Cisco-router als een externe VPN-server die een voorbeeld van de configuratie van AIM gebruikt

Inhoud

Inleiding

Dit document beschrijft hoe u het Cisco Security apparaat Manager (DSM) kunt gebruiken om de Cisco router te configureren om op te treden als een Makkelijk VPN-server. Cisco PDM u uw router als een VPN-server voor de Cisco VPN-client kunt configureren met behulp van een gebruikersvriendelijke interface op basis van webbeheer. Nadat de Cisco-routerconfiguratie is voltooid, kan deze worden geverifieerd met behulp van de Cisco VPN-client.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de router van Cisco volledig operationeel en gevormd is om Cisco PDM toe te staan om configuratieveranderingen aan te brengen.

Opmerking: Verwijs naar Toestemming voor HTTPS Toegang voor Sm om de router toe te staan om te worden gevormd door het Sdm.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 3640 router met Cisco IOS® softwarerelease 12.3(14T)
- Security apparaat Manager versie 2.3.1
- Cisco VPN-client versie 4.8

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

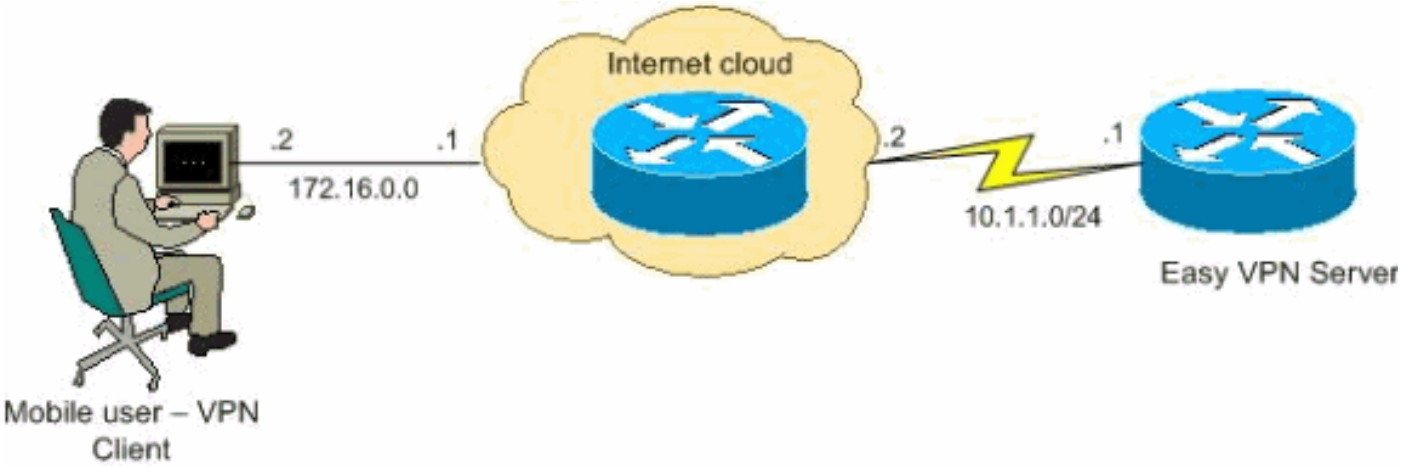
Configureren

In deze sectie, wordt u voorgesteld met de informatie om de eigenschappen van de Makkelijk VPN Server te vormen die een verre eindgebruiker toelaat om te communiceren met IPsec met om het even welke Cisco IOS® VPN gateway.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

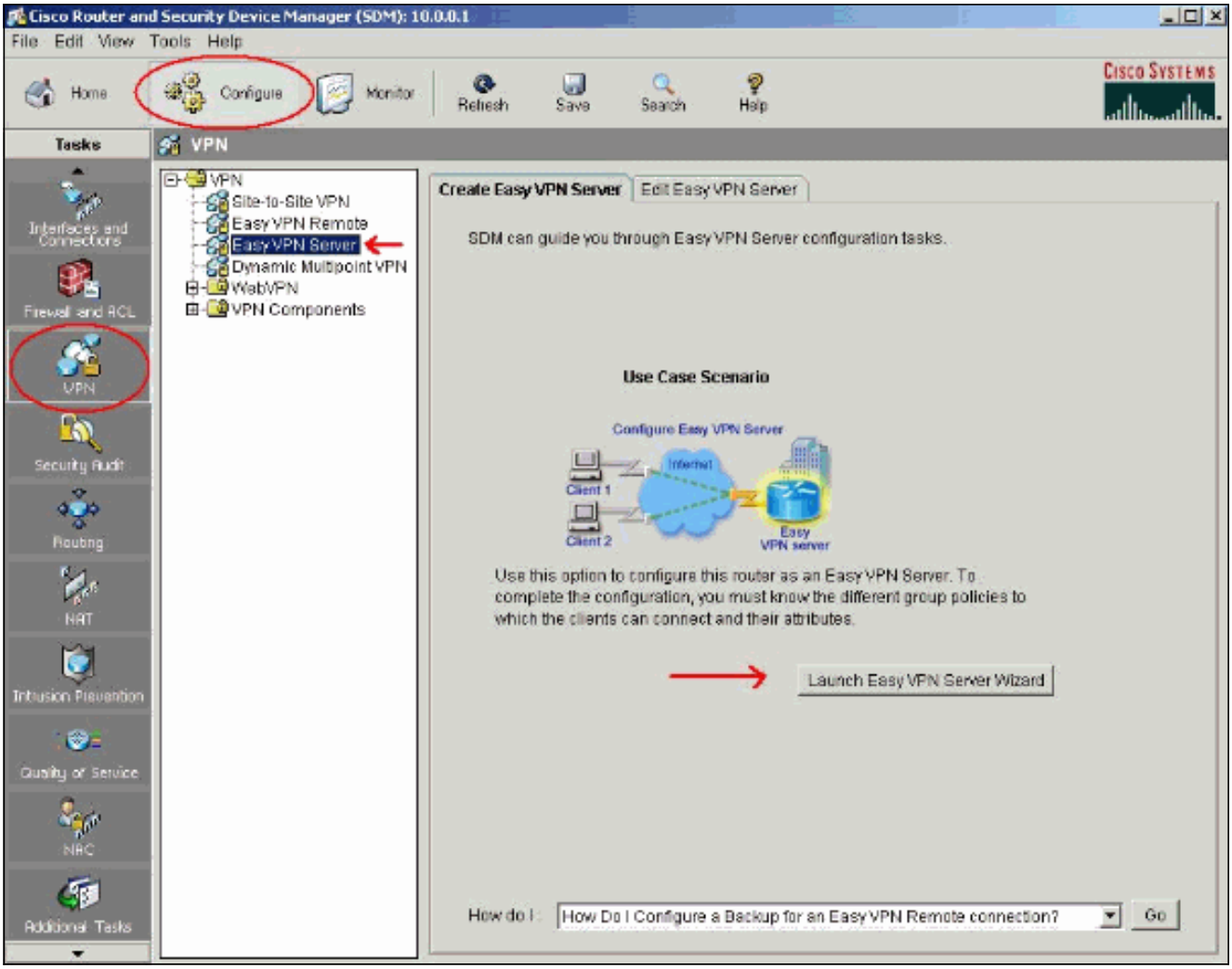
Het netwerk in dit document is als volgt opgebouwd:



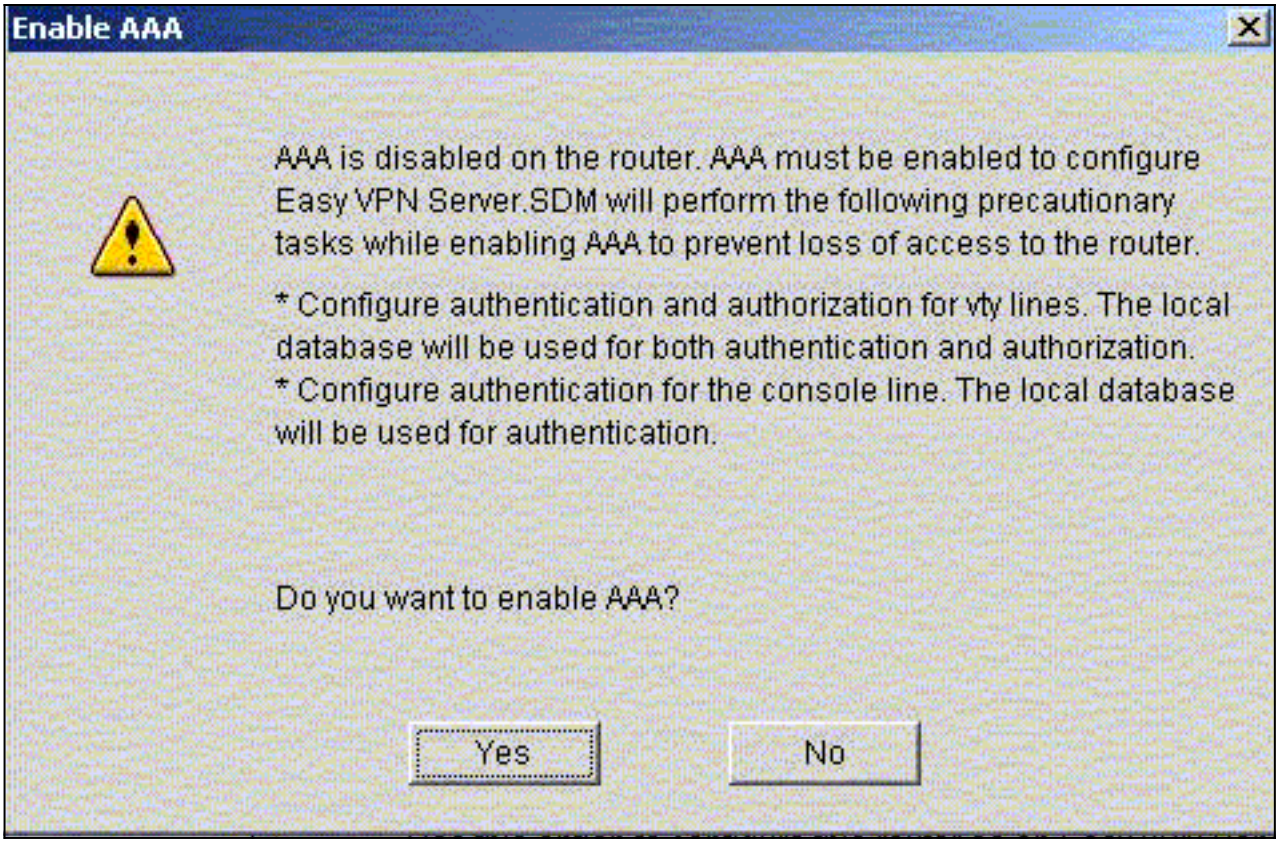
Configuratieprocedure

Voltooi deze stappen om de router van Cisco als een verre server van VPN te vormen die ontwikkel.

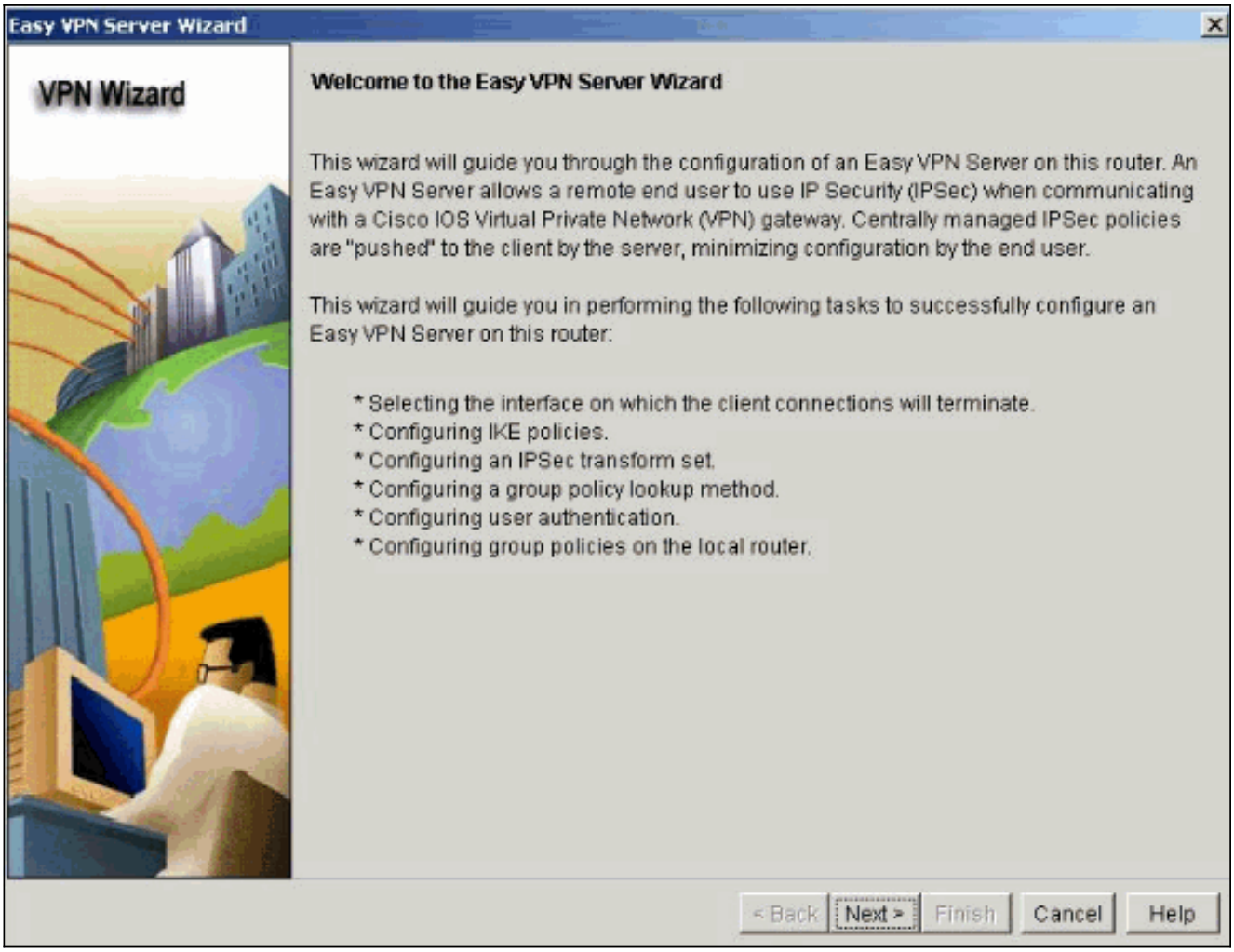
1. Selecteer **Configureren > VPN > Makkelijk VPN-server** vanuit het Home-venster en klik op **Start Easy VPN Server**.



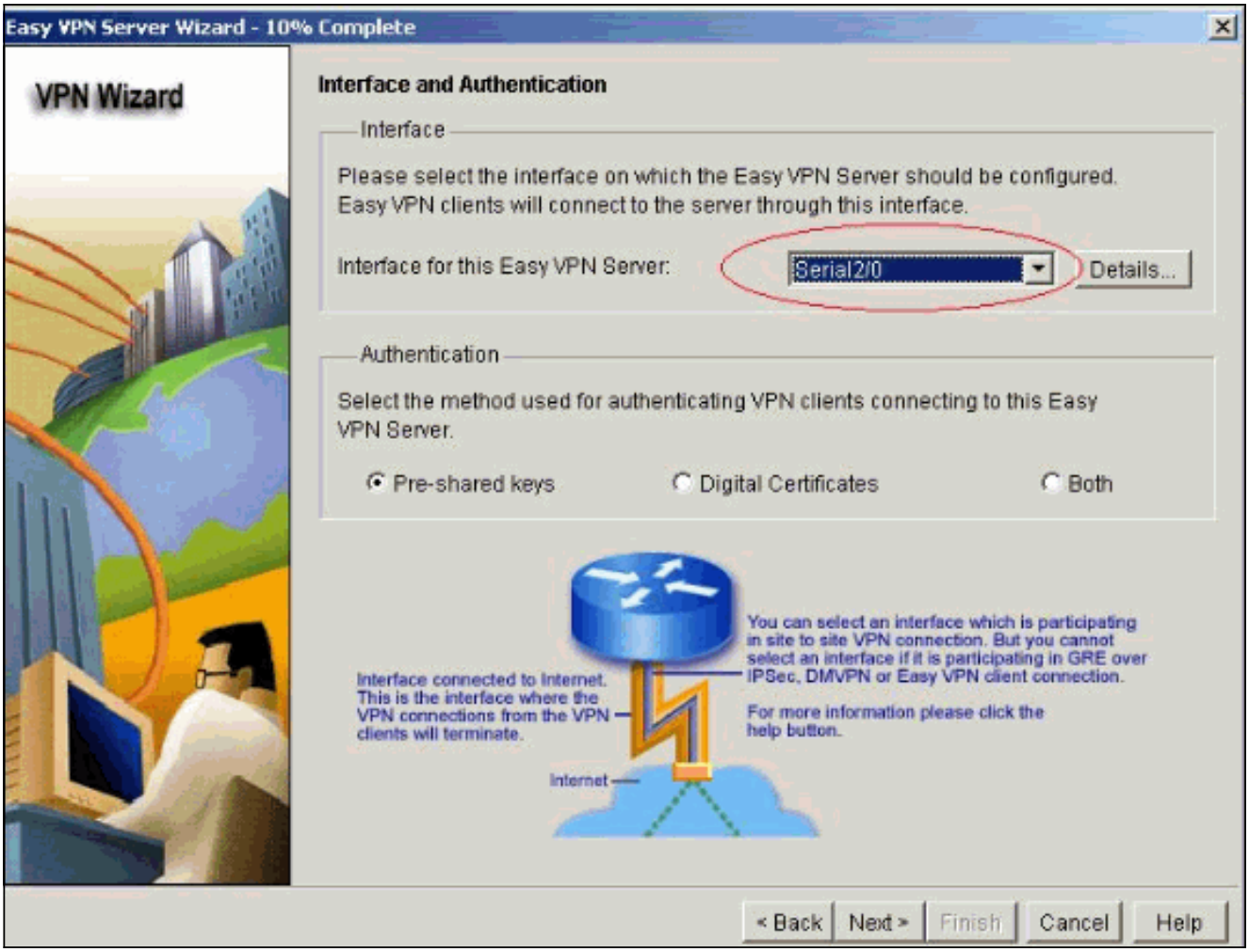
2. AAA moet op de router zijn ingeschakeld voordat de configuratie van de Makkelijke VPN-server is gestart. Klik op **Ja** om verder te gaan met de configuratie.De 'AAA' is geactiveerd op de router' berichtdisplays in het venster. Klik op **OK** om de configuratie van Makkelijk VPN-server te
starten.



