# Esempio di configurazione SDM per un router Cisco come server VPN remoto

## Sommario



## Introduzione

In questo documento viene descritto come usare Cisco Security Device Manager (SDM) per configurare il router Cisco in modo che agisca come server Easy VPN. Cisco SDM consente di configurare il router come server VPN per il client VPN Cisco utilizzando un'interfaccia di gestione basata sul Web di facile utilizzo. Una volta completata la configurazione del router Cisco, è possibile verificarla utilizzando il client VPN Cisco.

## Prerequisiti

### Requisiti

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

**Nota:** per consentire al router di essere configurato dal modulo SDM, consultare il documento sull'autorizzazione dell'accesso HTTPS per SDM.

### Componenti usati

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

- Router Cisco 3640 con software Cisco IOS® versione 12.3(14T)
- Security Device Manager versione 2.31
- Cisco VPN Client versione 4.8

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.

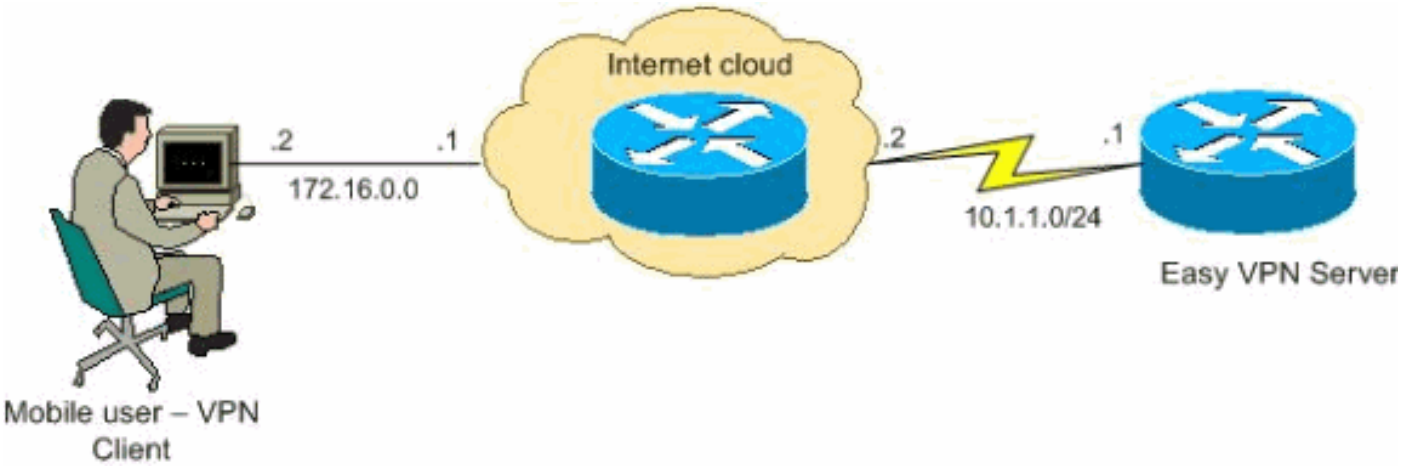
# Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare la funzionalità Easy VPN Server che consente a un utente finale remoto di comunicare tramite IPsec con qualsiasi gateway VPN di Cisco IOS®.

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

## Esempio di rete

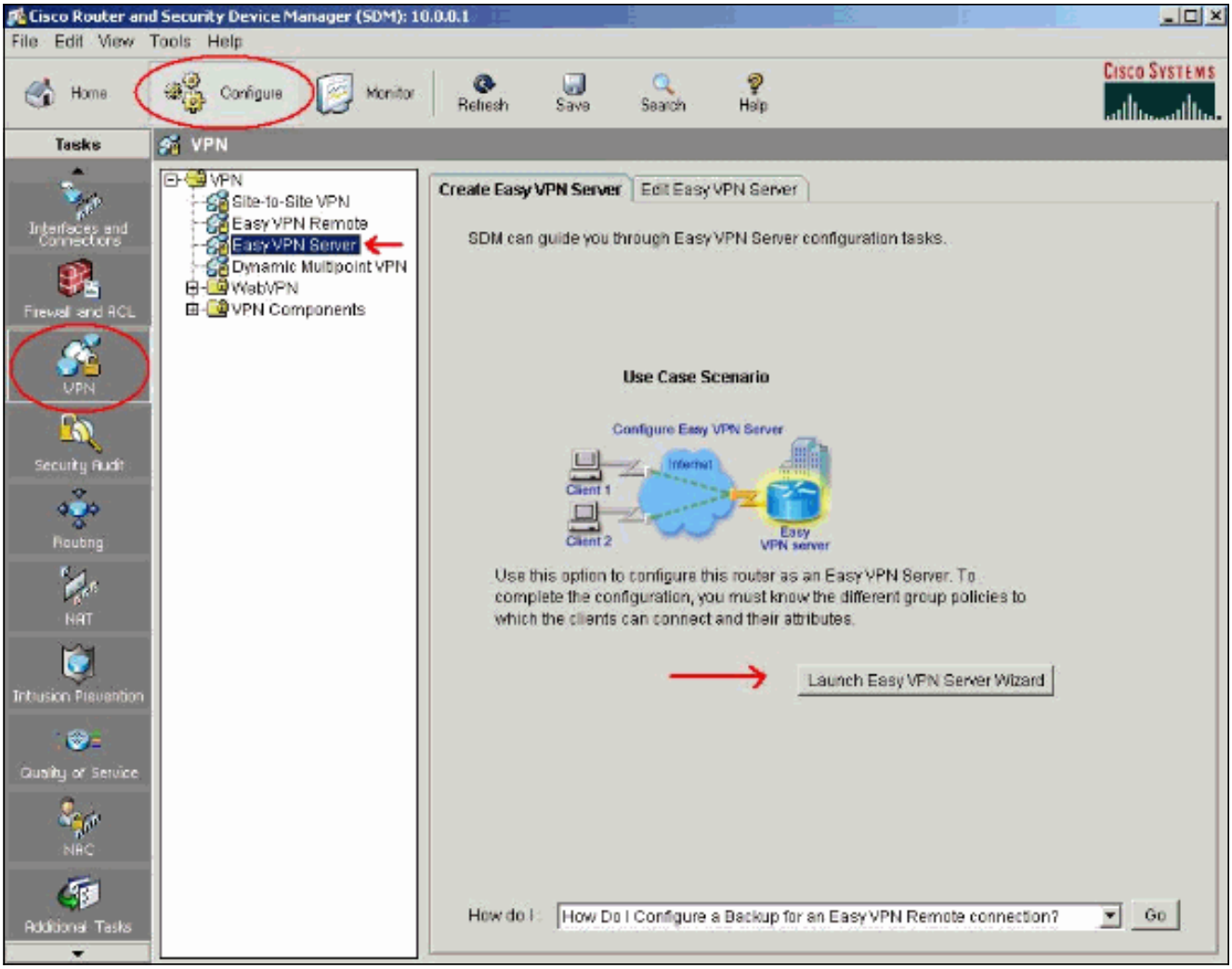
Nel documento viene usata questa impostazione di rete:



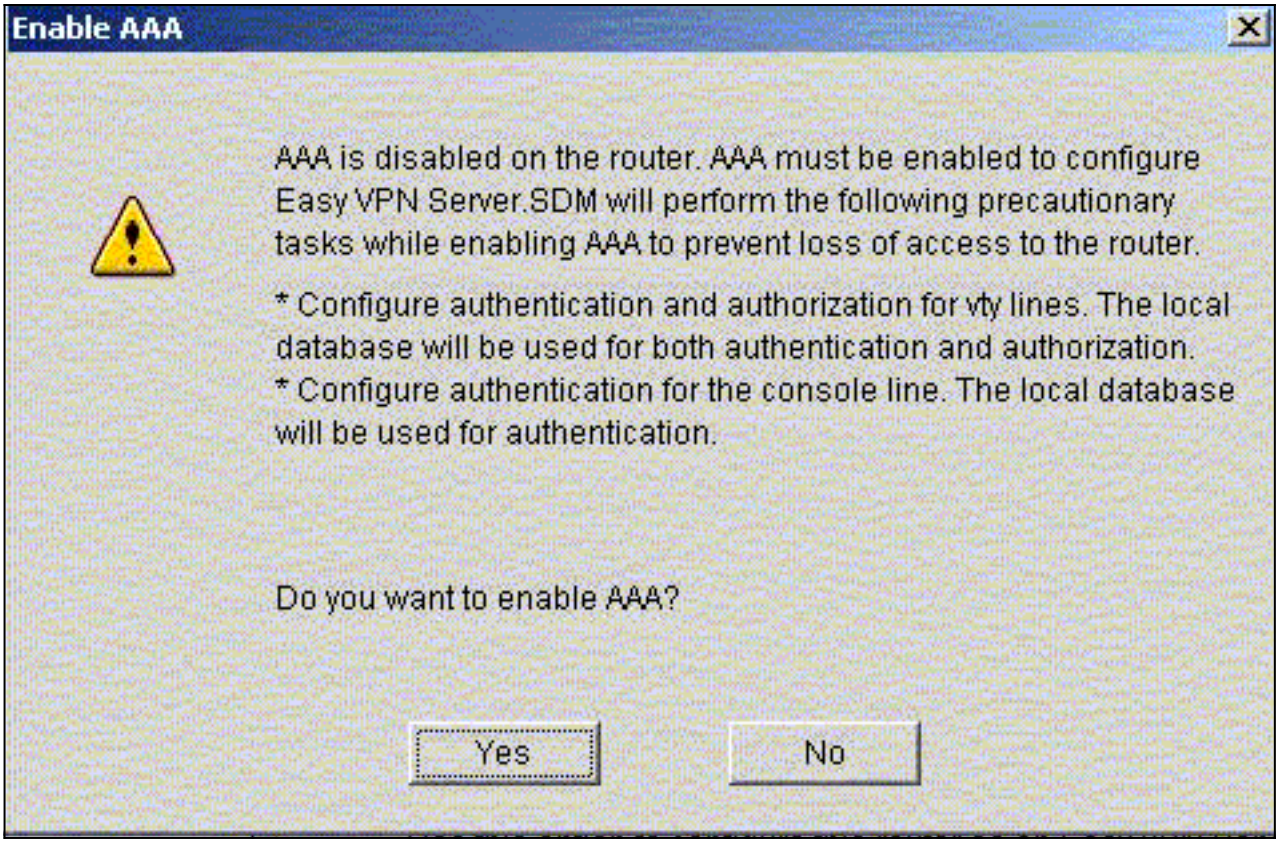

## Procedura di configurazione

Completare la procedura seguente per configurare il router Cisco come server VPN remoto con SDM.

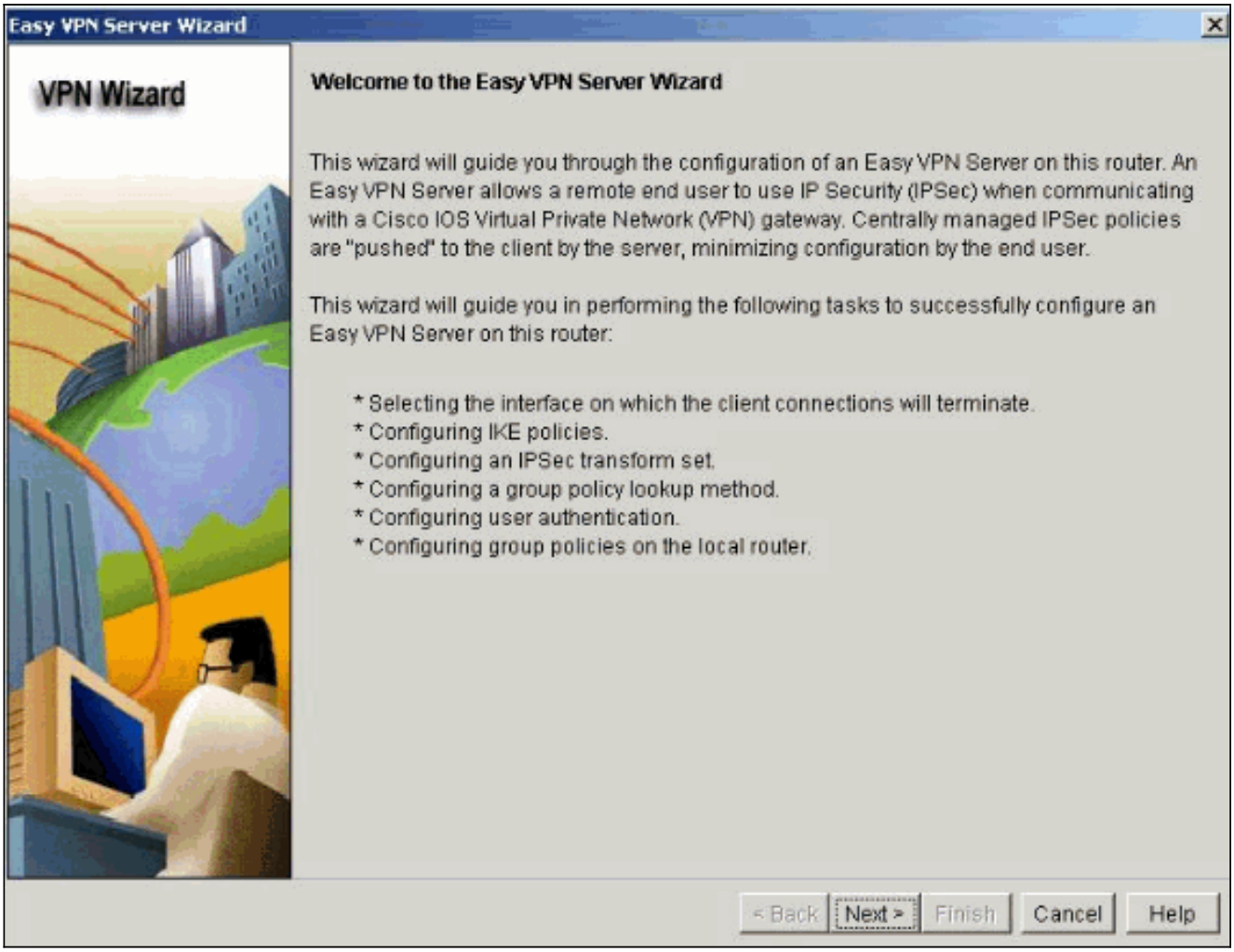
1. Selezionare **Configure > VPN > Easy VPN Server** dalla finestra Home e fare clic su **Launch Easy VPN Server Wizard**.



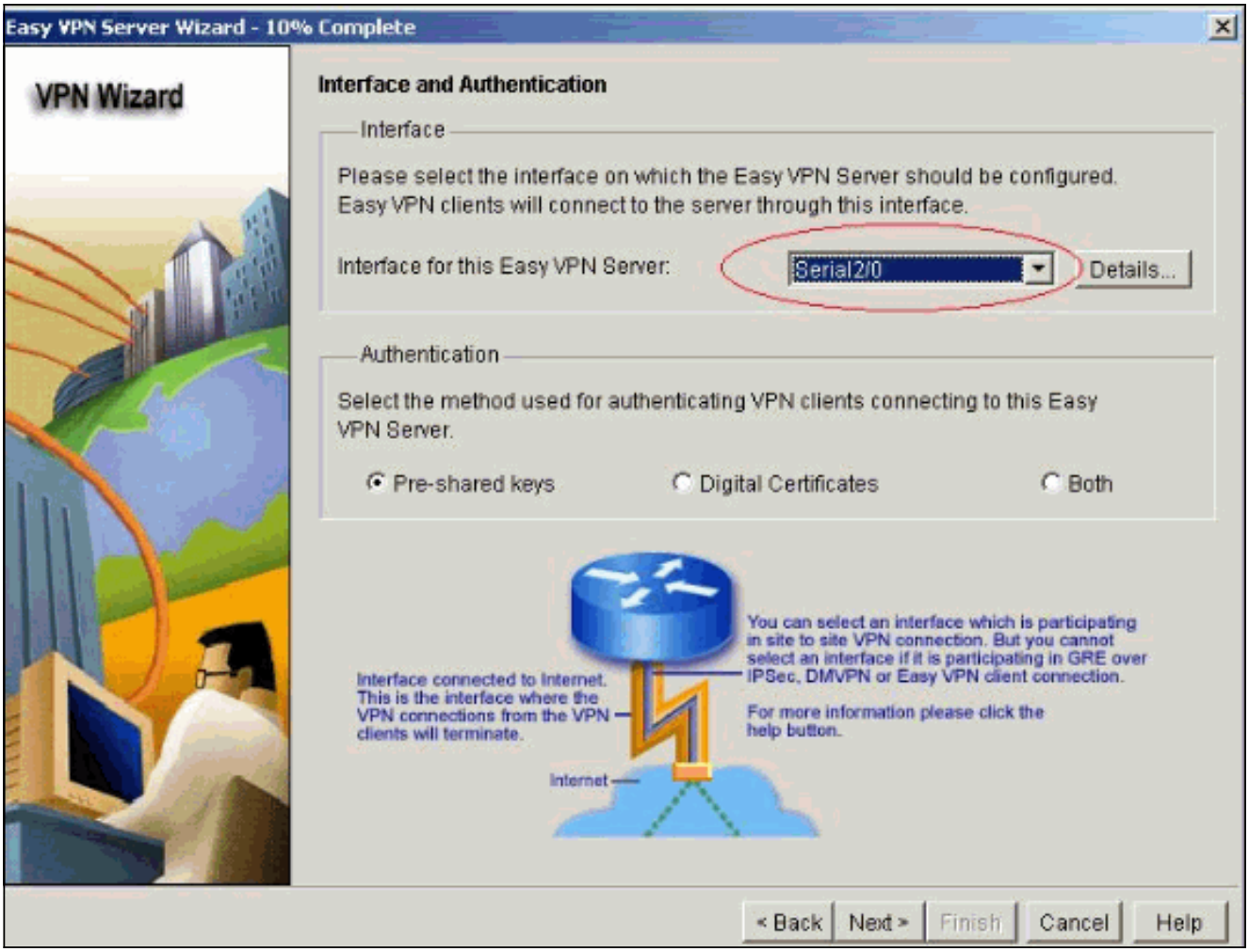

2. È necessario abilitare AAA sul router prima di avviare la configurazione di Easy VPN Server. Fare clic su **Sì** per continuare con la configurazione.Il messaggio "AAA abilitato sul router" viene visualizzato nella finestra. Fare clic su **OK** per avviare la configurazione di Easy VPN Server.



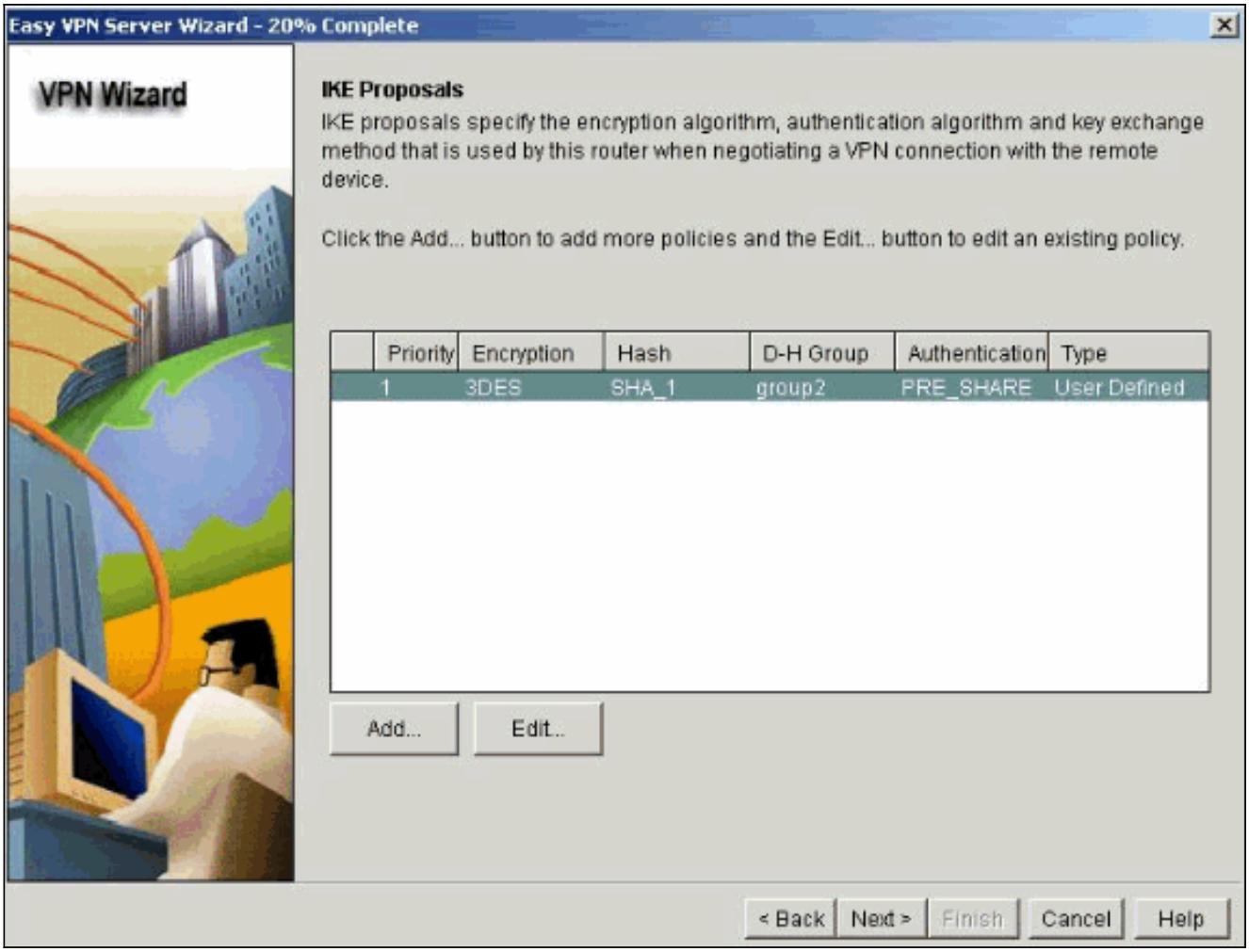
3. Fare clic su **Avanti** per avviare la procedura guidata Easy VPN Server.



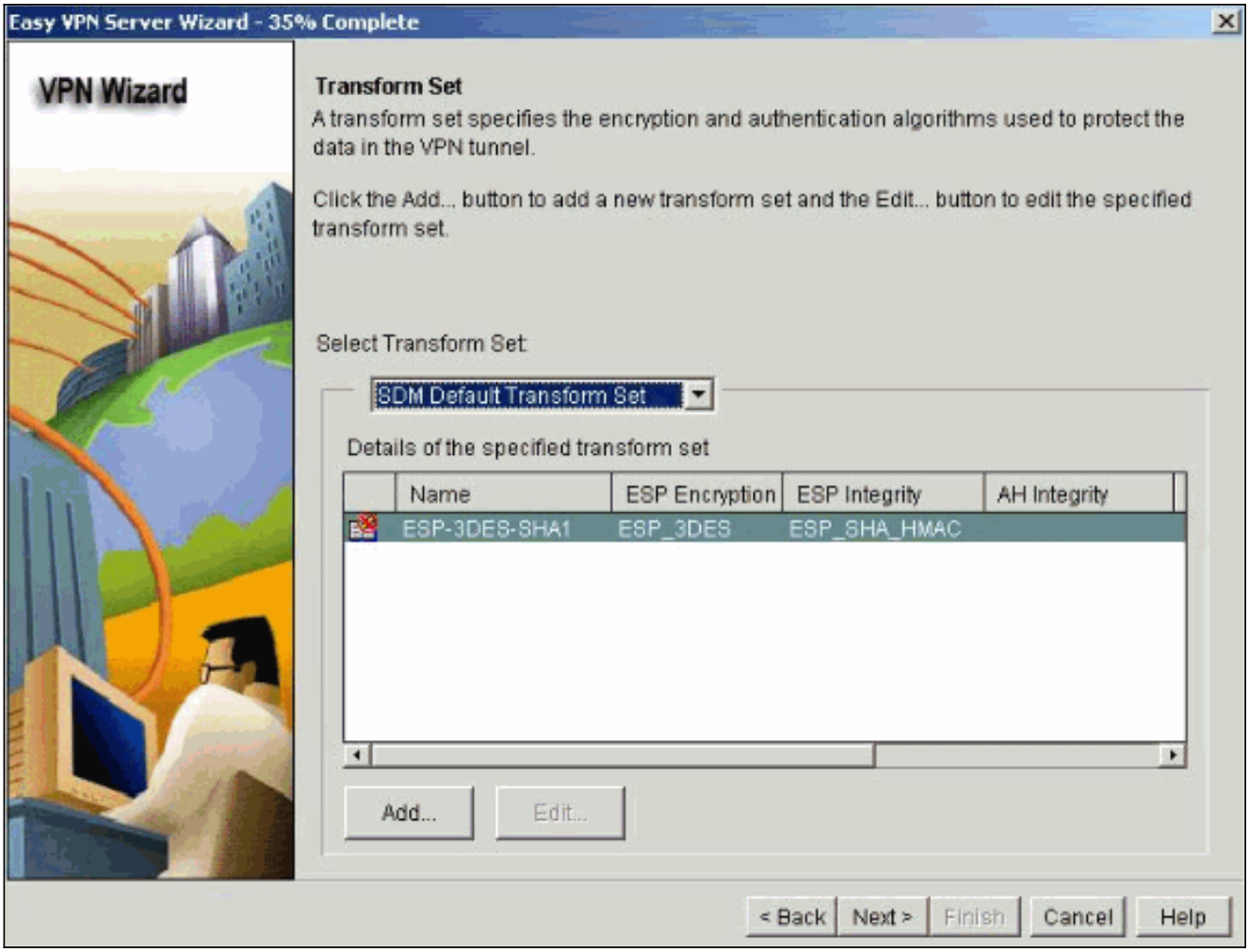

4. Selezionare l'interfaccia su cui terminano le connessioni client e il tipo di autenticazione.



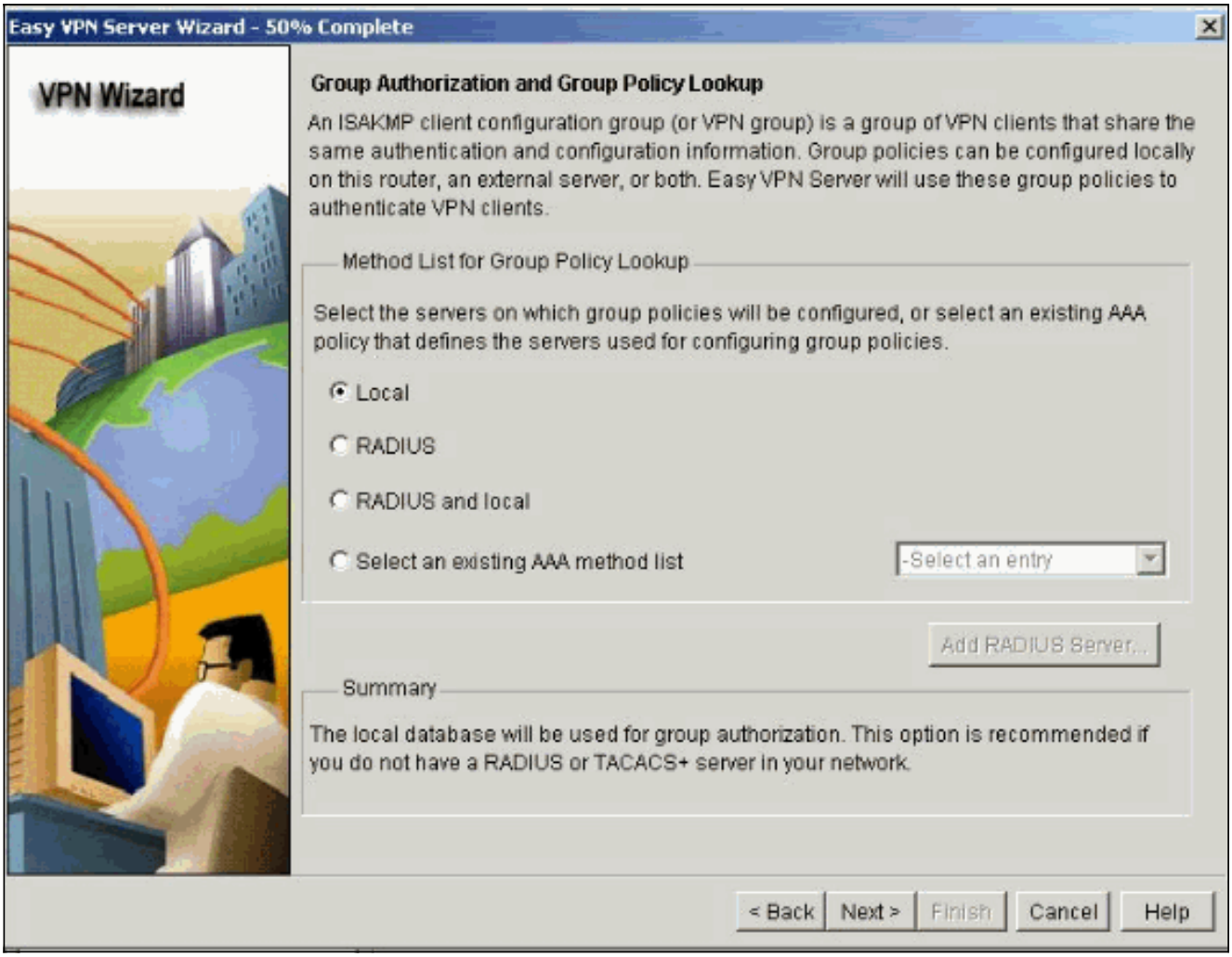

5. Fare clic su **Avanti** per configurare i criteri IKE (Internet Key Exchange) e utilizzare il pulsante **Aggiungi** per creare il nuovo criterio.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente. Tuttavia, il client VPN Cisco seleziona automaticamente la configurazione corretta. Non è pertanto necessaria alcuna configurazione IKE sul PC client.



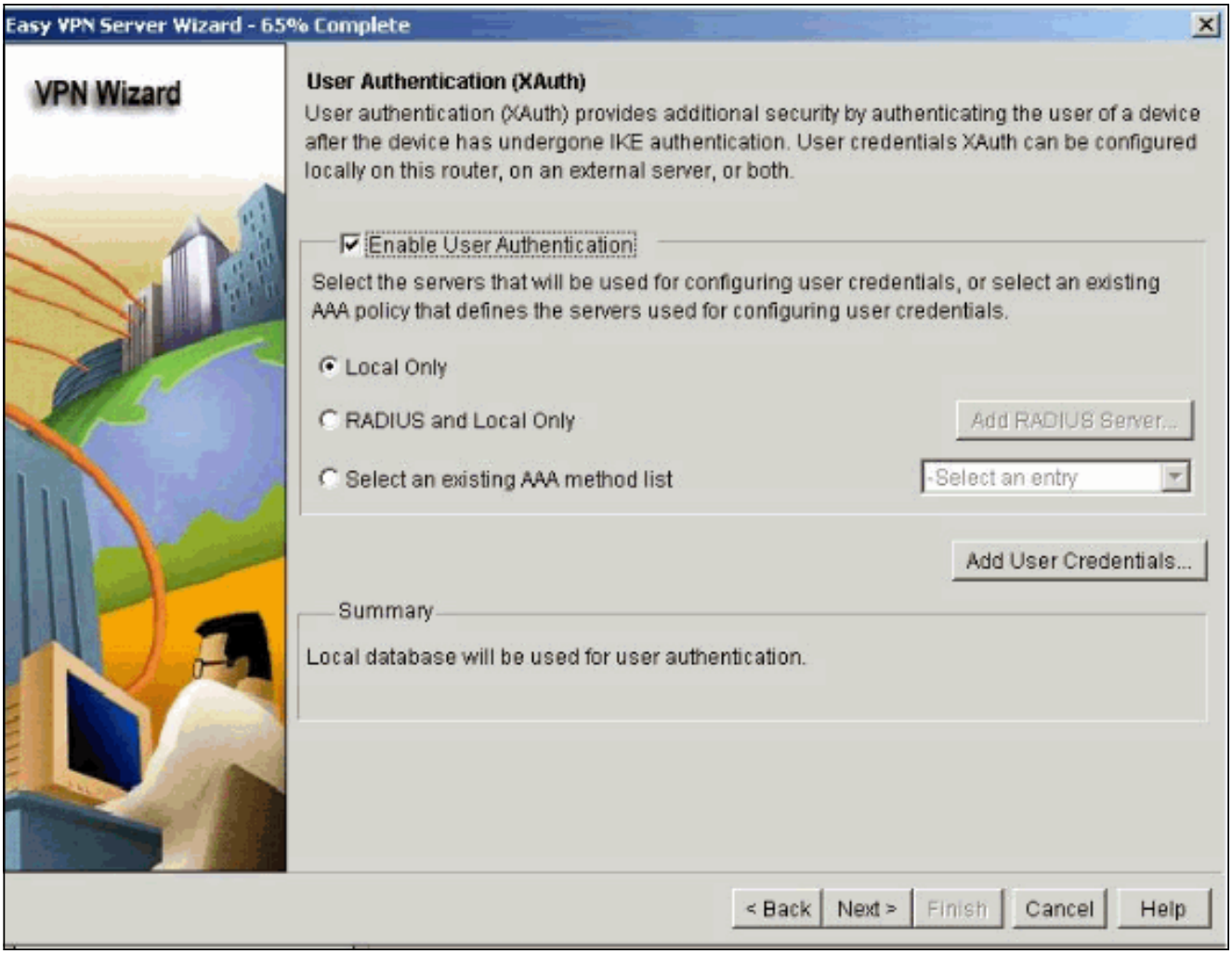

6. Fare clic su **Avanti** per scegliere il set di trasformazioni predefinito o aggiungere il nuovo set di trasformazioni per specificare l'algoritmo di crittografia e autenticazione. In questo caso, viene utilizzato il set di trasformazioni predefinito.



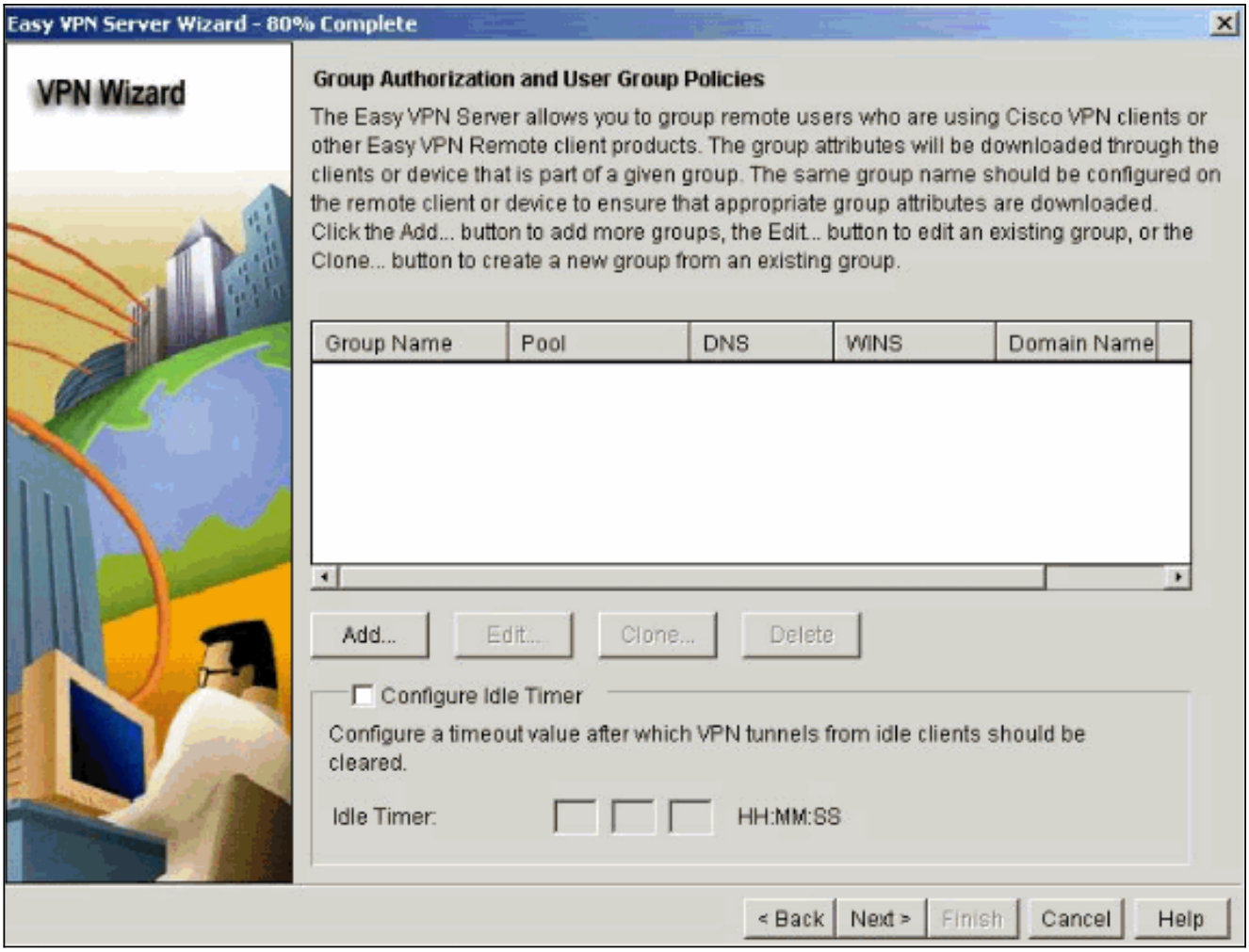

7. Fare clic su **Avanti** per creare un nuovo elenco di metodi di rete di autorizzazione Autenticazione, autorizzazione e accounting (AAA) per la ricerca di Criteri di gruppo o per scegliere un elenco di metodi di rete esistente utilizzato per l'autorizzazione di gruppo.



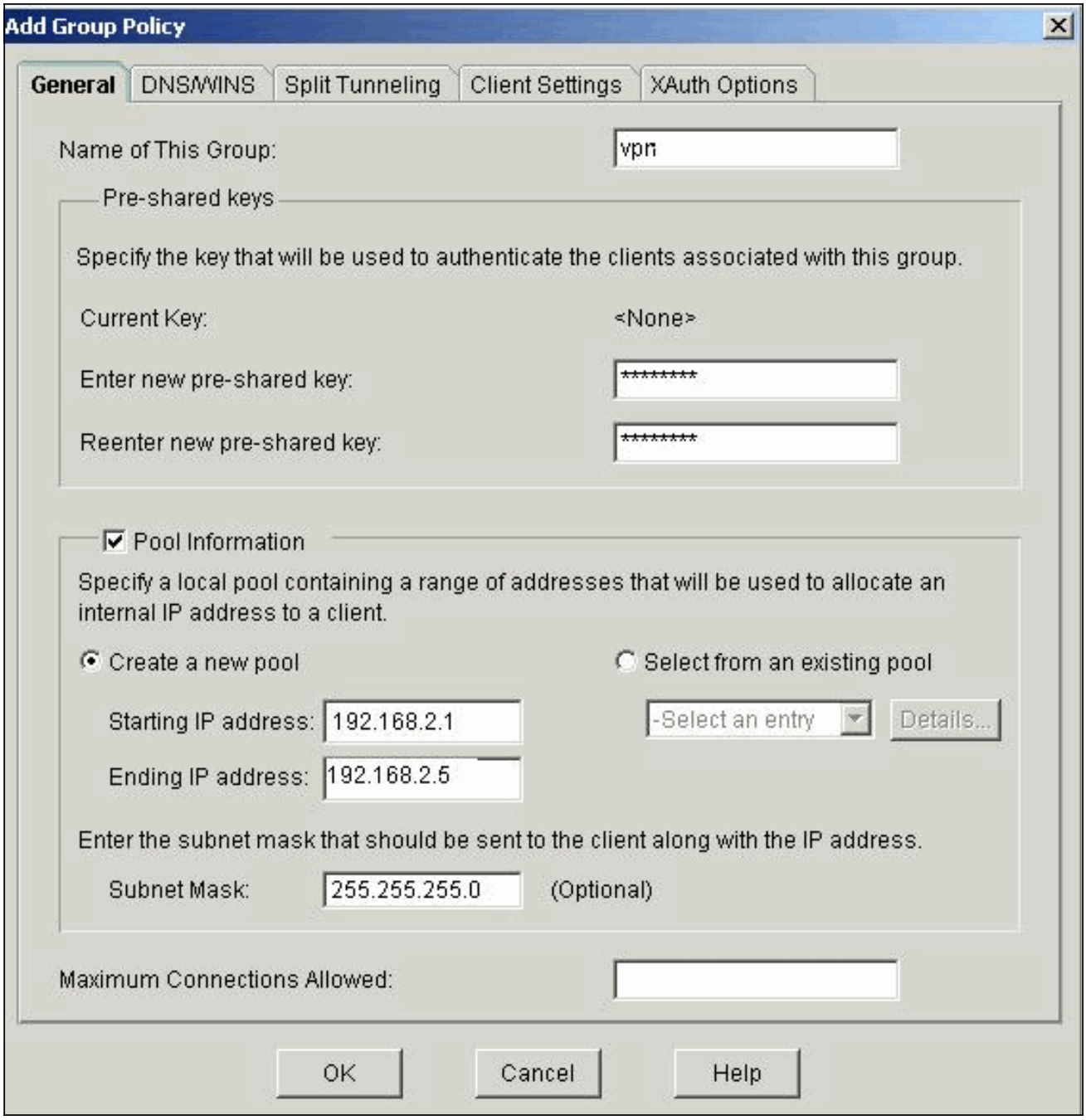

8. Configurare l'autenticazione utente sul server Easy VPN.Èpossibile memorizzare i dettagli di autenticazione degli utenti su un server esterno, ad esempio un server RADIUS o un database locale oppure su entrambi. L'elenco dei metodi di autenticazione di accesso AAA viene utilizzato per stabilire l'ordine in cui cercare i dettagli di autenticazione dell'utente.



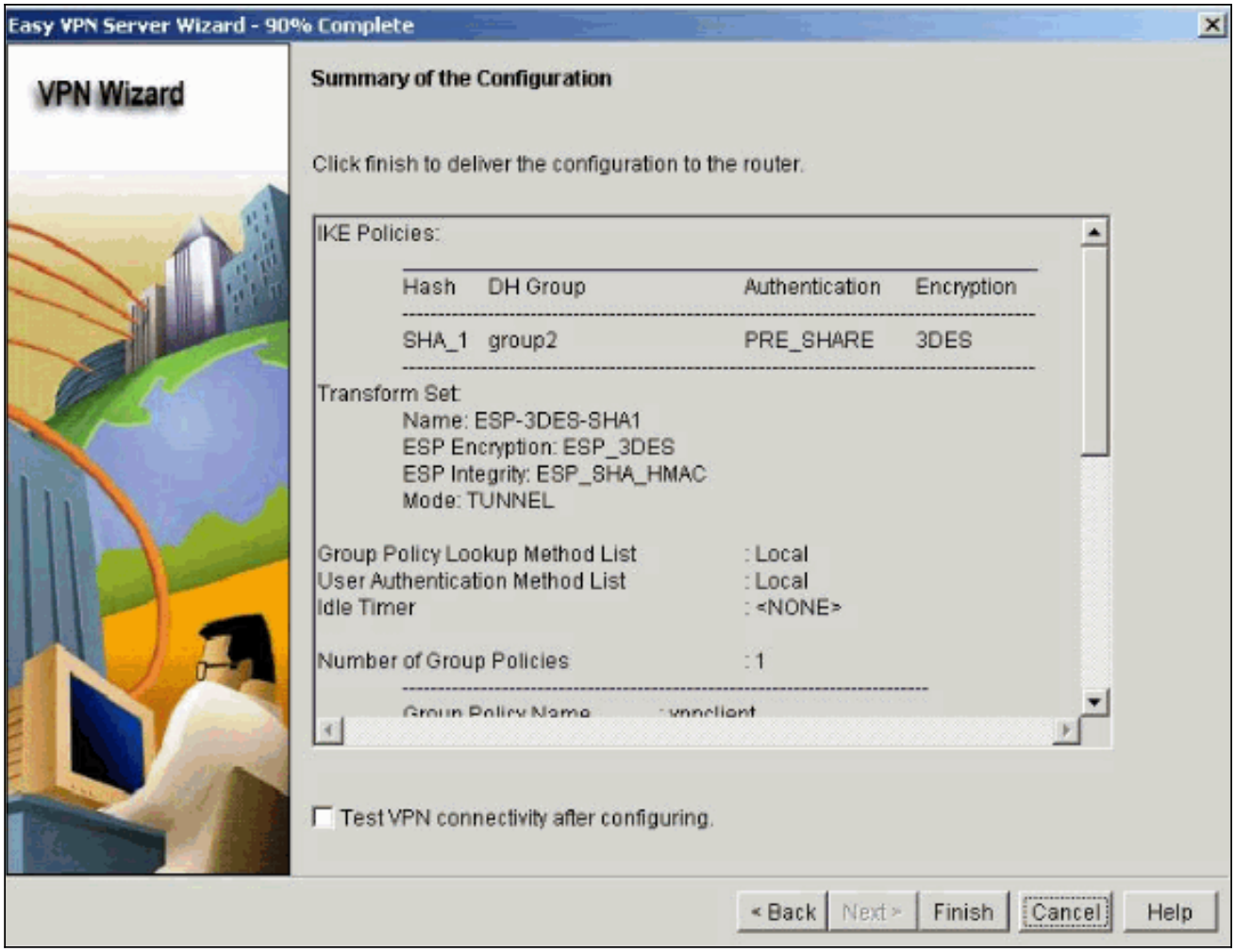

9. Questa finestra consente di aggiungere, modificare, duplicare o eliminare i criteri di gruppo degli utenti nel database
locale.




10. Immettere un nome per il nome del gruppo di tunnel. Specificare la chiave già condivisa utilizzata per le informazioni di autenticazione.Creare un nuovo pool o selezionare un pool esistente utilizzato per allocare gli indirizzi IP ai client
VPN.

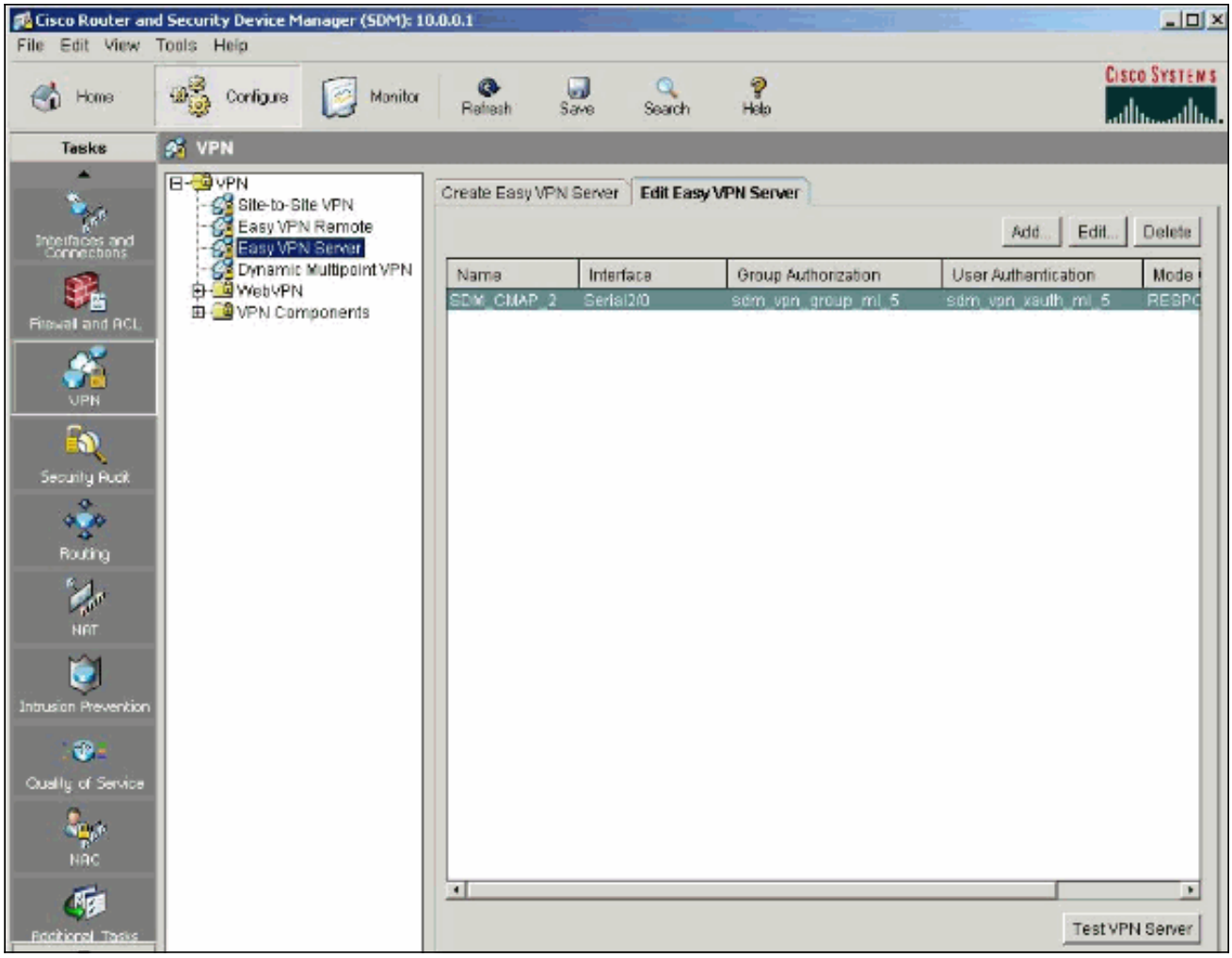



11. Questa finestra mostra un riepilogo delle azioni intraprese. Se la configurazione è soddisfacente, fare clic su
**Fine**.




12. Il modulo SDM invia la configurazione al router per aggiornare la configurazione in esecuzione. Fare clic su **OK** per completare l'operazione.

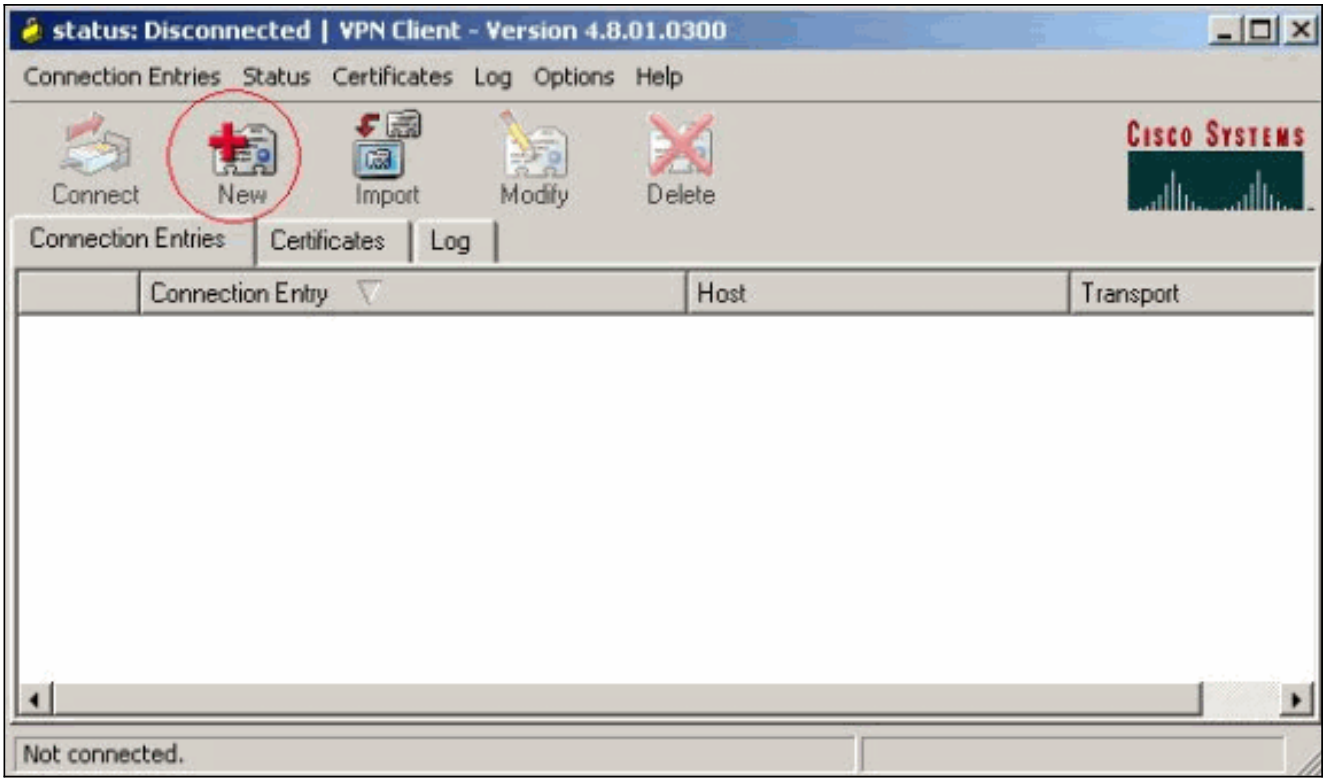

13. Al termine, è possibile modificare le modifiche apportate alla configurazione, se necessario.



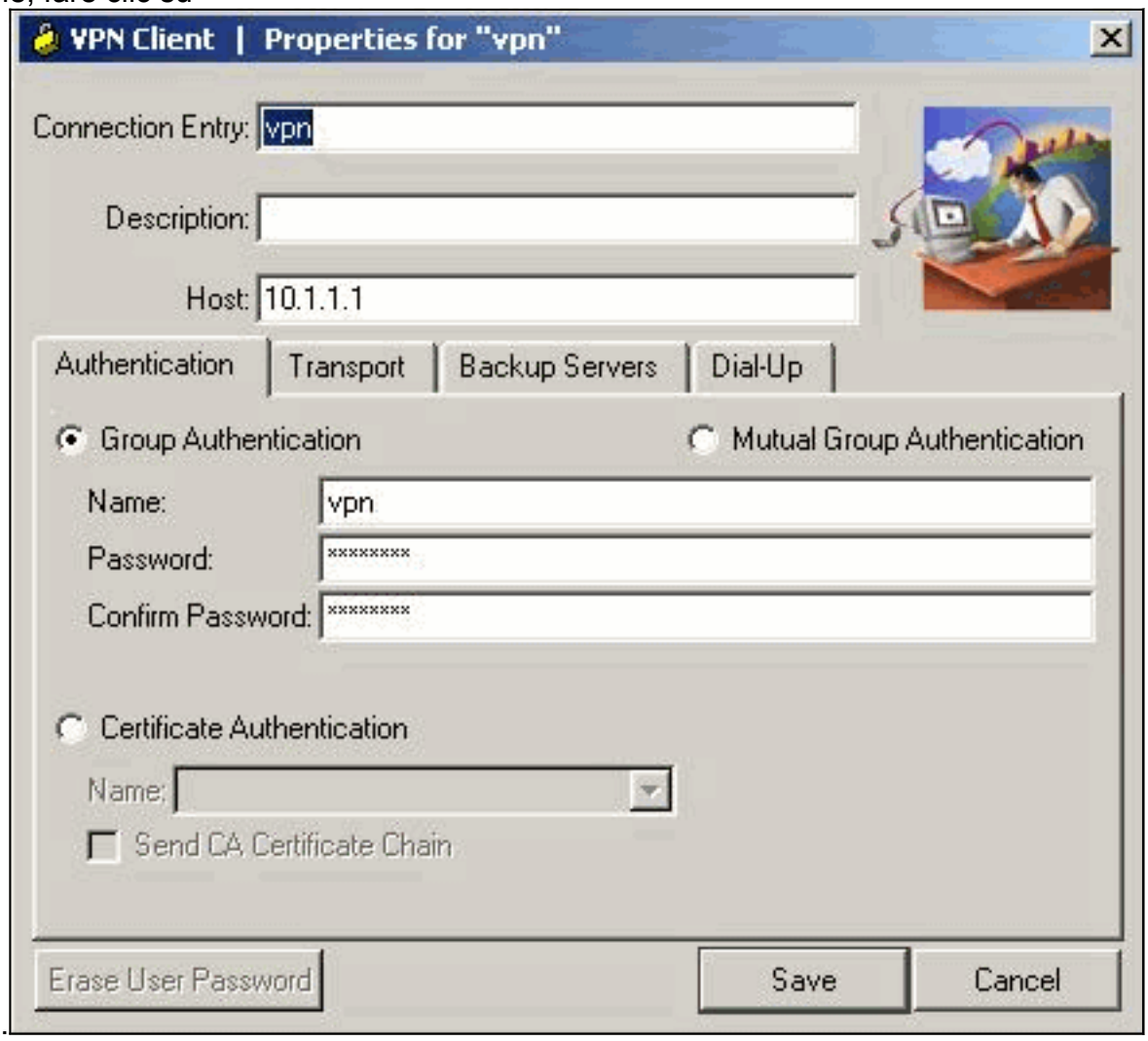

## Verifica

Tentare di connettersi al router Cisco utilizzando il client VPN Cisco per verificare che il router Cisco sia configurato correttamente.

1. Selezionare **Voci di connessione > Nuovo**.



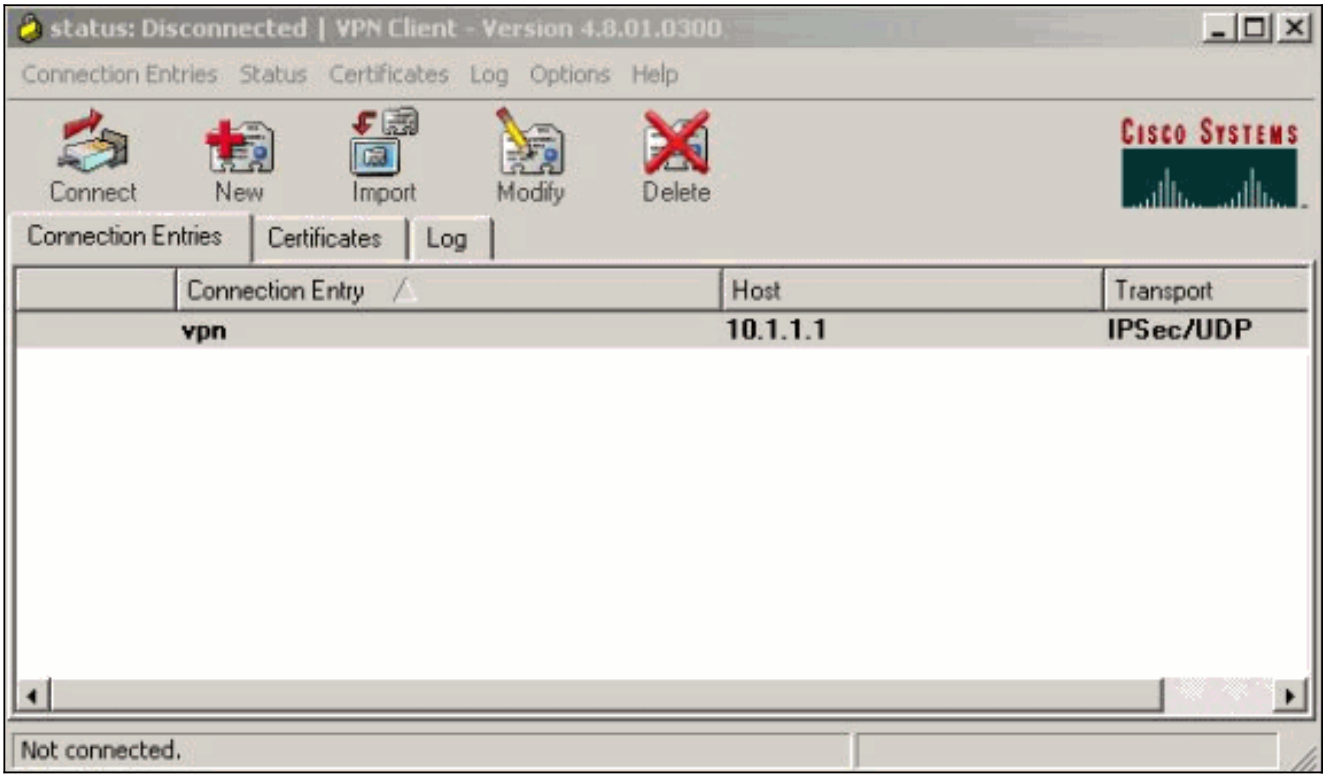

2. Specificare i dettagli della nuova connessione.Il campo Host deve contenere l'indirizzo IP o il nome host dell'endpoint del tunnel di Easy VPN Server (router Cisco). Le informazioni di autenticazione del gruppo devono corrispondere a quelle utilizzate nel passaggio 9. Al termine, fare clic su



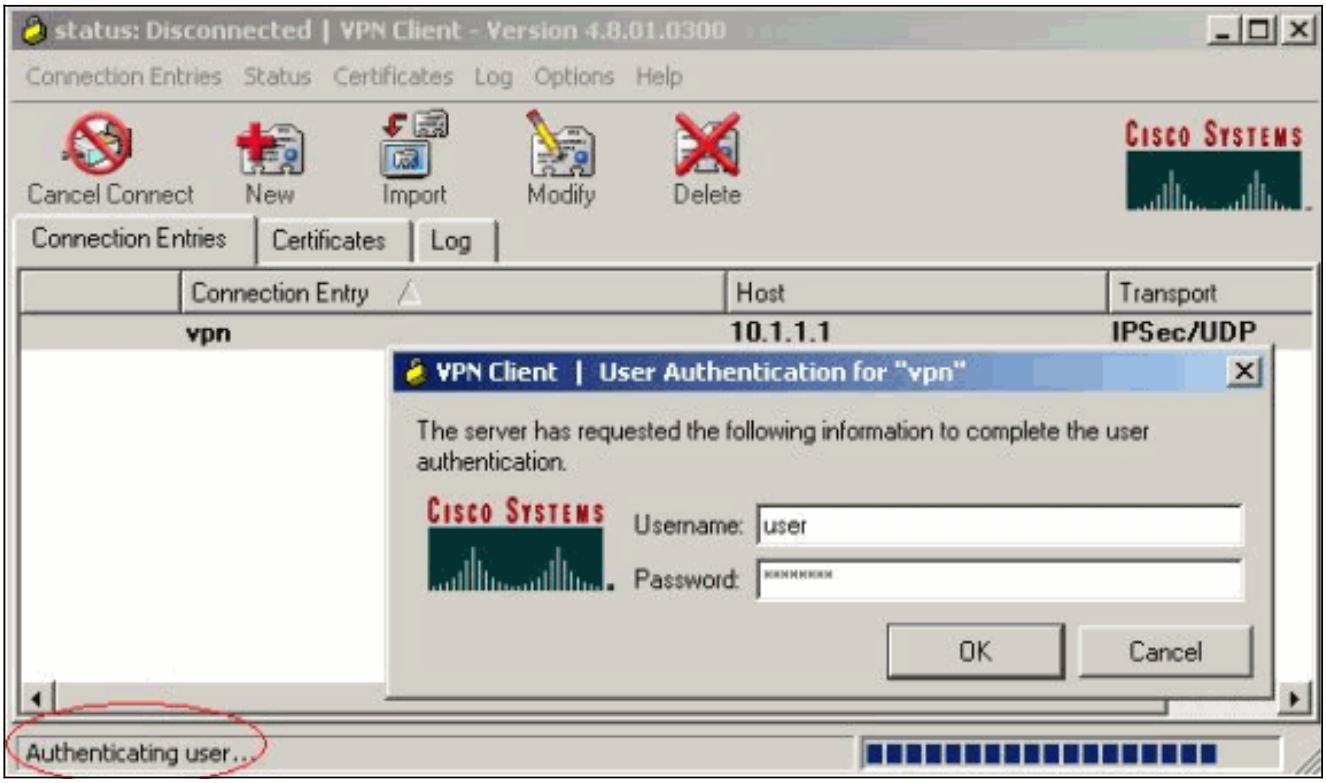

**Salva**.

3. Selezionare la connessione appena creata e fare clic su

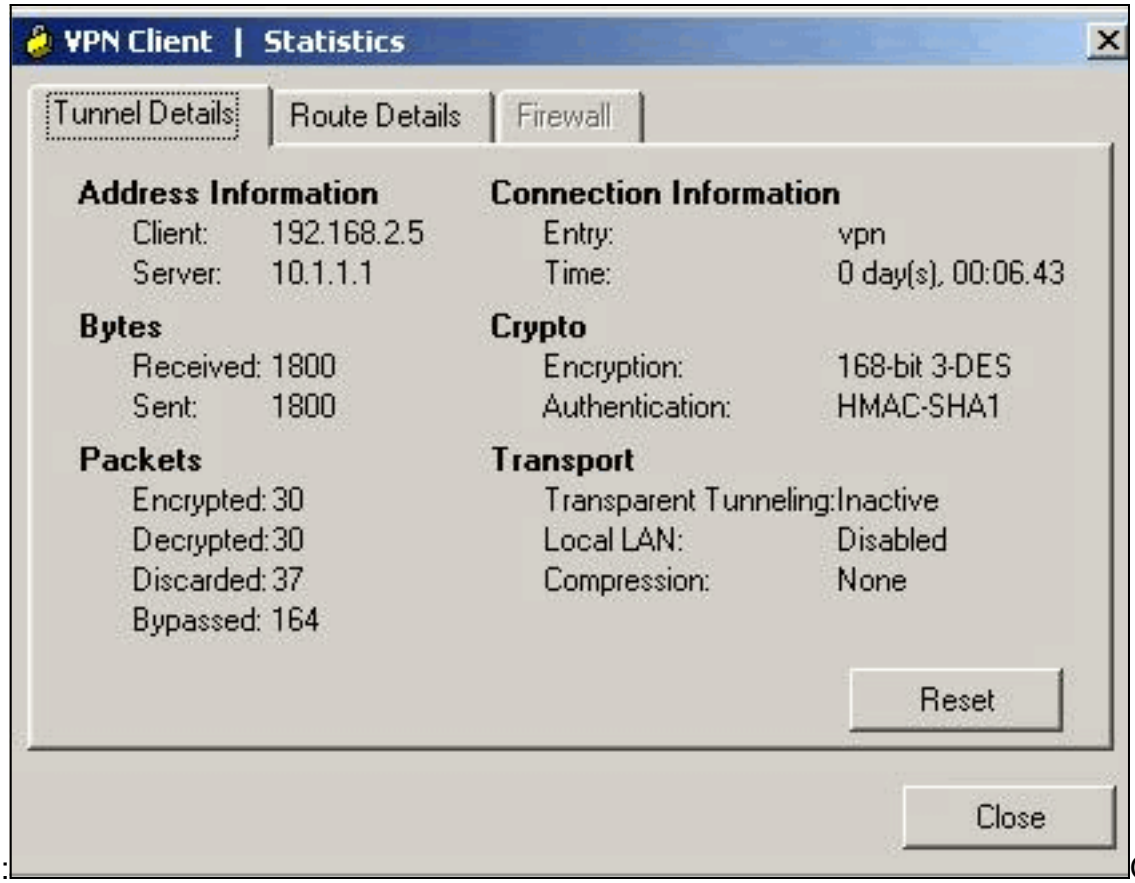
Connetti.




4. Immettere un nome utente e una password per l'autenticazione estesa (Xauth). Queste informazioni sono determinate dai parametri Xauth nel passaggio 7.

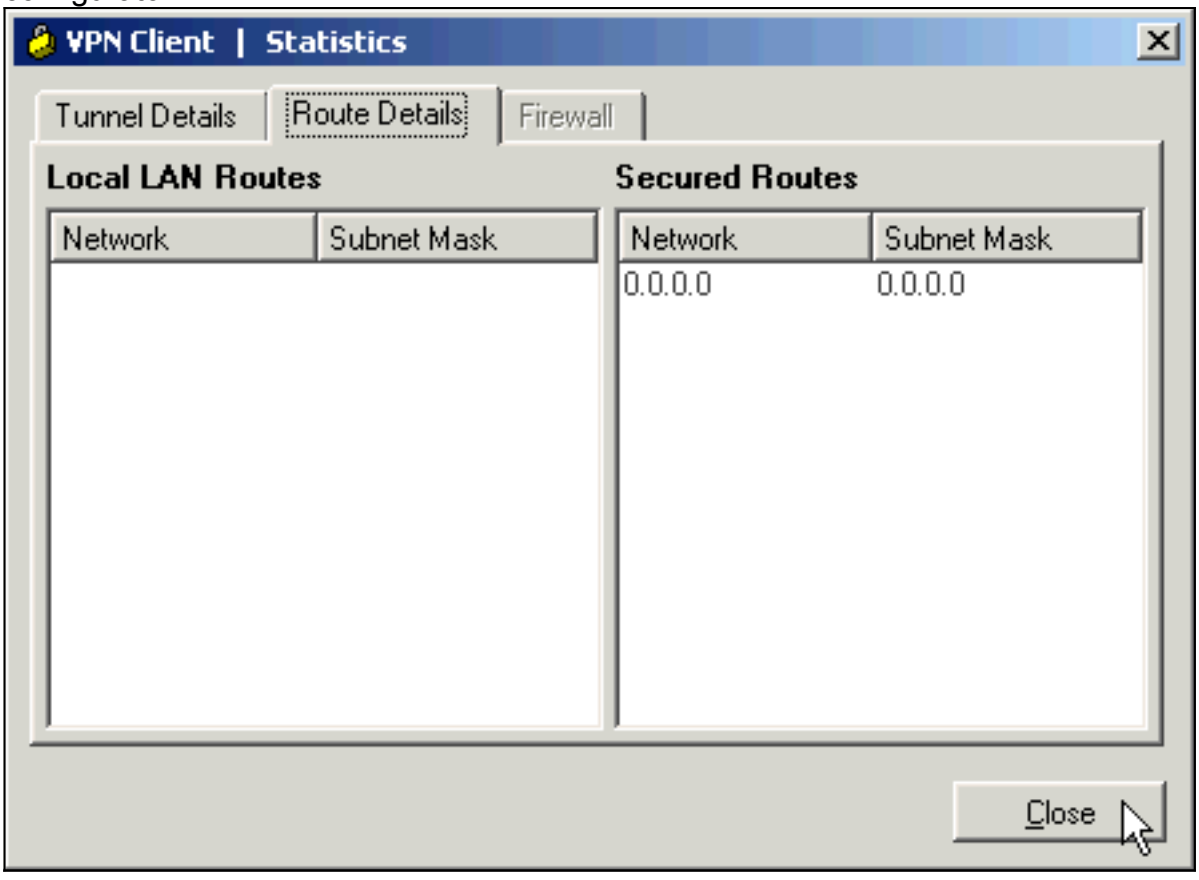



5. Una volta stabilita la connessione, selezionare **Statistics** dal menu Status per verificare i dettagli del tunnel.In questa finestra vengono visualizzate le informazioni sul traffico e sulla

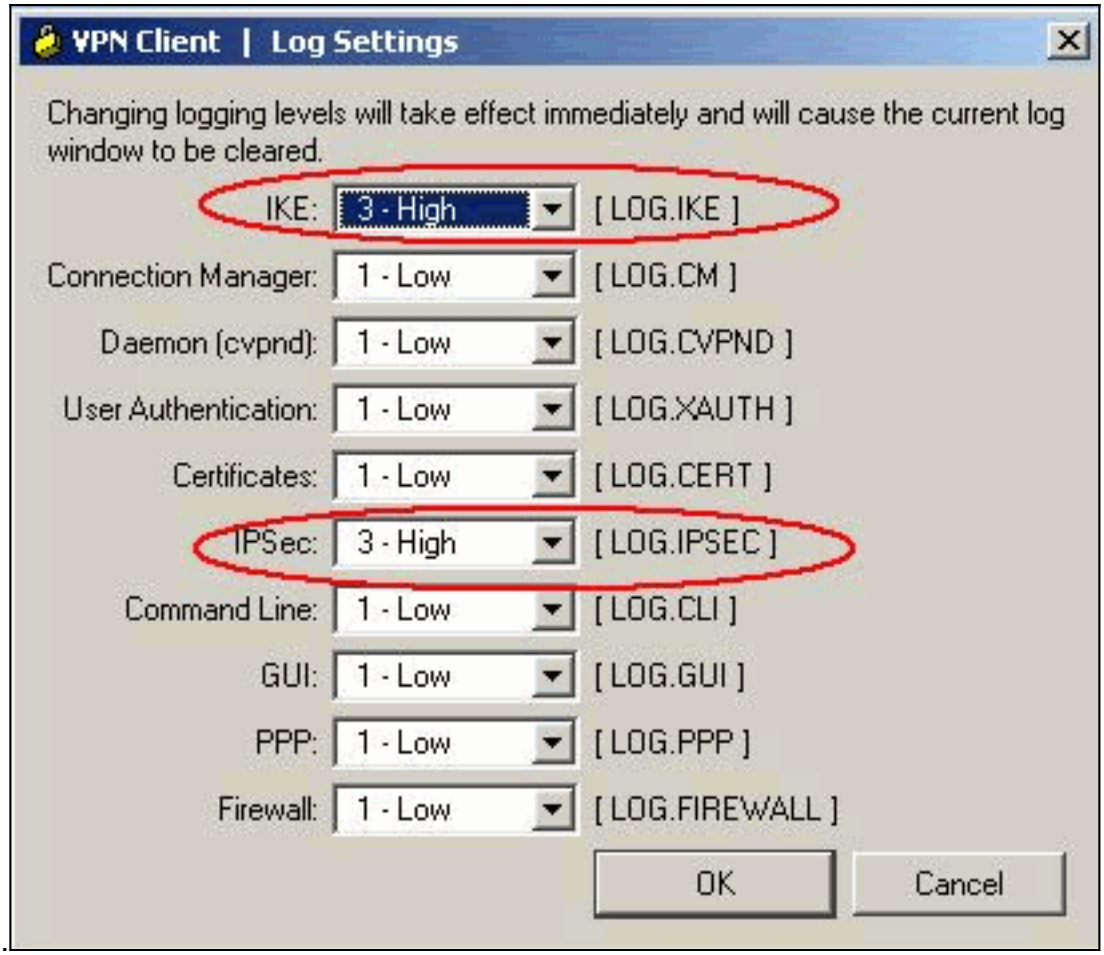



crittografia:Q

uesta finestra mostra le informazioni sul tunneling suddiviso, se configurato:



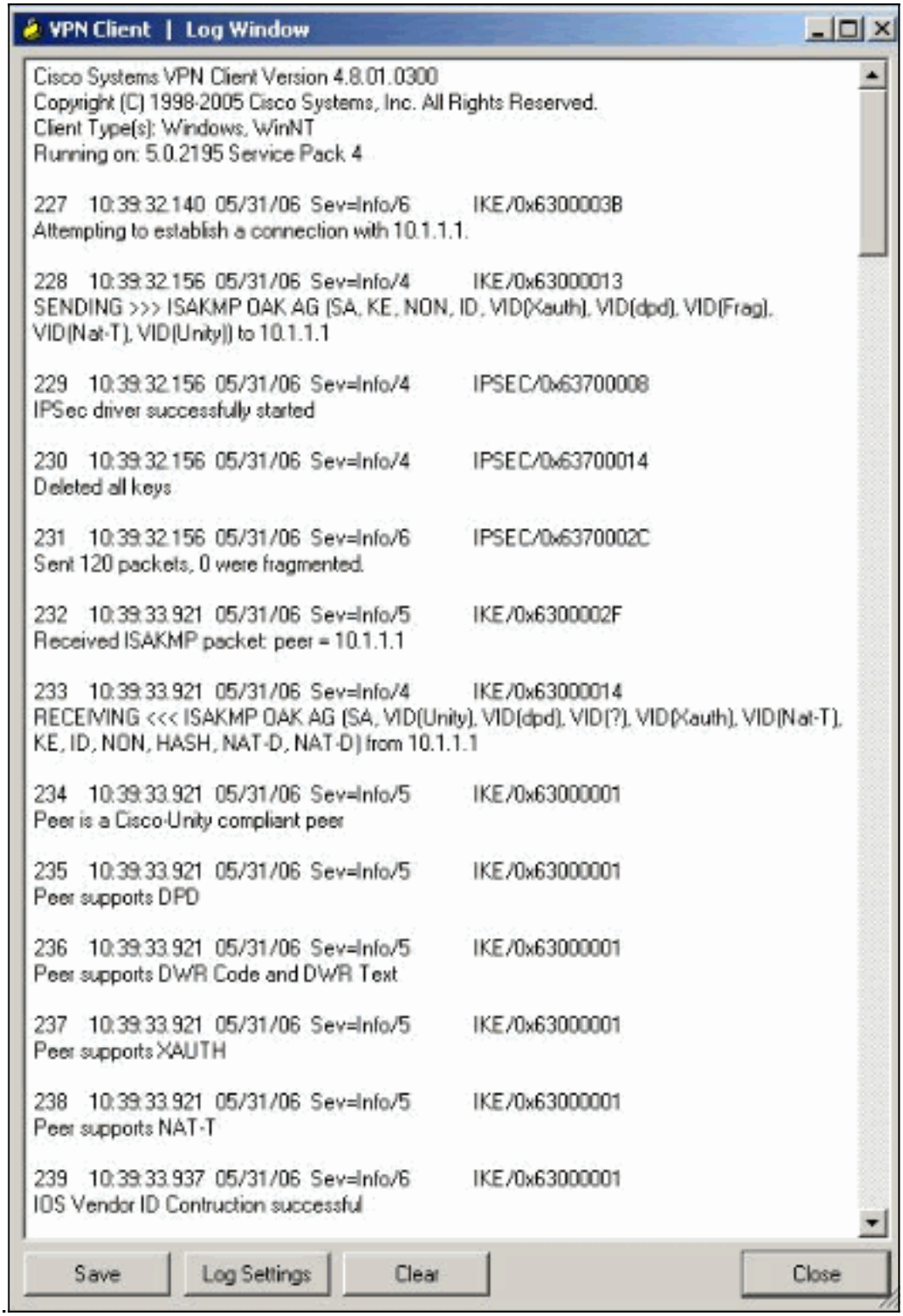

6. Selezionare **Log > Log Settings** per abilitare i livelli di log nel client VPN




Cisco.

7. Selezionare **Log > Log Windows** per visualizzare le voci di log nel client VPN

Cisco.




# Informazioni correlate

- Download e installazione di Cisco Router and Security Device Manager
- Pagina di supporto per Cisco VPN Client
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems