Configurazione di una VPN SSL thin-client (WebVPN) Cisco IOS con SDM

Sommario

Introduzione

La tecnologia VPN SSL thin client può essere utilizzata per consentire l'accesso sicuro alle applicazioni che utilizzano porte statiche. Gli esempi sono Telnet (23), SSH (22), POP3 (110), IMAP4 (143) e SMTP (25). Thin-Client può essere guidato dall'utente, basato su regole o entrambi. È possibile configurare l'accesso in base al singolo utente oppure creare criteri di gruppo che includono uno o più utenti. La tecnologia VPN SSL può essere configurata in tre modalità principali: VPN SSL senza client (WebVPN), VPN SSL thin client (inoltro porte) e client VPN SSL (modalità tunnel completo SVC).

1. VPN SSL senza client (WebVPN):

Un client remoto richiede solo un browser abilitato per SSL per accedere ai server Web abilitati per http o https sulla LAN aziendale. È inoltre possibile cercare file di Windows utilizzando il CIFS (Common Internet File System). Un buon esempio di accesso http è il client Outlook Web Access (OWA).

Per ulteriori informazioni sulla VPN SSL senza client, fare riferimento a VPN SSL senza client (WebVPN) su Cisco IOS con esempio di configurazione SDM.

2. VPN SSL thin-client (inoltro porte)

Un client remoto deve scaricare una piccola applet basata su Java per un accesso sicuro alle applicazioni TCP che utilizzano numeri di porta statici. UDP non supportato. Gli esempi includono l'accesso a POP3, SMTP, IMAP, SSH e Telnet. L'utente deve disporre di privilegi amministrativi locali perché vengono apportate modifiche ai file nel computer locale. Questo metodo di VPN SSL non funziona con le applicazioni che utilizzano assegnazioni dinamiche delle porte, ad esempio diverse applicazioni FTP.

3. Client VPN SSL (modalità tunnel SVC-Full):

Il client VPN SSL scarica un client di piccole dimensioni sulla workstation remota e consente l'accesso completo e sicuro alle risorse sulla rete aziendale interna. L'SVC può essere scaricato in modo permanente sulla stazione remota o rimosso al termine della sessione protetta.

Per ulteriori informazioni sul client VPN SSL, fare riferimento a SSL VPN Client (SVC) su IOS che utilizza la configurazione SDM.

In questo documento viene illustrata una configurazione semplice per la VPN SSL thin-client su un router Cisco IOS®. La VPN SSL thin-client viene eseguita sui seguenti router Cisco IOS:

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

Prerequisiti

Requisiti

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

Requisiti per il router Cisco IOS

- Uno dei router elencati caricato con SDM e un'immagine avanzata di IOS versione 12.4(6)T o successive
- Stazione di gestione caricata con SDMCisco invia ai nuovi router una copia preinstallata dell'SDM. Se sul router non è installato SDM, è possibile scaricare il software da Software Download-Cisco Security Device Manager. Devi possedere un account CCO con un contratto di assistenza. Per istruzioni dettagliate, consultare il documento sulla configurazione del router con Security Device Manager.

Requisiti per i computer client

- I client remoti devono disporre di privilegi amministrativi locali; non è obbligatorio, ma è altamente suggerito.
- I client remoti devono disporre di Java Runtime Environment (JRE) versione 1.4 o successiva.
- Browser client remoti: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 o Firefox 1.0
- Cookie attivati e popup consentiti su client remoti

Componenti usati

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

hardware:

- Cisco Advanced Enterprise Software Image 12.4(9)T
- Cisco 3825 Integrated Services Router
- Cisco Router and Security Device Manager (SDM) versione 2.3.1

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. Gli indirizzi IP utilizzati per questa configurazione provengono dallo spazio di indirizzi della RFC 1918. Non sono legali su Internet.

Convenzioni

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

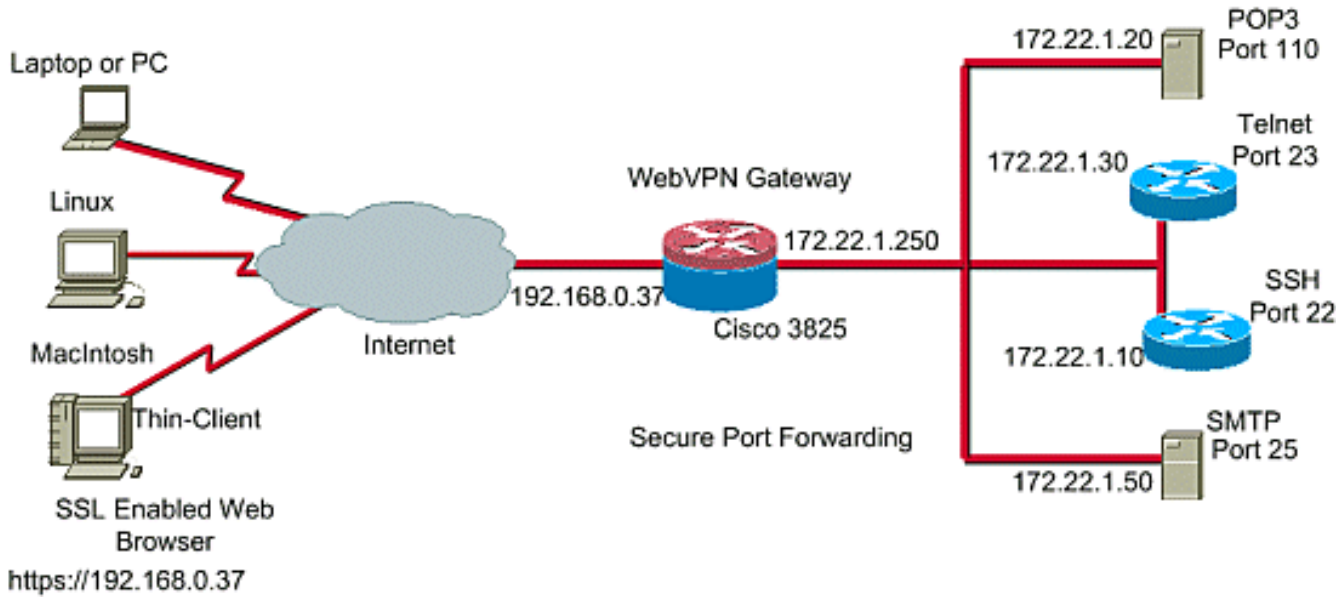
Configurazione

Attività

Questa sezione contiene le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

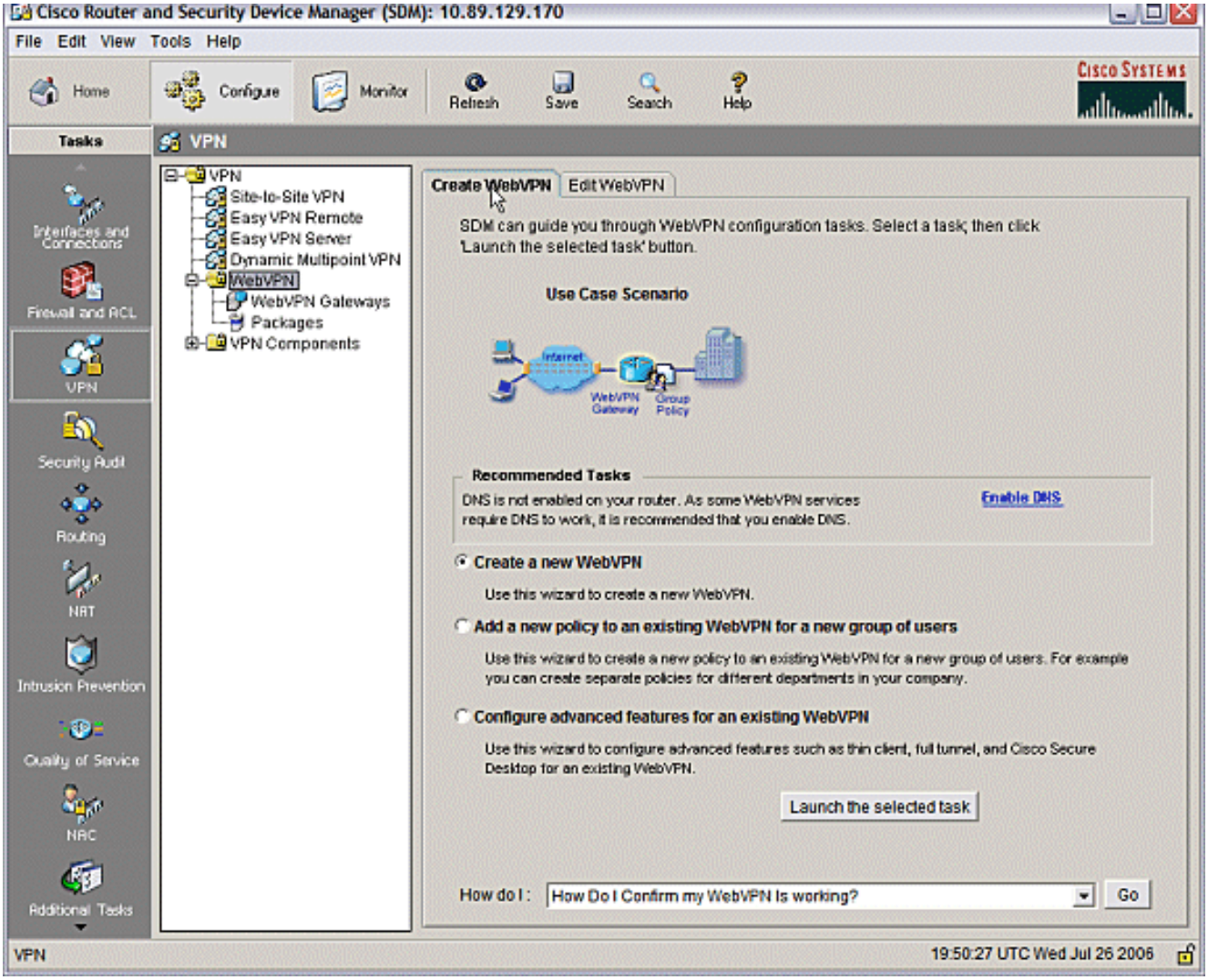
Nel documento viene usata questa impostazione di rete:



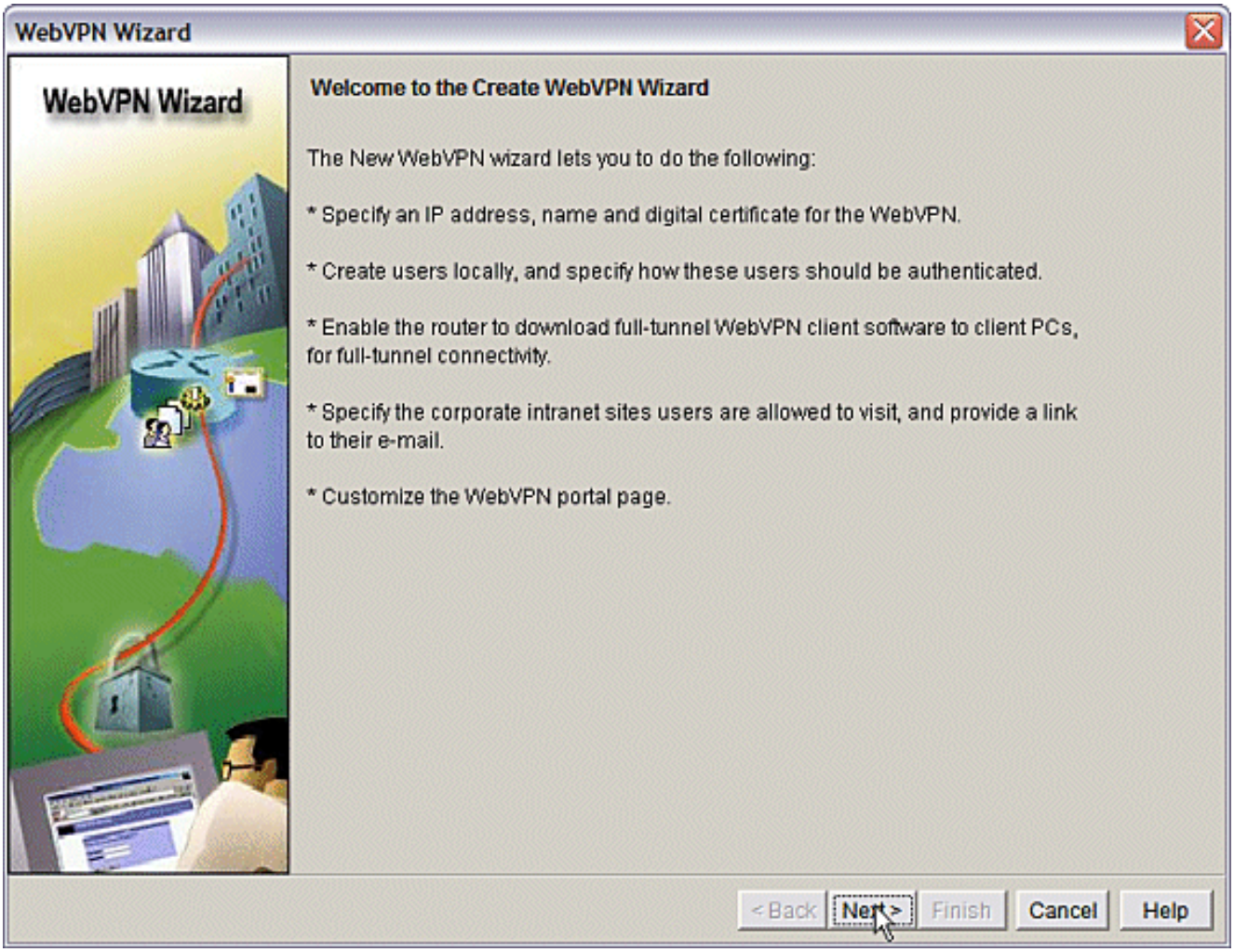
Configurare la VPN SSL thin client

Utilizzare la procedura guidata fornita nell'interfaccia di Security Device Manager (SDM) per configurare la VPN SSL thin-client su Cisco IOS o configurarla nell'interfaccia della riga di comando (CLI) o manualmente nell'applicazione SDM. In questo esempio viene utilizzata la procedura guidata.

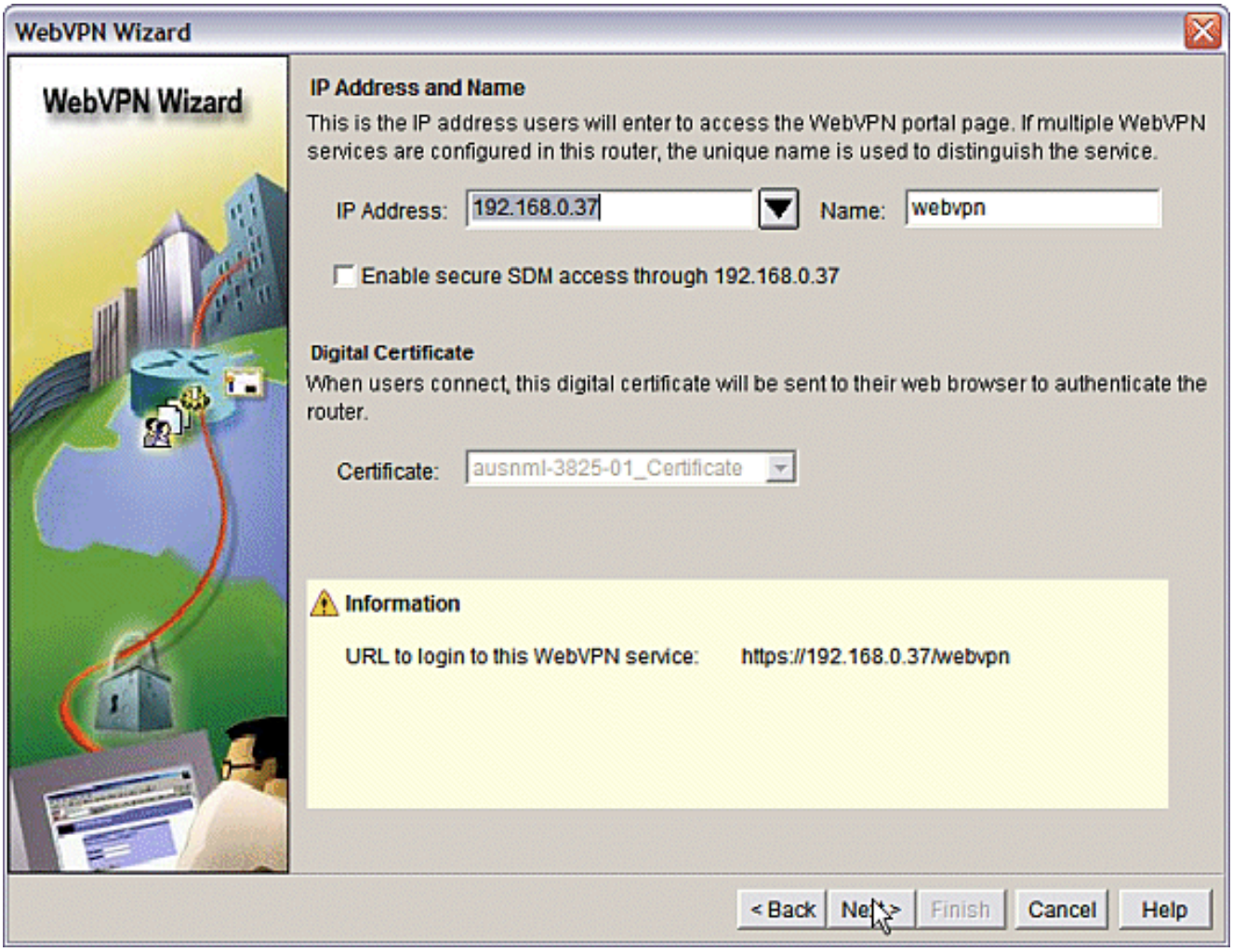
1. Scegliere la scheda **Configura**.Dal pannello di navigazione, scegliere **VPN > WebVPN**.Fare clic sulla scheda **Crea WebVPN**.Fare clic sul pulsante di opzione accanto a **Crea una nuova WebVPN**.Fare clic sul pulsante **Avvia il task selezionato**.



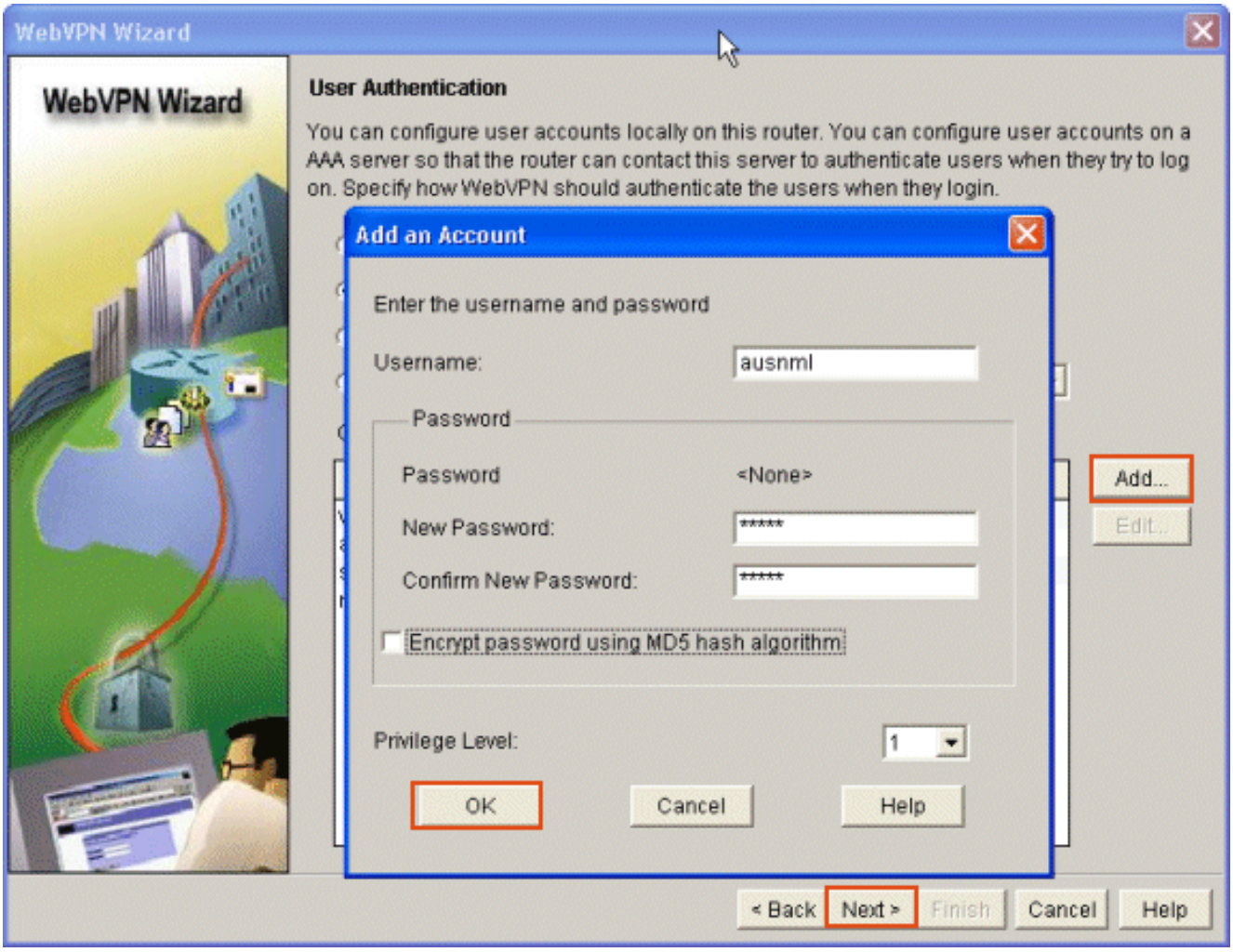
2. Verrà avviata la Creazione guidata WebVPN. Fare clic su **Next** (Avanti).



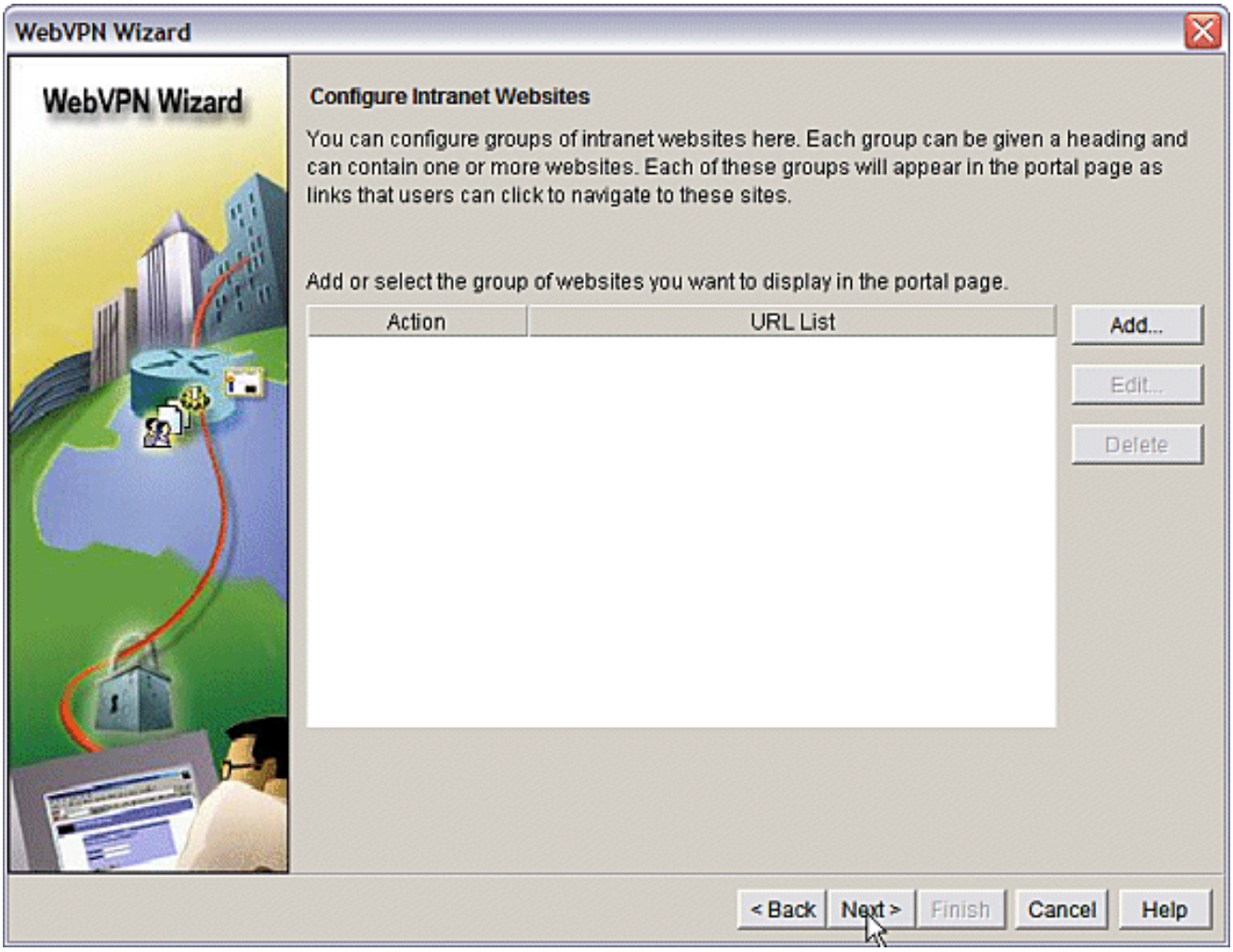
Immettere l'indirizzo IP e un nome univoco per il gateway WebVPN. Fare clic su **Next** (Avanti).



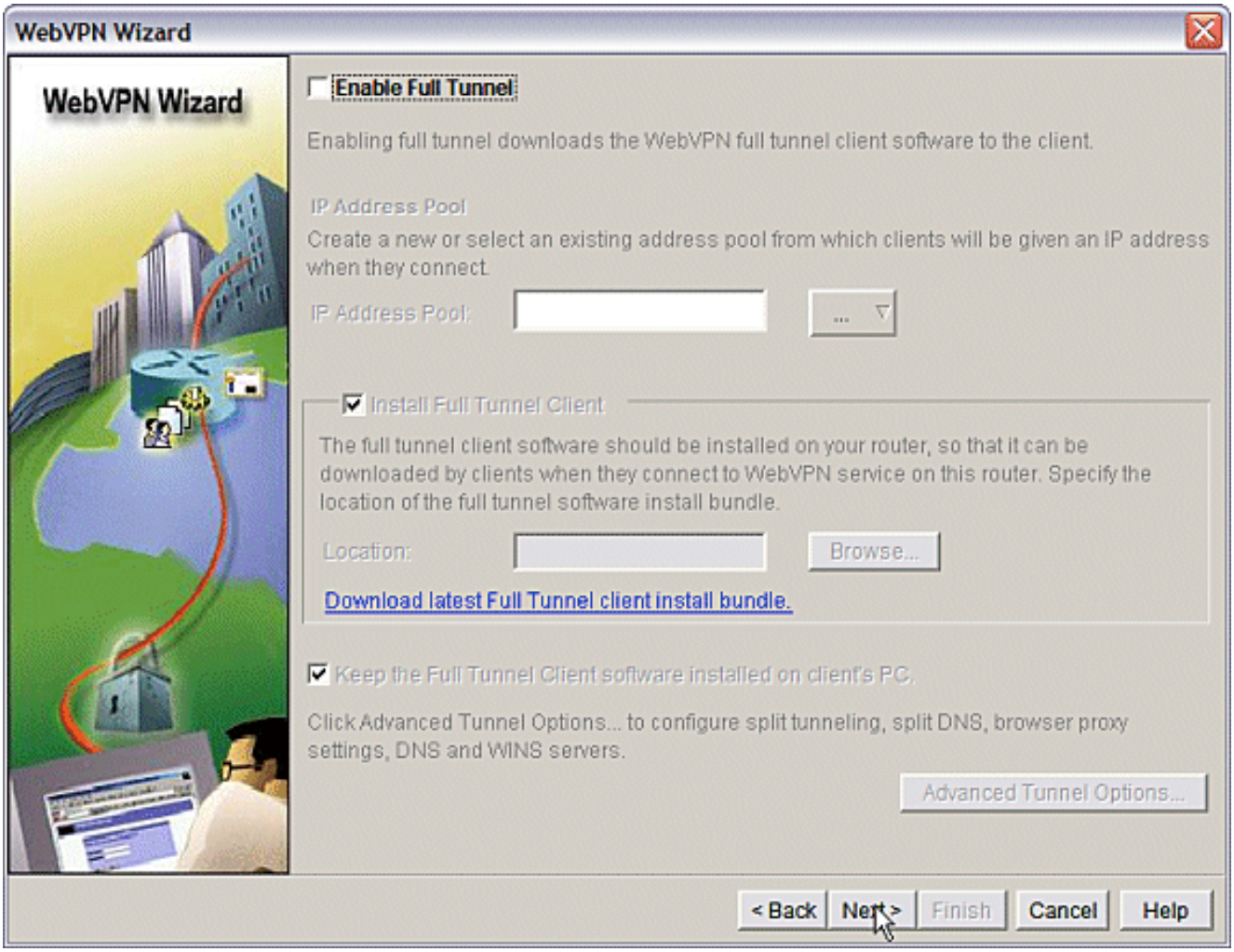
3. La schermata Autenticazione utente consente di fornire l'autenticazione degli utenti. Questa configurazione utilizza un account creato localmente sul router. È inoltre possibile utilizzare un server di autenticazione, autorizzazione e accounting (AAA).Per aggiungere un utente, fare clic su **Aggiungi**.Immettere le informazioni utente nella schermata Aggiungi account e fare clic su **OK**.Fare clic su **Avanti** nella schermata Autenticazione utente.



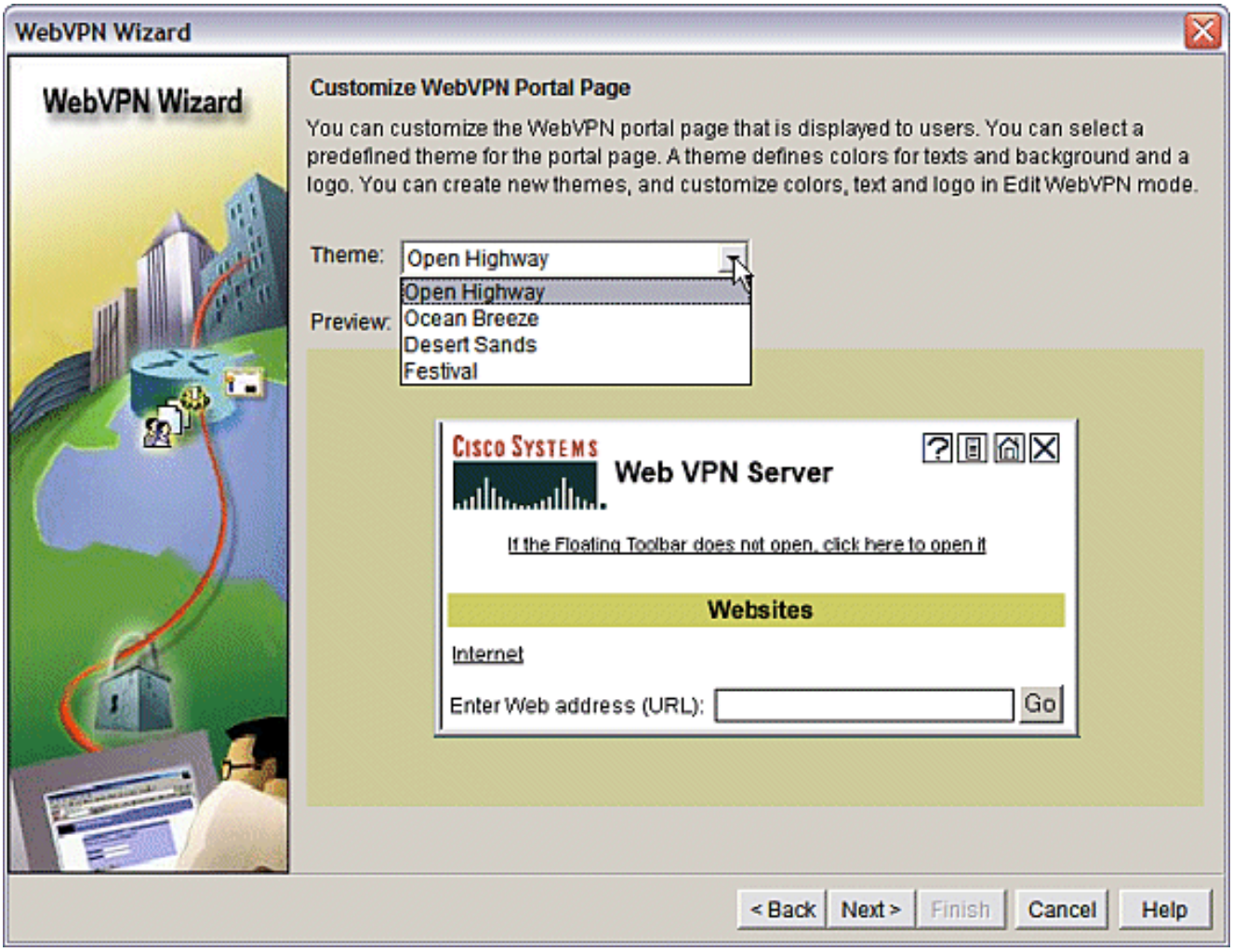
La schermata Creazione guidata WebVPN consente la configurazione dei siti Web Intranet, ma questo passaggio viene omesso perché per l'accesso all'applicazione viene utilizzato l'inoltro porta. Per consentire l'accesso ai siti Web, utilizzare le configurazioni VPN SSL senza client o client completo, che non rientrano nell'ambito di questo documento.



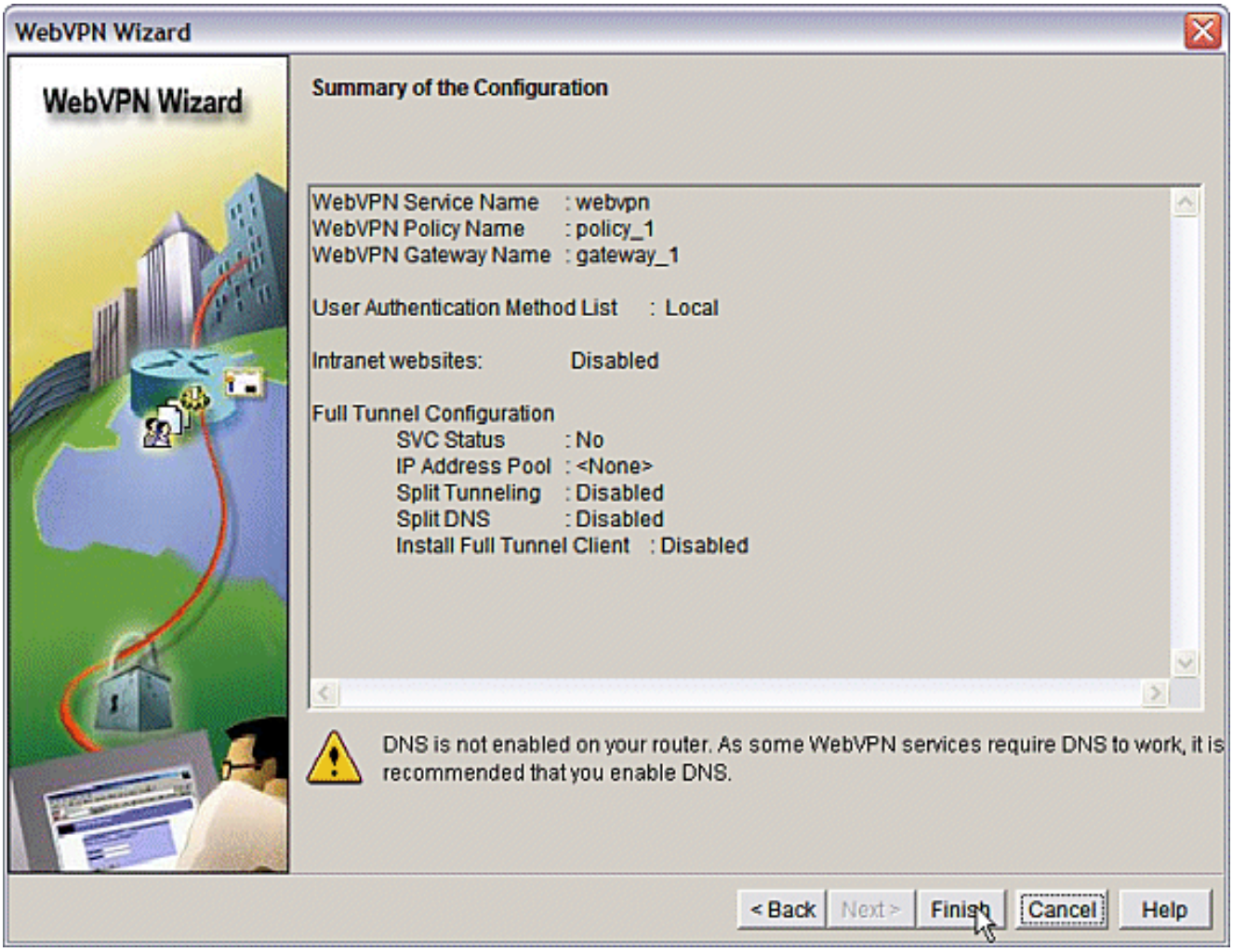
Fare clic su **Next** (Avanti). Verrà visualizzata una schermata che consente di configurare il client del tunnel completo. Ciò non si applica alla VPN SSL thin-client (Port Forwarding).Deselezionare **Abilita tunnel completo**. Fare clic su **Next** (Avanti).



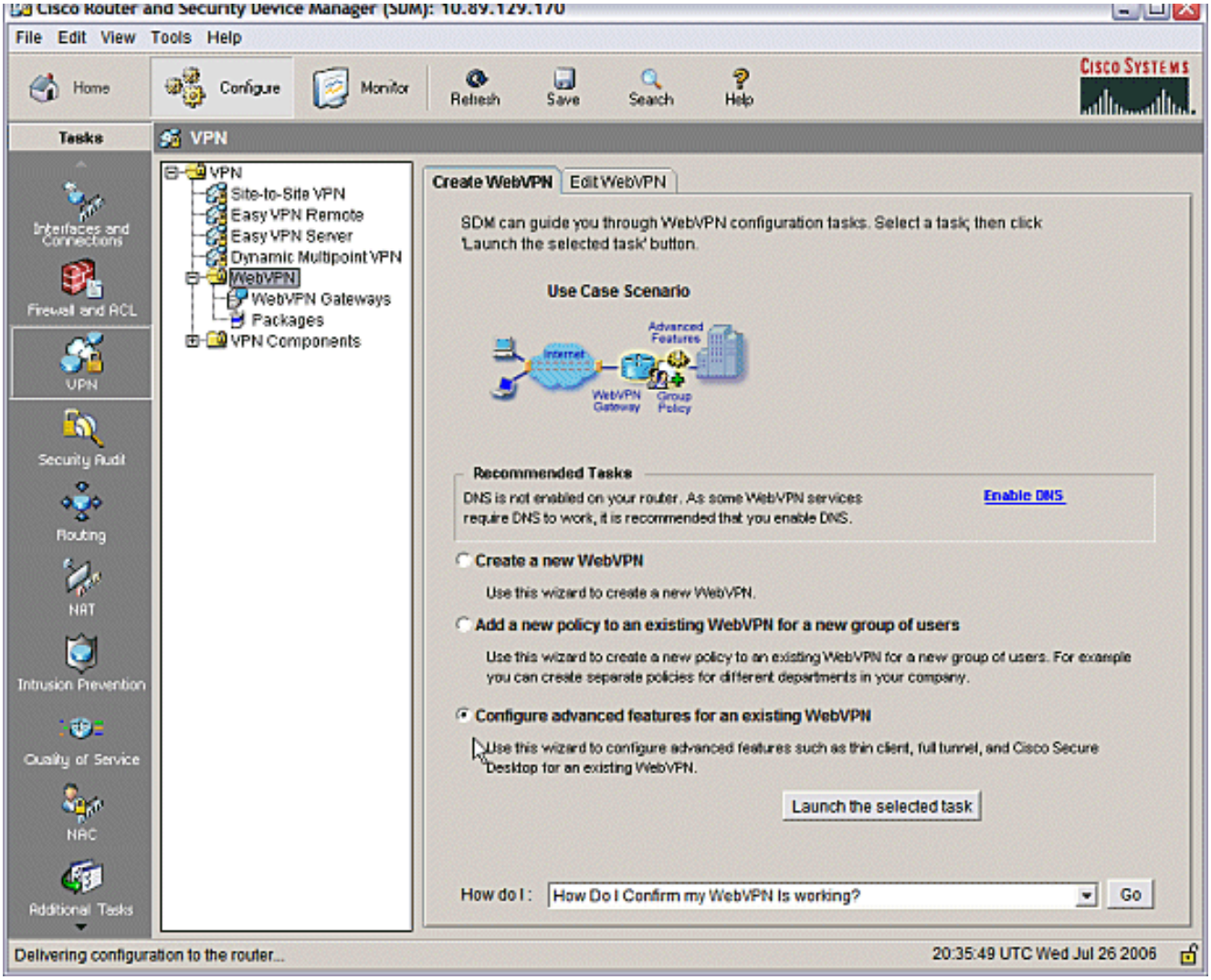
4. Consente di personalizzare l'aspetto della pagina del portale WebVPN o di accettare quello predefinito.Fare clic su **Next**
(Avanti).



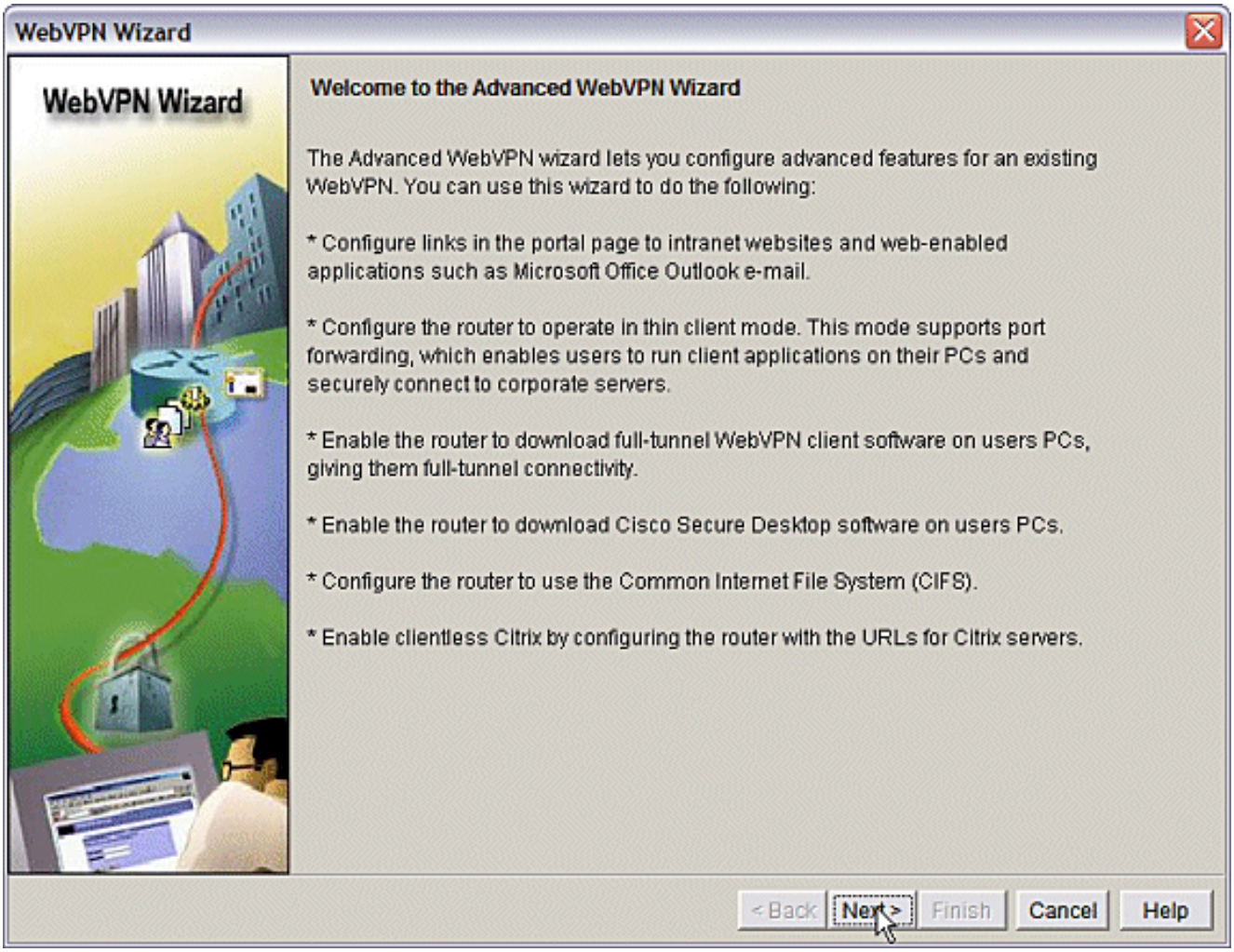
Visualizzare in anteprima il riepilogo della configurazione e fare clic su **Fine > Salva**.



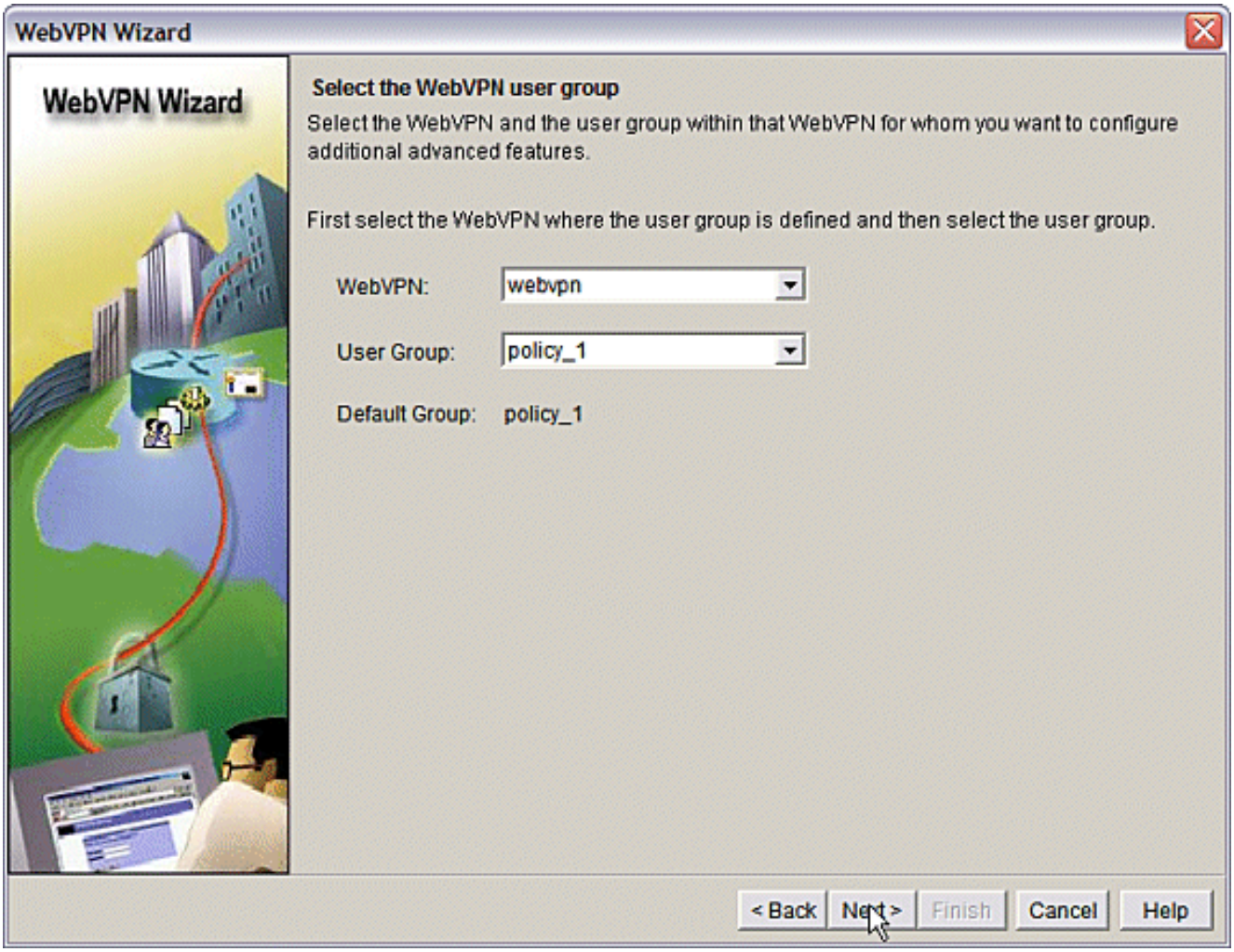
5. Sono stati creati un gateway WebVPN e un contesto WebVPN con Criteri di gruppo collegati. Configurare le porte thin-client, che vengono rese disponibili quando i client si connettono a WebVPN.Scegliere **Configura**.Scegliete **VPN > WebVPN**.Scegliere **Crea WebVPN**.Scegliere il pulsante di opzione **Configura funzionalità avanzate per una WebVPN esistente** e fare clic su **Avvia l'attività selezionata**.



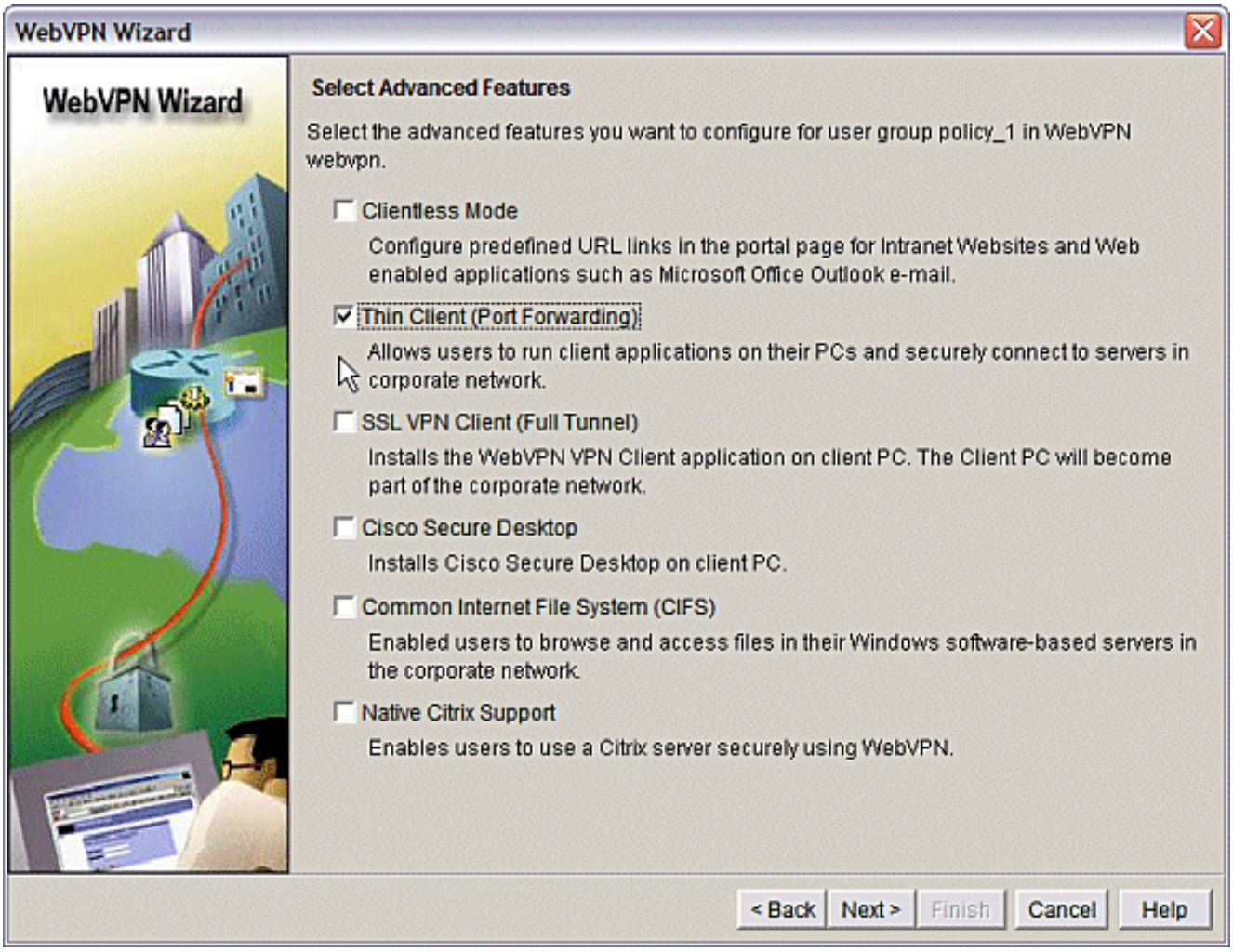
Nella schermata iniziale vengono evidenziate le funzionalità della procedura guidata. Fare clic su **Next**
(Avanti).



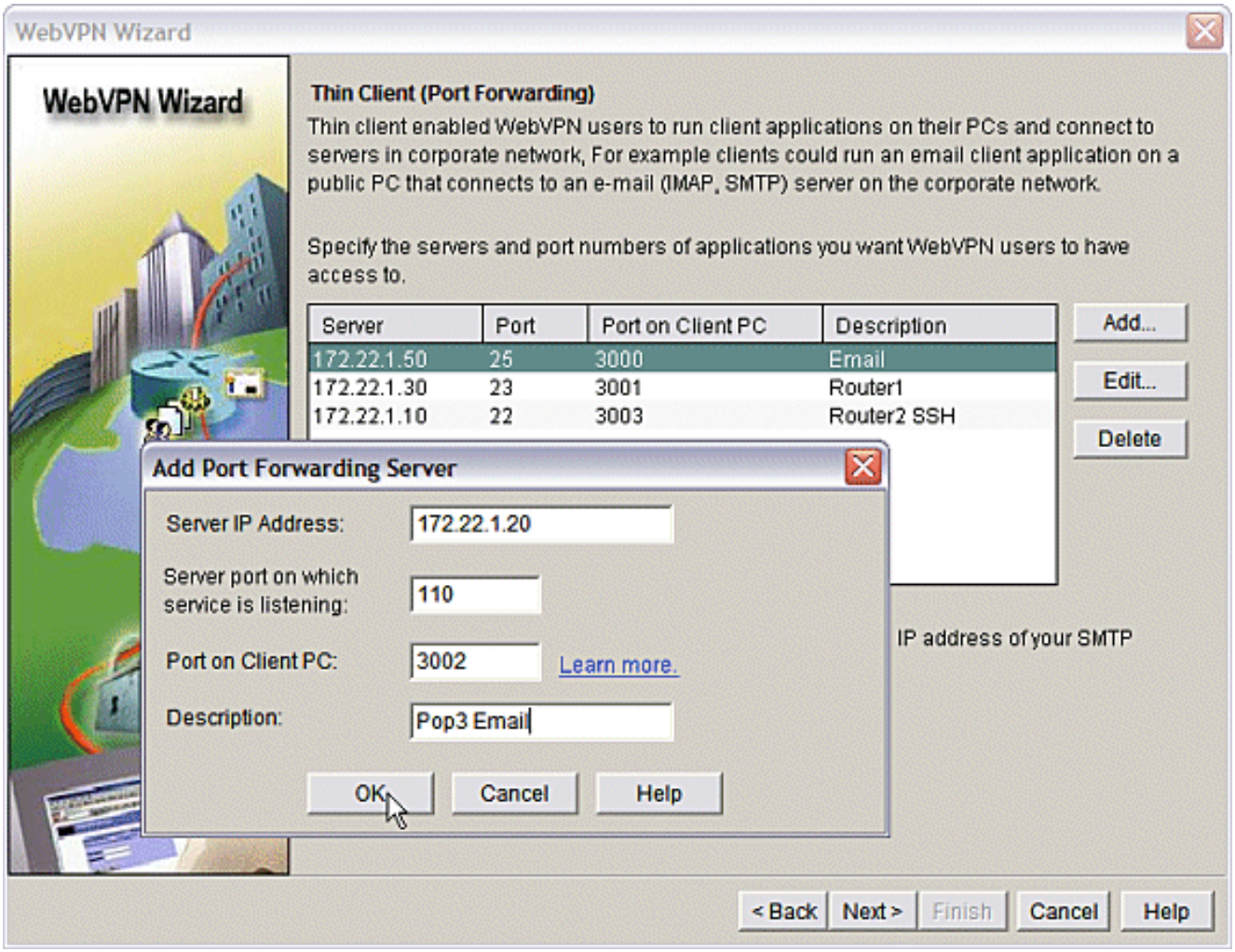
Scegliere il contesto WebVPN e il gruppo di utenti dai menu a discesa. Fare clic su **Next** (Avanti).



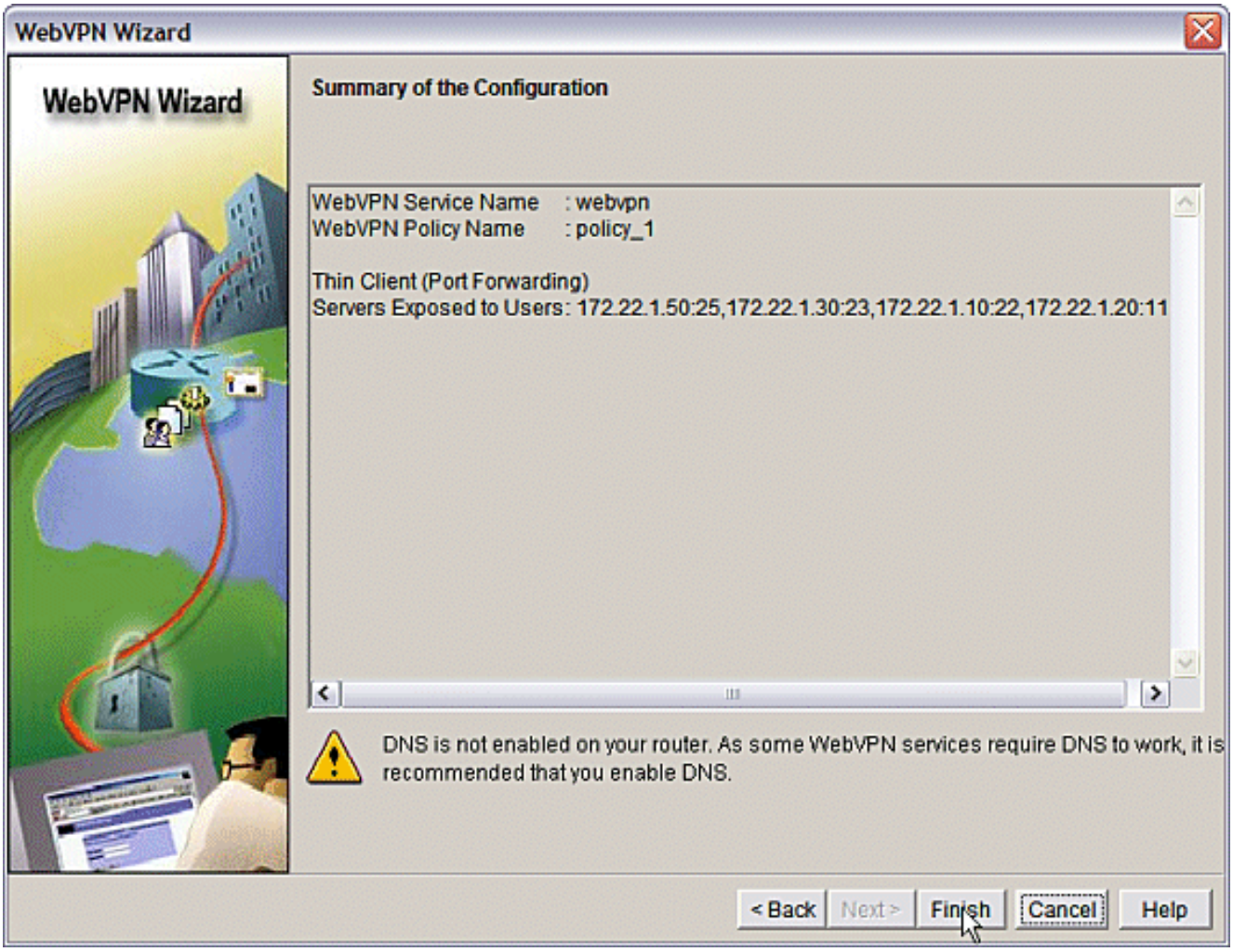
Selezionare **Thin Client (Port Forwarding)** e fare clic su **Avanti**.



Immettere le risorse che si desidera rendere disponibili tramite Inoltro porta. La porta del servizio deve essere una porta statica, ma è possibile accettare la porta predefinita sul PC client assegnato dalla procedura guidata. Fare clic su **Next** (Avanti).



Visualizzare in anteprima il riepilogo della configurazione e fare clic su **Fine > OK > Salva**.



Configurazione

Risultati della configurazione SDM.

ausnml-3825-01

```
Building configuration...

Current configuration : 4343 bytes
!
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
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
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
```

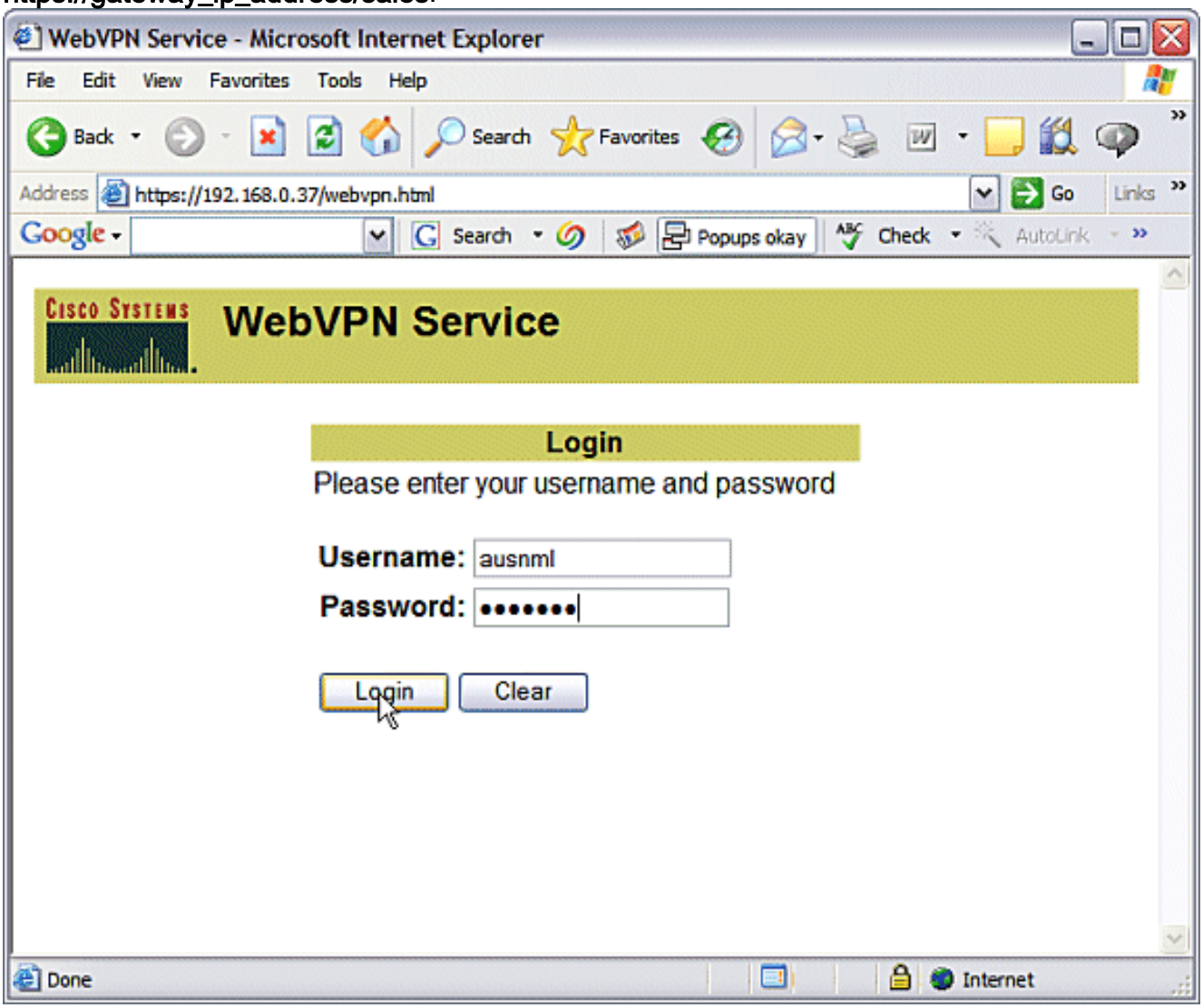
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !---------------------- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! 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 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```

Verifica

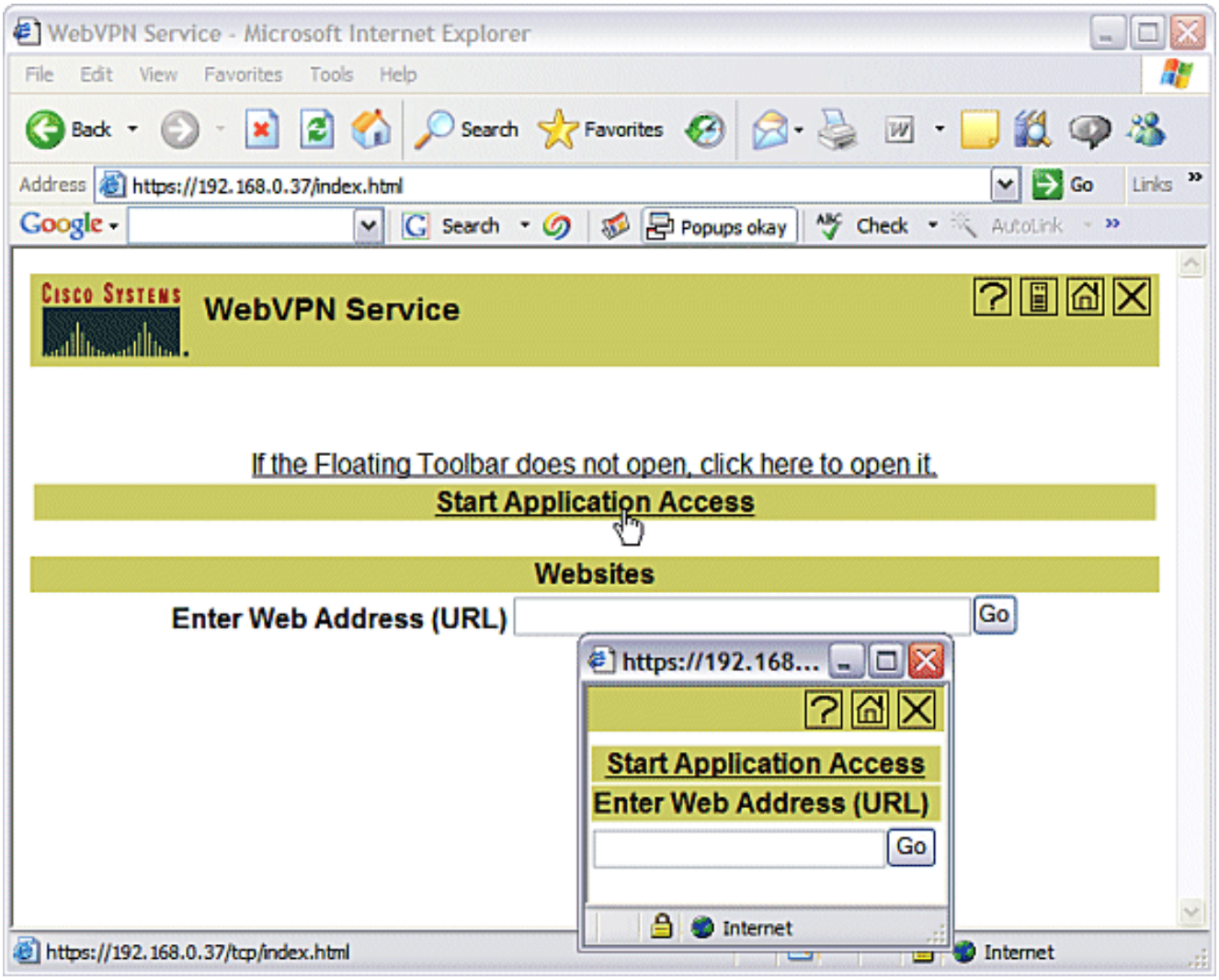
Verifica della configurazione

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

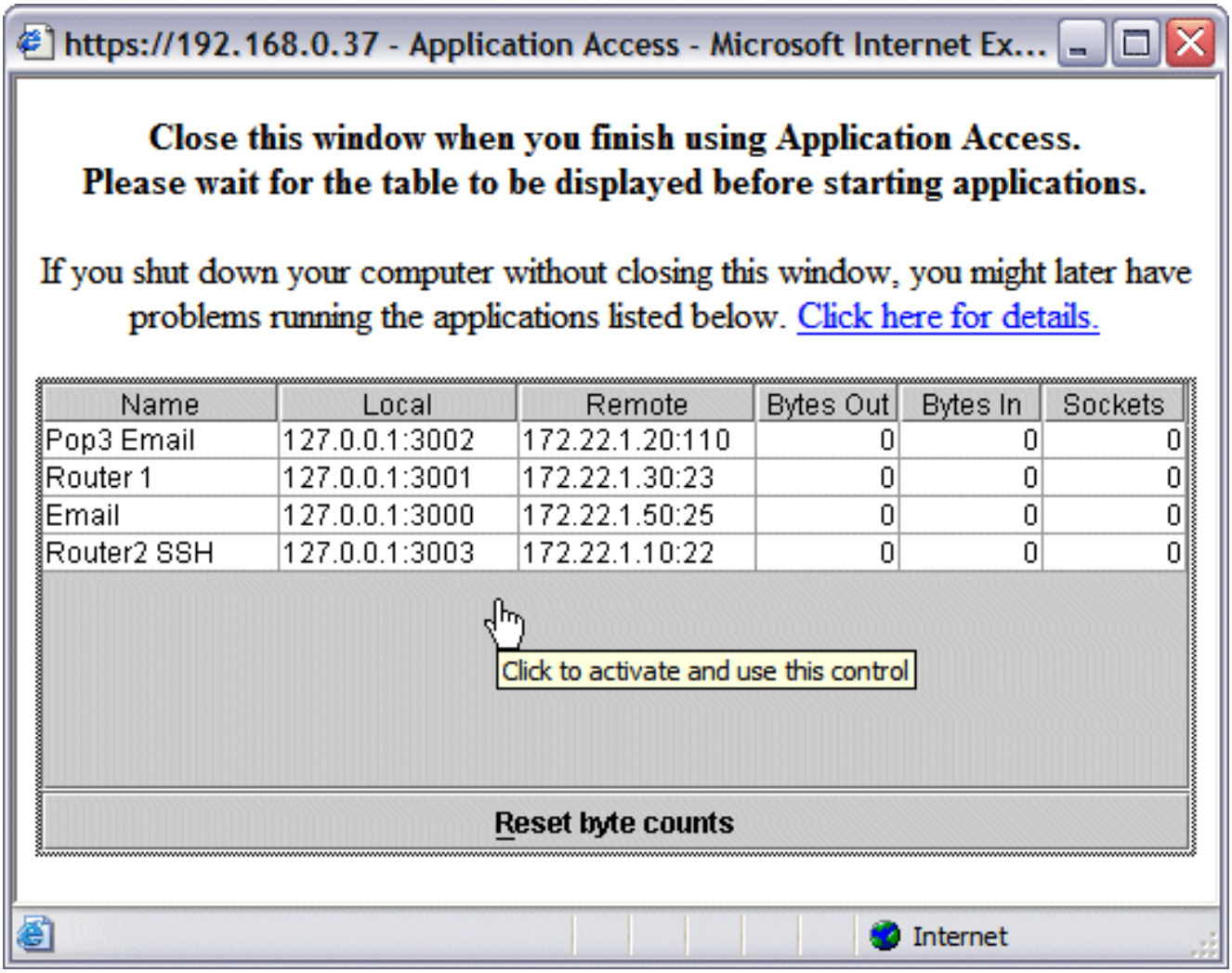
1. Utilizzare un computer client per accedere al gateway WebVPN all'indirizzo **https://gateway_ip_address.** Ricordarsi di includere il nome di dominio WebVPN se si creano contesti WebVPN univoci. Ad esempio, se è stato creato un dominio denominato sales, immettere **https://gateway_ip_address/sales**.



2. Accedere e accettare il certificato offerto dal gateway WebVPN. Fare clic su **Avvia accesso applicazione**.



3. Viene visualizzata la schermata Accesso applicazione. È possibile accedere a un'applicazione con il numero di porta locale e l'indirizzo IP di loopback locale. Ad esempio, per Telnet su Router 1, immettere **telnet 127.0.0.1 3001**. La piccola applet Java invia queste informazioni al gateway WebVPN, che quindi collega le due estremità della sessione in modo sicuro. Se le connessioni riescono, le colonne **Byte in uscita** e **Byte in ingresso** potrebbero aumentare.



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 ulteriori informazioni sull'utilizzo dei comandi **show**, consultare il documento sulla verifica della configurazione di WebVPN.

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.

I computer client devono essere caricati con SUN Java versione 1.4 o successive. Ottieni una copia di questo software da Java Software Download

Comandi utilizzati per la risoluzione dei problemi

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

- **show webvpn ?**—Sono disponibili molti comandi **show** associati a WebVPN. Queste

operazioni possono essere eseguite dalla CLI per visualizzare le statistiche e altre informazioni. Per ulteriori informazioni sull'utilizzo dei comandi **show**, consultare il documento sulla verifica della configurazione WebVPN.

- **debug webvpn ?**: l'uso dei comandi di **debug** può influire negativamente sul router. Per ulteriori informazioni sull'uso dei comandi di **debug**, consultare il documento sull'uso dei comandi di debug di WebVPN.

Informazioni correlate

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Domande e risposte su Cisco IOS WebVPN
- Documentazione e supporto tecnico – Cisco Systems