IOS-router als Makkelijke VPN-server met Configuration Professional Configuration-voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco IOS® router kunt configureren als een Makkelijk VPN-server (EzVPN) met Cisco Configuration Professional (Cisco CP) en de CLI. Met de functie Makkelijk VPN Server kan een externe eindgebruiker communiceren met behulp van IP Security (IPsec) met elke Cisco IOS Virtual Private Network (VPN) poort. Centraal beheerd IPsec beleid wordt "geduwd" naar het clientapparaat door de server, waardoor de configuratie door de eindgebruiker wordt geminimaliseerd.

Raadpleeg voor meer informatie over Makkelijk VPN-server het gedeelte Makkelijk VPN-server van de Secure Connectivity Configuration Guide Library, Cisco IOS release 12.4T.

Voorwaarden

Gebruikte componenten

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

- Cisco 1841 router met Cisco IOS-softwarerelease 12.4(15T)

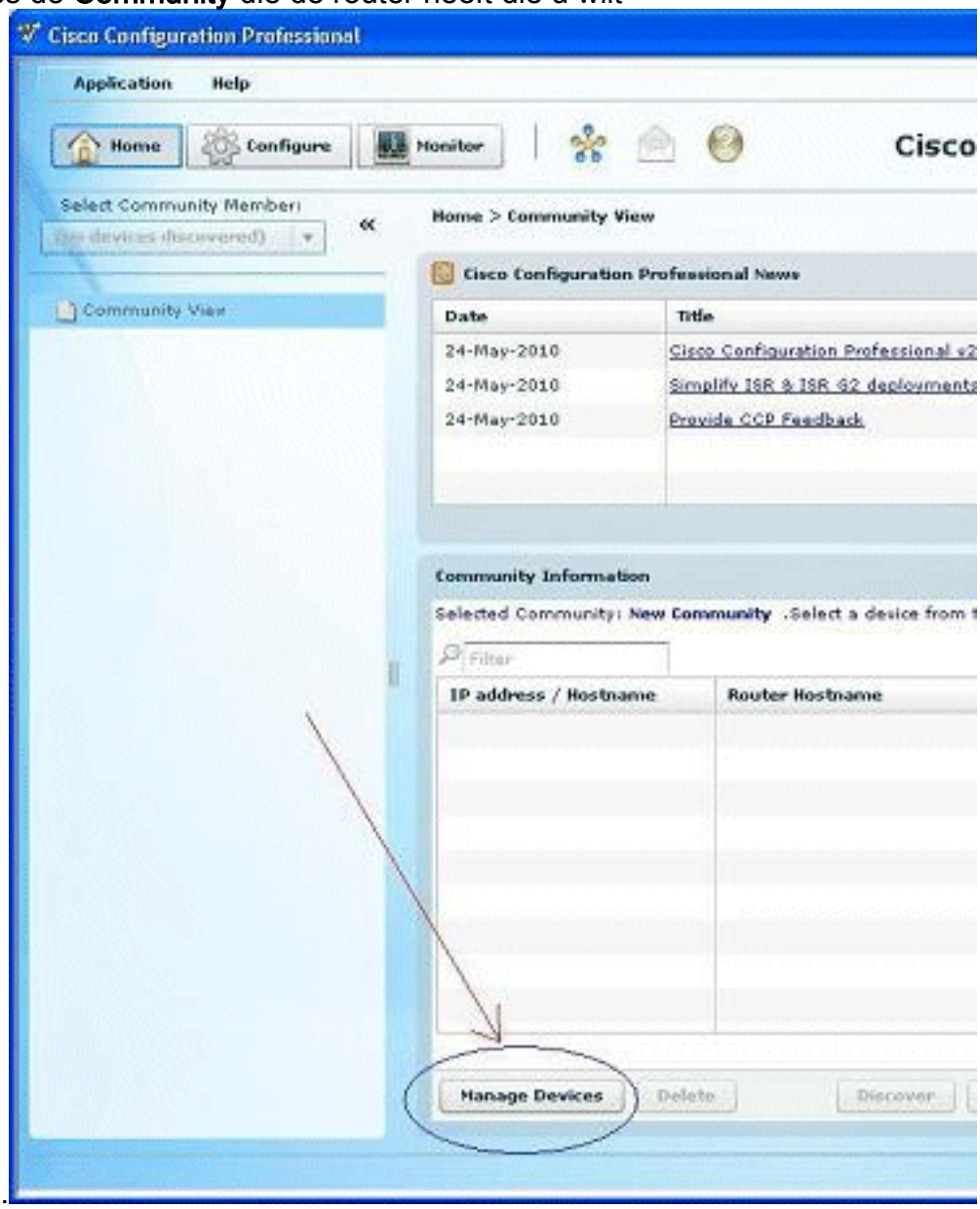
- Cisco CP versie 2.1

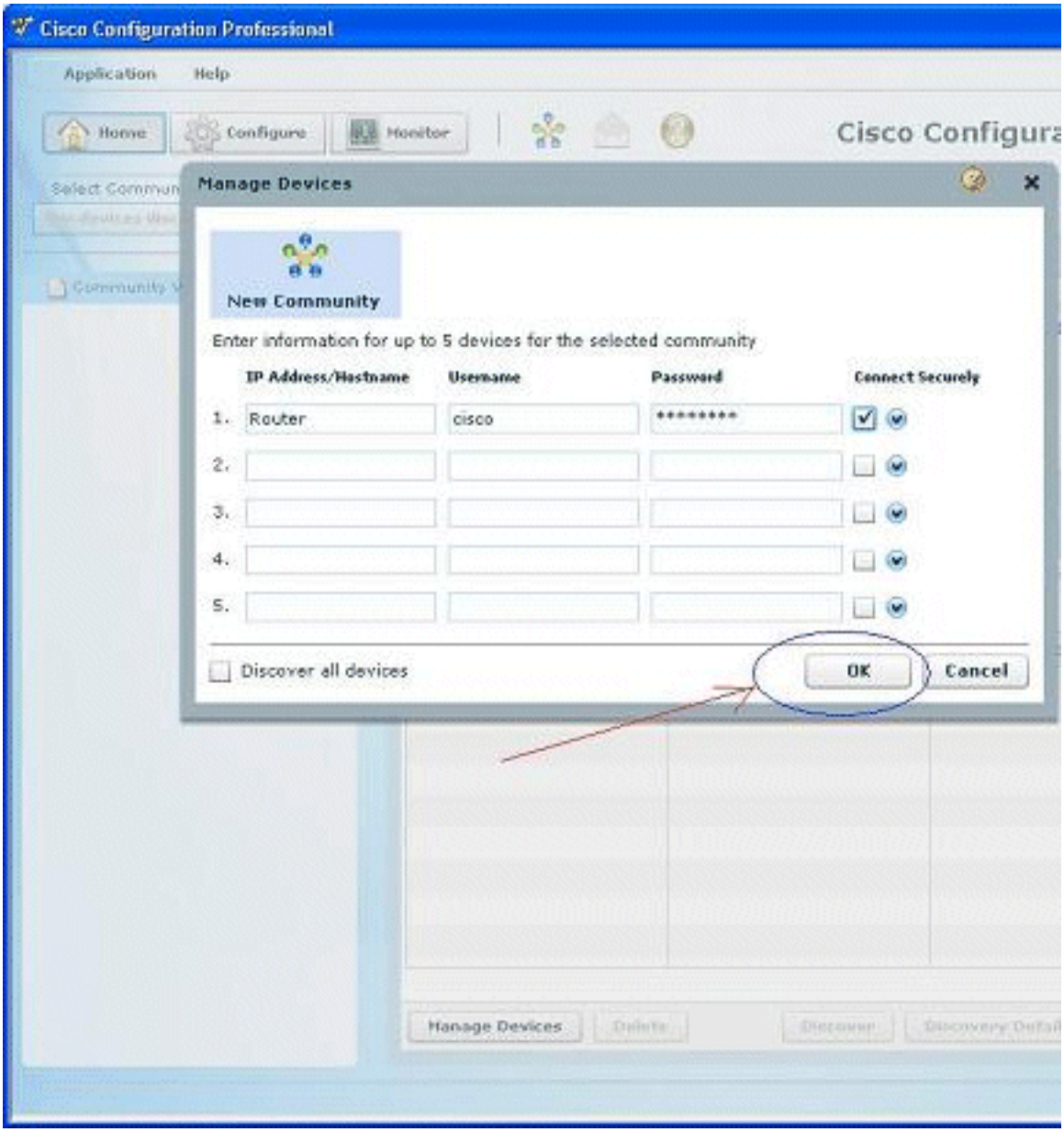
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Cisco CP installeren

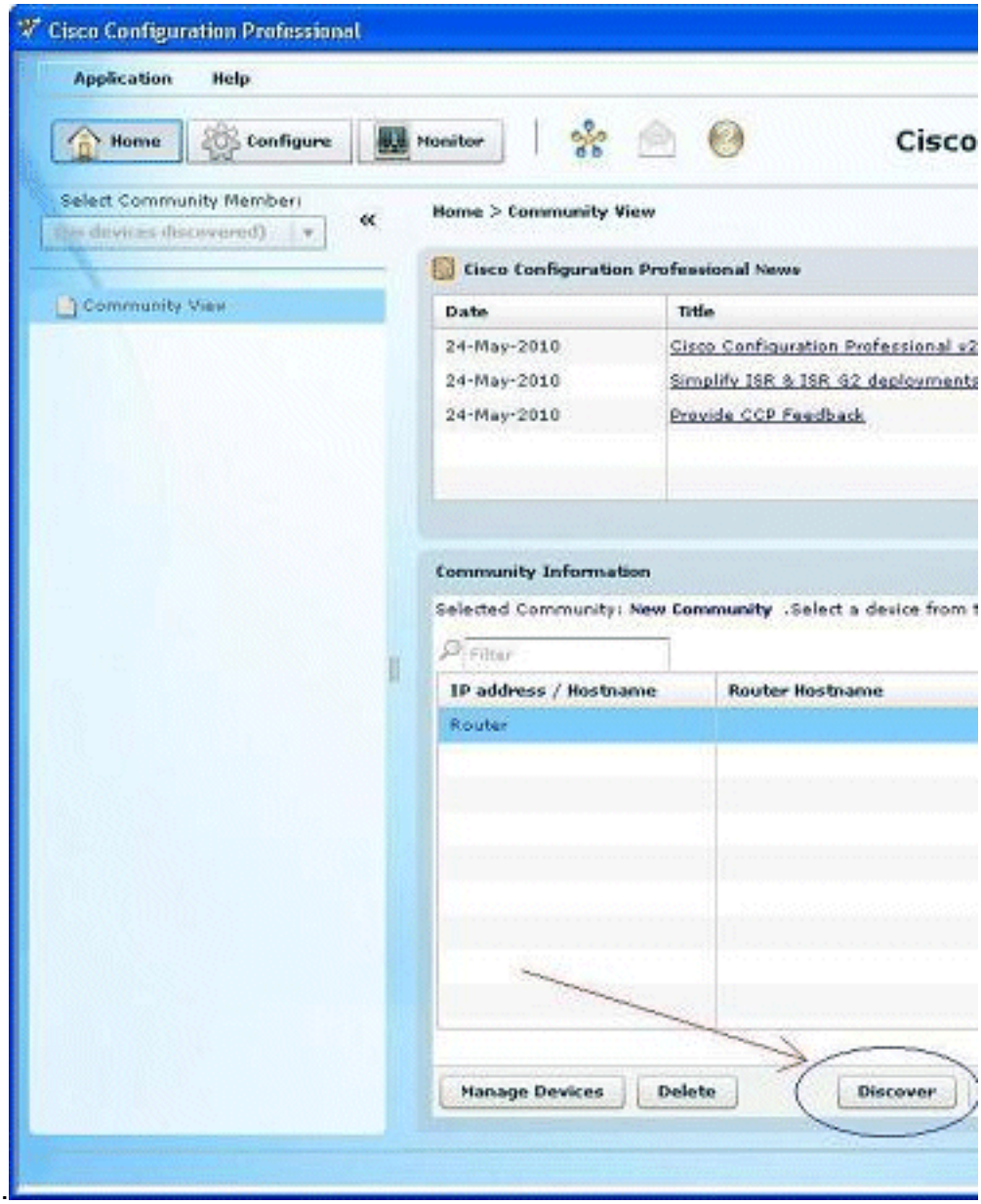
Voer deze stappen uit om Cisco CP te installeren:

1. Download Cisco CP V2.1 van het Cisco Software Center (alleen geregistreerde klanten) en installeer het op uw lokale pc.De laatste versie van Cisco CP is te vinden op de Cisco CP-website.
2. Start Cisco CP van uw lokale pc via **Start > Programma's > Cisco Configuration Professional (CCP)** en kies de **Community** die de router heeft die u wilt configureren.





