Cisco Router als Remote-VPN-Server mit SDM-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Cisco Security Device Manager (SDM) zum Konfigurieren des Cisco Routers als Easy VPN-Server verwendet wird. Mit Cisco SDM können Sie Ihren Router als VPN-Server für den Cisco VPN Client über eine benutzerfreundliche webbasierte Verwaltungsschnittstelle konfigurieren. Sobald die Konfiguration des Cisco Routers abgeschlossen ist, kann sie mit dem Cisco VPN Client verifiziert werden.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass der Cisco Router voll betriebsbereit und so konfiguriert ist, dass das Cisco SDM Konfigurationsänderungen vornehmen kann.

Hinweis: Informationen zur Konfiguration des Routers durch das SDM finden Sie unter Zulassen von HTTPS-Zugriff für SDM.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco 3640 Router mit Cisco IOS® Software, Version 12.3(14T)
- Security Device Manager Version 2.31
- Cisco VPN Client Version 4.8

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

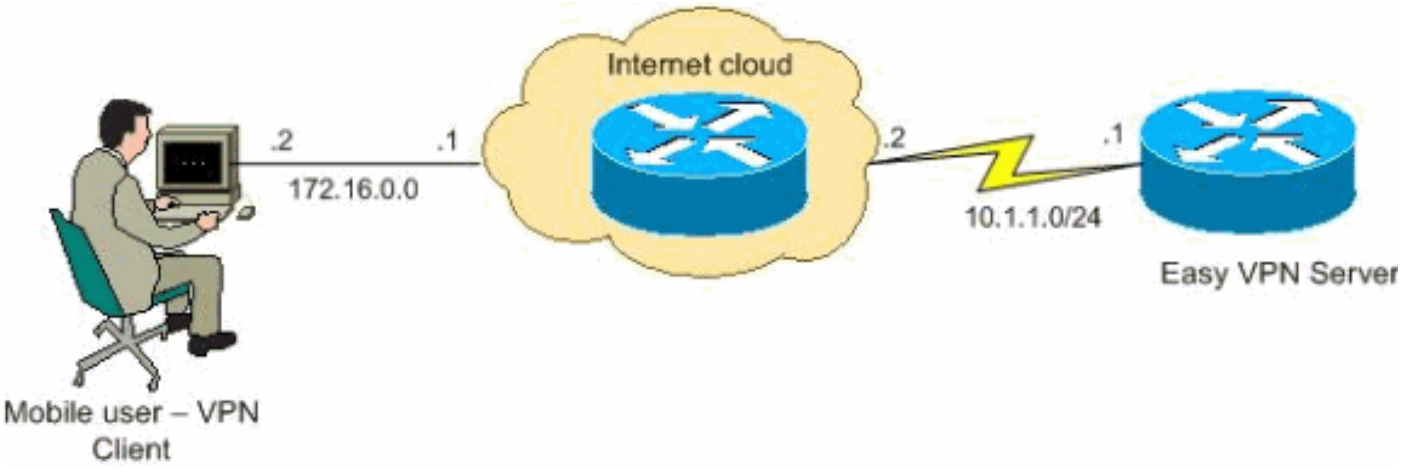
Konfigurieren

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der Easy VPN Server-Funktion, mit der ein Remote-Endbenutzer über IPsec mit einem beliebigen Cisco IOS® VPN-Gateway kommunizieren kann.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

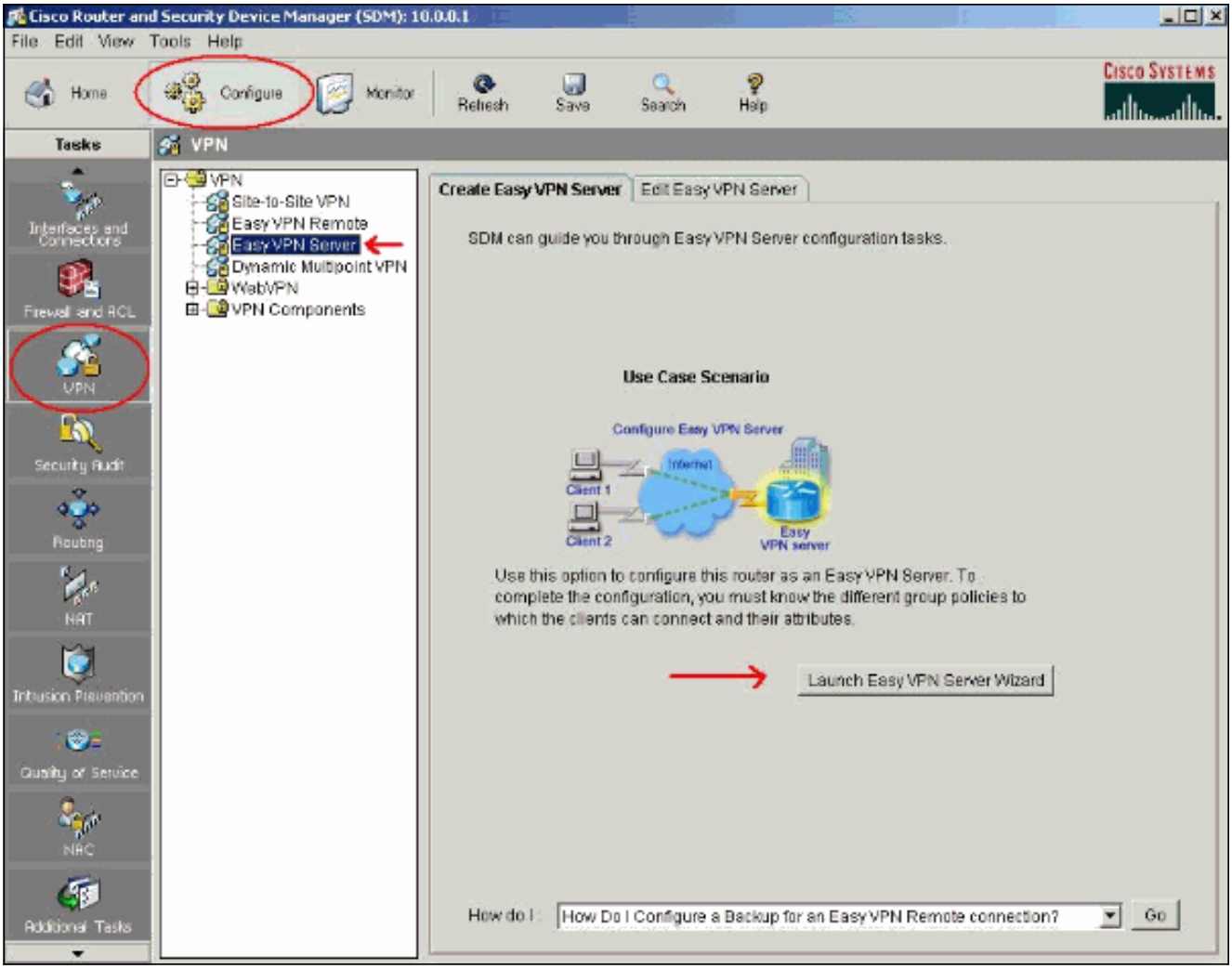
In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



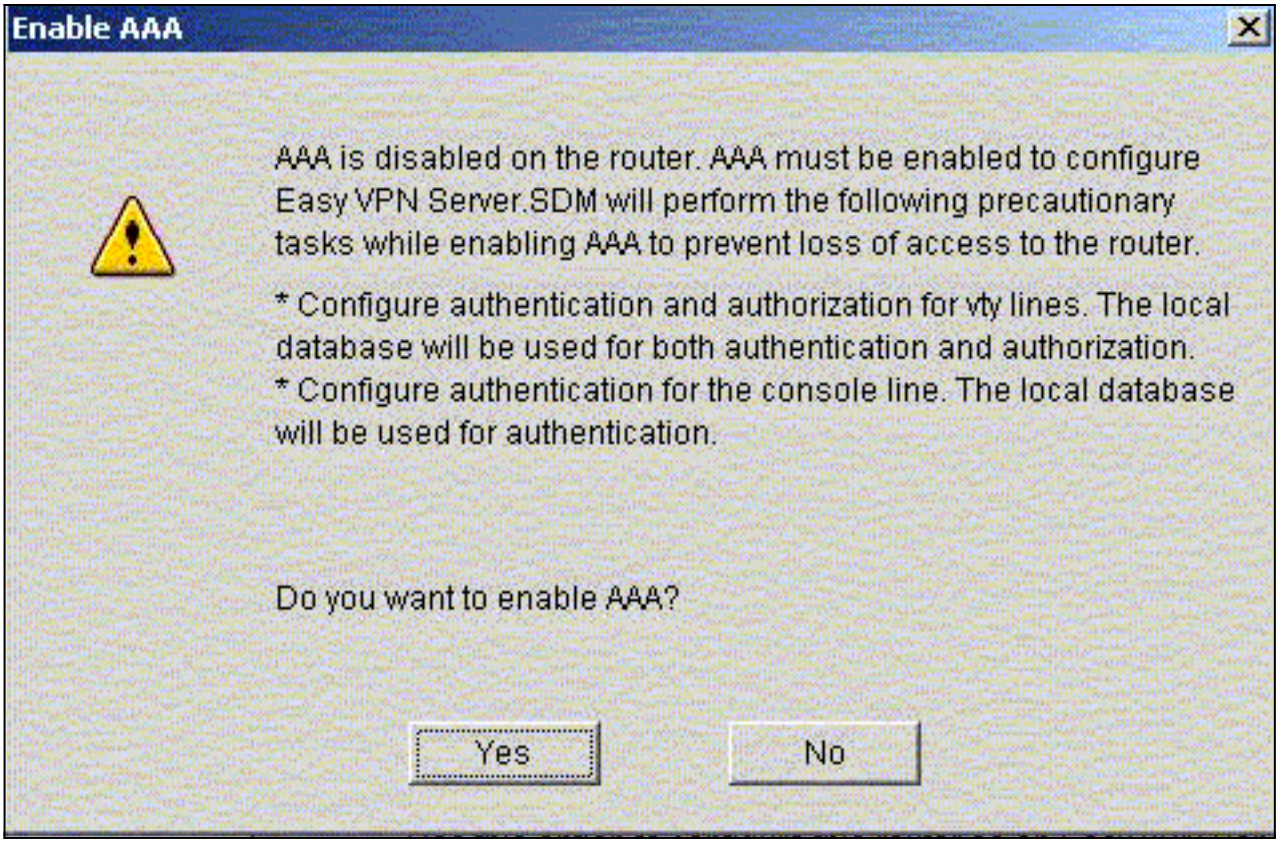
Konfigurationsverfahren

Führen Sie diese Schritte aus, um den Cisco Router mithilfe von SDM als Remote-VPN-Server zu konfigurieren.

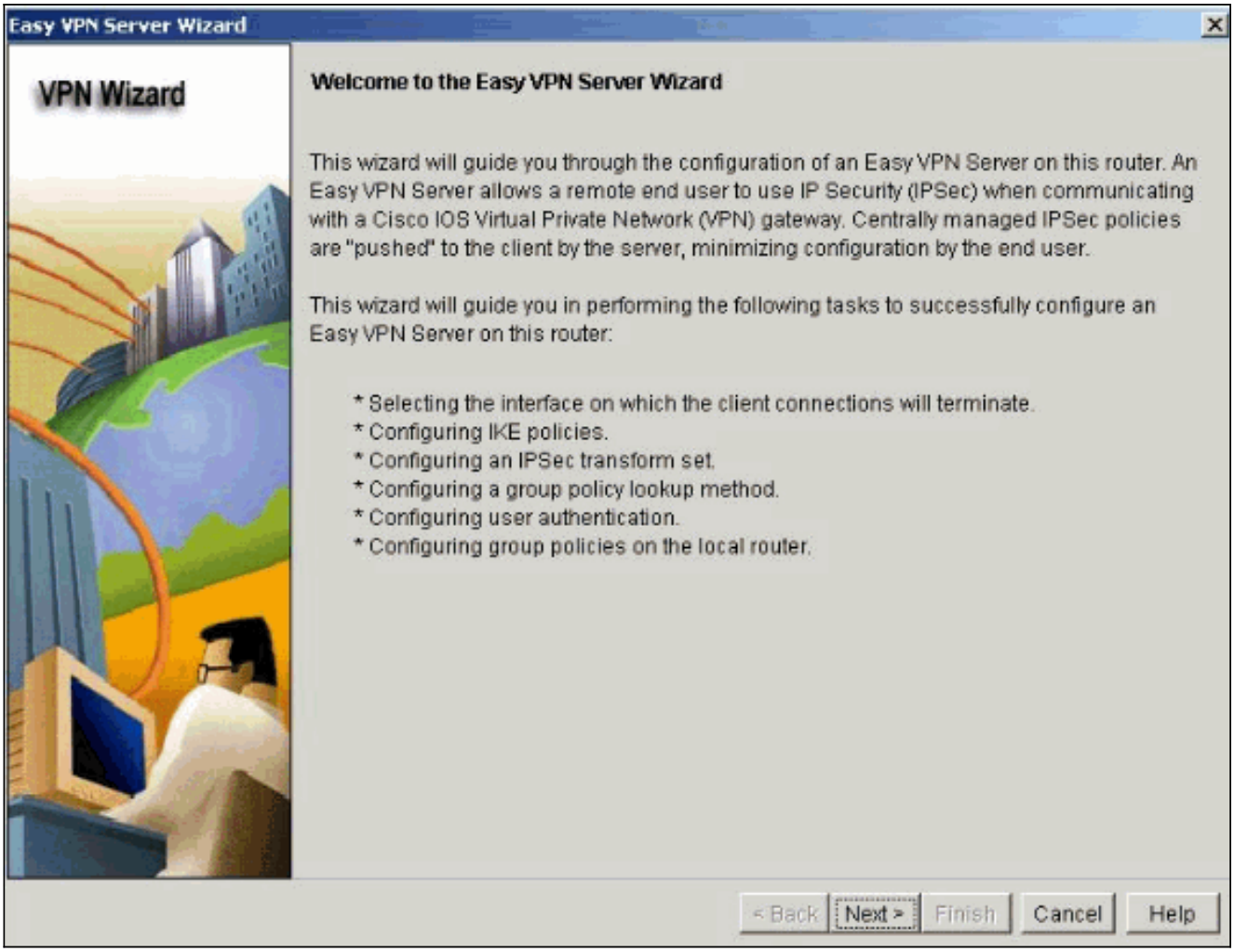
1. Wählen Sie **Configure > VPN > Easy VPN Server** im Home-Fenster aus, und klicken Sie auf **Easy VPN Server Wizard**.



2. AAA muss auf dem Router aktiviert werden, bevor die Konfiguration des Easy VPN-Servers beginnt. Klicken Sie auf **Ja**, um mit der Konfiguration fortzufahren.Die Meldung "AAA wurde erfolgreich auf dem Router aktiviert" wird im Fenster angezeigt. Klicken Sie auf **OK**, um die Konfiguration des Easy VPN-Servers zu starten.

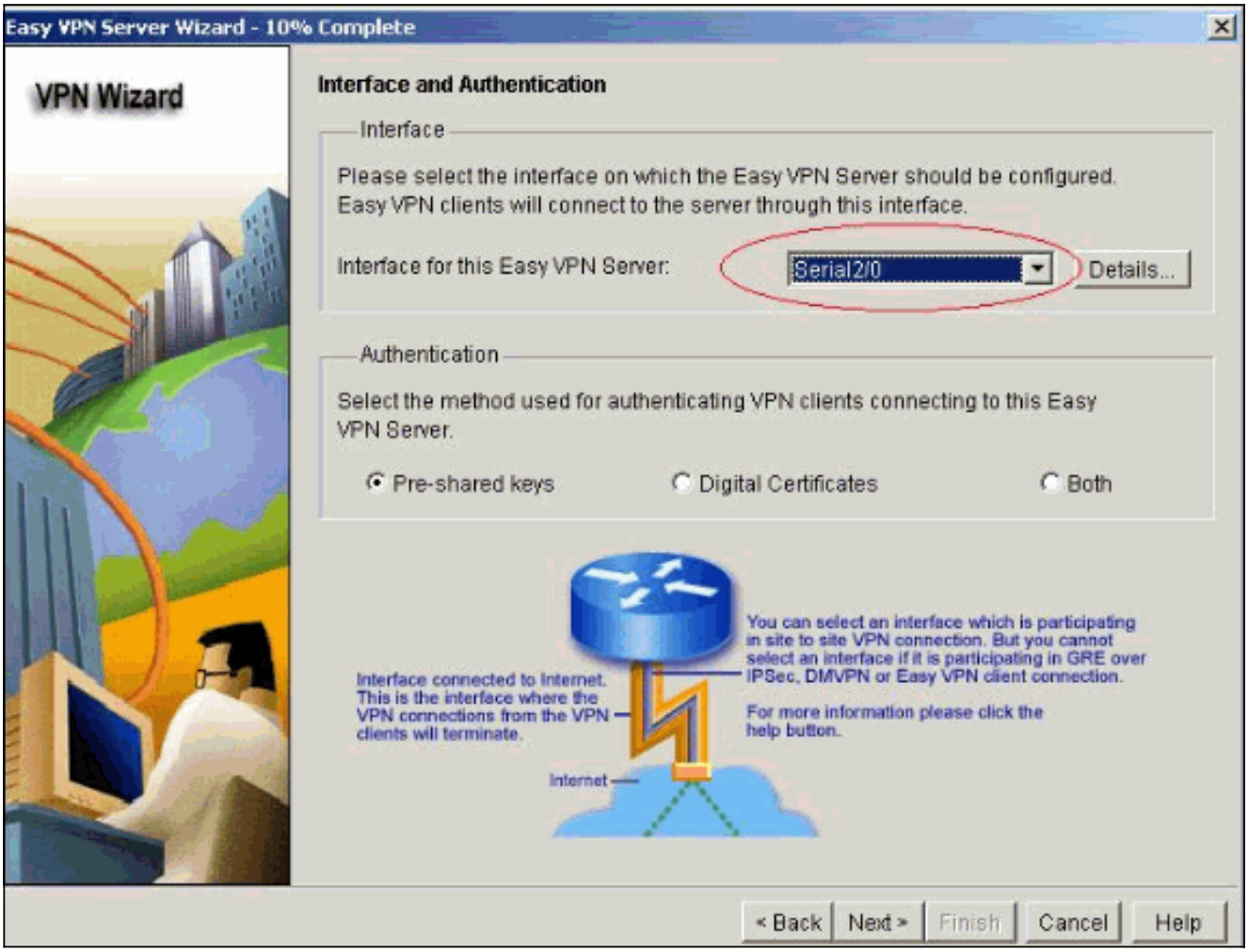


3. Klicken Sie auf **Weiter**, um den Easy VPN Server-Assistenten zu starten.

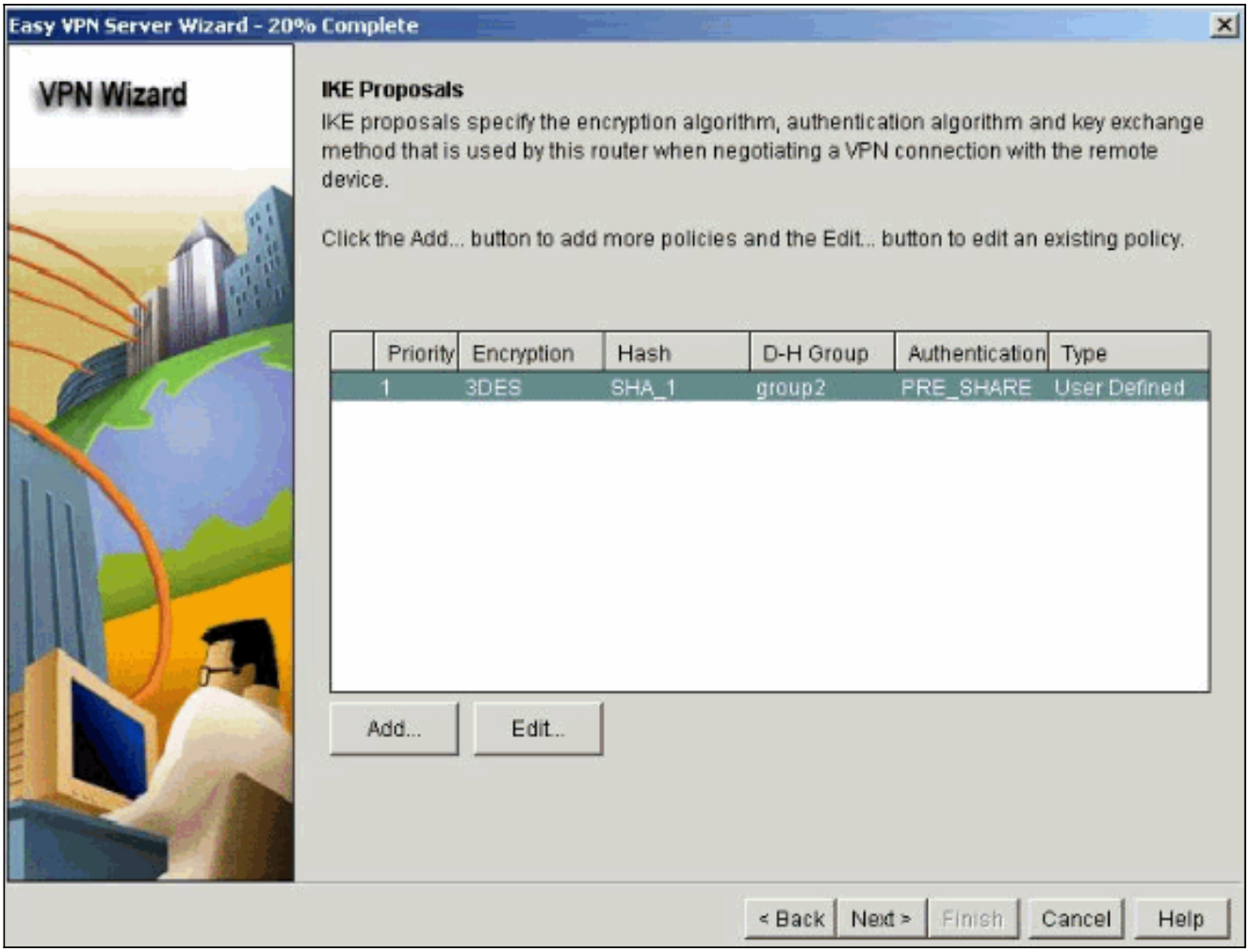


4. Wählen Sie die Schnittstelle, auf der die Clientverbindungen enden, und den Authentifizierungstyp

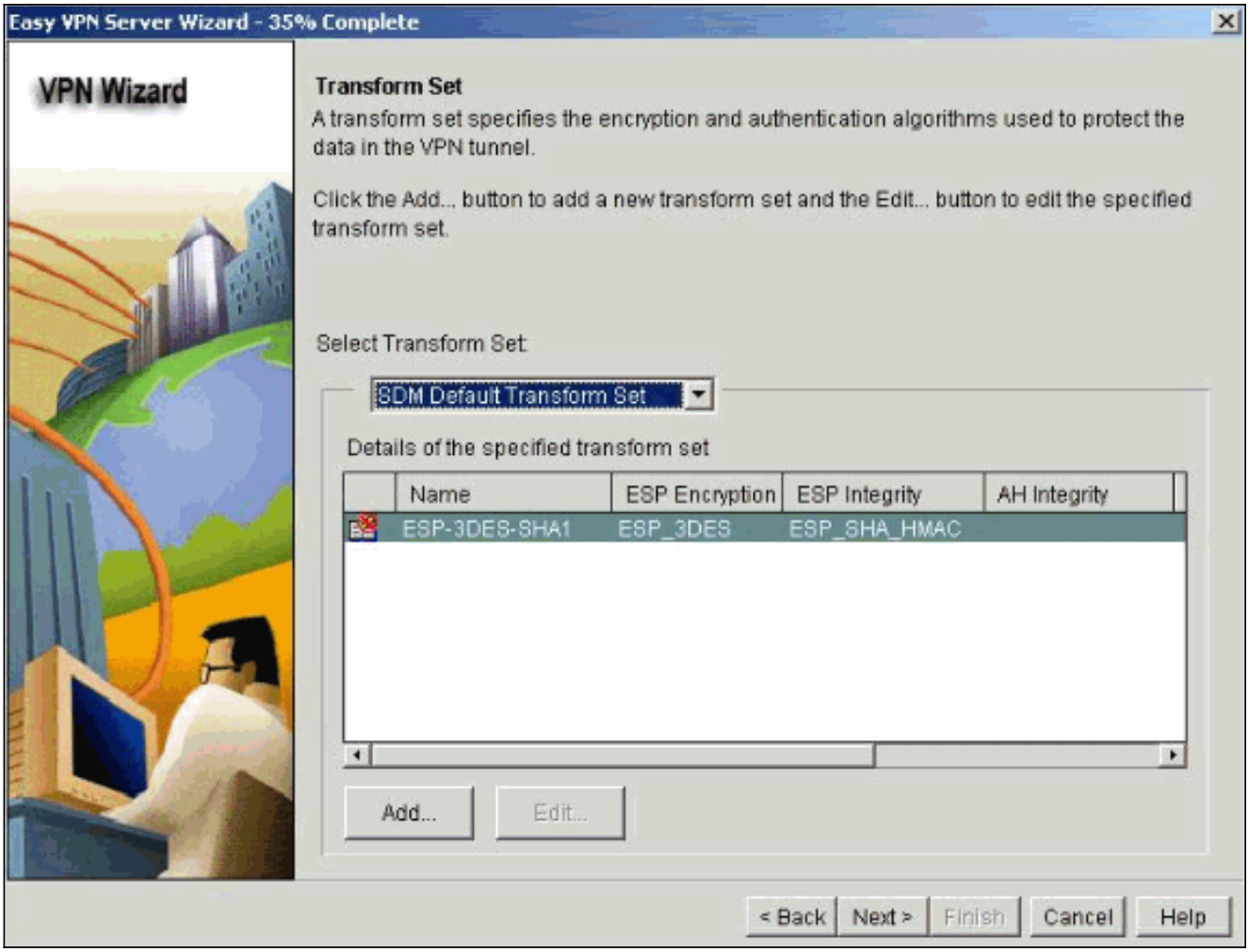
aus.



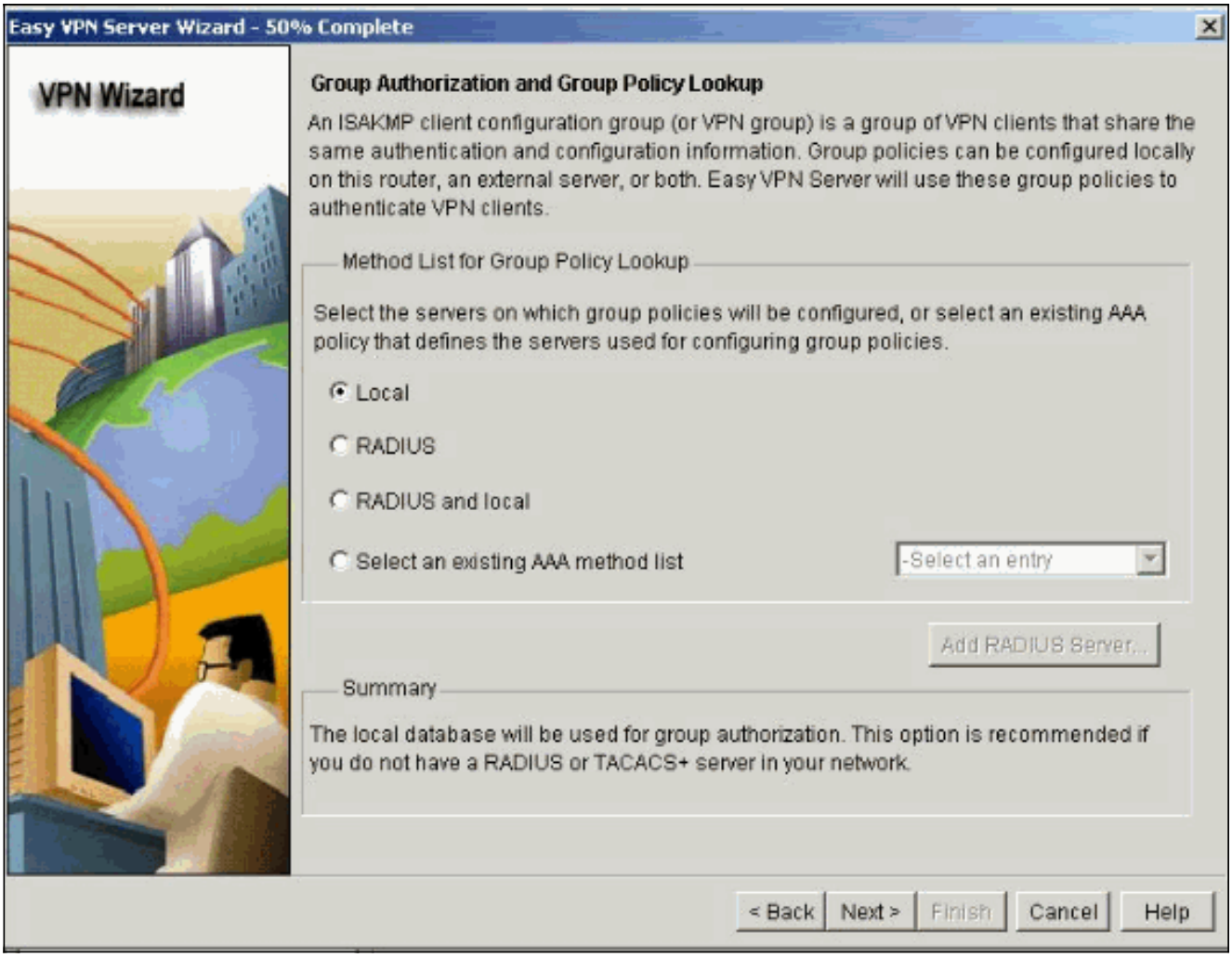
5. Klicken Sie auf **Weiter**, um die IKE-Richtlinien (Internet Key Exchange) zu konfigurieren, und verwenden Sie die Schaltfläche **Hinzufügen**, um die neue Richtlinie zu erstellen.Konfigurationen auf beiden Seiten des Tunnels müssen genau übereinstimmen. Der Cisco VPN Client wählt jedoch automatisch die richtige Konfiguration für sich aus. Daher ist auf dem Client-PC keine IKE-Konfiguration
erforderlich.



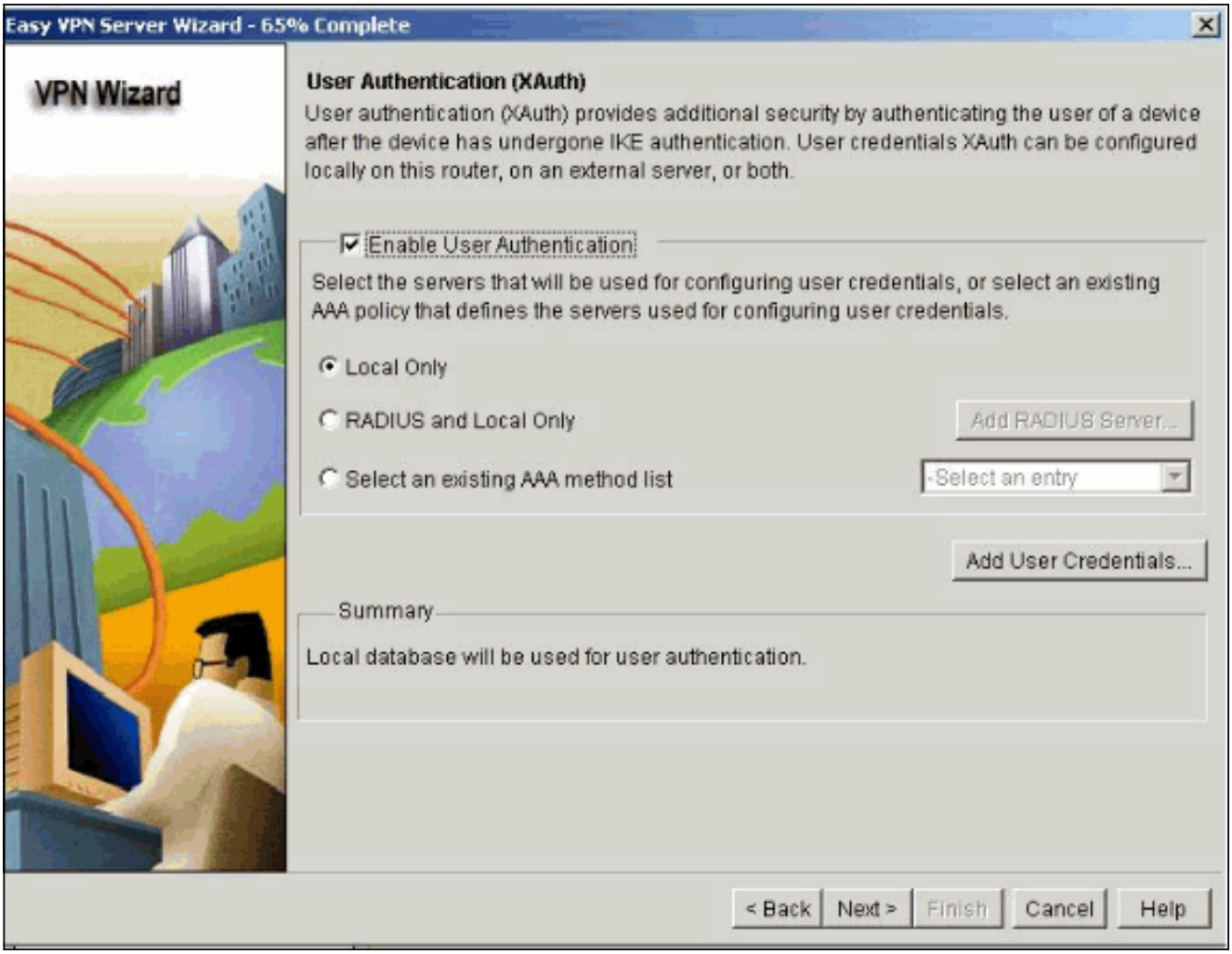
6. Klicken Sie auf **Weiter**, um den Standard-Transformationssatz auszuwählen, oder fügen Sie den neuen Transformationssatz hinzu, um den Verschlüsselungs- und Authentifizierungsalgorithmus anzugeben. In diesem Fall wird der Standard-Transformationssatz
verwendet.



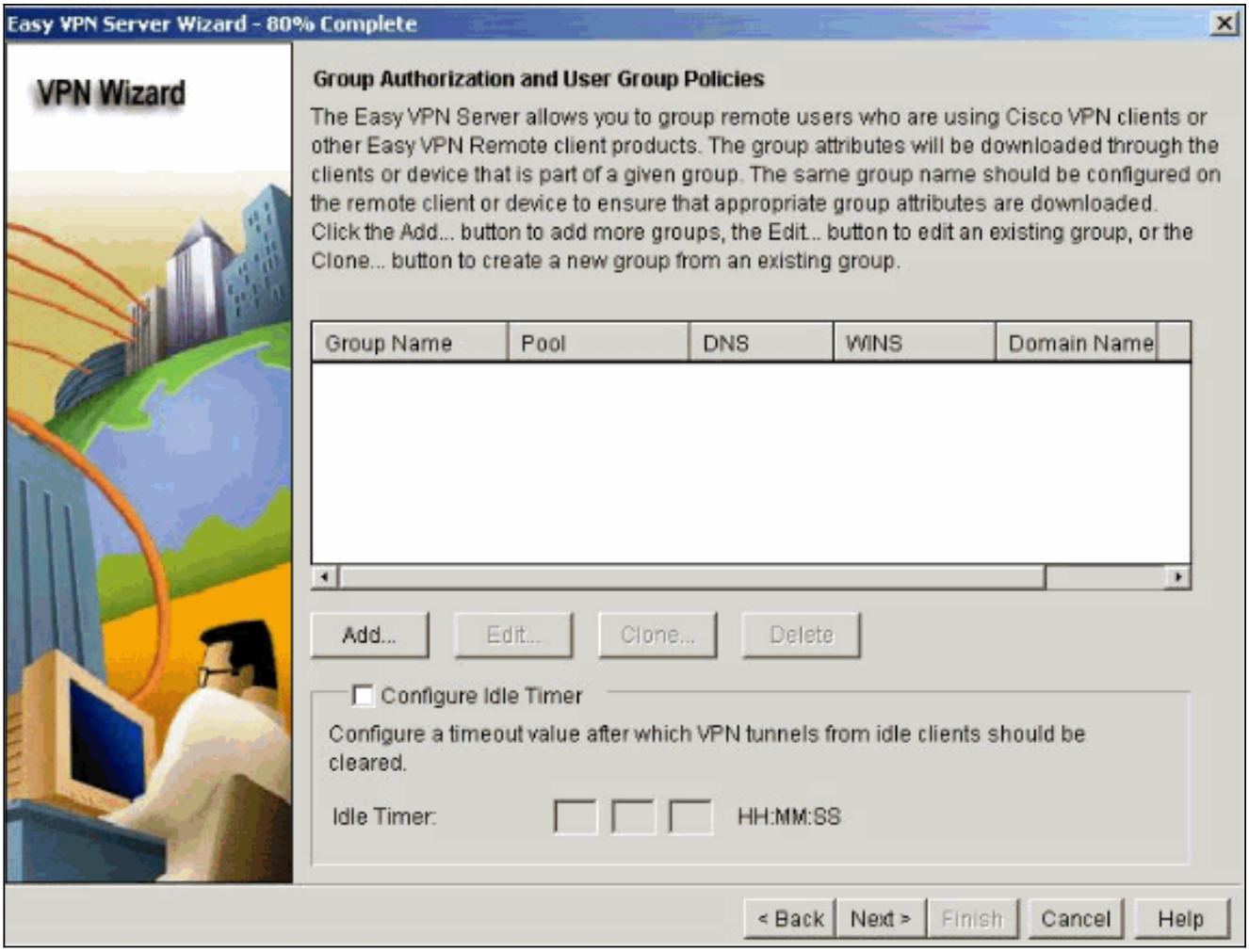
7. Klicken Sie auf **Weiter**, um eine neue Authentifizierungs-, Autorisierungs- und Abrechnungsnetzwerkmethodenliste (Authentication, Authorization, Accounting - AAA) für die Gruppenrichtliniensuche zu erstellen, oder um eine vorhandene Netzwerkmethodenliste für die Gruppenautorisierung
auszuwählen.



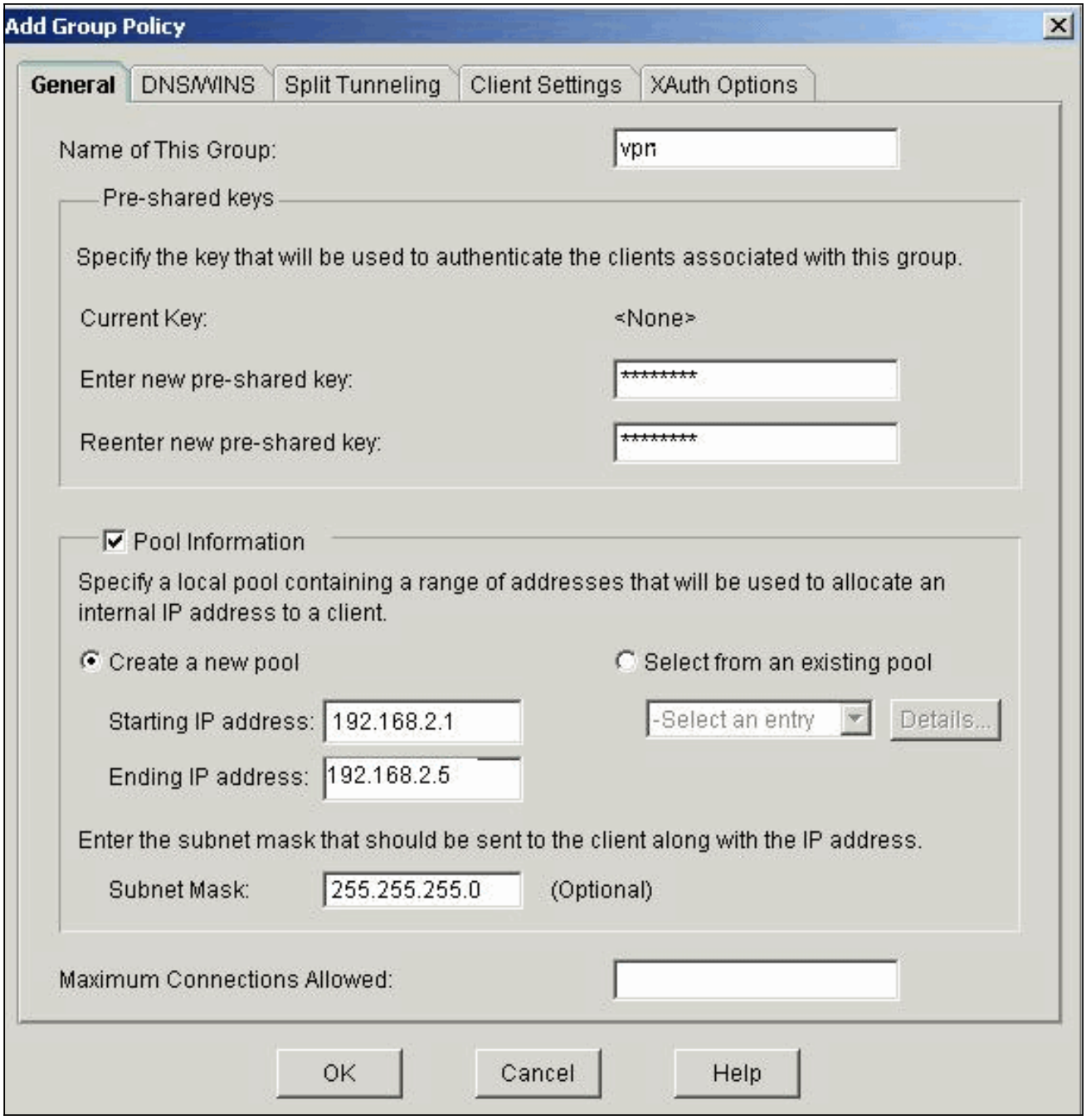
8. Konfigurieren Sie die Benutzerauthentifizierung auf dem Easy VPN-Server.Sie können Benutzerauthentifizierungsdetails auf einem externen Server, z. B. einem RADIUS-Server, einer lokalen Datenbank oder auf beiden speichern. Eine Liste mit AAA-Authentifizierungsmethoden wird verwendet, um die Reihenfolge festzulegen, in der die Benutzerauthentifizierungsdetails durchsucht werden
sollen.



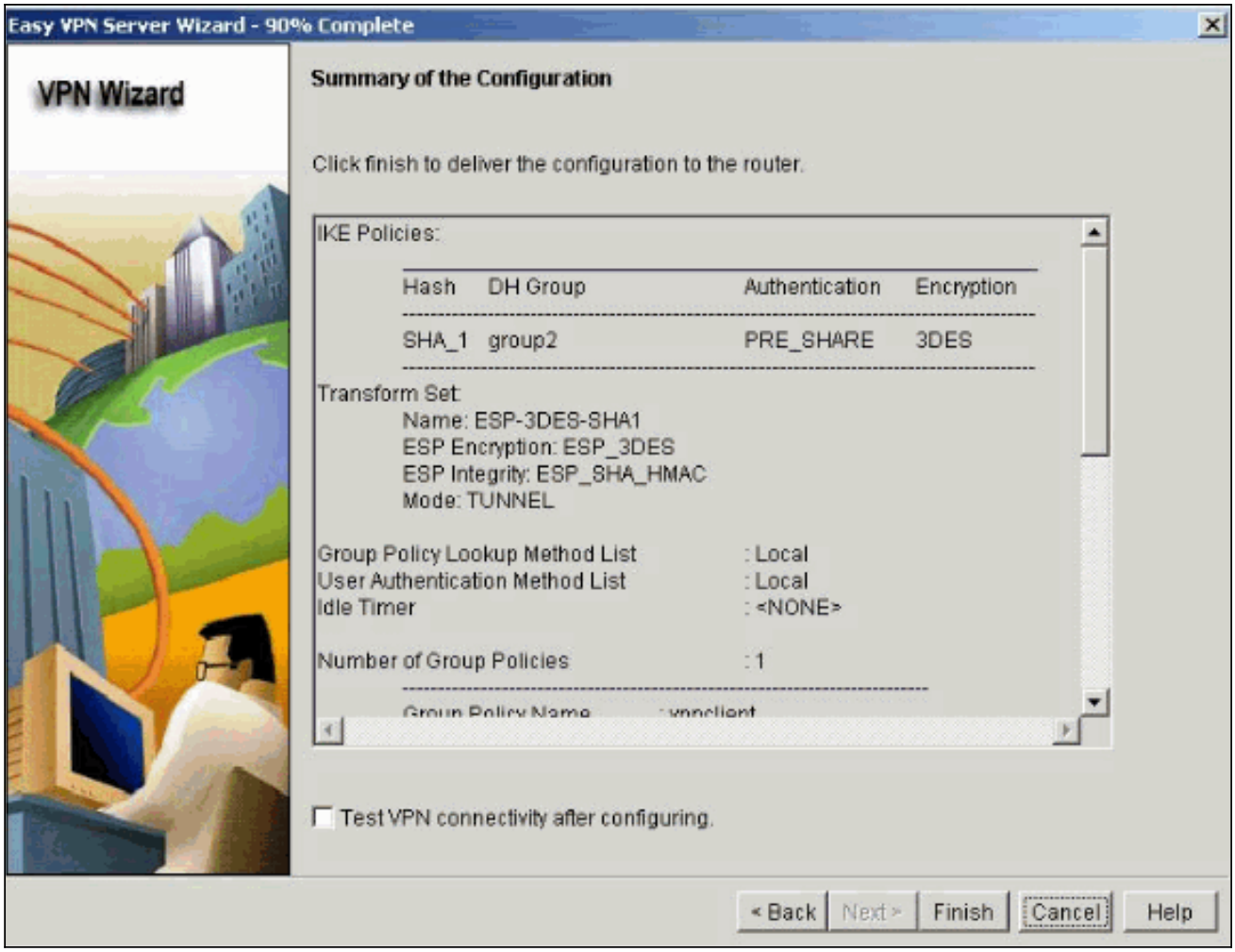
9. In diesem Fenster können Sie Benutzergruppenrichtlinien in der lokalen Datenbank hinzufügen, bearbeiten, klonen oder
löschen.



10. Geben Sie einen Namen für den Tunnelgruppennamen ein. Geben Sie den für die Authentifizierungsinformationen verwendeten vorinstallierten Schlüssel an.Erstellen Sie einen neuen Pool, oder wählen Sie einen vorhandenen Pool aus, aus dem die IP-Adressen den VPN-Clients zugewiesen
    werden.

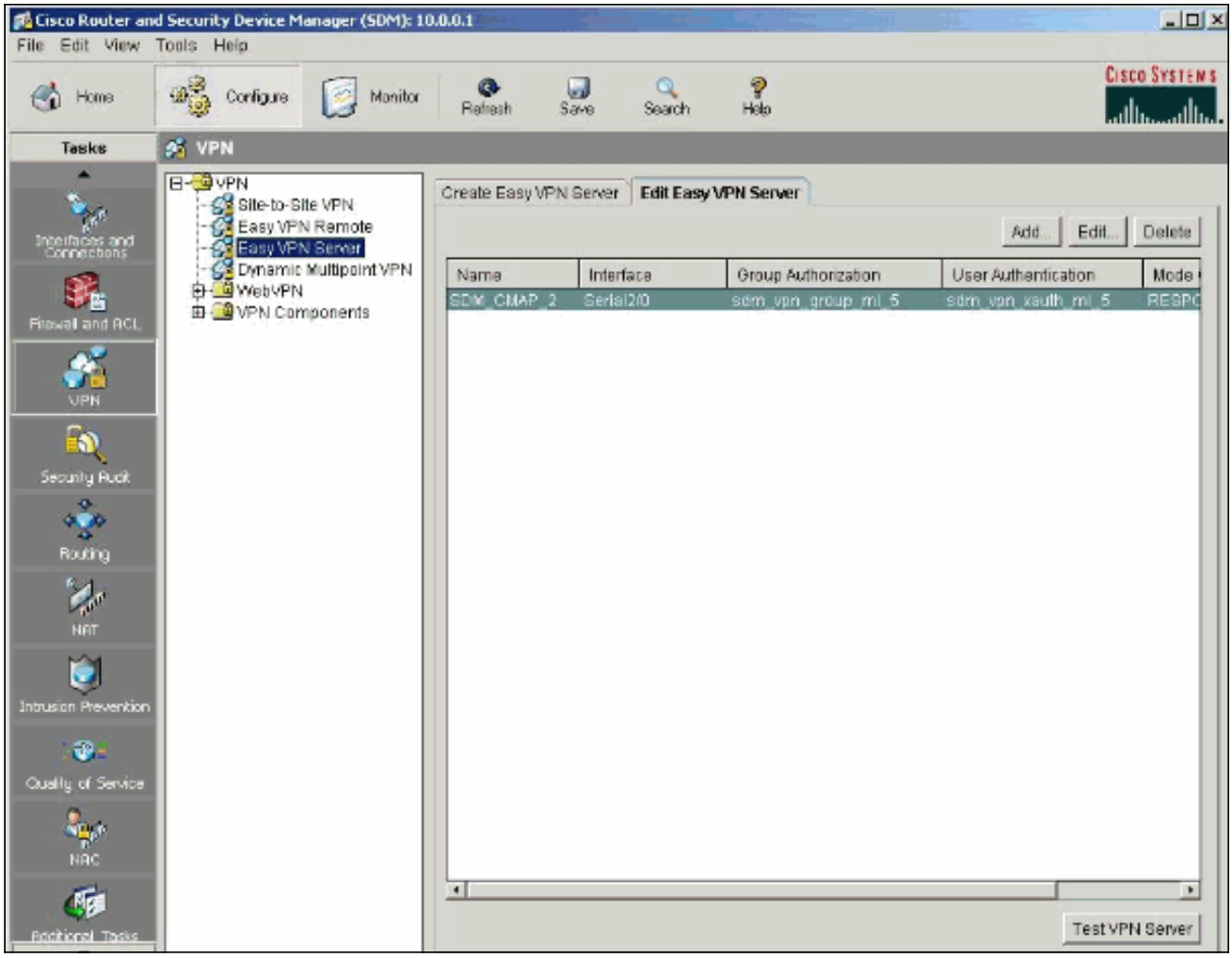


11. In diesem Fenster wird eine Zusammenfassung der von Ihnen ergriffenen Maßnahmen angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie mit Ihrer Konfiguration zufrieden sind.



12. Das SDM sendet die Konfiguration an den Router, um die aktuelle Konfiguration zu aktualisieren. Klicken Sie zum Abschließen auf OK.

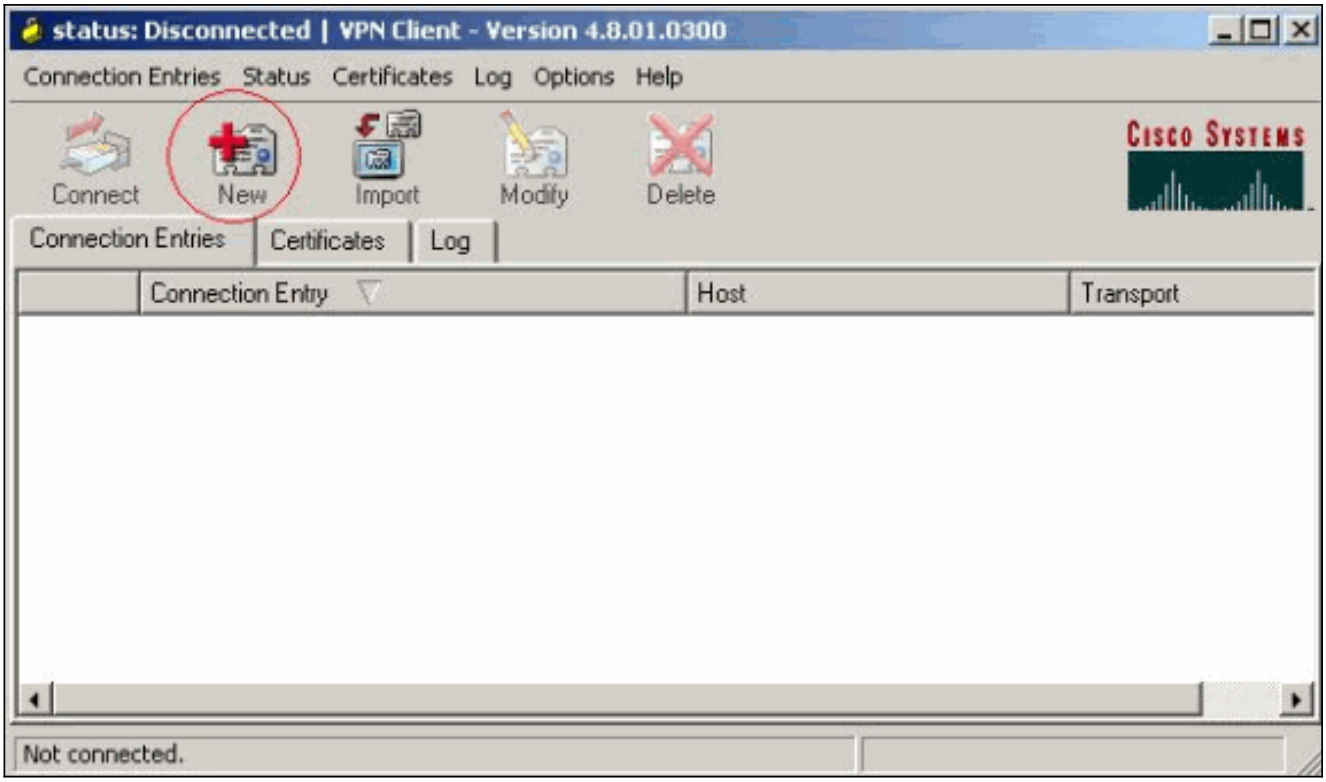
13. Nach Abschluss können Sie die Änderungen in der Konfiguration bei Bedarf bearbeiten und ändern.



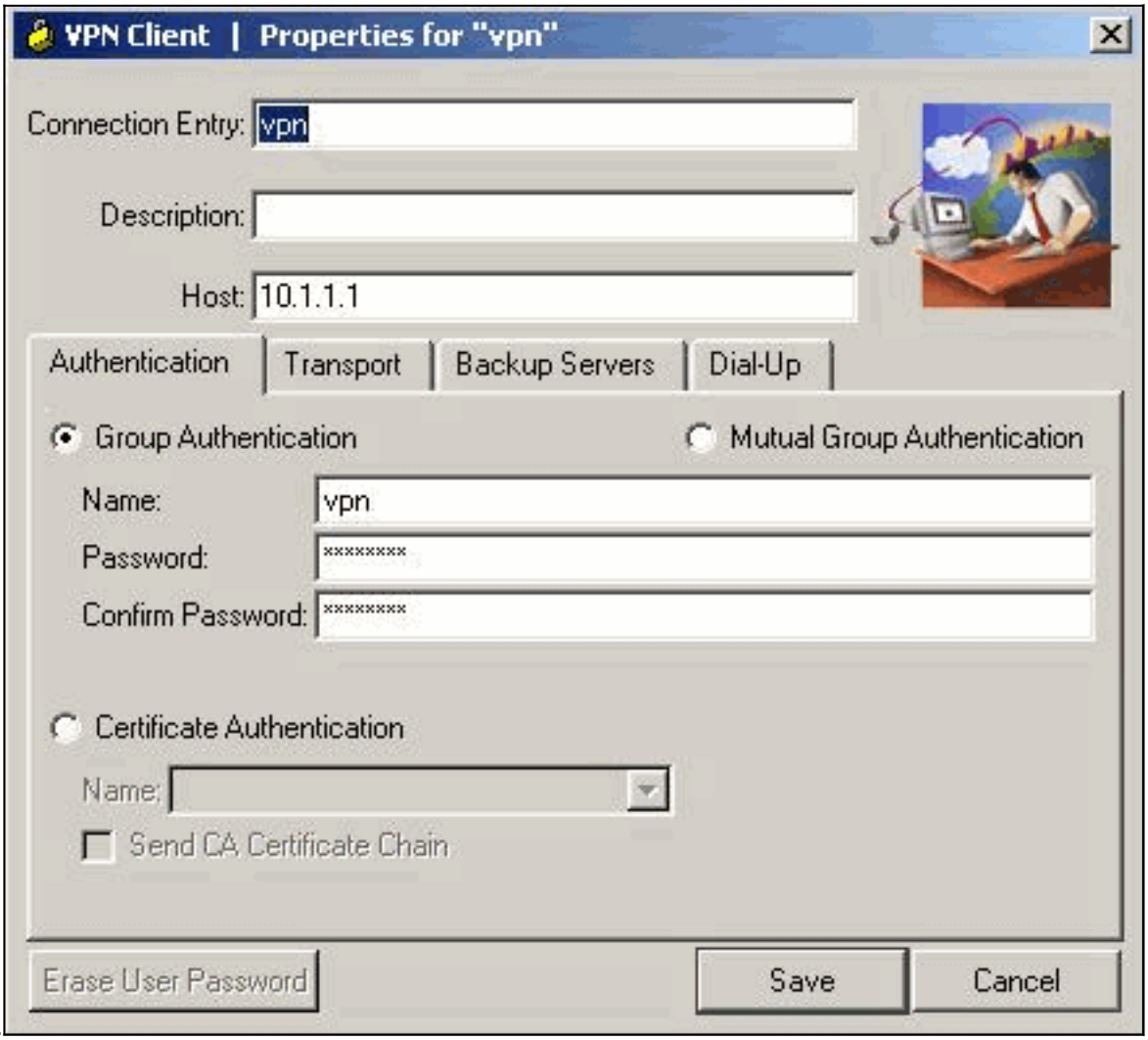
Überprüfen

Versuchen Sie, über den Cisco VPN-Client eine Verbindung zum Cisco Router herzustellen, um zu überprüfen, ob der Cisco Router erfolgreich konfiguriert wurde.

1. Wählen Sie **Connection Entries > New aus**.



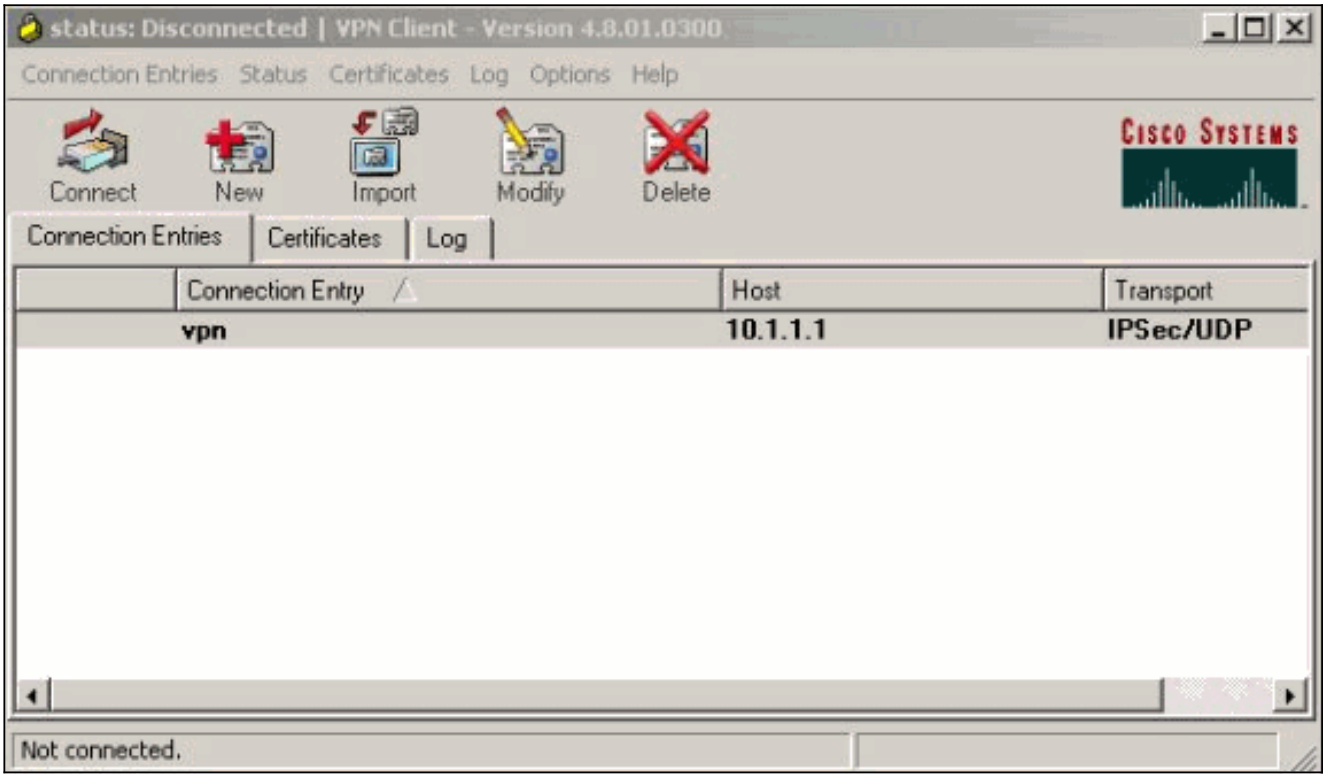
2. Füllen Sie die Details Ihrer neuen Verbindung aus.Das Host-Feld sollte die IP-Adresse oder den Hostnamen des Tunnel-Endpunkts des Easy VPN-Servers (Cisco Router) enthalten. Die Informationen zur Gruppenauthentifizierung müssen mit denen in Schritt 9 übereinstimmen. Klicken Sie abschließend auf



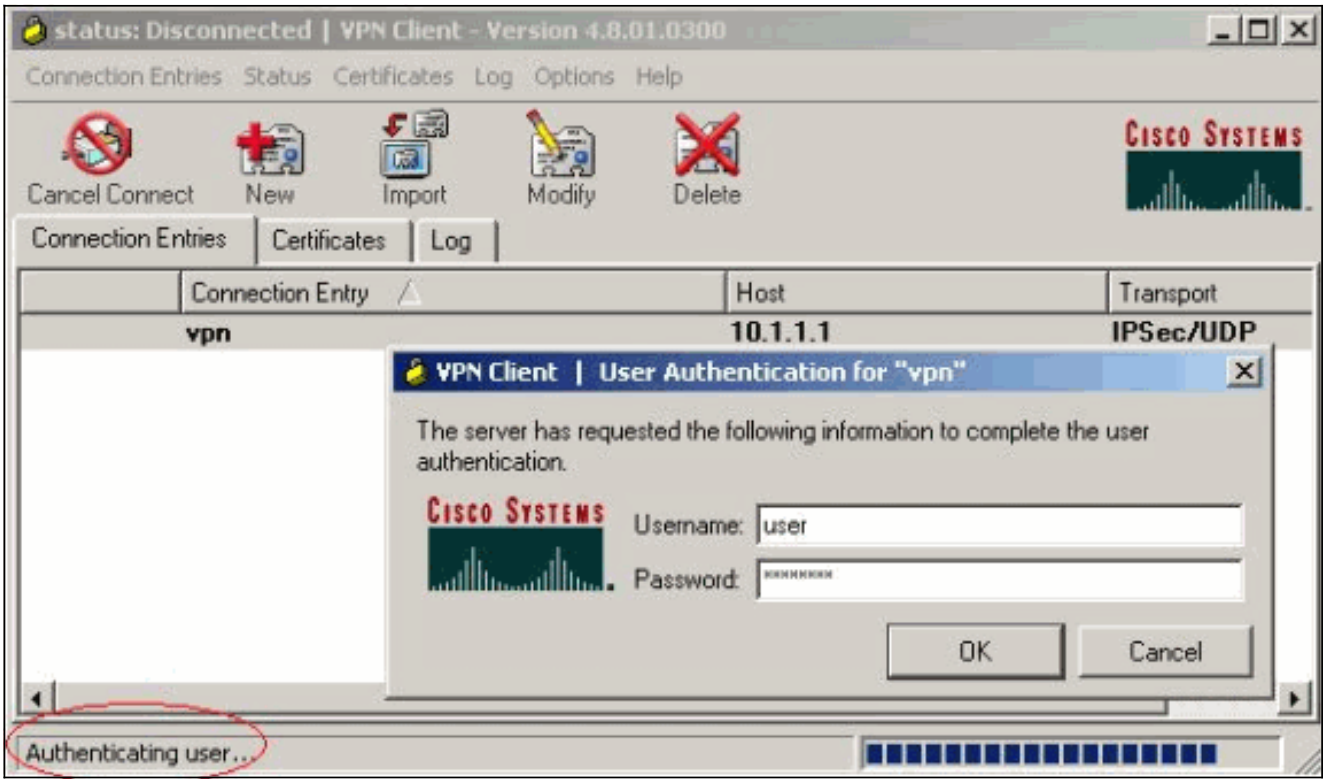
Speichern.

3. Wählen Sie die neu erstellte Verbindung aus, und klicken Sie auf

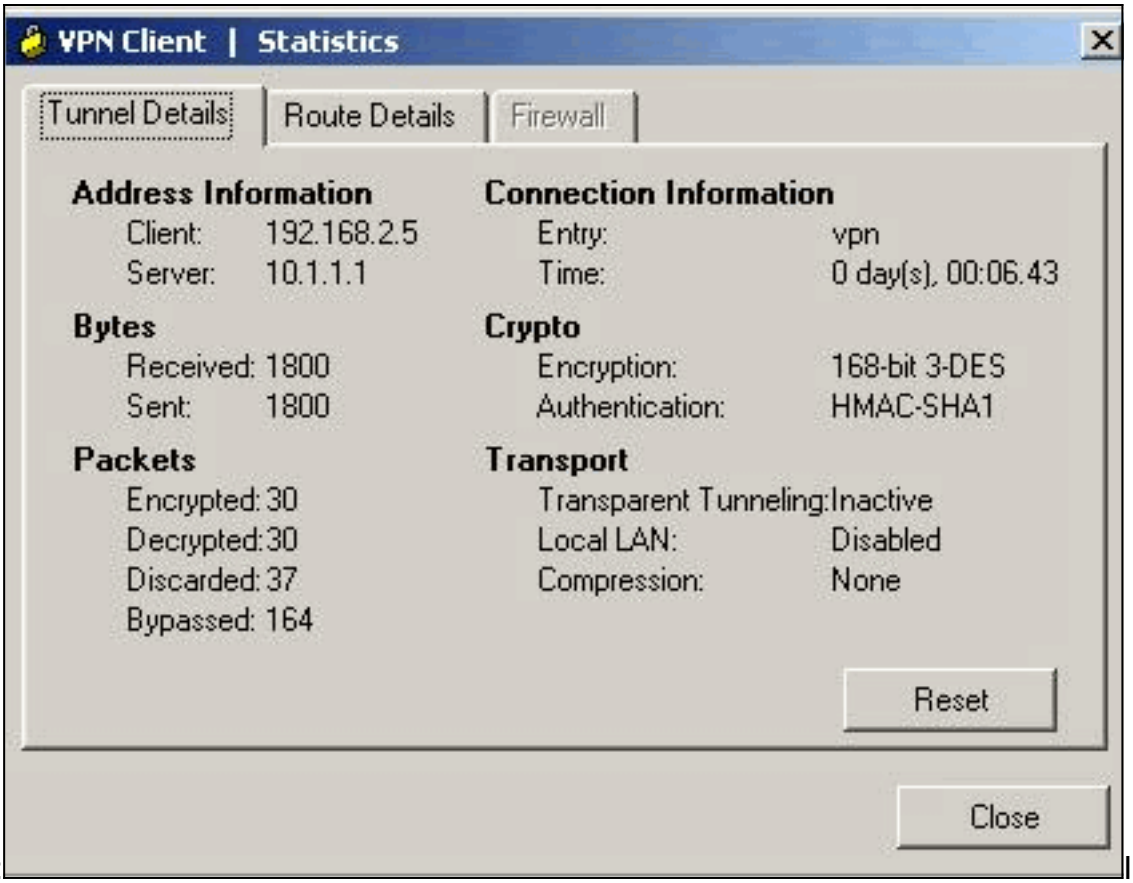
Verbinden.



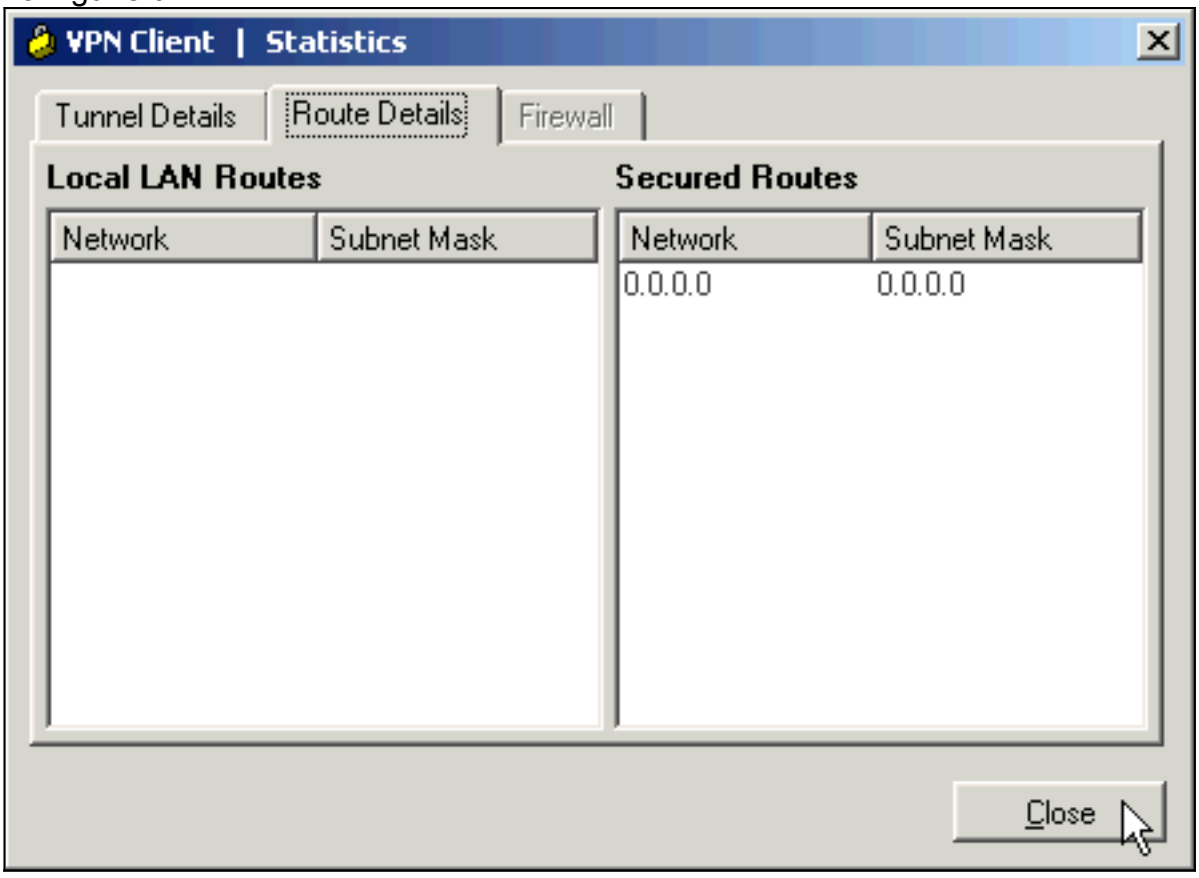
4. Geben Sie einen Benutzernamen und ein Kennwort für die erweiterte Authentifizierung (Xauth) ein. Diese Informationen werden durch die Xauth-Parameter in Schritt 7 bestimmt.



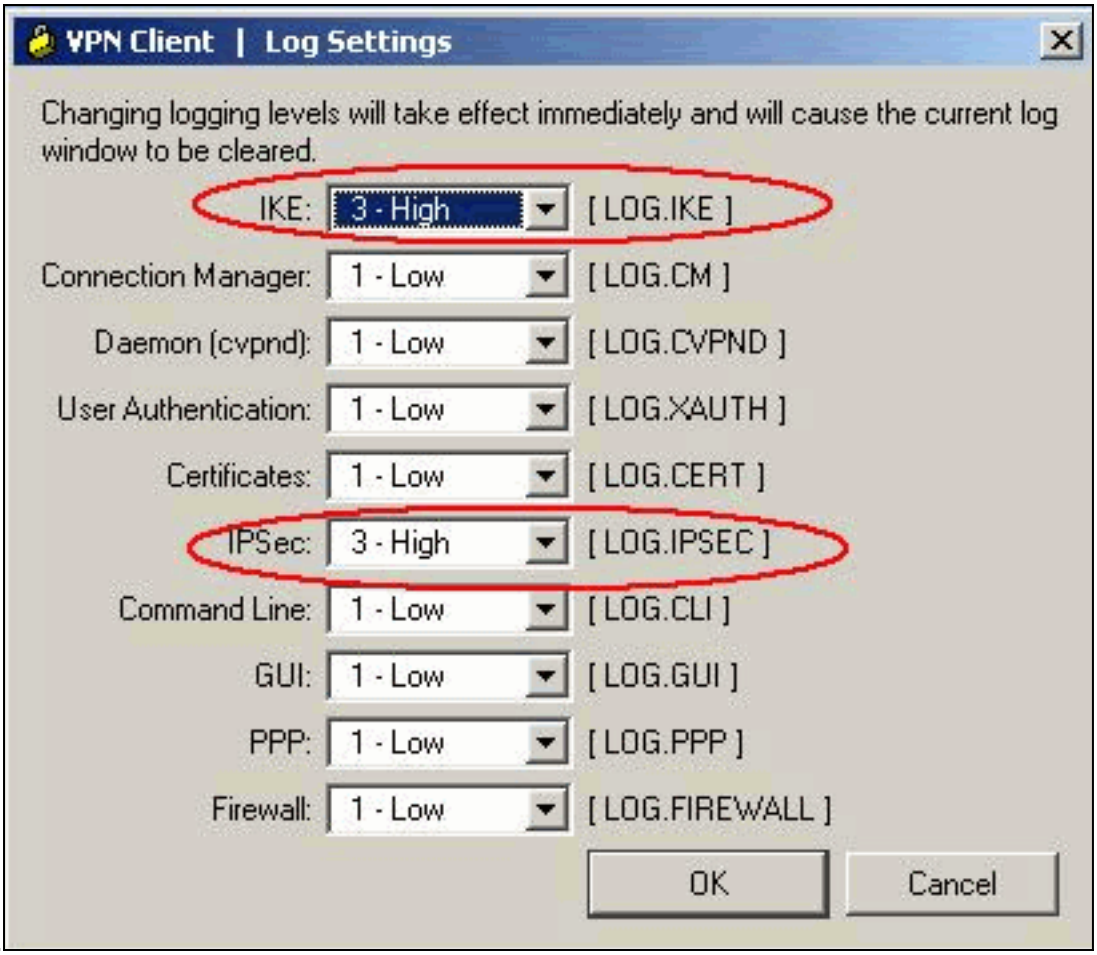
5. Wenn die Verbindung erfolgreich hergestellt wurde, wählen Sie im Menü Status die Option **Statistik** aus, um die Details des Tunnels zu überprüfen.In diesem Fenster werden der Datenverkehr und die Verschlüsselungsinformationen



angezeigt: In diesem Fenster werden Split-Tunneling-Informationen angezeigt, falls konfiguriert:



6. Wählen Sie **Protokoll > Protokolleinstellungen**, um die Protokollstufen im Cisco VPN-Client



zu aktivieren.

7. Wählen Sie **Log > Log Windows**, um die Protokolleinträge im Cisco VPN Client

anzuzeigen.

Zugehörige Informationen

- Herunterladen und Installieren von Cisco Router und Security Device Manager
- Support-Seite für Cisco VPN-Clients
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems