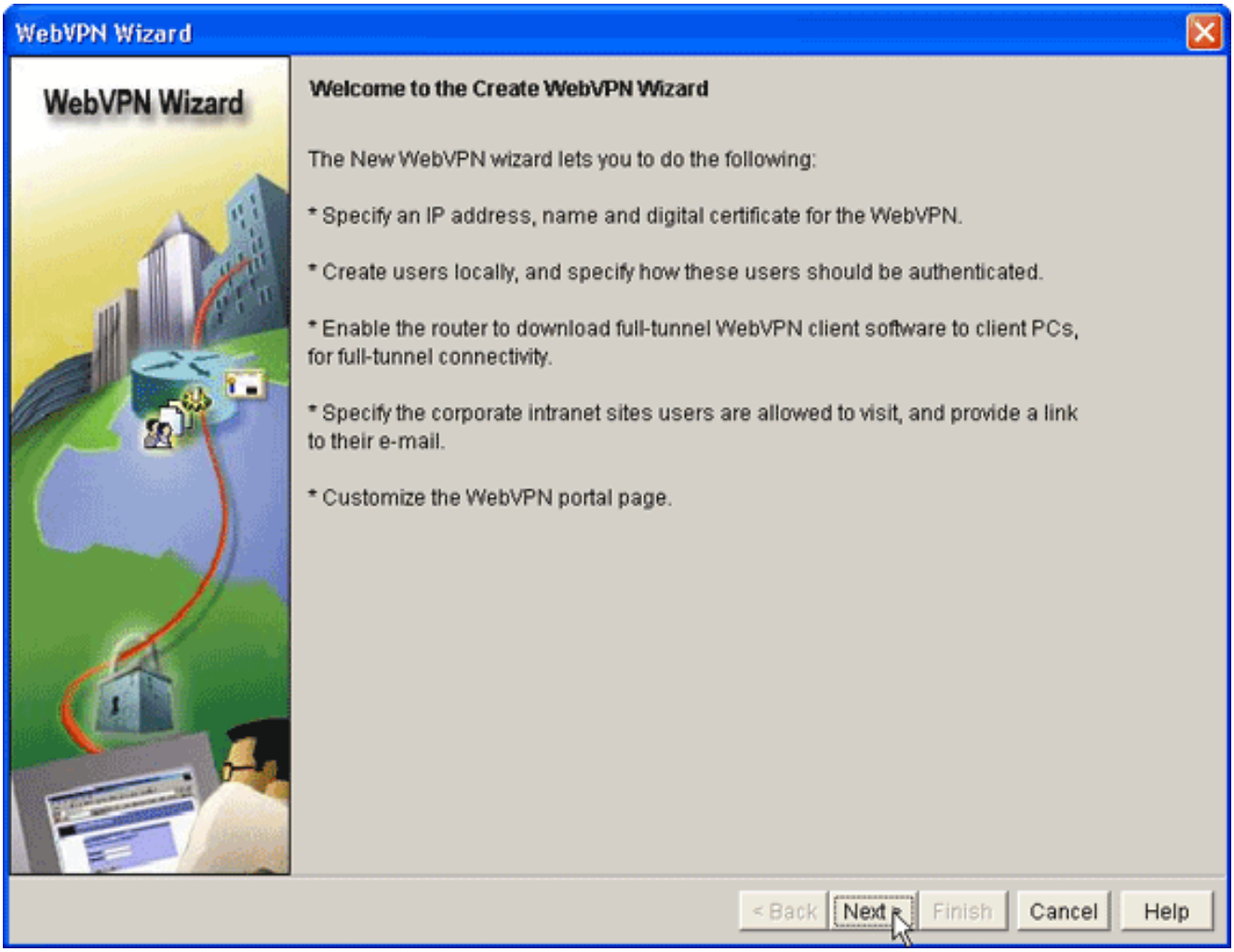
Passaggio 2. Configurare un contesto WebVPN e un gateway WebVPN con la procedura guidata SDM

Per configurare un contesto WebVPN e un gateway WebVPN, completare i seguenti passaggi:

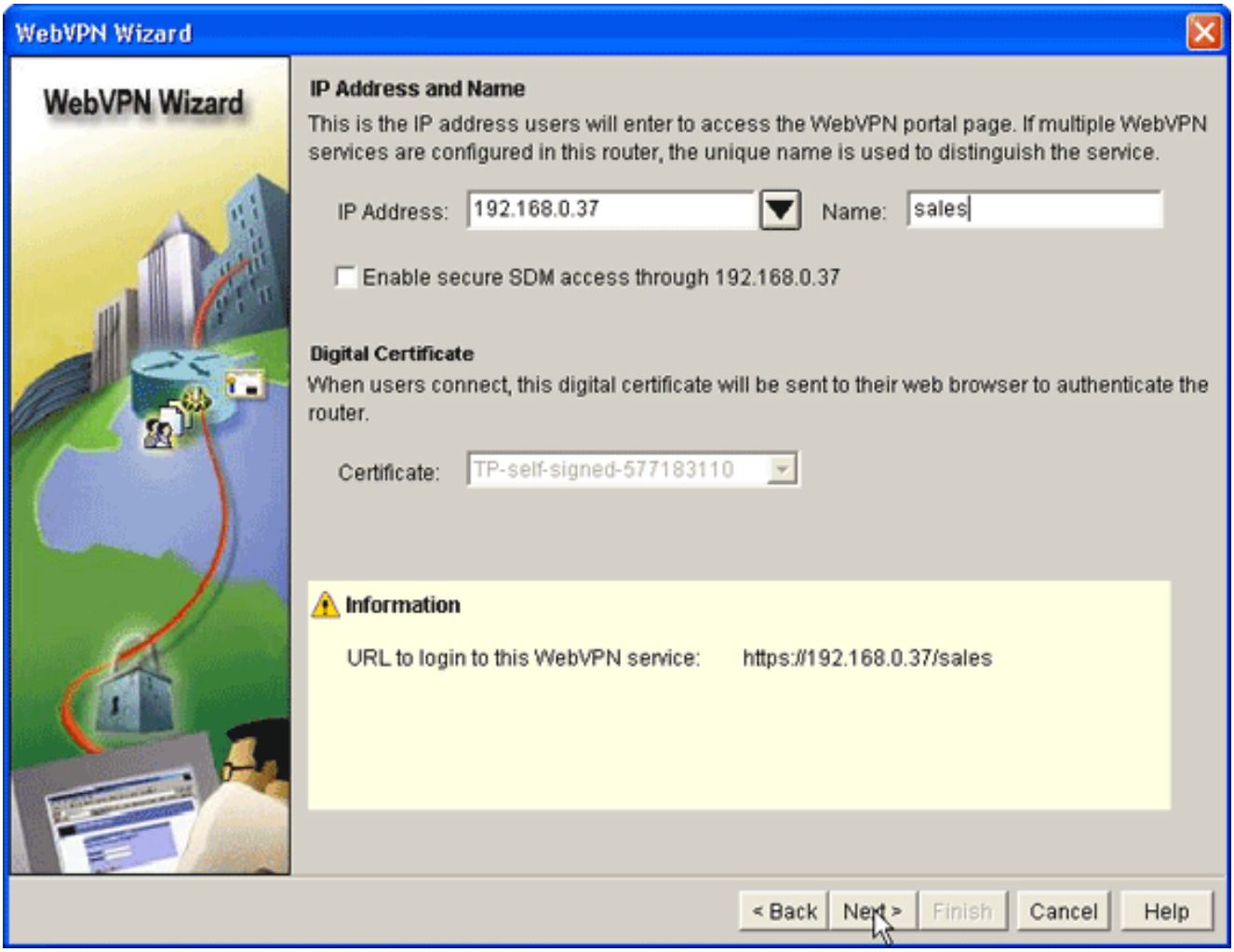
1. Dopo aver installato SVC sul router, fare clic su **Configure** (Configura), quindi su **VPN**.
2. Fare clic su **WebVPN**, quindi selezionare la scheda **Crea WebVPN**.



3. Selezionare il pulsante di opzione **Crea nuova WebVPN** e quindi fare clic su **Avvia l'attività selezionata**.Verrà visualizzata la finestra di dialogo Creazione guidata WebVPN.



4. Fare clic su **Next** (Avanti).



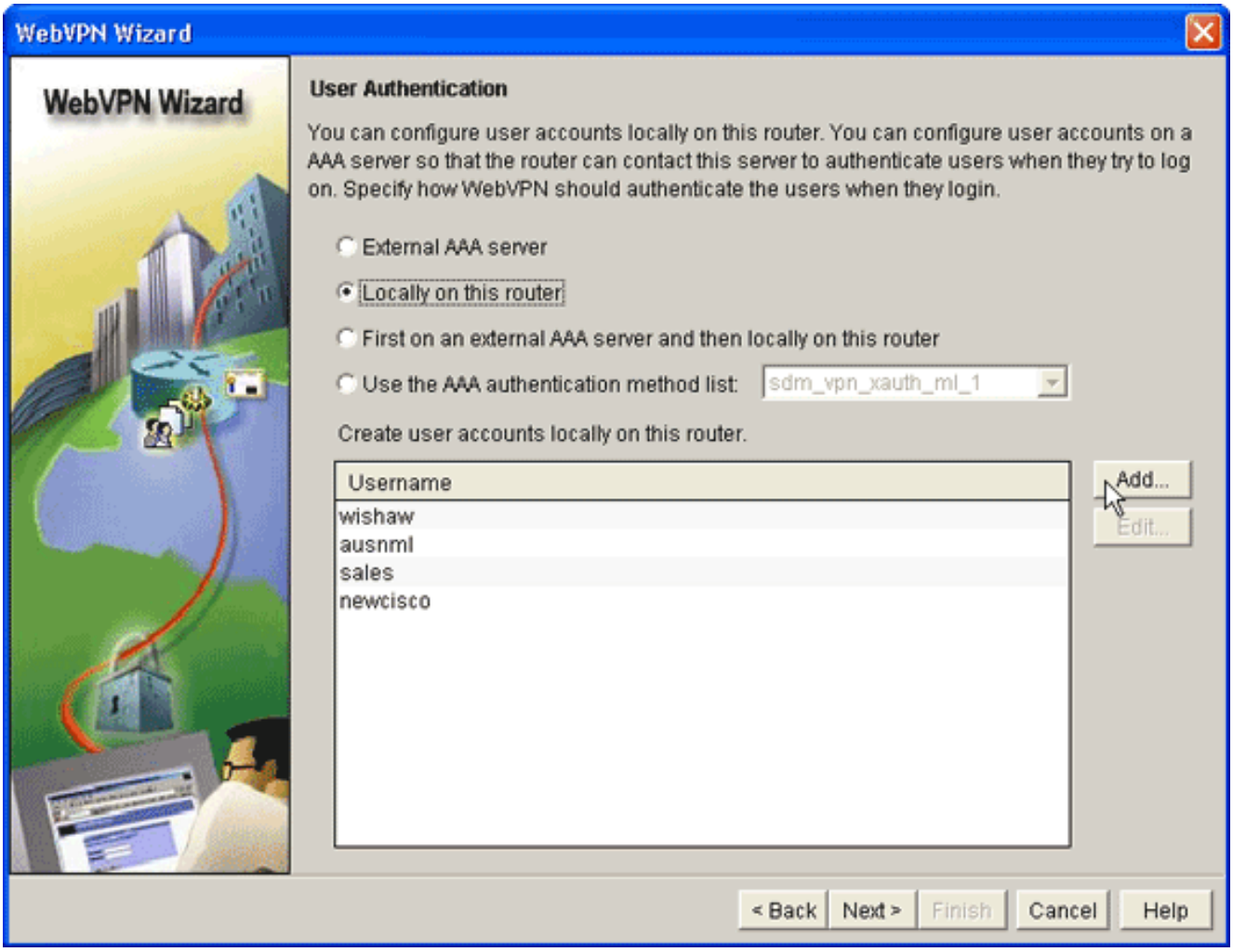
5. Immettere l'indirizzo IP del nuovo gateway WebVPN e un nome univoco per il contesto WebVPN.Èpossibile creare contesti WebVPN diversi per lo stesso indirizzo IP (gateway WebVPN), ma ogni nome deve essere univoco. In questo esempio viene utilizzato il seguente indirizzo IP: *https://192.168.0.37/sales*
6. Fare clic su **Avanti** e continuare con il passo 3.

Passaggio 3. Configurare il database utenti per gli utenti SVC

Per l'autenticazione, è possibile utilizzare un server AAA, utenti locali o entrambi. In questo esempio di configurazione vengono utilizzati per l'autenticazione gli utenti creati localmente.

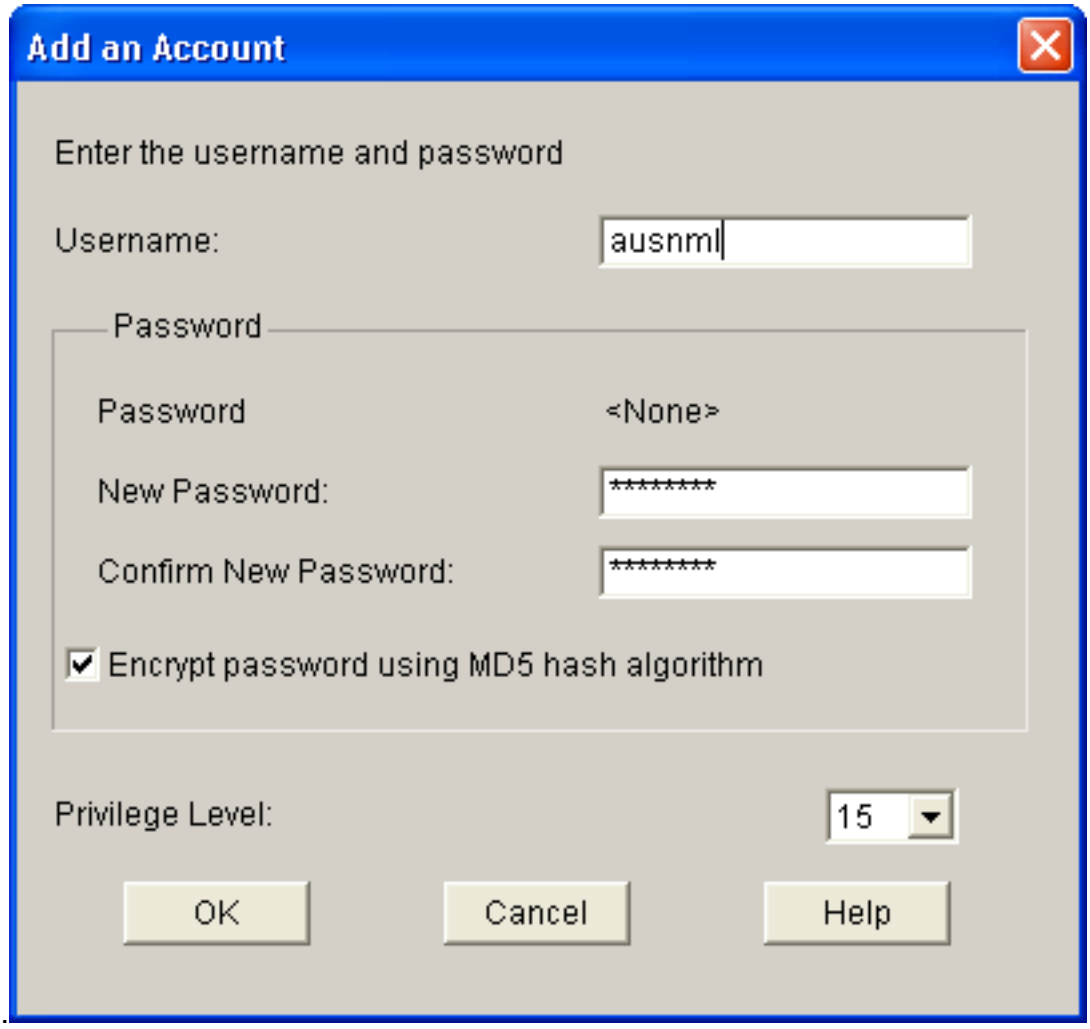
Per configurare il database utenti per gli utenti SVC, completare i seguenti passaggi:

1. Dopo aver completato il passaggio 2, fare clic sul pulsante di opzione **Localmente su questo router** nella finestra di dialogo Autenticazione utente della procedura guidata WebVPN.



Questa finestra di dialogo consente di aggiungere utenti al database locale.

2. Fare clic su **Add** (Aggiungi) e immettere le informazioni



sull'utente.