3. Om het apparaat te ontdekken dat u wilt configureren, markeert u de router en klikt u op



Ophalen.

Opmerking: Raadpleeg het gedeelte Compatibele Cisco IOS-releases voor informatie over de Cisco-routermodellen en IOS-releases die compatibel zijn met Cisco CP v2.1.

Opmerking: Raadpleeg het gedeelte Systeemvereisten voor informatie over de PC-vereisten waarin Cisco CP v2.1 wordt uitgevoerd.

Routerconfiguratie om Cisco CP te starten

Voer deze configuratiestappen uit om Cisco CP op een Cisco-router uit te voeren:

1. Sluit aan op uw router met telnet, SSH of via de console.Geef de configuratie van het hele gebied op met deze opdracht:
```
Router(config)#enable
Router(config)#
```
2. Als HTTP en HTTPS ingeschakeld en geconfigureerd zijn om niet-standaard poortnummers te gebruiken, kunt u deze stap overslaan en simpelweg het poortnummer gebruiken dat al ingesteld is.Schakel de router HTTP- of HTTPS-server in met de opdrachten van Cisco IOS-software:
```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

3. Een gebruiker met voorkeursniveau 15 maken:
```
Router(config)# username privilege 15 password 0
```

   Opmerking: Vervang ***<gebruikersnaam>*** en *<wachtwoord>* ***door de gebruikersnaam en het wachtwoord die u wilt configureren.***
4. Configureer SSH en telnet voor lokaal inloggen en toegangsniveau 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. (Optioneel) Toegang voor lokale houtkap om de monitorfunctie voor logbestanden te ondersteunen:
```
Router(config)# logging buffered 51200 warning
```

Vereisten

Dit document gaat ervan uit dat de Cisco-router volledig gebruiksklaar is en is geconfigureerd om Cisco CP in staat te stellen configuratiewijzigingen door te voeren.

Voor volledige informatie over hoe u kunt beginnen met het gebruik van Cisco CP, raadpleegt u Introductie met Cisco Configuration Professional.

Conventies

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

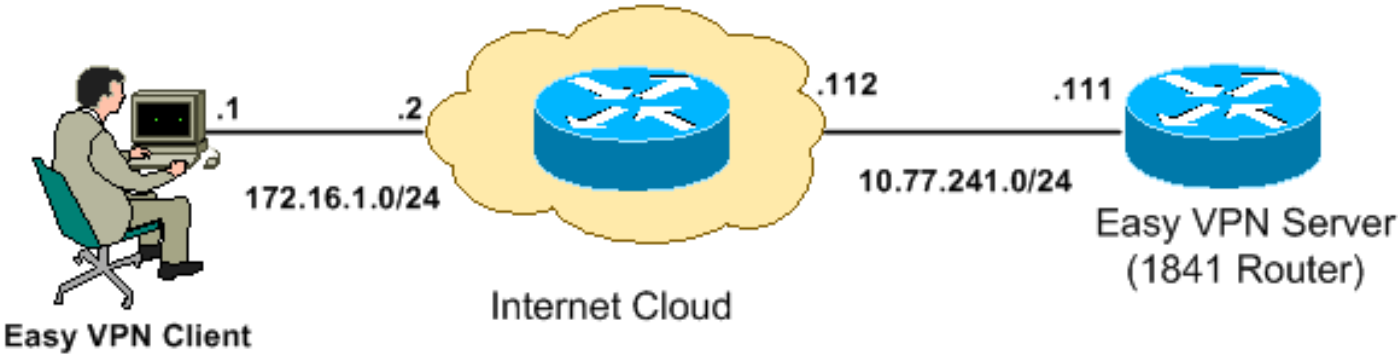
Configureren

In deze sectie, wordt u voorgesteld met de informatie om de basisinstellingen voor een router in een netwerk te vormen.

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:

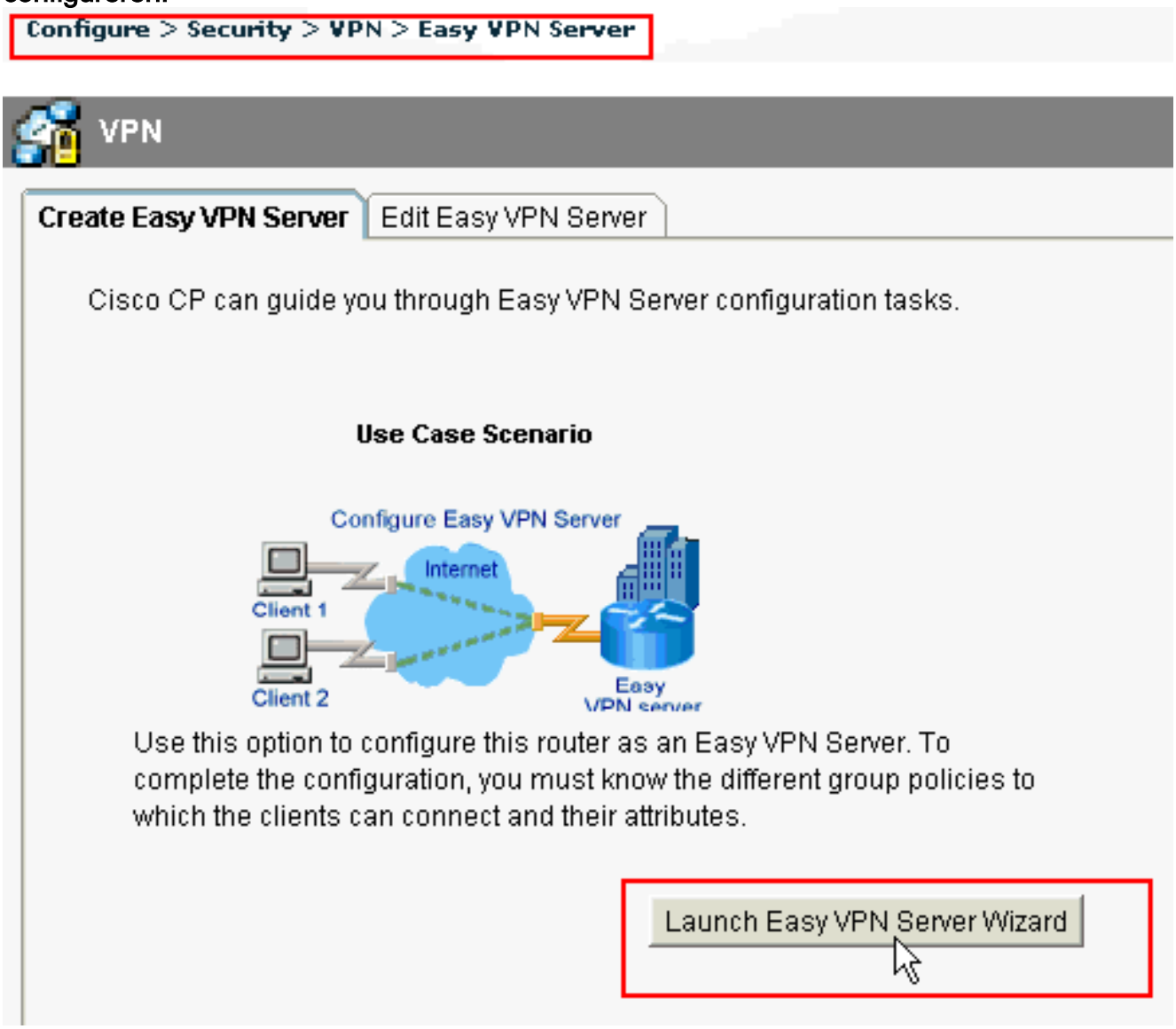


Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

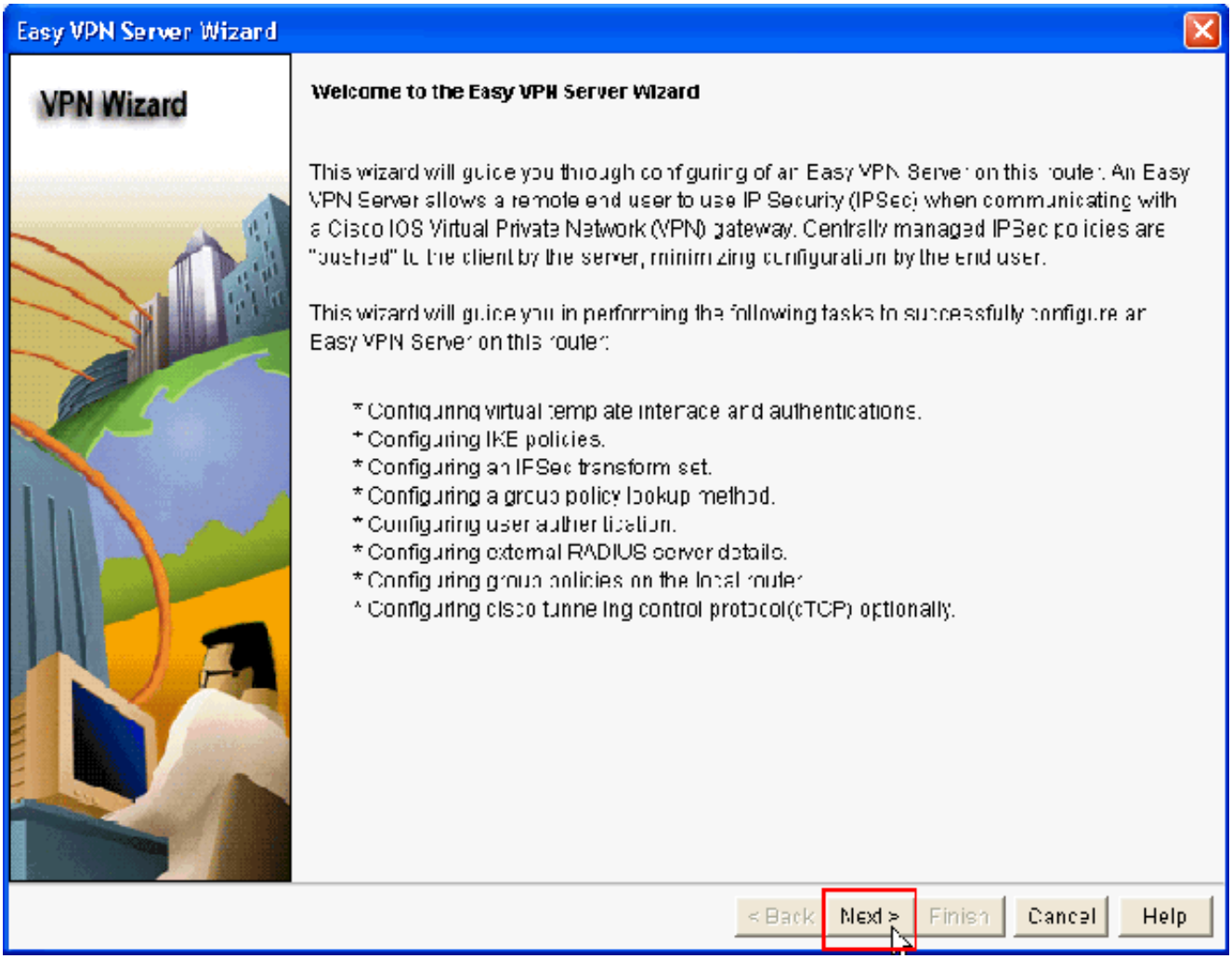
Cisco CP - Makkelijk VPN-serverconfiguratie

Voer deze stappen uit om de Cisco IOS-router als een Makkelijk VPN-server te configureren:

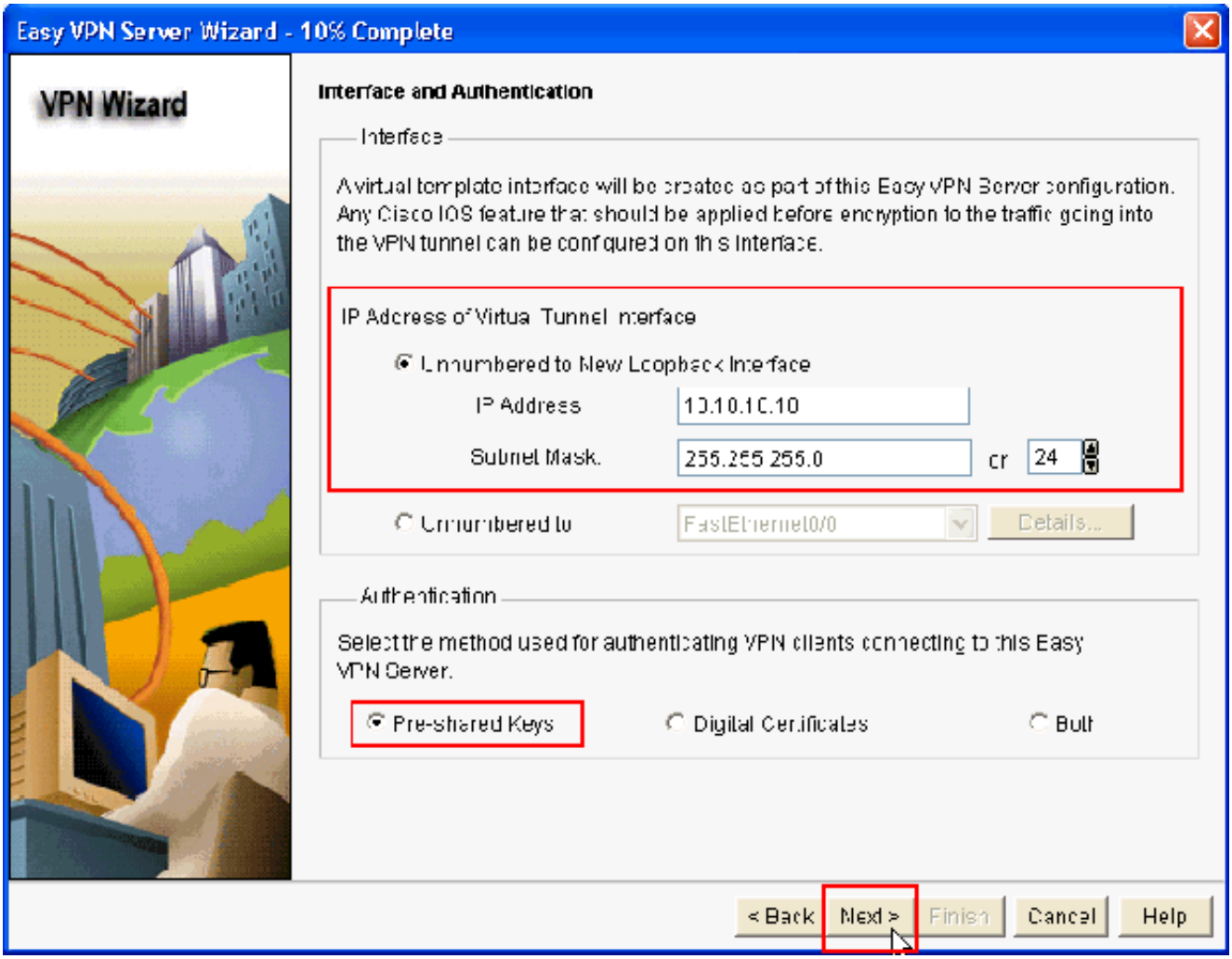
1. Kies **Configureren > Beveiliging > VPN > Makkelijk VPN-server > Makkelijk VPN-server maken en klik op Wizard Makkelijk VPN-server starten om de Cisco IOS-router als een Makkelijk VPN-server te configureren:**



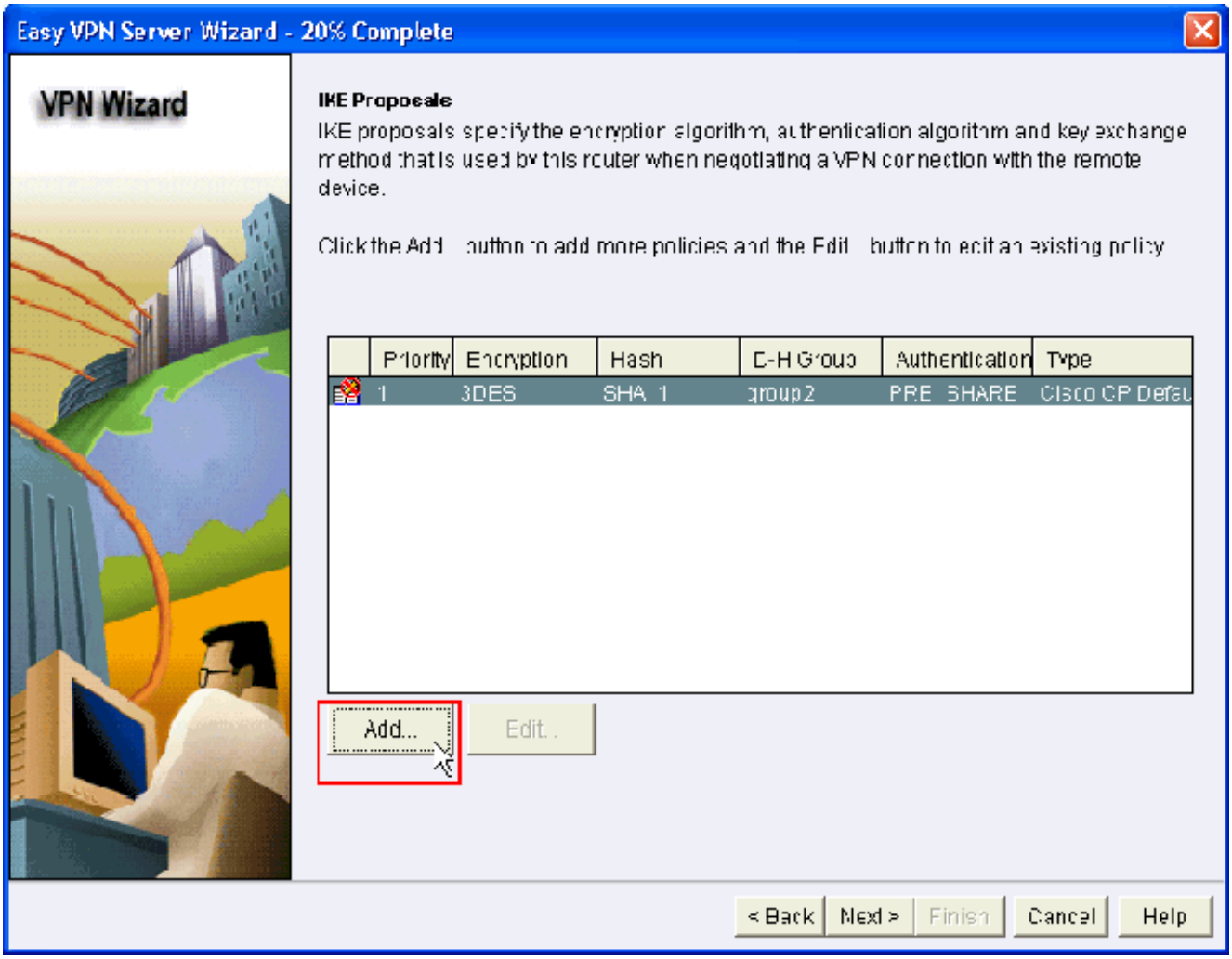
2. Klik op **Volgende** om verder te gaan met de configuratie **Makkelijk VPN-server**.



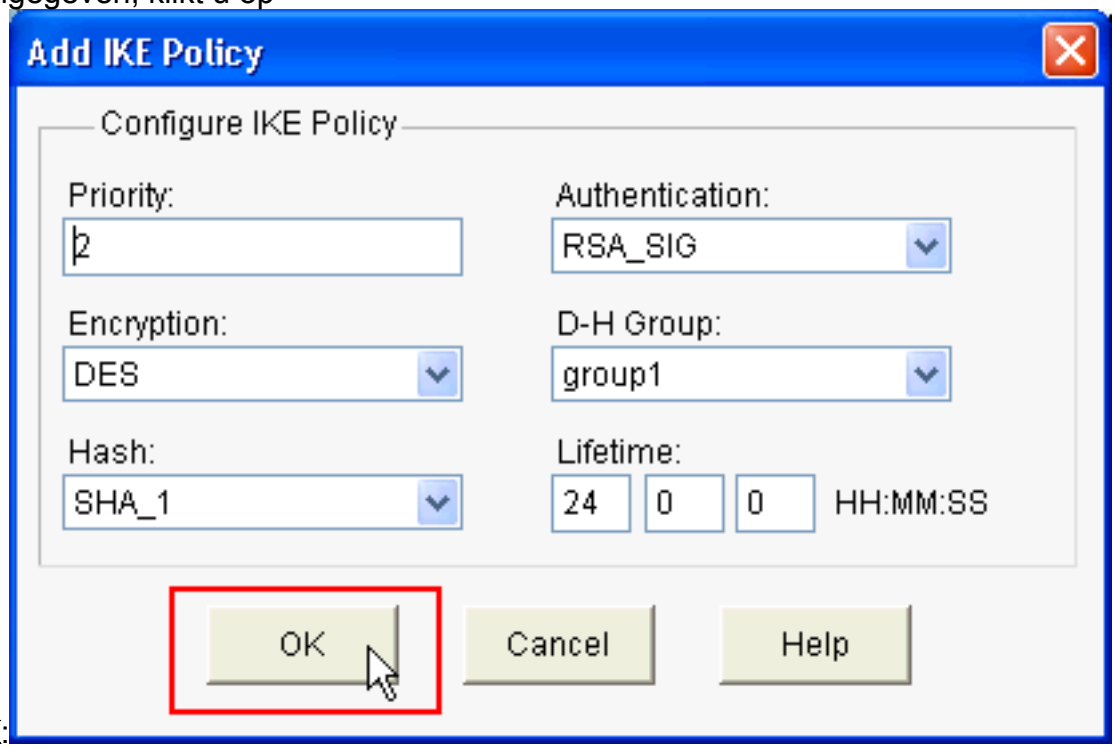
3. In het resulterende venster wordt een **virtuele interface** ingesteld als deel van de configuratie Makkelijk VPN-server. Typ het **IP-adres van de virtuele tunnelinterface** en kies ook de **verificatiemethode** die wordt gebruikt voor het authentiseren van de VPN-clients. Hier wordt de **Pre-Shared Keys** van de authenticatiemethode gebruikt. Klik op **Volgende**:



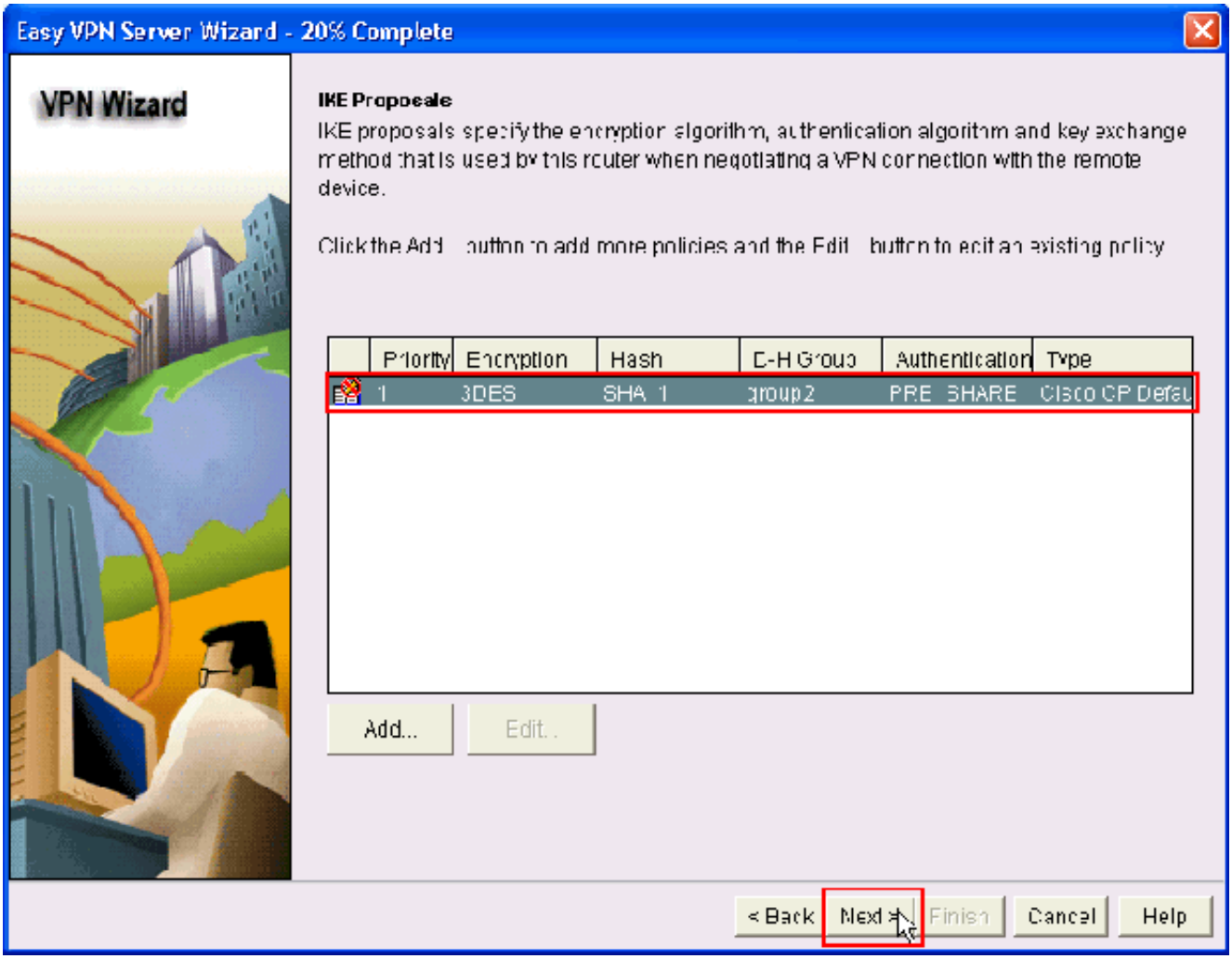
4. Specificeer het **algoritme voor encryptie, verificatie-algoritme en** de **methode** voor **belangrijke uitwisseling** die door deze router moet worden gebruikt bij onderhandelingen met het afstandsapparaat. Een standaard IKE-beleid is aanwezig op de router die indien nodig kan worden gebruikt. Als u een nieuw IKE-beleid wilt toevoegen, klikt u op Toevoegen.



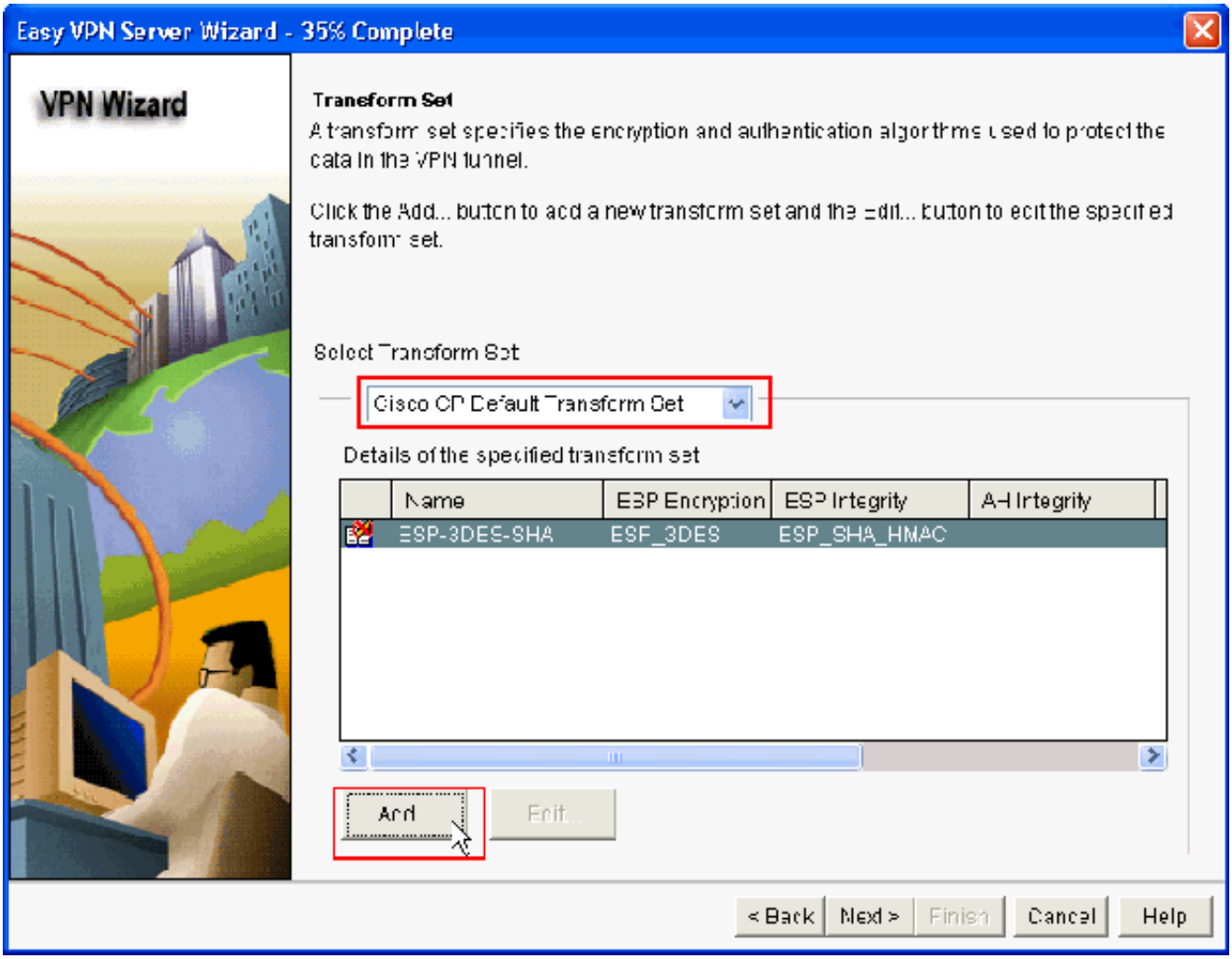
5. **Encryption Algorithm**, **verificatie-algoritme** en de **Key Exchange-methode** zoals hier aangegeven, klikt u op **OK**:



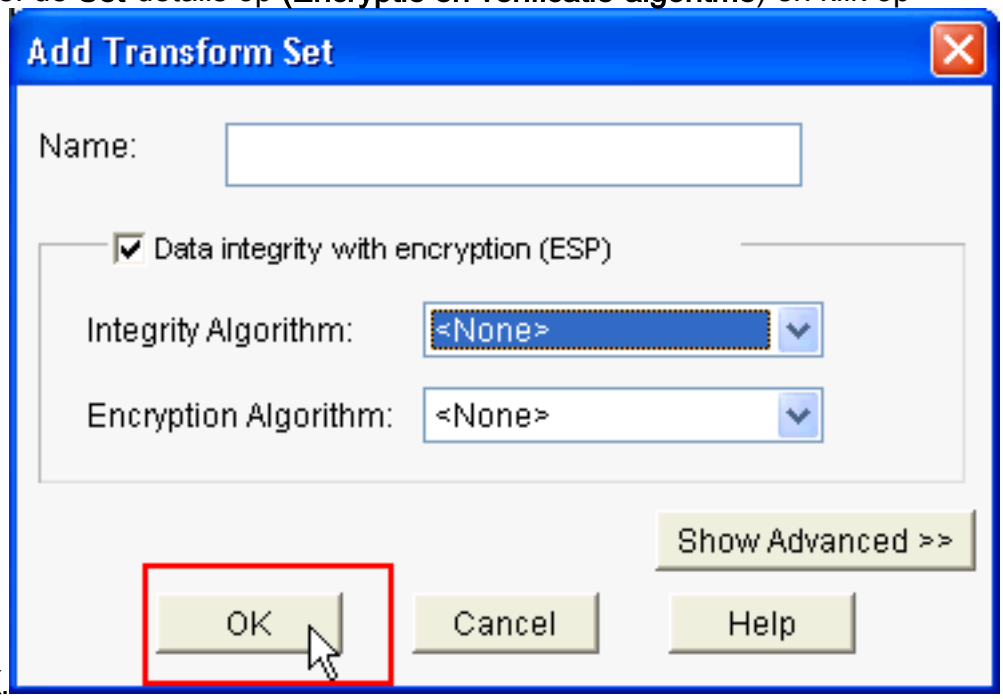
6. Het **beleid** voor **standaard IKE** wordt in dit voorbeeld gebruikt. Kies het standaard IKE-beleid en klik op **Volgende**.



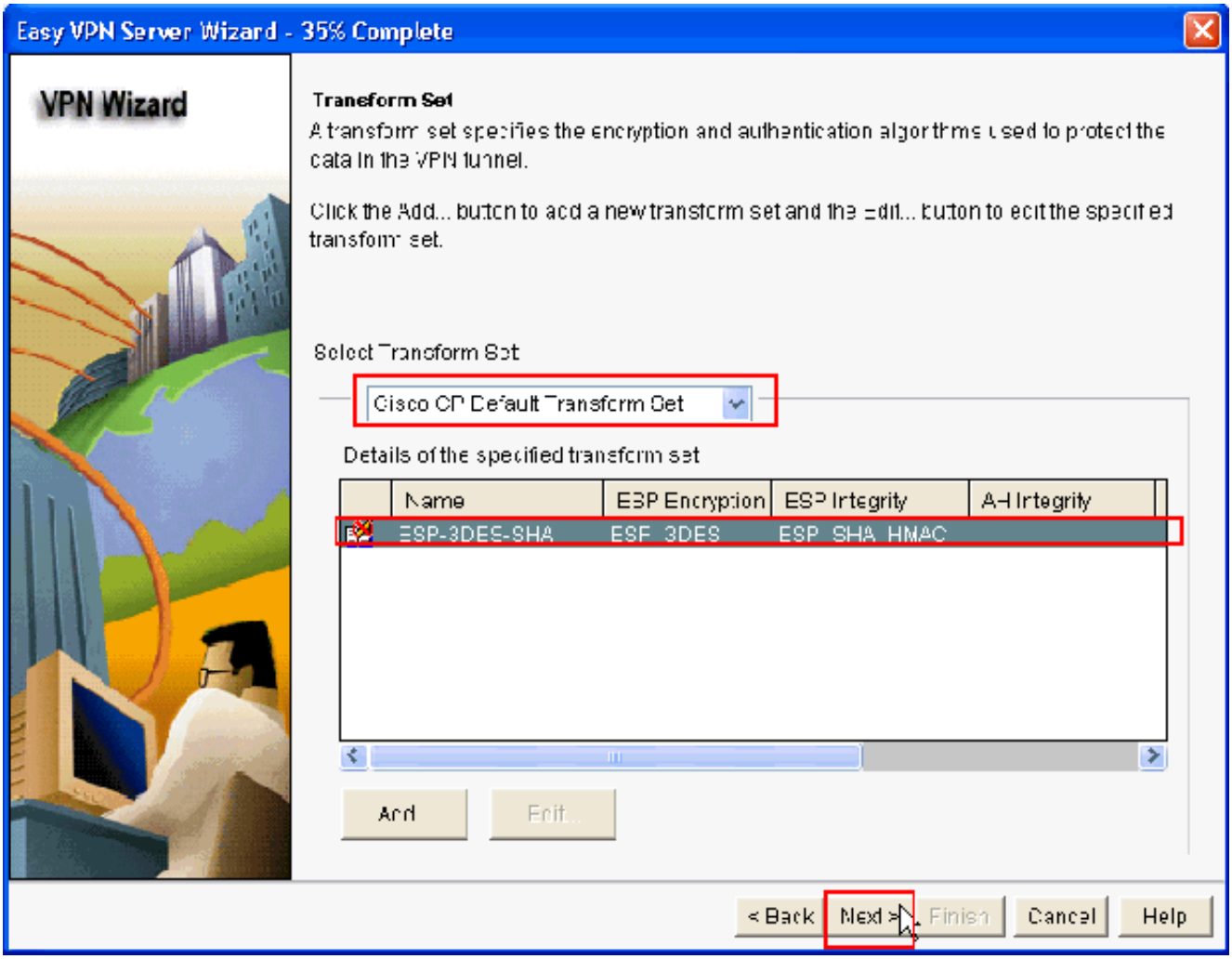
7. In het nieuwe venster dienen de gegevens **over** de **verzameling** transformaties te worden verstrekt. Met de Instellen Omzetten wordt de **Encryptie** en **verificatie**-algoritmen gespecificeerd die worden gebruikt om **gegevens in VPN-tunnels** te beschermen. Klik op **Add** om deze details te geven. U kunt indien nodig een aantal transformatiesets toevoegen wanneer u op **Toevoegen** klikt en de details opgeeft.**Opmerking: CP Standaard transformatie-set** is standaard op de router aanwezig als deze wordt geconfigureerd met behulp van **Cisco CP**.



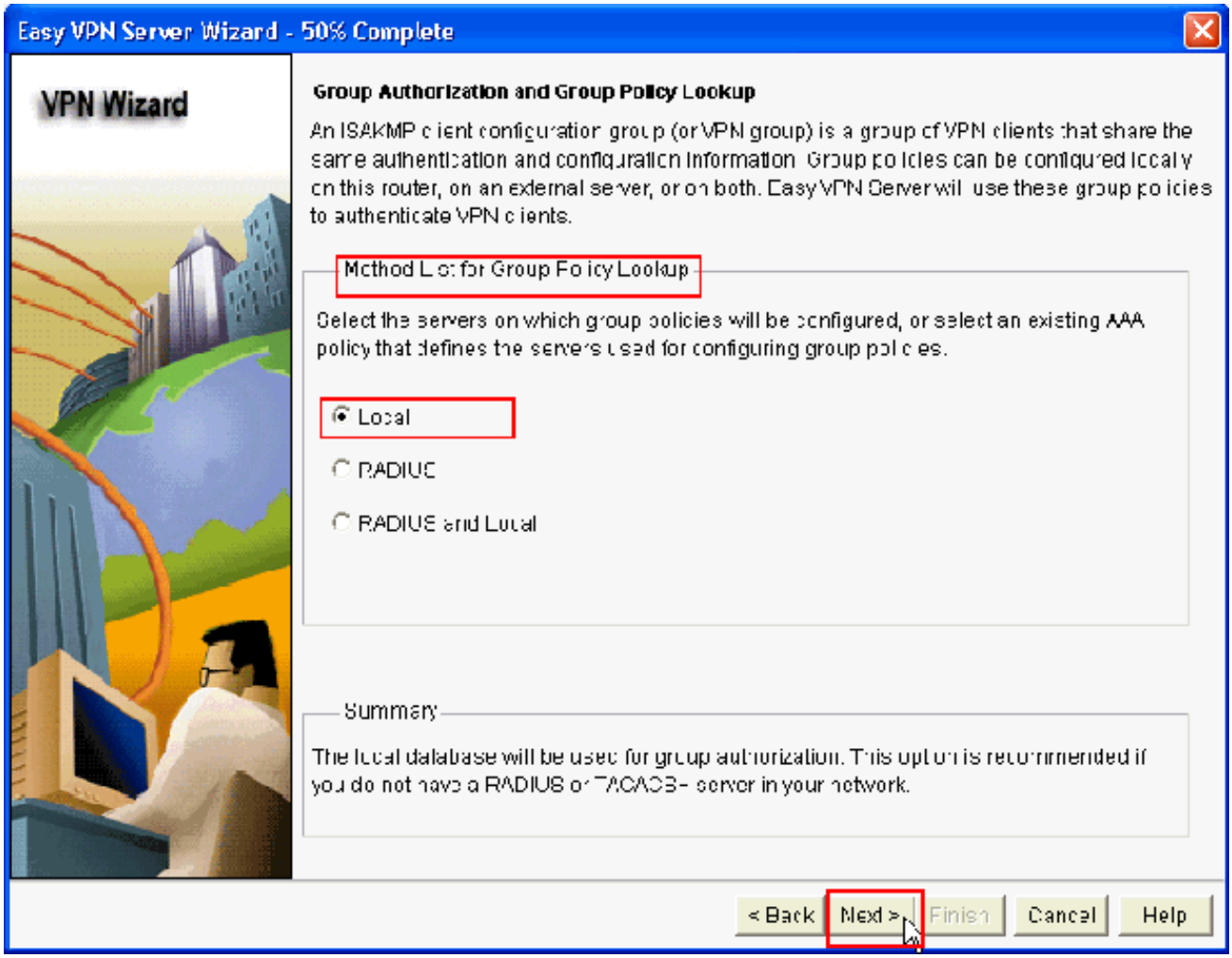
8. Geef de **Set**-details op **(Encryptie en verificatie-algoritme)** en klik op **OK**.



