Esempio di configurazione professionale di un router IOS come server VPN facile

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Componenti usati](#)
[Installa Cisco CP](#)
[Configurazione del router per eseguire Cisco CP](#)
[Requisiti](#)
[Convenzioni](#)
[Configurazione](#)
[Esempio di rete](#)
[Cisco CP - Configurazione facile del server VPN](#)
[Configurazione CLI](#)
[Verifica](#)
[Easy VPN Server - Comandi show](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare un router Cisco IOS® come server Easy VPN (EzVPN) con Cisco Configuration Professional (Cisco CP) e la CLI. La funzionalità Easy VPN Server consente a un utente finale remoto di comunicare utilizzando IP Security (IPsec) con qualsiasi gateway VPN (Virtual Private Network) di Cisco IOS. I criteri IPSec gestiti centralmente vengono "spinti" sul dispositivo client dal server, riducendo al minimo la configurazione da parte dell'utente finale.

Per ulteriori informazioni su Easy VPN Server, fare riferimento alla sezione Easy VPN Server della libreria della guida alla configurazione della connettività sicura, Cisco IOS versione 12.4T.

Prerequisiti

Componenti usati

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

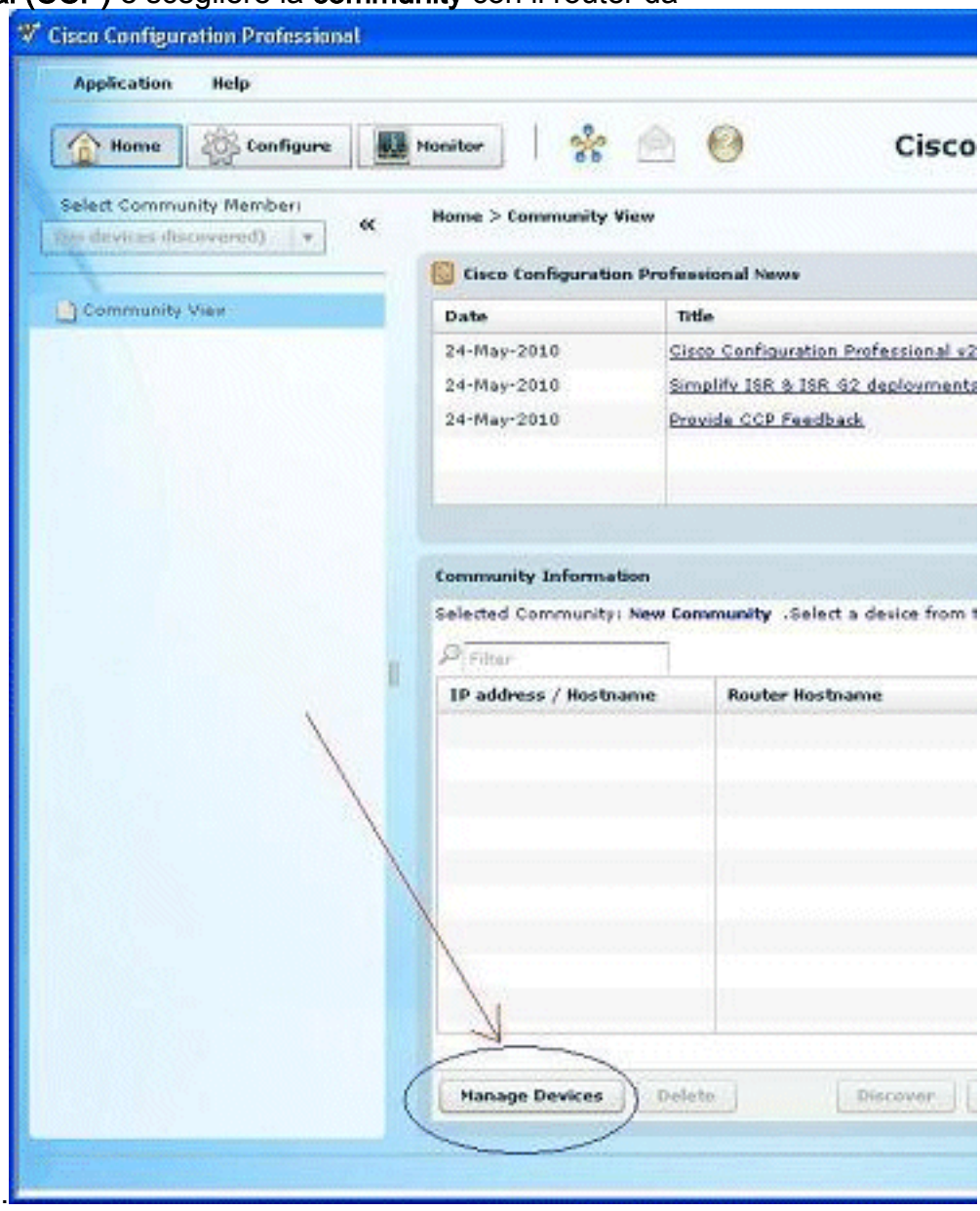
- Cisco 1841 Router con software Cisco IOS versione 12.4(15T)
- Cisco CP versione 2.1

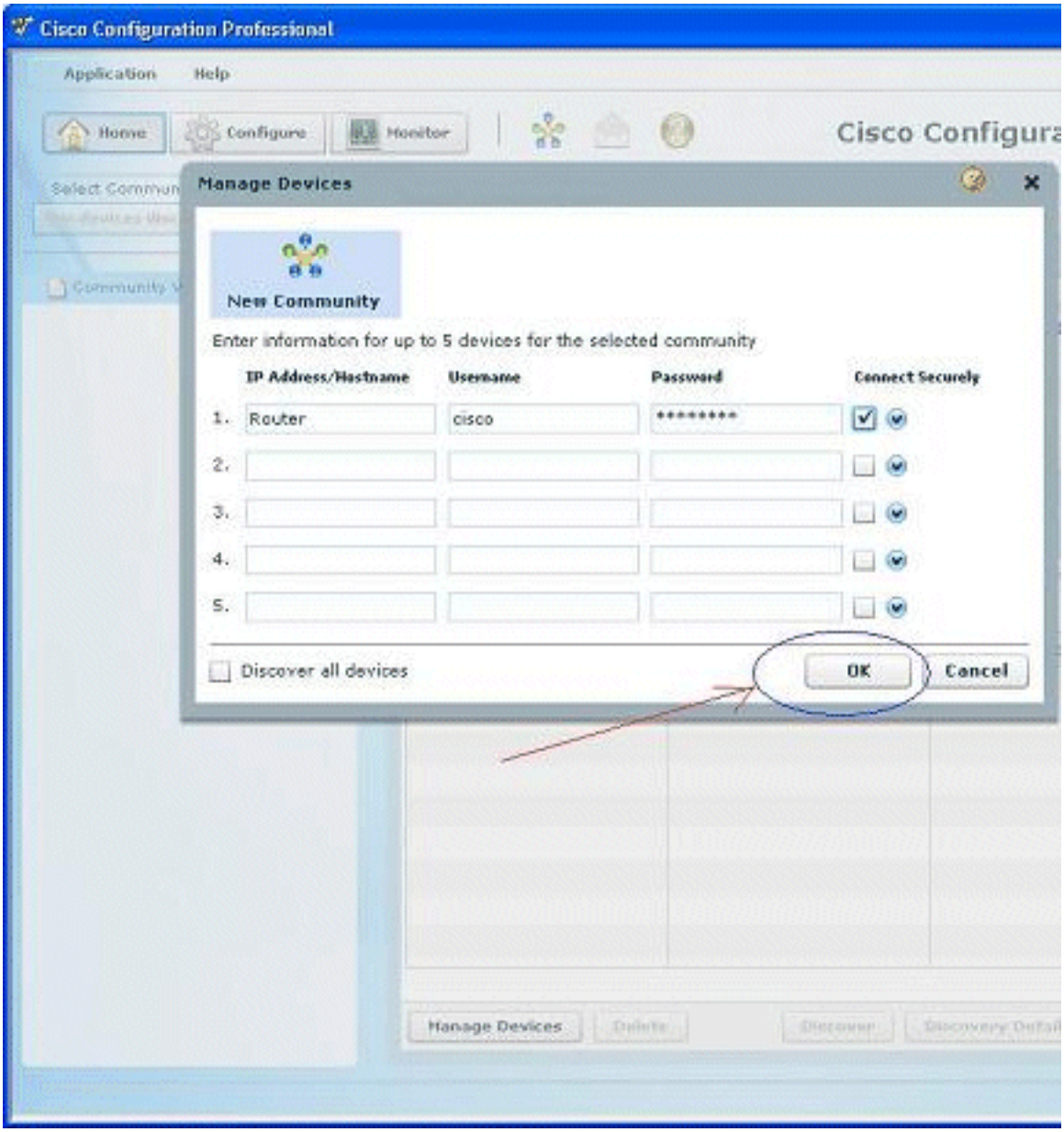
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Installa Cisco CP

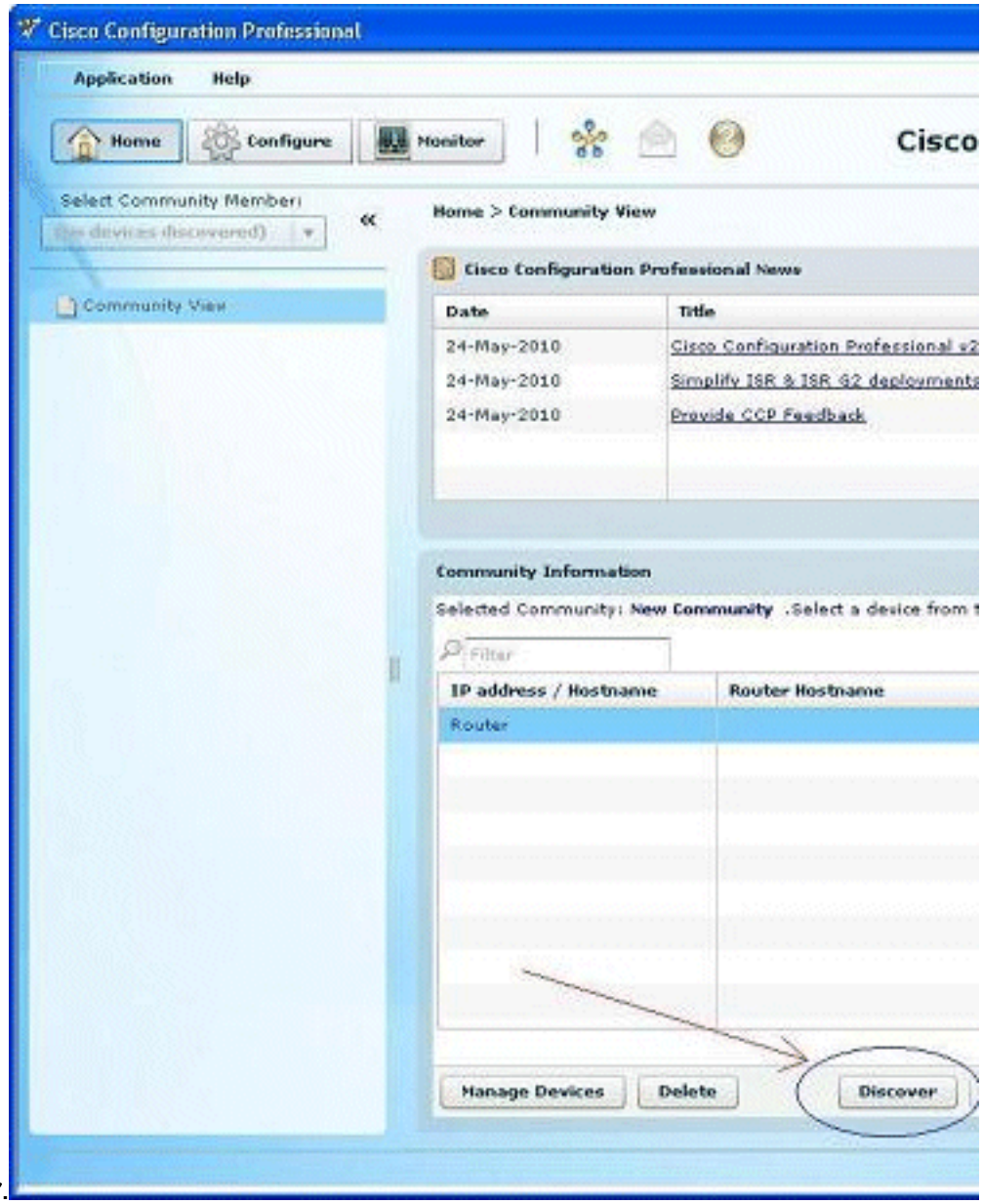
Per installare Cisco CP, attenersi alla seguente procedura:

1. Scaricare Cisco CP V2.1 da Cisco Software Center (solo utenti registrati) e installarlo sul PC locale.L'ultima versione di Cisco CP è disponibile sul sito Web di Cisco CP.
2. Avviare Cisco CP dal PC locale tramite **Start > Programmi > Cisco Configuration Professional (CCP)** e scegliere la **community** con il router da configurare.





3. Per individuare il dispositivo che si desidera configurare, evidenziare il router e fare clic su

Discover. 

Nota: per informazioni sui modelli di router Cisco e sulle versioni IOS compatibili con Cisco CP v2.1, fare riferimento alla sezione Versioni Cisco IOS compatibili.

Nota: per informazioni sui requisiti del PC con Cisco CP v2.1, fare riferimento alla sezione Requisiti di sistema.

Configurazione del router per eseguire Cisco CP

Per eseguire Cisco CP su un router Cisco, eseguire la configurazione seguente:

1. Collegarsi al router in modalità Telnet, SSH o tramite la console.Immettere la modalità di configurazione globale utilizzando questo comando:
   ```
   Router(config)#enable
   Router(config)#
   ```
2. Se HTTP e HTTPS sono abilitati e configurati per l'utilizzo di numeri di porta non standard, è possibile ignorare questo passaggio e utilizzare semplicemente il numero di porta già configurato.Abilitare il server HTTP o HTTPS del router utilizzando i seguenti comandi del software Cisco IOS:
   ```
   Router(config)# ip http server
   Router(config)# ip http secure-server
   Router(config)# ip http authentication local
   ```

3. Creare un utente con livello di privilegio 15:
```
Router(config)# username privilege 15 password 0
```

   Nota: sostituire *<nomeutente>* e *<password>* con il nome utente e la password che si desidera configurare.