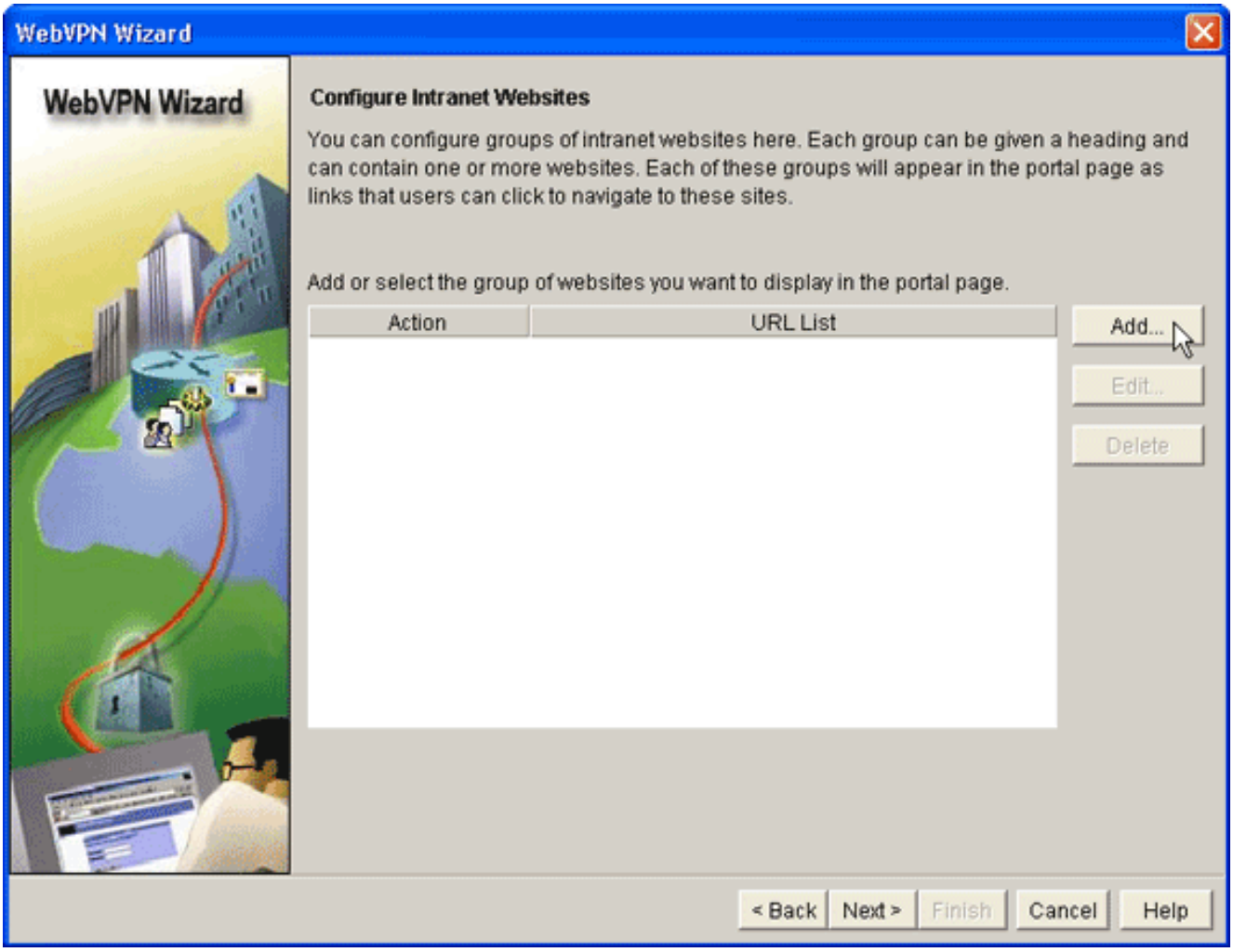
3. Fare clic su **OK** e aggiungere altri utenti, se necessario.
4. Dopo aver aggiunto gli utenti necessari, fare clic su **Avanti** e continuare con il passaggio 4.

Passaggio 4. Configurazione delle risorse da esporre agli utenti

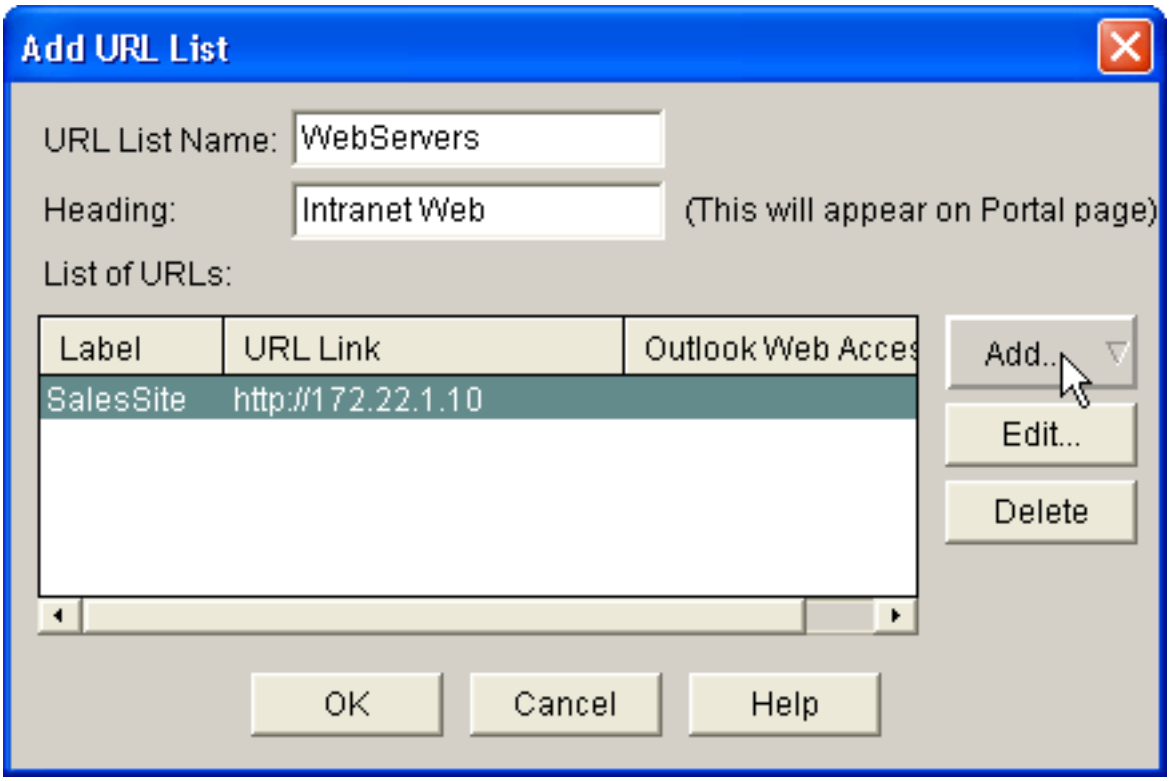
La finestra di dialogo Configurazione guidata WebVPN per Siti Web Intranet consente di selezionare le risorse Intranet che si desidera esporre ai client SVC.

Per configurare le risorse da esporre agli utenti, completare la procedura seguente:

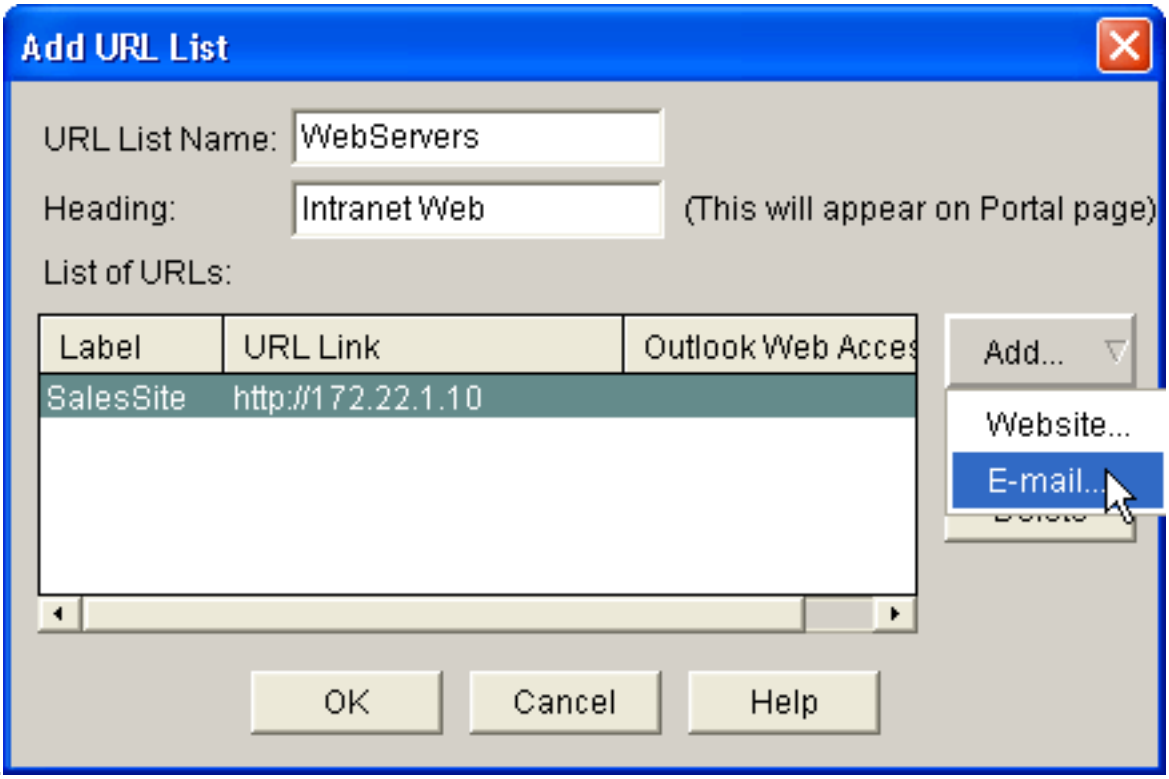
1. Dopo aver completato il passaggio 3, fare clic sul pulsante **Aggiungi** nella finestra di dialogo Configura siti Web
   Intranet.



2. Immettere il nome di un elenco di URL, quindi immettere un'intestazione.

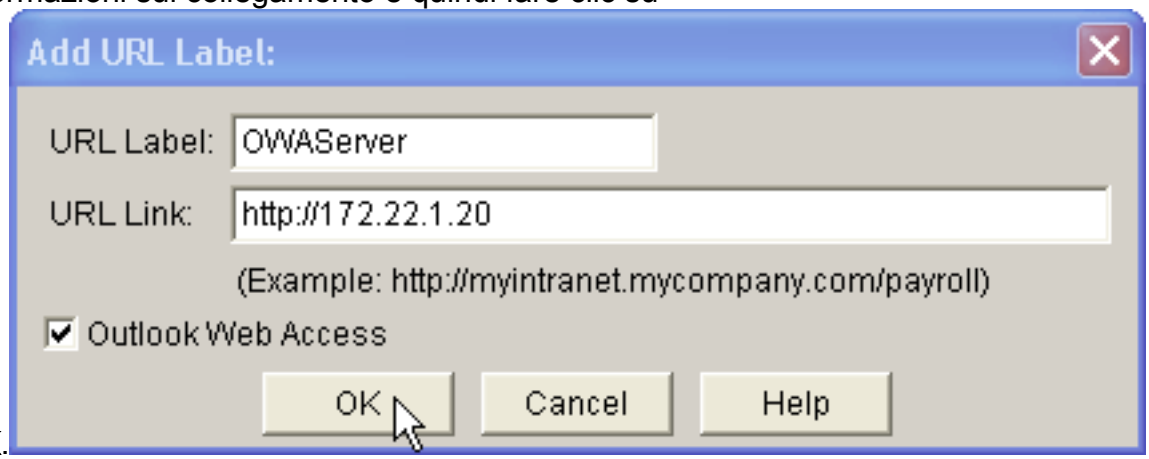


3. Fare clic su **Aggiungi** e scegliere **Sito Web** per aggiungere i siti Web che si desidera esporre al client.
4. Immettere l'URL e le informazioni sul collegamento e quindi fare clic su **OK**.
5. Per aggiungere l'accesso ai server OWA Exchange, fare clic su **Aggiungi** e scegliere **Posta**



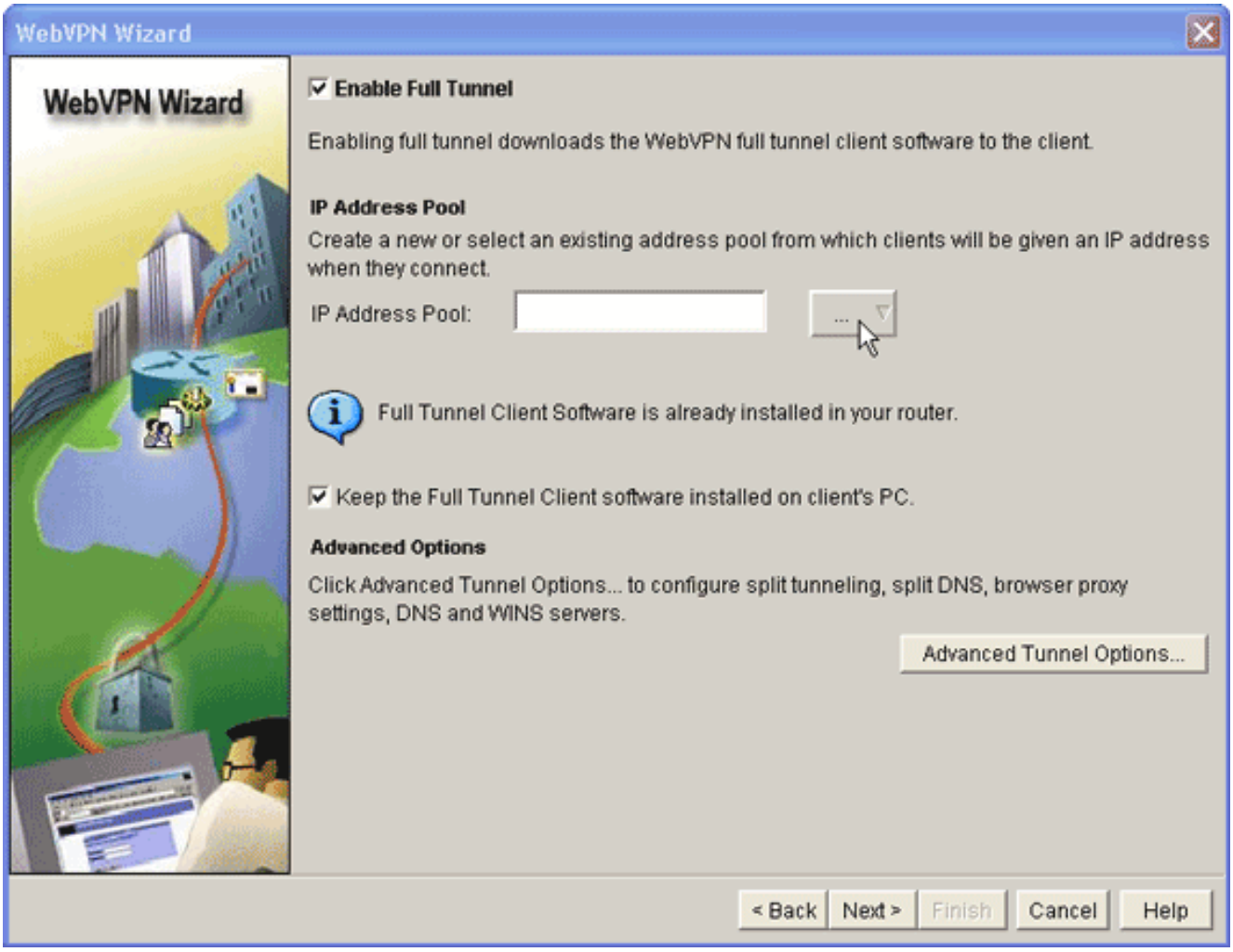
elettronica.

6. Selezionare la casella di controllo **Outlook Web Access**, immettere l'etichetta URL e le informazioni sul collegamento e quindi fare clic su

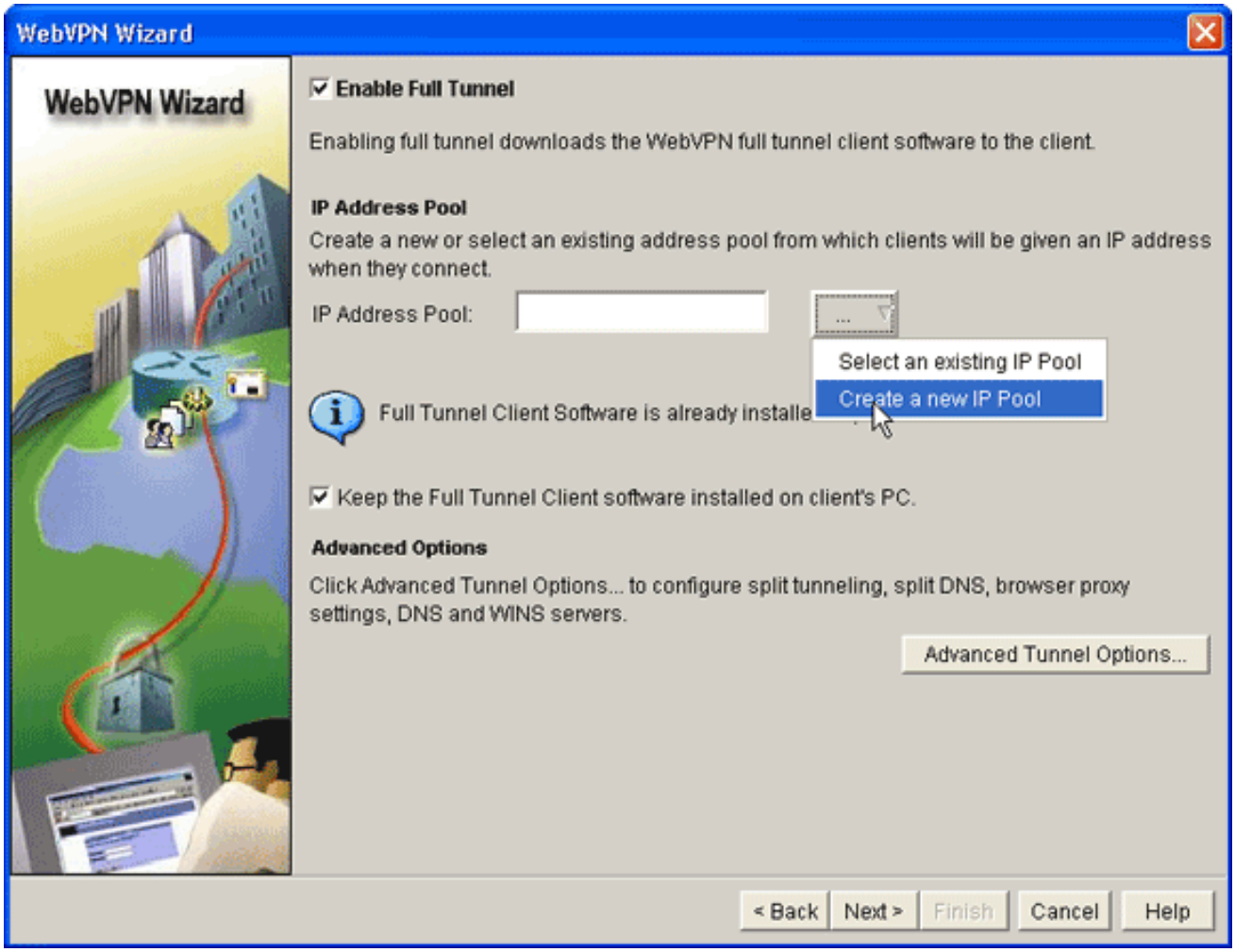


OK.

