IOS路由器作为Easy VPN Server使用配置专业人员配置示例

目录

简介

使用Cisco Configuration Professional (思科CP)和CLI，本文描述如何配置Cisco IOS路由器作为Easy VPN (ezvpn)服务器。Easy VPN Server功能允许一个远程最终用户联络使用IP安全与所有Cisco IOS虚拟专用网络(VPN)网关。在中央管理的IPsec策略“推送”到客户端设备由服务器，最小化配置由最终用户。

关于参考安全连接配置指南库的Easy VPN Server部分的Easy VPN Server的更多信息，Cisco IOS版本12.4T。

先决条件

使用的组件

本文档中的信息基于以下软件和硬件版本：

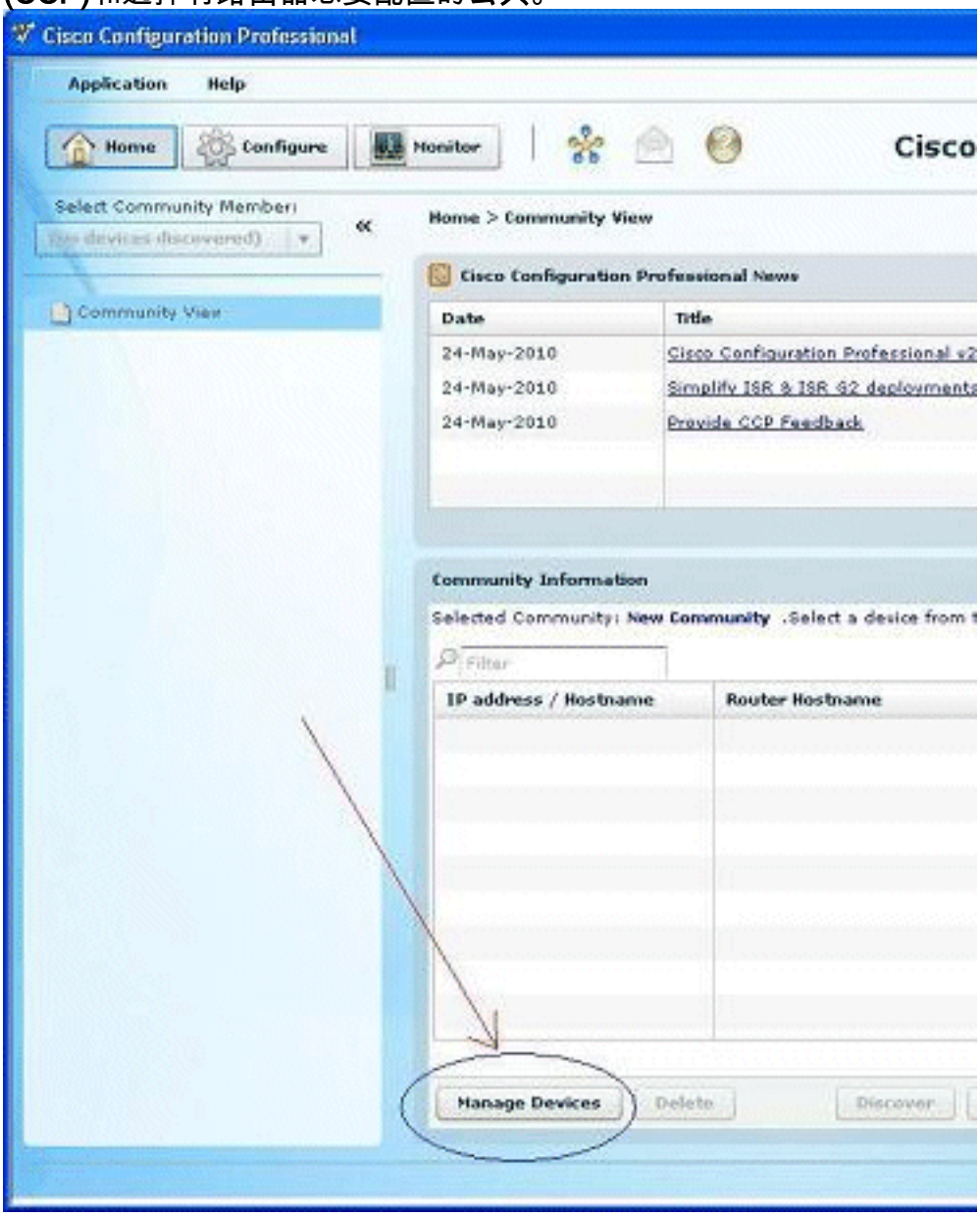
- 配备 Cisco IOS 软件版本 12.4(15T) 的 Cisco 1841 路由器
- Cisco CP 版本 2.1

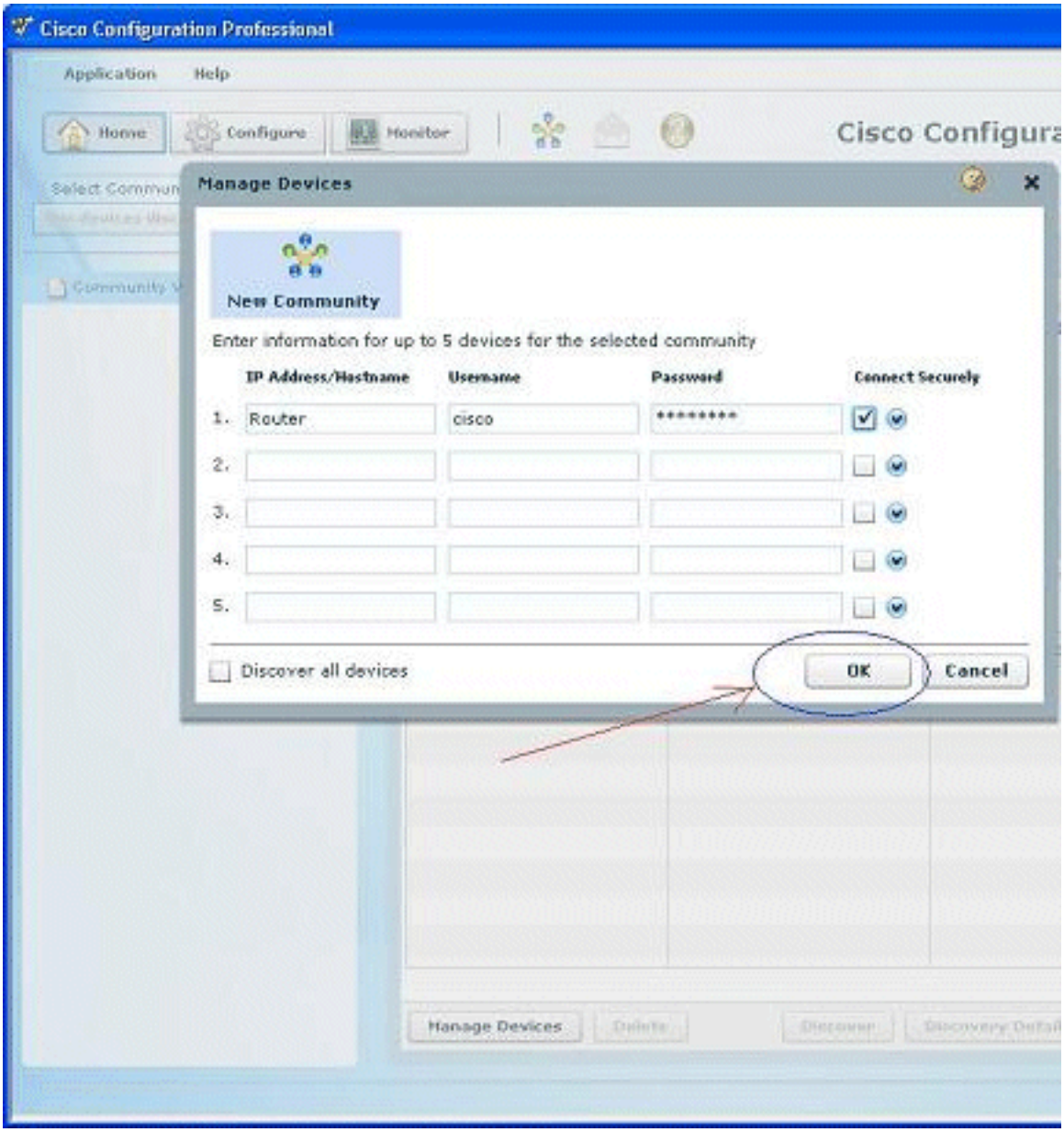
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

安装思科CP

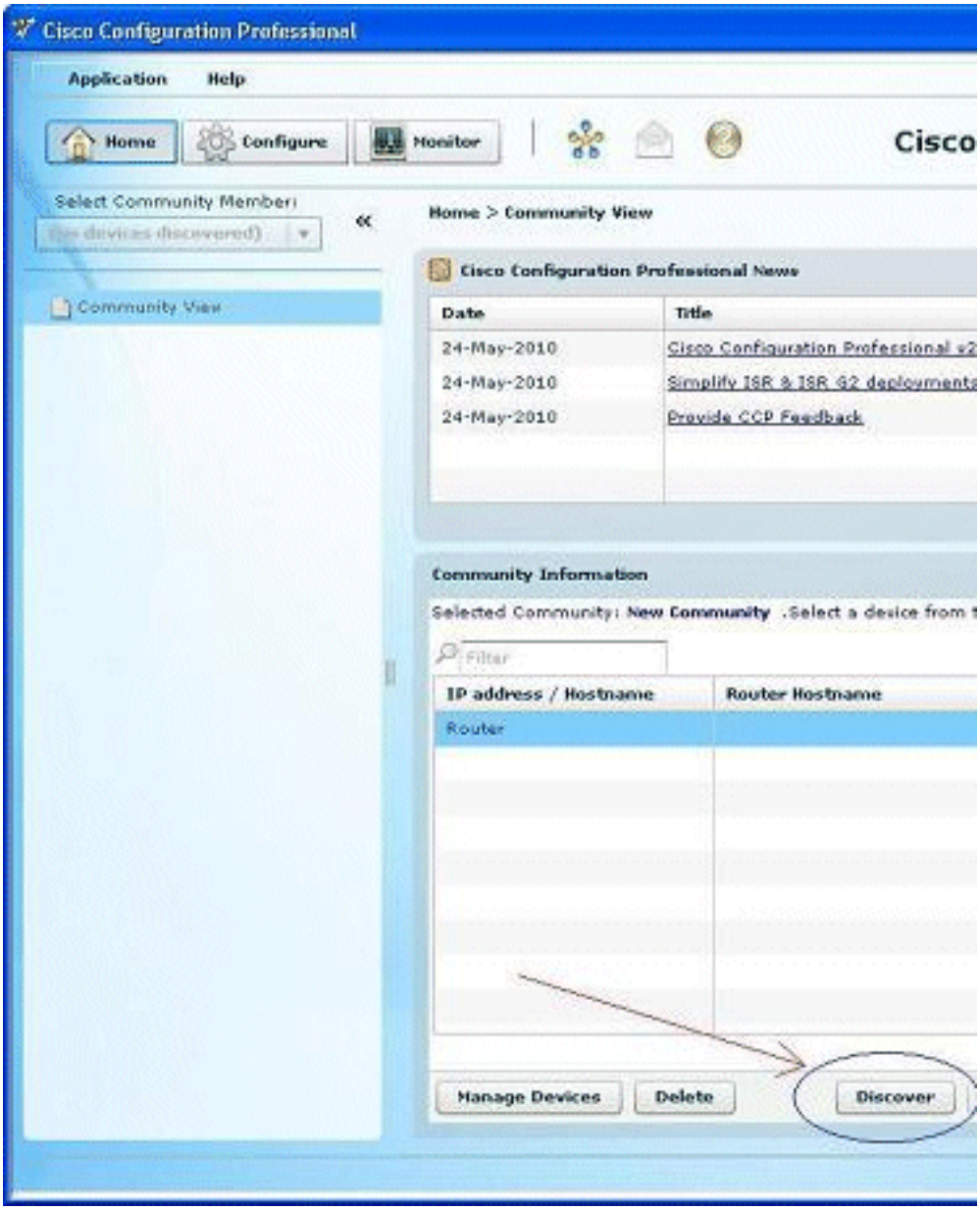
执行这些步骤为了安装思科CP ：

1. 下载从Cisco软件中心(仅限注册用户)的思科CP V2.1并且安装它在您的本地PC。思科CP新版本可以在思科CP网站找到。
2. 从您的本地PC的启动Cisco CP通过**Start > Programs > Cisco Configuration Professional (CCP)**和选择有路由器您要配置的**公共**。





3. 为了发现您要配置，突出显示路由器并且单击**发现的**设备。



注意： 关于是兼容对思科CP v2.1的Cisco路由器型号和IOS版本的信息，参考兼容Cisco IOS版本部分。

注意： 关于PC需求的信息运行的思科CP v2.1，参考System Requirements部分。

运行 Cisco CP 的路由器配置

要在 Cisco 路由器上运行 Cisco CP，请执行以下配置步骤：

1. 使用 Telnet、SSH 或控制台连接路由器。使用以下命令进入全局配置模式：`Router(config)#`**`enable`** `Router(config)#`
2. 如果启用了 HTTP 和 HTTPS 并将其配置为使用非标准端口号，则可跳过此步骤并直接使用已配置的端口号。使用以下 Cisco IOS 软件命令启用路由器 HTTP 或 HTTPS 服务器：`Router(config)#` **`ip http server`** `Router(config)#` **`ip http secure-server`** `Router(config)#` **`ip http authentication local`**
3. 创建一个权限级别为 15 的用户：`Router(config)#` **`username`** *`<username>`* **`privilege 15 password 0`** *`<password>`* **注意：** 使用要配置的用户名和口令替换 **<username>** 和 **<password>**。
4. 为本地登录和权限级别 15 配置 SSH 和 Telnet。`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. （可选）启用本地登录以支持日志监控功能：`Router(config)# logging buffered 51200 warning`

要求

本文假设， Cisco路由器是完全能操作和已配置的允许思科CP做配置更改。

使用思科CP，关于如何开始的全部信息，参考开始与Cisco Configuration Professional。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

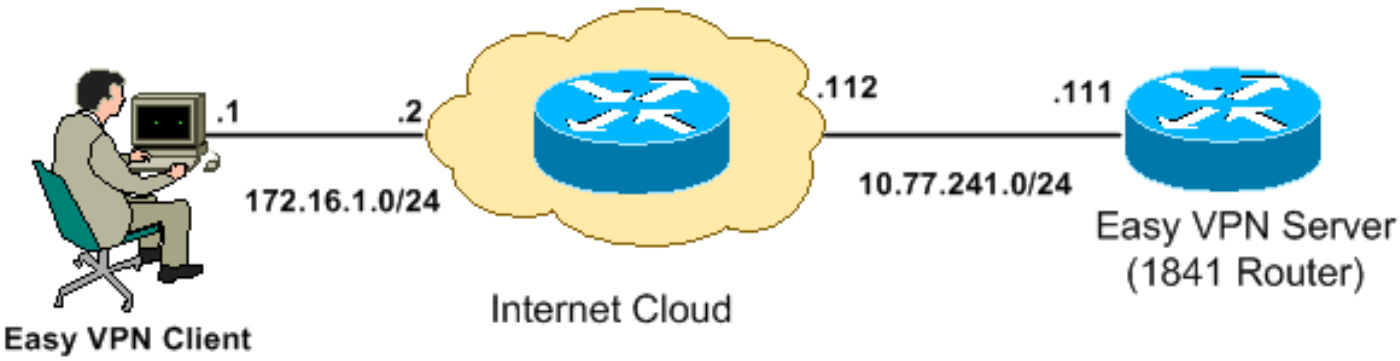
配置

在本部分中，您将了解有关网络中路由器基本设置的配置信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

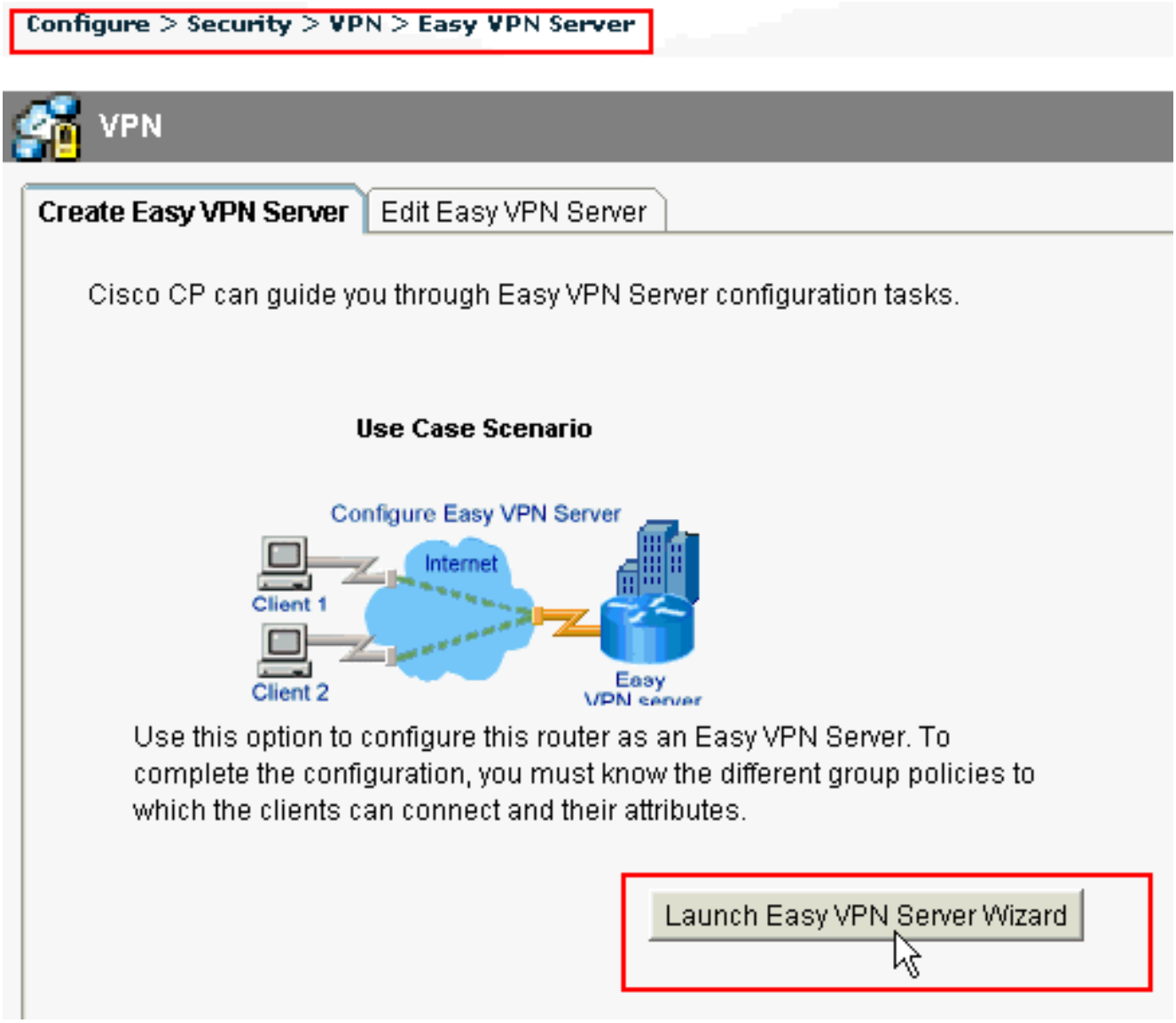


注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

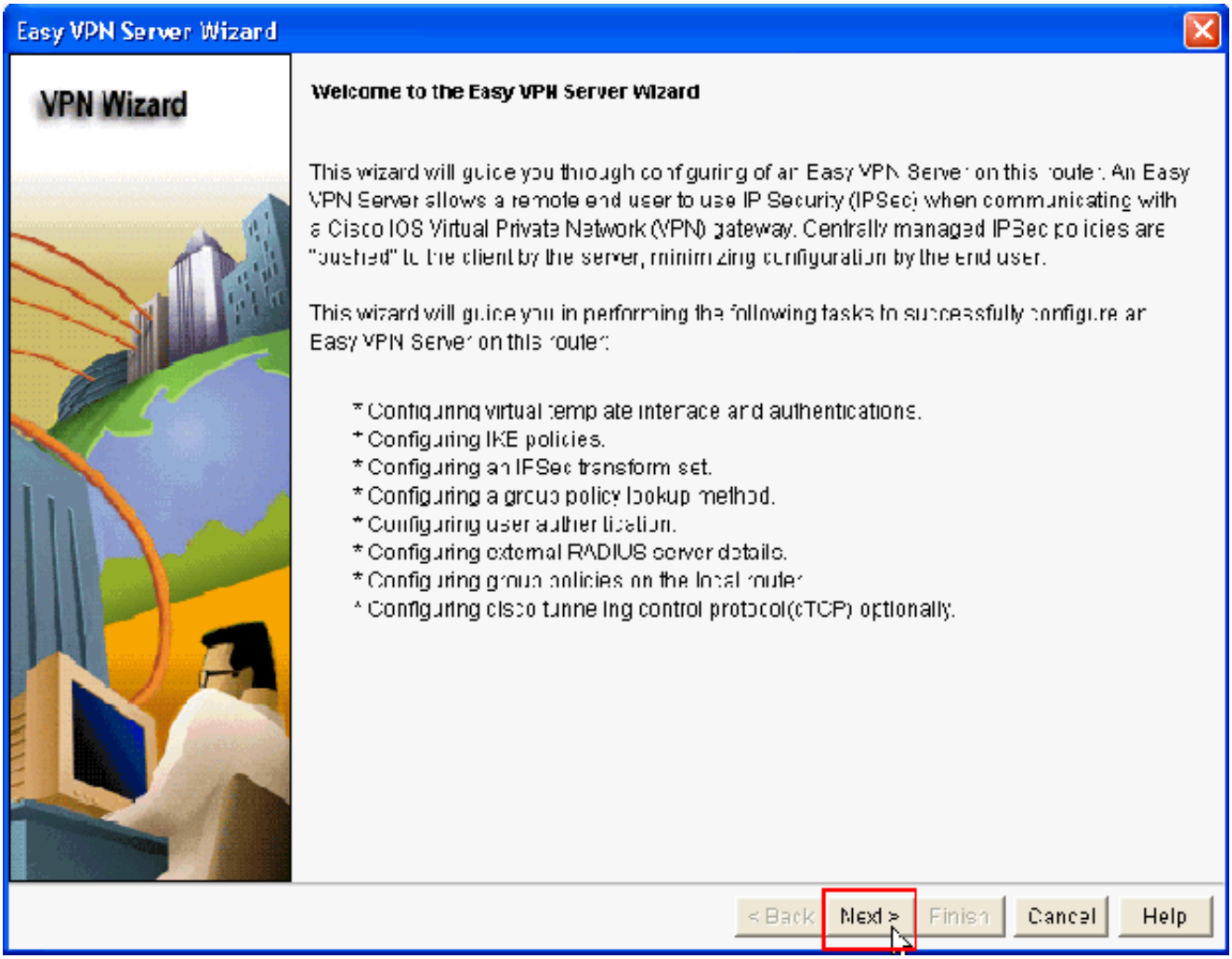
思科CP - Easy VPN Server配置

执行这些步骤为了配置Cisco IOS路由器作为Easy VPN Server ：

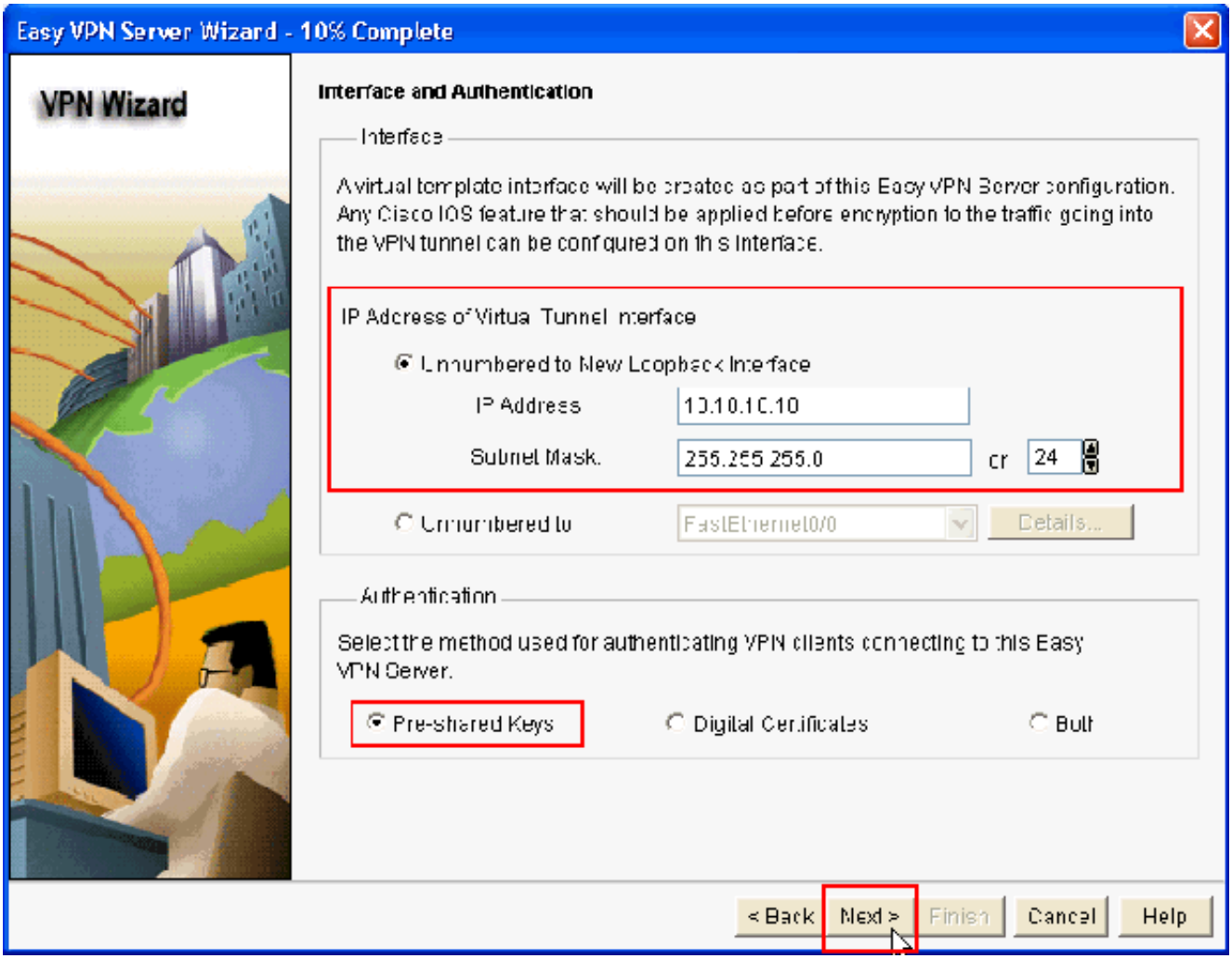
1. 选择**配置**> Security > **VPN** > **Easy VPN Server** >**创建Easy VPN Server**并且点击**启动Easy VPN Server向导**为了配置Cisco IOS路由器作为Easy VPN Server ：



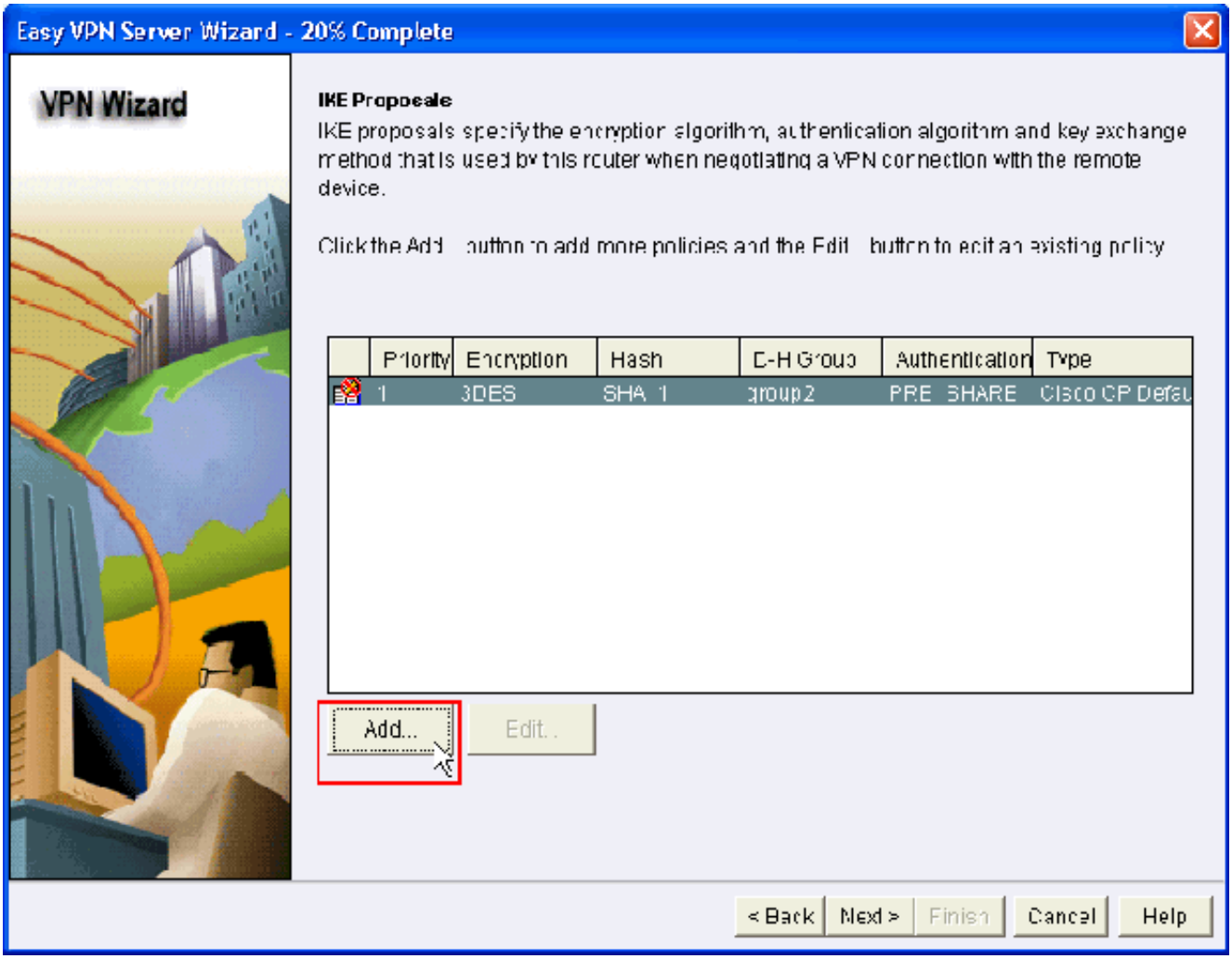
2. **其次**单击为了继续进行**Easy VPN Server**配置。



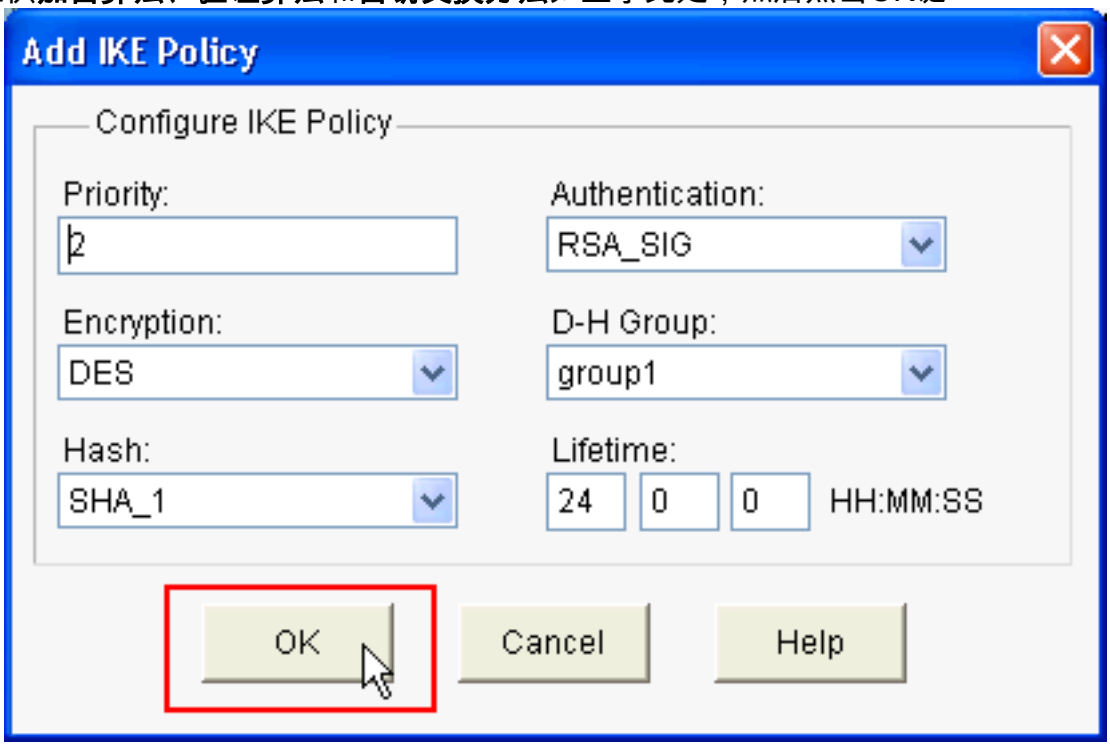
3. 在发生的窗口，**虚拟接口将**配置作为Easy VPN Server配置的部分。提供**虚拟隧道接口的IP地址**并且选择验证VPN客户端使用的**认证方法**。这里，**预先共享密钥**是使用的认证方法。单击“下一步
”:



4. 当协商用远程设备时，请指定**加密算法、验证算法和**此路由器将使用的**密钥交换方法**。默认IKE策略是存在可以如果必须使用的路由器。如果想要添加新的IKE策略，请单击添加。

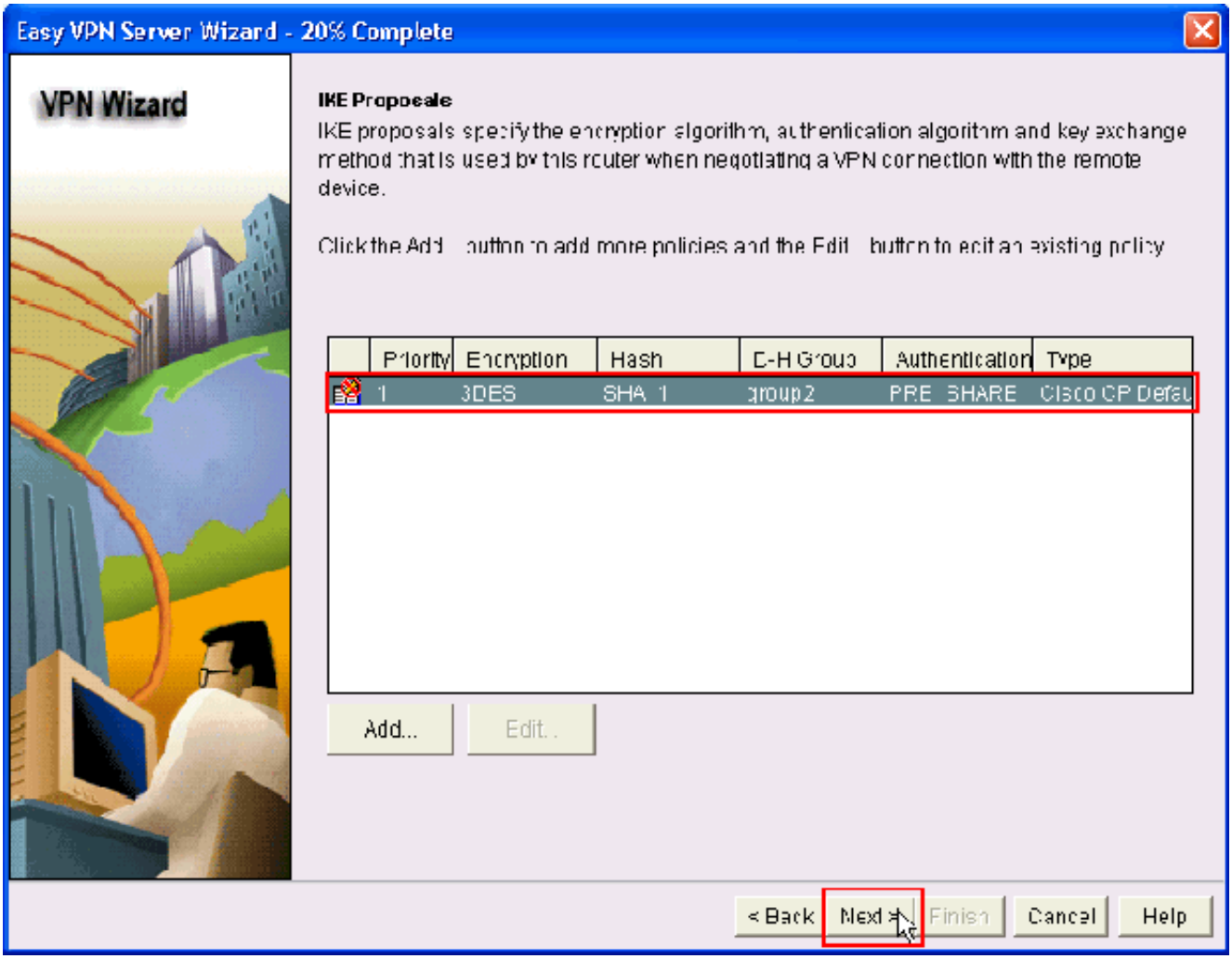


5. 提供**加密算法**、**验证算法**和**密钥交换方法**如显示此处，然后点击OK键

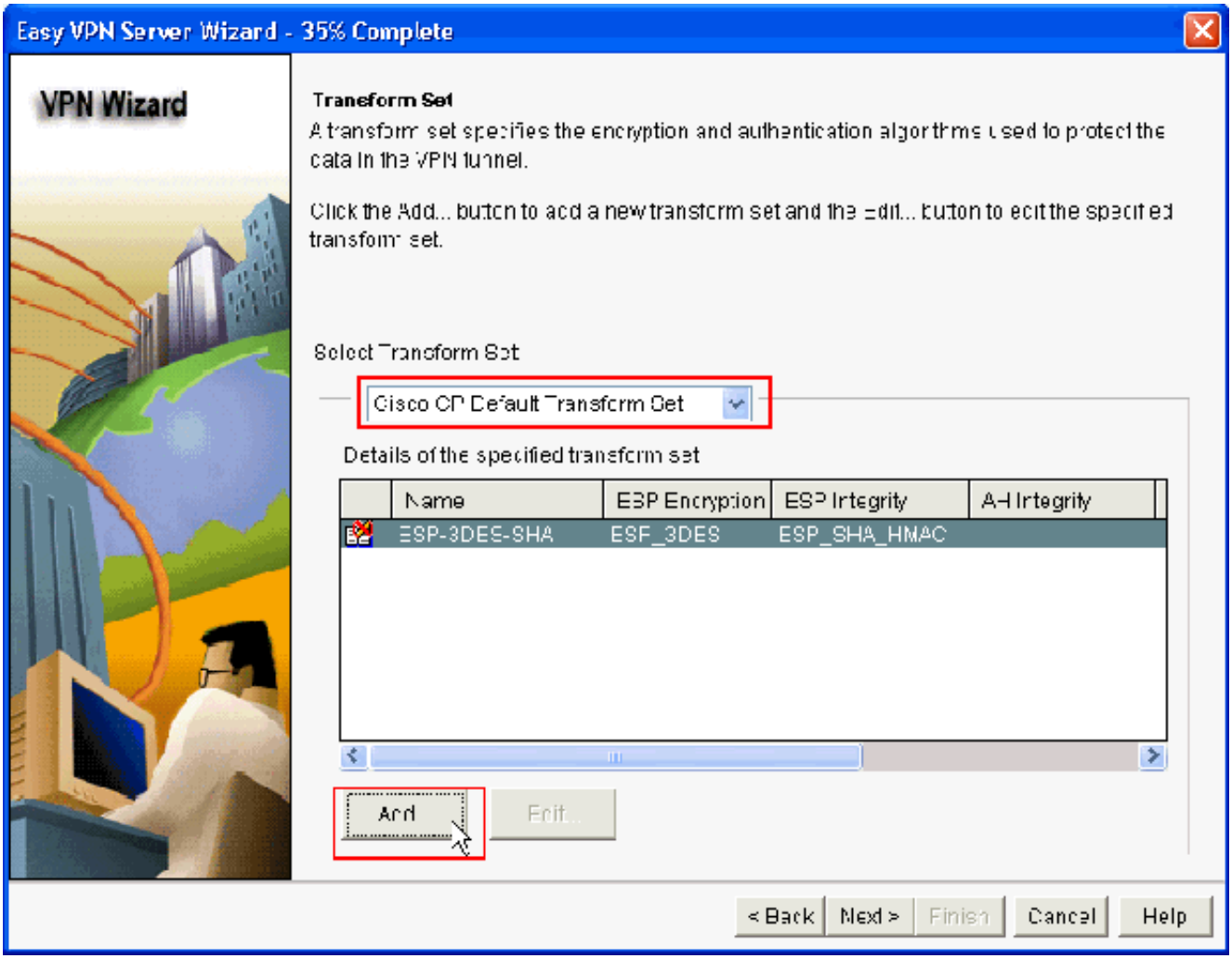


:

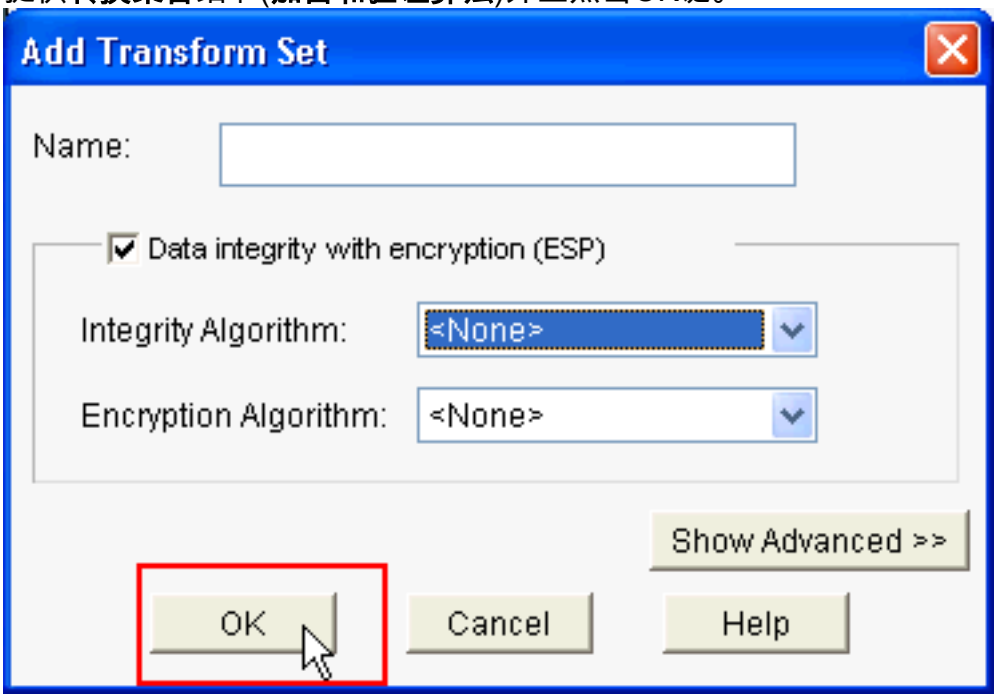
6. **默认IKE策略**用于此示例。结果，请选择默认IKE策略并且**其次**单击。



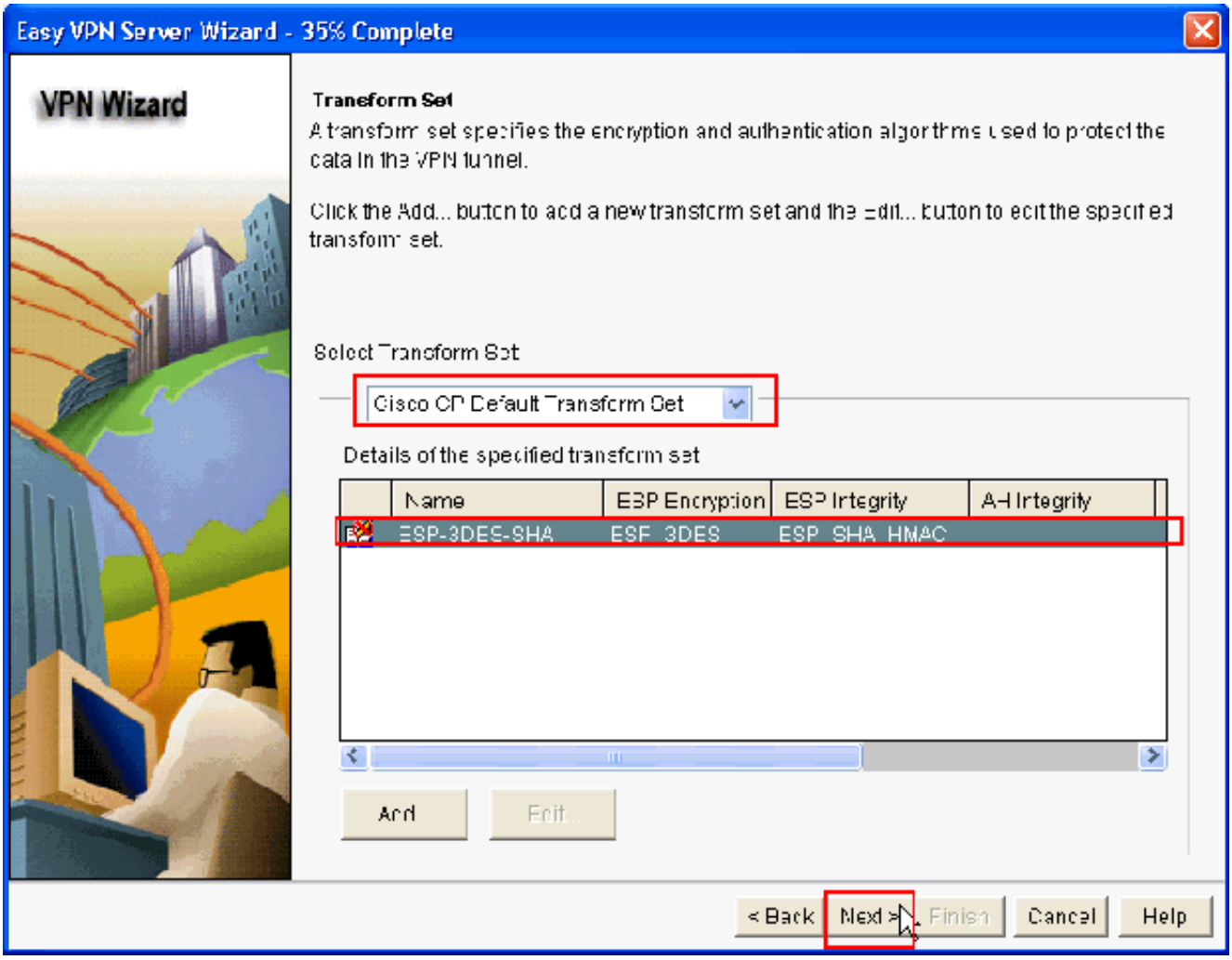
7. 在新窗口，应该提供**转换集合**细节。“转换集”指定用于保护 VPN 隧道中的数据的**加密**算法和验证算法。单击**添加**提供这些细节。您能添加任何数量的转换集，当需要，当您单击时请**添加**并且提供细节。**注意：** 默认情况下**CP默认转换集**是存在路由器，当配置使用**思科CP**。



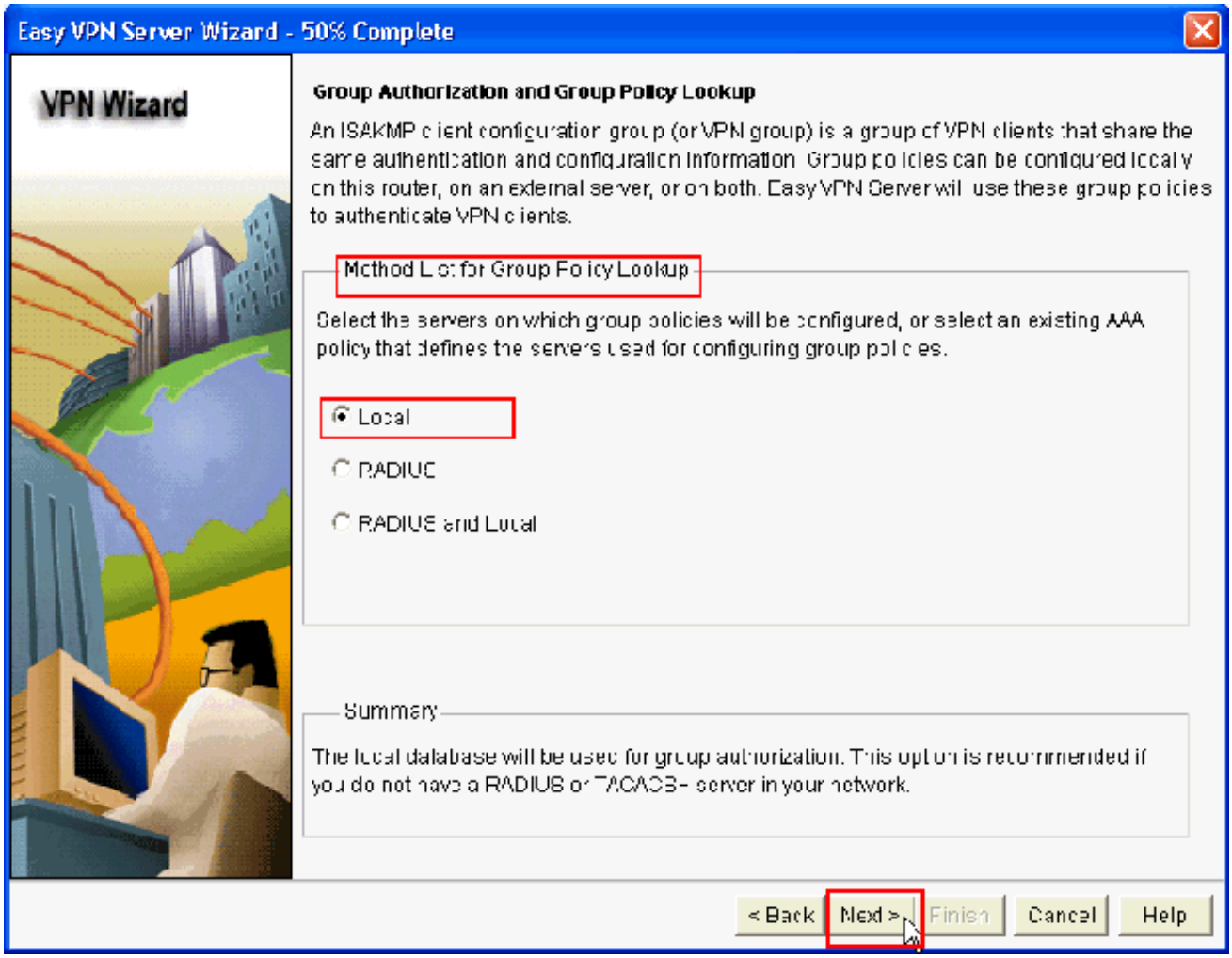
8. 提供**转换集合**细节(**加密和验证算法**)并且点击OK键。



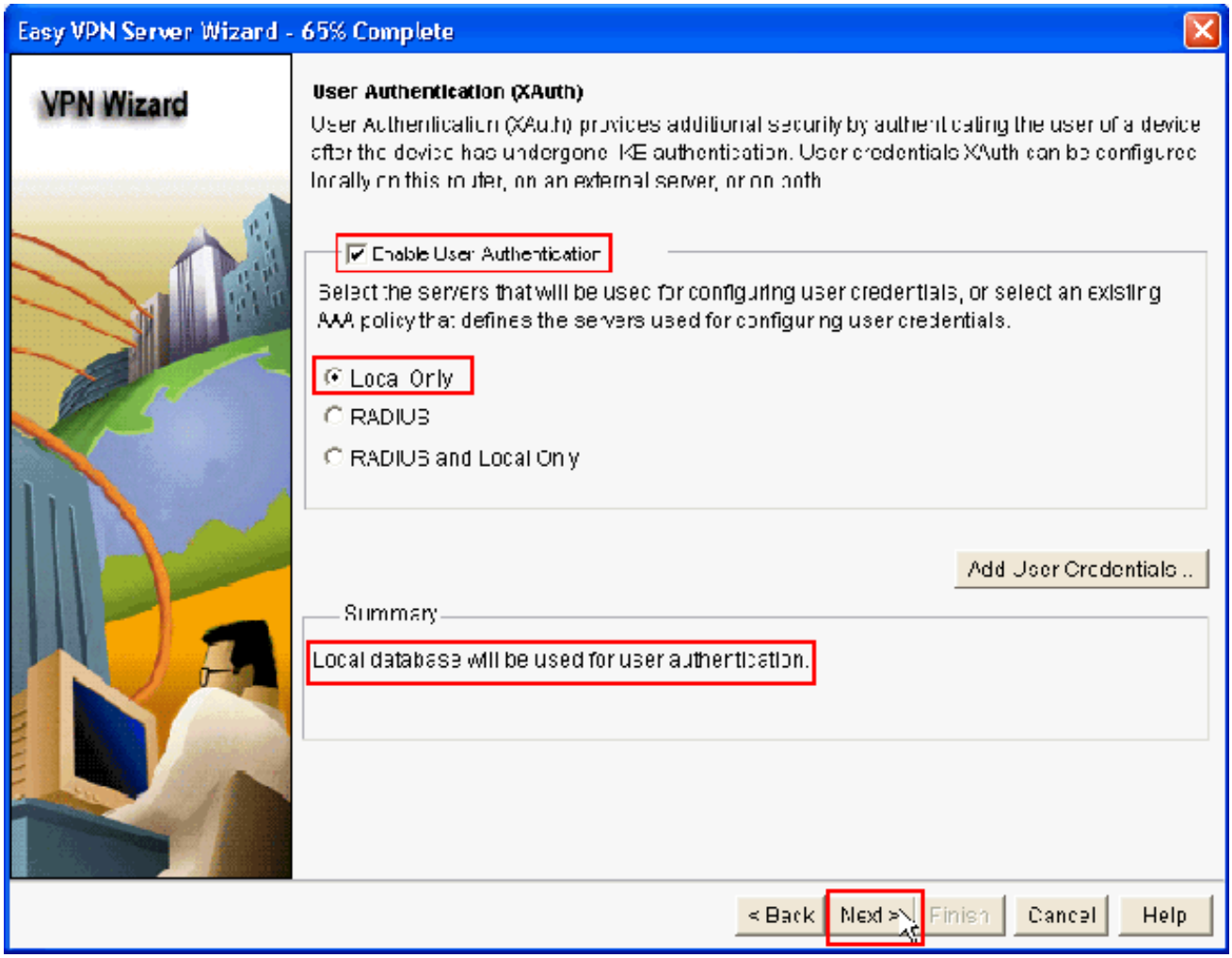
9. **默认转换集**名为**CP默认转换集**用于此示例。结果，请选择设置的默认转换并且**其次**单击。



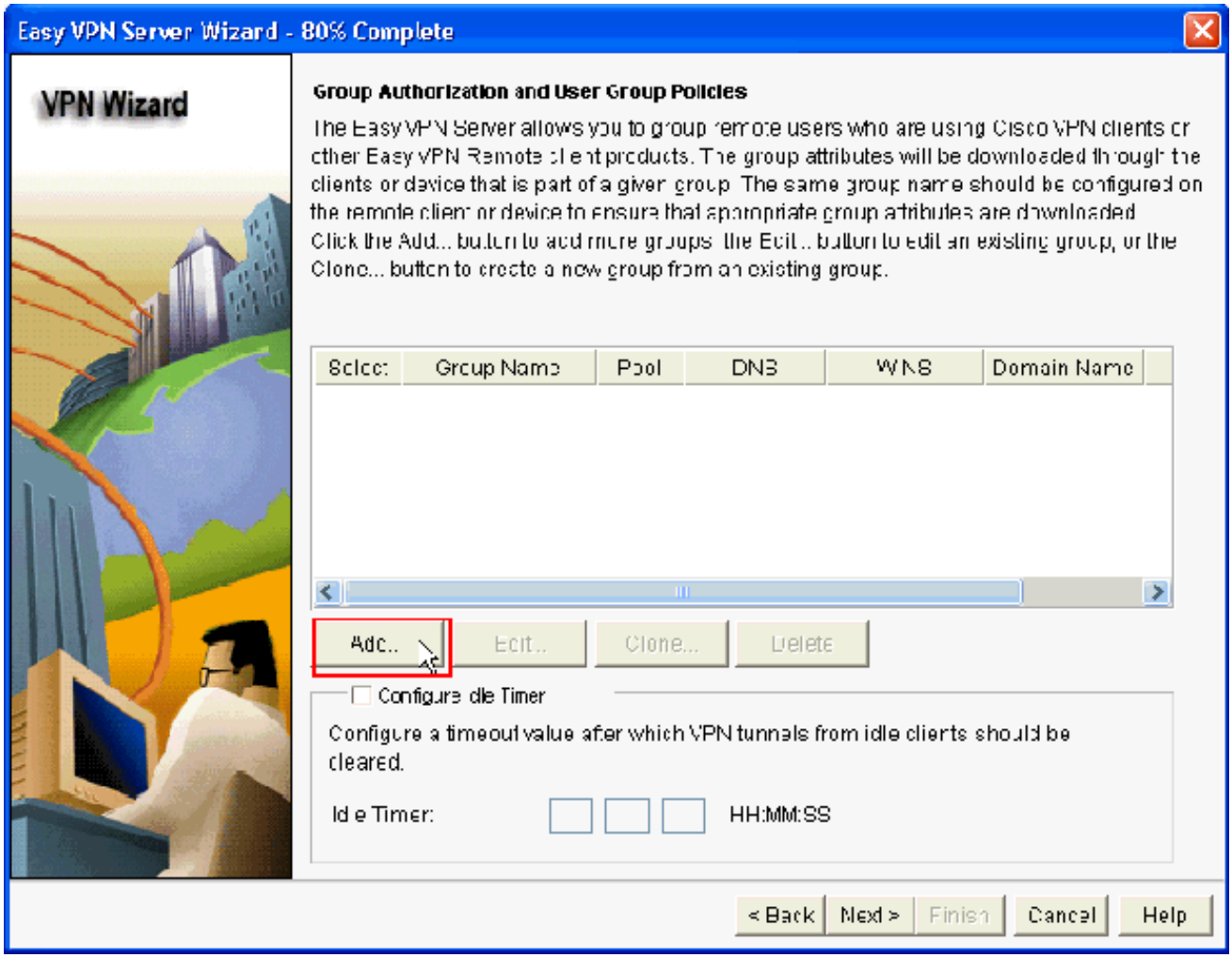
10. 在新窗口，请选择组策略将配置可以是**本地**或RADIUS或者**本地和RADIUS的**服务器。在本例中，我们使用**当地服务器**配置组策略。选择**本地**并且**其次**单击。



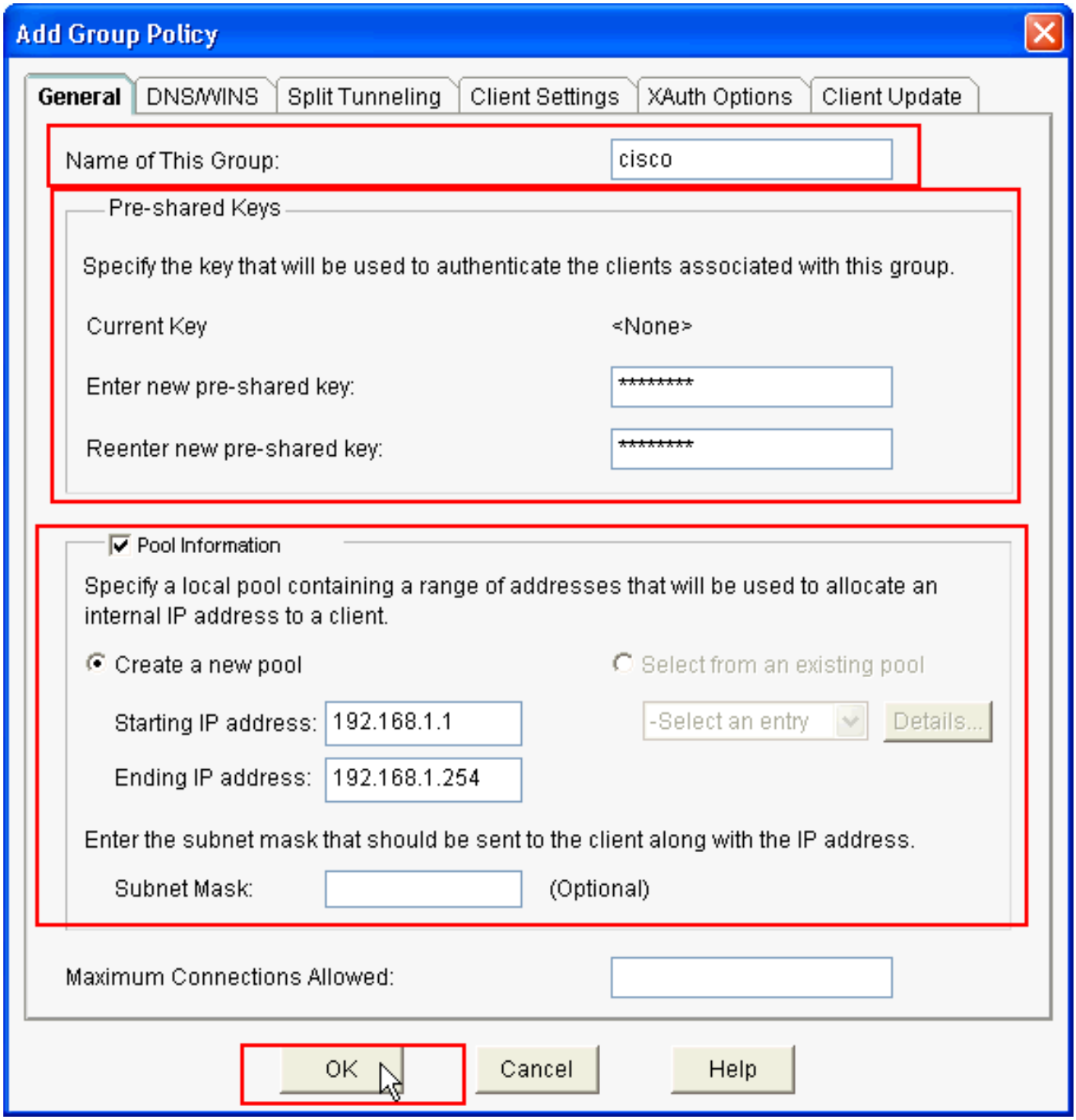
11. 选择将用于用户认证服务器在可以是**仅本地**或RADIUS或者**仅本地和RADIUS的**此新窗口。在本例中我们使用**当地服务器**配置验证的用户凭证。在**启用的用户验证旁边**确保复选框被检查。选择**仅本地**并且**其次**单击。



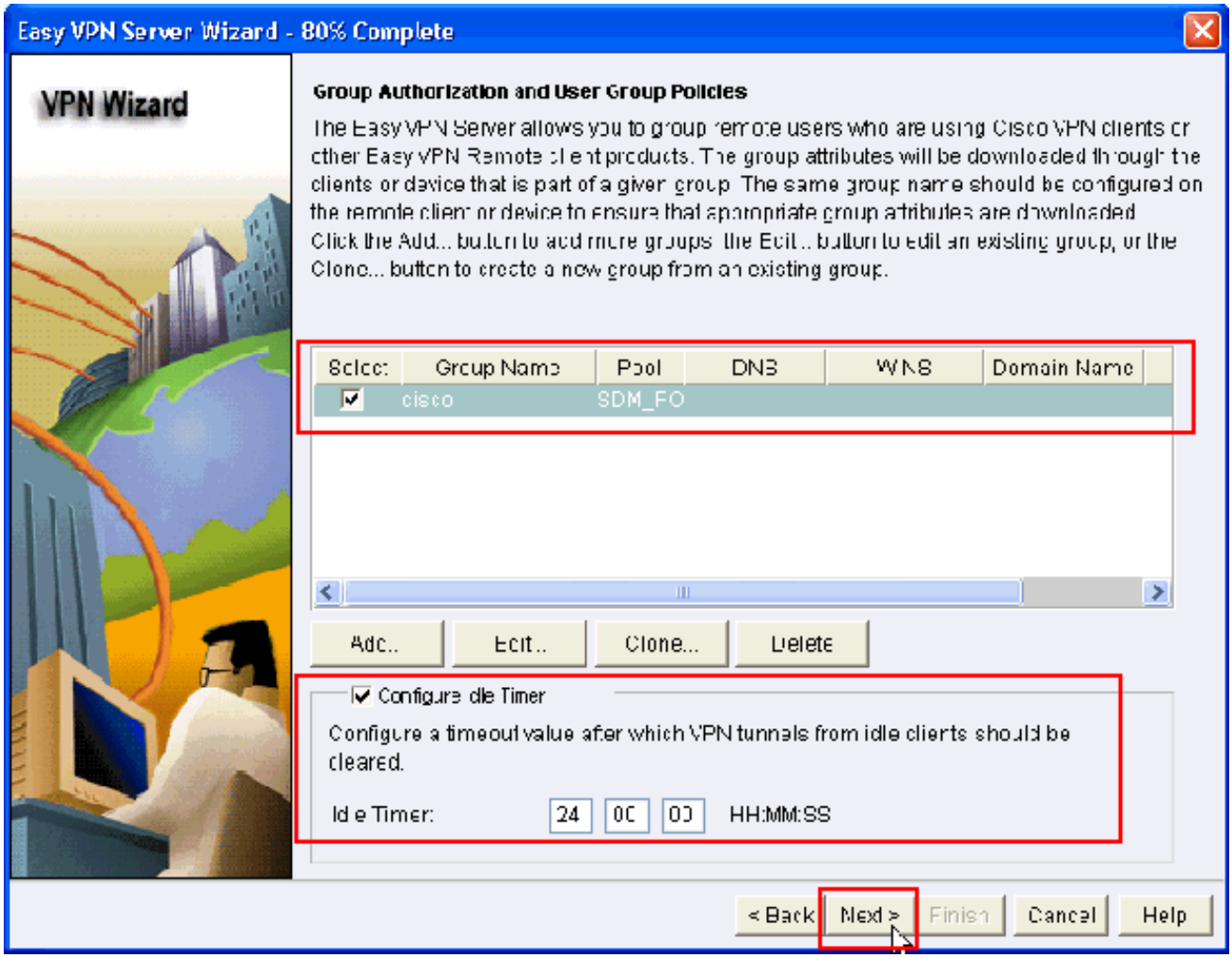
12. 单击**添加**创建一项新的组策略和添加远程用户在此组中。



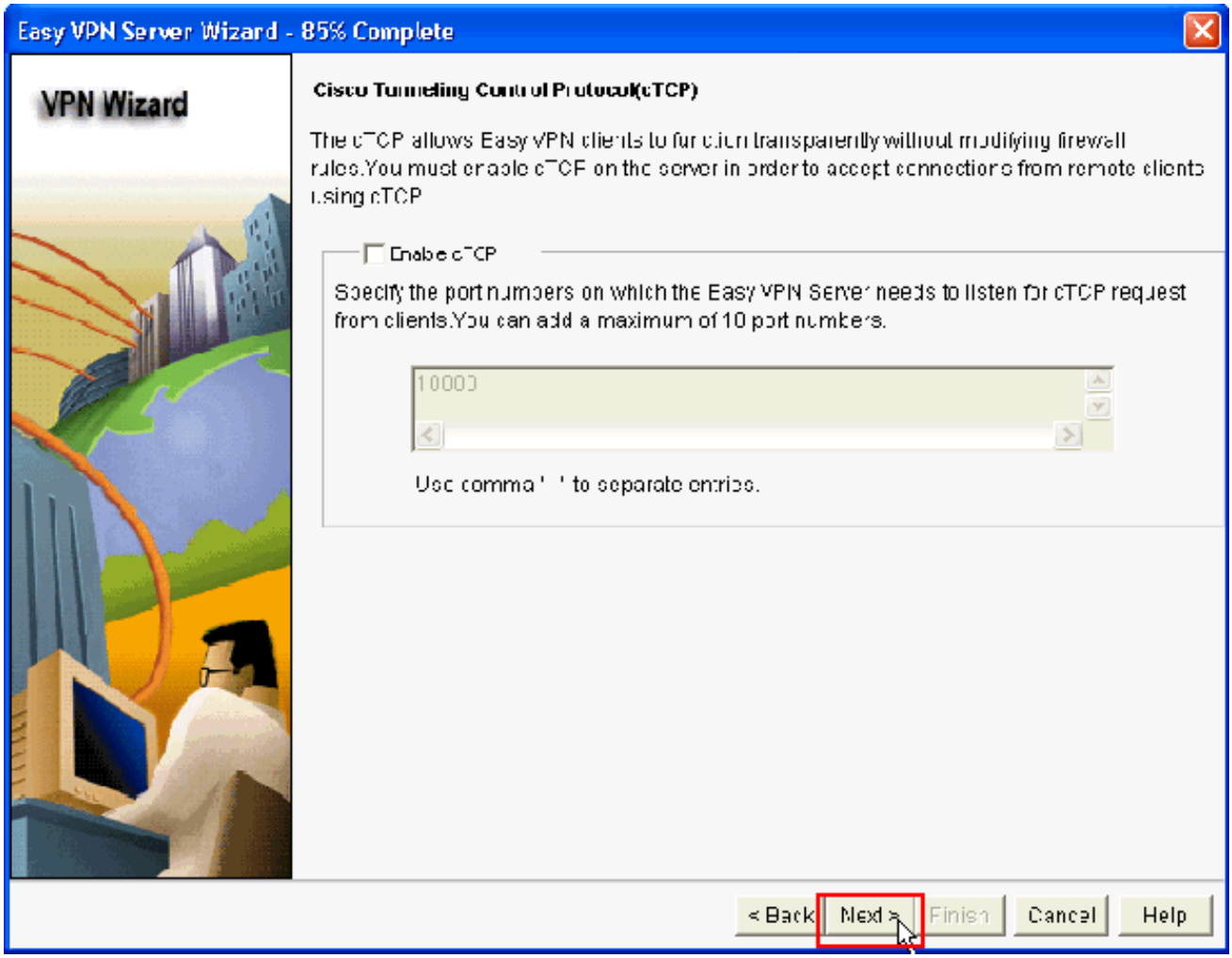
13. 在**添加组策略**窗口，请提供在空间的组名提供**此组**(在本例中的**cisco**)**名称**与**预先共享密钥一起**和**IP池**(**开始的IP地址**和**结束IP地址**)信息如显示并且点击OK键。**注意：** 若有您能创建一个新的IP池或使用一个现有IP池。



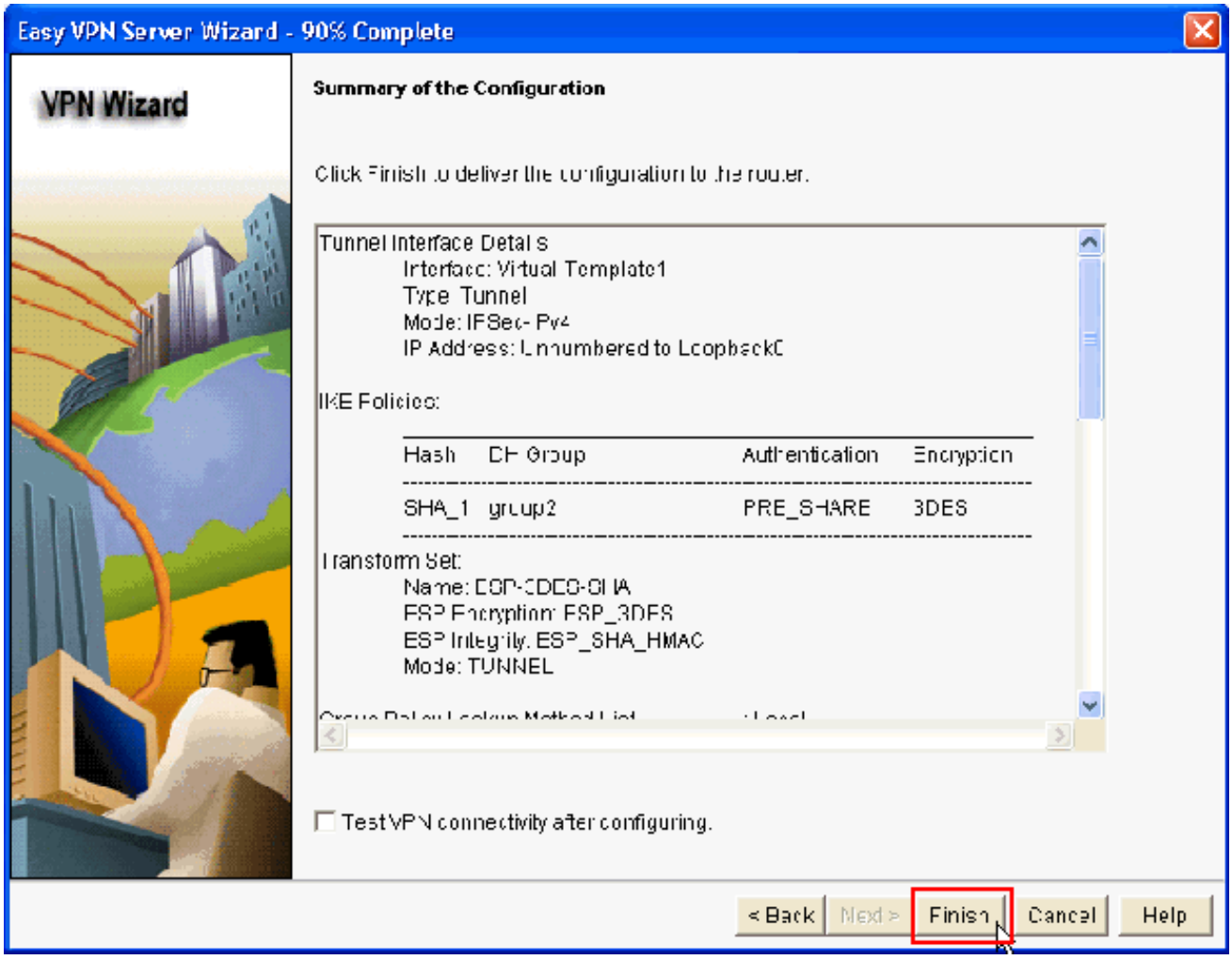
14. 现在请选择新的**组策略**创建与命名cisco然后单击复选框在旁边**配置空闲计时器**根据命令配置**空闲计时器需要**。单击 **Next**。



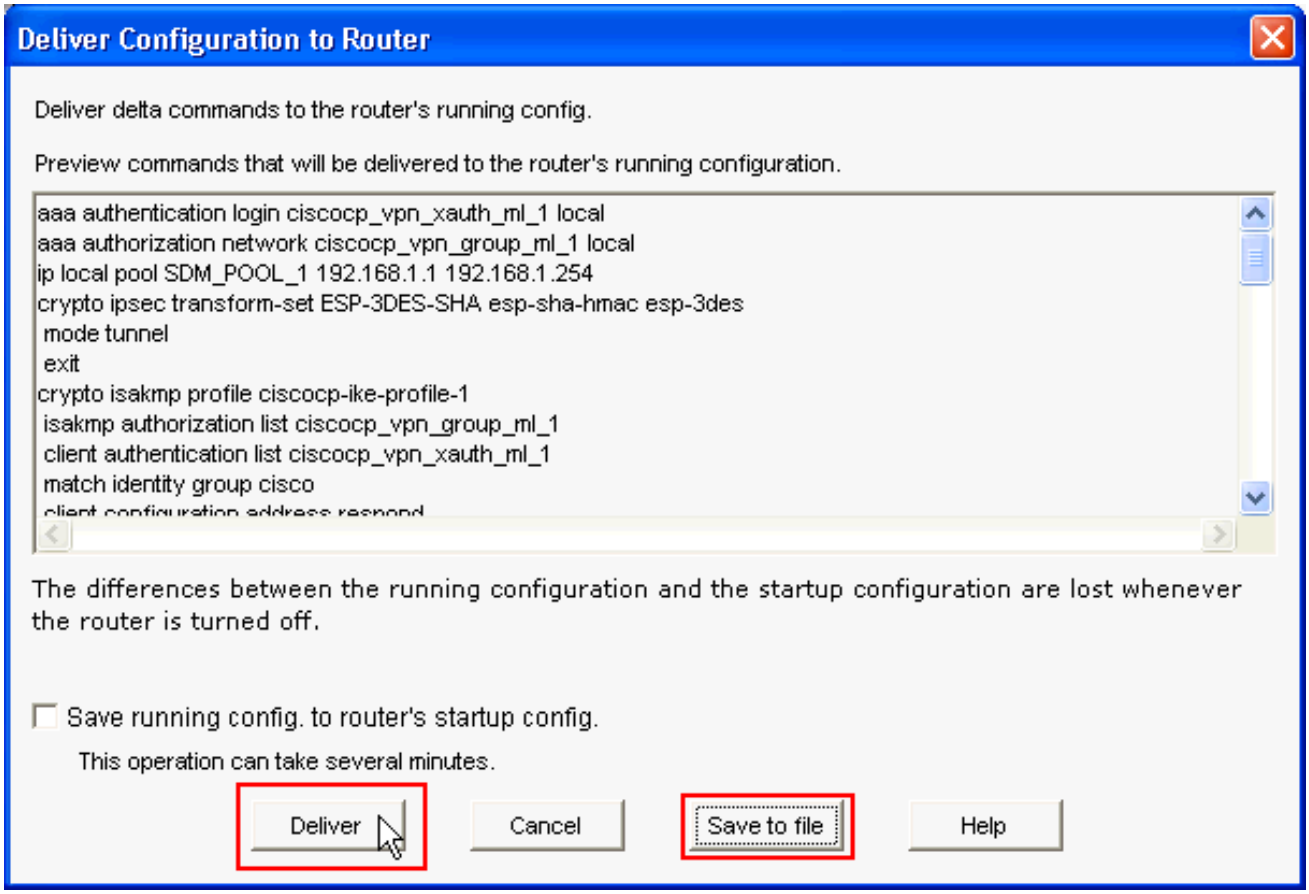
15. 启用如果必须**以隧道传输控制协议**(cTCP)的**思科**。否则，**其次请**单击。



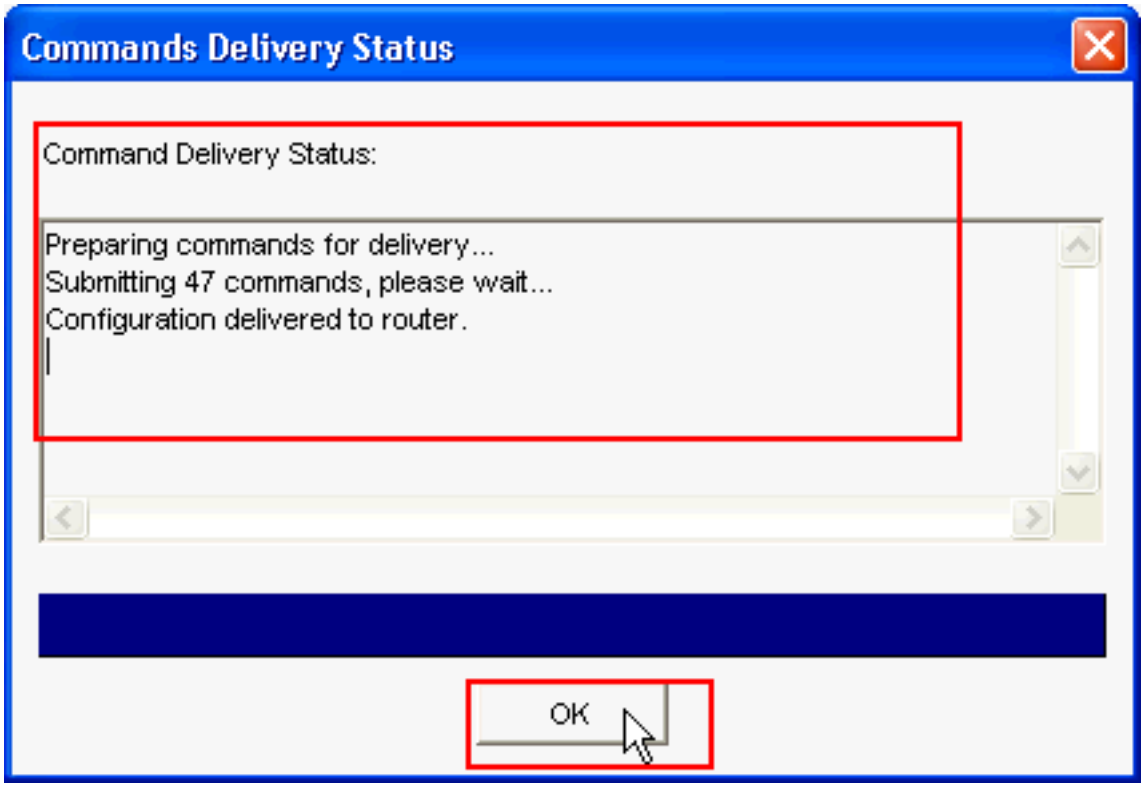
16. 查看**配置的摘要**。单击 **完成**。



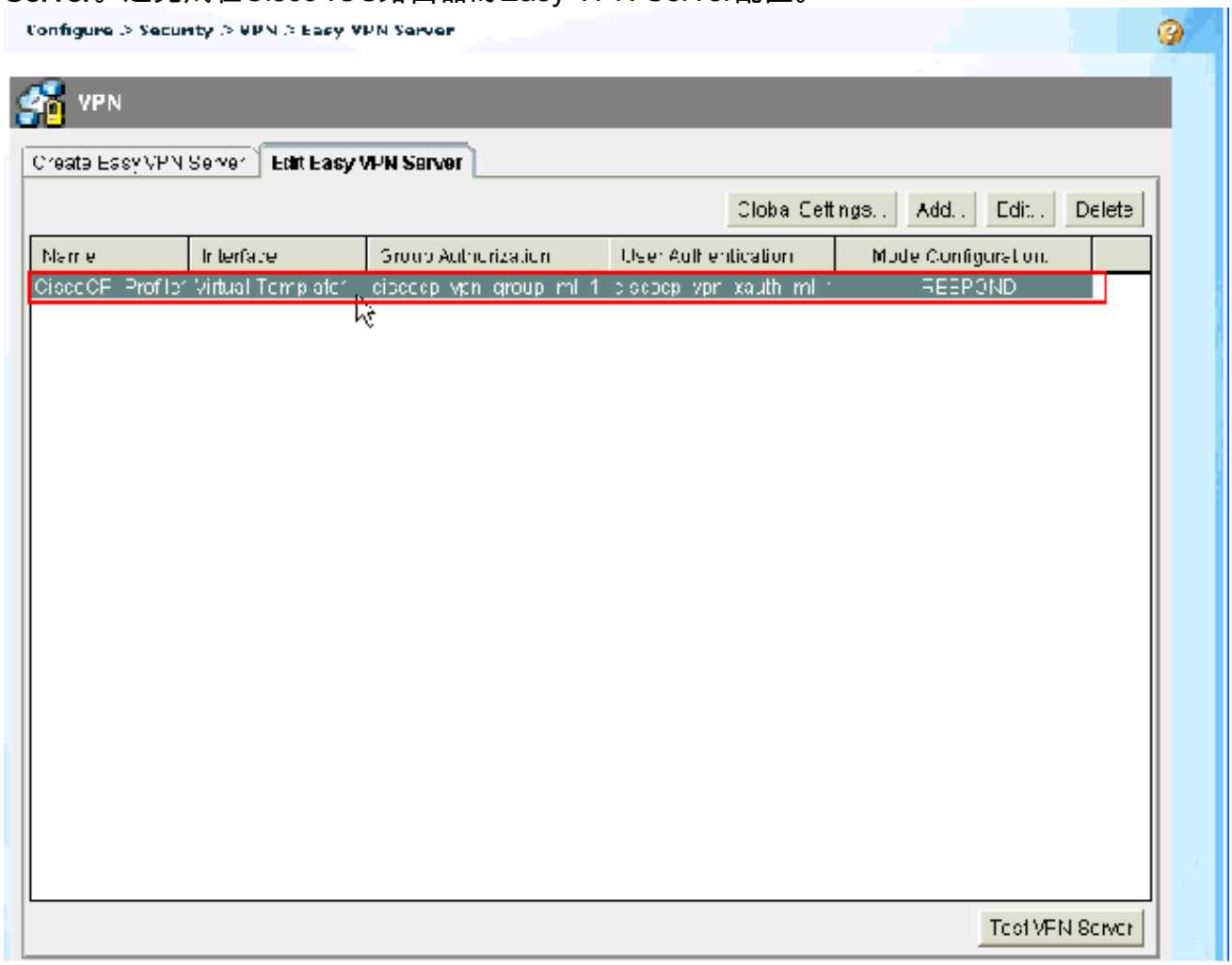
17. 在**对路由器**窗口的**传送配置中**，请单击**传送**提供配置到路由器。您能点击**"Save"到文件**保存配置作为在PC的一个文件。



18. **命令传送状态**窗口表示命令的传送状态到路由器。看起来作为**配置传送对路由器**。单击 **Ok**。



19. 您能看到新建立的Easy VPN Server。您能通过选择编辑现有的服务器**编辑Easy VPN Server**。这完成在Cisco IOS路由器的Easy VPN Server配置。



[CLI 配置]

路由器配置

```
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
```

验证

Easy VPN Server -请显示命令

使用本部分可确认配置能否正常运行。

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。`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** — 显示对等体上的所有当前 IPsec SA。`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`

故障排除

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- IPsec 协商/IKE 协议
- Cisco Configuration Professional 快速入门指南
- Cisco 产品支持页 - 路由器
- 技术支持和文档 - Cisco Systems