

# IOS-Router als Easy VPN-Server mit Konfigurationsbeispiel für Professional

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Installation von Cisco CP](#)

[Routerkonfiguration zum Ausführen des Cisco CP](#)

[Anforderungen](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Cisco CP = Easy VPN Server Configuration](#)

[CLI-Konfiguration](#)

[Überprüfen](#)

[Easy VPN-Server - Befehle anzeigen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie einen Cisco IOS<sup>®</sup>-Router mithilfe von [Cisco Configuration Professional \(Cisco CP\)](#) und der CLI als Easy VPN (EzVPN)-Server konfigurieren. Mit der Easy VPN Server-Funktion kann ein Remote-Endbenutzer über IP Security (IPsec) mit einem beliebigen Cisco IOS Virtual Private Network (VPN)-Gateway kommunizieren. Zentral verwaltete IPsec-Richtlinien werden vom Server auf das Client-Gerät "übertragen", wodurch die Konfiguration durch den Endbenutzer minimiert wird.

Weitere Informationen zu Easy VPN Server finden Sie im [Easy VPN Server-Abschnitt Secure Connectivity Configuration Guide Library, Cisco IOS Release 12.4T](#).

## Voraussetzungen

### Verwendete Komponenten

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

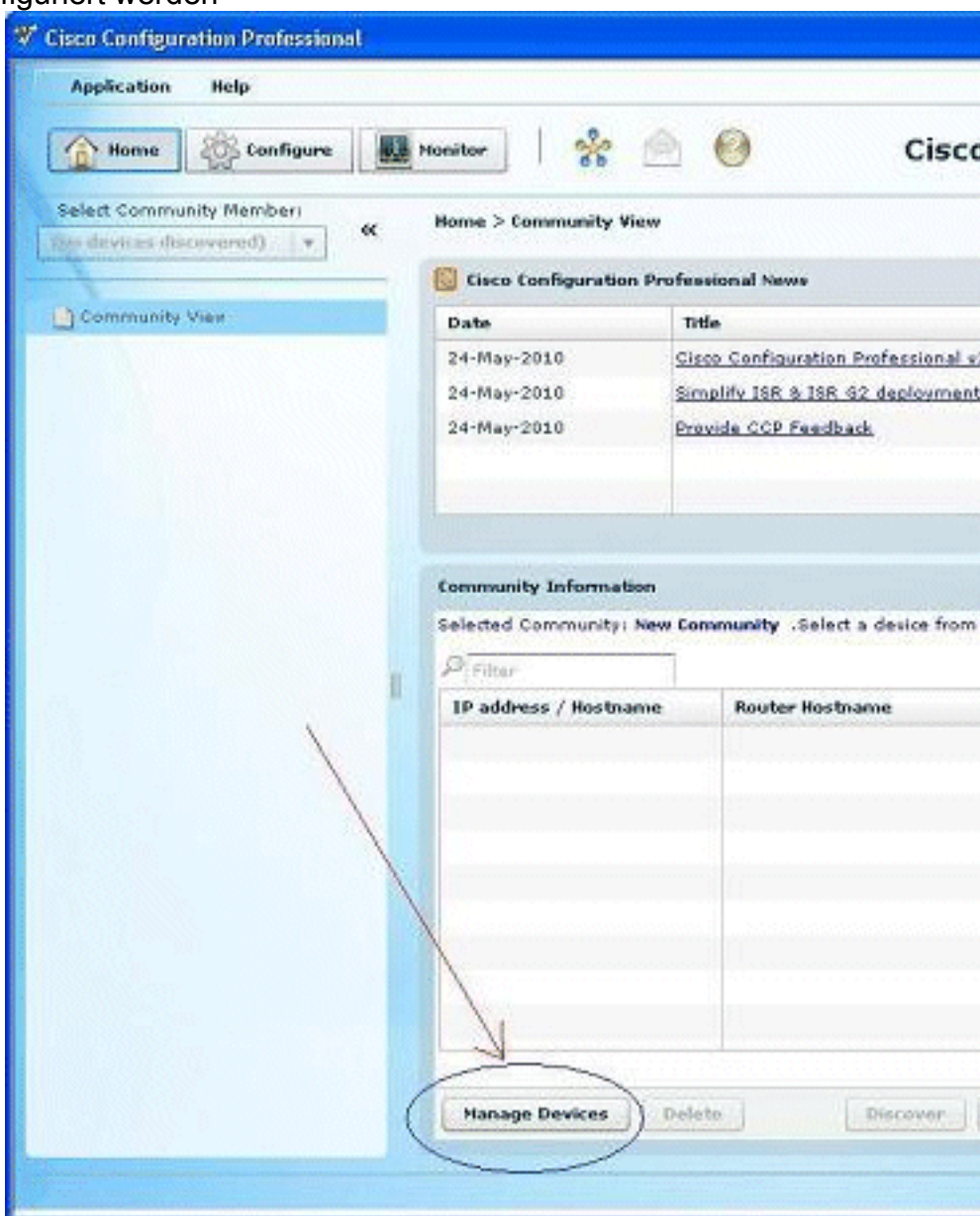
- Cisco 1841 Router mit Cisco IOS Software, Version 12.4(15T)
- Cisco CP-Version 2.1

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.

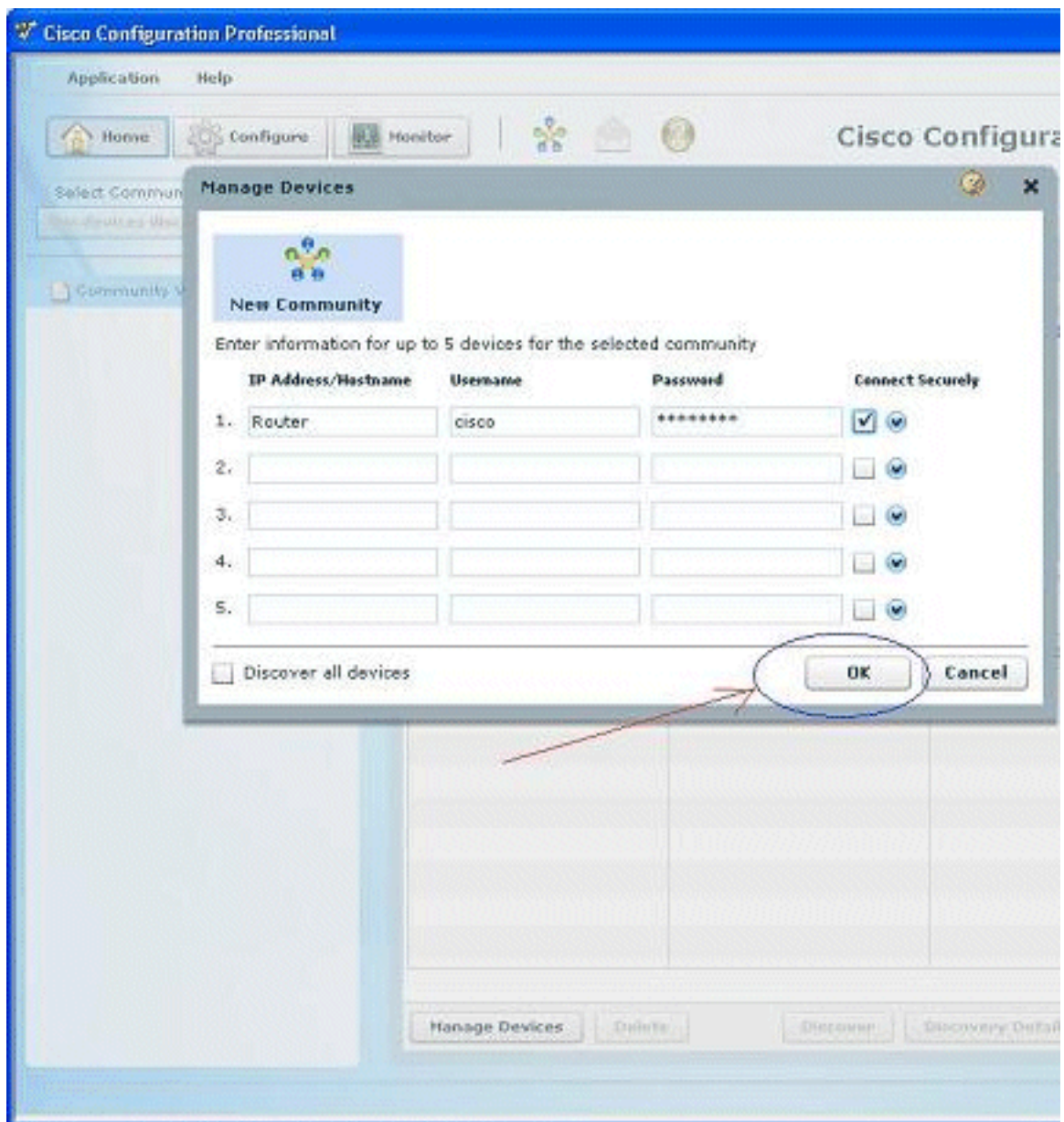
## Installation von Cisco CP

Führen Sie die folgenden Schritte aus, um Cisco CP zu installieren:

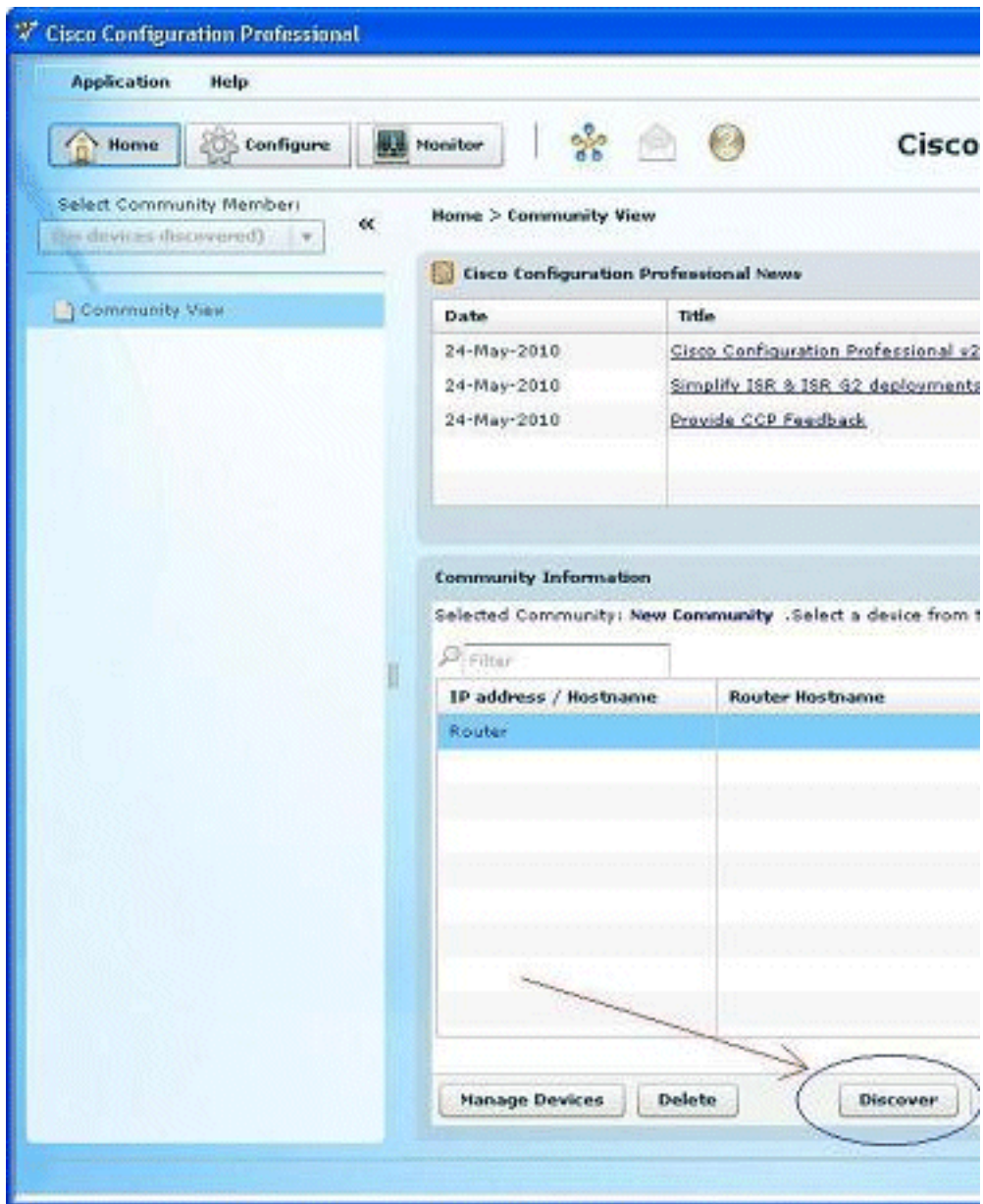
1. Laden Sie Cisco CP V2.1 vom [Cisco Software Center](#) (nur [registrierte](#) Kunden) herunter, und installieren Sie es auf Ihrem lokalen PC. Die neueste Version des Cisco CP finden Sie auf der [Cisco CP-Website](#).
2. Starten Sie Cisco CP von Ihrem lokalen PC aus über **Start > Programme > Cisco Configuration Professional (CCP)**, und wählen Sie die **Community** aus, für die der Router konfiguriert werden



soll.



3. Markieren Sie den Router, um das Gerät zu ermitteln, das Sie konfigurieren möchten, und klicken Sie auf **Discover**



(Erkennung).

**Hinweis:** Informationen zu den Cisco Router-Modellen und IOS-Versionen, die mit Cisco CP v2.1 kompatibel sind, finden Sie im Abschnitt [Kompatible Cisco IOS-Versionen](#).

**Hinweis:** Weitere Informationen zu den PC-Anforderungen, auf denen Cisco CP v2.1 ausgeführt wird, finden Sie im Abschnitt [Systemanforderungen](#).

## [Routerkonfiguration zum Ausführen des Cisco CP](#)

Führen Sie die folgenden Konfigurationsschritte aus, um Cisco CP auf einem Cisco Router auszuführen:

1. Stellen Sie über Telnet, SSH oder die Konsole eine Verbindung zum Router her. Wechseln Sie mit dem folgenden Befehl in den globalen Konfigurationsmodus:  

```
Router(config)#enable
Router(config)#
```
2. Wenn HTTP und HTTPS für die Verwendung von nicht standardmäßigen Portnummern aktiviert und konfiguriert sind, können Sie diesen Schritt überspringen und einfach die bereits konfigurierte Portnummer verwenden. Aktivieren Sie den HTTP- oder HTTPS-Router mithilfe der folgenden Cisco IOS Software-Befehle:  

```
Router(config)# ip http server
```

```
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

### 3. Erstellen eines Benutzers mit der Berechtigungsstufe 15:

```
Router(config)# username privilege 15 password 0
```

**Hinweis:** Ersetzen Sie *<Benutzername>* und *<Kennwort>* durch den Benutzernamen und das Kennwort, die Sie konfigurieren möchten.

### 4. Konfigurieren Sie SSH und Telnet für die lokale Anmeldung und die Berechtigungsebene 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. (Optional) Aktivieren Sie die lokale Protokollierung, um die Protokollüberwachungsfunktion zu unterstützen:

```
Router(config)# logging buffered 51200 warning
```

## Anforderungen

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

Vollständige Informationen zum Beginn der Verwendung von Cisco CP finden Sie unter [Erste Schritte mit Cisco Configuration Professional](#).

## Konventionen

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

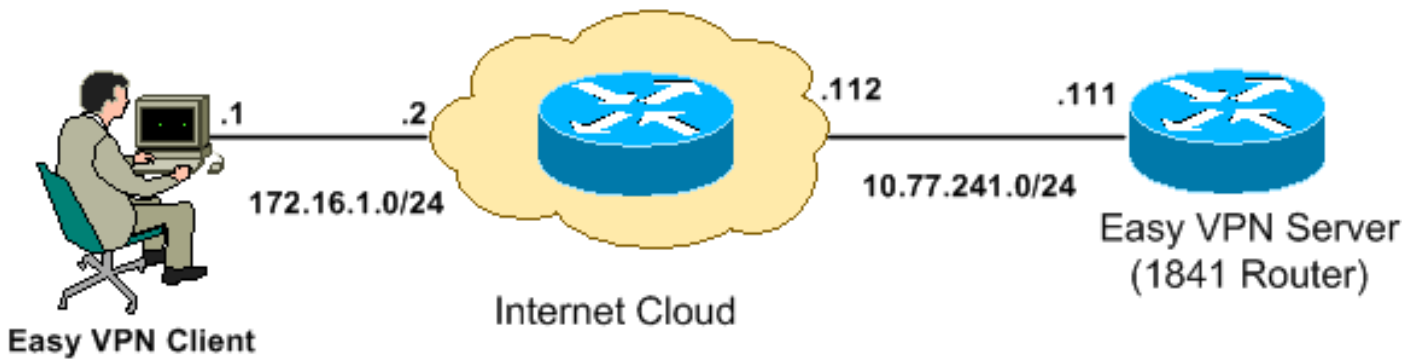
## Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der Grundeinstellungen für einen Router in einem Netzwerk.

**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:




**Hinweis:** Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind [RFC 1918](#) -Adressen, die in einer Laborumgebung verwendet werden.

## [Cisco CP = Easy VPN Server Configuration](#)

Führen Sie die folgenden Schritte aus, um den Cisco IOS-Router als Easy VPN-Server zu konfigurieren:

1. Wählen Sie **Configure > Security > VPN > Easy VPN Server > Create Easy VPN Server aus**, und klicken Sie auf **Launch Easy VPN Server Wizard** (Easy VPN-Serverassistent starten), um den Cisco IOS-Router als Easy VPN-Server zu konfigurieren:

**Configure > Security > VPN > Easy VPN Server**


VPN


---

Create Easy VPN Server

Edit Easy VPN Server

Cisco CP can guide you through Easy VPN Server configuration tasks.

**Use Case Scenario**



Configure Easy VPN Server

Client 1

Client 2

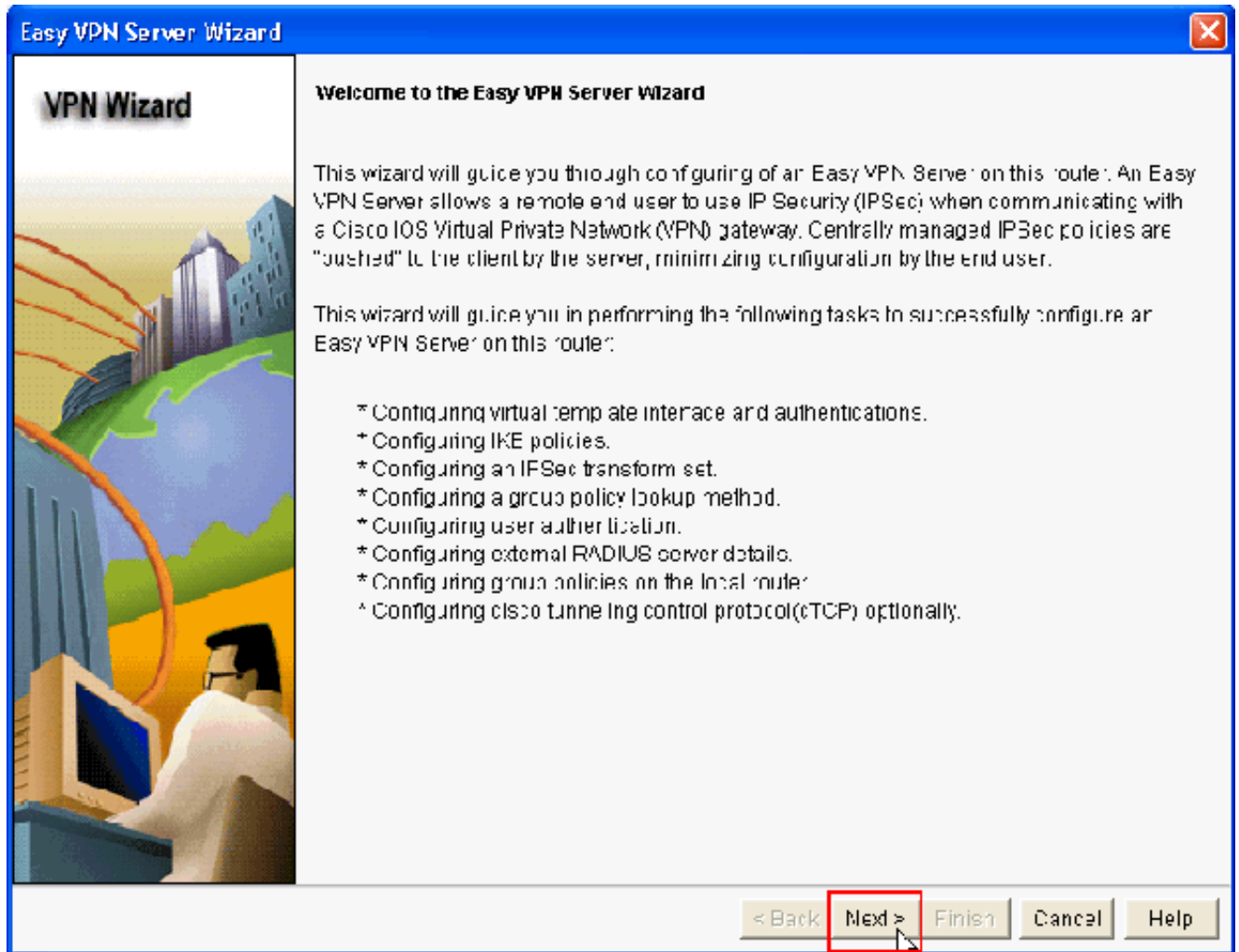
Internet

Easy VPN server

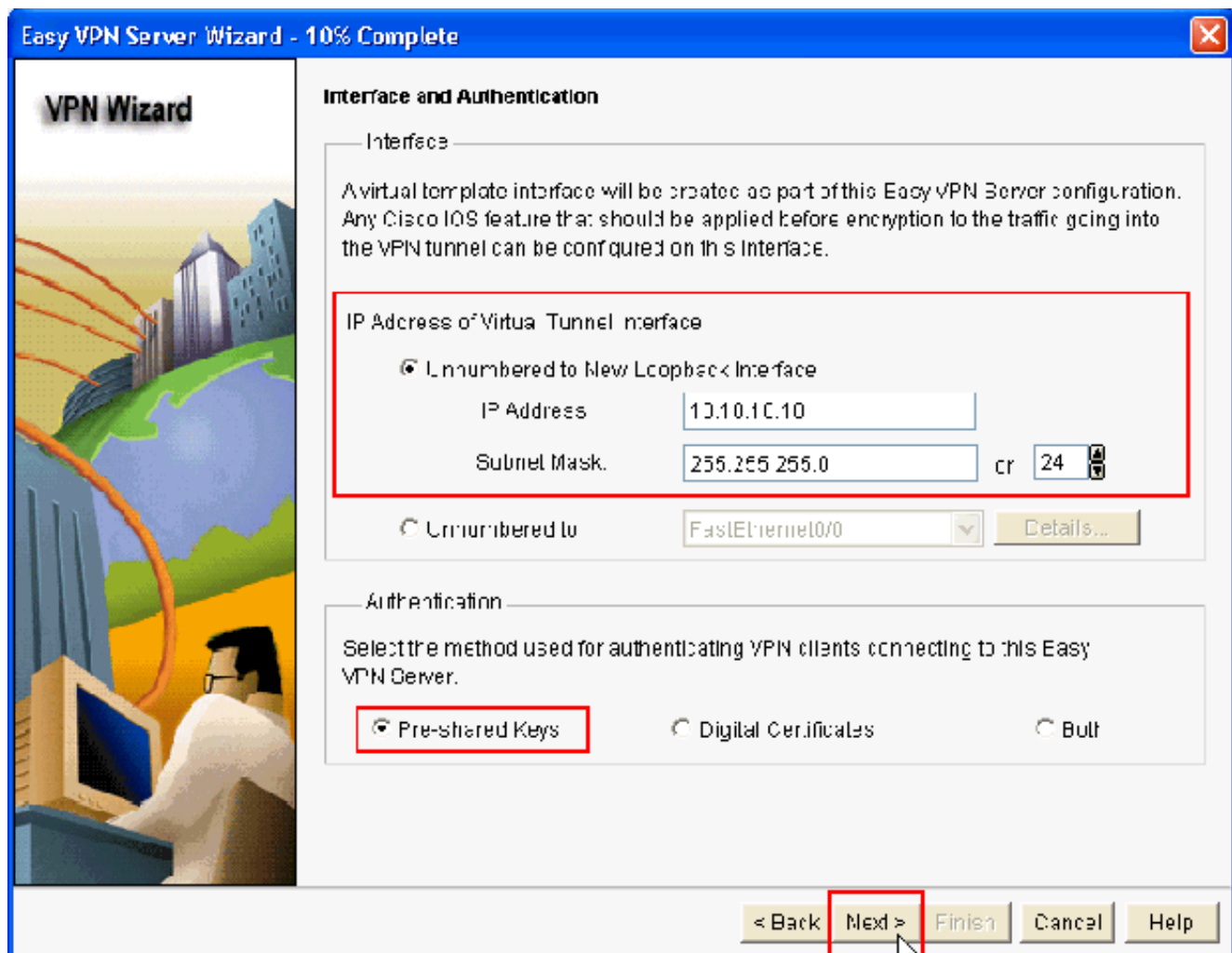
Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes.

Launch Easy VPN Server Wizard

2. Klicken Sie auf **Weiter**, um mit der **Easy VPN Server-Konfiguration** fortzufahren.

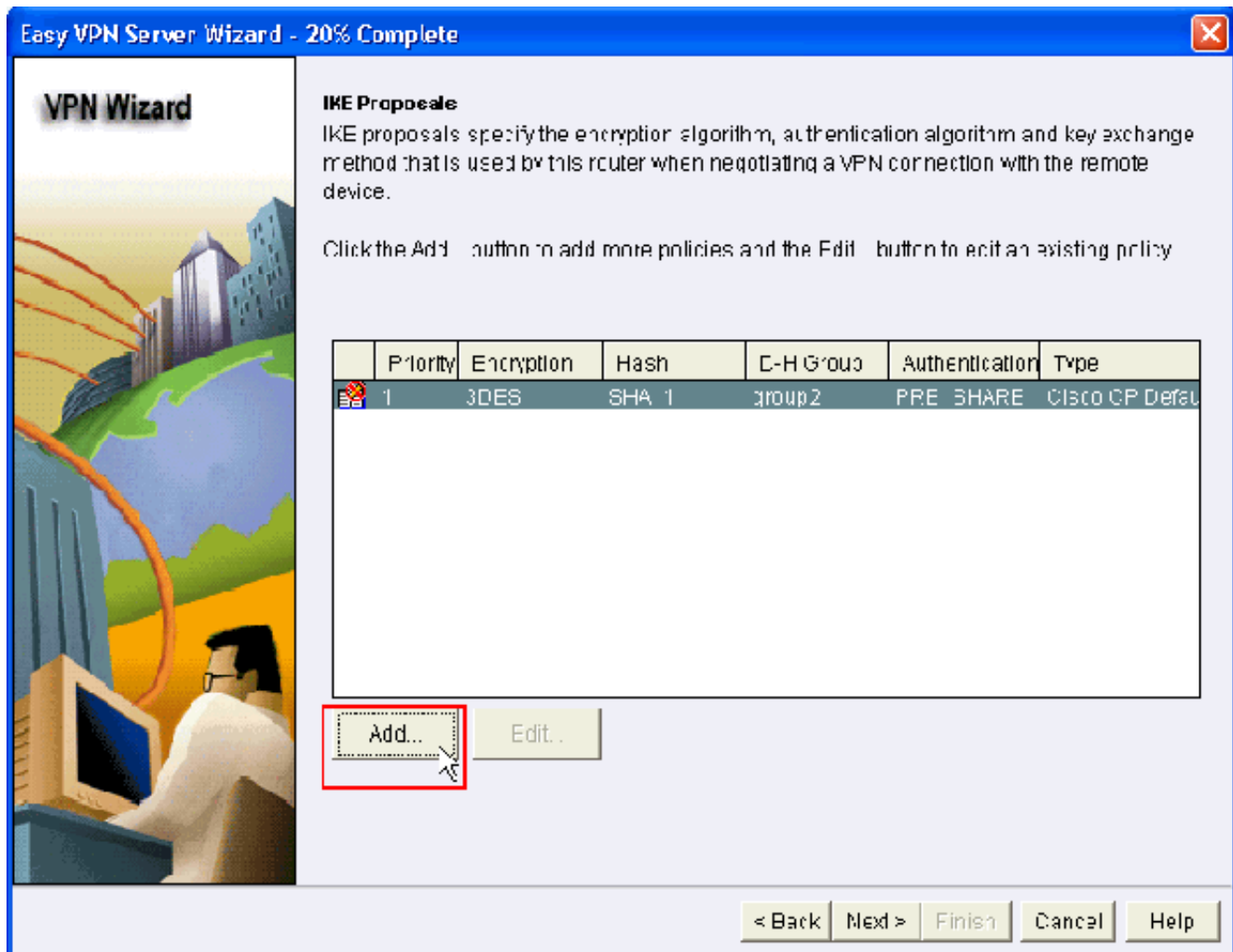


3. Im Ergebnisfenster wird eine **virtuelle Schnittstelle** als Teil der Easy VPN Server-Konfiguration konfiguriert. Geben Sie die **IP-Adresse der Virtual Tunnel Interface (Schnittstelle für virtuellen Tunnel)** an, und wählen Sie die **Authentifizierungsmethode** für die Authentifizierung der VPN-Clients aus. Hier wird die Authentifizierungsmethode **Pre-shared Keys** verwendet. Klicken Sie auf **Weiter**:

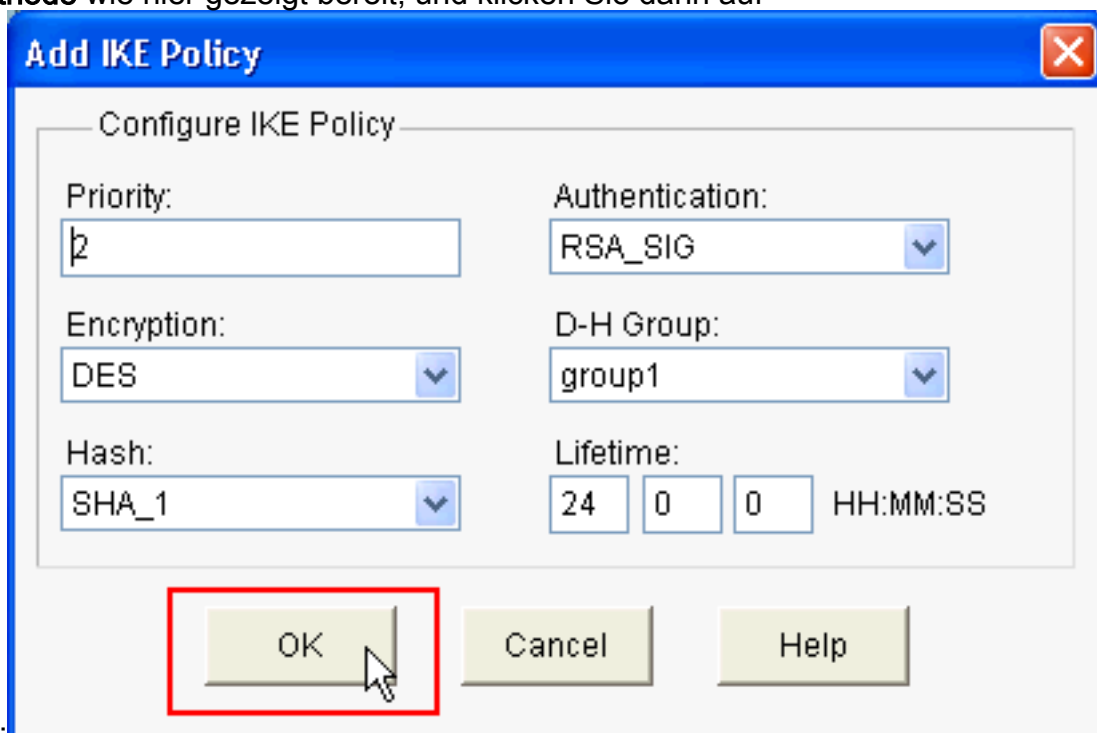


4. Geben Sie den **Verschlüsselungsalgorithmus**, den **Authentifizierungsalgorithmus** und die **Schlüsselaustauschmethode** an, die dieser Router bei Verhandlungen mit dem Remote-Gerät verwenden soll. Auf dem Router ist eine Standard-IKE-Richtlinie vorhanden, die bei Bedarf verwendet werden kann. Wenn Sie eine neue IKE-Richtlinie hinzufügen möchten, klicken Sie auf Hinzufügen.



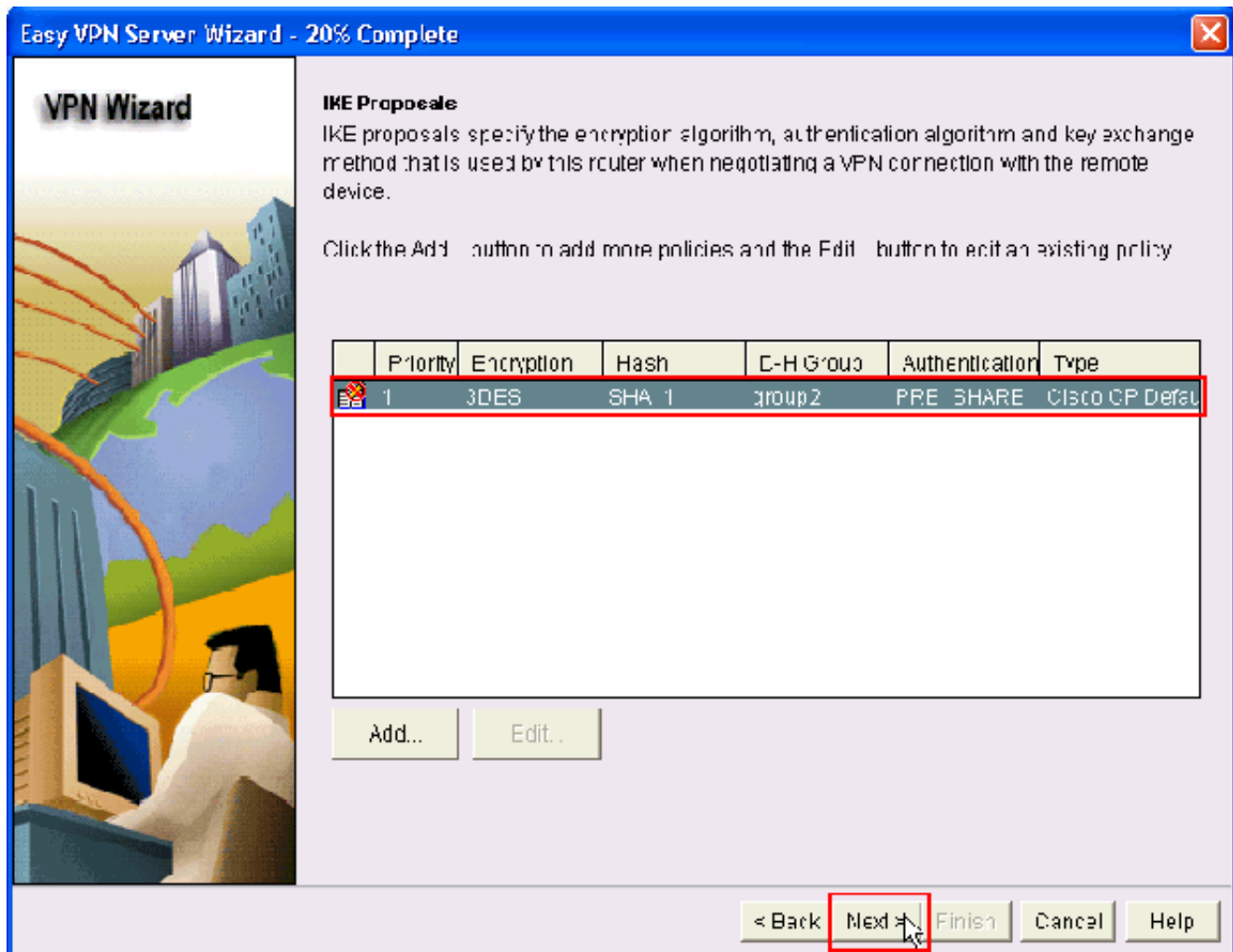


5. Stellen Sie **Verschlüsselungsalgorithmus**, **Authentifizierungsalgorithmus** und die **Exchange-Methode** wie hier gezeigt bereit, und klicken Sie dann auf

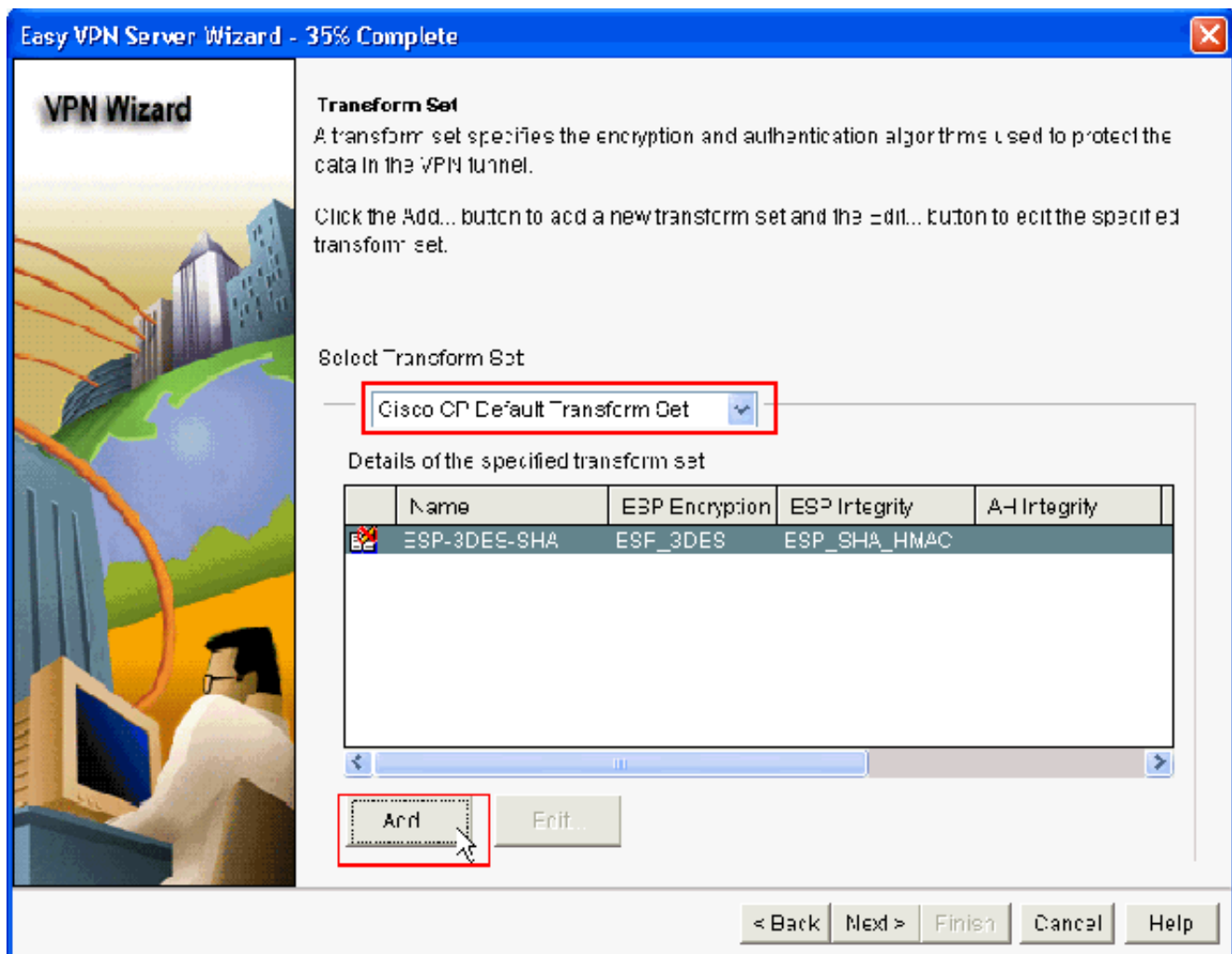


OK:

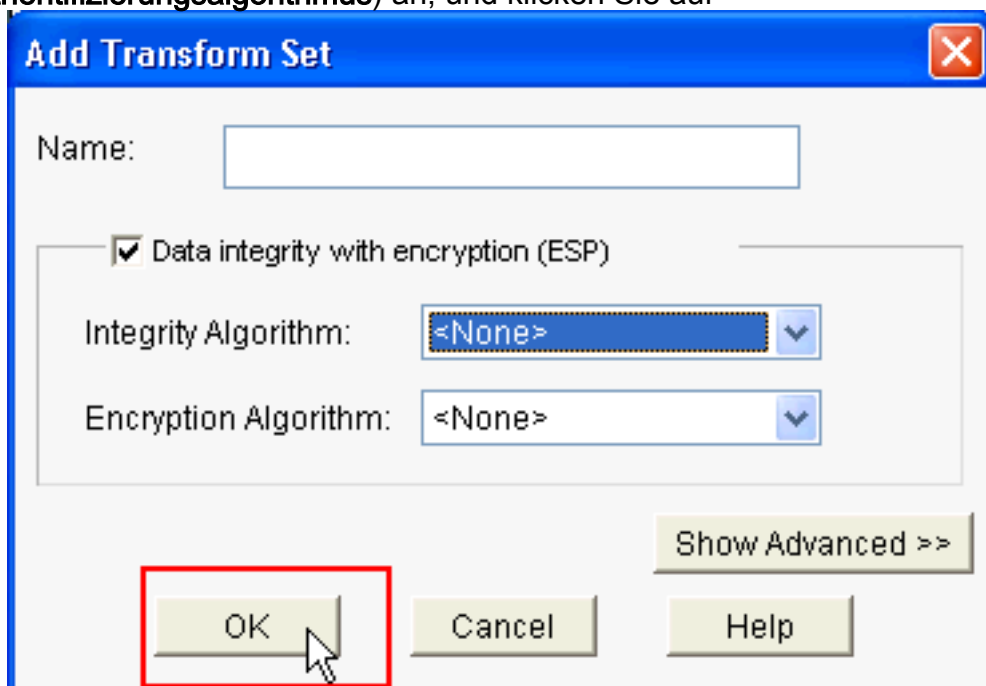
6. In diesem Beispiel wird die **Standard-IKE-Richtlinie** verwendet. Wählen Sie als Ergebnis die Standard-IKE-Richtlinie aus, und klicken Sie auf **Weiter**.



7. Im neuen Fenster sollten die Details zum **Konfigurationssatz** angegeben werden. Das Transform Set legt die **Verschlüsselungs-** und **Authentifizierungsalgorithmen** fest, die zum Schutz von Daten im VPN-Tunnel verwendet werden. Klicken Sie auf **Hinzufügen**, um diese Details anzugeben. Wenn Sie auf **Hinzufügen** klicken und die Details angeben, können Sie bei Bedarf beliebig viele Transform Sets hinzufügen. **Hinweis: Der standardmäßige Konfigurationssatz** des CP ist standardmäßig auf dem Router vorhanden, wenn er mit dem **Cisco CP** konfiguriert wurde.

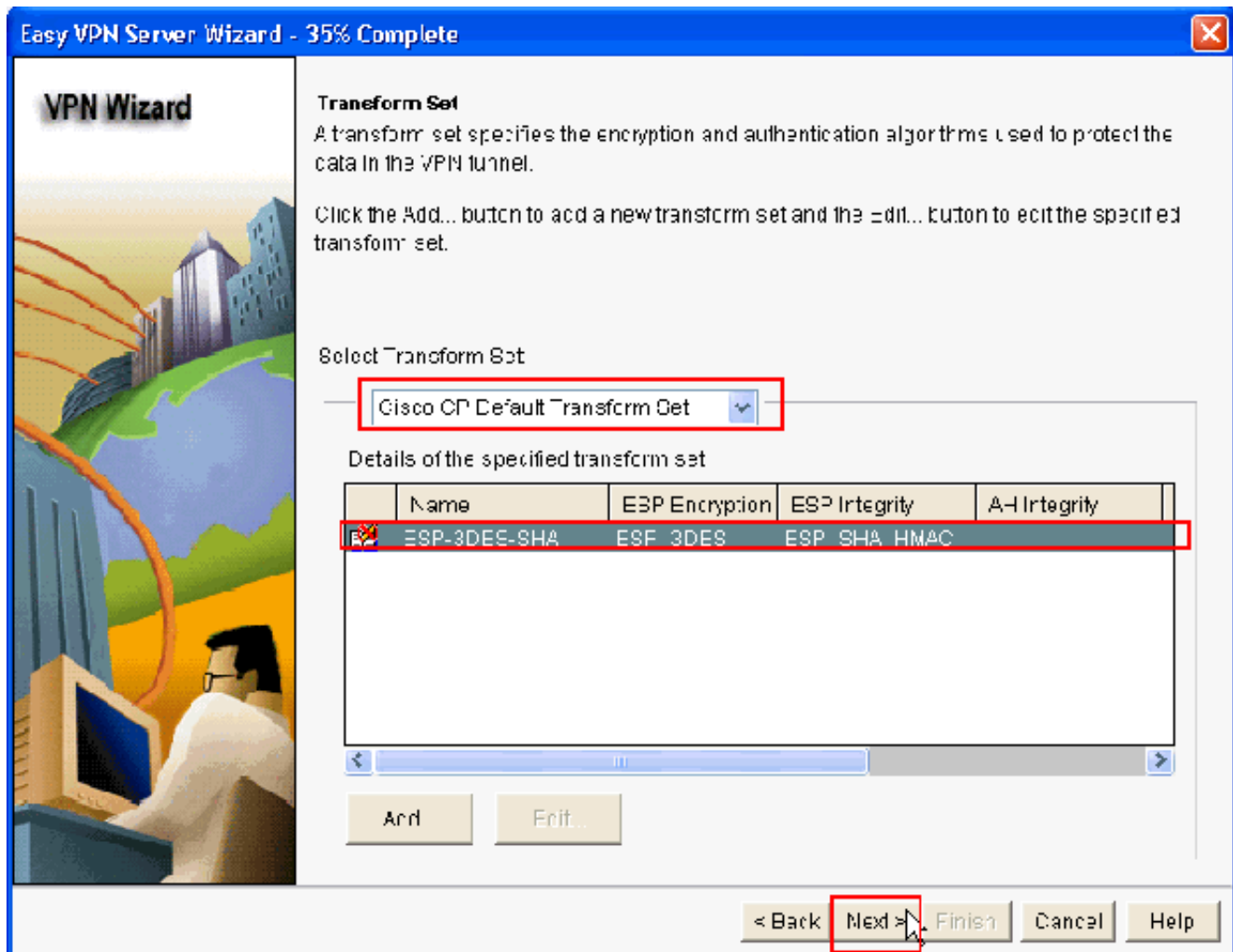


8. Geben Sie die Details zum **Transform Set (Verschlüsselungs- und Authentifizierungsalgorithmus)** an, und klicken Sie auf

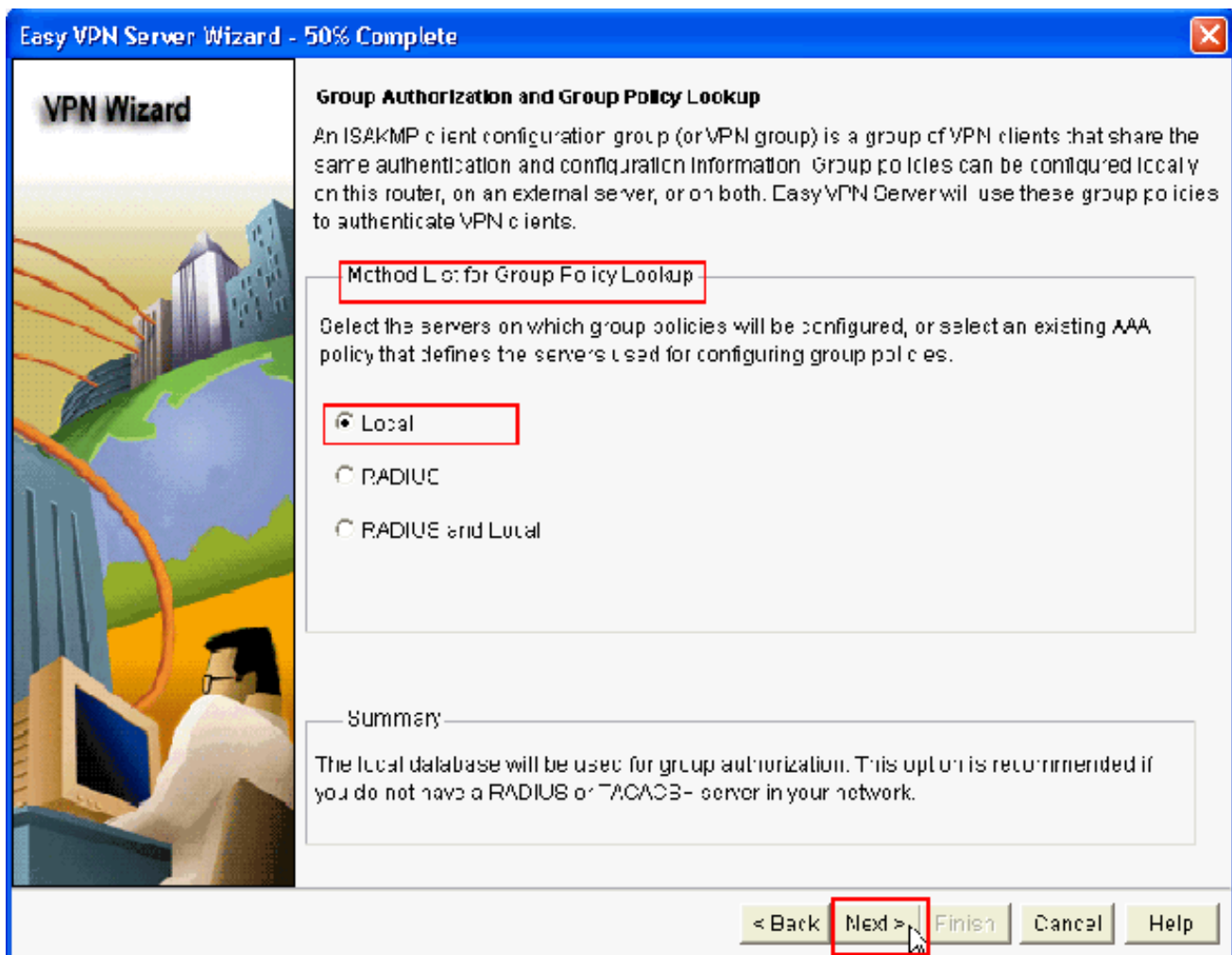


OK.

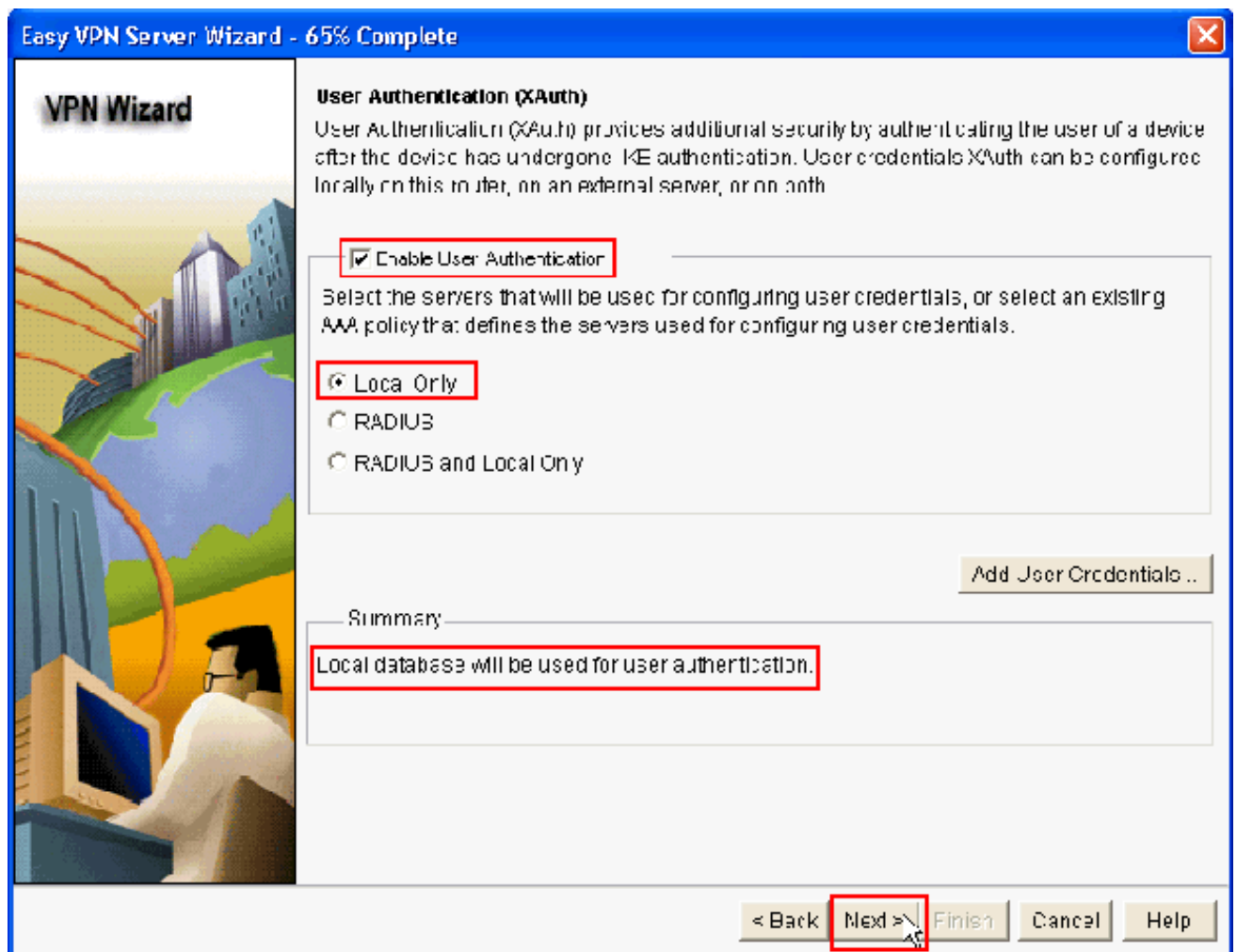
9. In diesem Beispiel wird der **Standard-Umwandlungssatz** mit dem Namen **CP-Standardtransformationssatz** verwendet. Wählen Sie als Ergebnis den Standard-Umwandlungssatz aus, und klicken Sie auf **Weiter**.



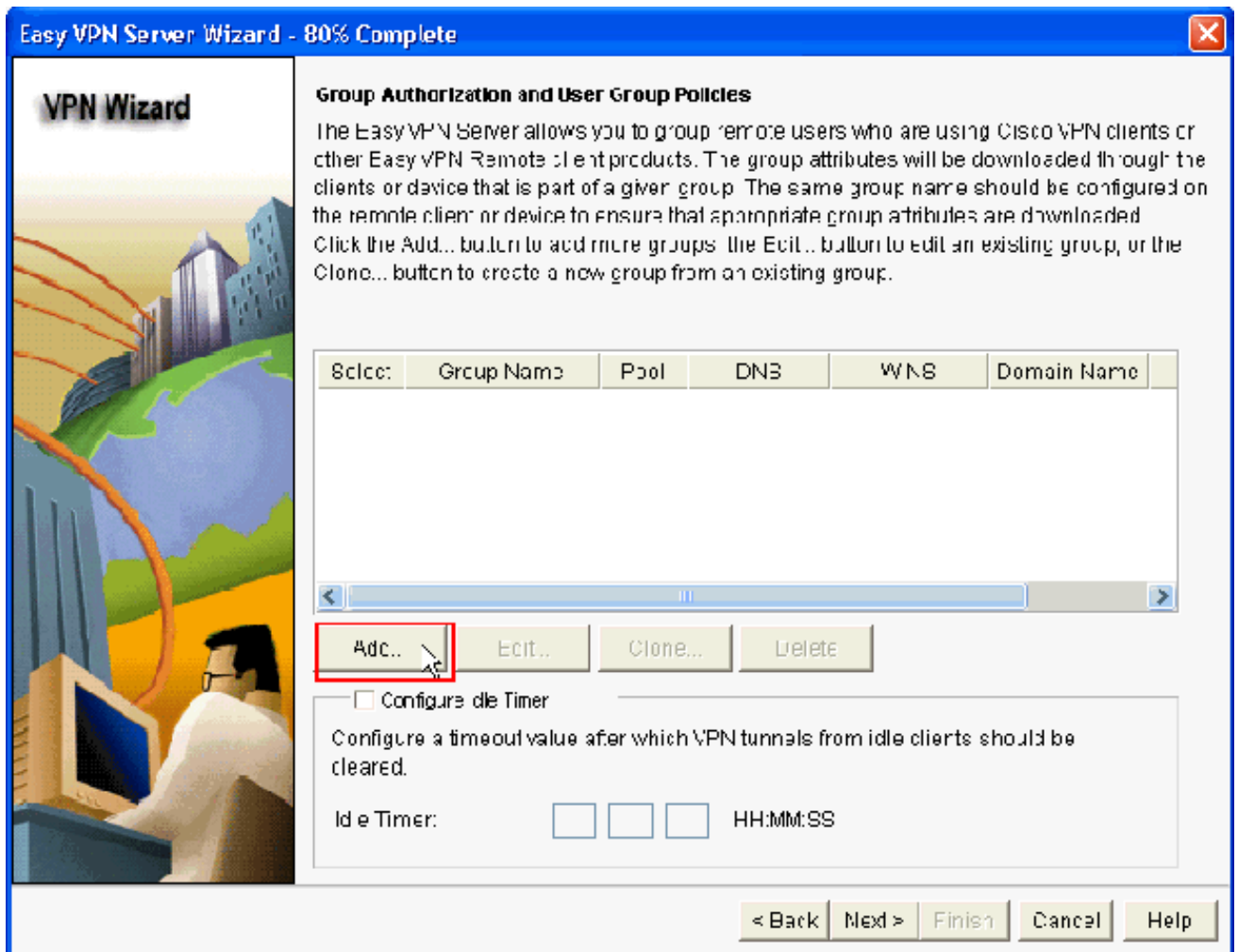
10. Wählen Sie im neuen Fenster den Server aus, auf dem die Gruppenrichtlinien konfiguriert werden sollen. Dabei kann es sich um **Local** oder **RADIUS** oder **Local und RADIUS handeln**. In diesem Beispiel verwenden wir den **lokalen Server**, um Gruppenrichtlinien zu konfigurieren. Wählen Sie **Lokal aus**, und klicken Sie auf **Weiter**.



11. Wählen Sie in diesem neuen Fenster den Server für die Benutzerauthentifizierung aus, der entweder **nur lokal** oder **RADIUS** oder sowohl **Nur lokal als auch RADIUS** sein kann. In diesem Beispiel verwenden wir den **lokalen Server**, um Benutzeranmeldeinformationen für die Authentifizierung zu konfigurieren. Stellen Sie sicher, dass das Kontrollkästchen neben **Benutzerauthentifizierung aktivieren** aktiviert ist. Wählen Sie **Lokal** und klicken Sie auf **Weiter**.



12. Klicken Sie auf **Hinzufügen**, um eine neue Gruppenrichtlinie zu erstellen und die Remote-Benutzer dieser Gruppe hinzuzufügen.



13. Geben Sie im Fenster Gruppenrichtlinie hinzufügen den Gruppennamen im Feld für den Namen dieser Gruppe (in diesem Beispiel cisco) zusammen mit dem vorinstallierten Schlüssel und die Informationen für den IP-Pool (die Start-IP-Adresse und die **End-IP-Adresse**) wie gezeigt an, und klicken Sie auf **OK**. **Hinweis:** Sie können einen neuen IP-Pool erstellen oder, falls vorhanden, einen vorhandenen IP-Pool verwenden.

**Add Group Policy**

**General** | DNS/WINS | Split Tunneling | Client Settings | XAuth Options | Client Update

Name of This Group:

**Pre-shared Keys**

Specify the key that will be used to authenticate the clients associated with this group.

Current Key: <None>

Enter new pre-shared key:

Reenter new pre-shared key:

**Pool Information**

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

Create a new pool       Select from an existing pool

Starting IP address:      

Ending IP address:

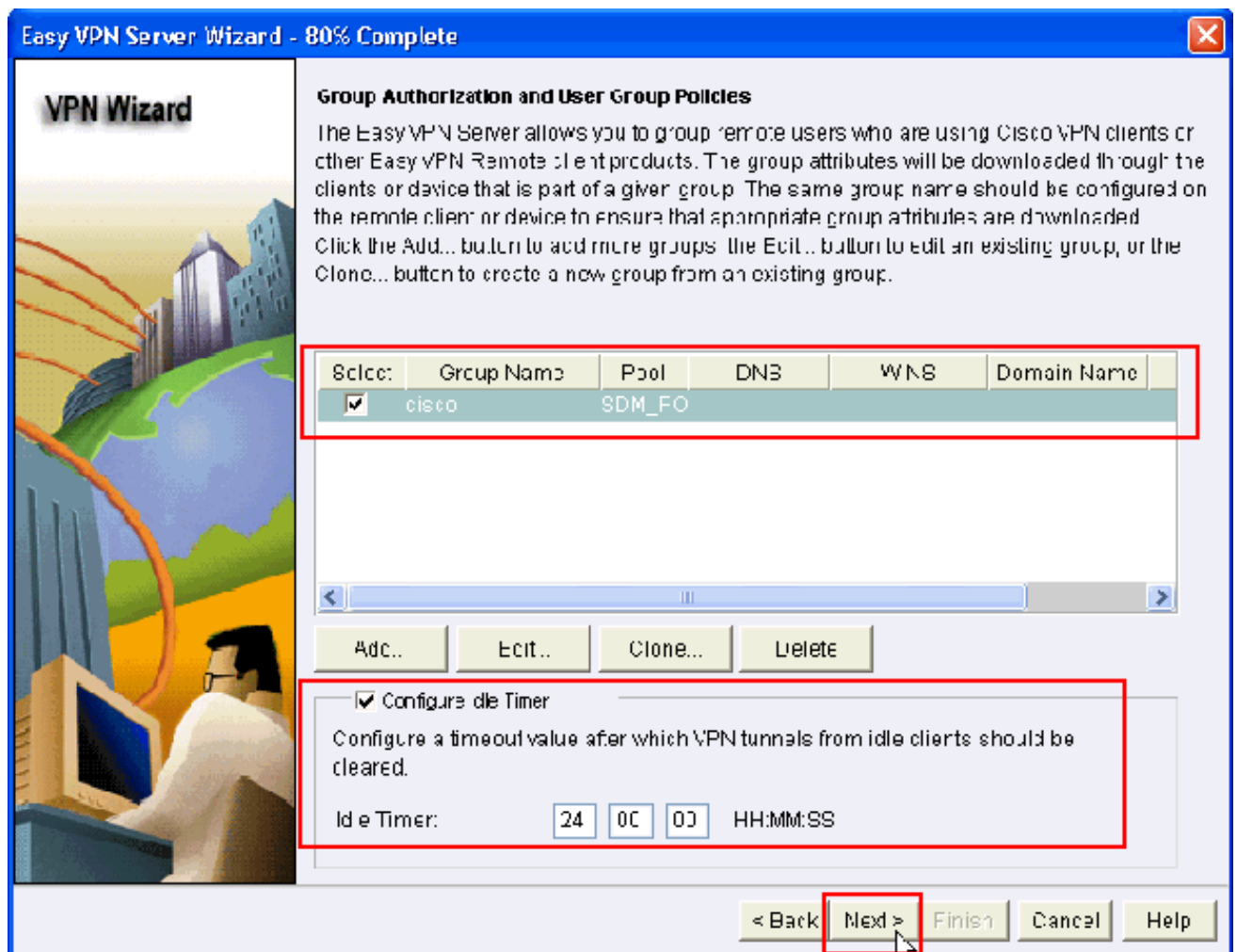
Enter the subnet mask that should be sent to the client along with the IP address.

Subnet Mask:  (Optional)

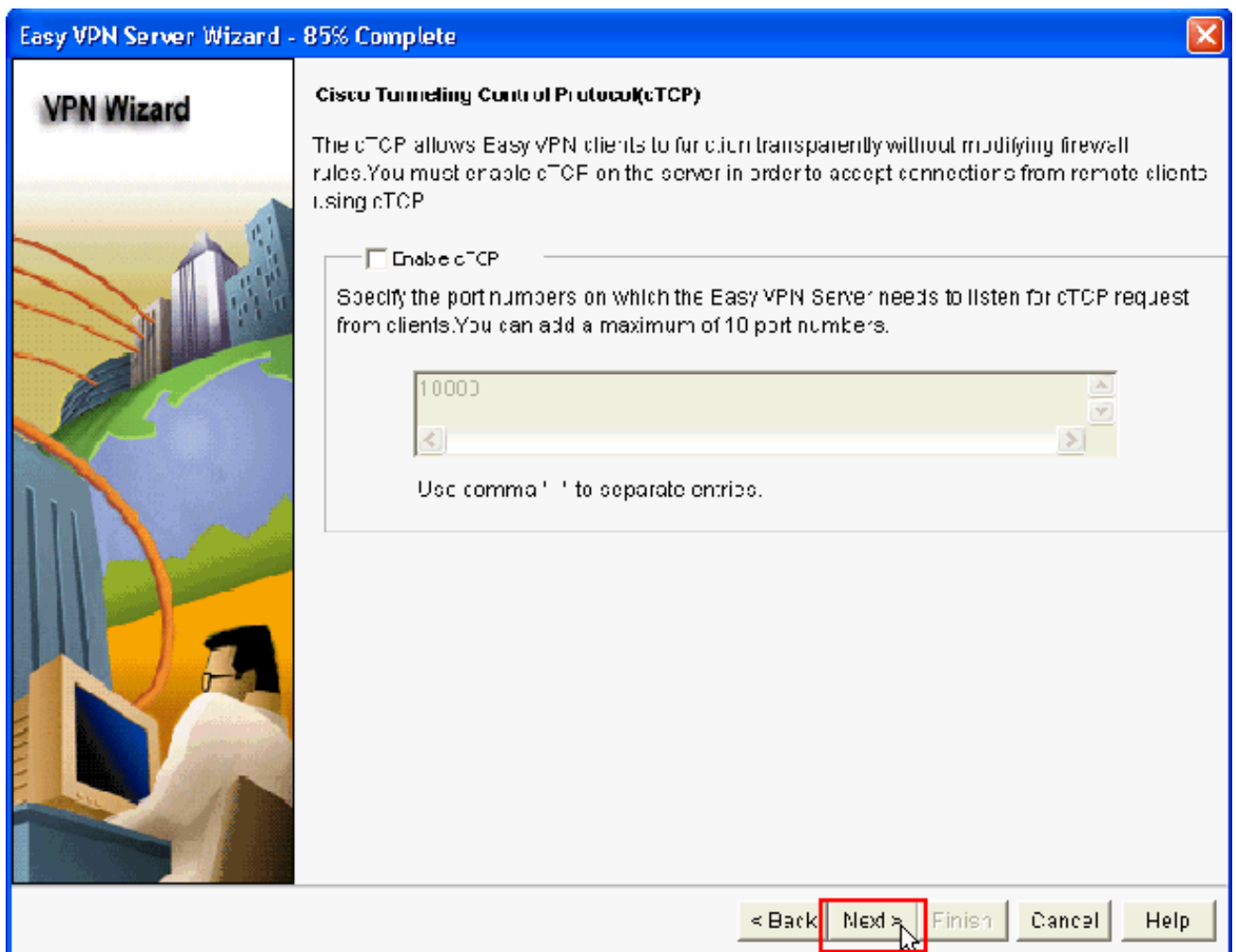
Maximum Connections Allowed:

14. Wählen Sie nun die neue **Gruppenrichtlinie** aus, die mit dem Namen **cisco** erstellt wurde, und aktivieren Sie dann das Kontrollkästchen neben **Configure Idle Timer (Inaktivitätszeitgeber konfigurieren)**, um den **Leerlaufzeitgeber** zu konfigurieren. Klicken Sie auf **Weiter**.

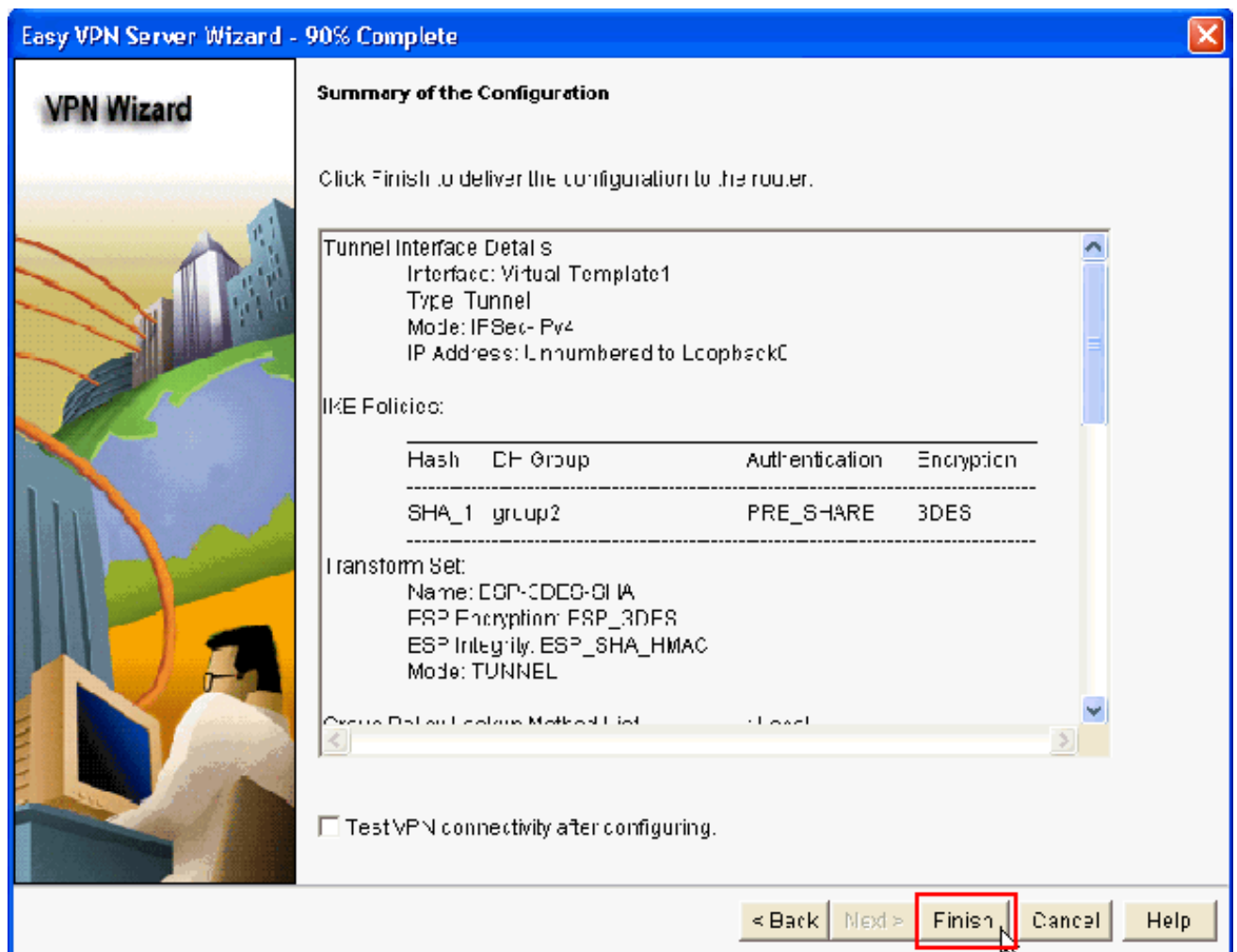




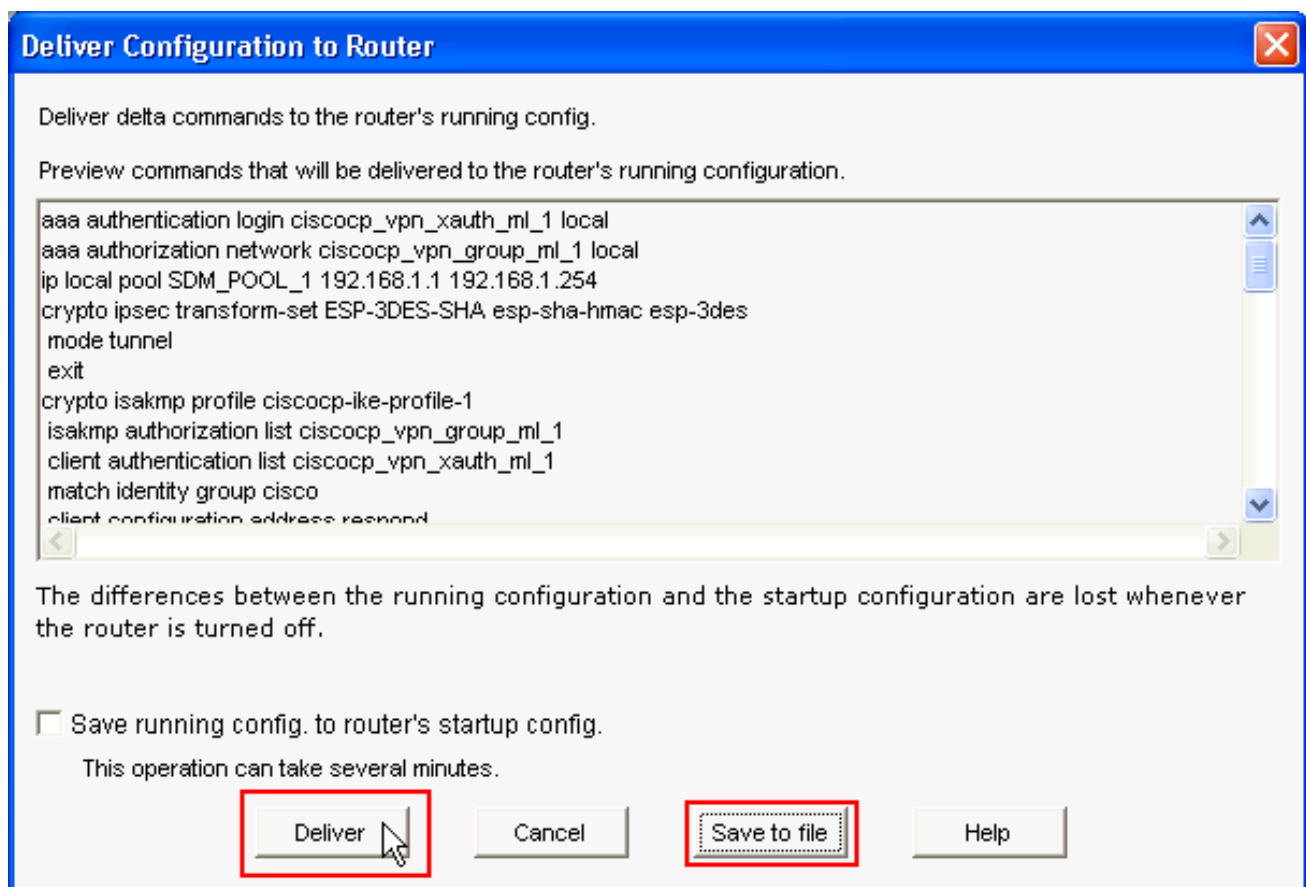
15. Aktivieren Sie bei Bedarf **Cisco Tunneling Control Protocol (cTCP)**. Andernfalls klicken Sie auf **Weiter**.



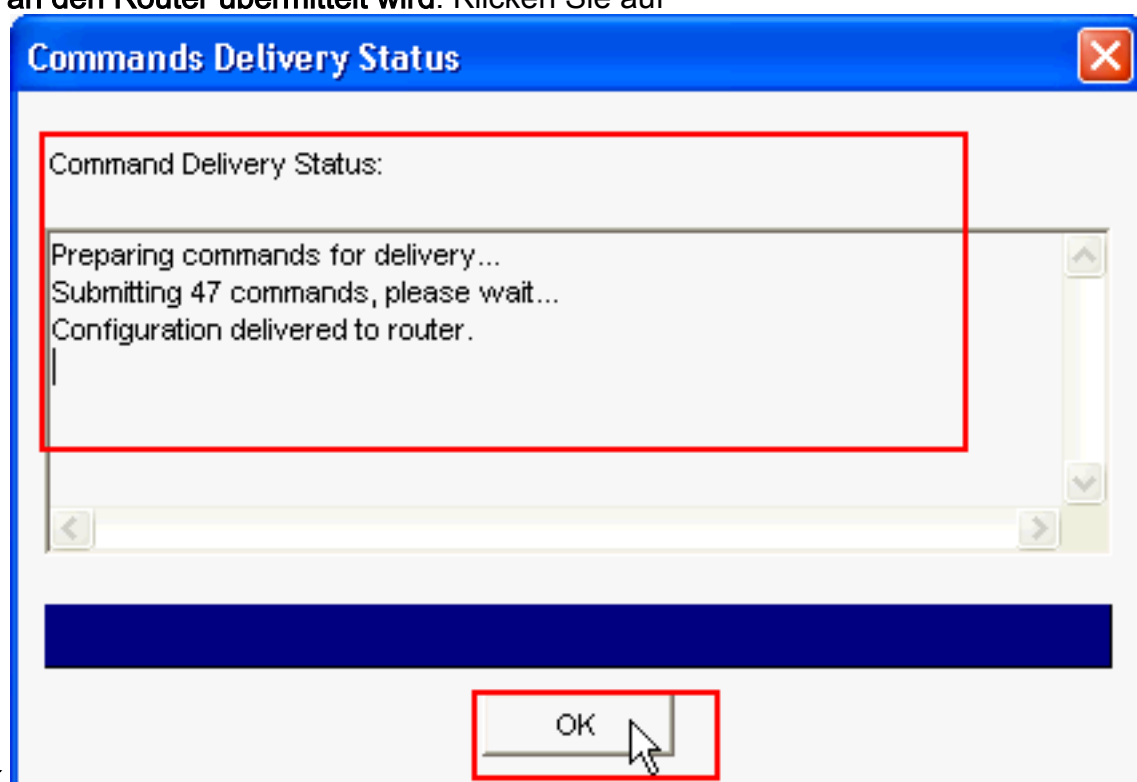
16. Überprüfen Sie die **Konfigurationsübersicht**. Klicken Sie auf **Fertigstellen**.



17. Klicken Sie im Fenster **Konfiguration an Router liefern** auf **Bereitstellen**, um die Konfiguration an den Router zu übertragen. Sie können auf **In Datei speichern** klicken, um die Konfiguration als Datei auf dem PC zu speichern.

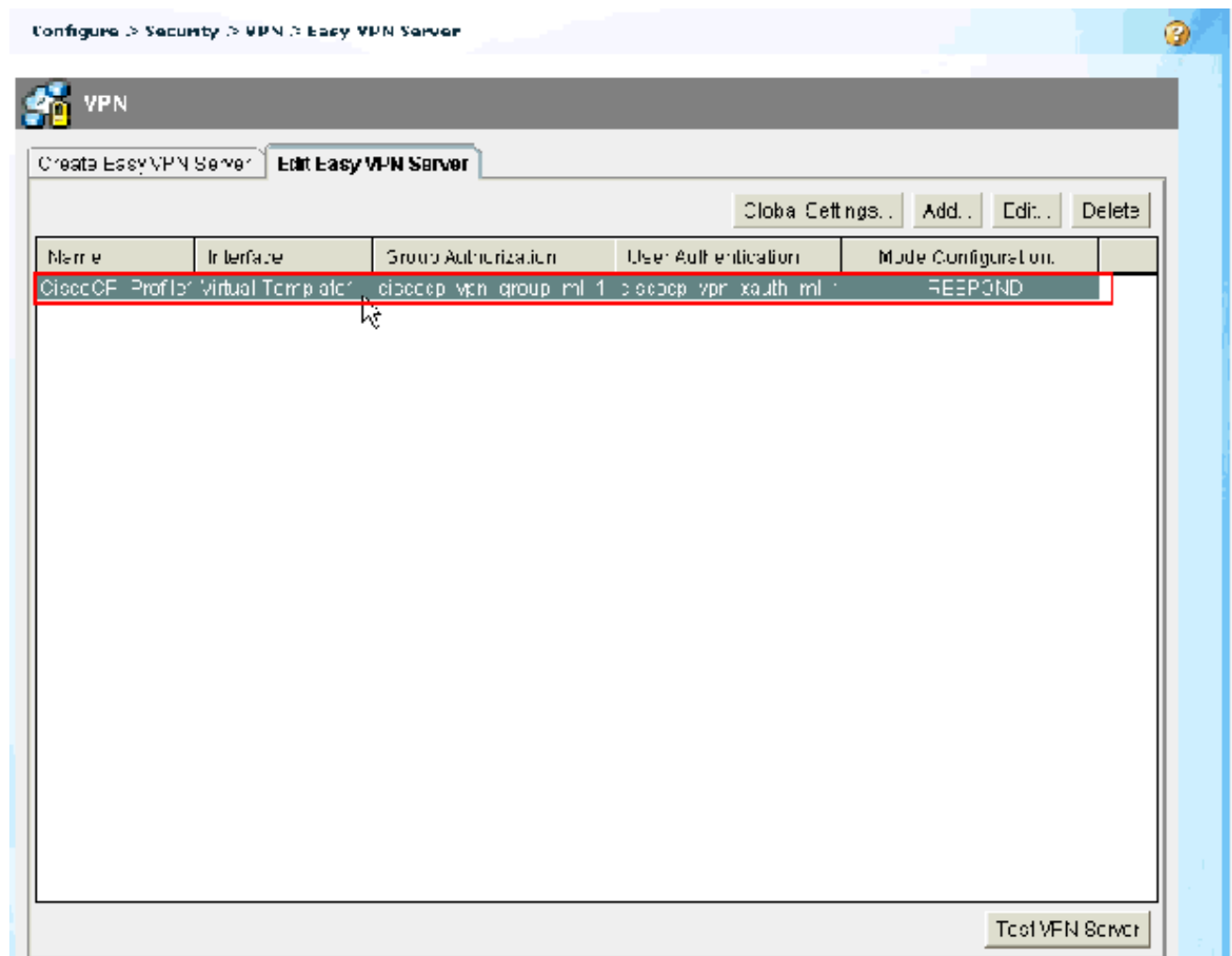


18. Das Fenster **Command Delivery Status** (Bereitstellungsstatus für Befehle) zeigt den Bereitstellungsstatus der Befehle an den Router an. Sie wird als **Konfiguration** angezeigt, die an den Router übermittelt wird. Klicken Sie auf



OK.

19. Sie sehen den neu erstellten Easy VPN-Server. Sie können den vorhandenen Server bearbeiten, indem Sie **Easy VPN-Server bearbeiten** auswählen. Damit ist die Easy VPN-Serverkonfiguration auf dem Cisco IOS-Router abgeschlossen.



## CLI-Konfiguration

### Routerkonfiguration

```
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 ciscocep_vpn_xauth_ml_1 local
aaa authorization network ciscocep_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-Templatel 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
```

## Überprüfen

### Easy VPN-Server - Befehle anzeigen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-SAs in einem Peer an.

```
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** - Zeigt alle aktuellen IPsec-SAs in einem Peer an.

```
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): (192.168.1.3/255.255.255/0/0)
```

```
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
```

## Fehlerbehebung

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

**Hinweis:** Bevor Sie Debugbefehle ausgeben, lesen Sie die [wichtigen Informationen zu Debug-Befehlen](#).

## Zugehörige Informationen

- [IPSec-Aushandlung/IKE-Protokolle](#)
- [Schnellstartanleitung für Cisco Configuration Professional](#)
- [Cisco Produkt-Support-Seite - Router](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)