IOS Router como o Easy VPN Server usando o exemplo de configuração do profissional da configuração

Índice

Introdução

Este documento descreve como configurar um roteador do ® do Cisco IOS como um server fácil VPN (EzVPN) usando o Cisco Configuration Professional (Cisco CP) e o CLI. A característica Easy VPN Server permite que um usuário final remoto comunique-se usando a Segurança IP (IPsec) com qualquer gateway da Rede Privada Virtual (VPN) do Cisco IOS. As políticas de IPsec centralmente gerenciadas são "empurradas" ao dispositivo de cliente pelo servidor, minimizando a configuração pelo usuário final.

Para obter mais informações sobre do Easy VPN Server refira a seção do Easy VPN Server da biblioteca do manual de configuração da conectividade segura, Cisco IOS Release 12.4T.

Pré-requisitos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 1841 Router com Cisco IOS Software Release 12.4(15T)

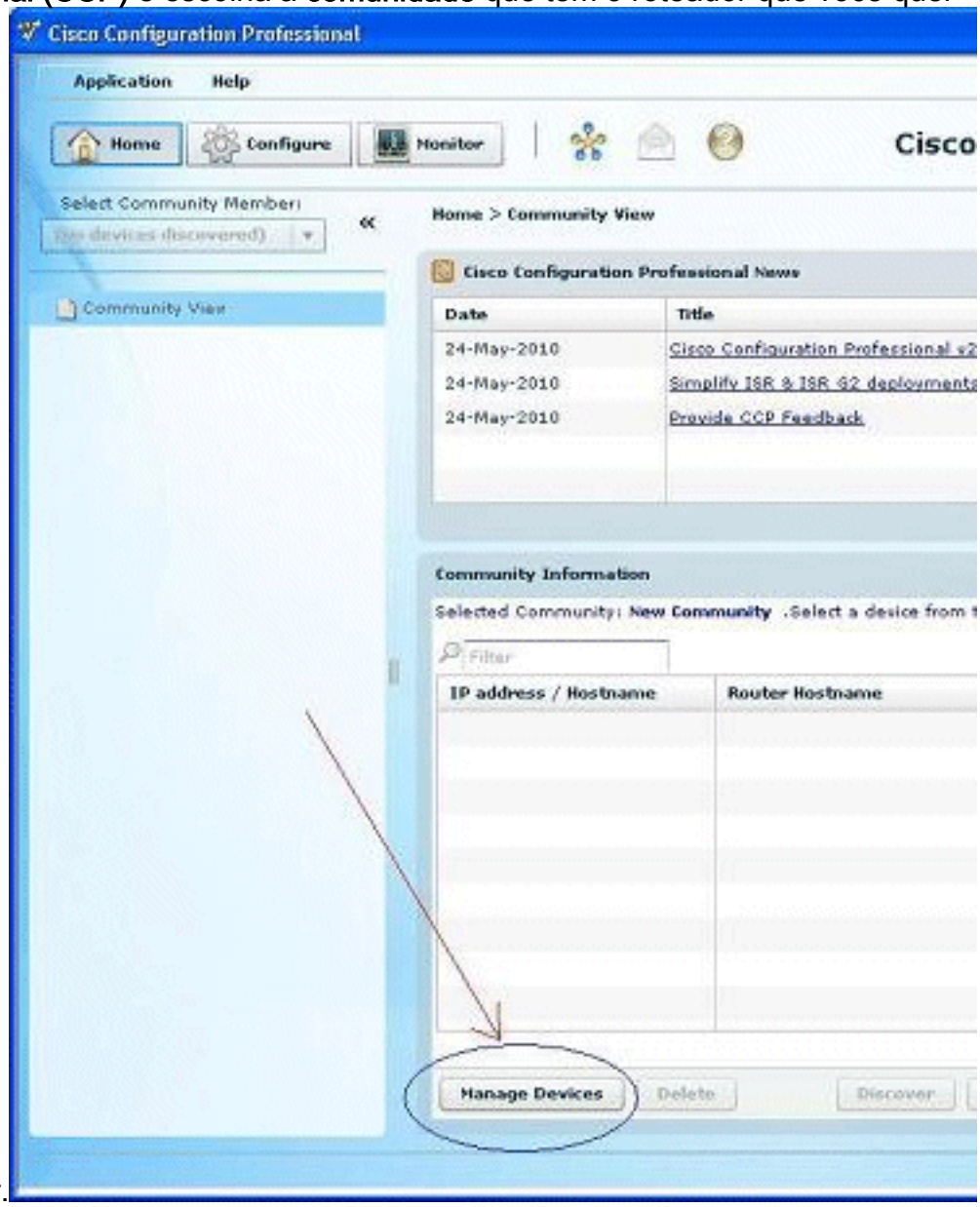
- Versão 2.1 de Cisco CP

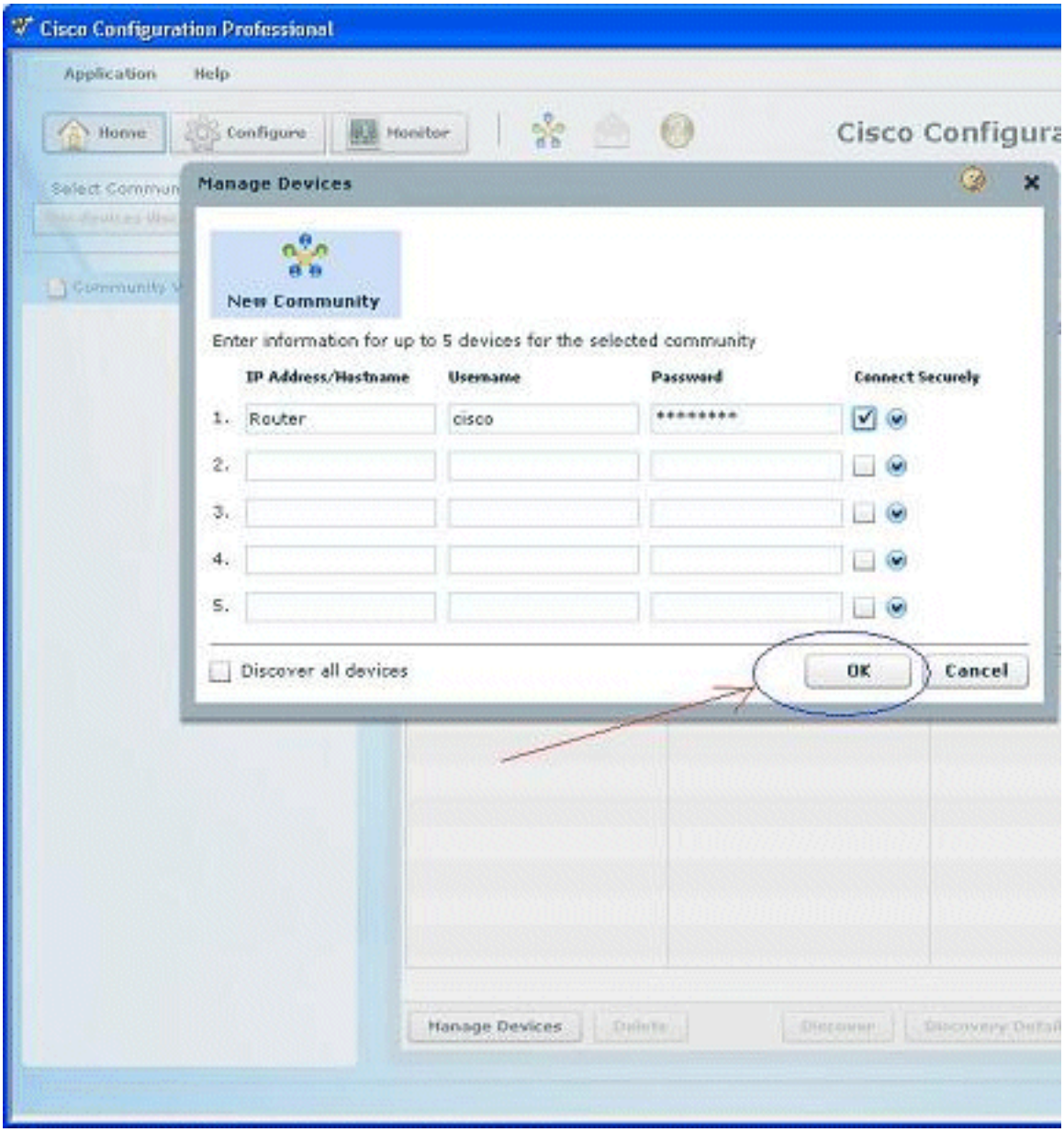
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Instale Cisco CP

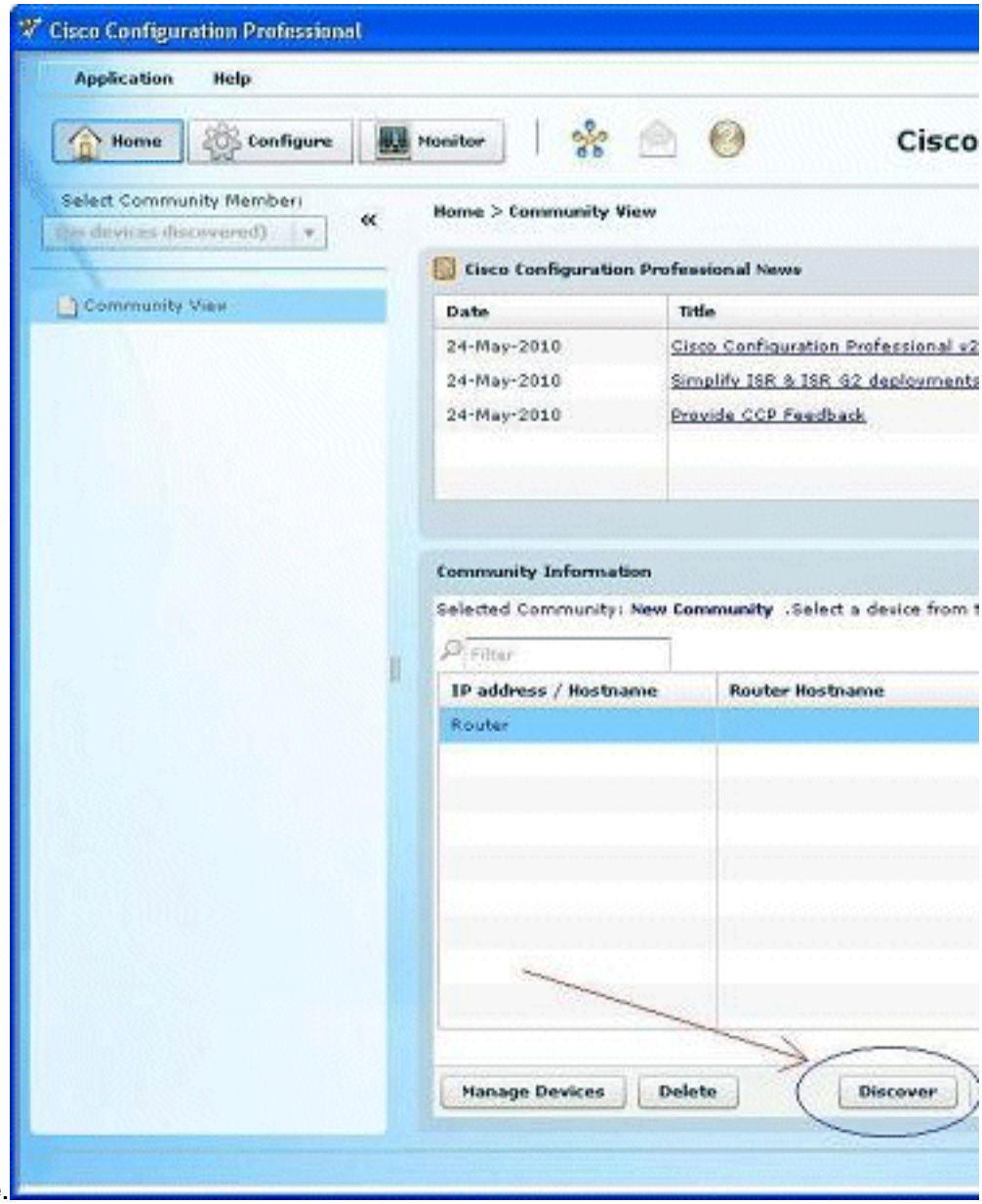
Execute estas etapas a fim instalar Cisco CP:

1. Transfira Cisco CP V2.1 do Centro de Software da Cisco (clientes registrados somente) e instale-o em seu PC local.A versão a mais atrasada de Cisco CP pode ser encontrada no Web site de Cisco CP.
2. Lance Cisco CP de seu PC local através do **Start > Programs >** do **Cisco Configuration Professional (CCP)** e escolha a **comunidade** que tem o roteador que você quer configurar.





3. A fim descobrir o dispositivo que você quer configurar, para destacar o roteador e o clique

descobre. 

Nota: Para obter informações sobre dos modelos e das versões do IOS do roteador Cisco que são compatíveis a Cisco CP v2.1, refira a seção compatível das liberações do Cisco IOS.

Nota: Para obter informações sobre das exigências PC que dirige Cisco CP v2.1, refira a seção dos requisitos do sistema.

Configuração de roteador para dirigir Cisco CP

Execute estas etapas de configuração a fim dirigir Cisco CP em um roteador Cisco:

1. Conecte a seu roteador que usa o telnet, SSH, ou através do console.Incorpore o modo de configuração global usando este comando:`Router(config)#`**`enable`** `Router(config)#`
2. Se o HTTP e o HTTPS são permitidos e configurados de usar números de porta não padronizados, você pode saltar esta etapa e simplesmente usar o número de porta já configurado.Permita o roteador HTTP ou o servidor HTTPS usando estes comandos do Cisco IOS Software:`Router(config)#` **`ip http server`** `Router(config)#` **`ip http secure-server`** `Router(config)#` **`ip http authentication local`**
3. Crie um usuário com o nível de privilégio 15:`Router(config)#` **`username`** *`<username>`* **`privilege 15 password 0`** *`<password>`* **Nota:** Substitua o *<username>* e o *<password>* com o nome de usuário e senha que você quer configurar.

4. Configurar o SSH e o telnet para o login local e o nível de privilégio 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. (Opcional) permita o logging local de apoiar a função de monitoramento do log:`Router(config)# logging buffered 51200 warning`

Requisitos

Este documento supõe que o roteador Cisco é plenamente operacional e configurado para permitir que Cisco CP faça alterações de configuração.

Para obter informações completas sobre de como começar usar Cisco CP, refira a obtenção começado com Cisco Configuration Professional.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

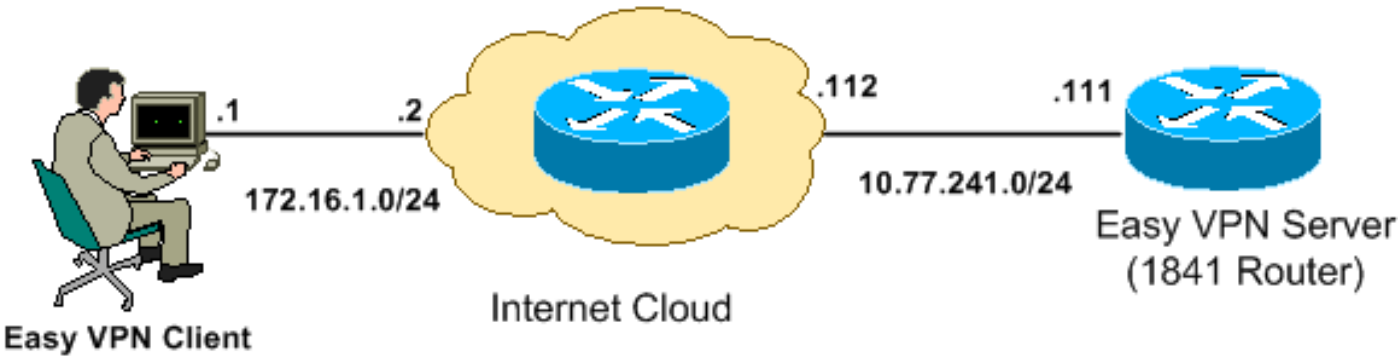
Configurar

Nesta seção, você é presentado com a informação para configurar as configurações básicas para um roteador em uma rede.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

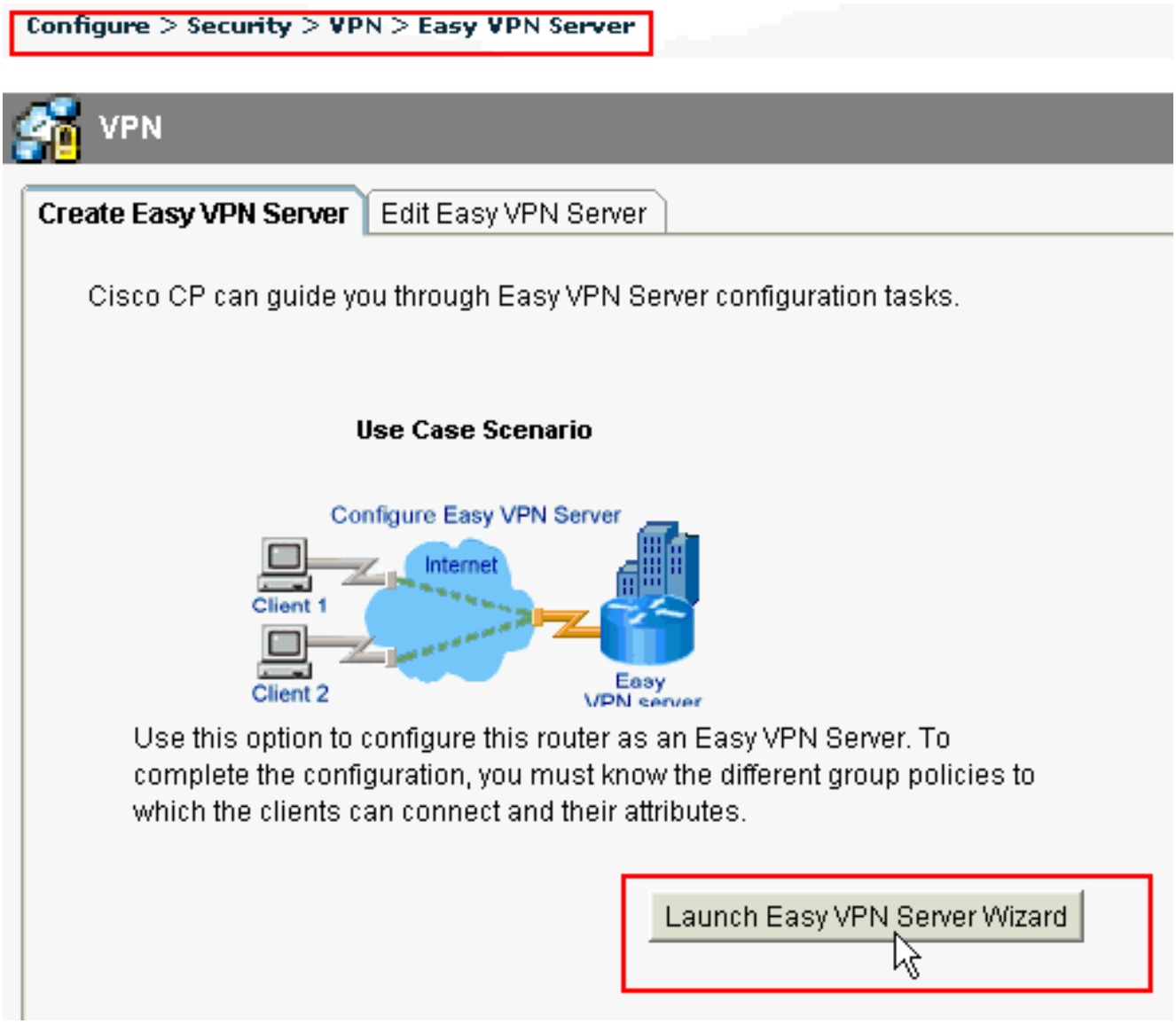


Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

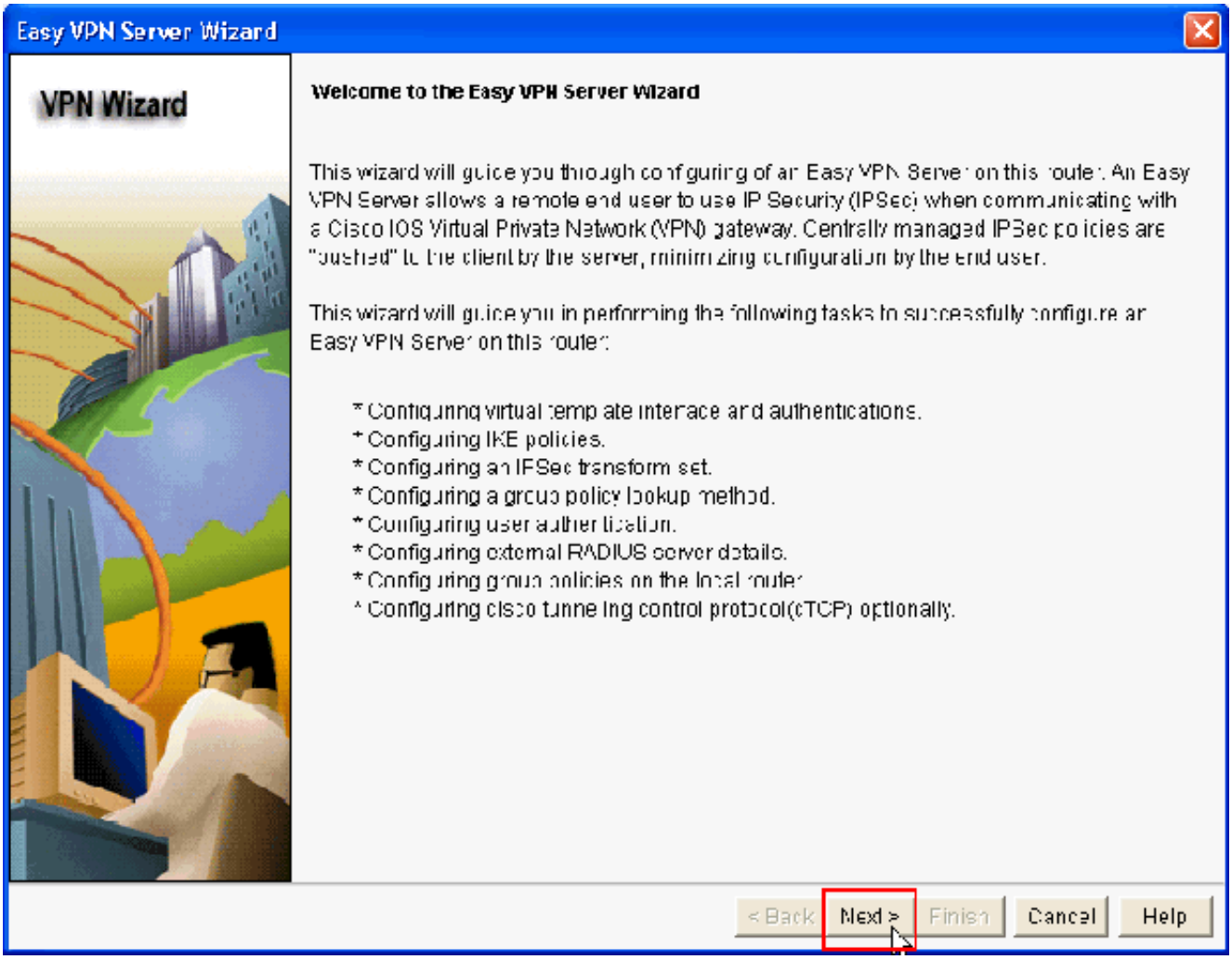
Cisco CP - Configuração do Easy VPN Server