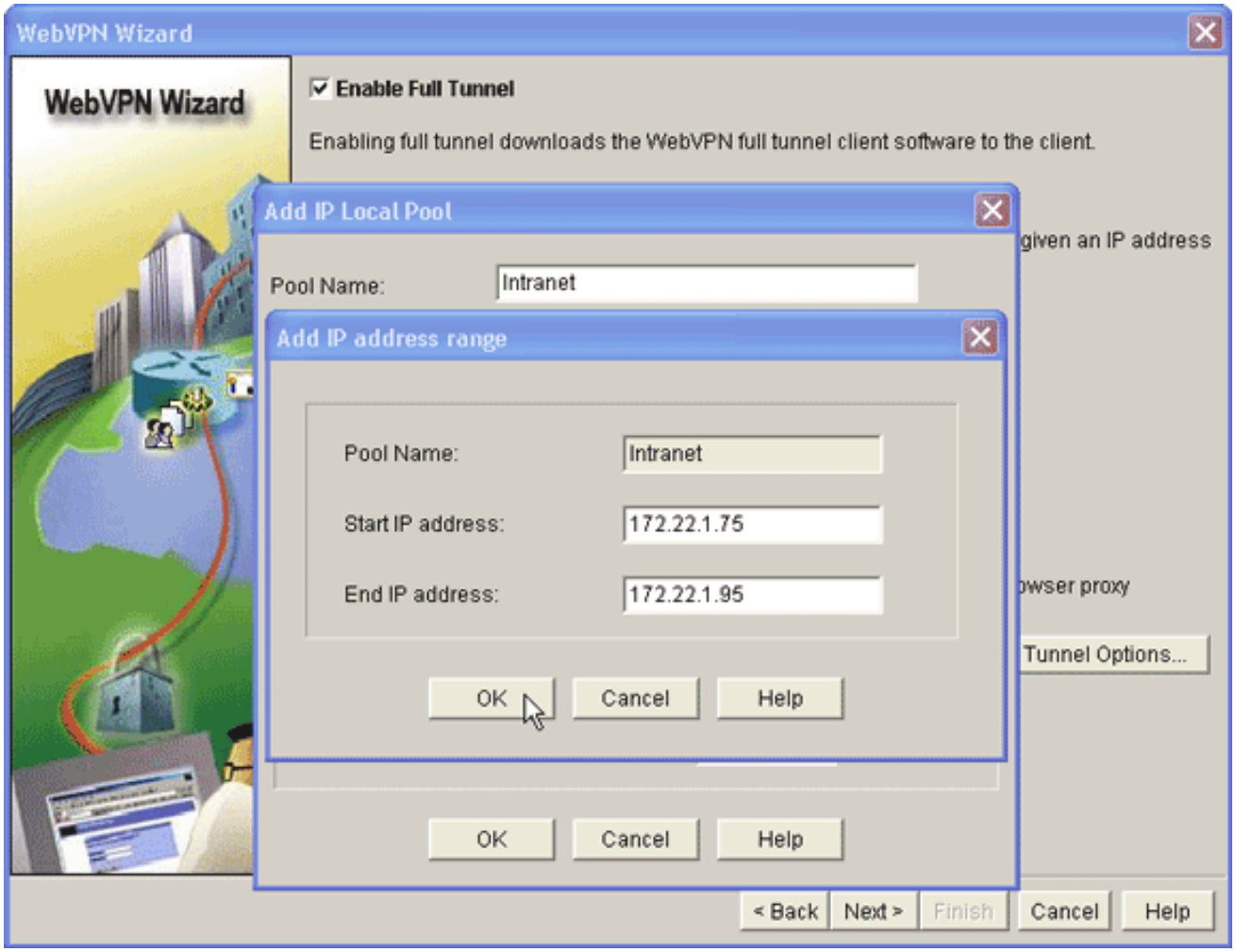
7. Dopo aver aggiunto le risorse desiderate, fare clic su **OK** e quindi su **Avanti**.Verrà visualizzata la finestra di dialogo Tunnel completo di Creazione guidata WebVPN.



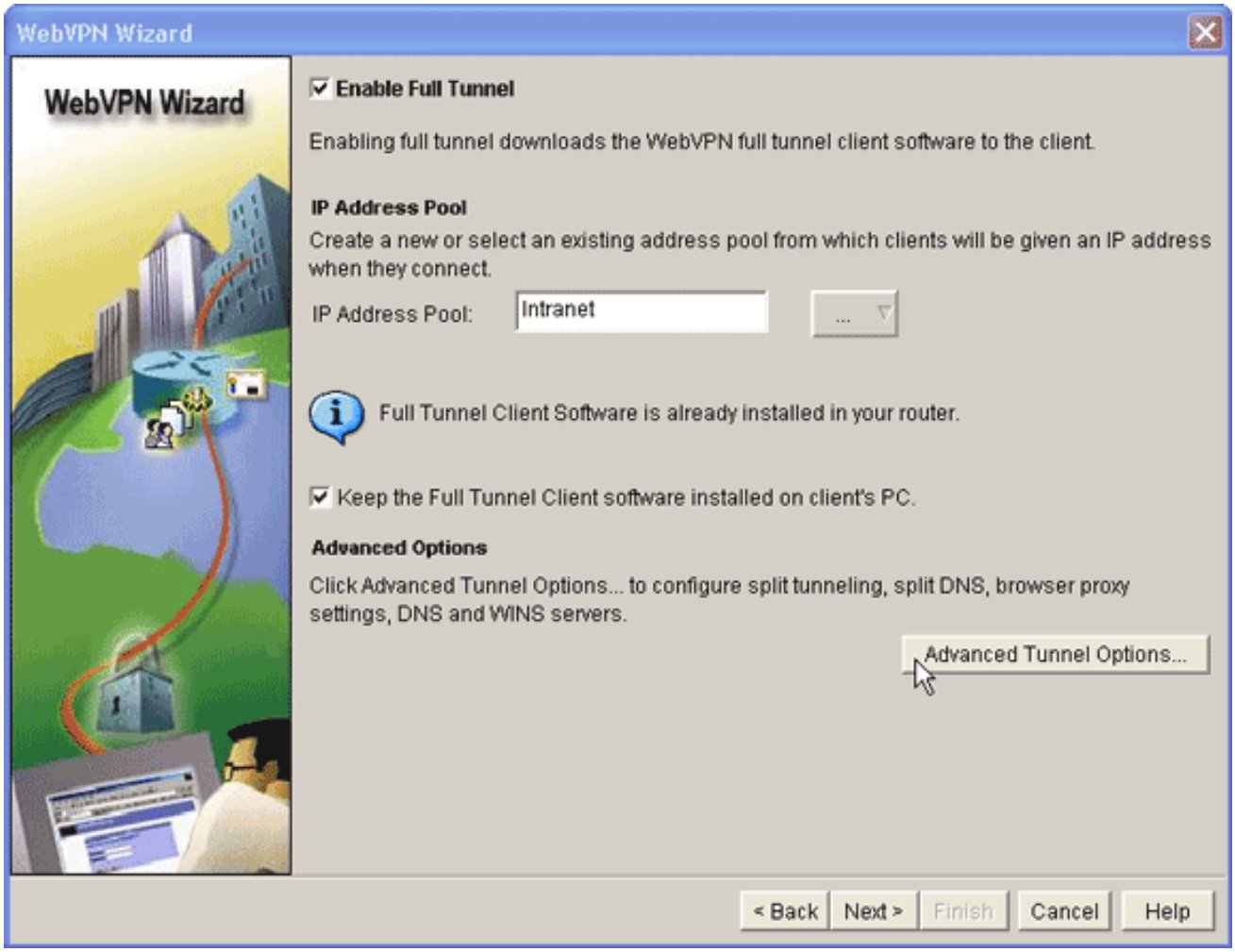
8. Verificare che la casella di controllo **Abilita tunnel completo** sia selezionata.
9. Crea un pool di indirizzi IP utilizzabili dai client di questo contesto WebVPN. Il pool di indirizzi deve corrispondere agli indirizzi disponibili e instradabili nella Intranet.
10. Fare clic sui puntini di sospensione (**...**) accanto al campo Pool di indirizzi IP e scegliere **Crea nuovo pool IP**.



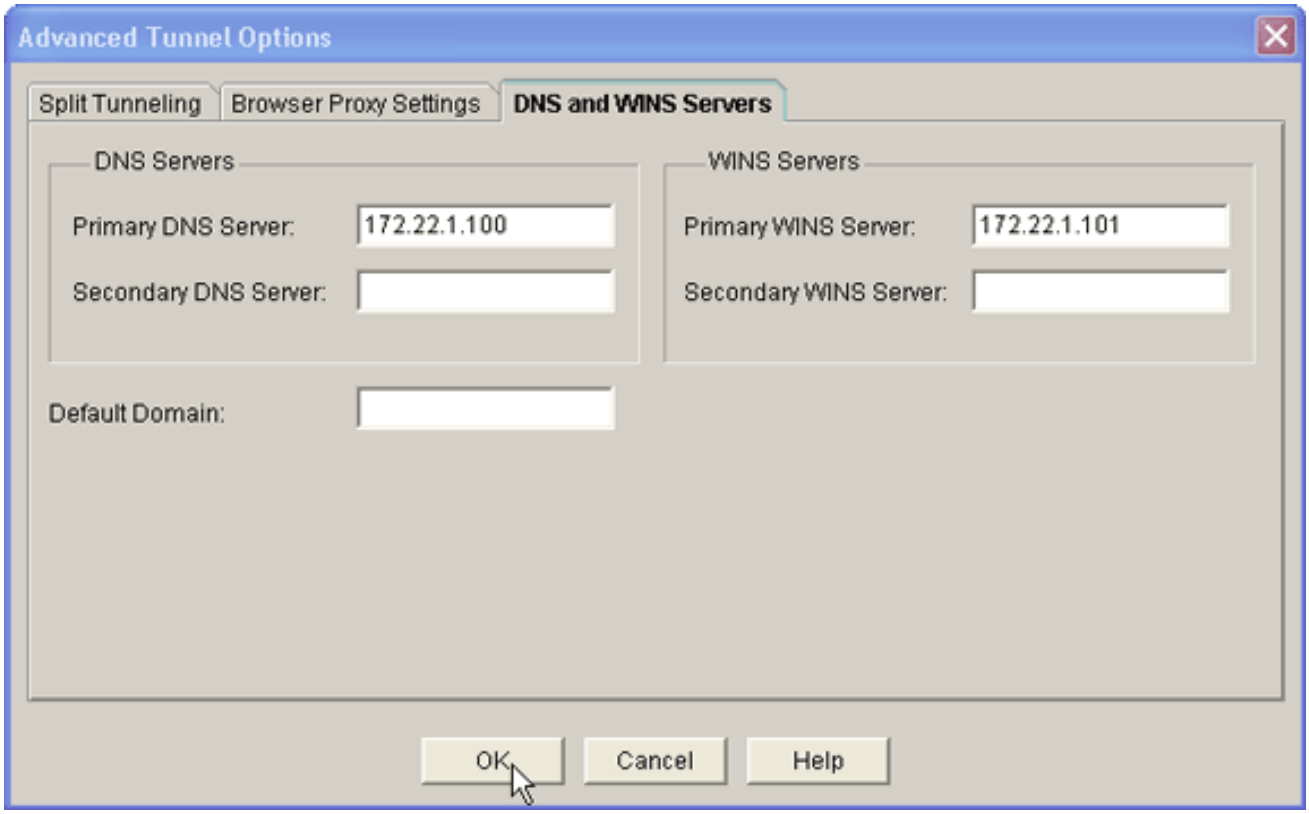
11. Nella finestra di dialogo Aggiungi pool locale IP, immettere un nome per il pool e fare clic su **Aggiungi**.



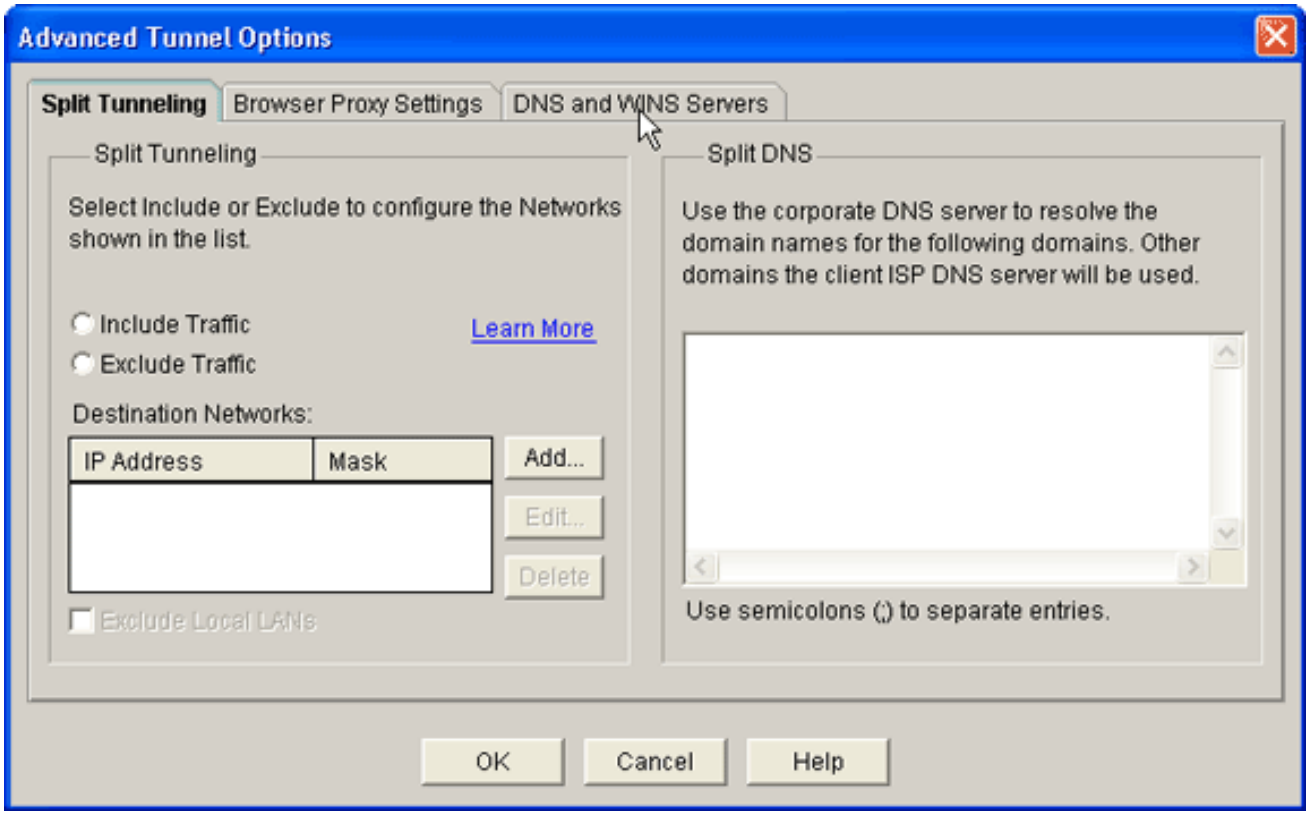
12. Nella finestra di dialogo Aggiungi intervallo di indirizzi IP, immettere l'intervallo di pool di indirizzi per i client SVC e fare clic su **OK**.**Nota:** il pool di indirizzi IP deve essere compreso in un intervallo di un'interfaccia connessa direttamente al router. Se si desidera utilizzare un intervallo di pool diverso, è possibile creare un indirizzo di loopback associato al nuovo pool per soddisfare questo requisito.
13. Fare clic su
    OK.



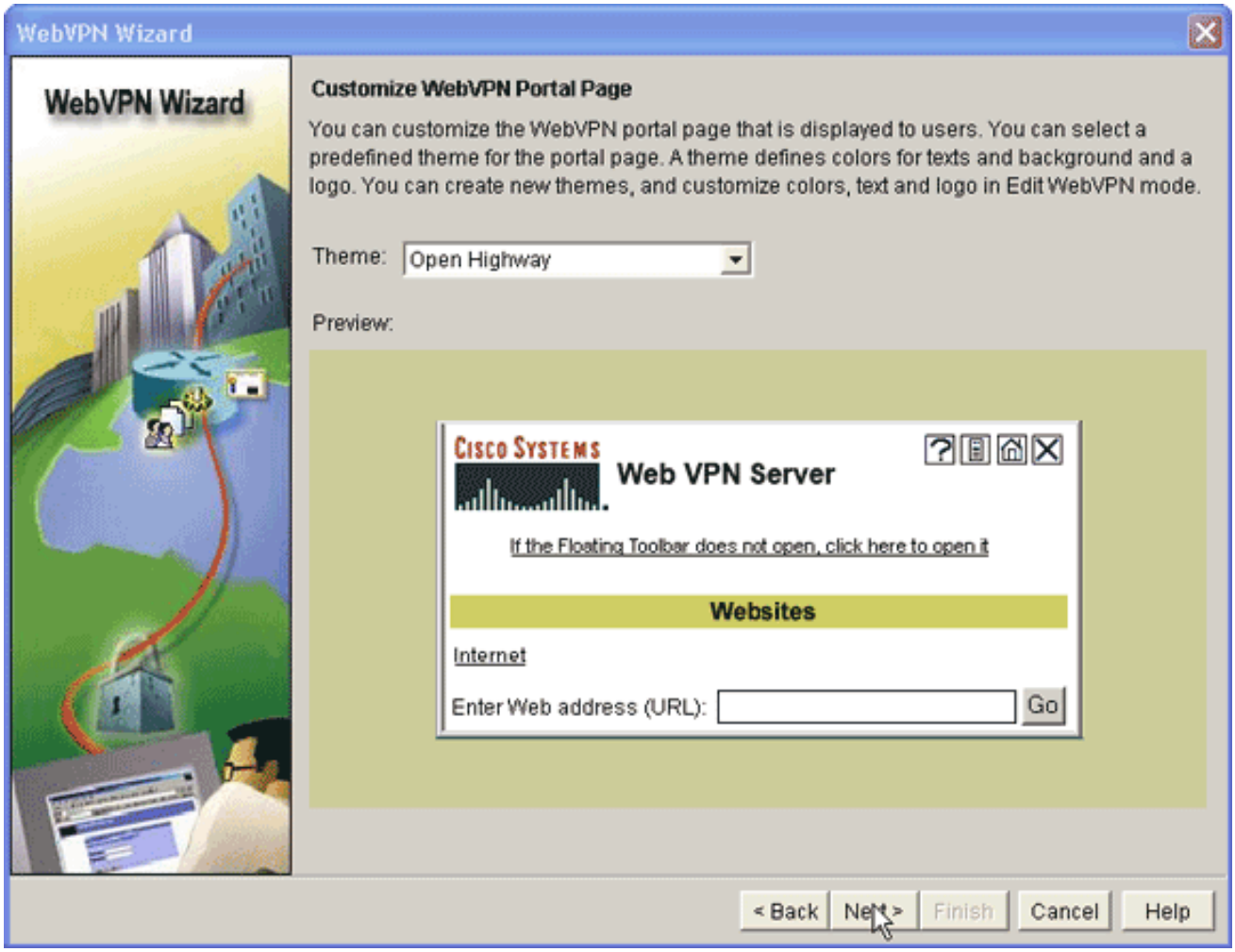
14. Se si desidera che i client remoti memorizzino in modo permanente una copia dell'SVC, selezionare la casella di controllo **Mantieni il software client del tunnel completo installato sul PC del client**. Deselezionare questa opzione per richiedere al client di scaricare il software SVC ogni volta che si connette un client.
15. Configurare le opzioni avanzate del tunnel, ad esempio il tunneling suddiviso, il DNS suddiviso, le impostazioni proxy del browser e i server DNS e WNS. Cisco consiglia di configurare almeno i server DNS e WINS.Per configurare le opzioni avanzate del tunnel, procedere come segue:Fare clic sul pulsante **Opzioni avanzate tunnel**.



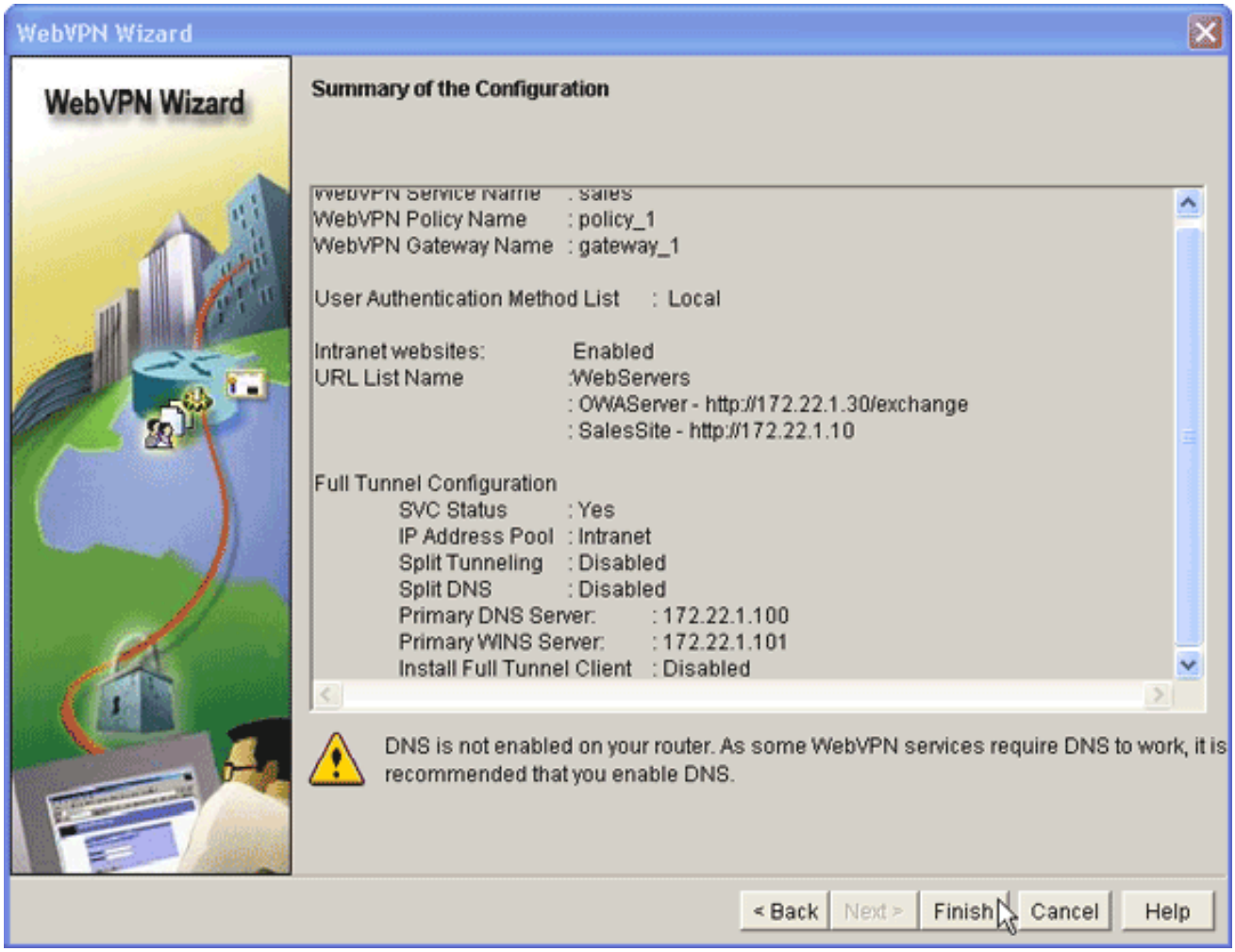
Fare clic sulla scheda **Server DNS e WINS** e immettere gli indirizzi IP primari per i server DNS e WINS.Per configurare le impostazioni del tunneling suddiviso e del proxy del browser, fare clic sulla scheda **Tunneling suddiviso** o **Impostazioni proxy browser**.



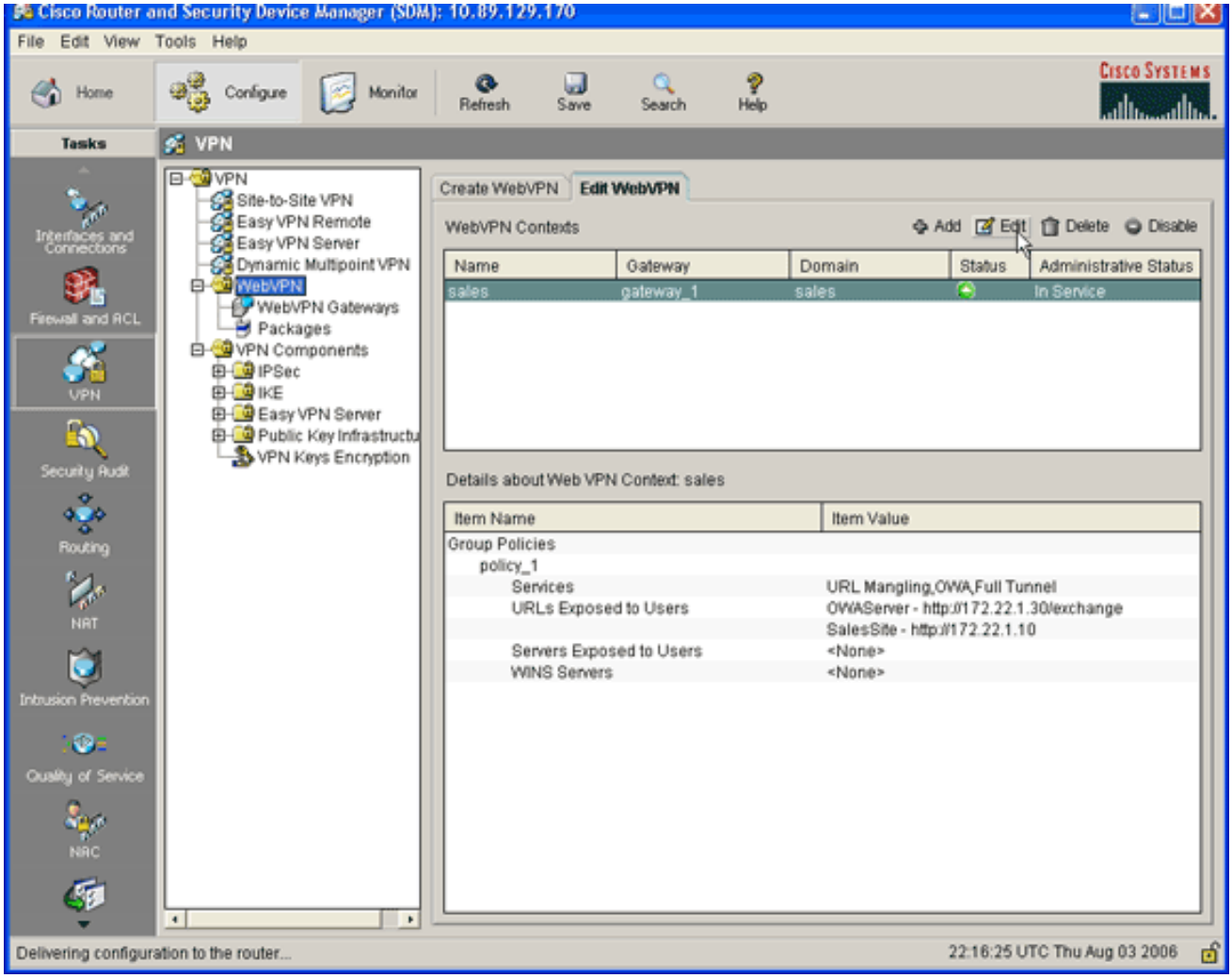
16. Dopo aver configurato le opzioni necessarie, fare clic su **Avanti**.
17. Personalizzare la pagina del portale WebVPN o selezionare i valori predefiniti.La pagina Personalizza portale WebVPN consente di personalizzare l'aspetto della pagina portale WebVPN per i
clienti.



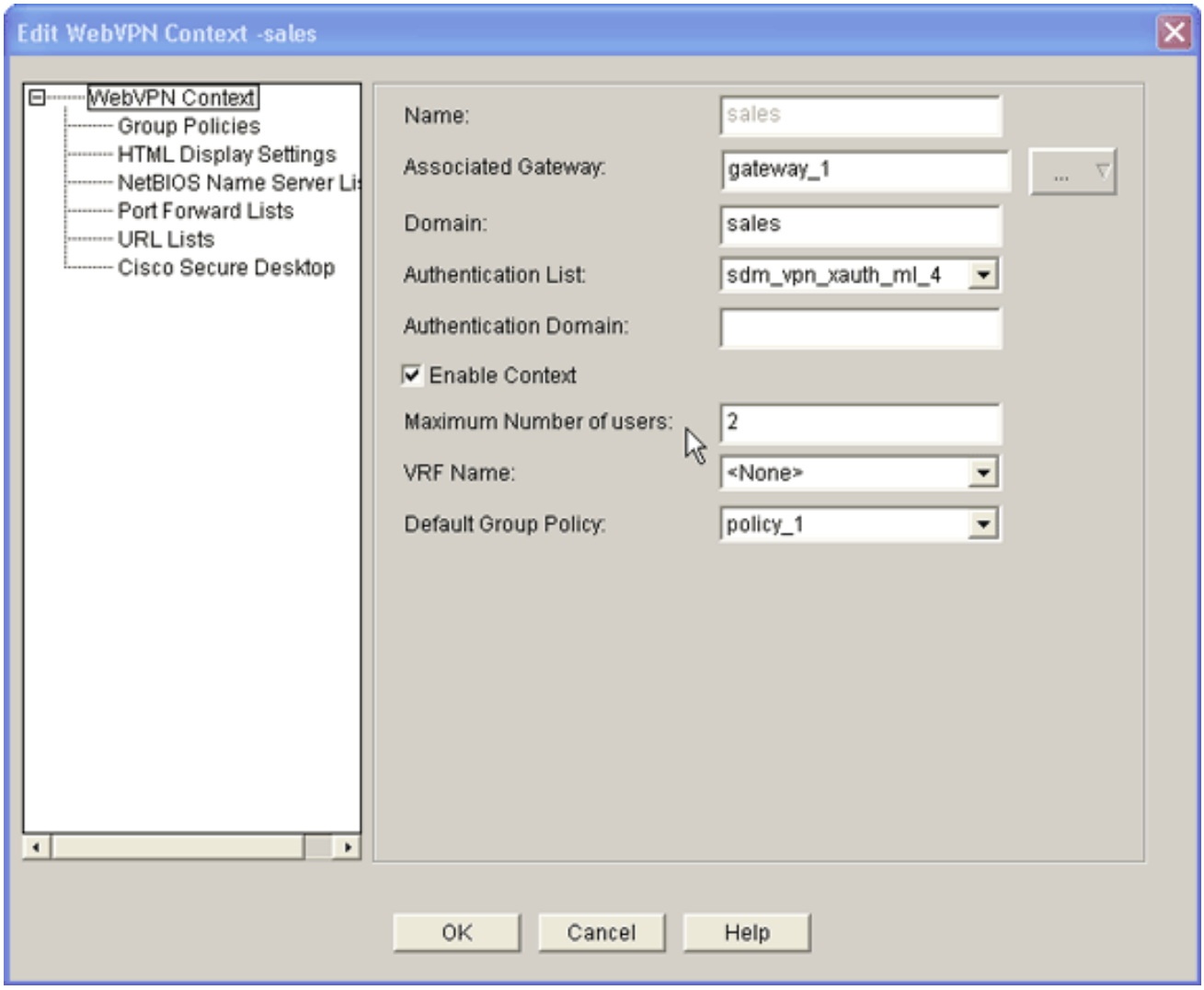
18. Dopo aver configurato la pagina del portale WebVPN, fare clic su **Avanti**, su **Fine** e quindi su **OK**.La Creazione guidata WebVPN invia i comandi della presentazione al router.
19. Fare clic su **OK** per salvare la configurazione.**Nota:** se viene visualizzato un messaggio di errore, la licenza WebVPN potrebbe non essere corretta. Nell'immagine viene visualizzato un messaggio di errore di
    esempio:



Per risolvere un problema di licenza, attenersi alla seguente procedura:Fare clic su **Configura** e quindi su **VPN**.Espandere **WebVPN** e fare clic sulla scheda **Modifica WebVPN**.



Evidenziare il contesto appena creato e fare clic sul pulsante **Modifica**.



Nel campo Numero massimo di utenti, immettere il numero corretto di utenti per la licenza.Fare clic su **OK**, quindi su **OK**.I comandi vengono scritti nel file di configurazione.Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

Risultati

ASDM crea le seguenti configurazioni della riga di comando:

ausnml-3825-01

```
ausnml-3825-01#show run
Building configuration...

Current configuration : 4393 bytes
!
! Last configuration change at 22:24:06 UTC Thu Aug 3
2006 by ausnml
! NVRAM config last updated at 22:28:54 UTC Thu Aug 3
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
```

```
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
!
aaa new-model
!
!--- Added by SDM for local aaa authentication. aaa
authentication login sdm_vpn_xauth_ml_1 local aaa
authentication login sdm_vpn_xauth_ml_2 local aaa
authentication login sdm_vpn_xauth_ml_3 local aaa
authentication login sdm_vpn_xauth_ml_4 local ! aaa
session-id common ! resource policy ! ip cef ! ip domain
name cisco.com ! voice-card 0 no dspfarm !--- Digital
certificate information. crypto pki trustpoint TP-self-
signed-577183110 enrollment selfsigned subject-name
cn=IOS-Self-Signed-Certificate-577183110 revocation-
check none rsakeypair TP-self-signed-577183110 ! crypto
pki certificate chain TP-self-signed-577183110
certificate self-signed 01 3082024E 308201B7 A0030201
02020101 300D0609 2A864886 F70D0101 04050030 30312E30
2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274 69666963 6174652D 35373731 38333131 30301E17
0D303630 37323731 37343434 365A170D 32303031 30313030
30303030 5A303031 2E302C06 03550403 1325494F 532D5365
6C662D53 69676E65 642D4365 72746966 69636174 652D3537
37313833 31313030 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100 F43F6DD9 32A264FE 4C5B0829
698265DC 6EC65B17 21661972 D363BC4C 977C3810 !--- Output
suppressed. quit username wishaw privilege 15 secret 5
$1$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
15 password 7 044E1F505622434B username sales privilege
15 secret 5 $1$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
newcisco privilege 15 secret 5
$1$Axlm$7k5PWspXKxUpoSReHo7IQ1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
ip virtual-reassembly duplex auto speed auto media-type
rj45 no keepalive ! interface GigabitEthernet0/1 ip
address 172.22.1.151 255.255.255.0 duplex auto speed
auto media-type rj45 !--- Clients receive an address
from this pool. ip local pool Intranet 172.22.1.75
172.22.1.95 ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip
http server ip http authentication local ip http secure-
server ip http timeout-policy idle 600 life 86400
requests 100 ! control-plane ! line con 0 stopbits 1
line aux 0 stopbits 1 line vty 0 4 ! scheduler allocate
20000 1000 !--- Identify the gateway and port. webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint TP-self-signed-577183110
inservice !--- SVC package file. webvpn install svc
flash:/webvpn/svc.pkg ! !--- WebVPN context. webvpn
context sales title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all ! !---
Resources available to this context. url-list
"WebServers" heading "Intranet Web" url-text "SalesSite"
url-value "http://172.22.1.10" url-text "OWAServer" url-
value "http://172.22.1.20/exchange" ! nbns-list NBNS-
Servers nbns-server 172.22.1.15 master !--- Group policy
for the context. policy group policy_1 url-list
"WebServers" functions svc-enabled svc address-pool
"Intranet" svc default-domain "cisco.com" svc keep-
client-installed svc dns-server primary 172.22.1.100 svc
wins-server primary 172.22.1.101 default-group-policy
```

```
policy_1 aaa authentication list sdm_vpn_xauth_ml_4
gateway gateway_1 domain sales max-users 2 inservice ! !
end
```

Verifica

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

Procedura

Per verificare la configurazione, immettere *http://192.168.0.37/sales* in un browser Web client abilitato per SSL.

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.

Problema di connettività SSL

Problema: I client VPN SSL non sono in grado di connettere il router.

Soluzione: Il problema potrebbe essere causato da indirizzi IP insufficienti nel pool di indirizzi IP. Per risolvere il problema, aumentare il numero di indirizzi IP nel pool di indirizzi IP sul router.

Comandi per la risoluzione dei problemi

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

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

- Cisco IOS SSLVPN

- SSL VPN - WebVPN
- Esempio di configurazione di una VPN SSL senza client (WebVPN) su Cisco IOS con SDM
- Esempio di configurazione di IOS per una VPN SSL thin-client (WebVPN) con SDM
- Guida all'installazione di WebVPN e DMVPN Convergence
- Documentazione e supporto tecnico – Cisco Systems