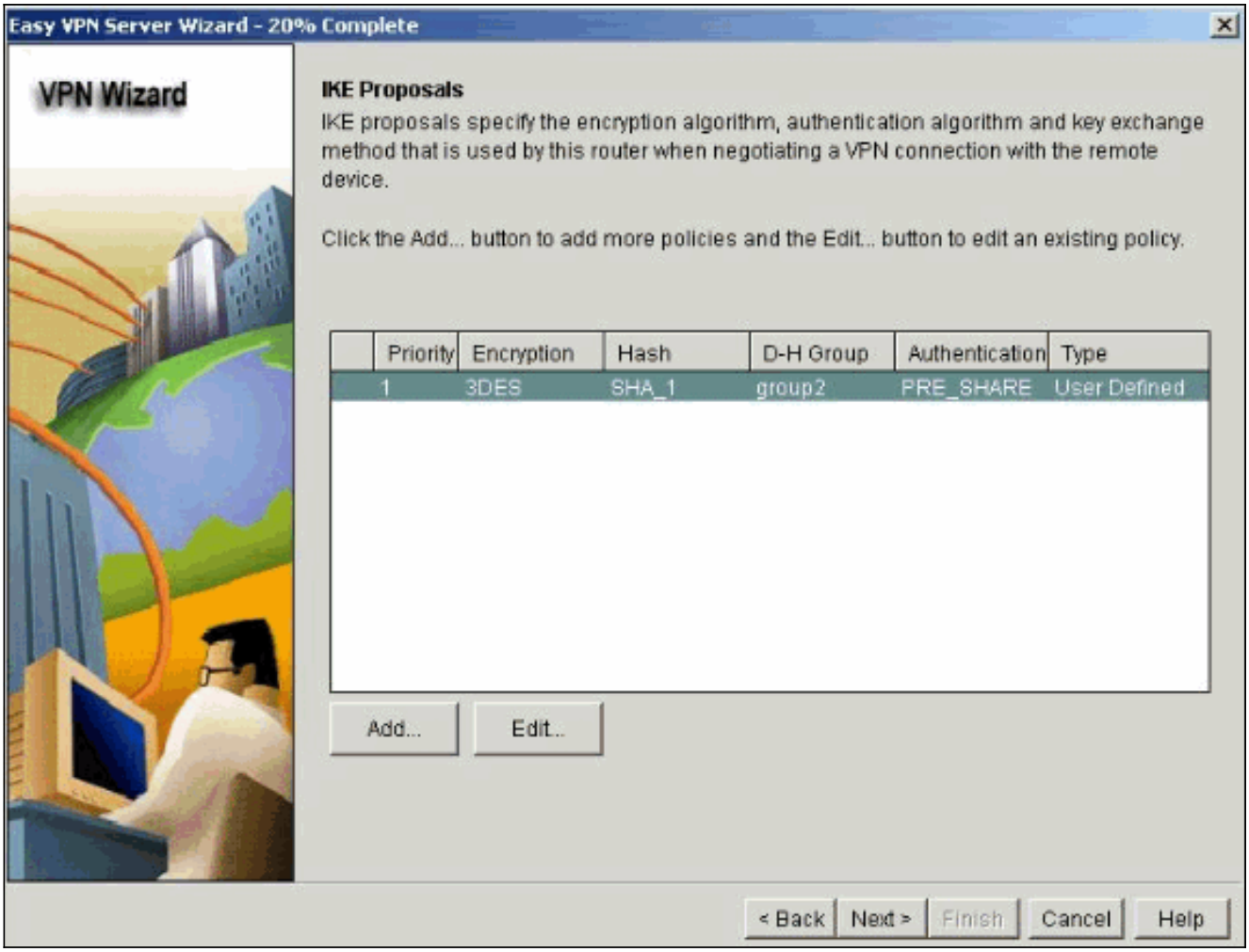
3. Klik op **Next** om de Easy VPN Server-wizard te starten.



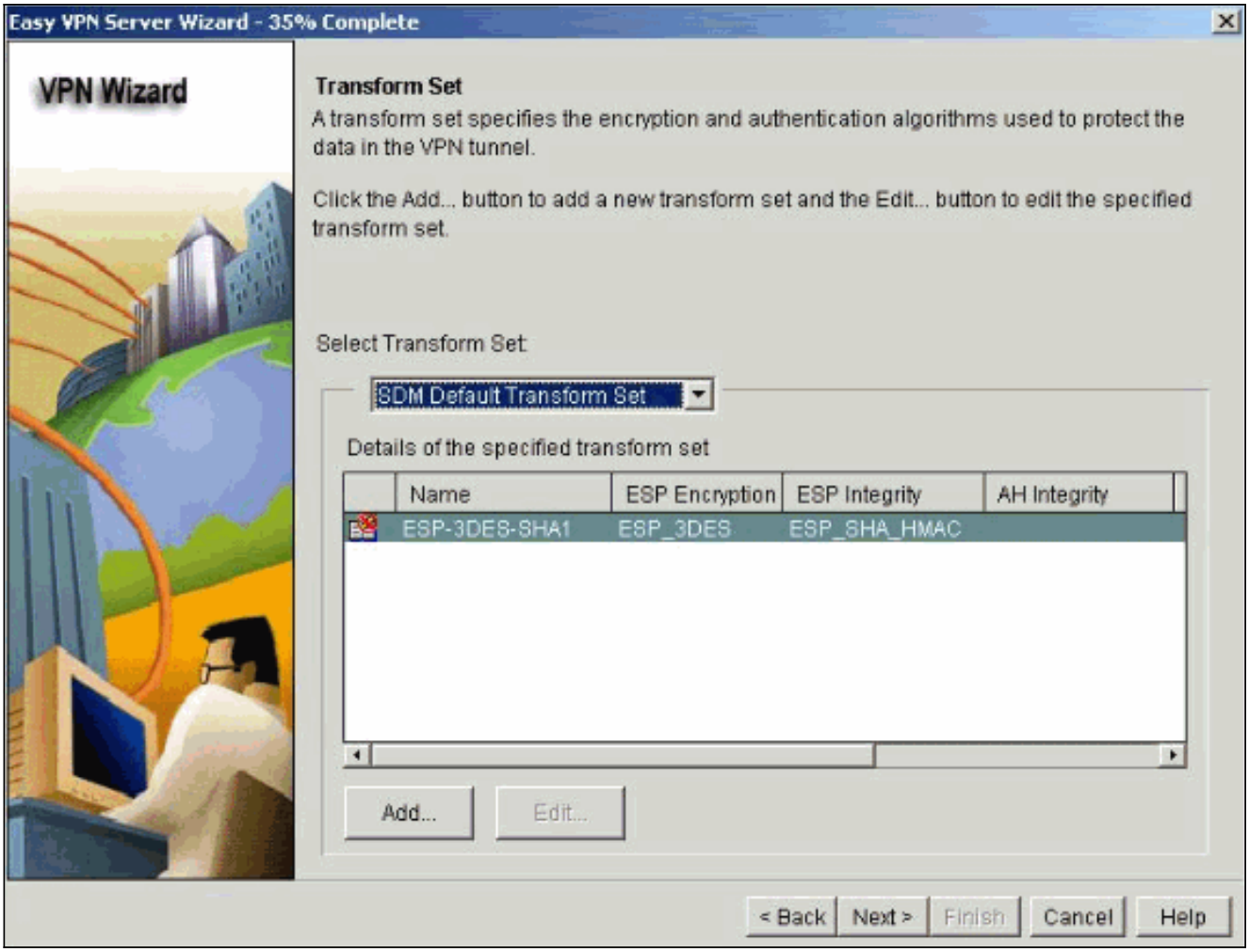
4. Selecteer de interface waarop de clientverbindingen worden afgesloten en het verificatietype.



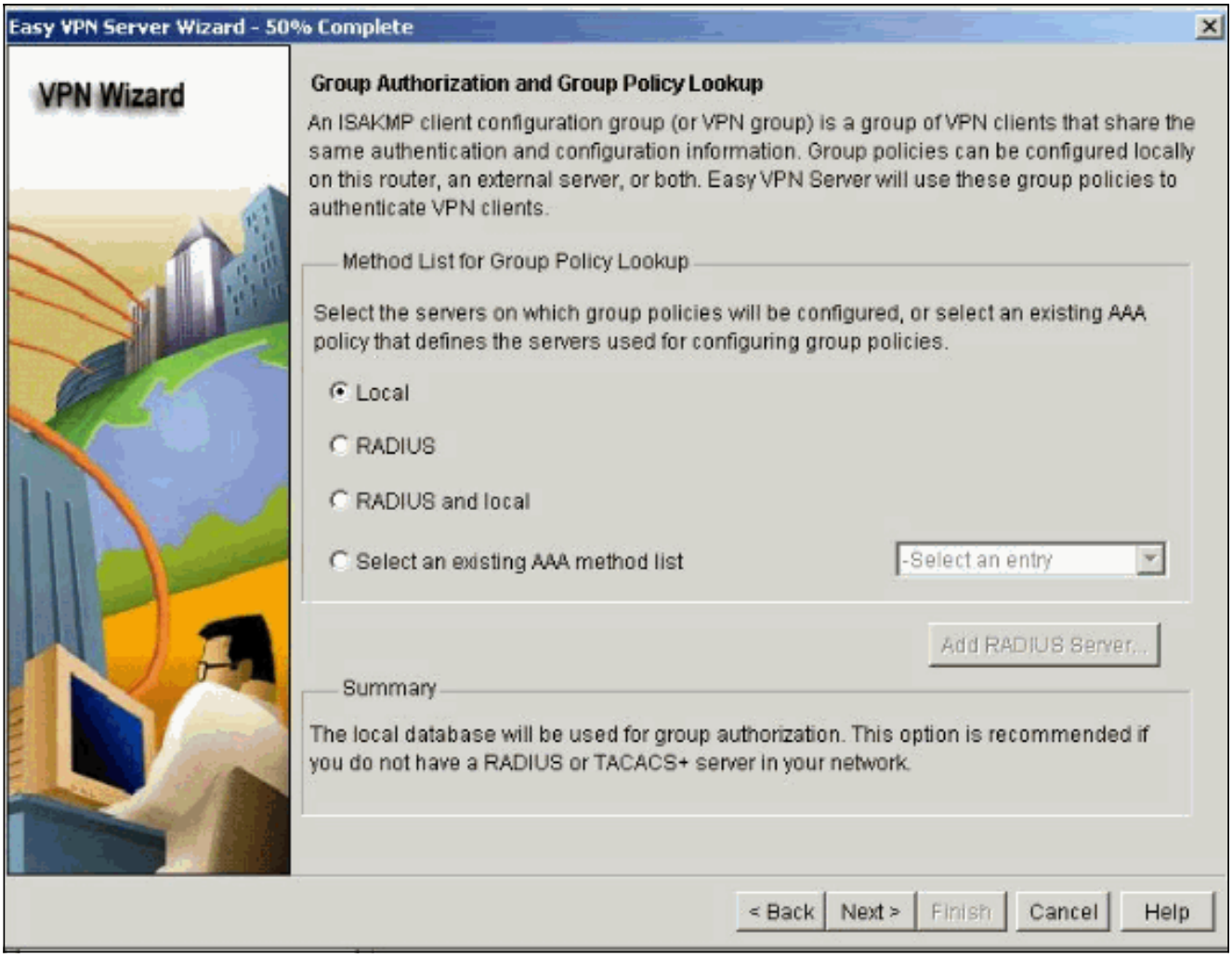
5. Klik op **Next** om het beleid van Internet Key Exchange (IKE) te configureren en gebruik de knop **Add** om het nieuwe beleid te maken.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen. Maar de Cisco VPN-client selecteert automatisch de juiste configuratie voor zichzelf. Daarom is geen IKE-configuratie nodig op de client-pc.