Execute estas etapas a fim configurar o roteador do Cisco IOS como um Easy VPN Server:

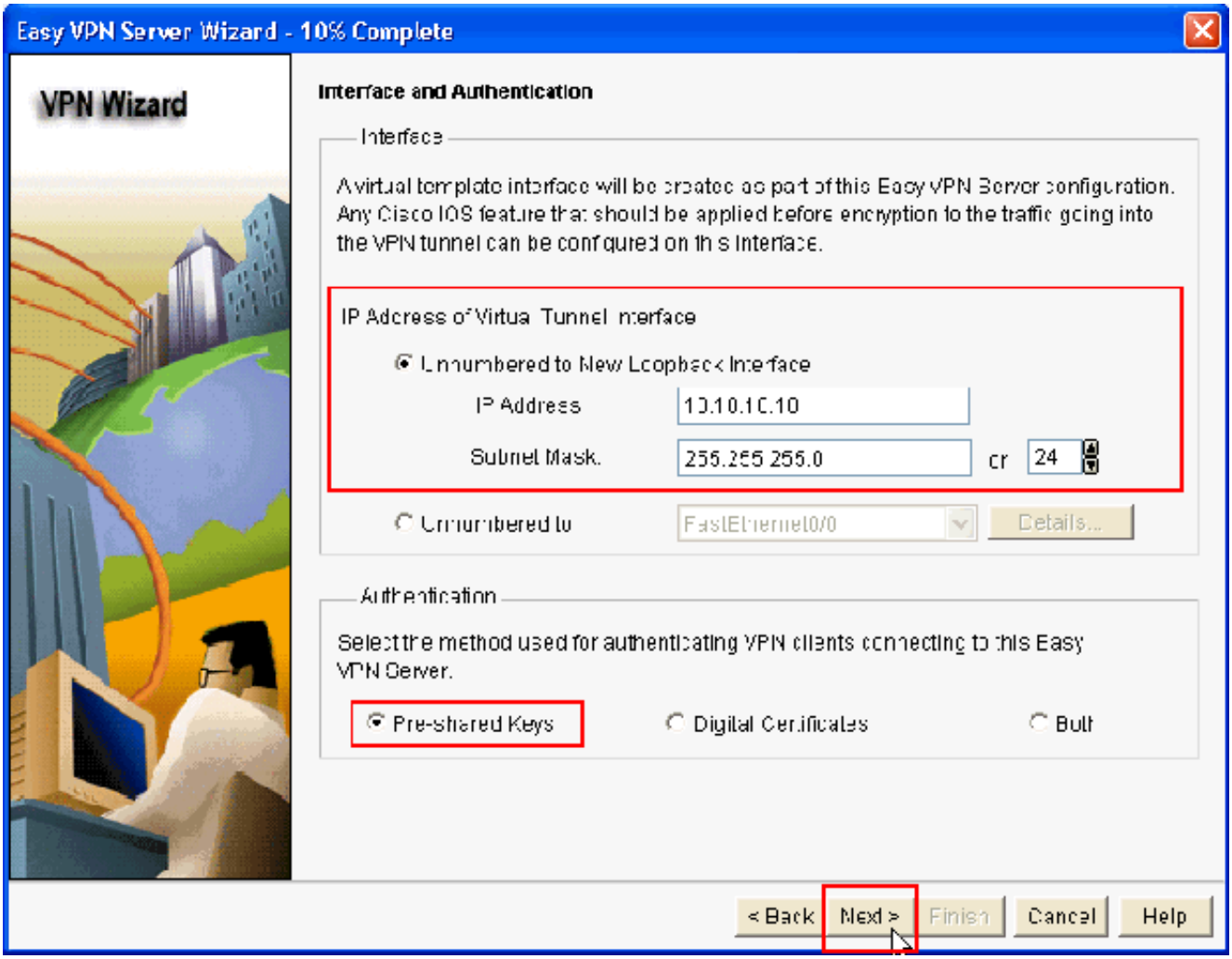
1. Escolha **configuram o** > segurança > o **VPN** > o **Easy VPN Server** > **criam o Easy VPN Server** e clicam o **assistente do Easy VPN Server do lançamento** a fim configurar o roteador do Cisco IOS como um Easy VPN Server:



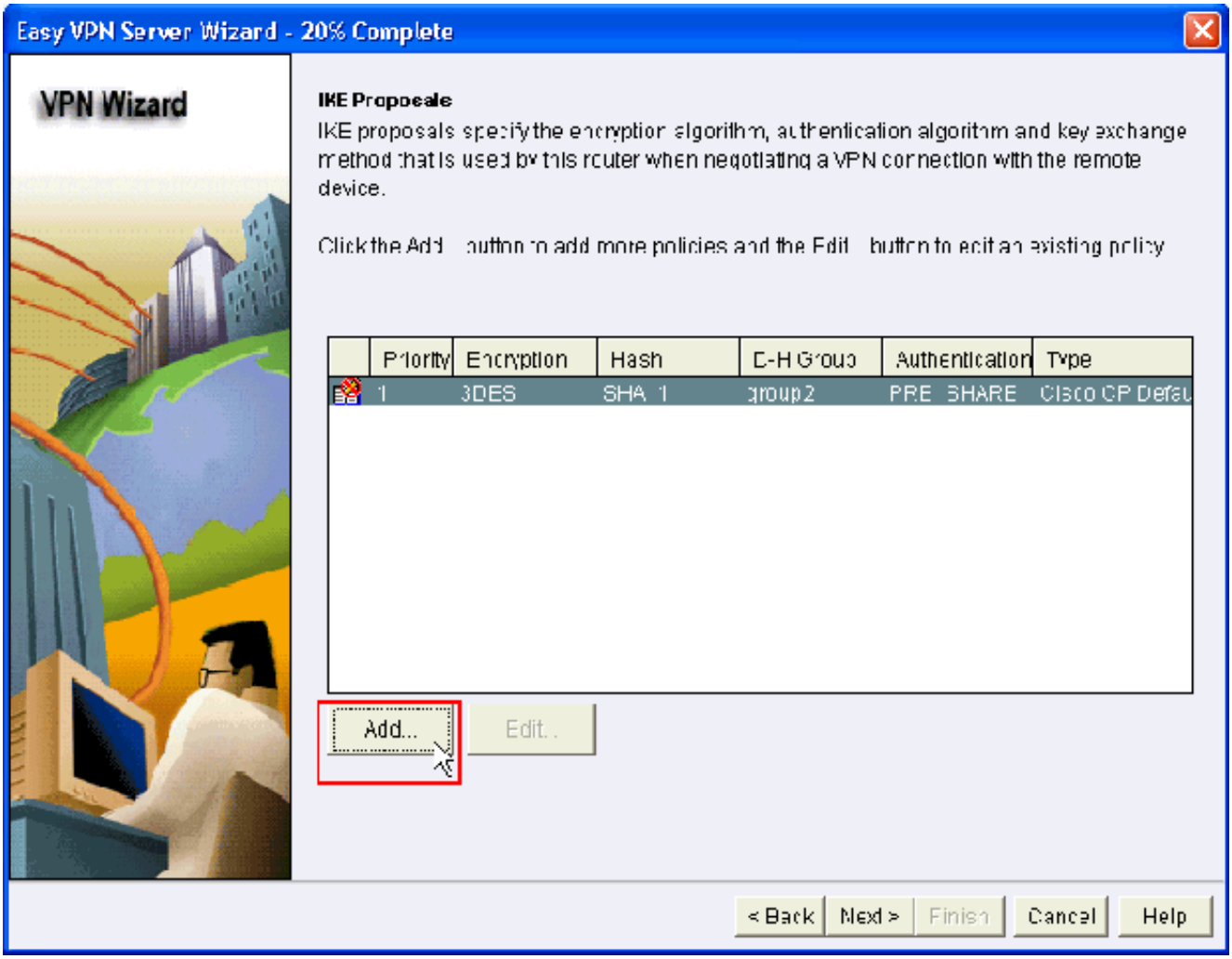
2. Clique **em seguida** a fim continuar com a configuração do **Easy VPN Server**.



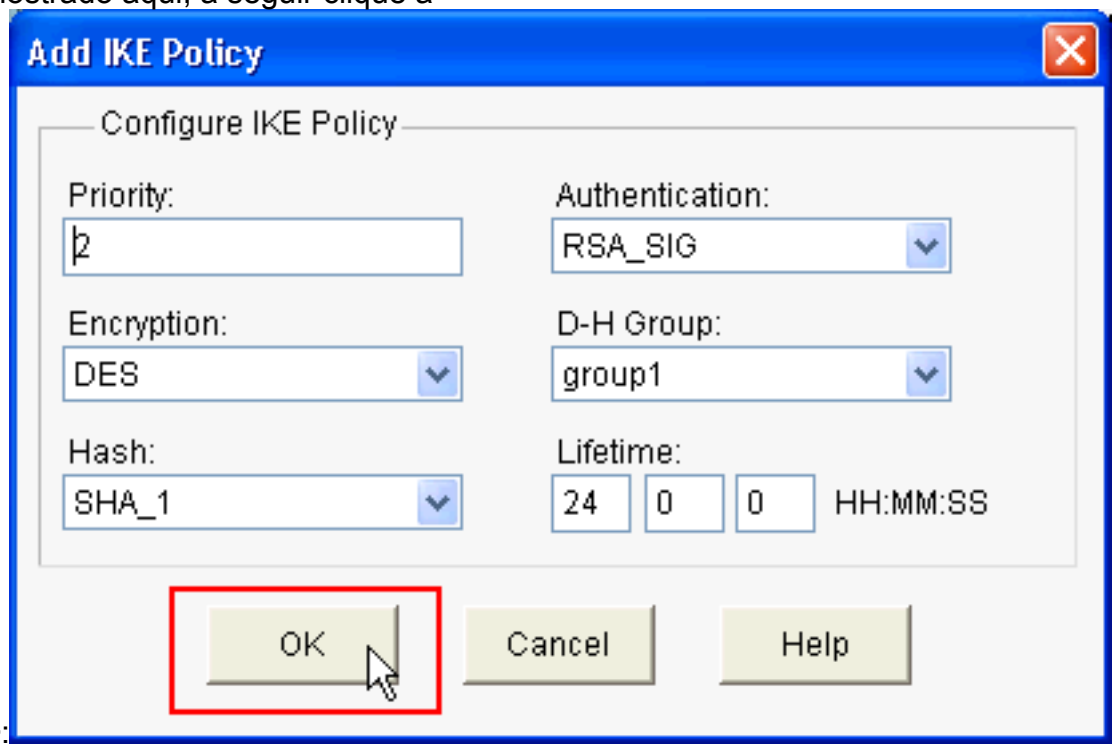
3. No indicador resultante, uma **interface virtual** será configurada como parte da configuração do Easy VPN Server. Forneça o **endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de túnel virtual** e igualmente escolha o **método de autenticação** usado autenticando os clientes VPN. Aqui, as **chaves pré-compartilhada** são o método de autenticação usado. Clique **em**
seguida:



4. Especifique o **algoritmo de criptografia, o algoritmo de autenticação e o método das trocas de chave** a ser usado por este roteador ao negociar com o dispositivo remoto. Uma política de IKE do padrão esta presente no roteador que pode ser usado se for necessário. Se você quer adicionar uma política de IKE nova, o clique
adiciona.

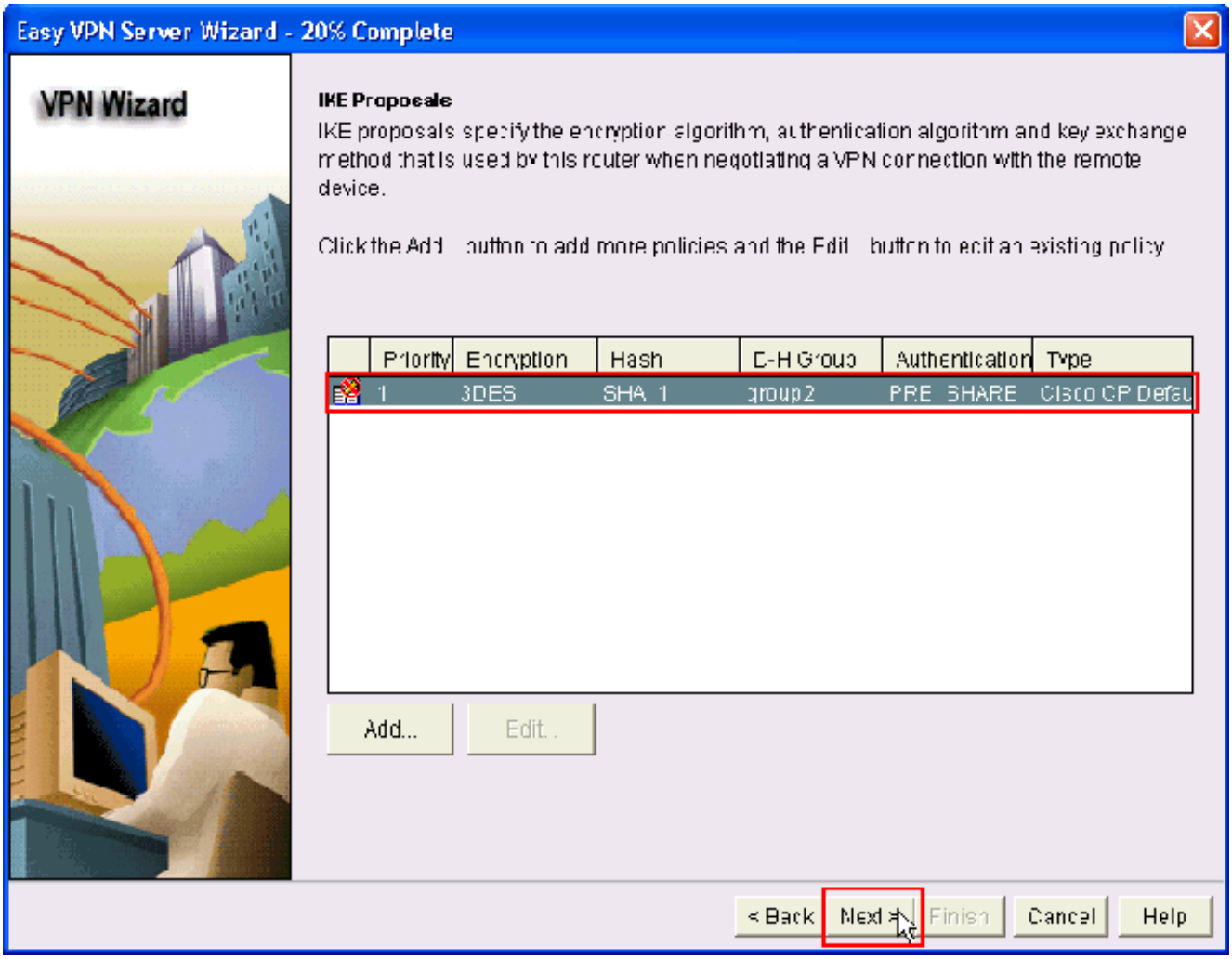


5. Forneça o **algoritmo de criptografia**, o **algoritmo de autenticação**, e o **método das trocas de chave** como mostrado aqui, a seguir clique a

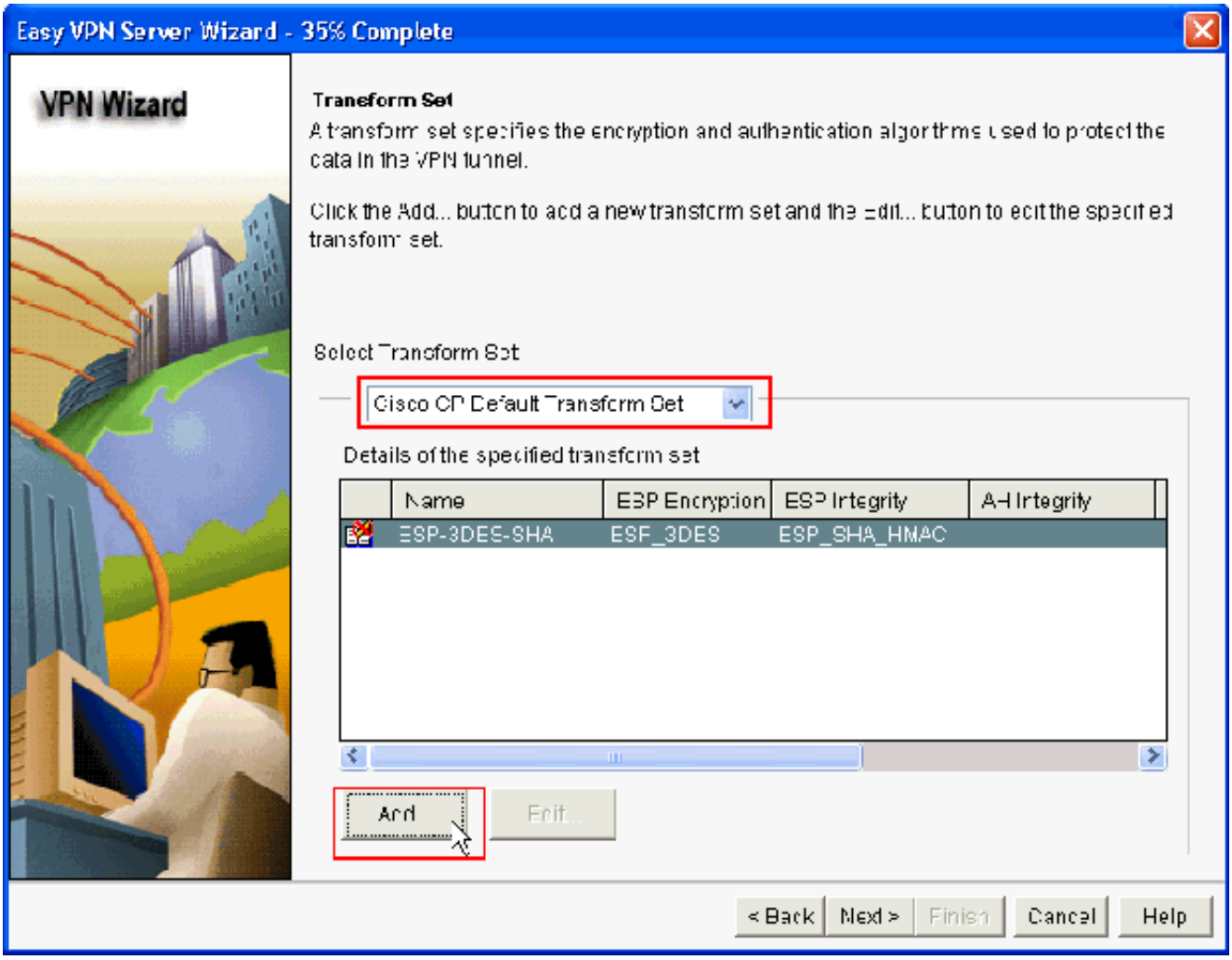


APROVAÇÃO:

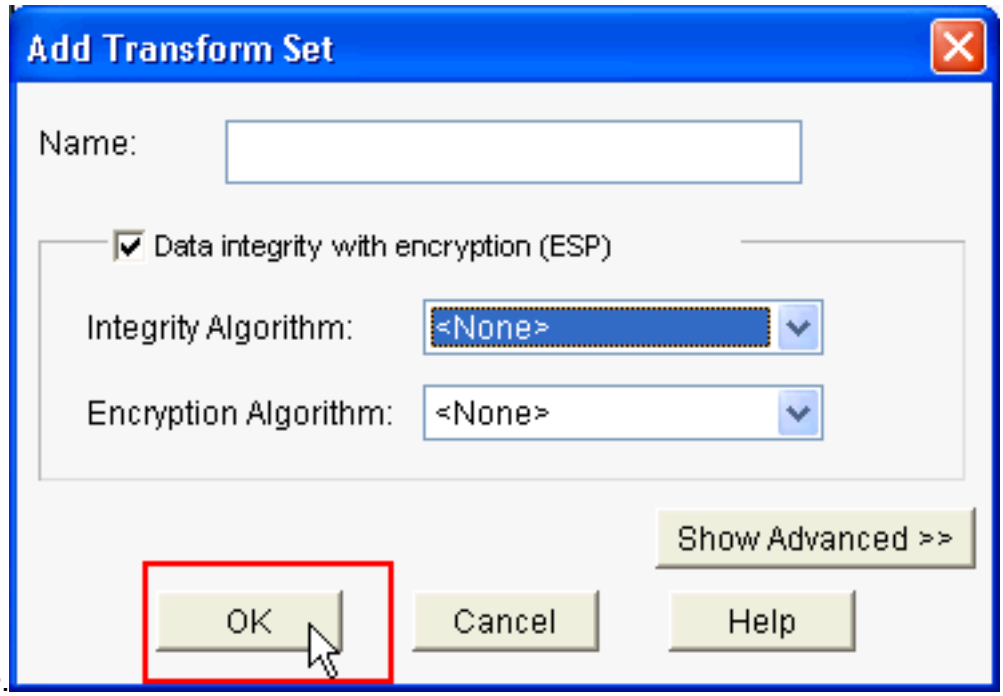
6. **A política de IKE do padrão** é usada neste exemplo. Em consequência, escolha a política de IKE do padrão e clique-a **em seguida**.



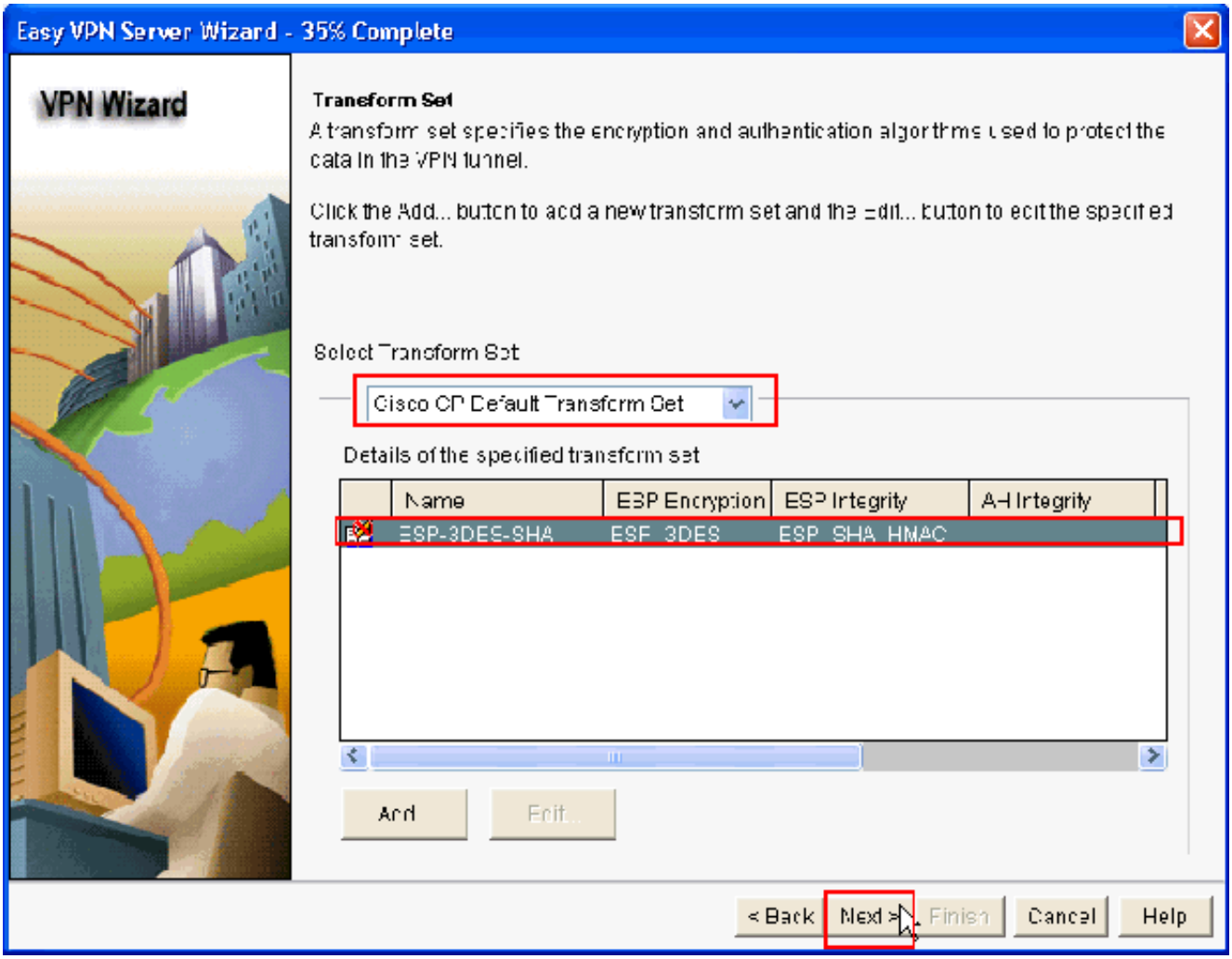
7. Na nova janela, os detalhes **ajustados da transformação** devem ser fornecidos. O grupo da transformação especifica a **criptografia** e os **algoritmos de autenticação** usados para proteger **dados no VPN escavam um túnel**. O clique **adiciona** para fornecer estes detalhes. Você pode adicionar todo o número de grupos Transform como necessário quando você clique **adiciona** e fornece os detalhes.**Nota: O padrão CP transforma o grupo** esta presente à revelia no roteador quando configurado usando **Cisco CP**.



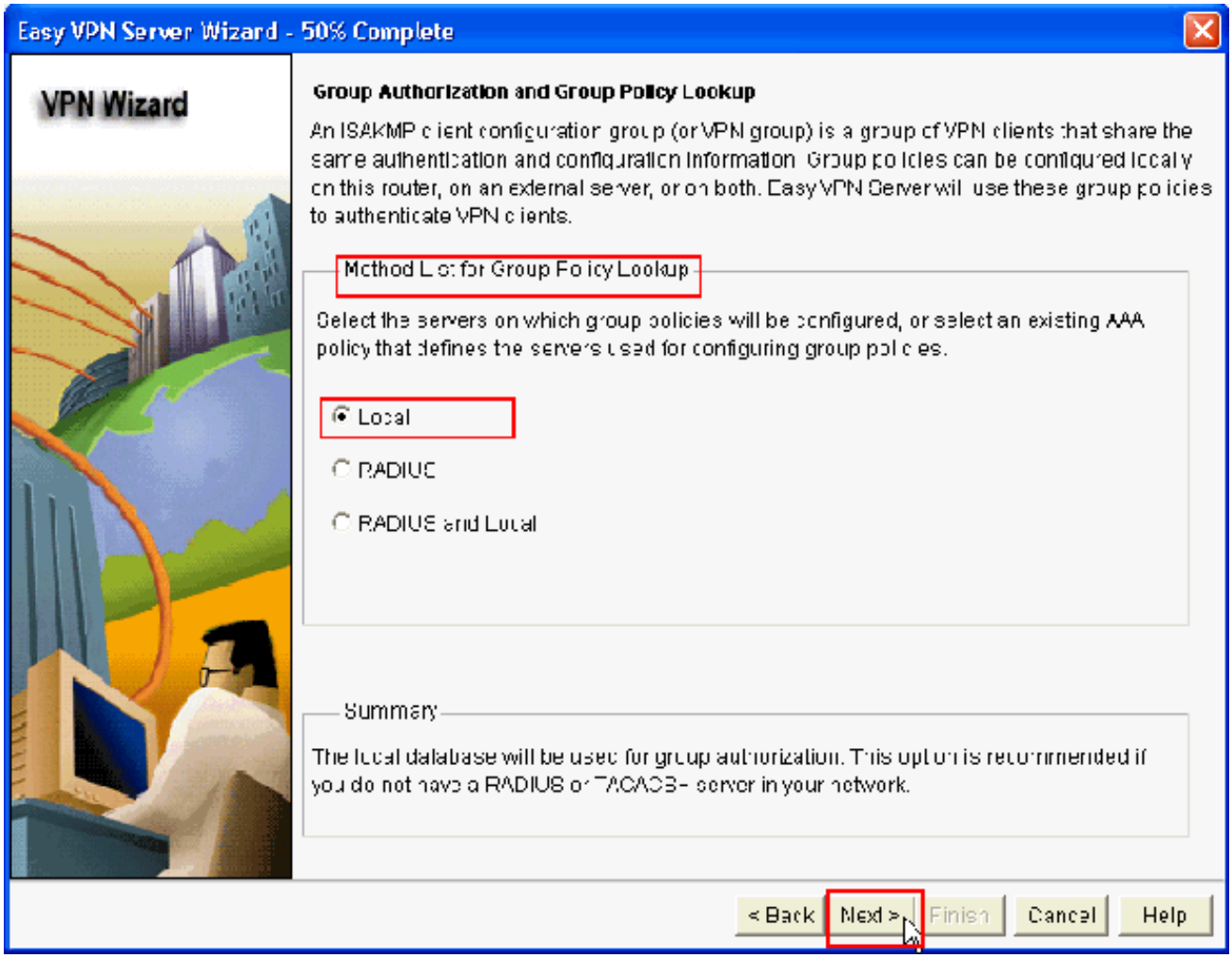
8. Forneça os detalhes **ajustados da transformação** (**criptografia e algoritmo de autenticação**) e clique a APROVAÇÃO.



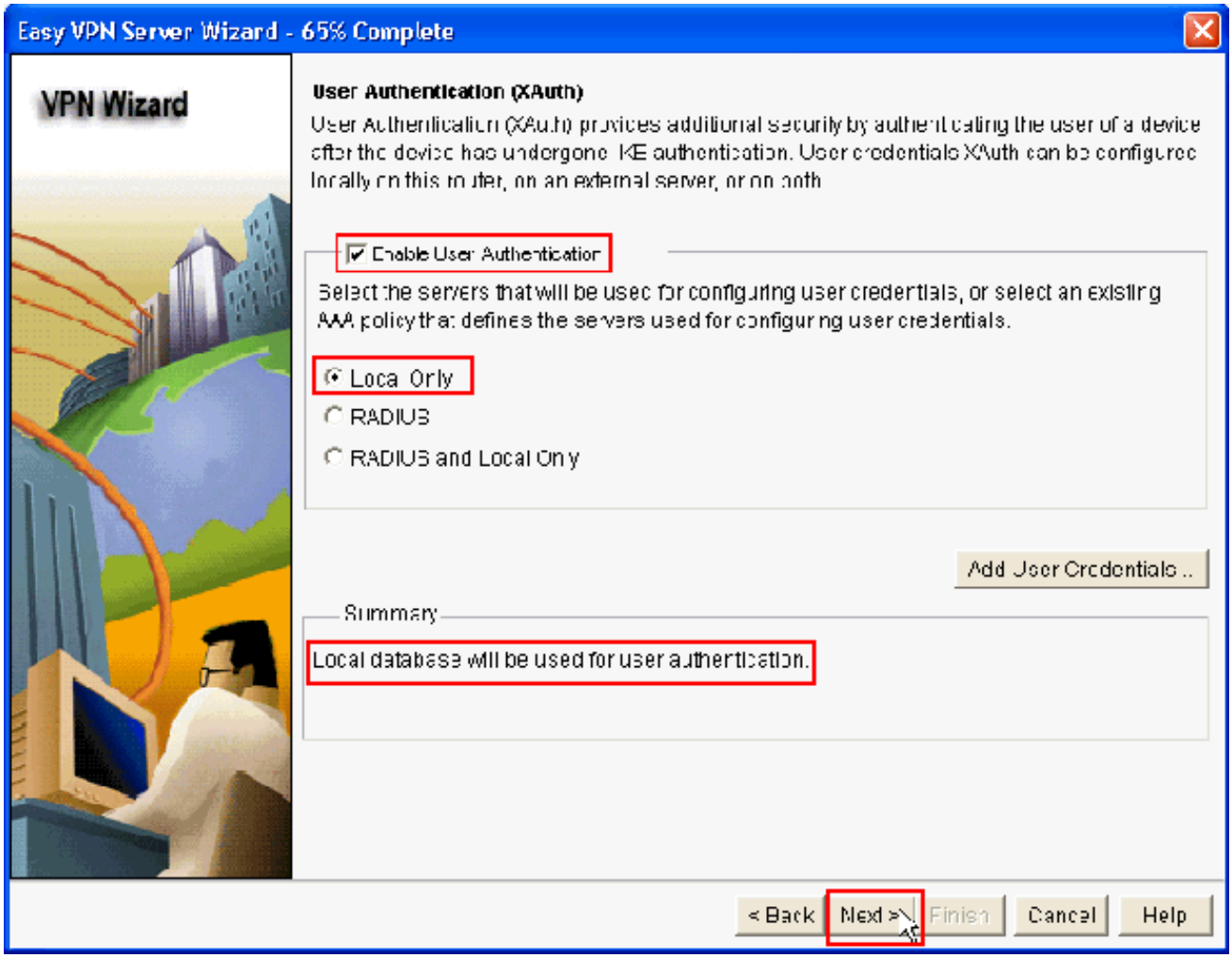
9. **O padrão transforma o padrão** nomeado **grupo CP transforma o grupo** é usado neste exemplo. Em consequência, escolha o padrão transformam o grupo e clicam-no **em seguida**.



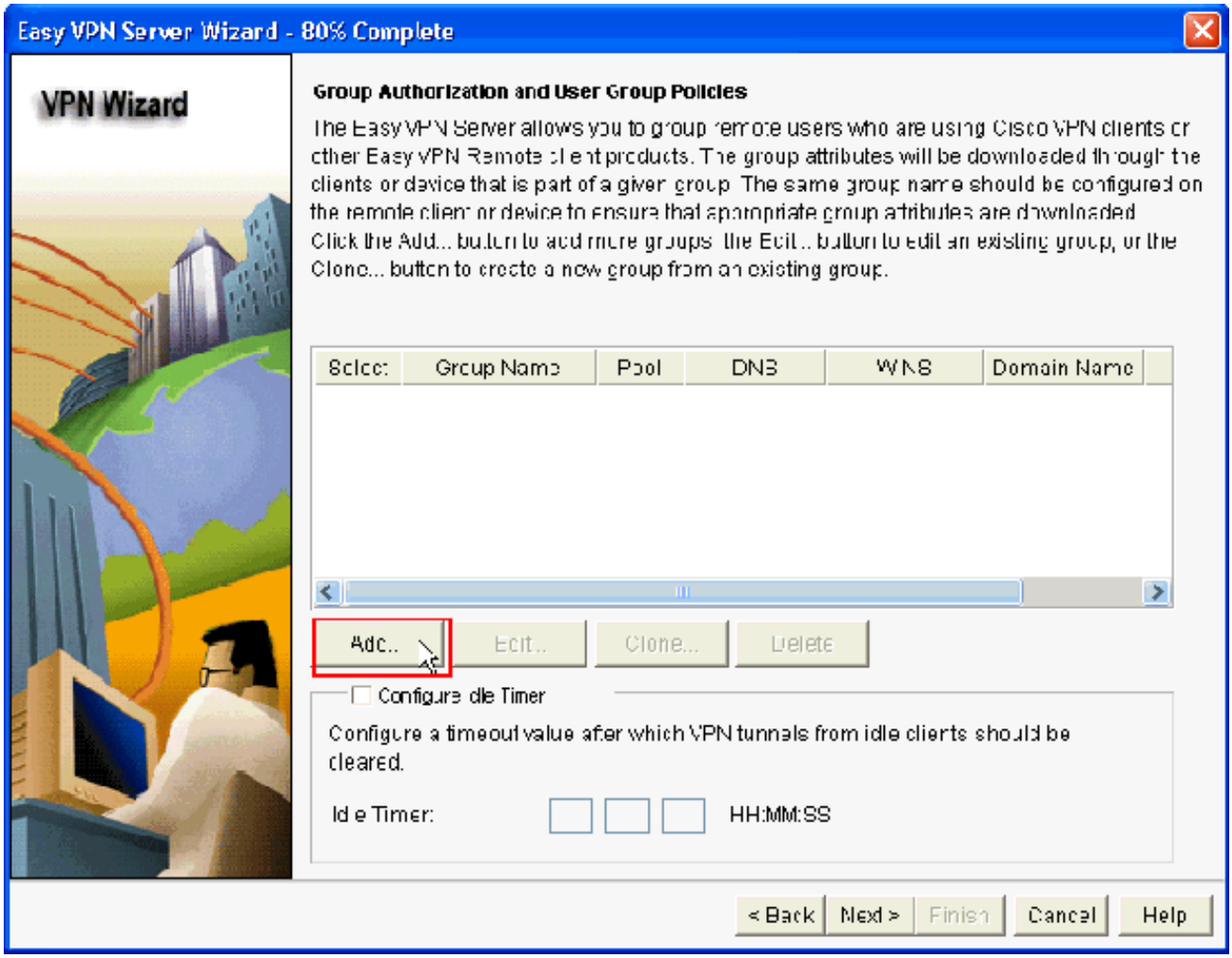
10. Na nova janela, escolha o server em que as políticas do grupo serão configuradas que podem ser **Local** ou **RAIO** ou **Local e RAIO**. Neste exemplo, nós usamos o **servidor local** para configurar políticas do grupo. Escolha o **Local** e clique-o **em seguida**.



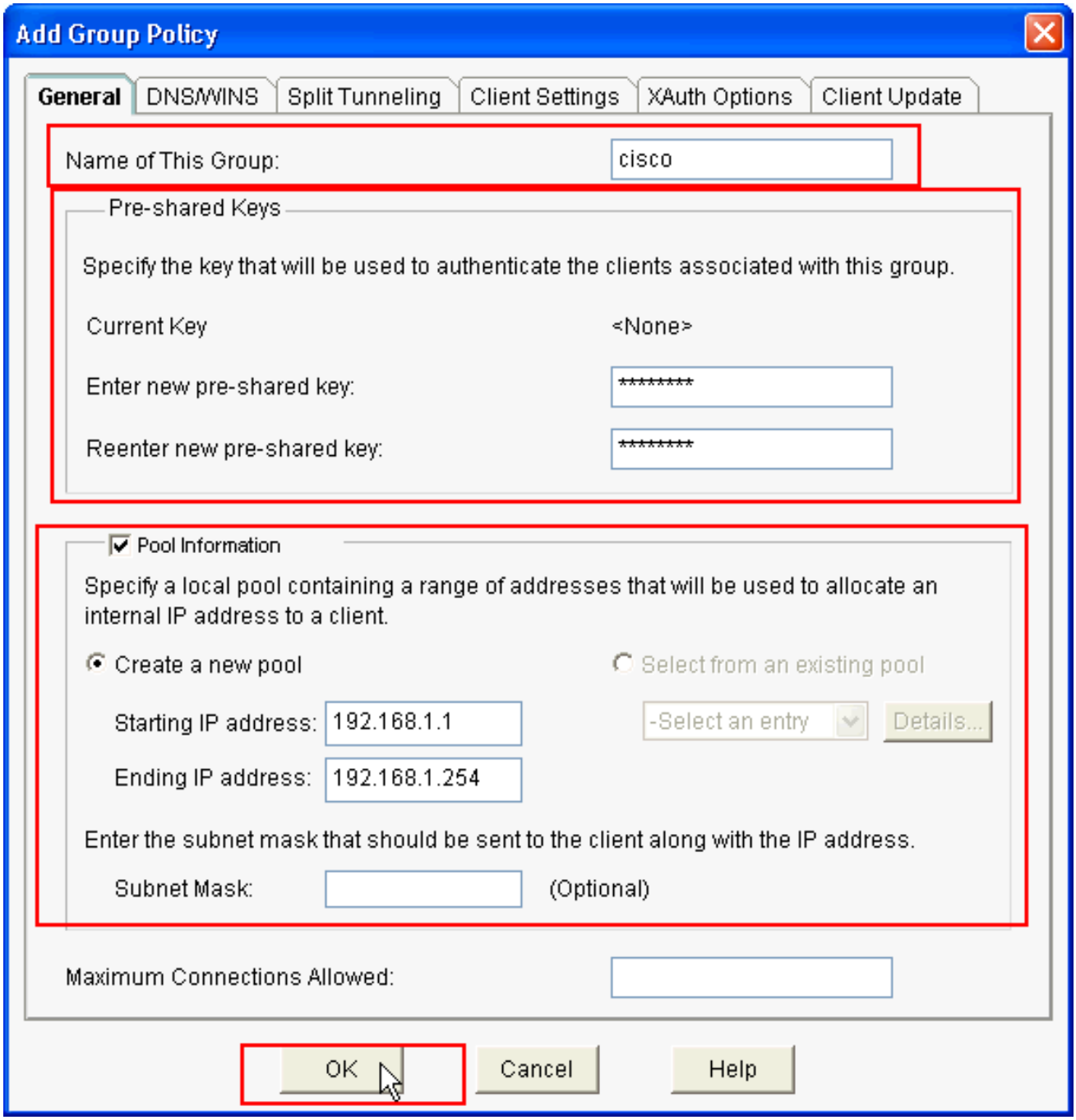
11. Escolha o server a ser usado para a autenticação de usuário nesta nova janela que pode ser **Local somente** ou **RAIO** ou **Local somente e RAIO**. Neste exemplo nós usamos o **servidor local** para configurar credenciais do usuário para a autenticação. Certifique-se que a caixa de verificação ao lado de **para permitir a autenticação de usuário** está verificada. Escolha o **Local somente** e clique-o **em seguida**.



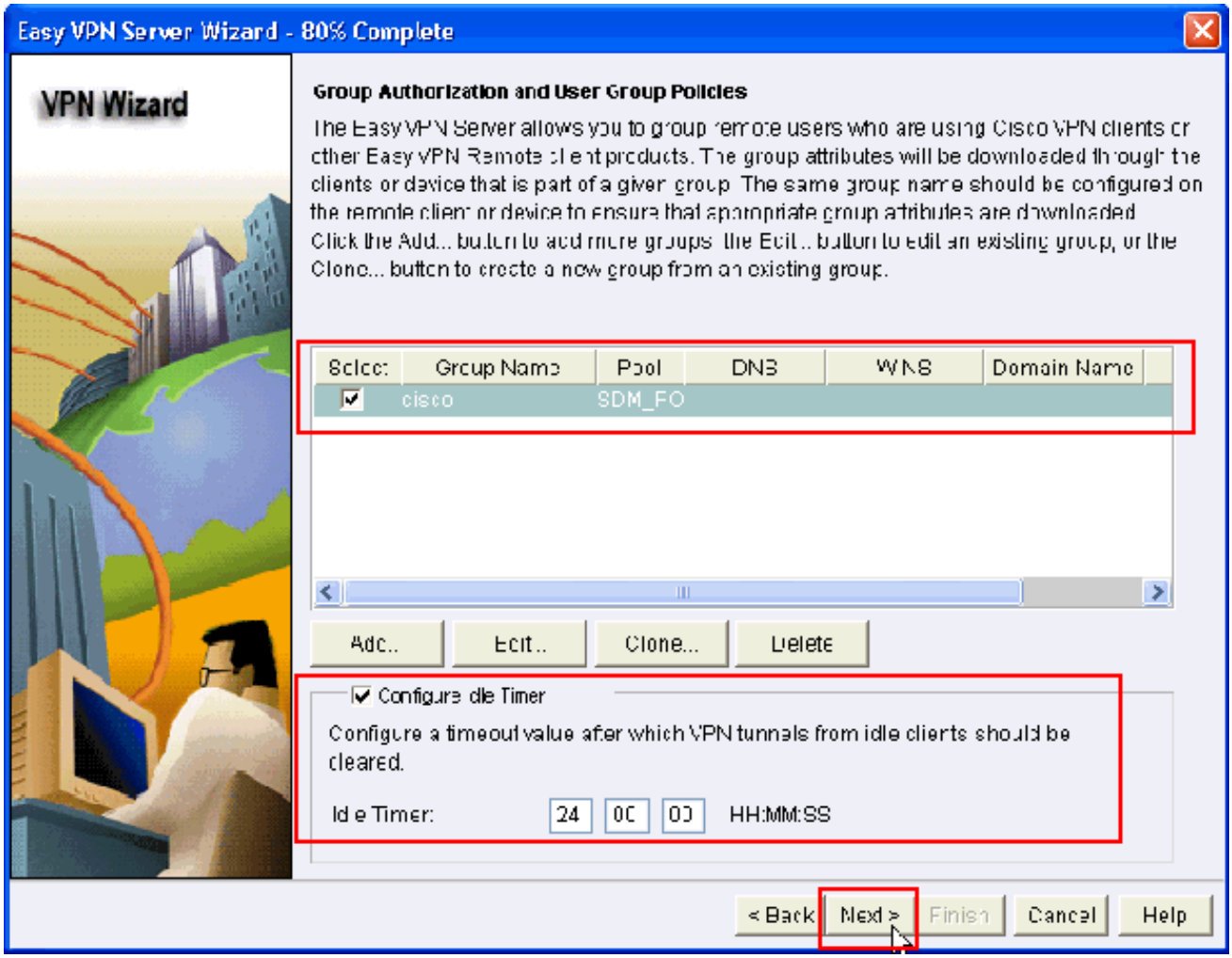
12. O clique **adiciona** para criar uma política nova do grupo e para adicionar os usuários remotos neste
grupo.



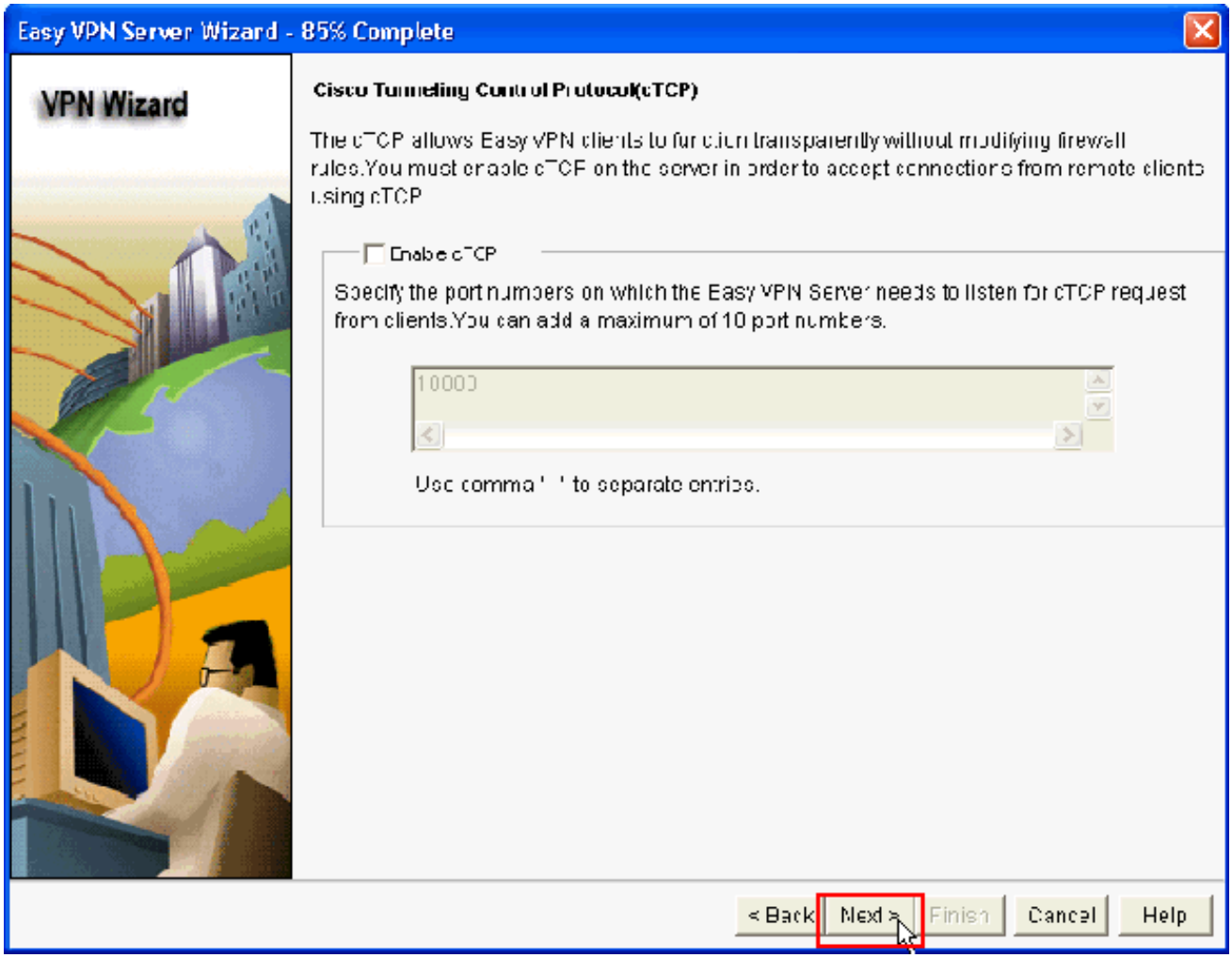
13. **Na janela de política do grupo adicionar**, forneça o nome do grupo no espaço preveem o **nome deste grupo** (**Cisco** neste exemplo) junto com a **chave pré-compartilhada**, e a informação do **IP pool** (o **endereço IP de Um ou Mais Servidores Cisco ICM NT começando** e **endereço IP de Um ou Mais Servidores Cisco ICM NT do término**) como mostrado e a **APROVAÇÃO do** clique.**Nota:** Você pode criar um IP pool novo ou usar um IP pool existente se
presente.



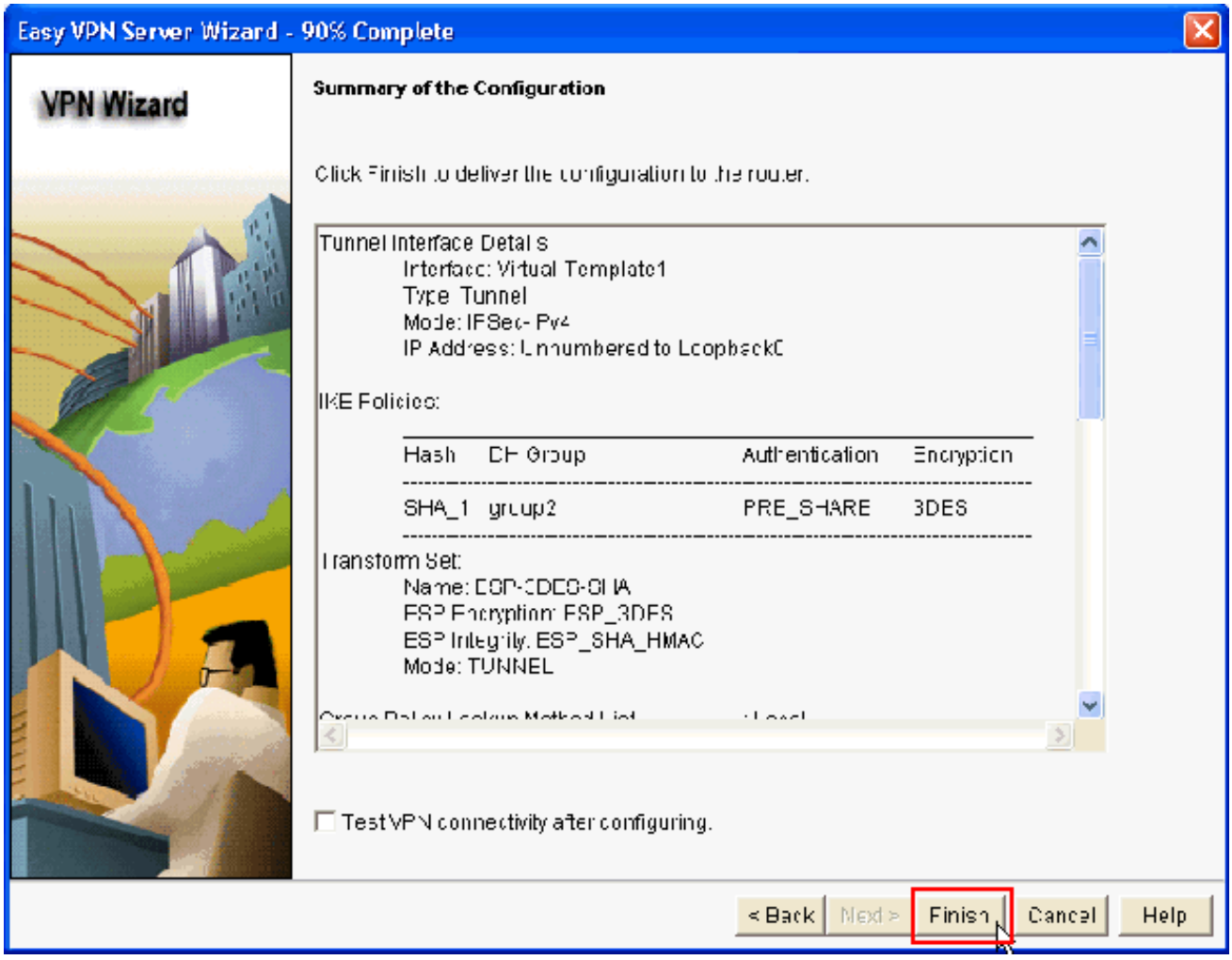
14. Escolha agora a **política** nova do **grupo** criada com o nome **Cisco** e clique então a caixa de verificação ao lado do **configuram o temporizador de ociosidade** como exigido na ordem para configurar o **temporizador de ociosidade**. Clique em
Next.



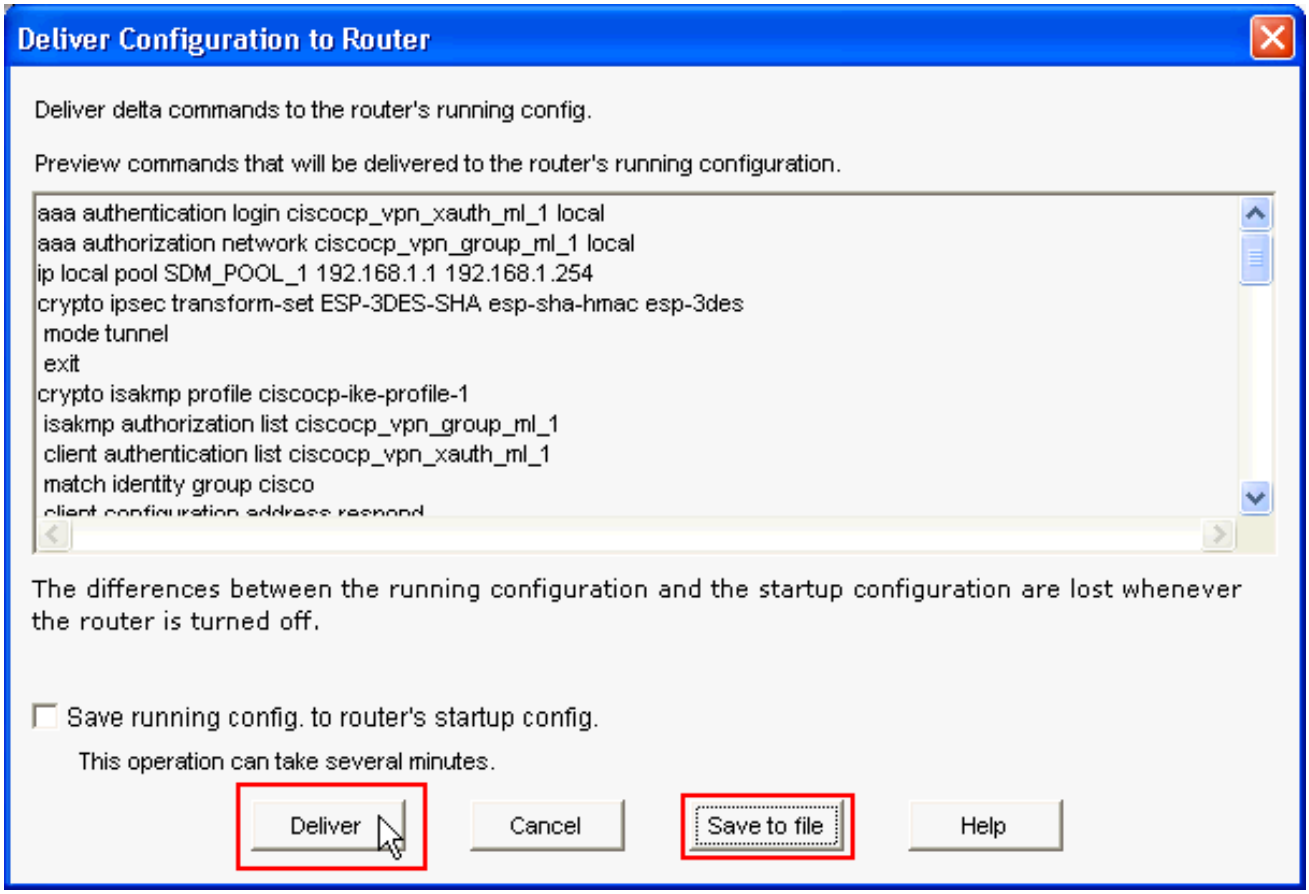
15. Permita **Cisco que escava um túnel o protocolo de controle** (cTCP) se for necessário. Se não, clique **em seguida**.



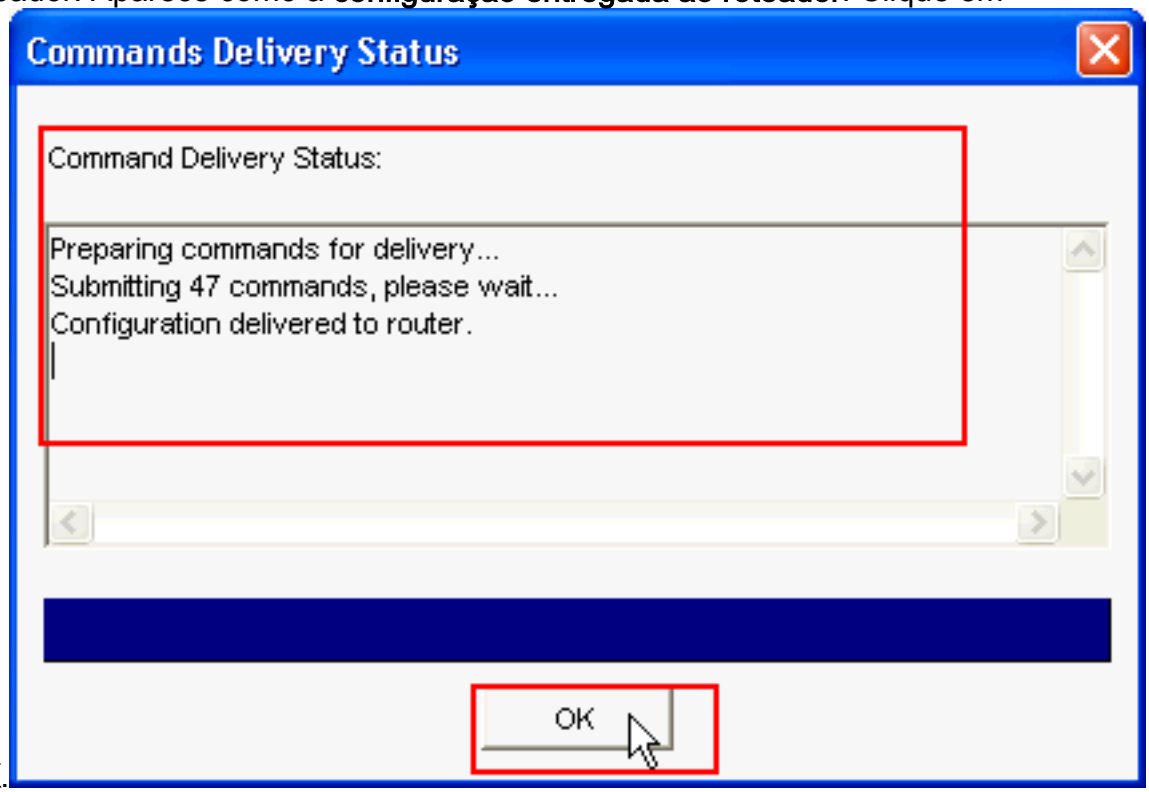
16. Reveja o **sumário da configuração**. Clique em Finish.



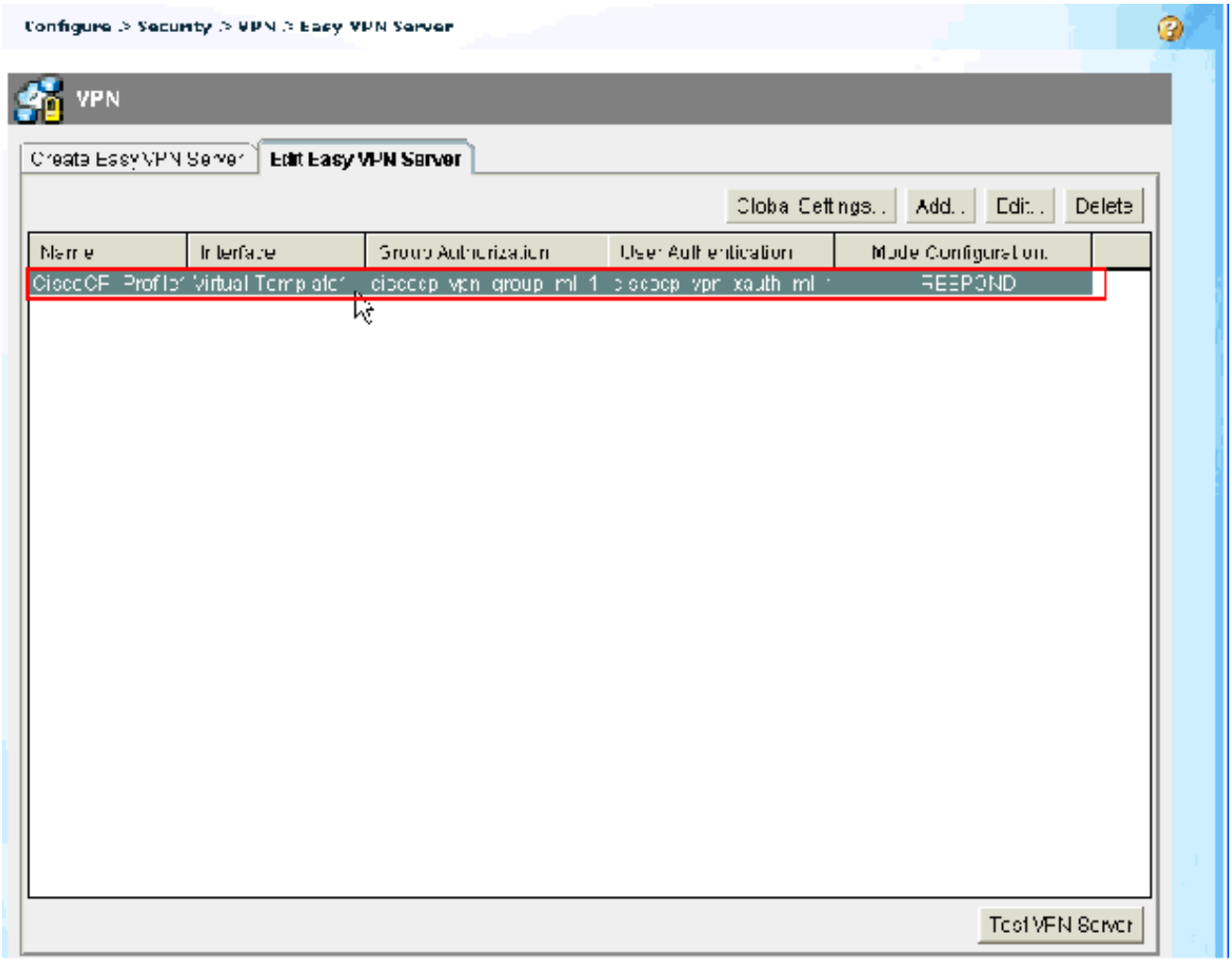
17. **Na configuração do fornecimento à janela de roteador**, o clique **entrega** para entregar a configuração ao roteador. Você pode clicar sobre a **salvaguarda para arquivar** para salvar a configuração como um arquivo no
PC.



18. **A janela de status da entrega do comando** mostra o estado da entrega dos comandos ao roteador. Aparece como a **configuração entregada ao roteador**. Clique em **OK**.



19. Você pode ver o Easy VPN Server recém-criado. Você pode editar o servidor existente escolhendo **edita o Easy VPN Server**. Isto termina a configuração do Easy VPN Server no roteador do Cisco
IOS.



Configuração de CLI

Configuração do roteador
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
```

Verificar

Easy VPN Server - comandos show

Use esta seção para confirmar se a sua configuração funciona corretamente.

- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.`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`
- **mostre IPsec cripto sa** — Mostra todo o sas de IPSec atual em um par.`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`

Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Debugação antes de usar comandos **debug**.

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Guia de início rápido do Cisco Configuration Professional
- Página de suporte dos produtos da Cisco - Roteadores
- Suporte Técnico e Documentação - Cisco Systems