4. Configurare SSH e Telnet per l'accesso locale e il livello di privilegio 15.
```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

5. (Facoltativo) Abilitare la registrazione locale per supportare la funzione di monitoraggio del registro:
```
Router(config)# logging buffered 51200 warning
```

Requisiti

In questo documento si presume che il router Cisco sia completamente operativo e configurato per consentire a Cisco CP di apportare modifiche alla configurazione.

Per informazioni complete su come iniziare a utilizzare Cisco CP, fare riferimento a Guida introduttiva a Cisco Configuration Professional.

Convenzioni

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

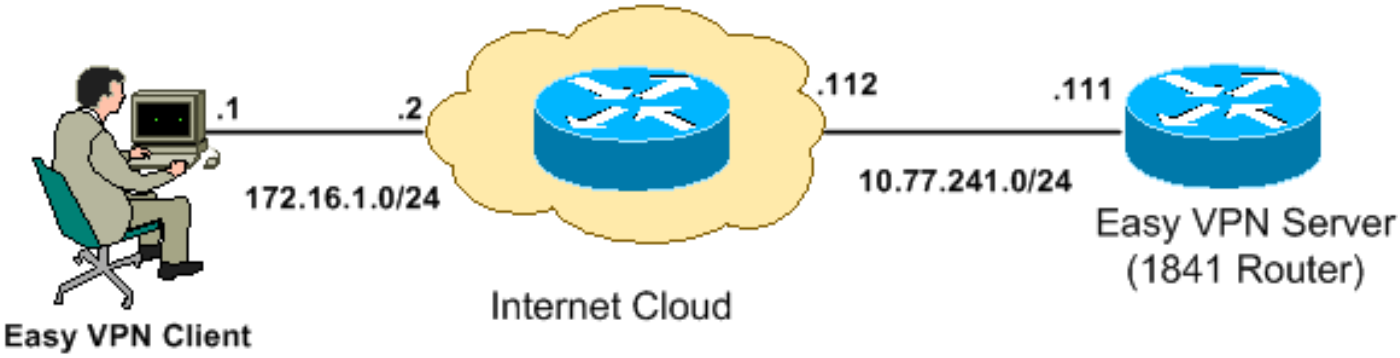
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le impostazioni di base di un router in una rete.

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:

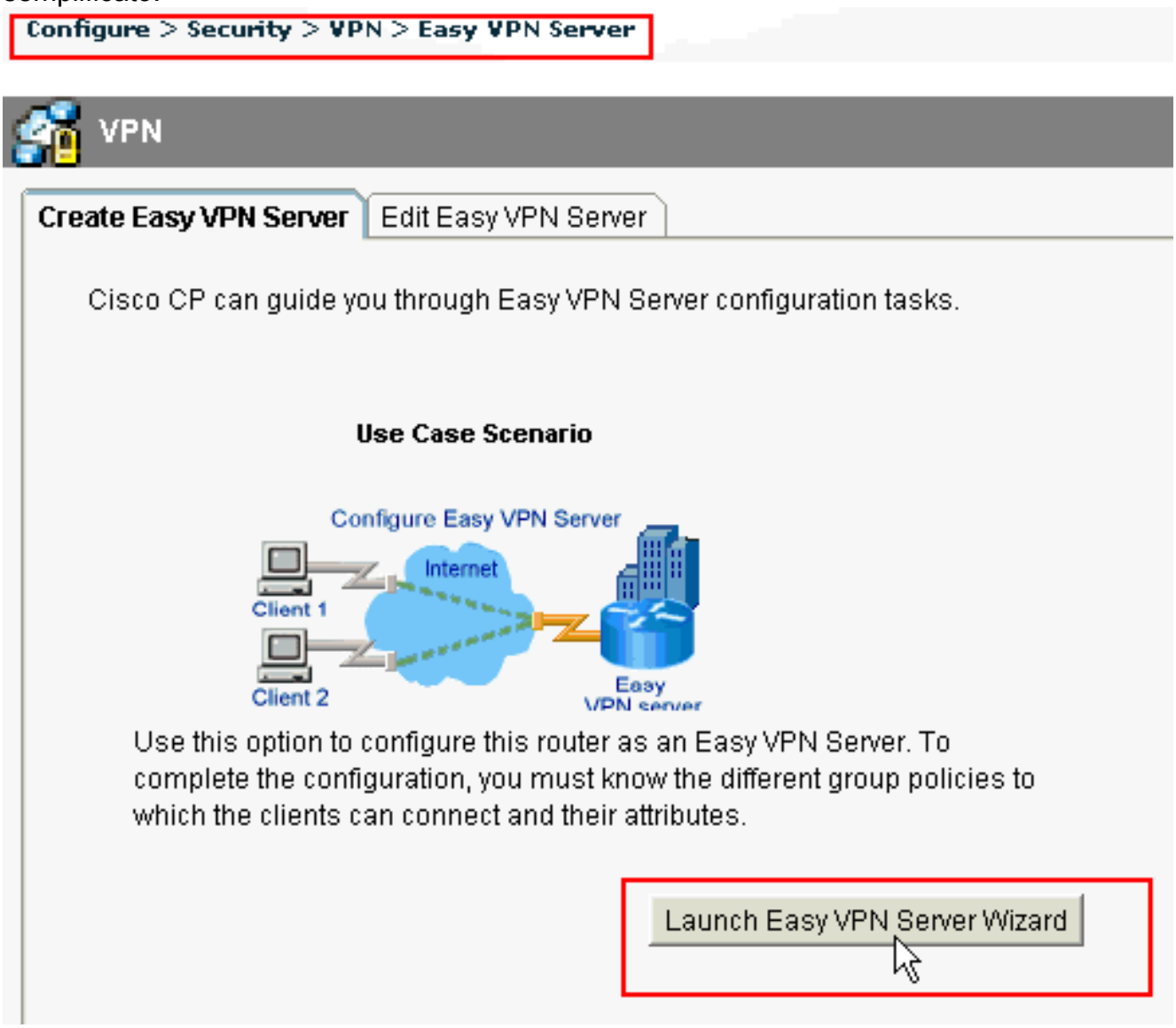


Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Cisco CP - Configurazione facile del server VPN

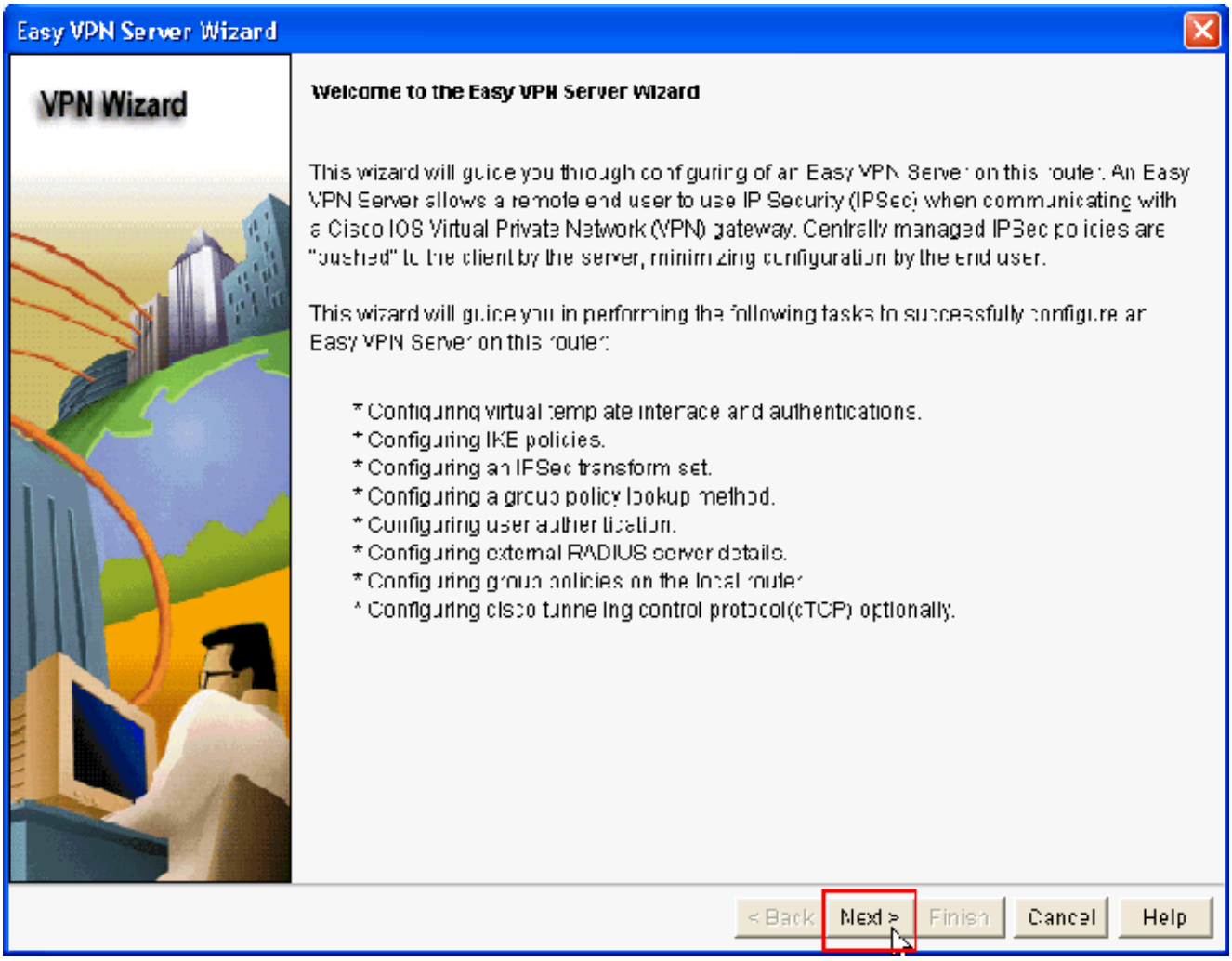
Per configurare il router Cisco IOS come server Easy VPN, eseguire la procedura seguente:

1. Scegliere Configura > Sicurezza > VPN > **Server VPN semplificato** > **Crea server VPN semplificato** e fare clic su **Avvia procedura guidata server VPN semplificato** per configurare il router Cisco IOS come server VPN semplificato:

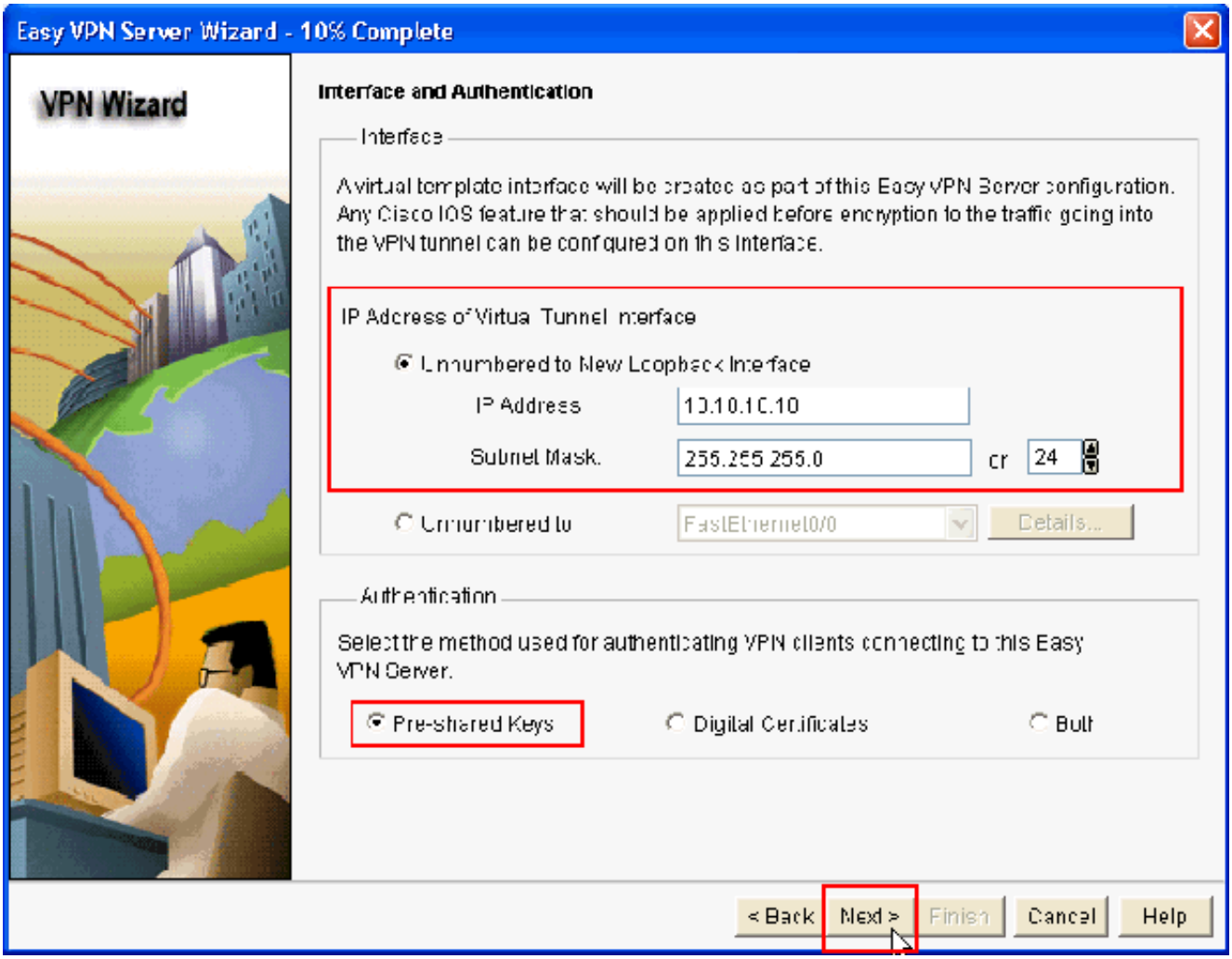


2. Fare clic su **Next** (Avanti) per procedere con la configurazione di **Easy VPN**

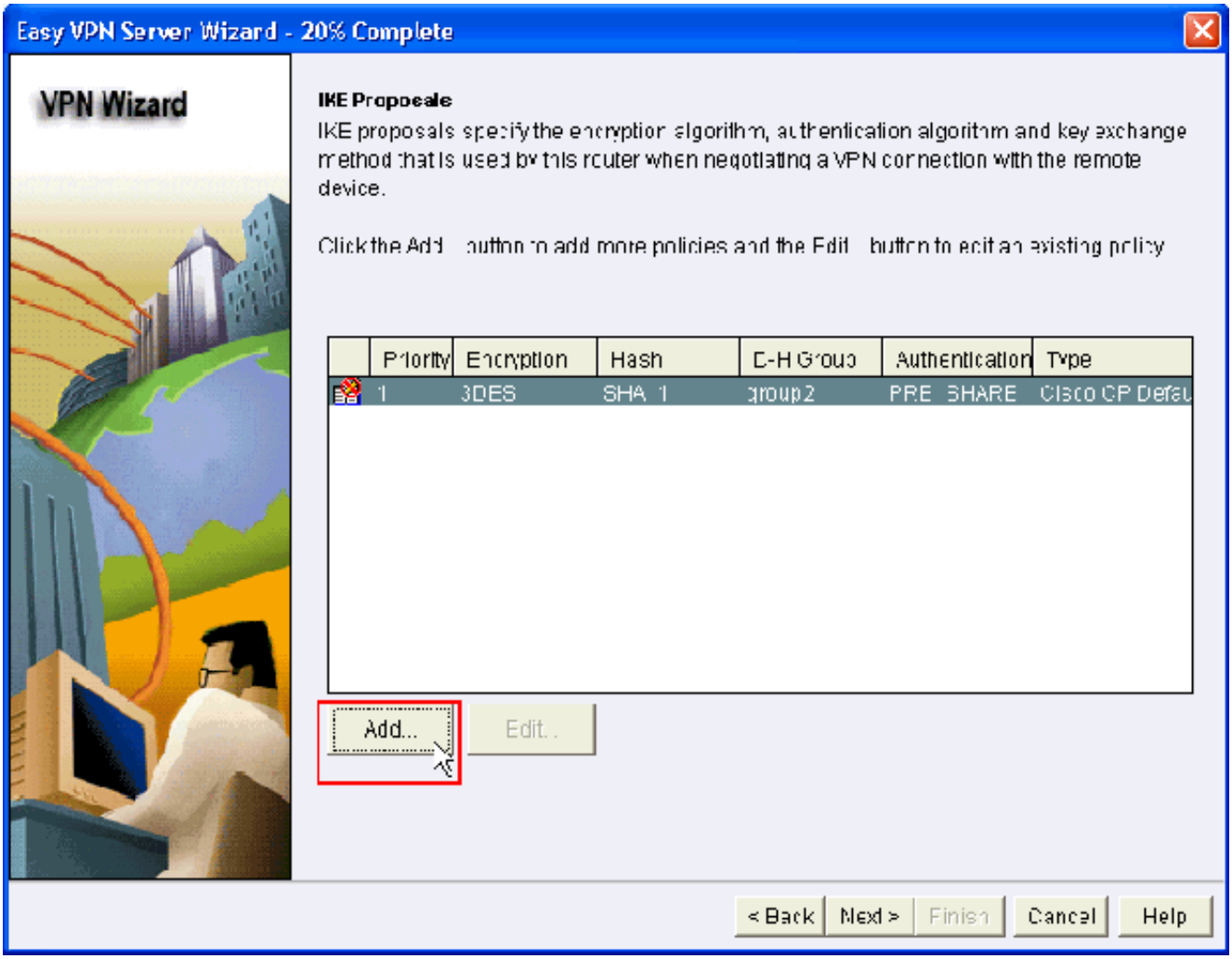
Server.



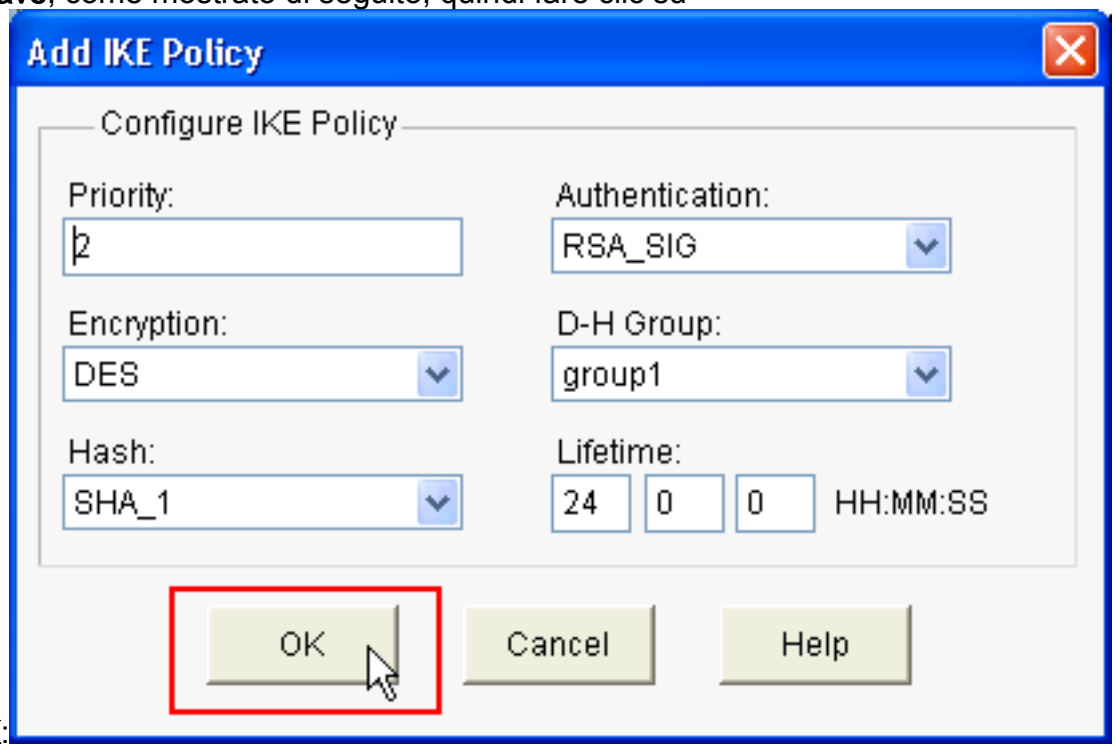
3. Nella finestra risultante, un'**interfaccia virtuale** verrà configurata come parte della configurazione di Easy VPN Server. Specificare l'**indirizzo IP dell'interfaccia del tunnel virtuale** e scegliere anche il **metodo di autenticazione** utilizzato per autenticare i client VPN. In questo caso, **Chiavi già condivise** è il metodo di autenticazione utilizzato. Fare clic su **Avanti**:



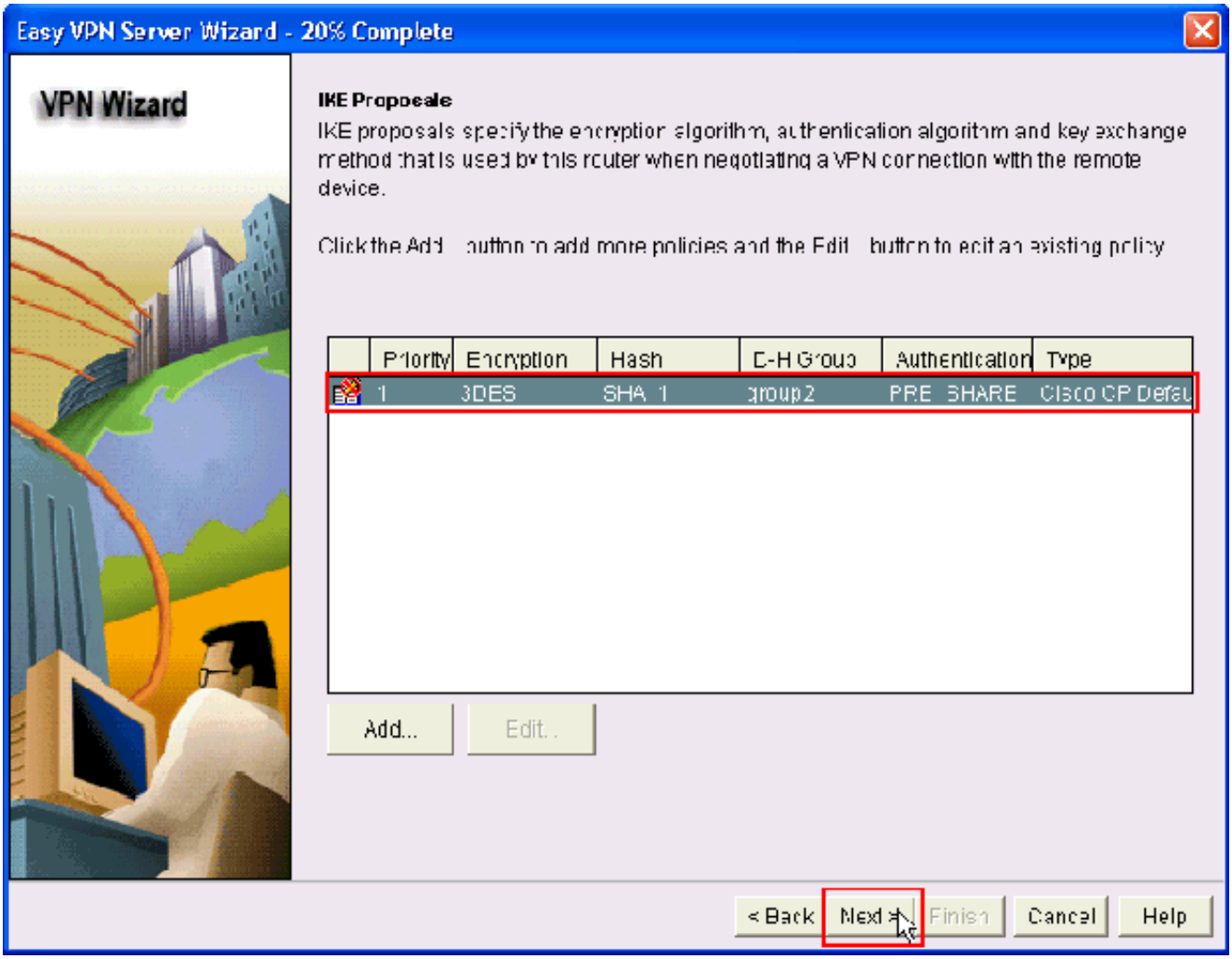
4. Specificare l'**algoritmo di crittografia, l'algoritmo di autenticazione e il metodo di scambio chiavi** che il router deve utilizzare durante la negoziazione con il dispositivo remoto. Sul router è presente un criterio IKE predefinito che può essere utilizzato se necessario. Per aggiungere un nuovo criterio IKE, fare clic su
Aggiungi.



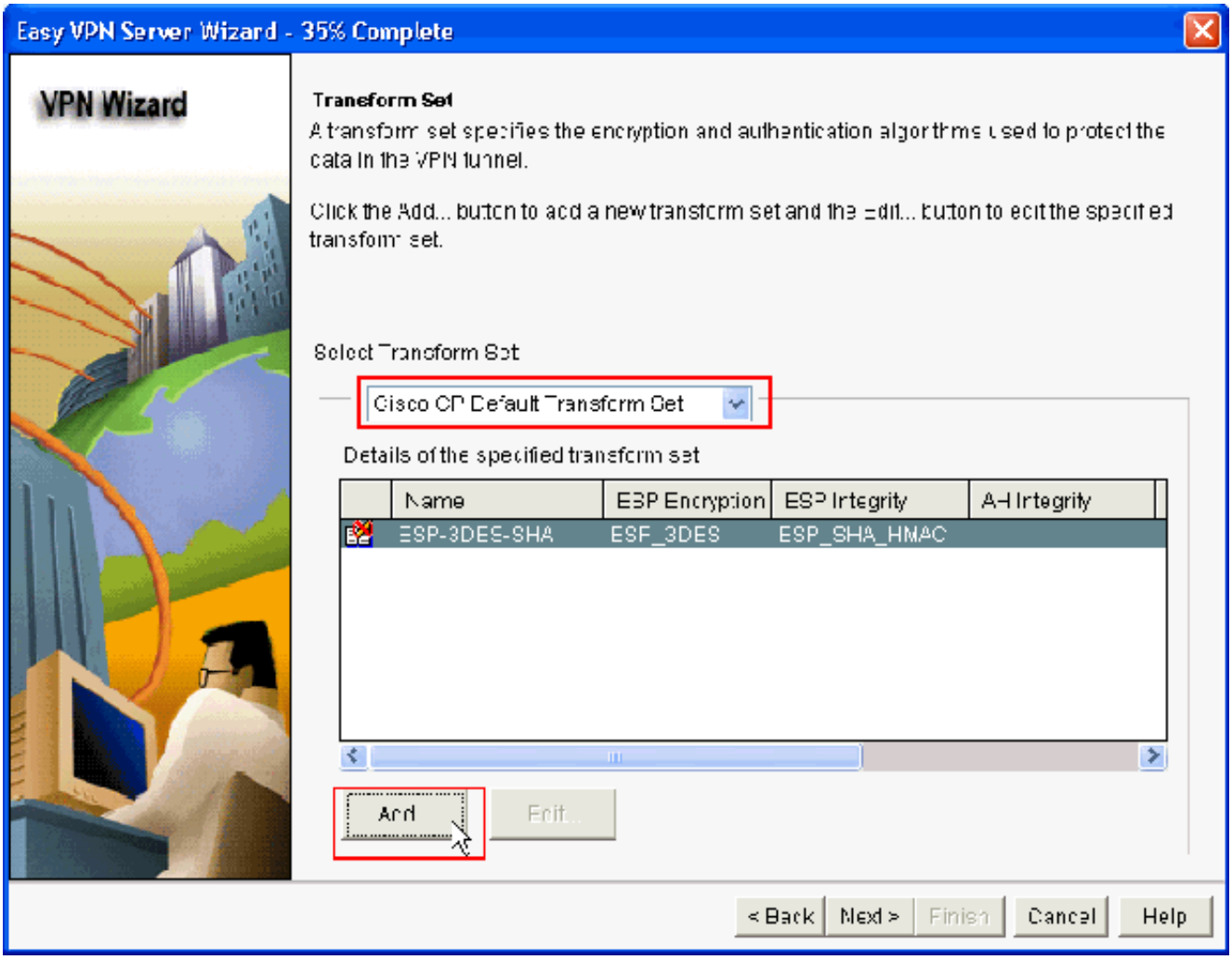
5. Specificare **Algoritmo di crittografia**, **Algoritmo di autenticazione** e il **metodo di scambio chiave**, come mostrato di seguito, quindi fare clic su **OK**:



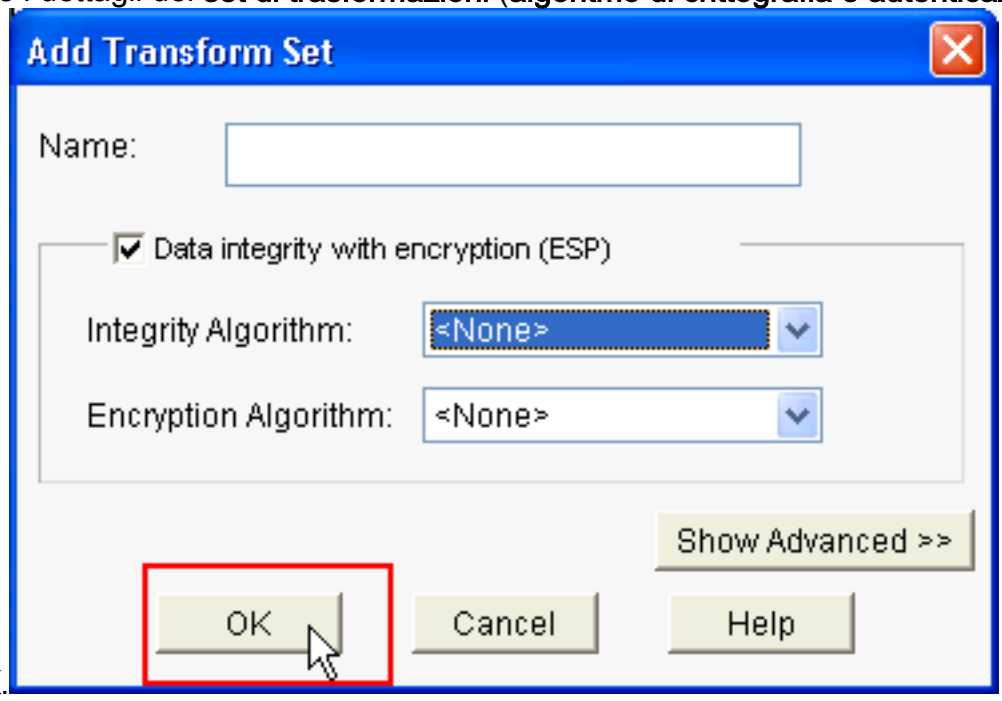
6. Nell'esempio viene utilizzato il **criterio IKE predefinito**. Di conseguenza, scegliere il criterio IKE predefinito e fare clic su **Avanti**.



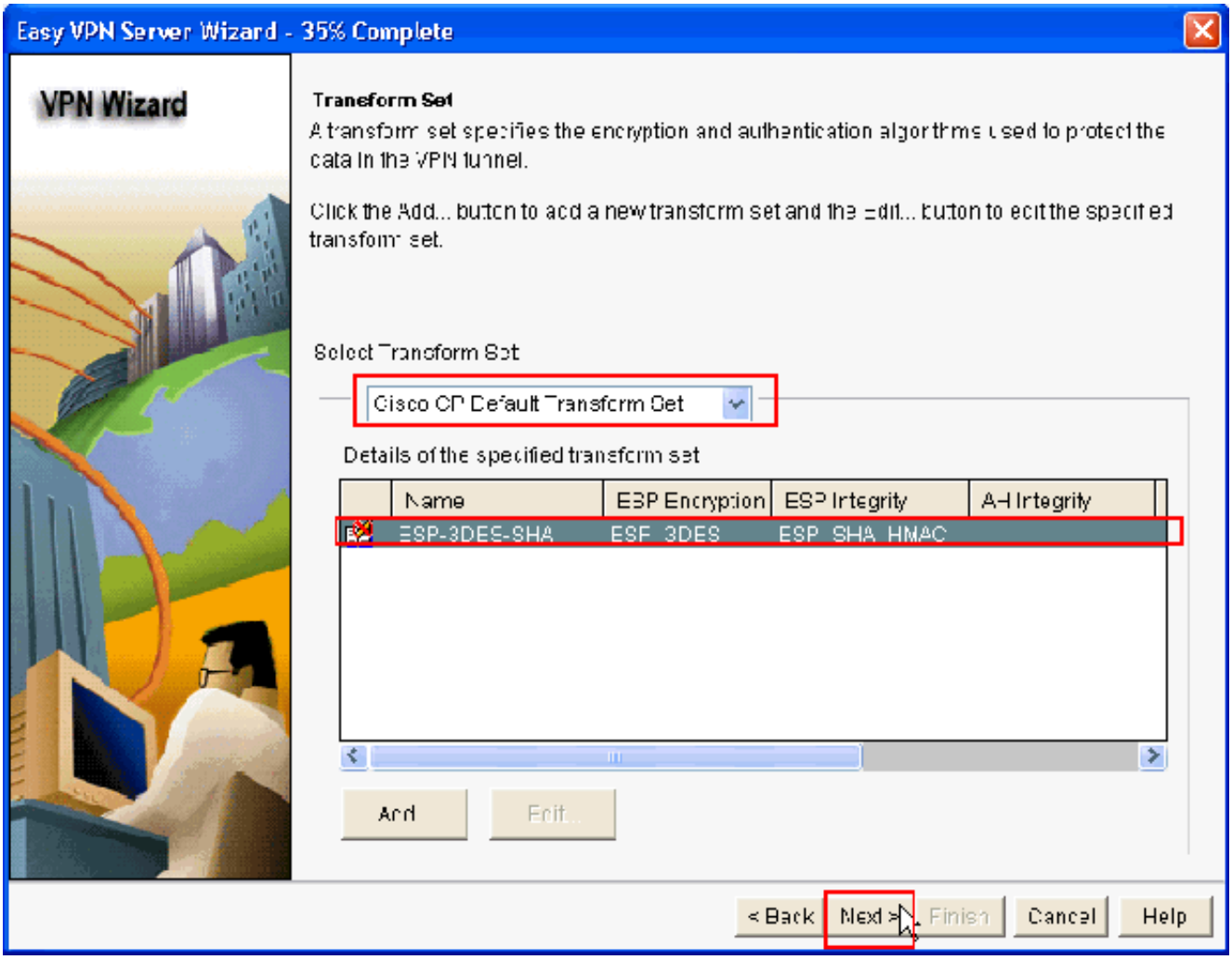
7. Nella nuova finestra dovrebbero essere forniti i dettagli **Set di trasformazioni**. Il set di trasformazioni specifica gli algoritmi di **crittografia** e **autenticazione** utilizzati per proteggere **i dati nel tunnel VPN**. Fare clic su **Add** (Aggiungi) per fornire questi dettagli. Quando si fa clic su **Aggiungi** e si forniscono i dettagli desiderati, è possibile aggiungere un numero qualsiasi di set di trasformazioni.**Nota: CP Default Transform Set** è presente per impostazione predefinita sul router quando è configurato con **Cisco CP**.



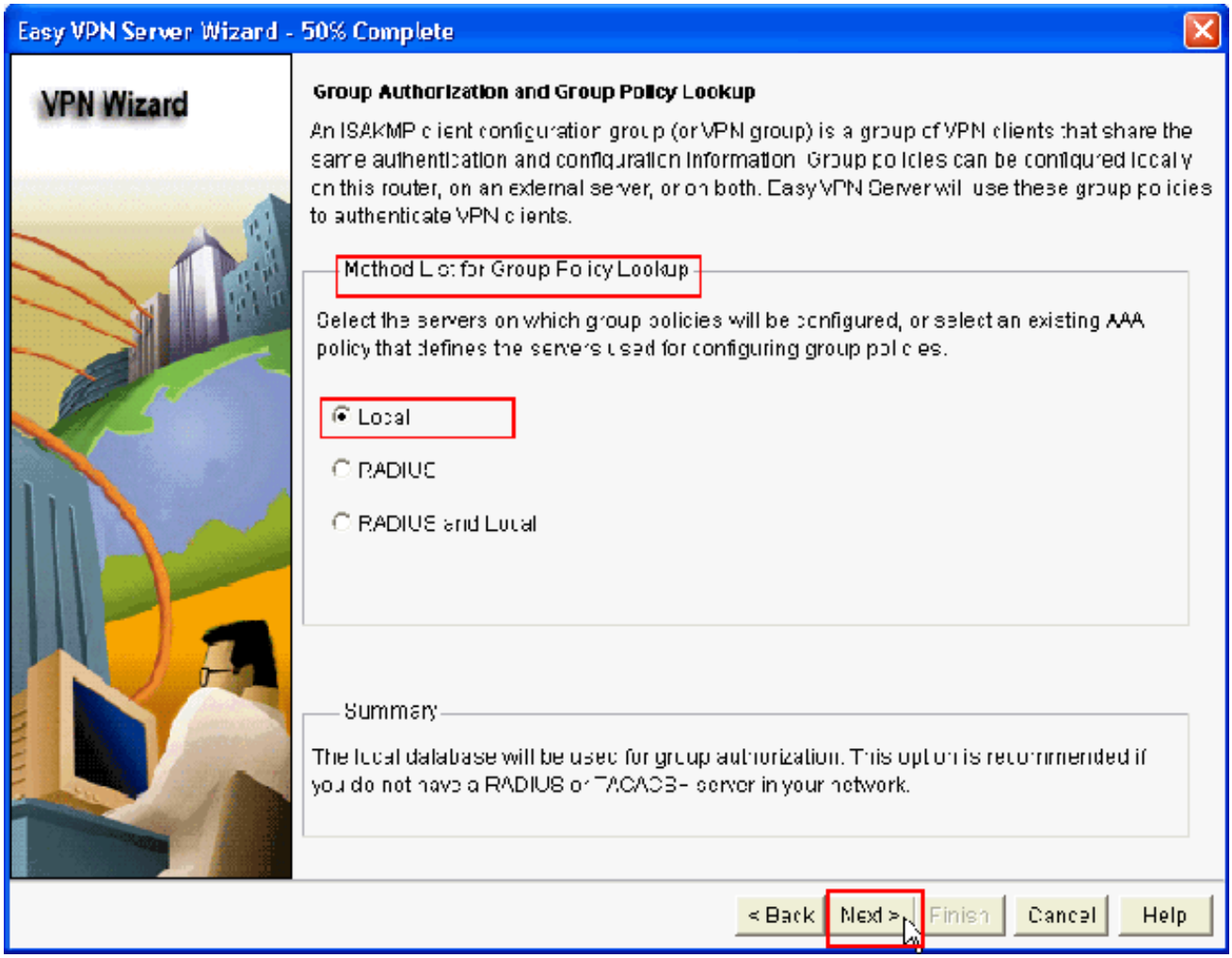
8. Specificare i dettagli del **set di trasformazioni** (**algoritmo di crittografia e autenticazione**) e fare clic su **OK**.



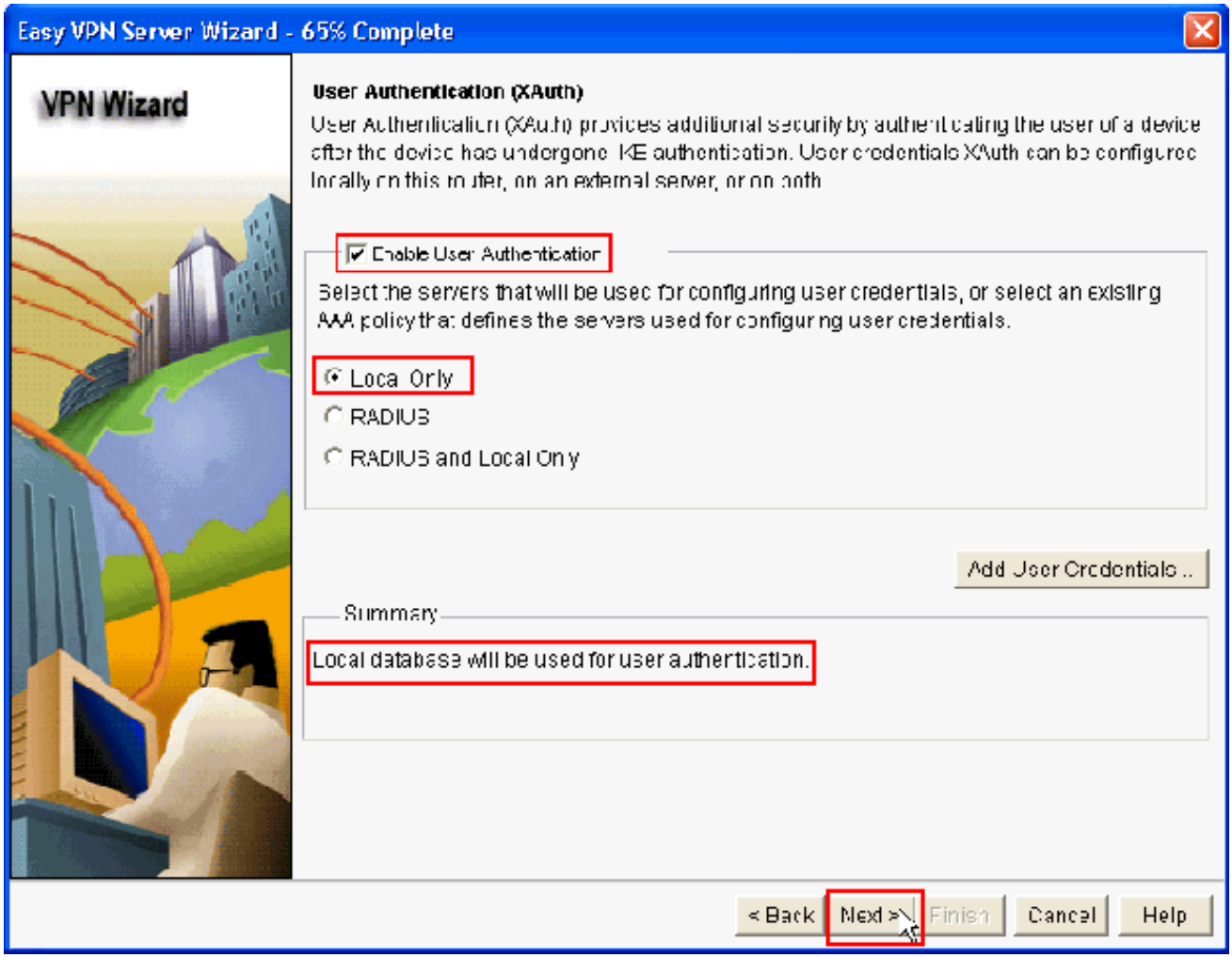
9. In questo esempio viene utilizzato l'**insieme di trasformazioni predefinito** denominato **insieme di trasformazioni predefinito CP**. Di conseguenza, scegliete il set di trasformazioni predefinito e fate clic su **Successivo**.



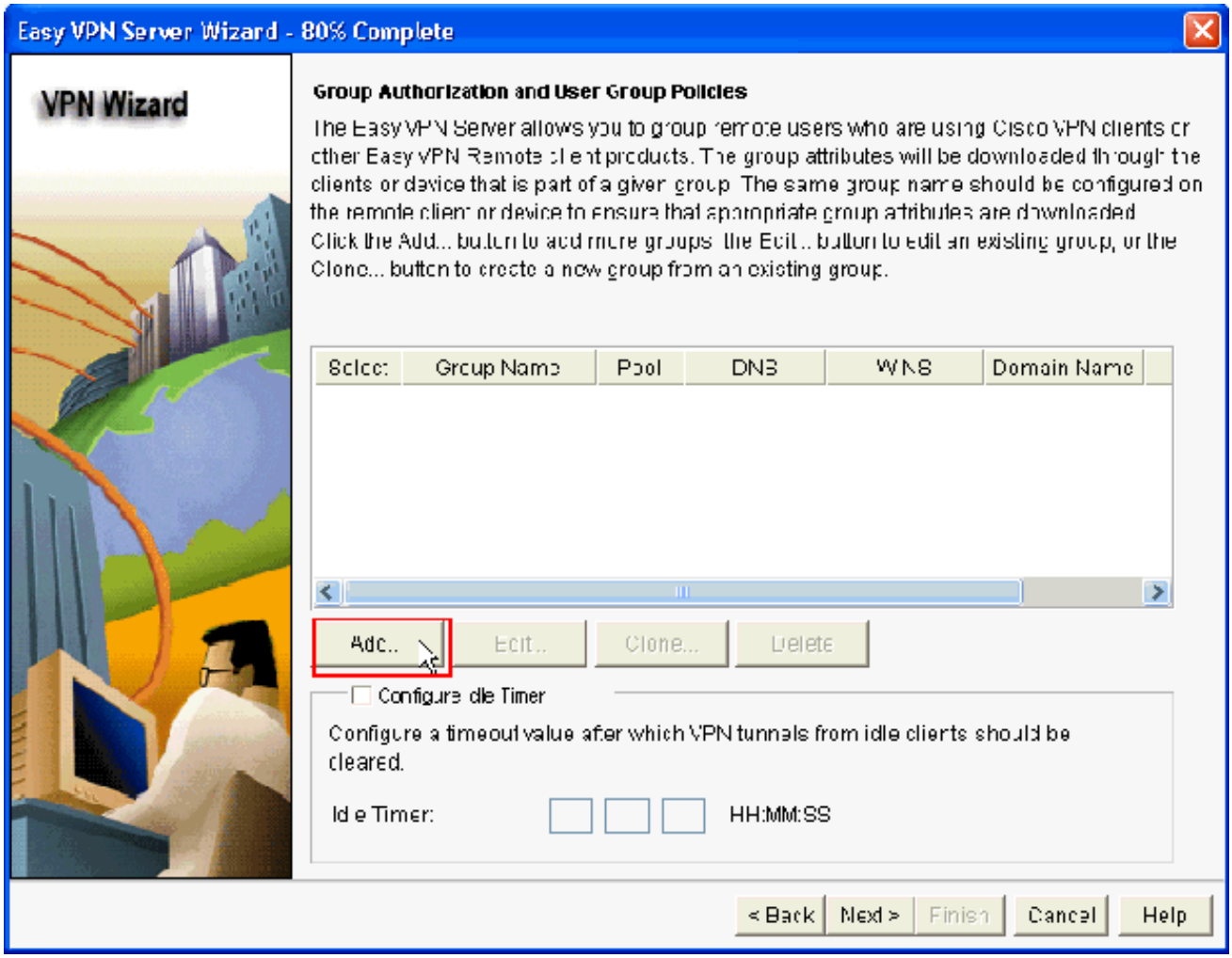
10. Nella nuova finestra scegliere il server in cui verranno configurati i Criteri di gruppo, che può essere **Locale** o **RADIUS** o entrambi **Locale e RADIUS**. In questo esempio viene utilizzato il **server locale** per configurare i criteri di gruppo. Scegliere **Locale** e fare clic su **Avanti**.



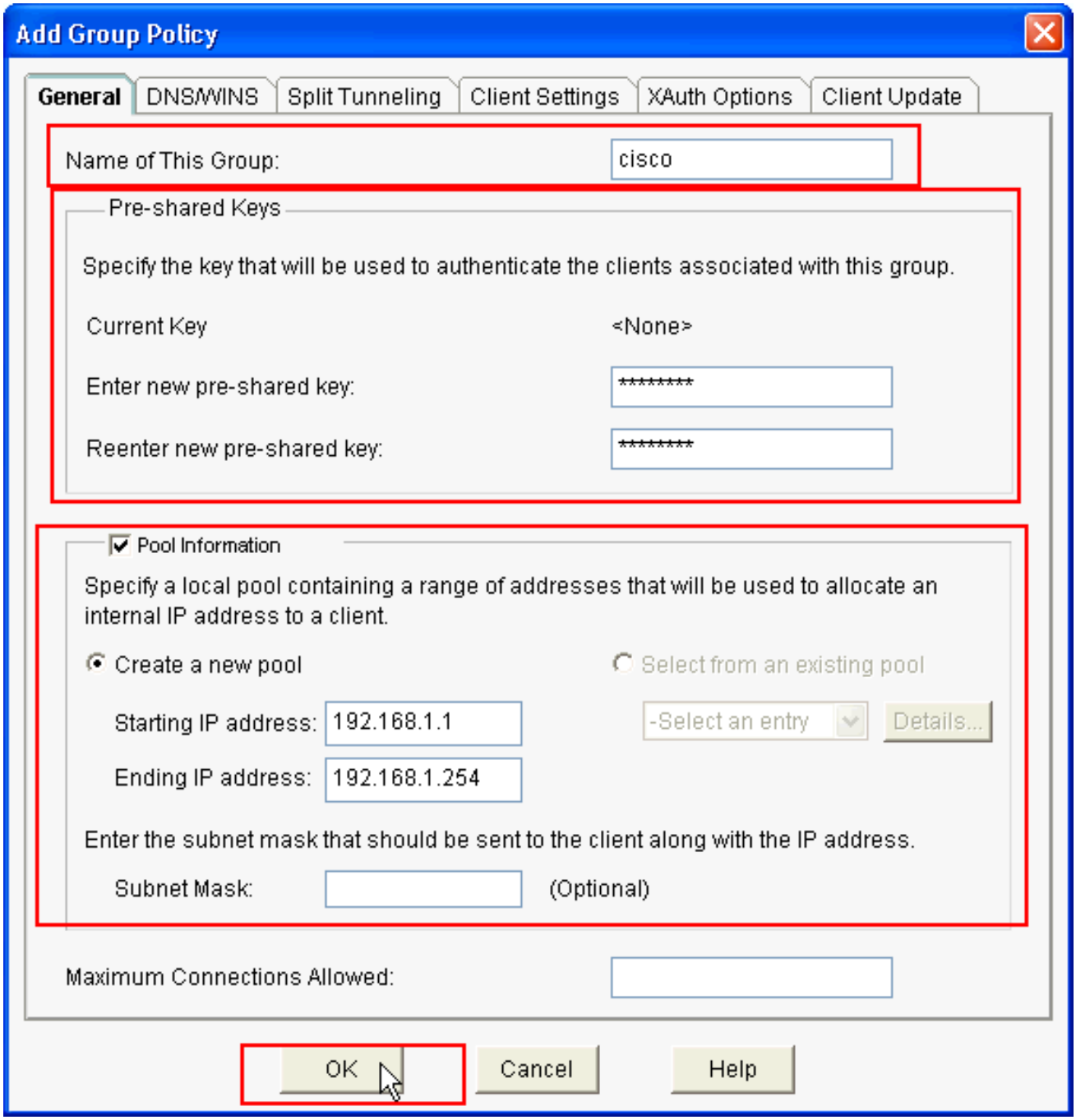
11. In questa nuova finestra scegliere il server da utilizzare per l'autenticazione utente, che può essere **Solo locale** o **RADIUS** o entrambi **Solo locale e RADIUS**. In questo esempio viene utilizzato il **server locale** per configurare le credenziali utente per l'autenticazione. Verificare che la casella di controllo accanto a **Abilita autenticazione utente** sia selezionata. Scegliere **Solo locale** e fare clic su
Avanti.



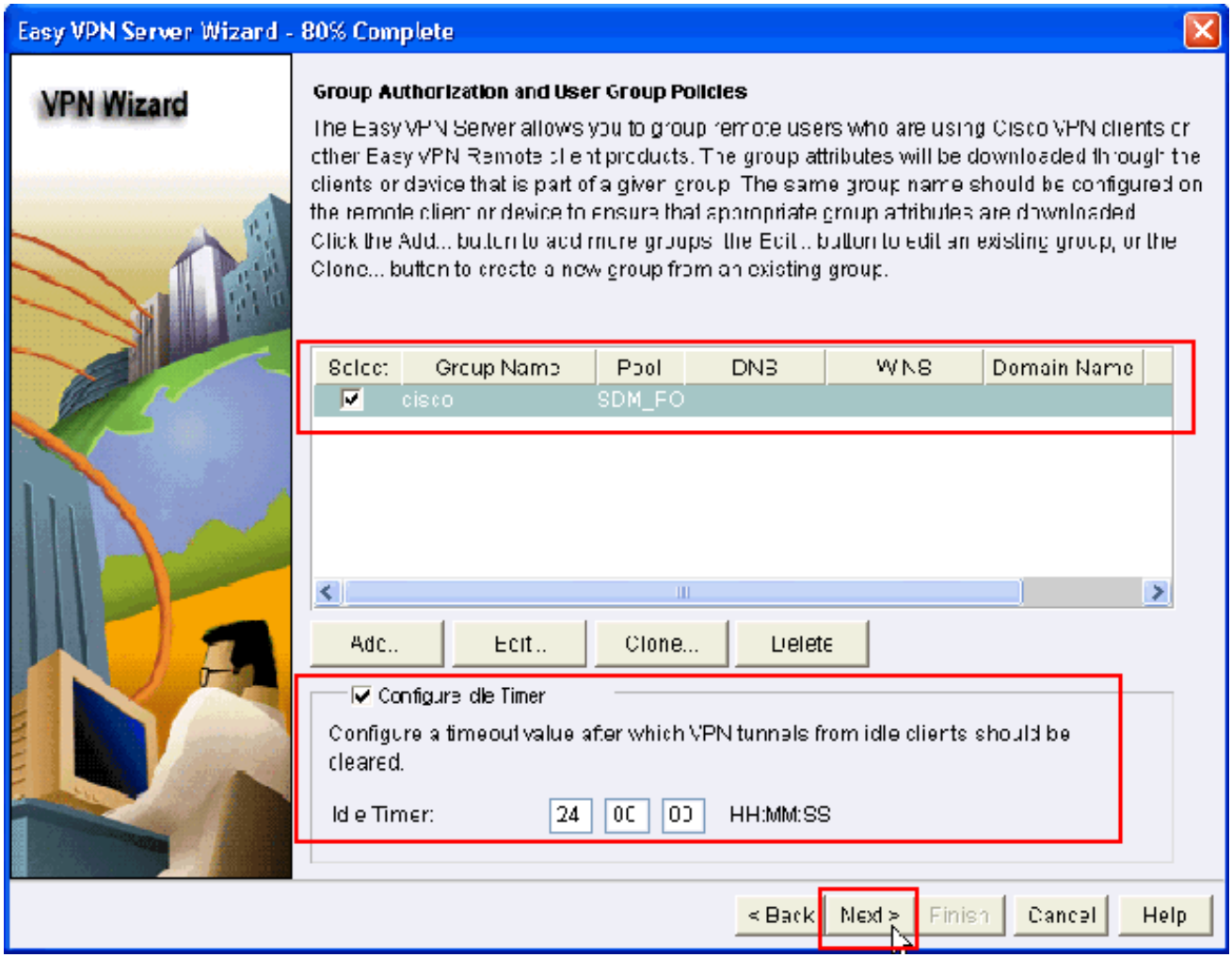
12. Fare clic su **Aggiungi** per creare un nuovo criterio di gruppo e aggiungere gli utenti remoti in questo
gruppo.



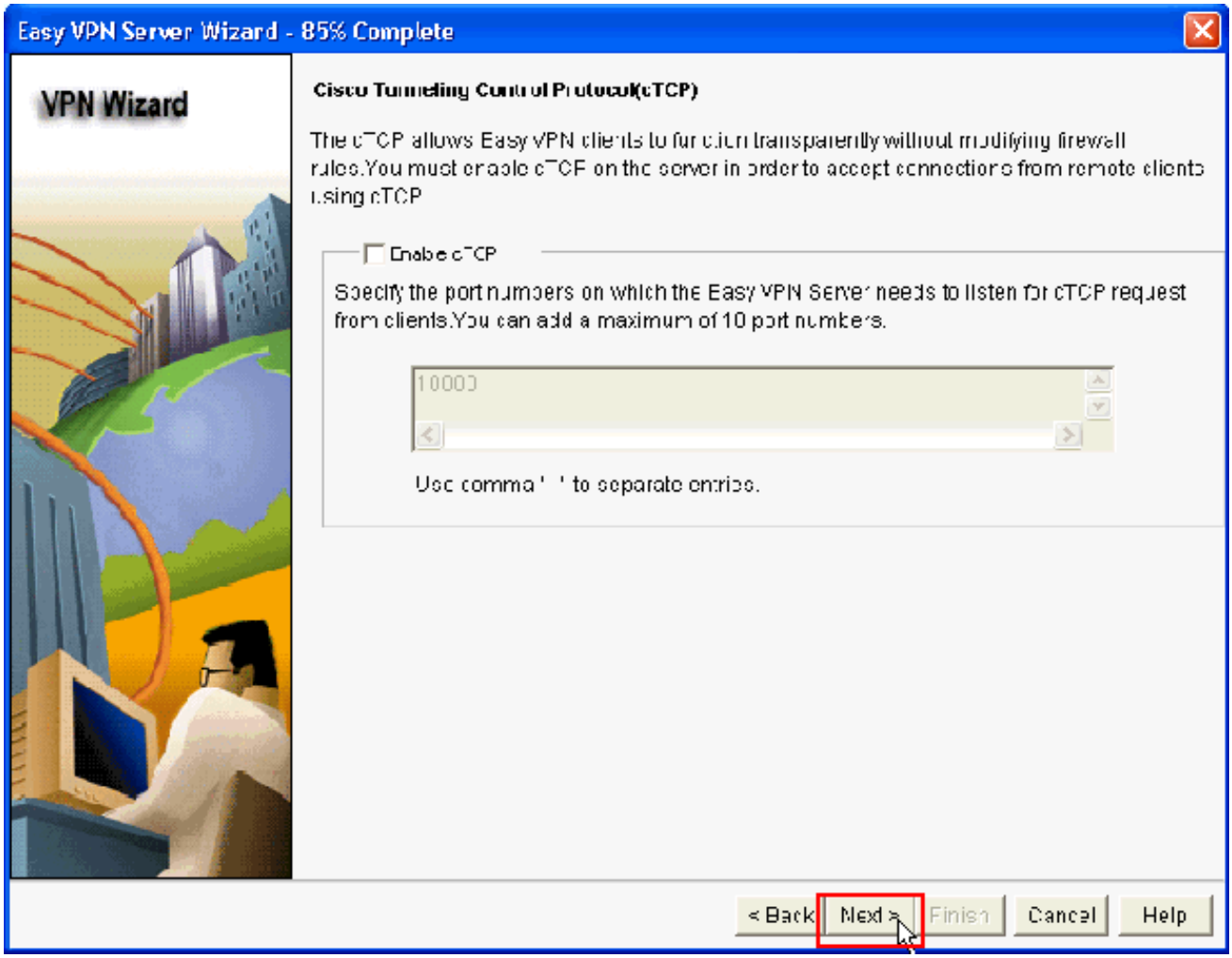
13. Nella finestra Aggiungi Criteri di gruppo, specificare il nome del gruppo nello spazio Specificare il Nome del gruppo (cisco nell'esempio) insieme alla chiave già condivisa e alle informazioni sul pool IP (indirizzo IP iniziale e indirizzo IP finale) come mostrato e fare clic su **OK**.**Nota:** è possibile creare un nuovo pool IP o utilizzare un pool IP esistente, se presente.



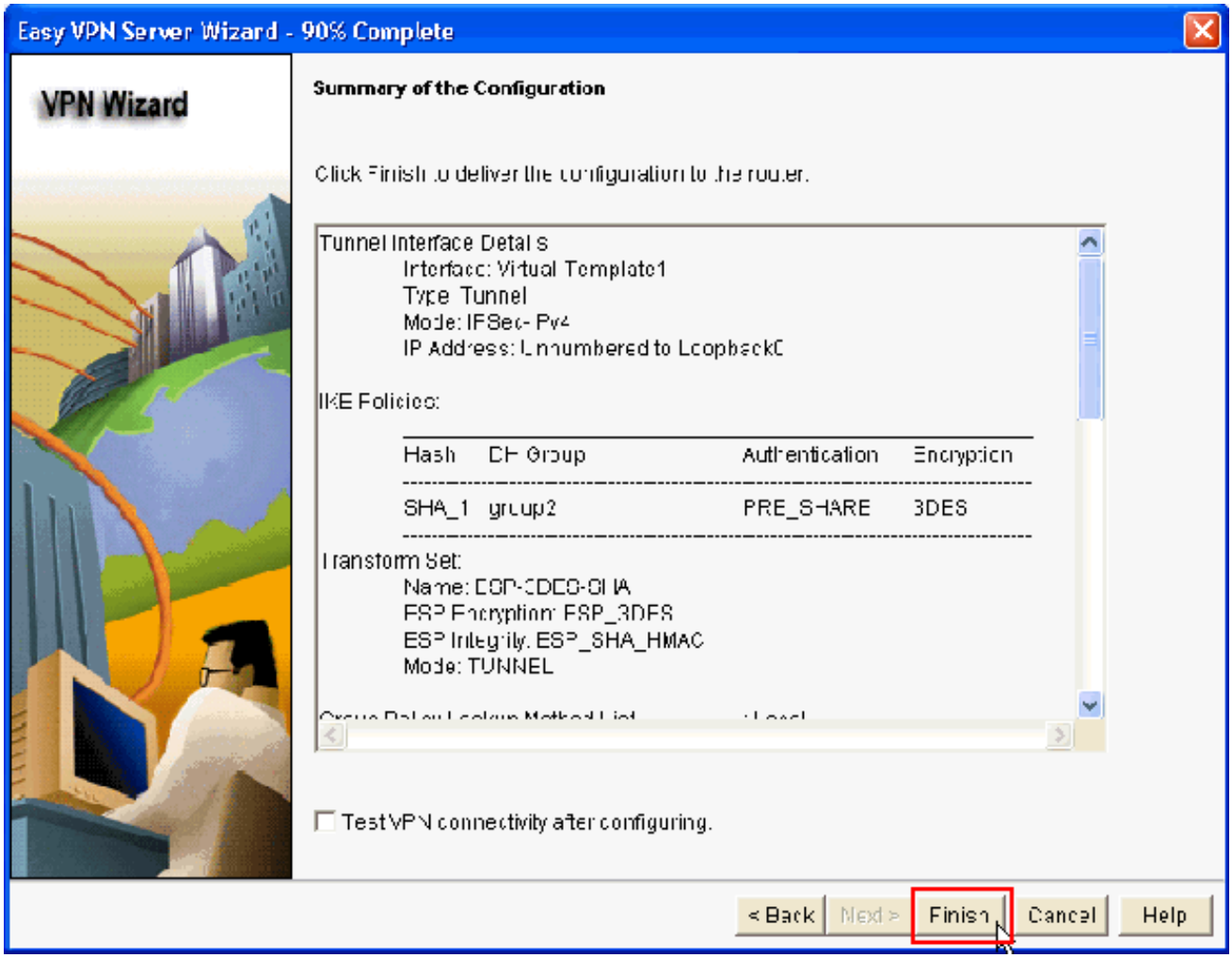
14. Scegliere il nuovo **Criteri di gruppo** creato con il nome **cisco** e quindi fare clic sulla casella di controllo accanto a **Configura timer inattività** in base alle esigenze per configurare il **timer di inattività**. Fare clic su **Next**
(Avanti).



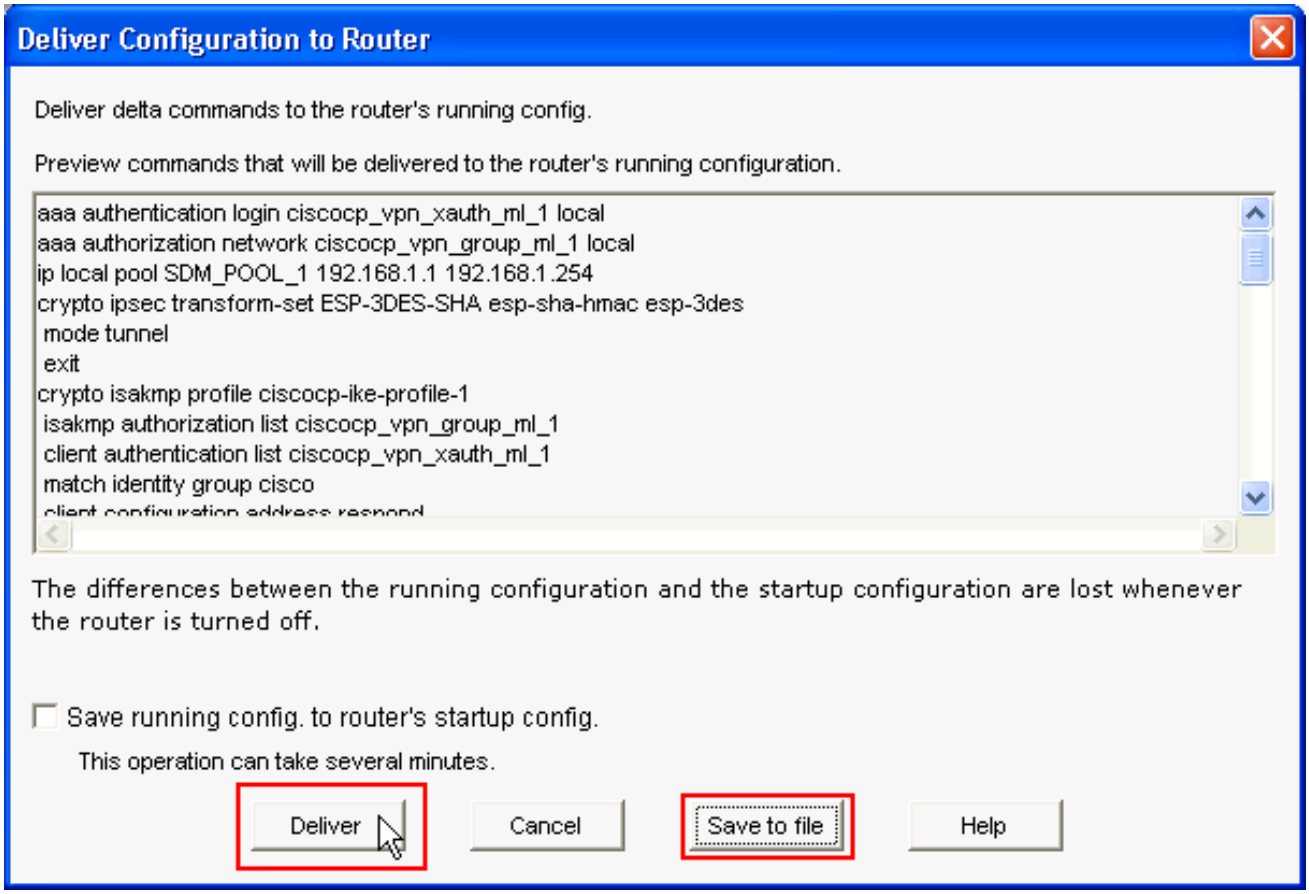
15. Se necessario, abilitare **Cisco Tunneling Control Protocol** (cTCP). In caso contrario, fare clic su
Avanti.



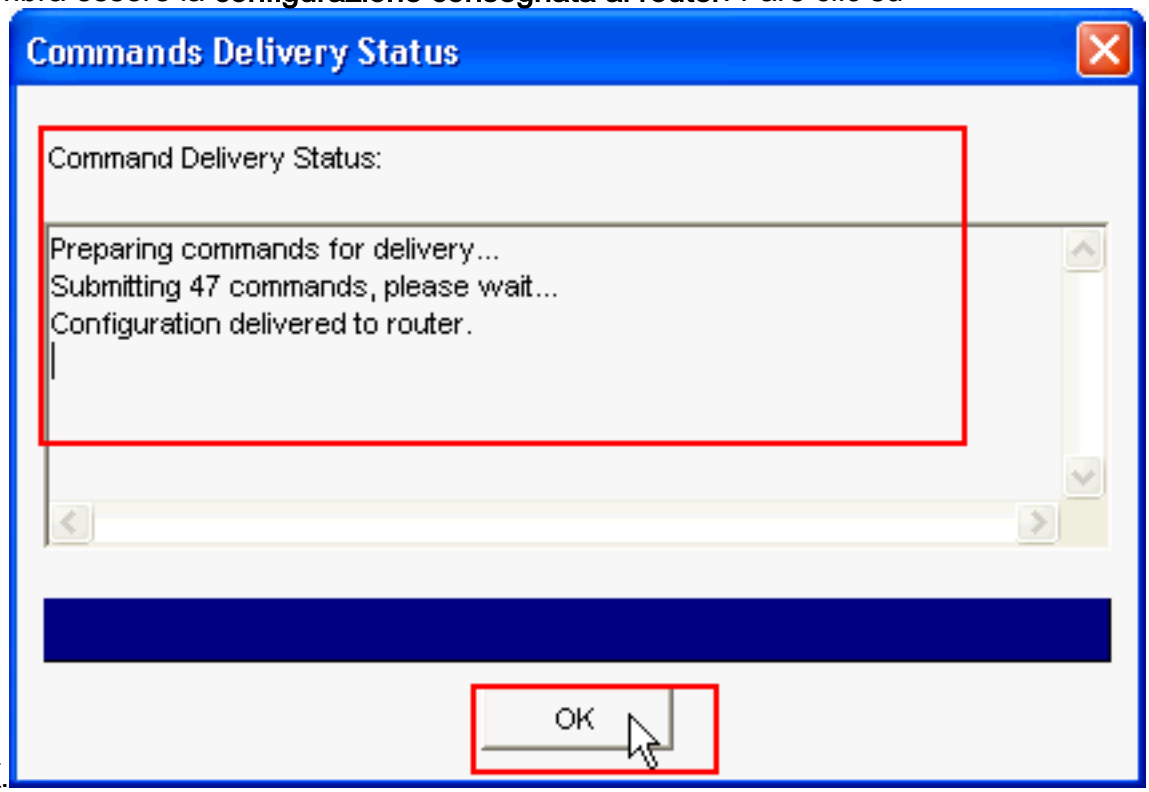
16. Esaminare il **riepilogo della configurazione**. Fare clic su **Finish** (Fine).



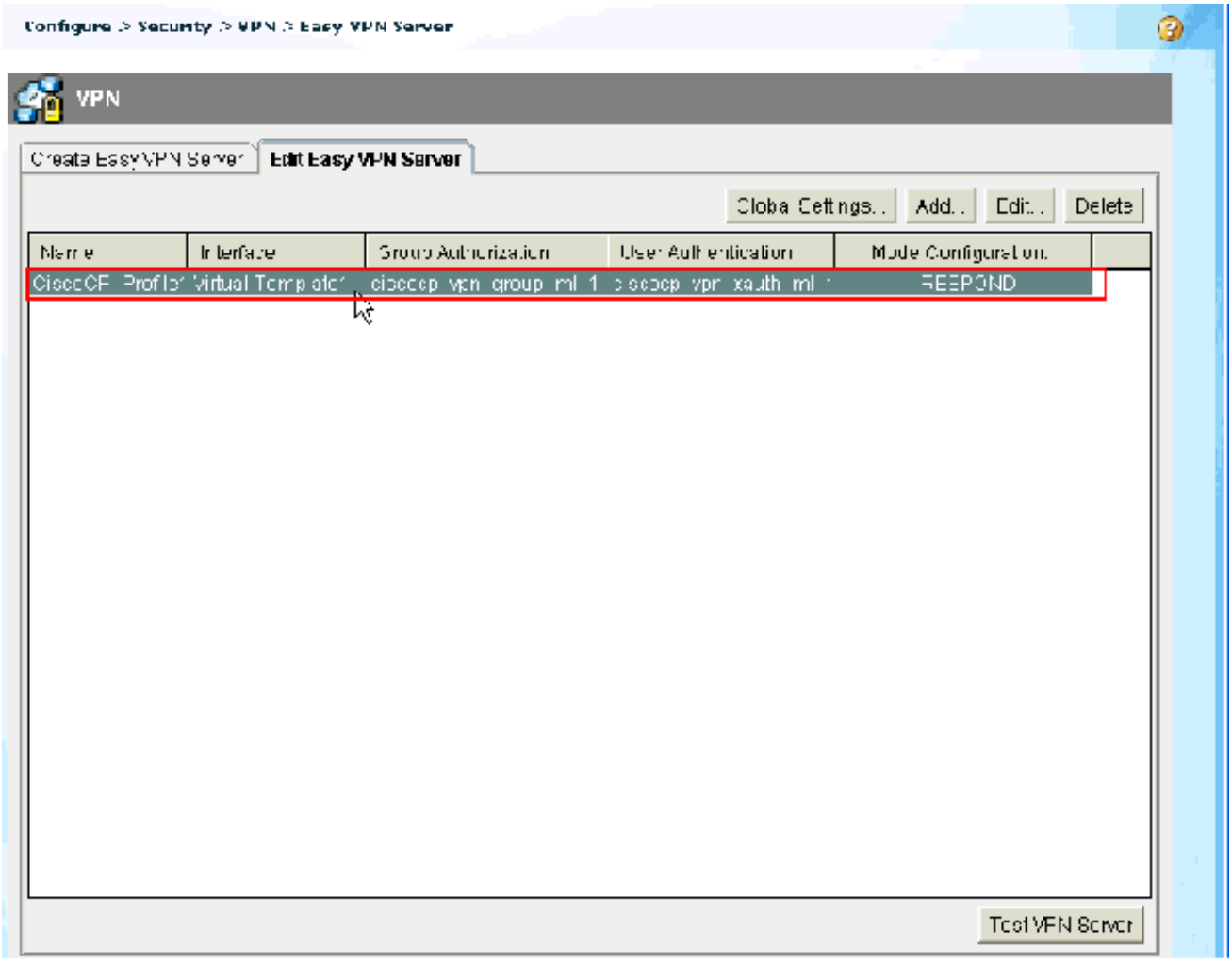
17. Nella finestra **Delivery Configuration to Router**, fare clic su **Deliver** per consegnare la configurazione al router. È possibile fare clic su **Save to file** per salvare la configurazione come file sul
PC.



18. La finestra **Command Delivery Status** mostra lo stato di recapito dei comandi al router. Sembra essere la **configurazione consegnata al router**. Fare clic su **OK**.



19. Èpossibile visualizzare il server Easy VPN appena creato. È possibile modificare il server esistente scegliendo **Modifica server Easy VPN**. La configurazione di Easy VPN Server sul router Cisco IOS è stata completata.



Configurazione CLI

Configurazione router

```
Router#show run
Building configuration...

Current configuration : 2069 bytes
! version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption hostname Router boot-start-marker
boot-end-marker no logging buffered enable password
cisco !---AAA enabled using aaa newmodel command. Also
AAA Authentication and Authorization are enabled---! aaa
new-model
!
!
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization network ciscocp_vpn_group_ml_1 local
!
!
aaa session-id common
ip cef
!
!
!
!
ip domain name cisco.com
!
```

```
multilink bundle-name authenticated
!
!
!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
 key cisco123
 pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1
   match identity group cisco
   client authentication list ciscocp_vpn_xauth_ml_1
   isakmp authorization list ciscocp_vpn_group_ml_1
   client configuration address respond
   virtual-template 1
!
!
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ESP-3DES-
SHA esp-3des esp-sha-hmac
!
crypto ipsec profile CiscoCP_Profile1
 set security-association idle-time 86400
 set transform-set ESP-3DES-SHA
 set isakmp-profile ciscocp-ike-profile-1
!
!
!
!--- RSA certificate generated after you enable the !---
ip http secure-server command.

crypto pki trustpoint TP-self-signed-1742995674
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1742995674
 revocation-check none
 rsakeypair TP-self-signed-1742995674

!--- Create a user account named cisco123 with all
privileges.

username cisco123 privilege 15 password 0 cisco123
archive
 log config
  hidekeys
!
!
!--- Interface configurations are done as shown below---
! interface Loopback0 ip address 10.10.10.10
255.255.255.0 ! interface FastEthernet0/0 ip address
10.77.241.111 255.255.255.192 duplex auto speed auto !
interface Virtual-Template1 type tunnel ip unnumbered
Loopback0 tunnel mode ipsec ipv4 tunnel protection ipsec
profile CiscoCP_Profile1 ! !--- VPN pool named
SDM_POOL_1 has been defined in the below command---! ip
```

```
local pool SDM_POOL_1 192.168.1.1 192.168.1.254

!--- This is where the commands to enable HTTP and HTTPS
are configured. ip http server ip http authentication
local ip http secure-server ! ! ! ! control-plane ! line
con 0 line aux 0 !--- Telnet enabled with password as
cisco. line vty 0 4 password cisco transport input all
scheduler allocate 20000 1000 ! ! ! ! end
```

Verifica

Easy VPN Server - Comandi show

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

- **show crypto isakmp sa**: visualizza tutte le associazioni di protezione IKE correnti in un peer.

```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.77.241.111   172.16.1.1     QM_IDLE           1003    0 ACTIVE
```

- **show crypto ipsec sa**: visualizza tutte le SA IPsec correnti in un peer.

```
Router#show crypto ipsec sa
interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
   current_peer 172.16.1.1 port 1086
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 2

     local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x186C05EF(409732591)

     inbound esp sas:
      spi: 0x42FC8173(1123844467)
        transform: esp-3des esp-sha-hmac
```

Risoluzione dei problemi

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

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

Informazioni correlate

- Negoziazione IPSec/protocolli IKE
- Guida rapida di Cisco Configuration Professional
- Pagina di supporto dei prodotti Cisco - Router
- Documentazione e supporto tecnico – Cisco Systems