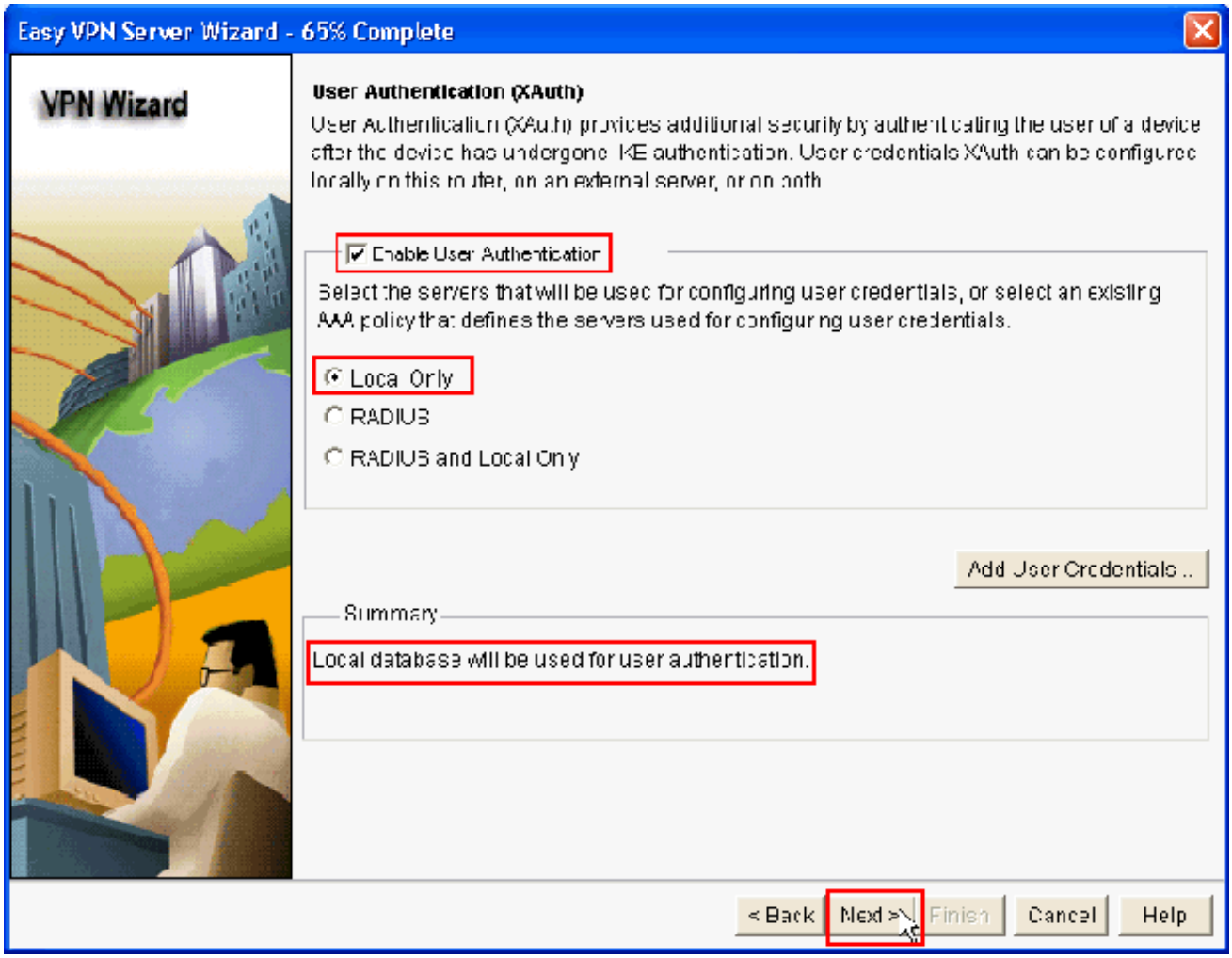
9. De **standaardinstelling voor het omzetten van de** naam **CP standaardtransformatie** wordt in dit voorbeeld gebruikt. Kies de standaardinstelling Omzetten en klik op **Volgende**.



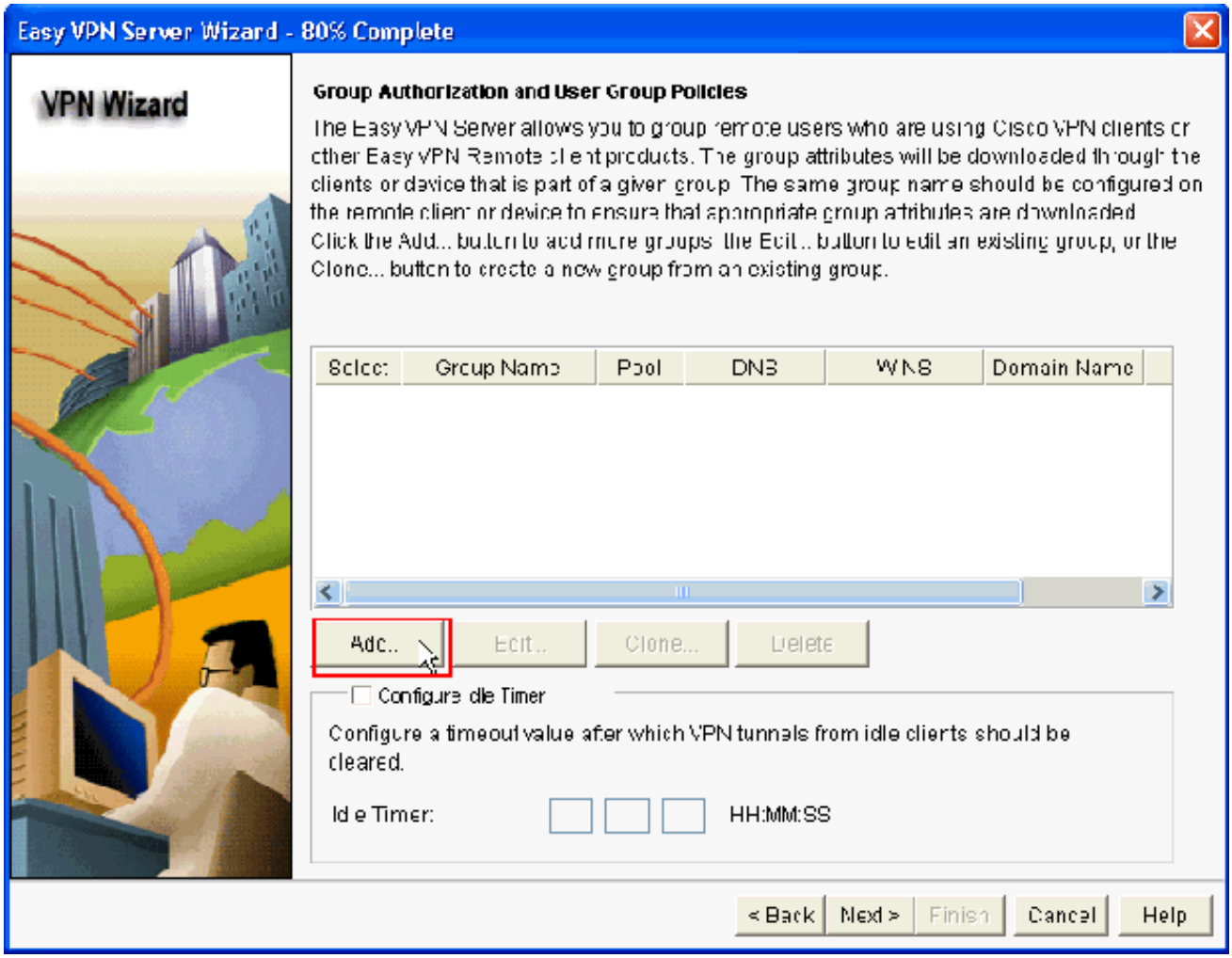
10. Kies in het nieuwe venster de server waarop het groepsbeleid wordt geconfigureerd, die ofwel **lokaal** of **RADIUS** kan zijn, ofwel **lokaal en RADIUS**. In dit voorbeeld gebruiken we **Local server** om groepsbeleid te configureren. Kies **Lokaal** en klik op **Volgende**.



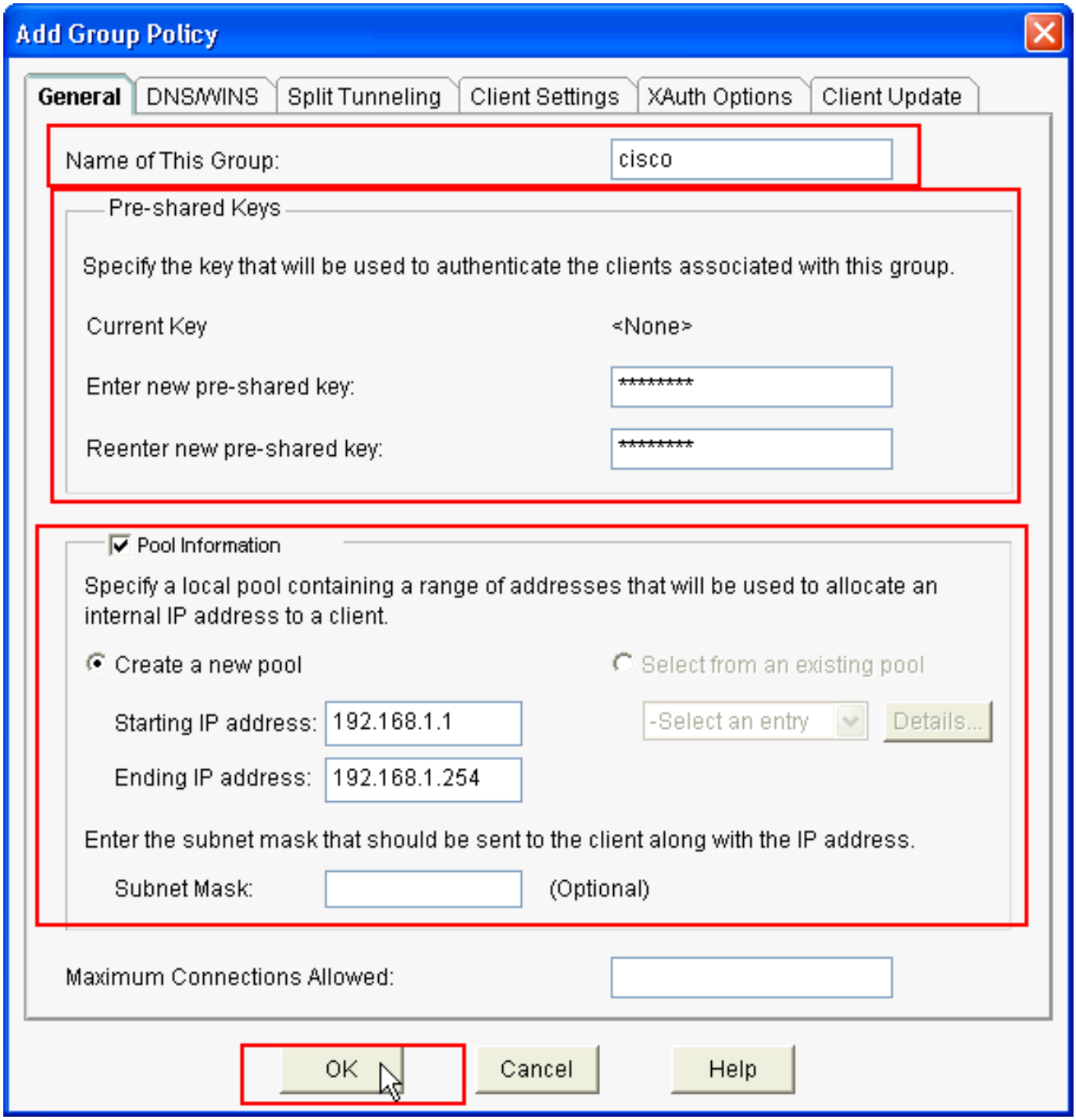
11. Kies de server die gebruikt moet worden voor gebruikersverificatie in dit nieuwe venster en die **alleen lokaal** of **RADIUS** kan zijn, **alleen lokaal en RADIUS**. In dit voorbeeld gebruiken we **lokale server** om gebruikersreferenties voor authenticatie te configureren. Controleer of het aankruisvakje naast **Gebruikersverificatie inschakelen** is ingeschakeld. Kies **alleen lokaal** en klik op
Volgende.



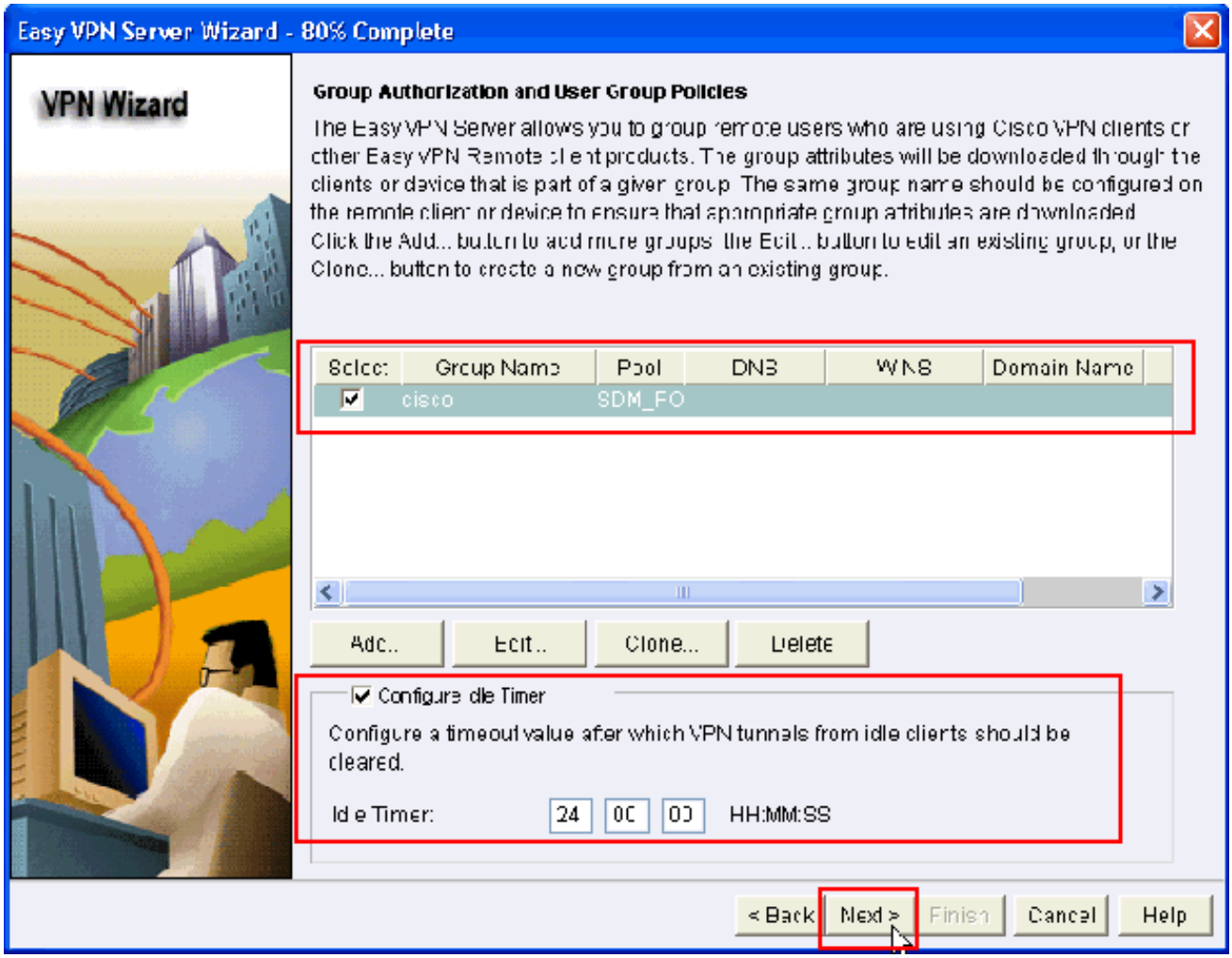
12. Klik op **Add** om een nieuw groepsbeleid te maken en de externe gebruikers in deze groep toe te
voegen.



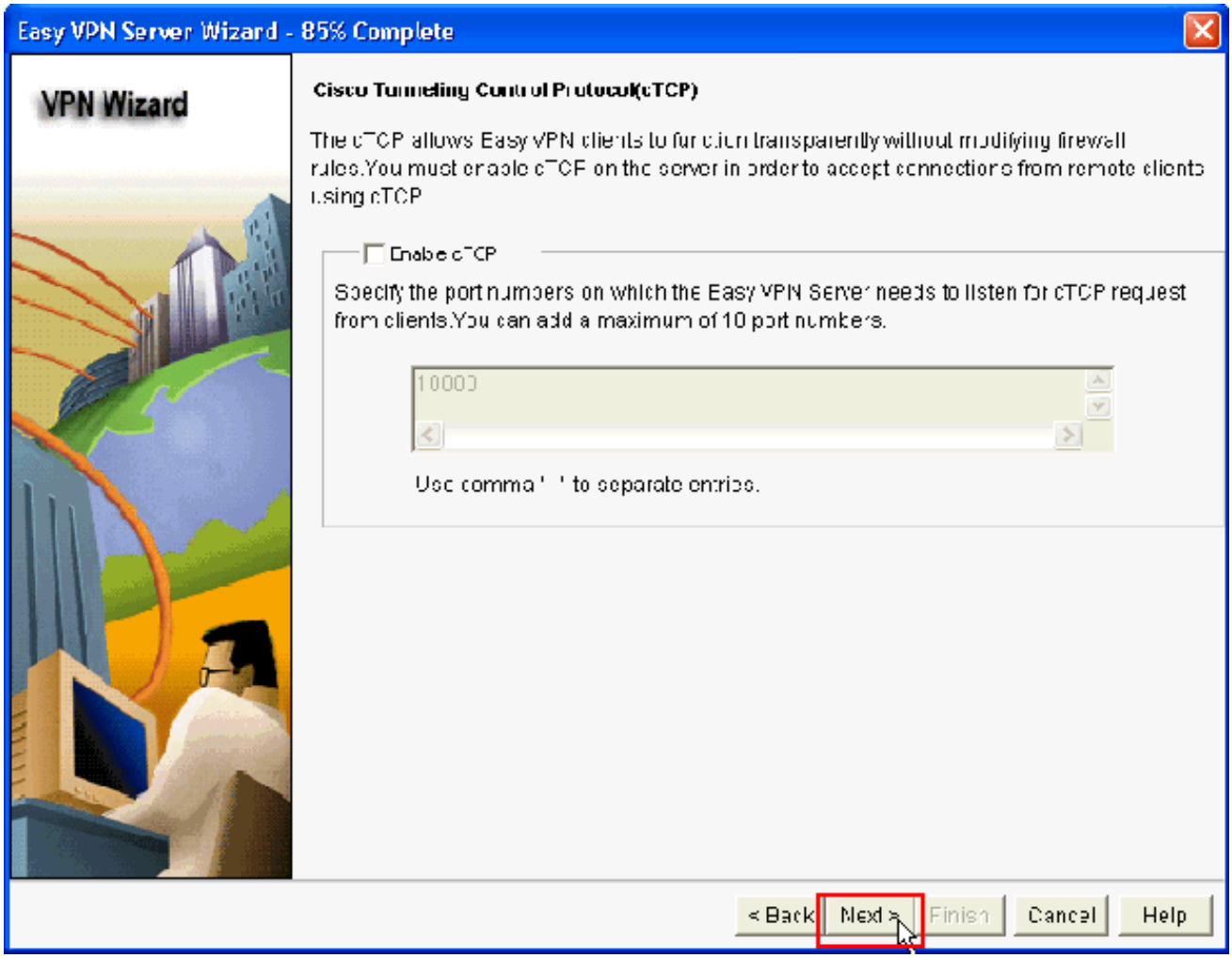
13. In het venster Add Group Policy, typt u de groepsnaam in de ruimte voor naam van deze groep (cisco in dit voorbeeld) samen met de pre-gedeelde toets en de IP-pool (het **IP-adres** en **IP-adres**) zoals weergegeven en klikt u op **OK.N.B.:** U kunt een nieuwe IP-pool maken of indien aanwezig een bestaande IP-pool
gebruiken.



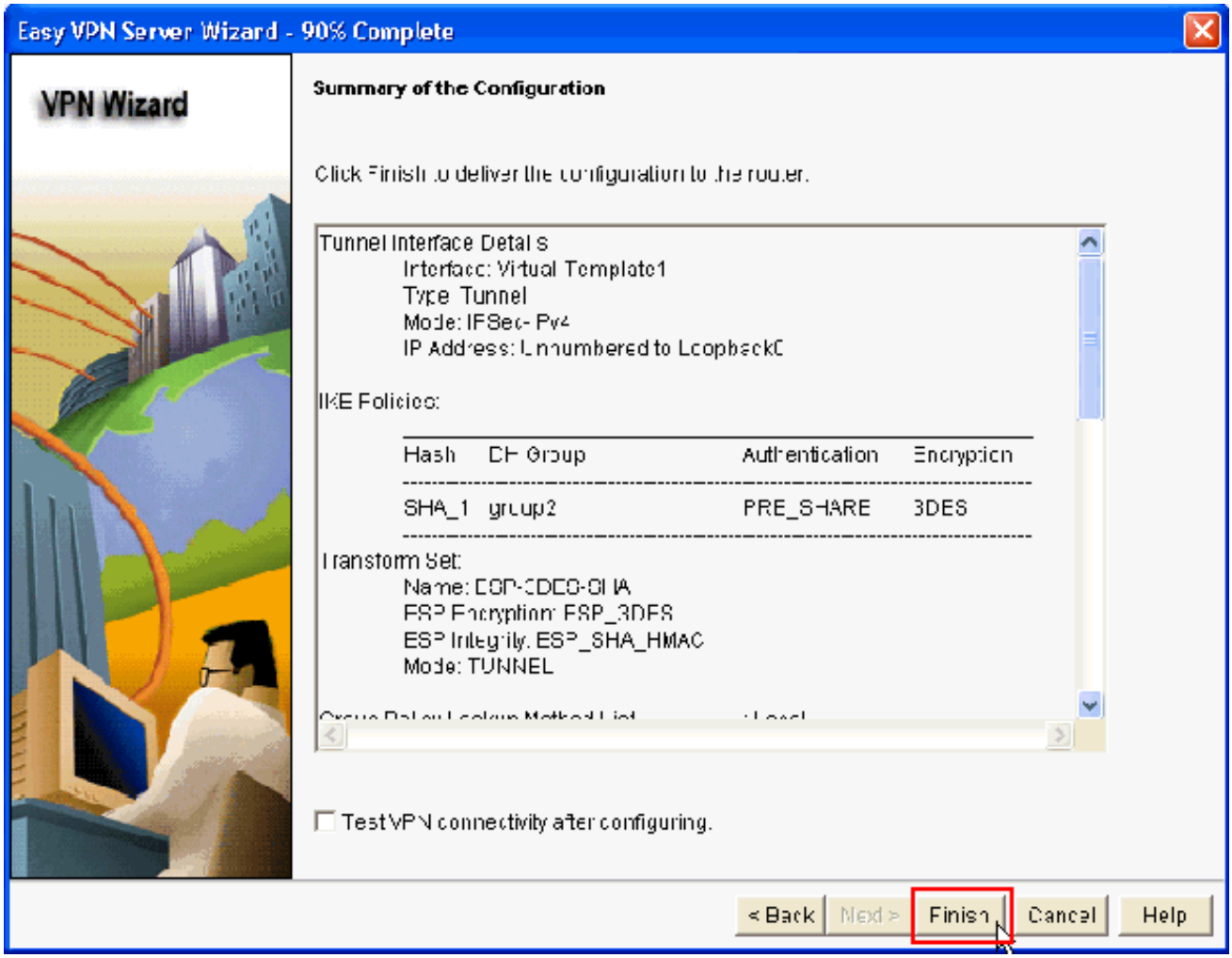
14. Kies nu het nieuwe **groepsbeleid** dat met de naam **cisco** is gemaakt en klik vervolgens op het aankruisvakje naast **het configureren van de inactiviteitstimer** zoals vereist om de **inactiviteitstimer** te configureren. Klik op **Volgende**.



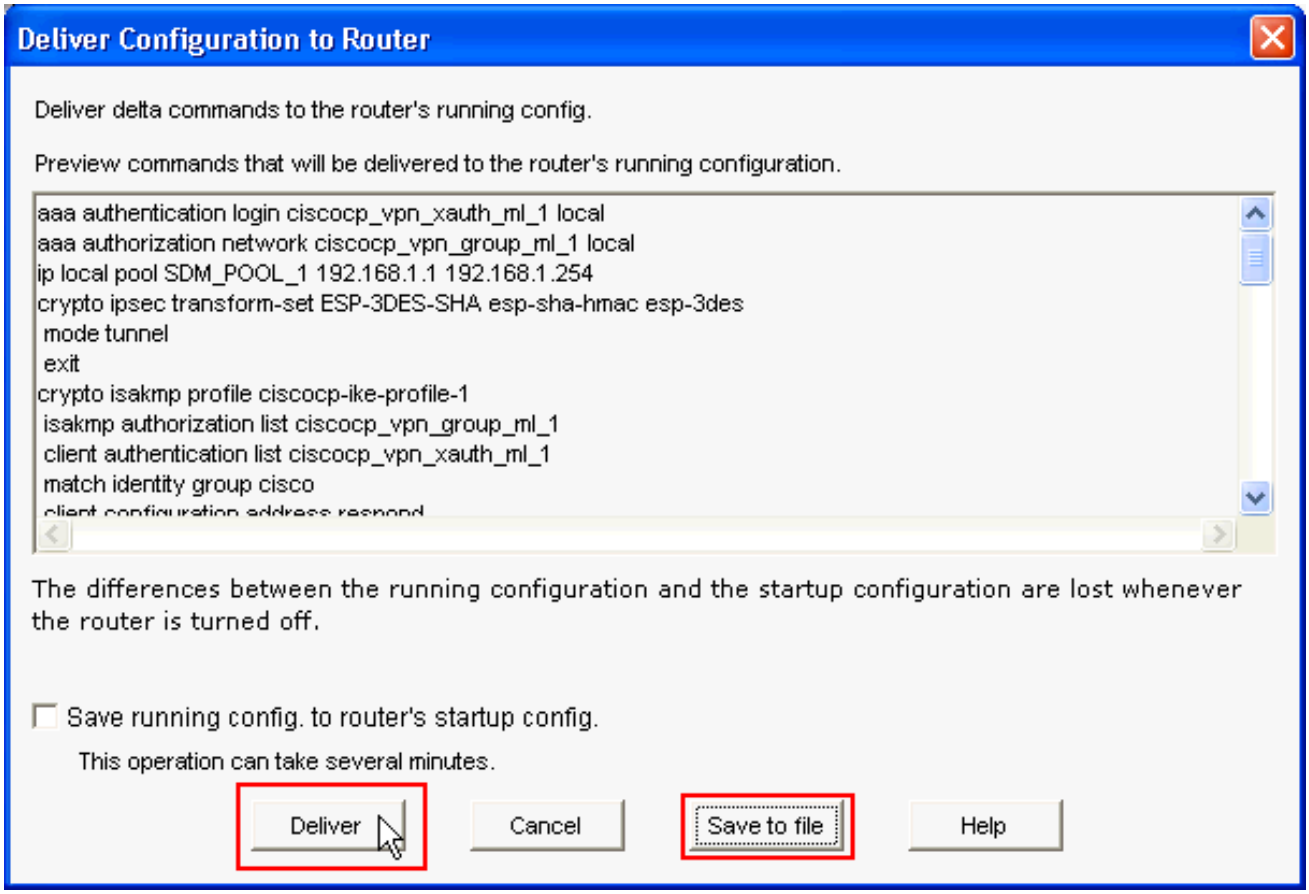
15. Schakel **Cisco Tunneling Control Protocol** (cTCP) indien nodig in. Klik anders op **Volgende**.



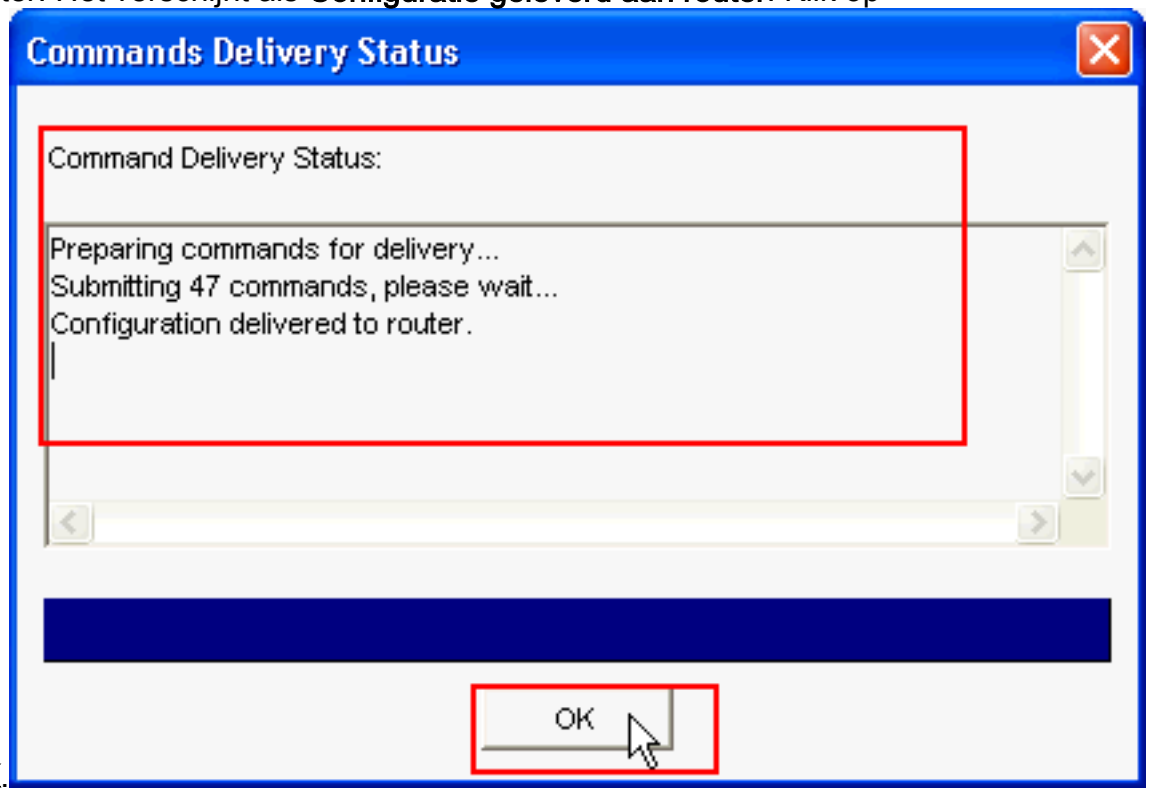
16. Bekijk de **samenvatting van de configuratie**. Klik op **Voltooien**.



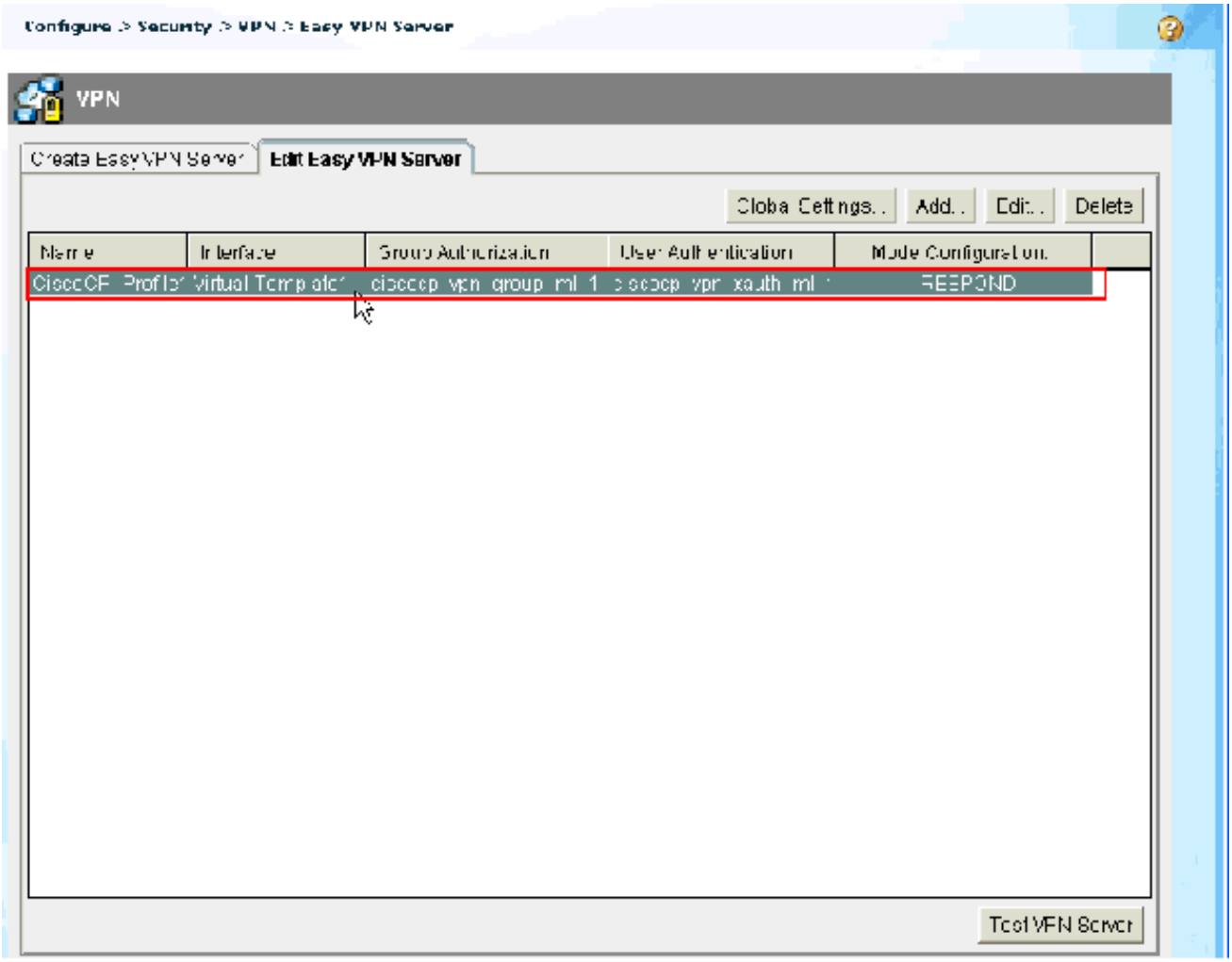
17. In het venster **Delivery Configuration to Router** klikt u op **Deliver** om de configuratie aan de router te leveren. U kunt op **Opslaan naar bestand** klikken om de configuratie als bestand op de PC op te
slaan.



18. Het venster **Opdracht Delivery Status** toont de leveringsstatus van de opdrachten naar de router. Het verschijnt als **Configuratie geleverd aan router**. Klik op **OK**.



19. U kunt de nieuwe Easy VPN-server zien. U kunt de bestaande server bewerken door te kiezen voor **Makkelijk VPN-server bewerken**. Dit voltooit de configuratie van de Gemakkelijke VPN-server op de Cisco IOS-router.



CLI-configuratie

Routerconfiguratie

```
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
```

Verifiëren

Makkelijk VPN-server - toont opdrachten

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

- **toon crypto isakmp sa**-toont alle huidige IKE SAs bij een 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
```

- **toon crypto ipsec sa**-Toont alle huidige IPsec SAs bij een 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
```

Problemen oplossen

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over Debug Commands voordat u debug-opdrachten geeft.

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- Cisco Configuration Professional Quick Start-handleiding
- Cisco-pagina voor productondersteuning - routers
- Technische ondersteuning en documentatie – Cisco Systems