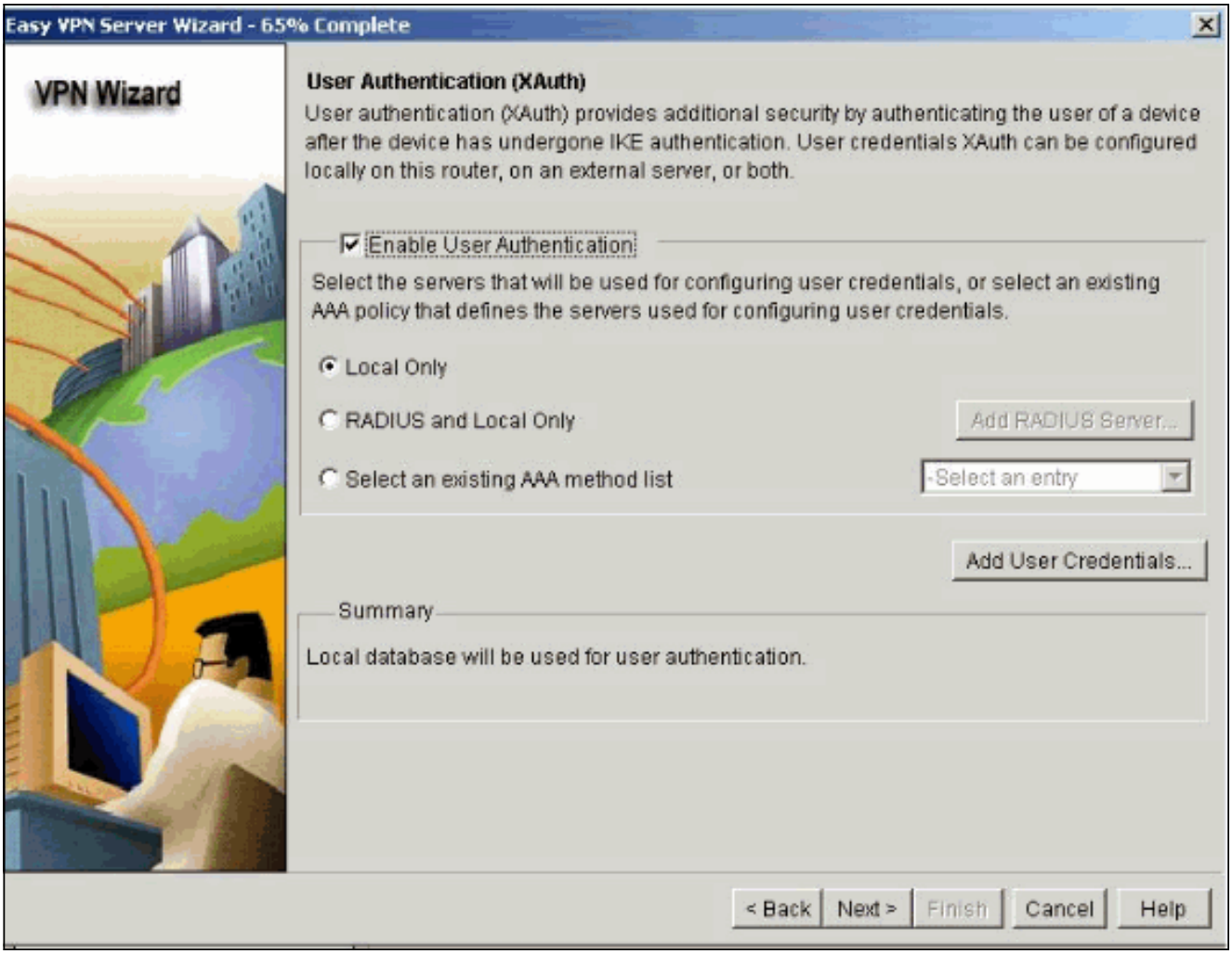
6. Klik op **Next** om de standaard transformatie set te kiezen of de nieuwe transformatie set toe te voegen om het encryptie- en verificatiealgoritme te specificeren. In dit geval wordt de standaard transformator
gebruikt.



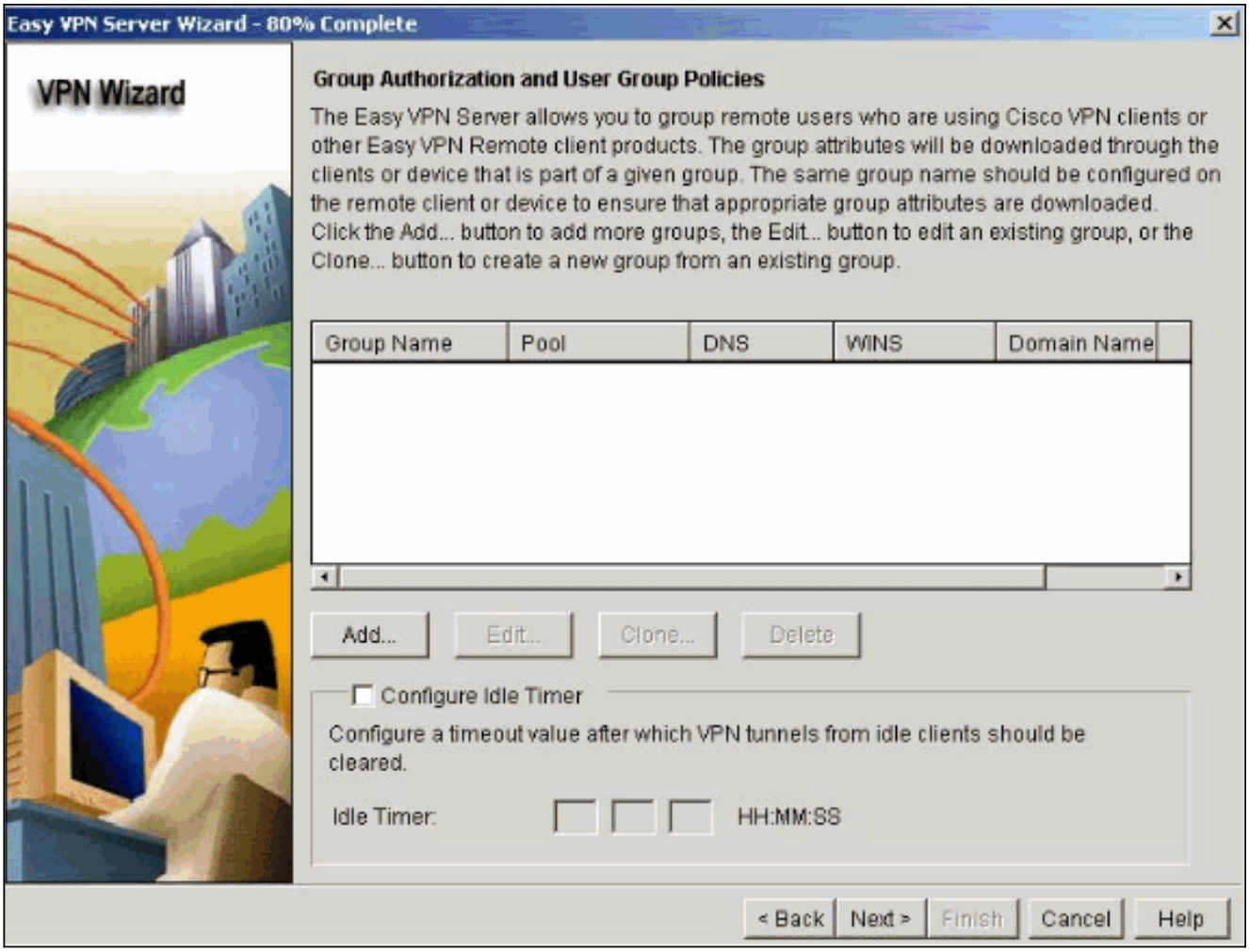
7. Klik op **Next** om een nieuwe lijst te maken met **de** autorisatie- en accounting (AAA) autorisatie voor de benadering van groepsbeleid of om een bestaande lijst van netwerkmethoden te kiezen die gebruikt wordt voor groepsautorisatie.



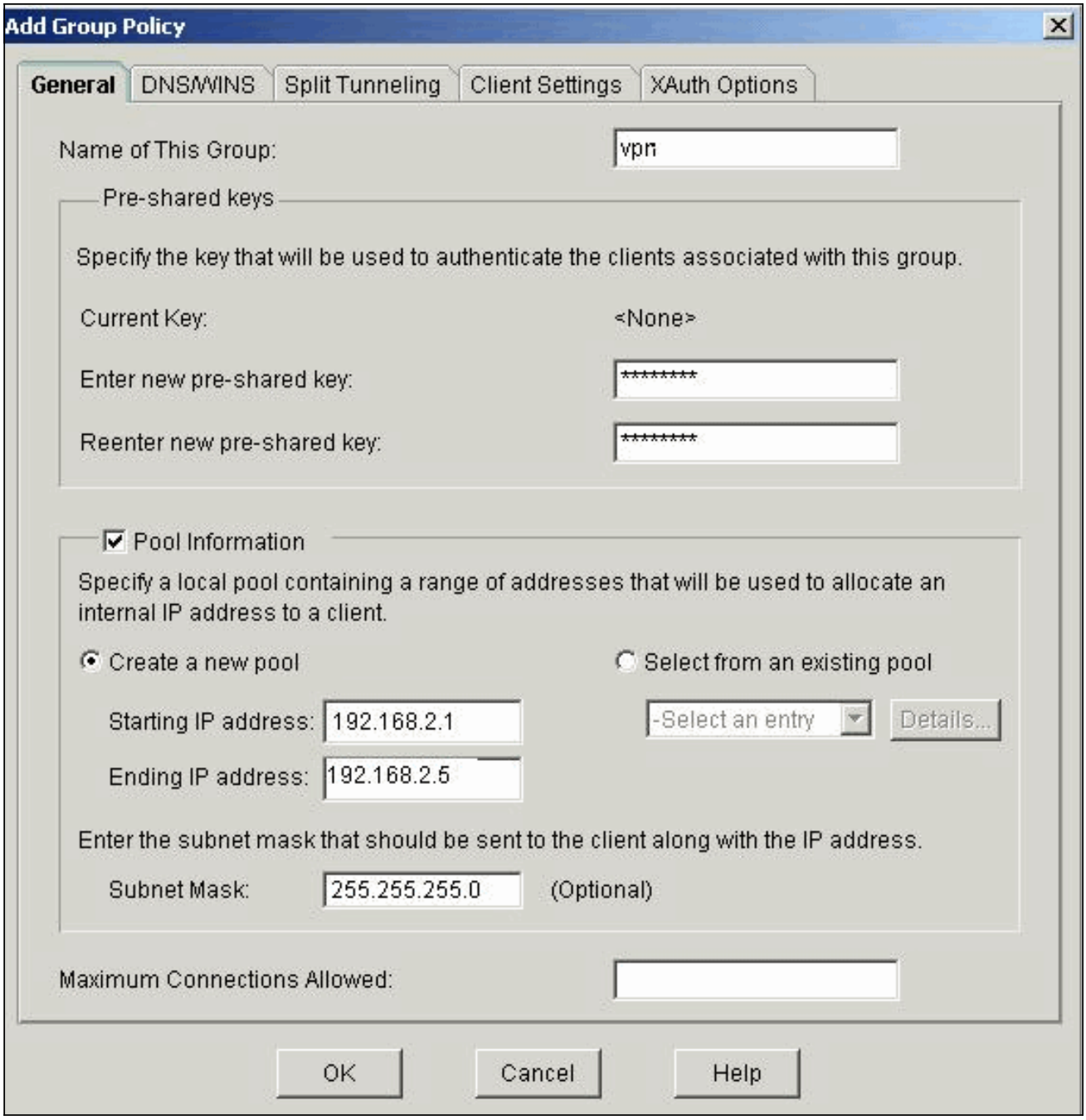
8. Configuratie van gebruikersverificatie op de Gemakkelijke VPN Server.U kunt gebruikersverificatiegegevens opslaan op een externe server zoals een RADIUS-server of een lokale database of op beide. Een lijst met AAA-inlogverificatiemethoden wordt gebruikt om te bepalen in welke volgorde de gebruikersverificatiedetails moeten worden doorzocht.



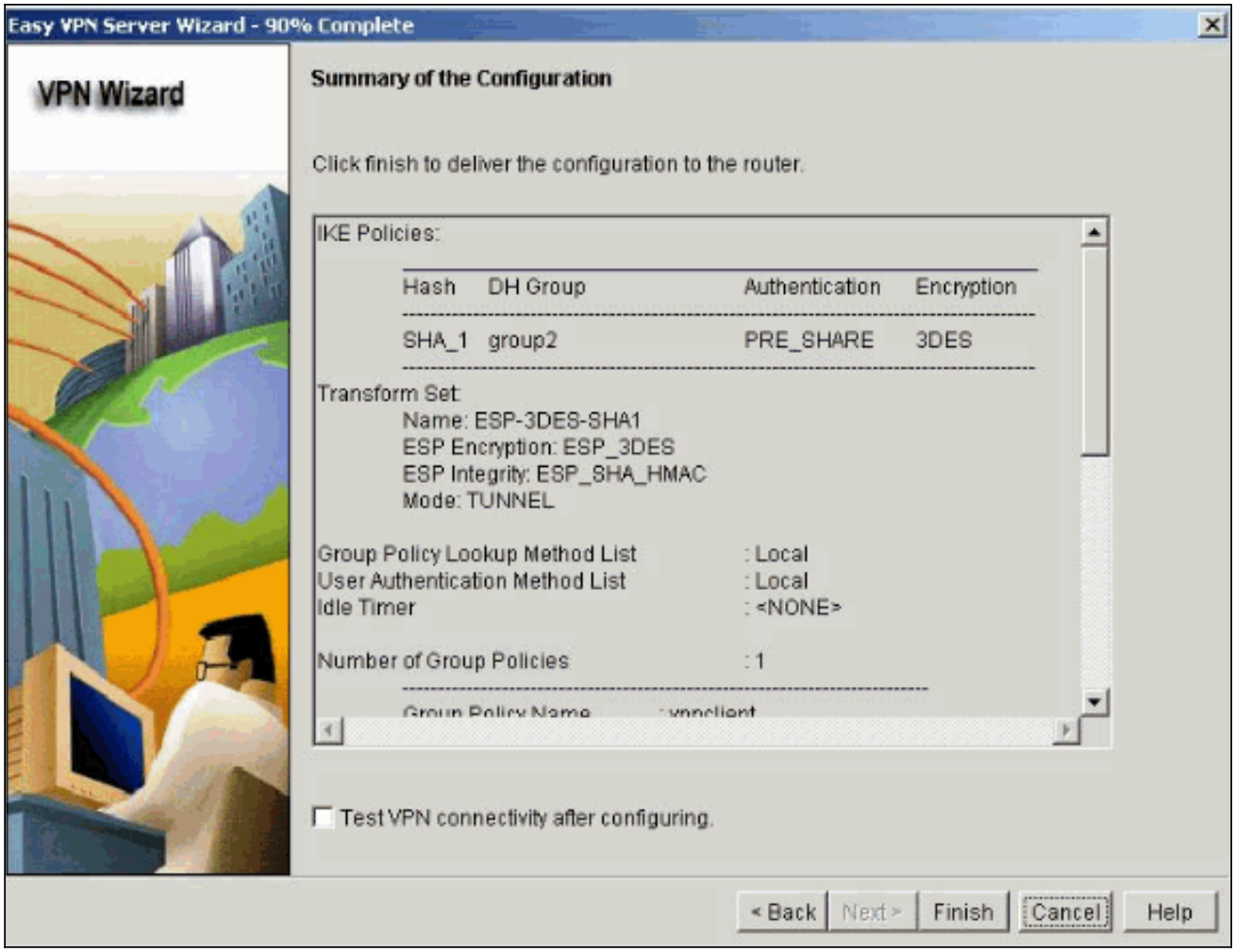
9. In dit venster kunt u gebruikersgroepbeleid in de lokale database toevoegen, bewerken, klonen of
verwijderen.



10. Voer een naam in voor de naam van de tunnelgroep. Geef de vooraf gedeelde sleutel aan die gebruikt wordt voor authenticatie informatie.Maak een nieuwe pool of selecteer een bestaande pool die wordt gebruikt om de IP-adressen aan de VPN-clients toe te wijzen.

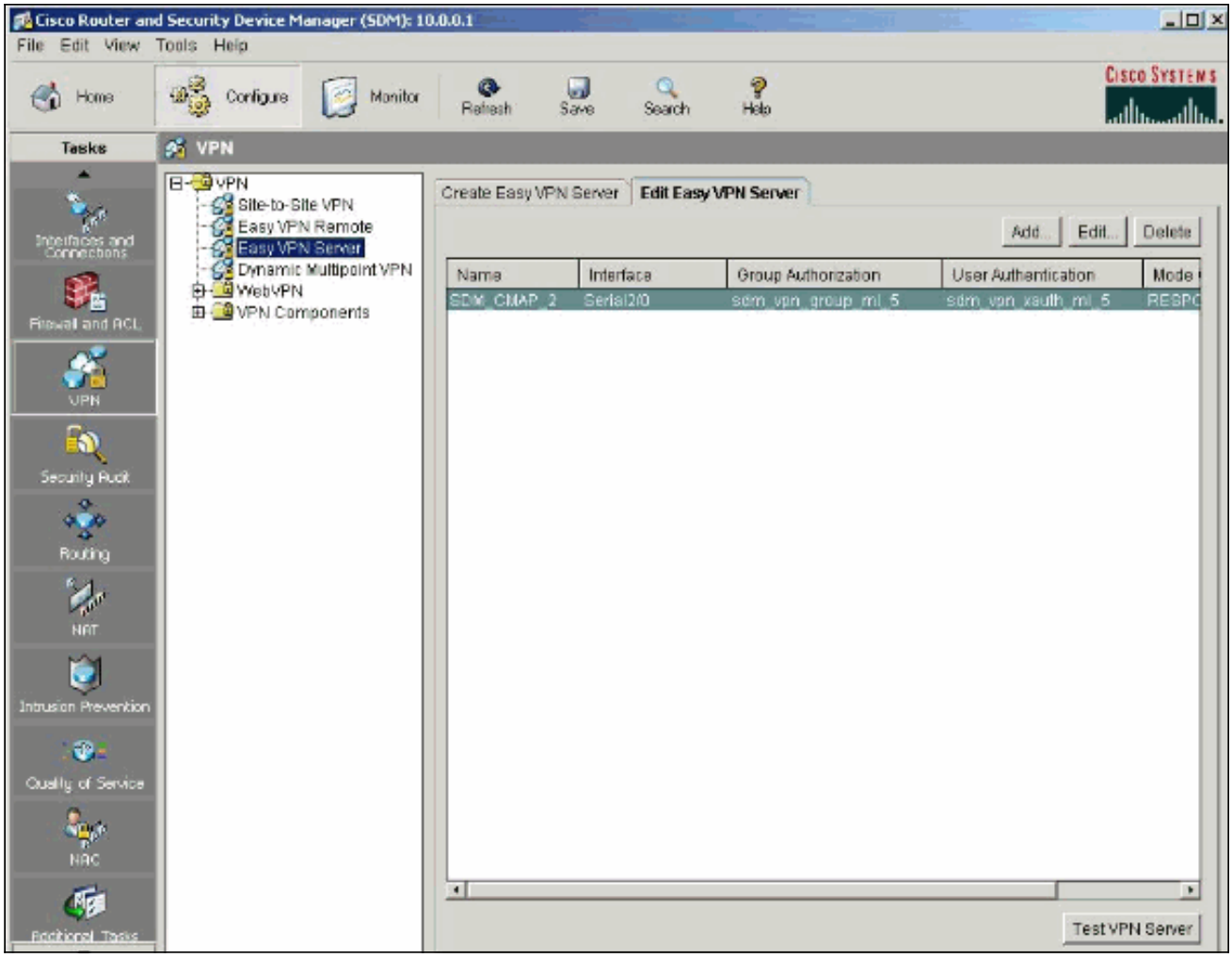


11. Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op **Voltooien** als u tevreden bent met de configuratie.



12. De sdm stuurt de configuratie naar de router om de actieve configuratie bij te werken. Klik op **OK** om dit te voltooien.

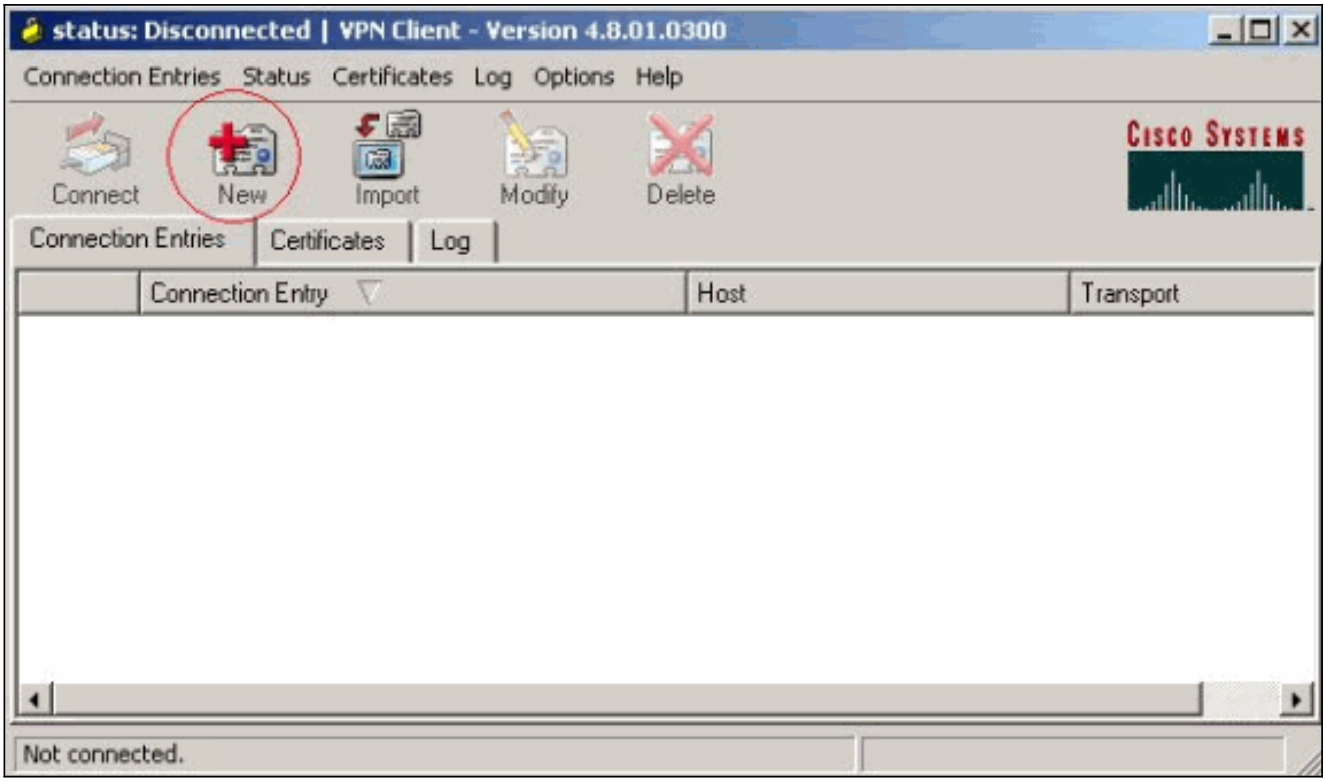
13. Na voltooiing, kunt u de veranderingen in de configuratie indien nodig bewerken en wijzigen.



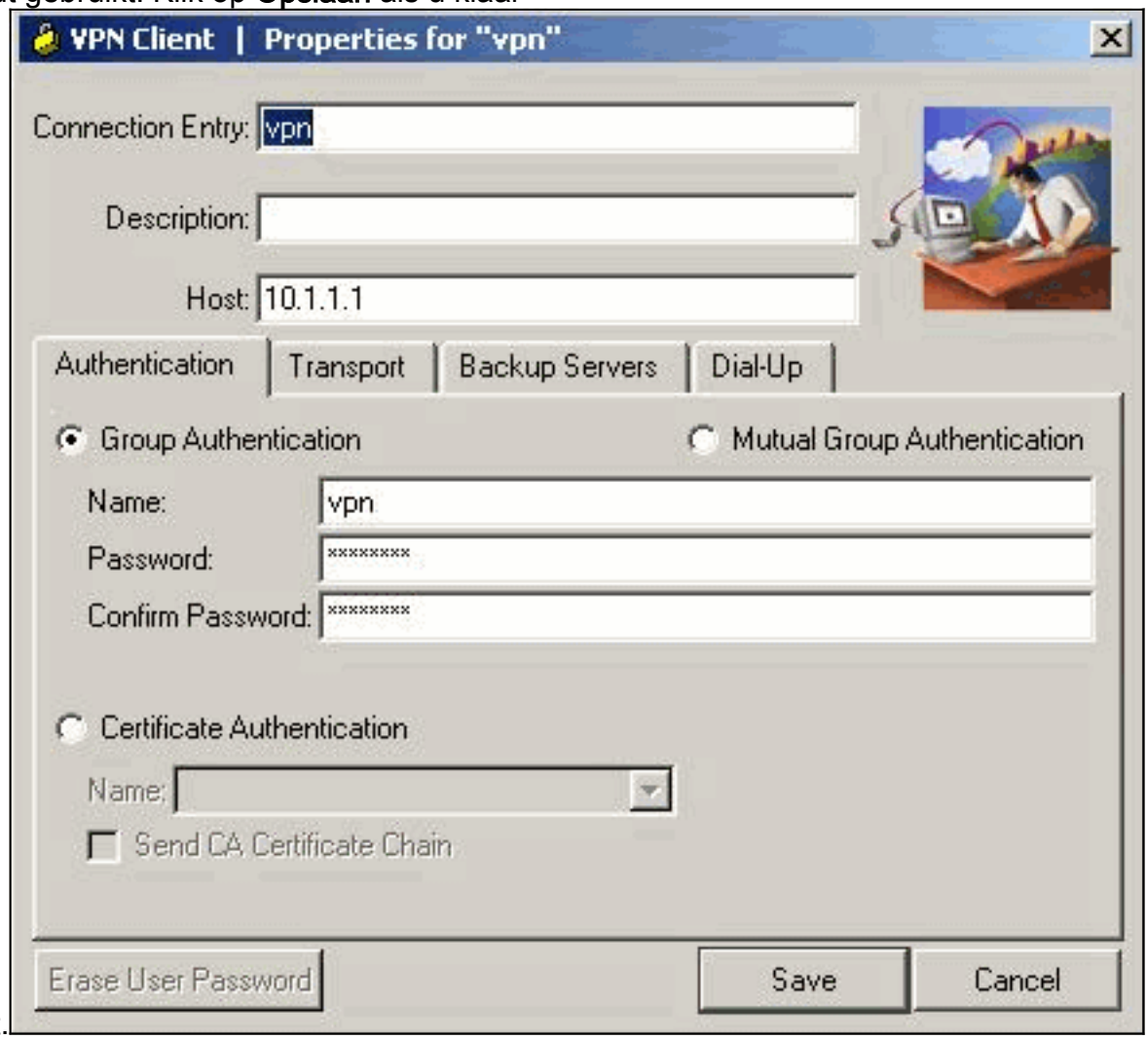
Verifiëren

Probeer met de Cisco-router een verbinding te maken met de Cisco VPN-client om te controleren of de Cisco-router met succes is geconfigureerd.

1. Selecteer **Connection Vermeldingen > New**.

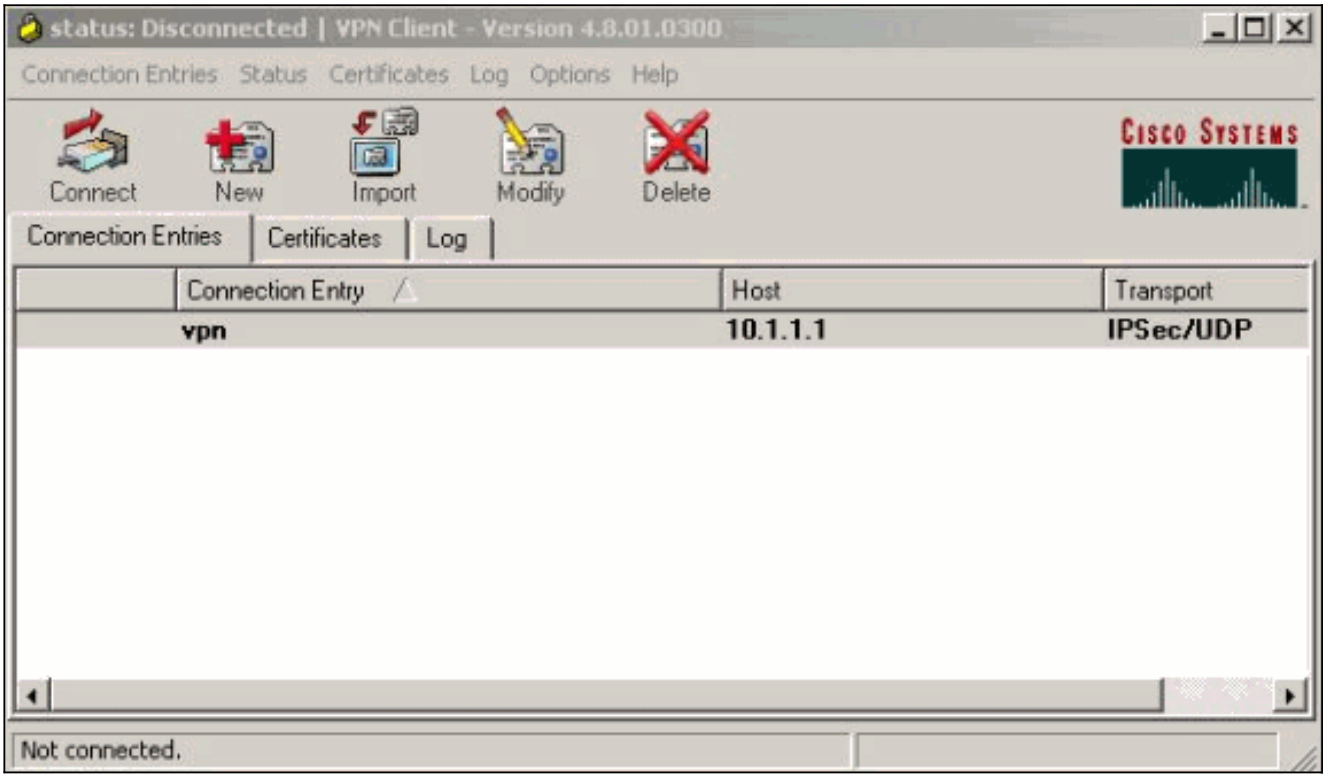


2. Vul de gegevens in van uw nieuwe aansluiting.Het veld Host moet het IP-adres of de hostnaam van het tunneleindpunt van de Makkelijk VPN-server (Cisco router) bevatten. De informatie over de groepsverificatie dient overeen te komen met de informatie die in stap 9 wordt gebruikt. Klik op **Opslaan** als u klaar bent.

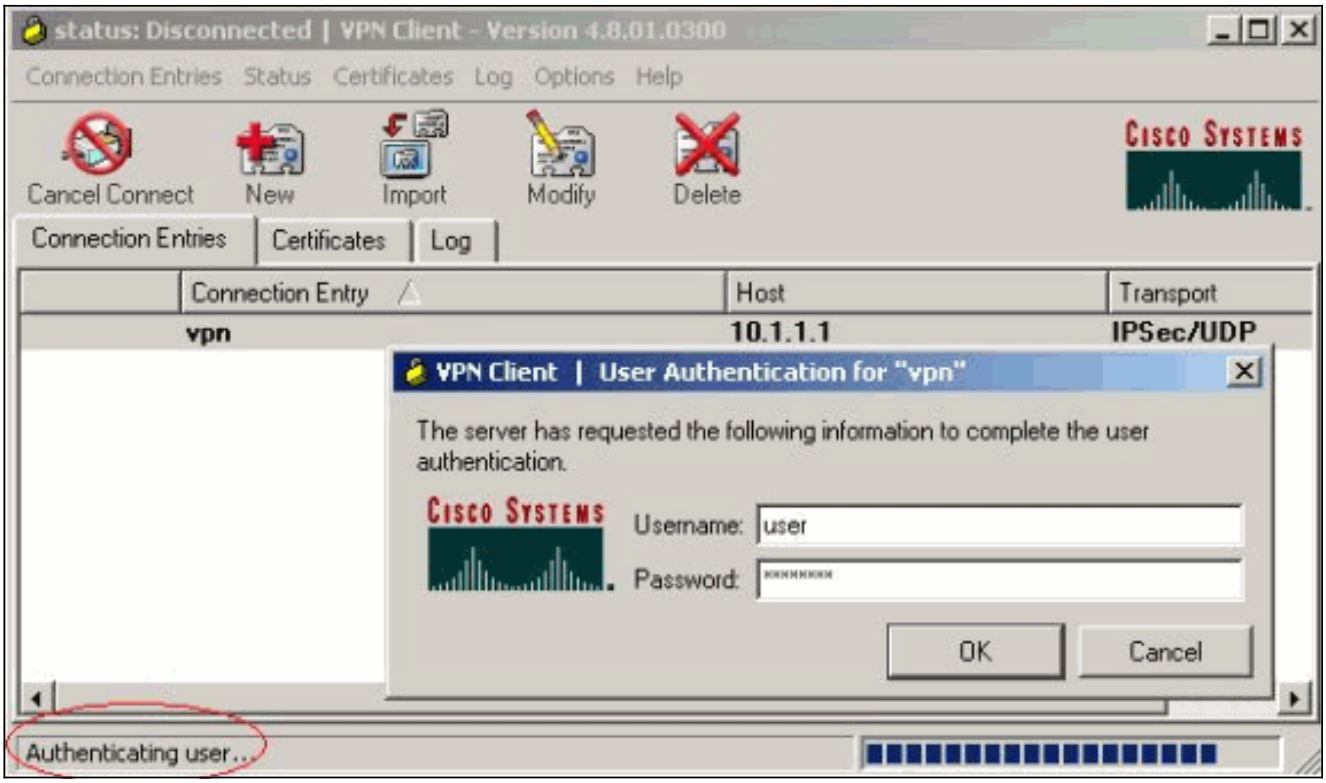


3. Selecteer de nieuwe verbinding en klik op

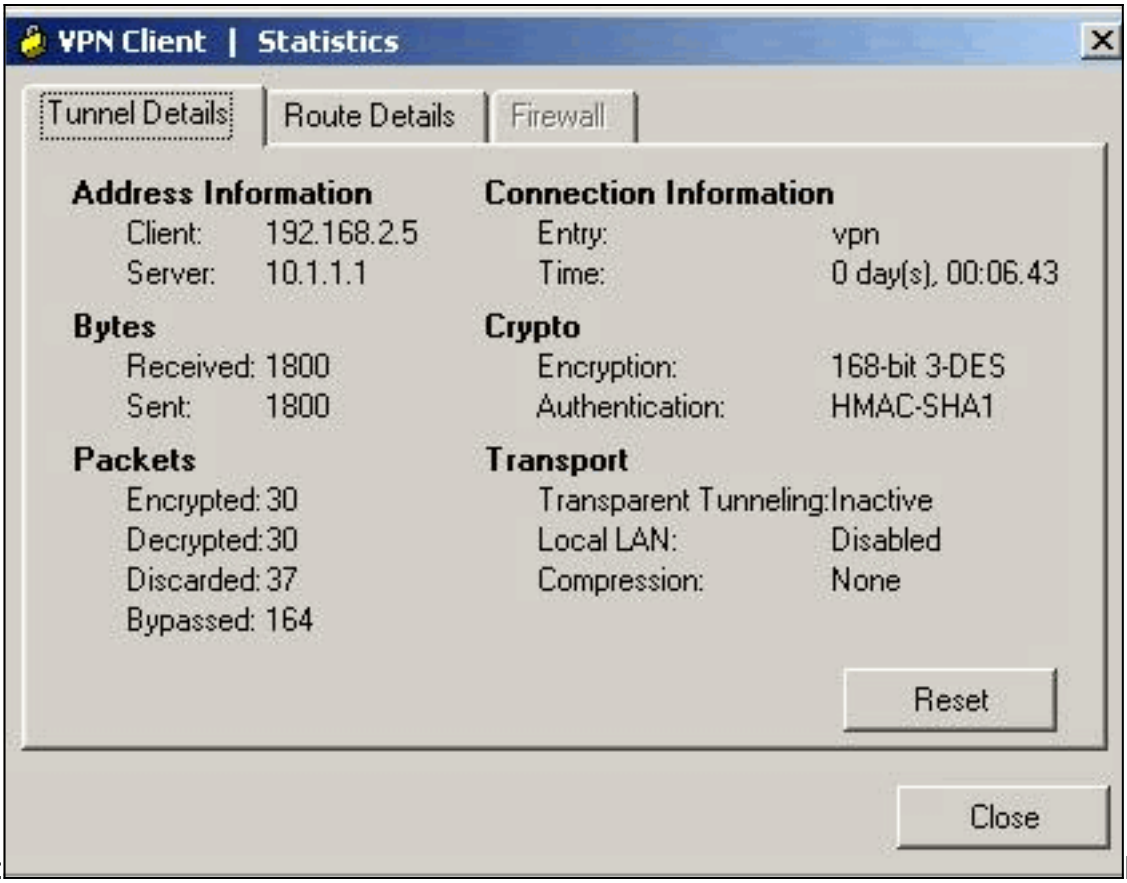
Connect.



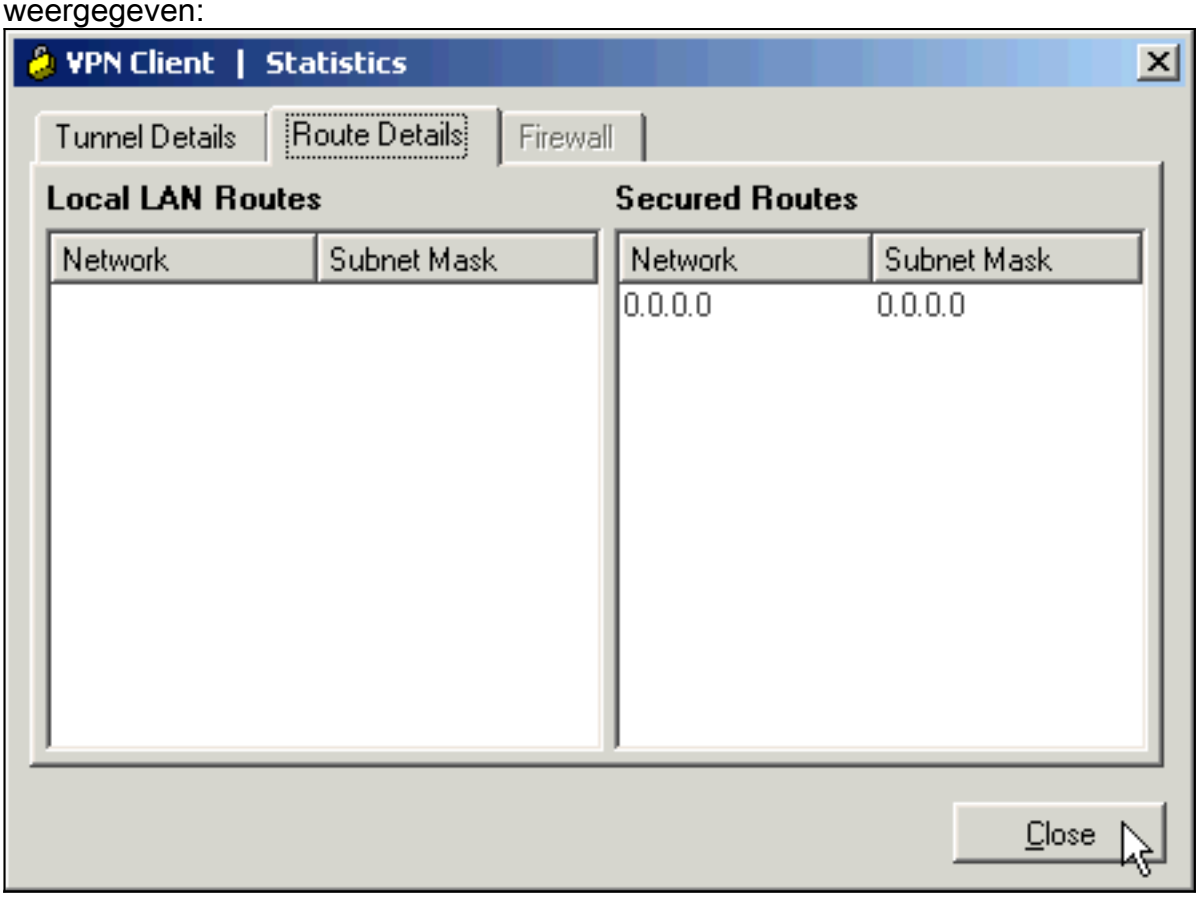
4. Voer een gebruikersnaam en wachtwoord in voor uitgebreide verificatie (Xauth). Deze informatie wordt bepaald door de Xauth-parameters in stap 7.



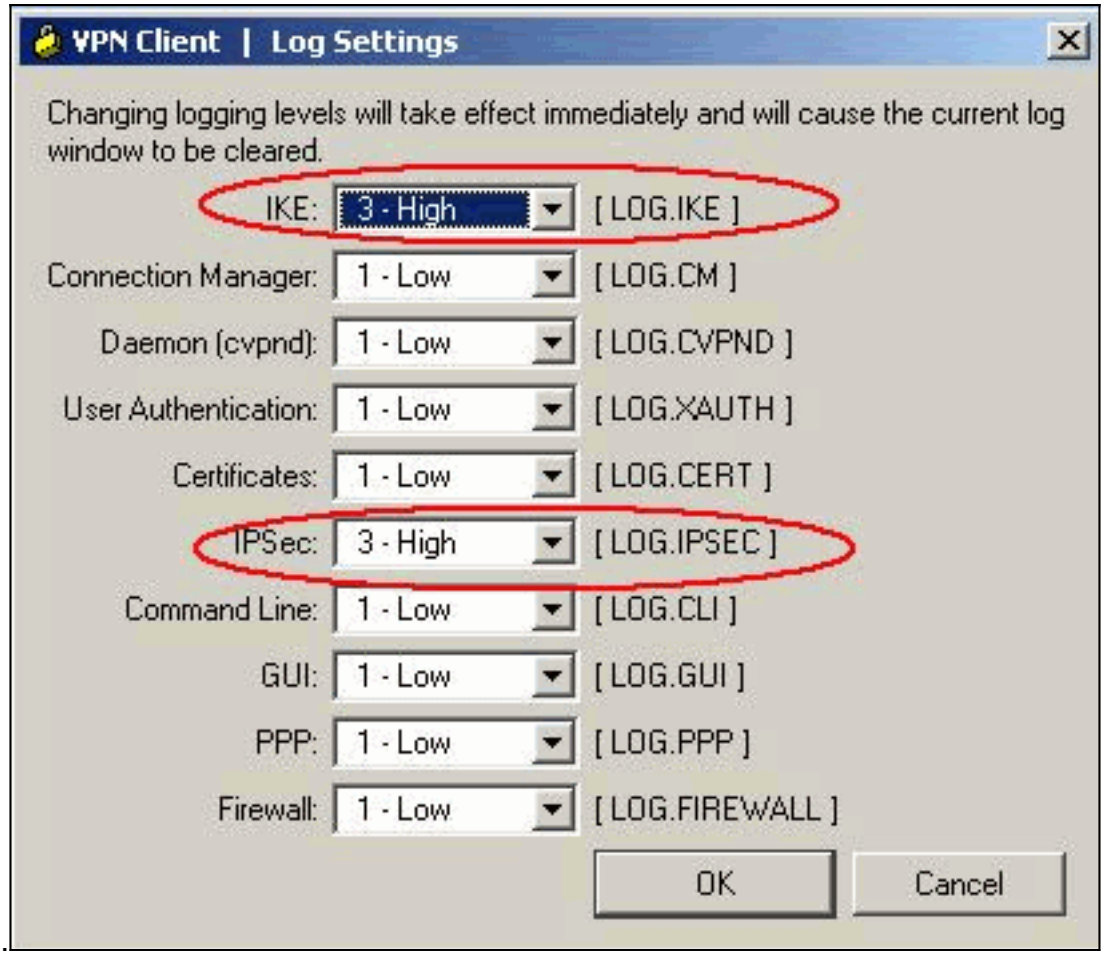
5. Zodra de verbinding met succes is ingesteld selecteert u **Statistieken** uit het menu Status om de details van de tunnel te controleren.Dit venster toont informatie over verkeer en



crypto: In dit venster wordt indien ingesteld informatie over gesplitste tunneling weergegeven:



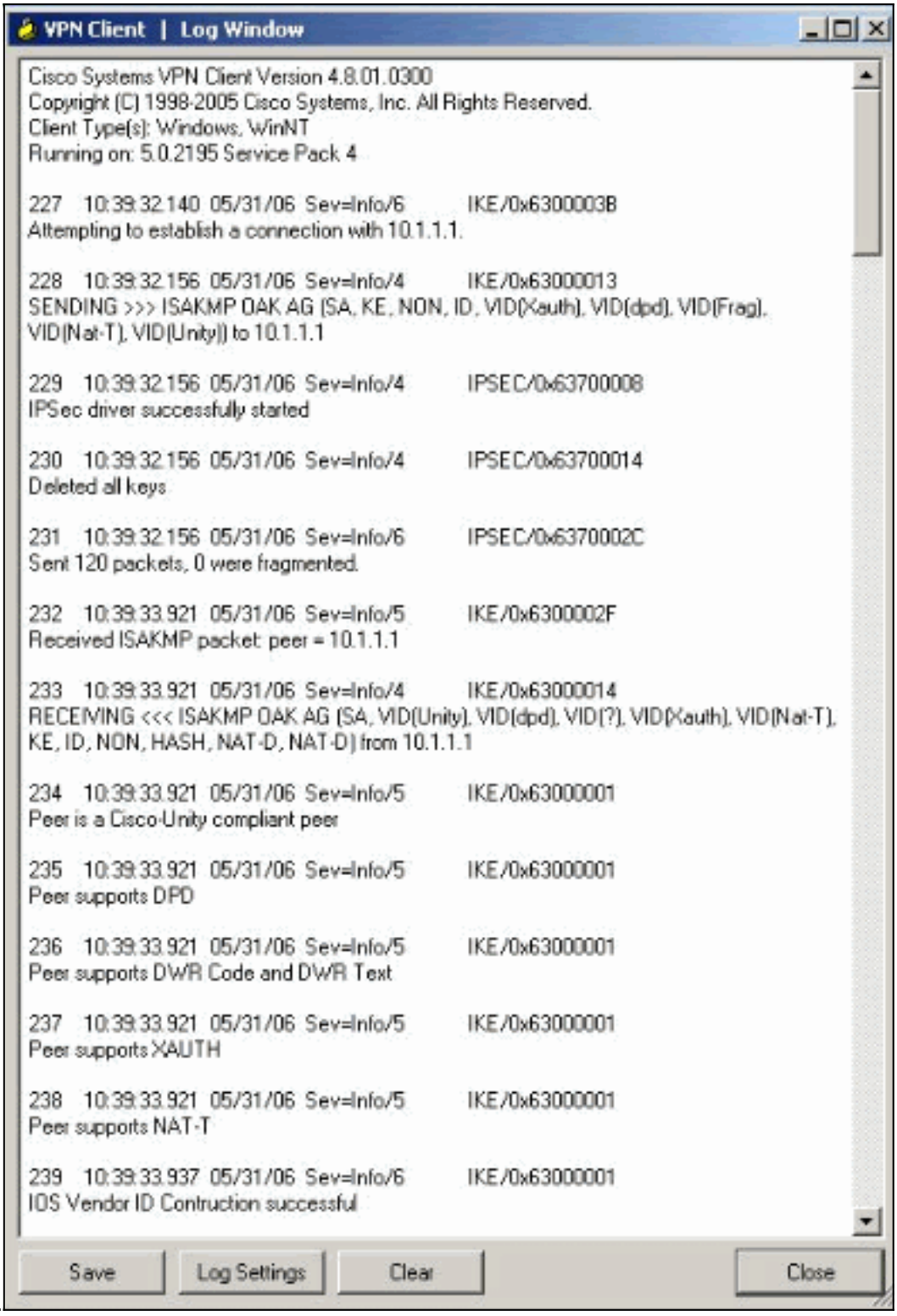
6. Selecteer **Log > Instellingen loggen** om de logniveaus in de Cisco VPN-client in te



schakelen.

7. Selecteer **Log > Log Windows** in om de logitems in de Cisco VPN-client te

bekijken.



Gerelateerde informatie

- Cisco-router en -security apparaatbeheer downloaden en installeren
- Cisco VPN-clientondersteuningspagina
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems