

# Roteador Cisco como um servidor de VPN remoto usando o exemplo da configuração de SDM

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Procedimento de configuração](#)

[Verificar](#)

[Informações Relacionadas](#)

## Introdução

[Este documento descreve como usar o Cisco Security Device Manager \(SDM\) para configurar um roteador cisco para atuar como um Easy VPN Server.](#) O Cisco SDM permite que você configure seu roteador como um servidor de VPN para o Cisco VPN Client usando uma interface de gerenciamento com base na web fácil de usar. Quando a configuração do roteador Cisco estiver completa, ela poderá ser verificada utilizando um Cisco VPN Client.

## Pré-requisitos

### Requisitos

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

**Nota:** Refira [permitir o acesso HTTPS para o SDM](#) a fim permitir que o roteador seja configurado pelo SDM.

### Componentes Utilizados

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

- Cisco 3640 Router com Software Release 12.3(14T) de Cisco IOS®
- Versão 2.31 do Security Device Manager

- Versão Cliente VPN Cisco 4.8

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.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

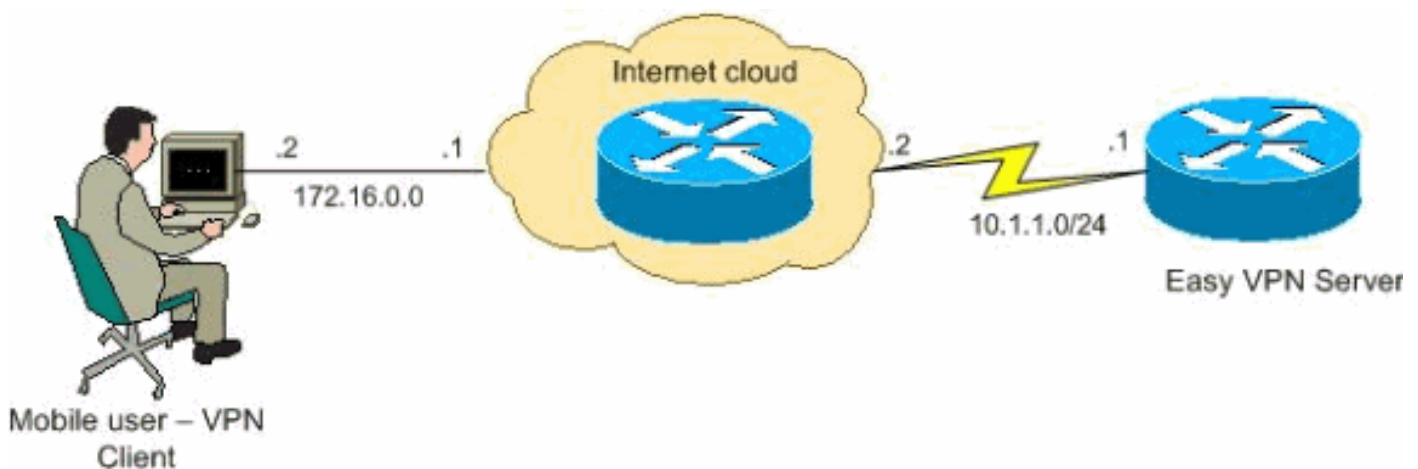
## Configurar

Nesta seção, você é apresentado com a informação para configurar a característica do Easy VPN Server que permite que um utilizador final remoto se comunique usando o IPsec com todo o gateway de VPN de Cisco IOS®.

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

## Diagrama de Rede

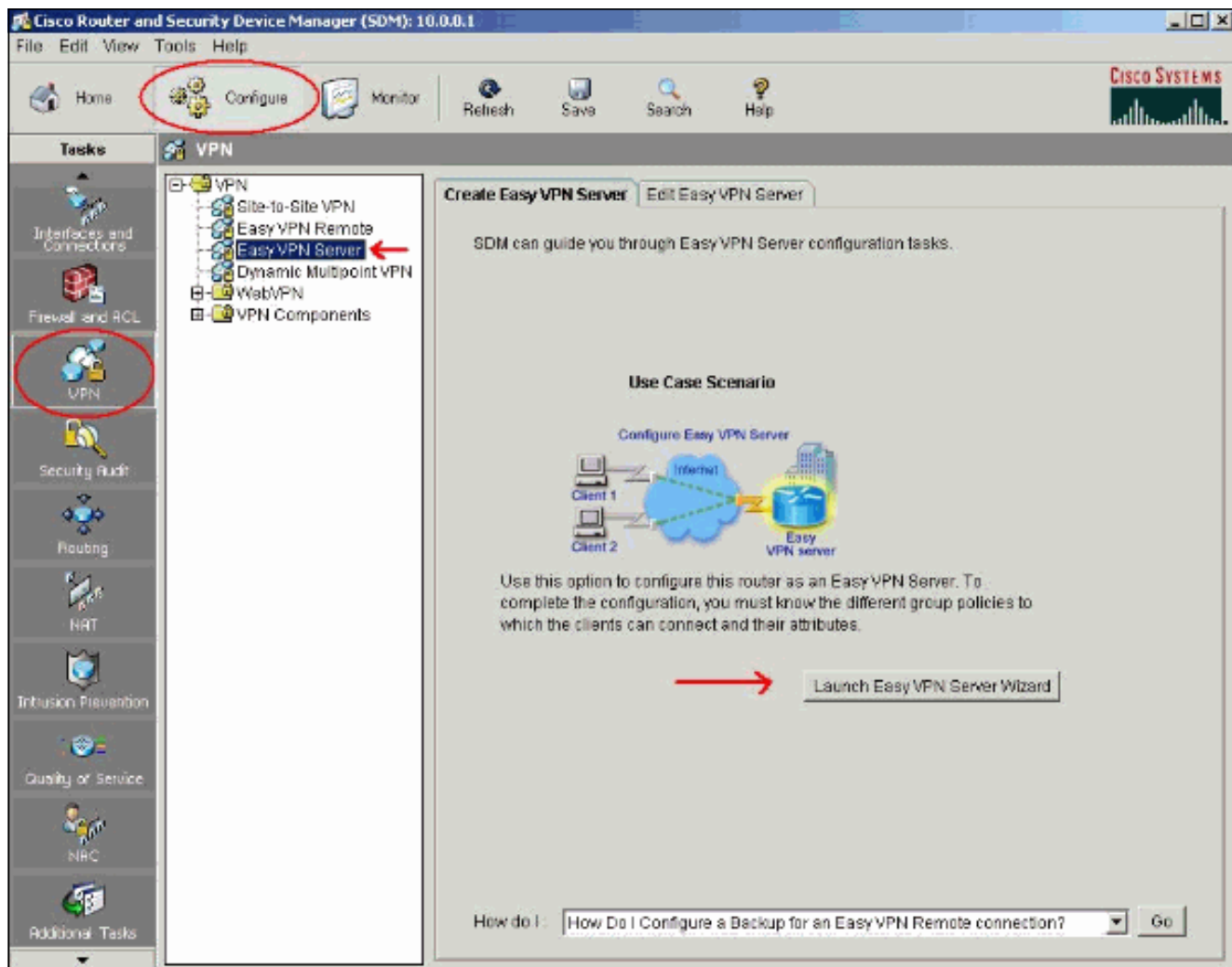
Este documento utiliza a seguinte configuração de rede:



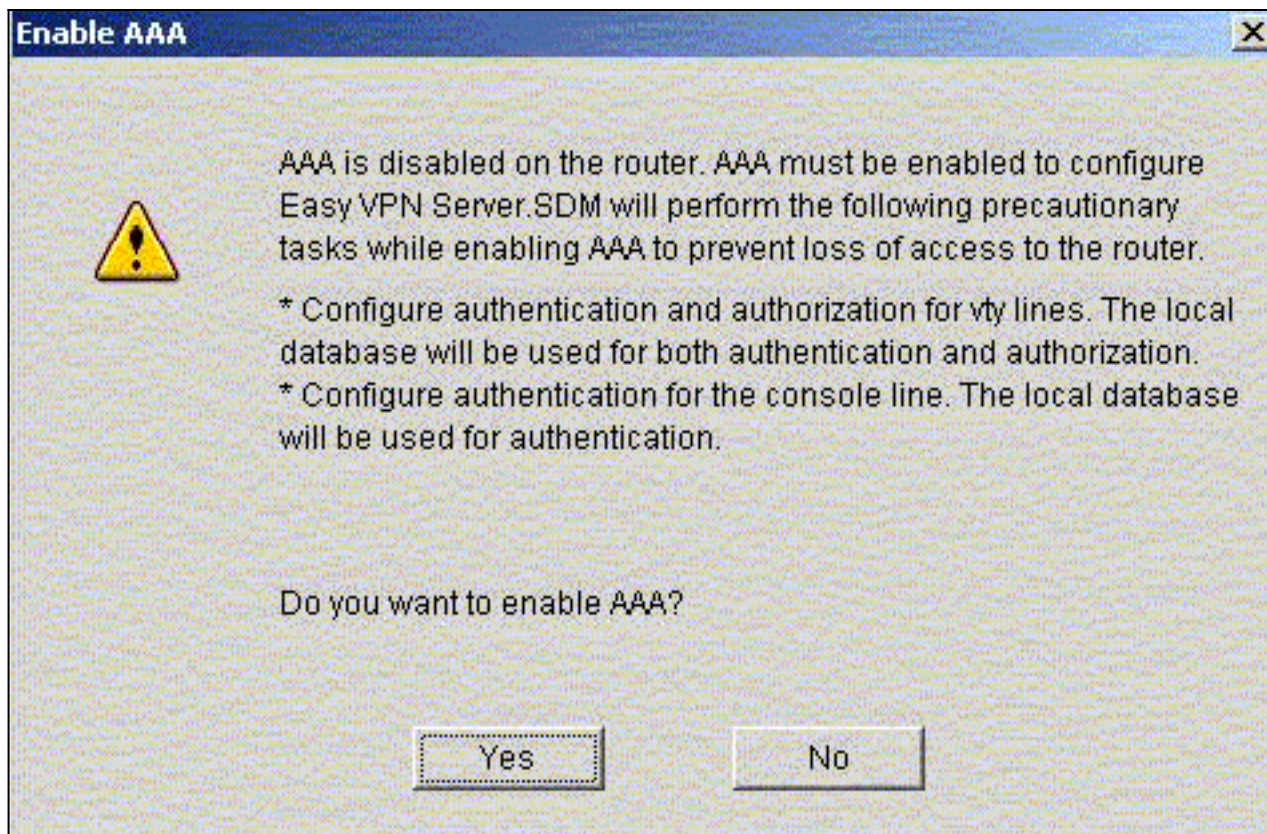
## Procedimento de configuração

Termine estas etapas para configurar o roteador Cisco como um servidor de VPN remoto usando o SDM.

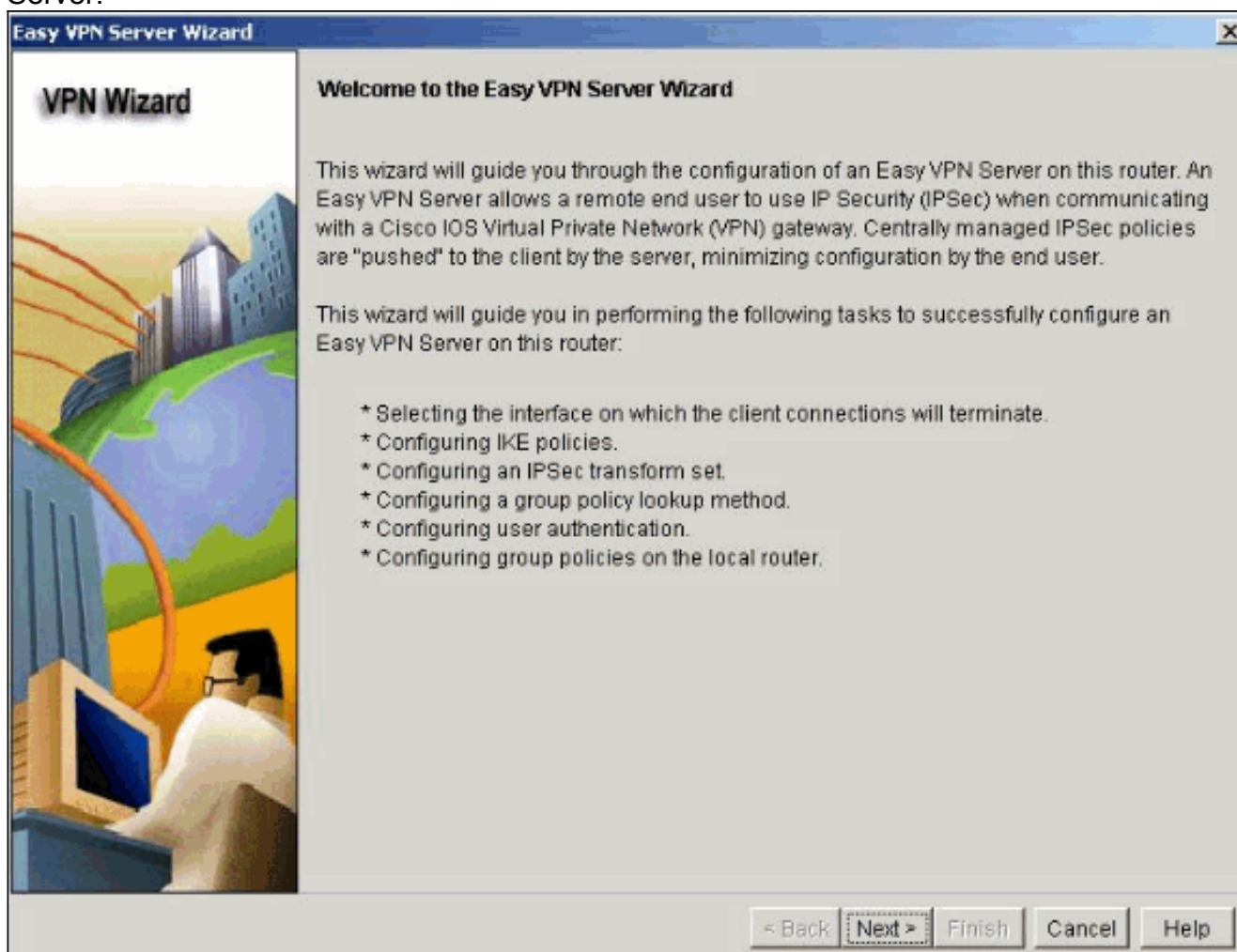
1. Seletor **configurar > VPN > Easy VPN Server** do indicador home e clique o **assistente do Easy VPN Server** do lançamento.



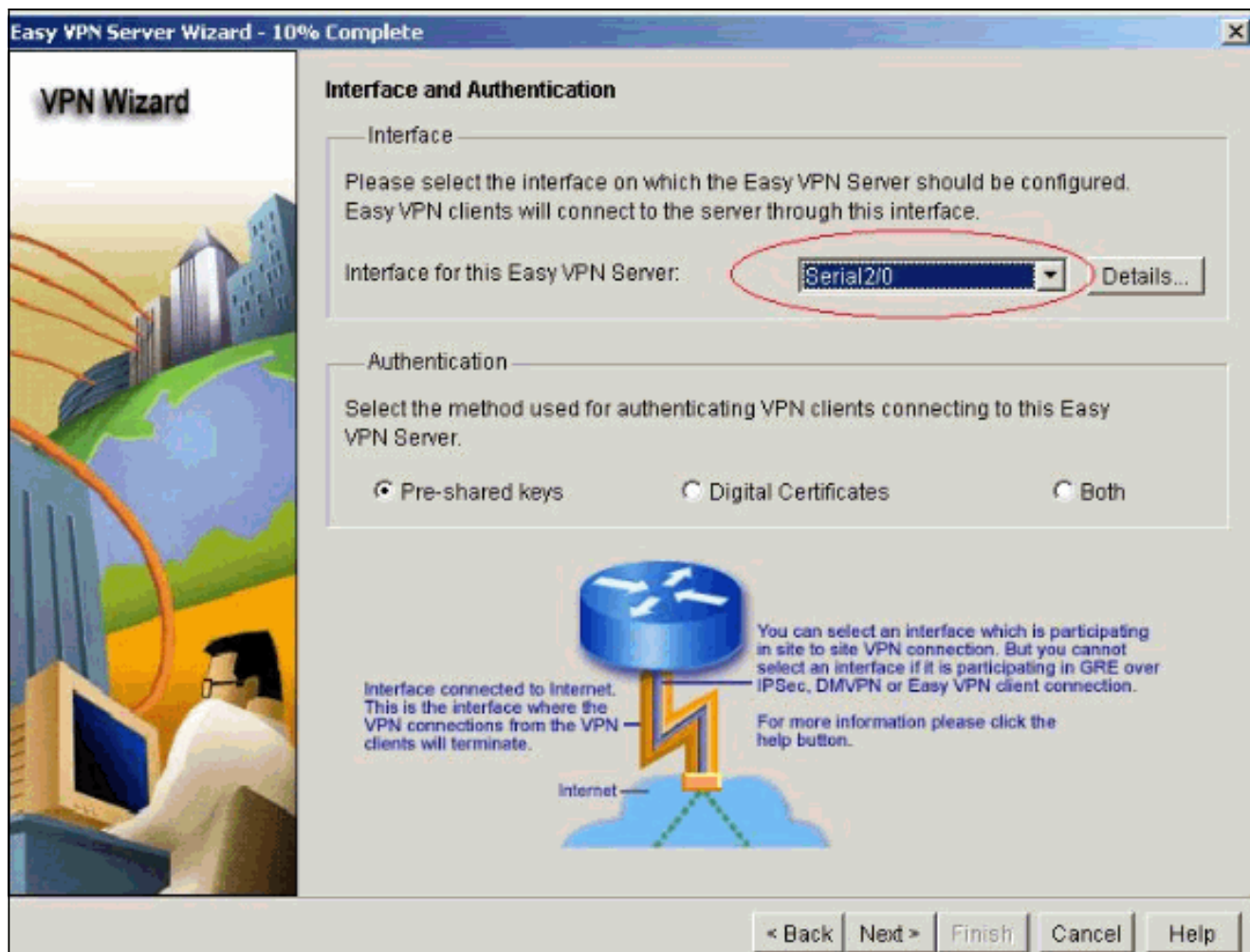
2. O AAA deve ser permitido no roteador antes que a configuração do Easy VPN Server comece. Clique **sim** para continuar com a configuração. O “AAA foi permitido com sucesso as exibições de mensagem no roteador” no indicador. **APROVAÇÃO** do clique para começar a configuração do Easy VPN Server.



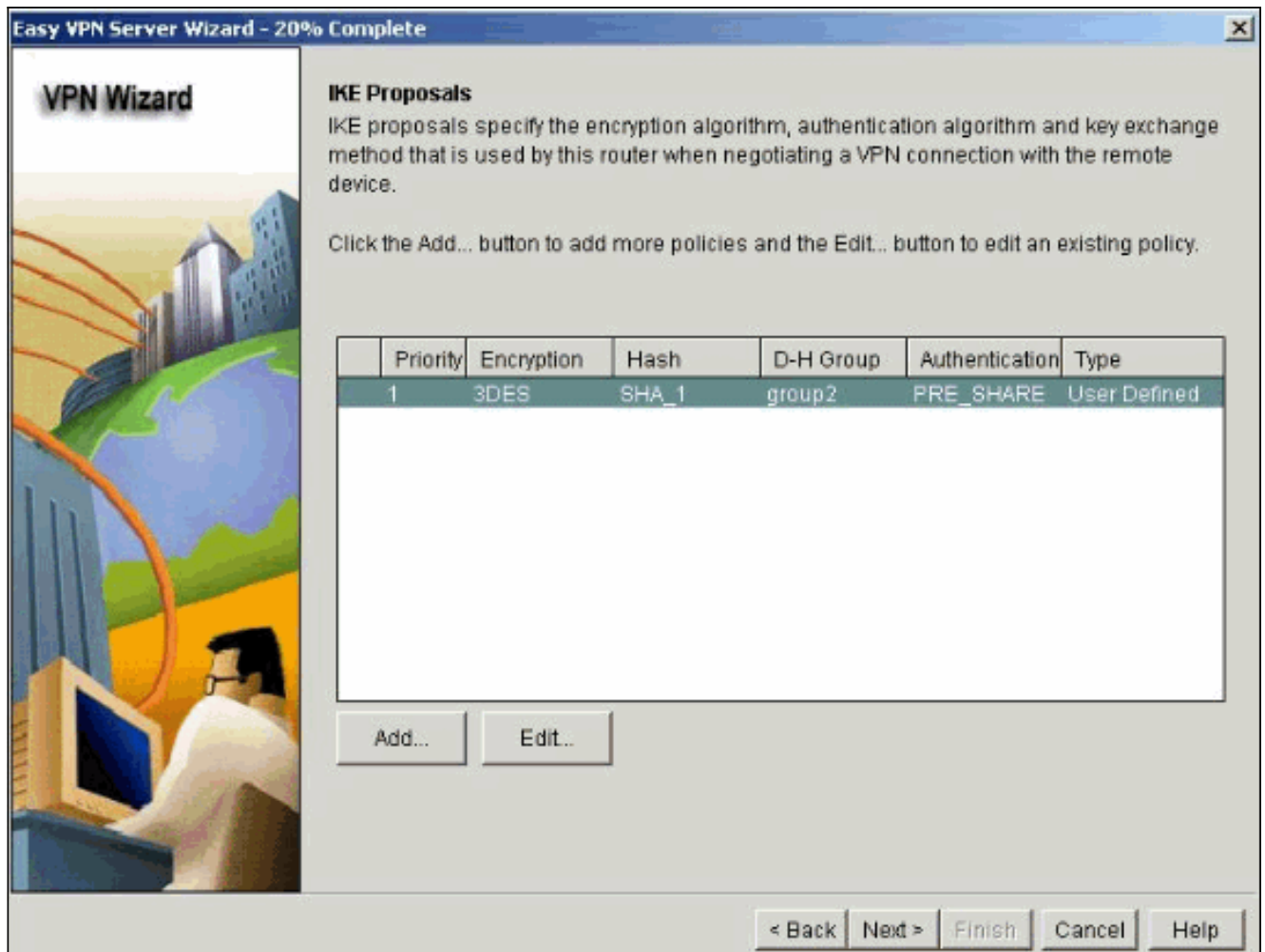
3. Clique ao lado do começo o assistente do Easy VPN Server.



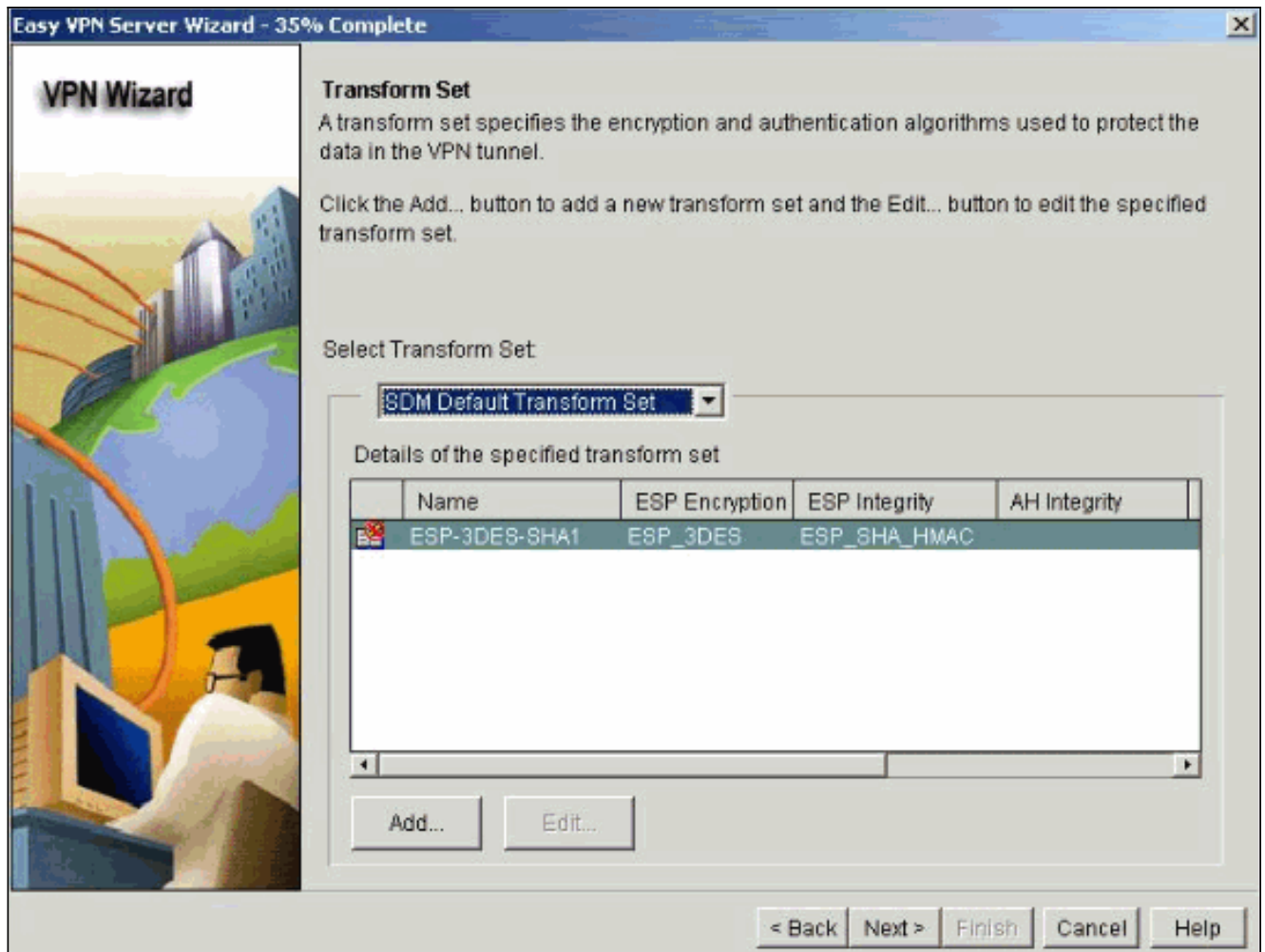
4. Selecione a relação em que as conexões de cliente terminam e o tipo do autenticação.



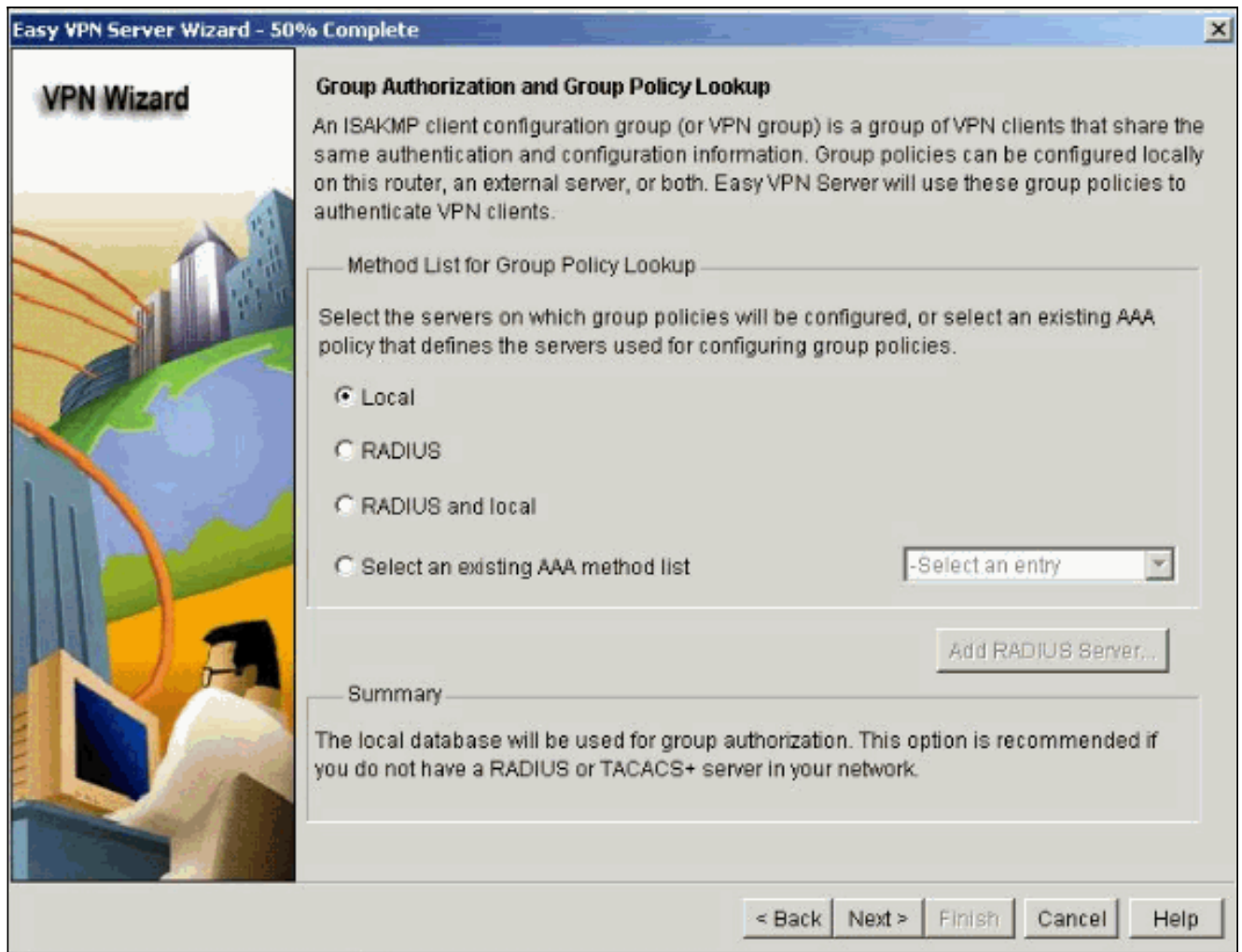
5. O clique ao lado de configura as políticas do Internet Key Exchange (IKE) e usa o botão Add para criar a política nova. As configurações em ambos os lados do túnel devem combinar exatamente. Contudo, o Cisco VPN Client seleciona automaticamente a configuração apropriada para se. Consequentemente, nenhuma configuração de IKE é necessária no PC cliente.



6. O clique ao lado de escolhe o padrão transforma o grupo ou adiciona o novo transforma o grupo para especificar a criptografia e o algoritmo de autenticação. Neste caso, o padrão transforma o grupo é usado.

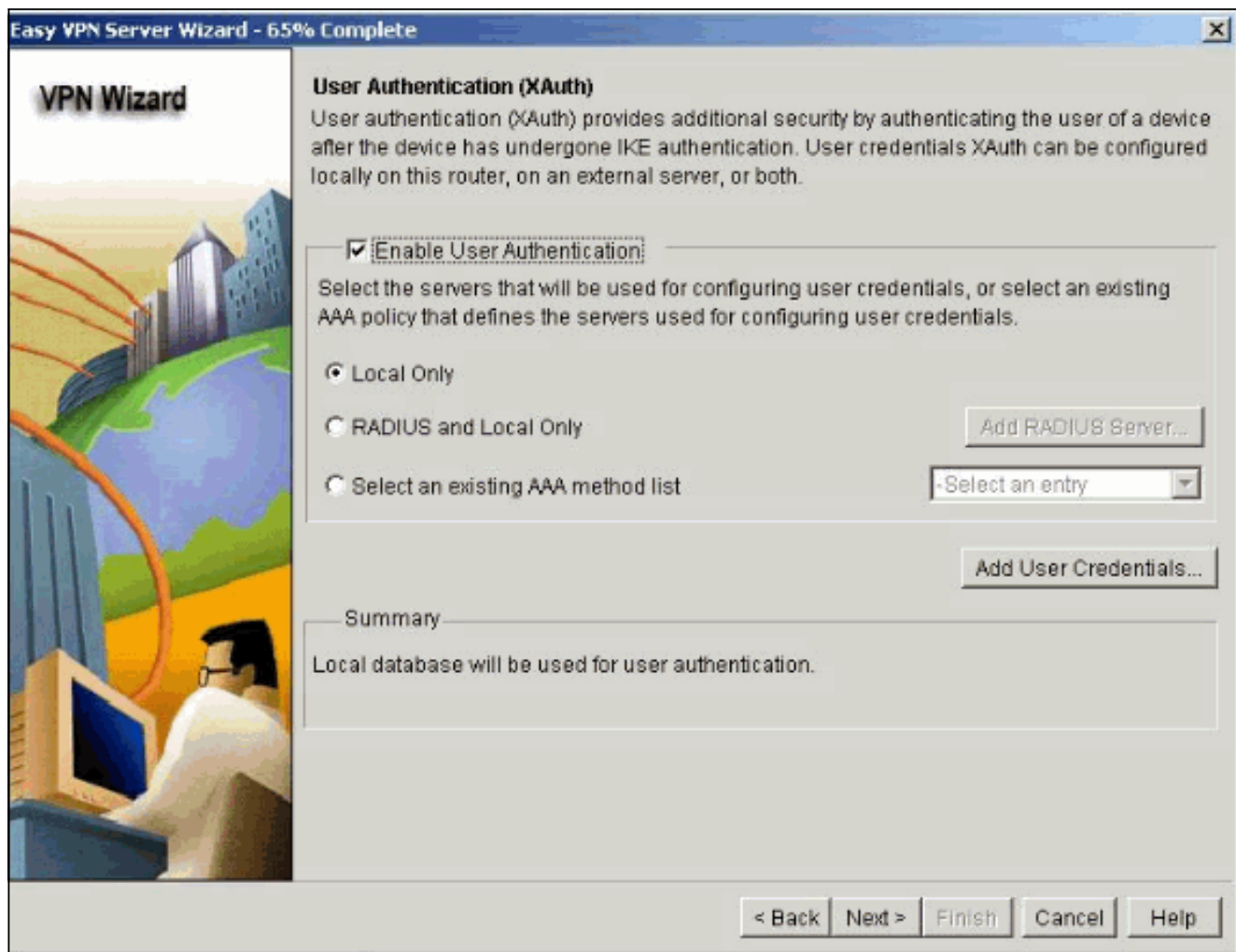


7. O clique ao lado de cria uma lista de método nova da rede da autorização do Authentication, Authorization, and Accounting (AAA) para a consulta da política do grupo ou para escolher uma lista de método da rede existente usada para a autorização do grupo.

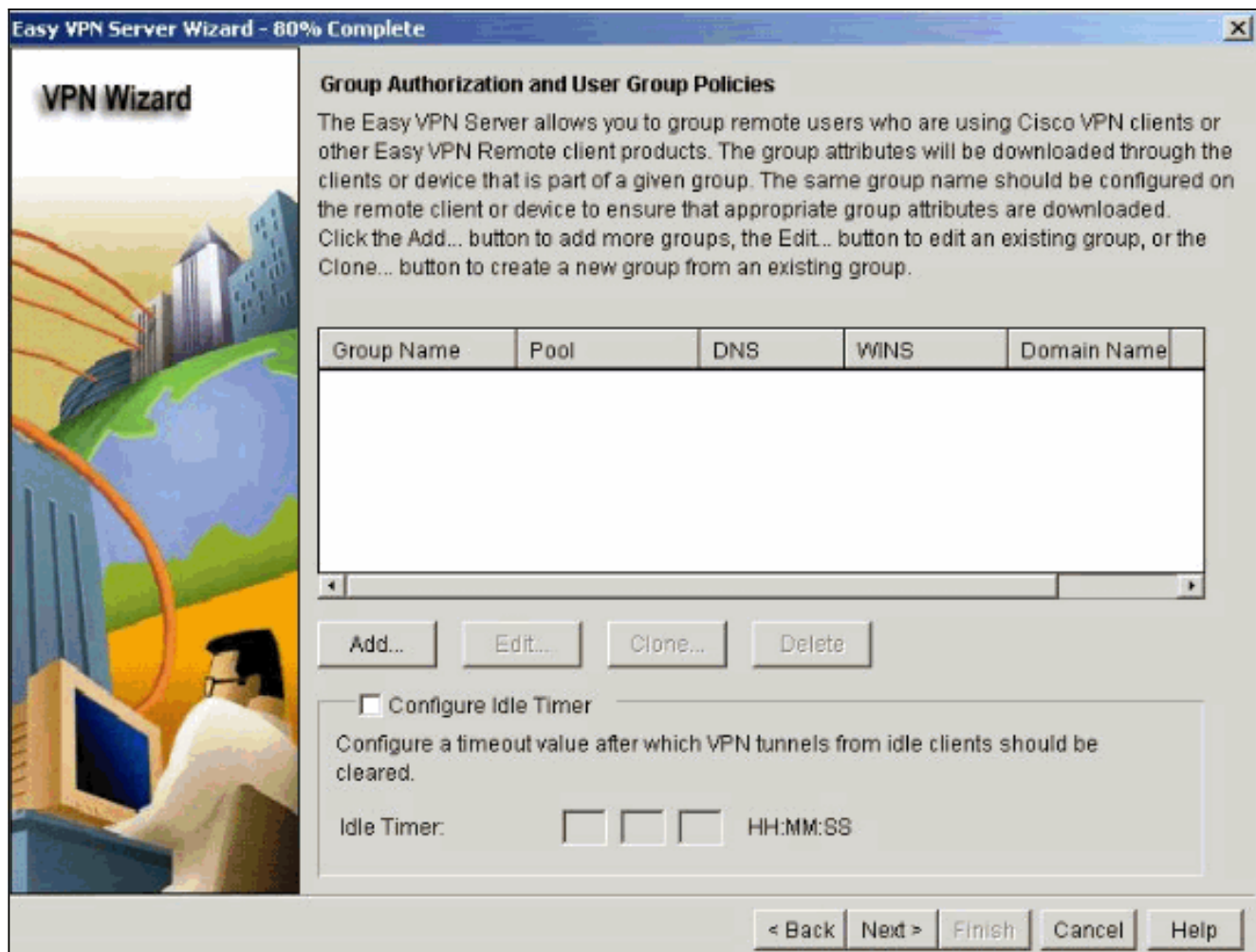


8. Configurar a autenticação de usuário no Easy VPN Server. Você pode armazenar detalhes da autenticação de usuário em um servidor interno tal como um servidor Radius ou um base de dados local ou em ambos. Uma lista de método da autenticação de login AAA é usada para decidir a ordem em que os detalhes da autenticação de usuário devem ser procurados.





9. Este indicador permite que você adicione, edite, clone, ou suprima de políticas do grupo de usuário no base de dados local.



10. Dê entrada com um nome para o nome de grupo de túneis. Forneça a chave pré-compartilhada usada para a informação da autenticação. Crie um pool novo ou selecione um pool existente usado para atribuir os endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN.

**Add Group Policy**

**General** | DNSWINS | Split Tunneling | Client Settings | XAuth Options

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:

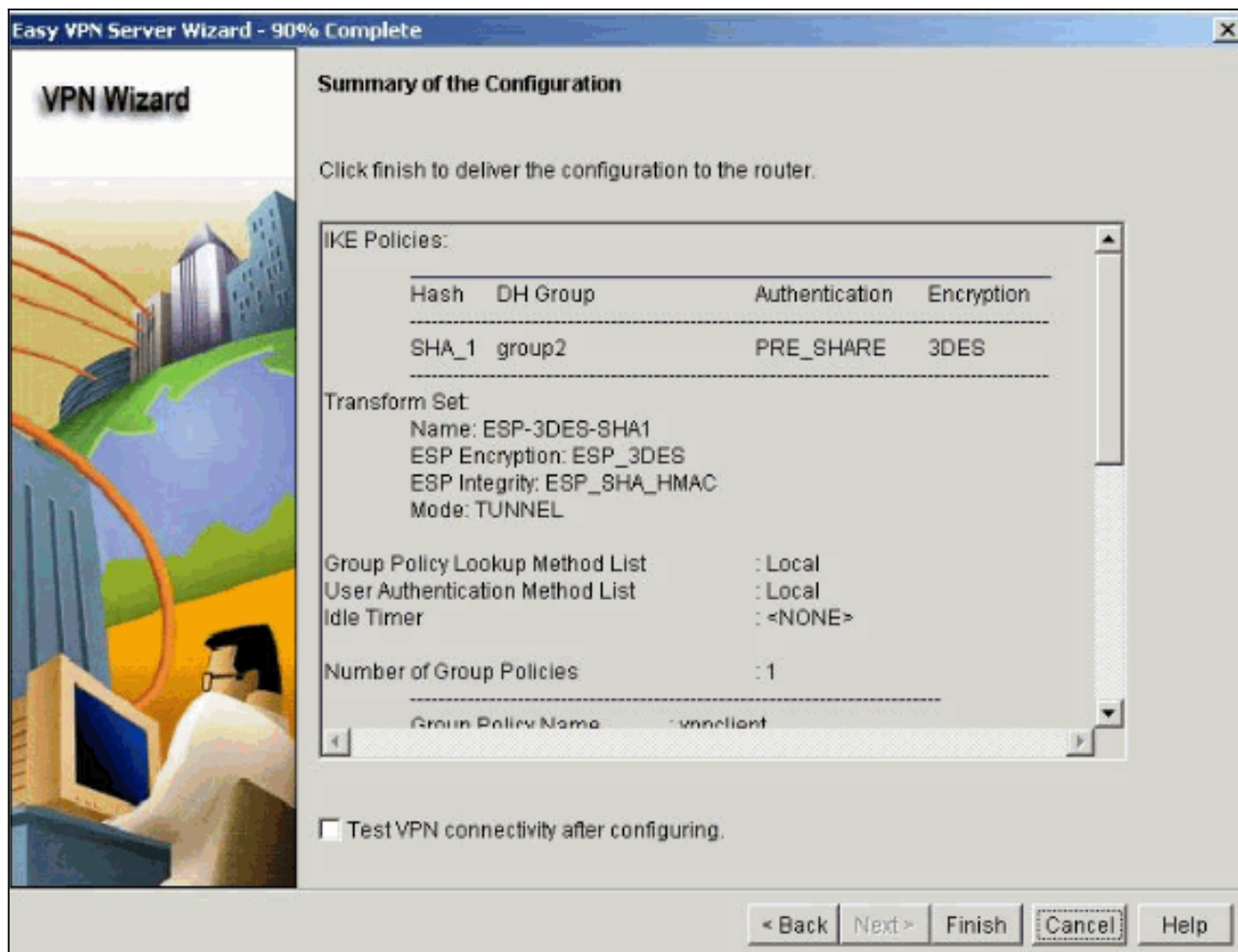
Enter the subnet mask that should be sent to the client along with the IP address.

Subnet Mask:  (Optional)

Maximum Connections Allowed:

11. Este indicador mostra um sumário das ações que você tomou. Clique o **revestimento** se você é satisfeito com sua configuração.

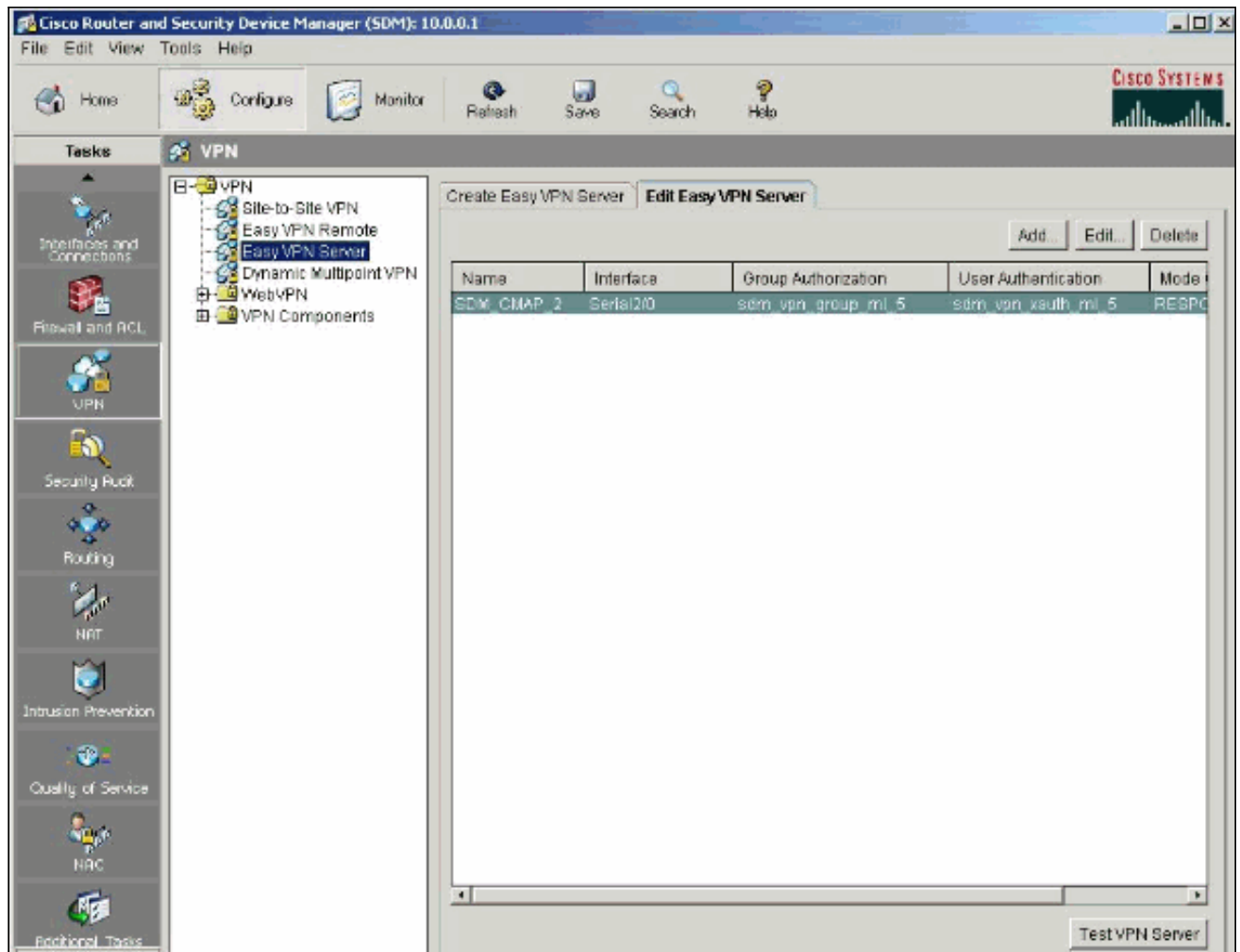


12. O SDM envia a configuração ao roteador para atualizar a configuração running.  
**APROVAÇÃO** do clique a



terminar.

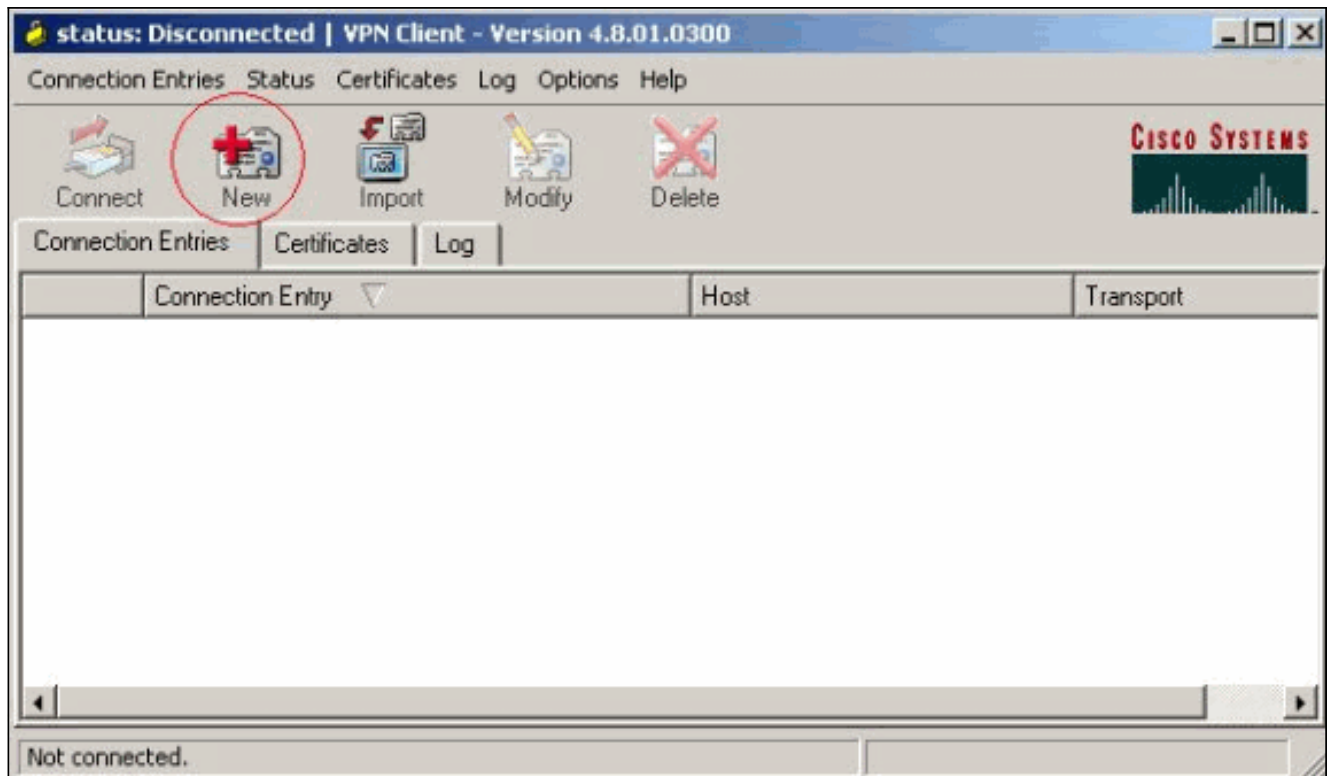
13. Após a conclusão, você pode editar e alterar as mudanças na configuração, se necessário.



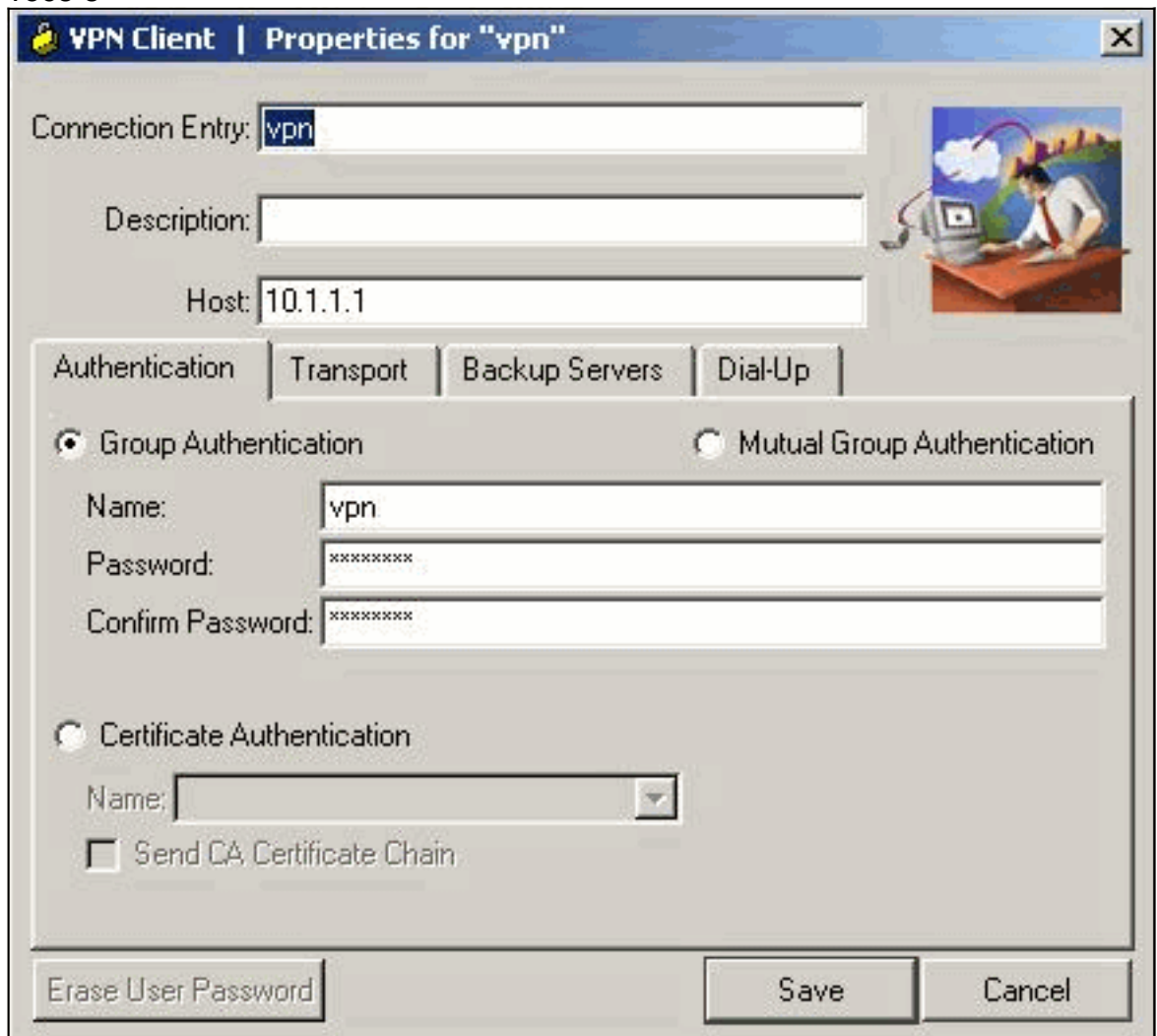
## Verificar

Tente conectar ao roteador Cisco usando o Cisco VPN Client a fim verificar que o roteador Cisco está configurado com sucesso.

1. Selecione **entradas de conexão > novo**.



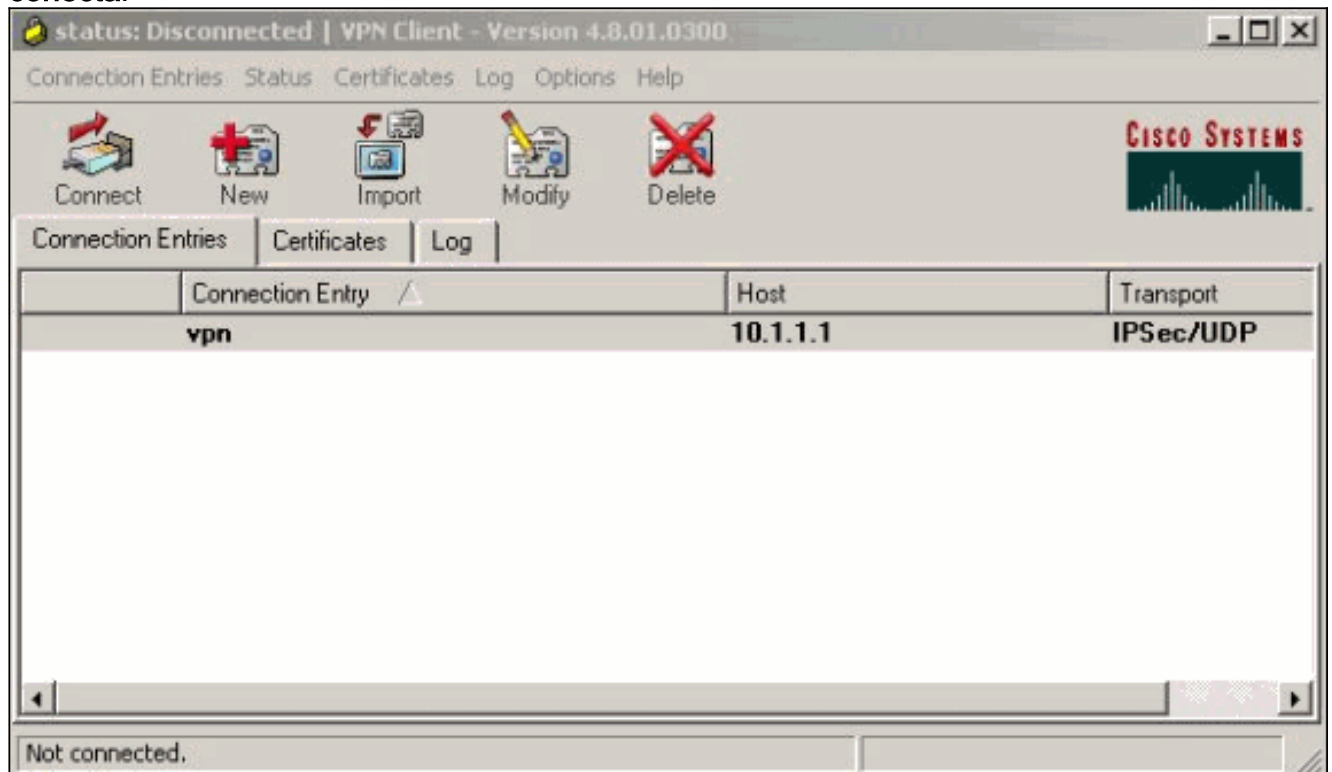
2. Preencha os detalhes de sua nova conexão. O campo do host deve conter o endereço IP ou nome do host do ponto final do túnel do Easy VPN Server (roteador Cisco). A informação da autenticação do grupo deve corresponder àquela usada na **salvaguarda** do clique de etapa 9. quando você é



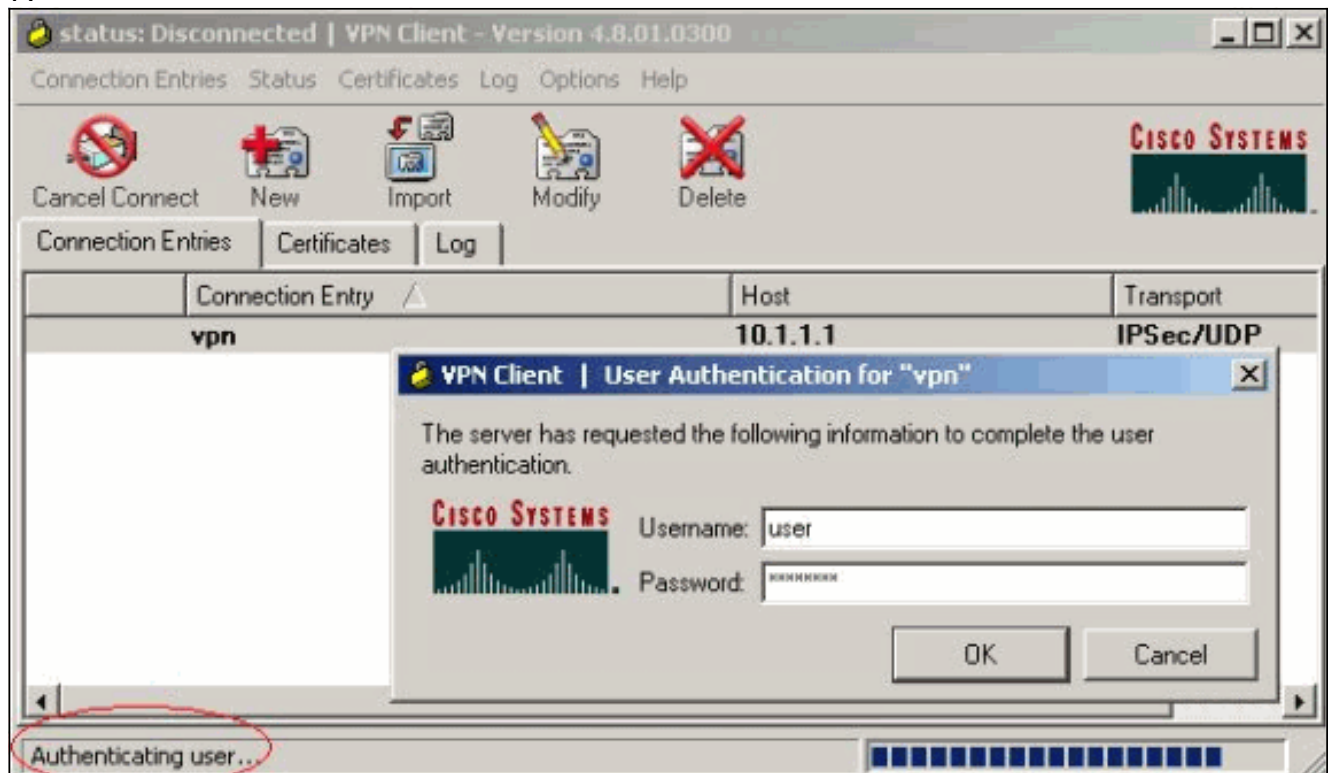
terminado.

3. Selecione a conexão recém-criado e o clique

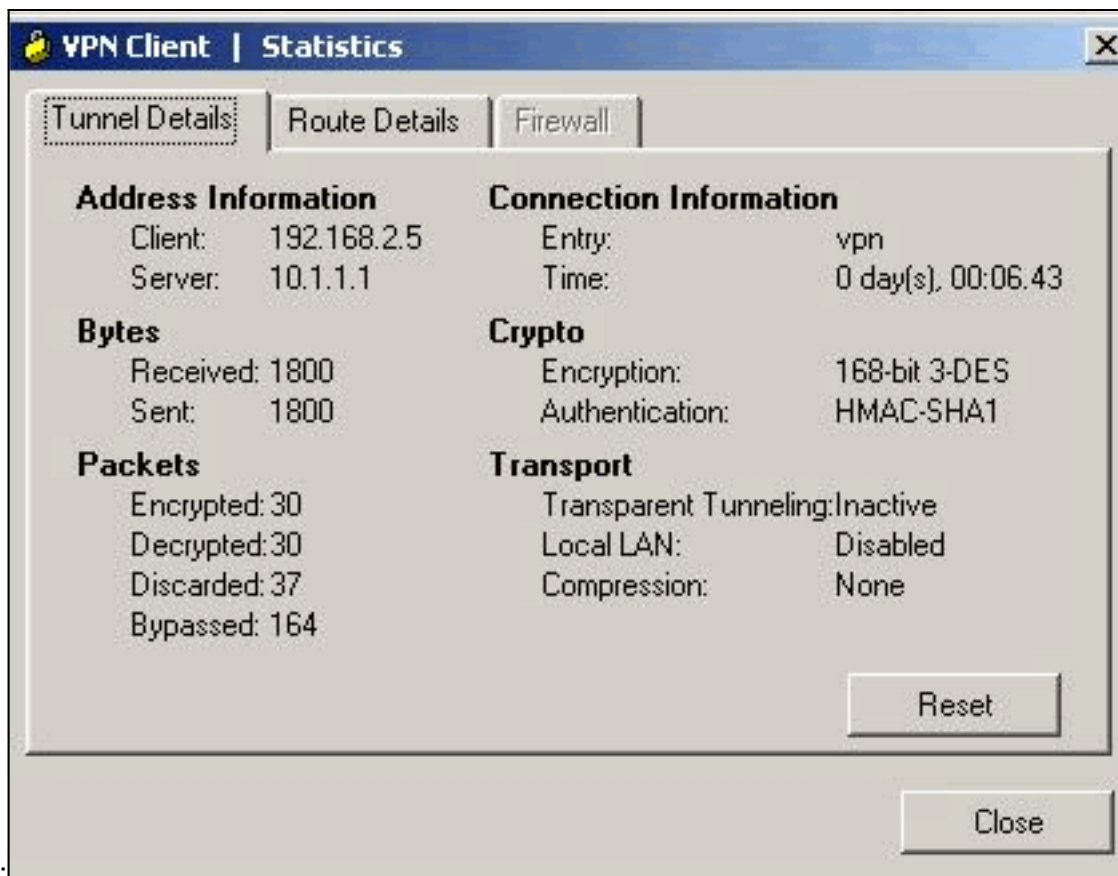
conecta.



4. Incorpore um nome de usuário e senha para a autenticação estendida (XAUTH). Esta informação é determinada pelos parâmetros do Xauth na etapa 7.

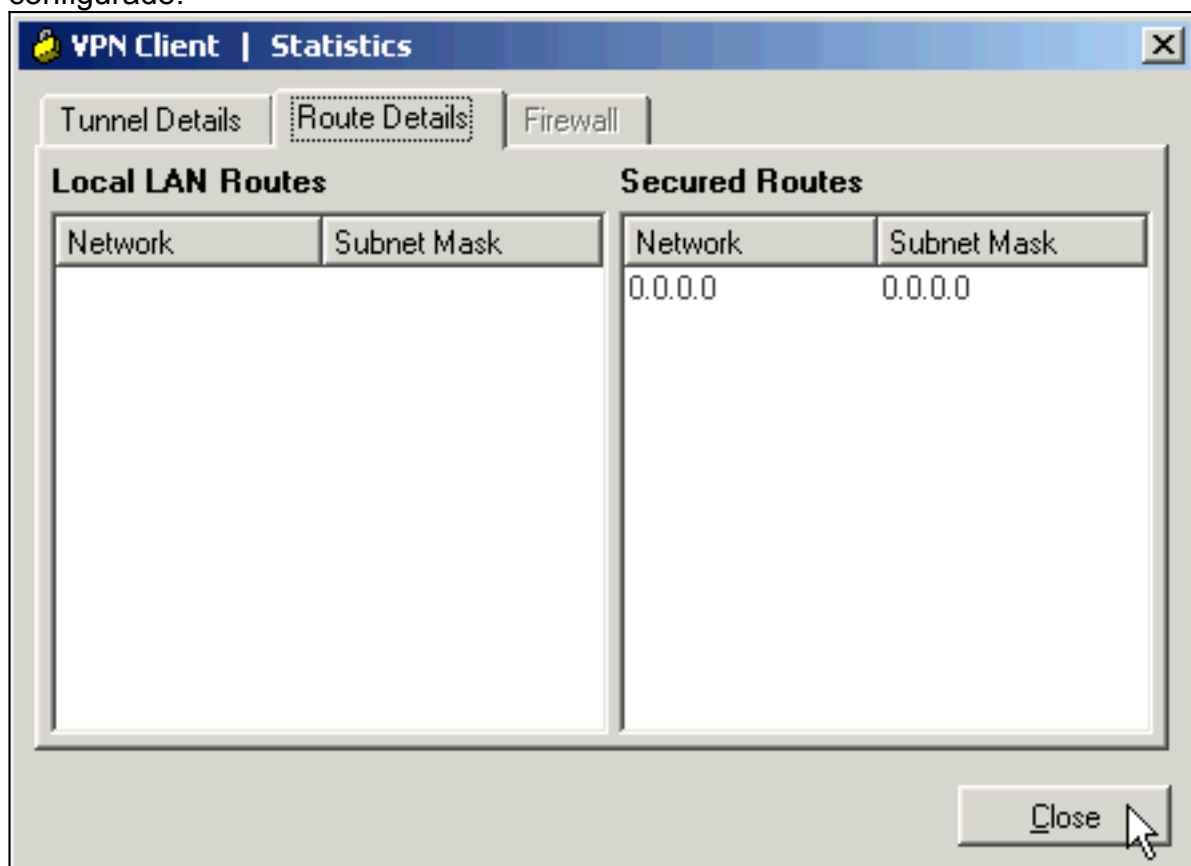


5. Uma vez que a conexão é **estatísticas** seletas com sucesso estabelecidas do menu de status para verificar os detalhes do túnel. Este indicador mostra o tráfego e a informação de



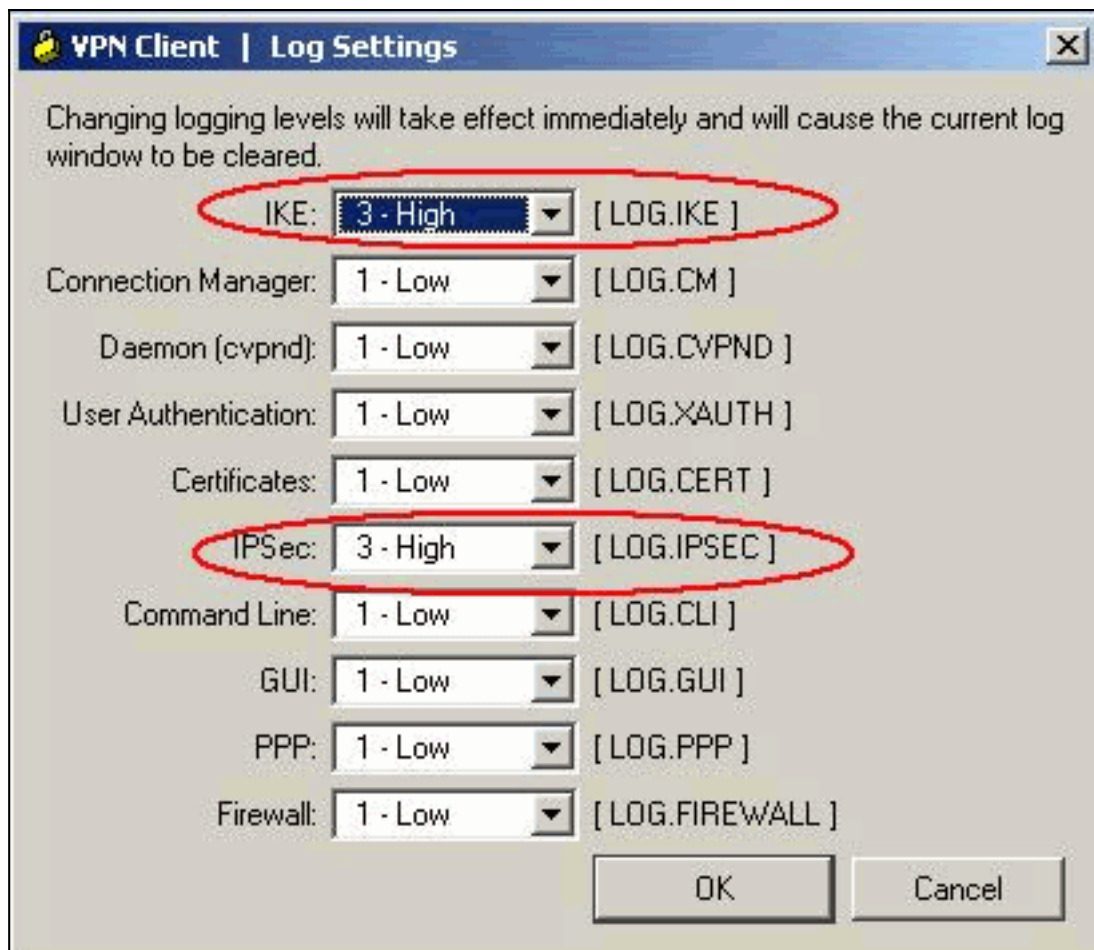
criptografia:

este indicador mostra a informação do Split Tunneling se configurado:



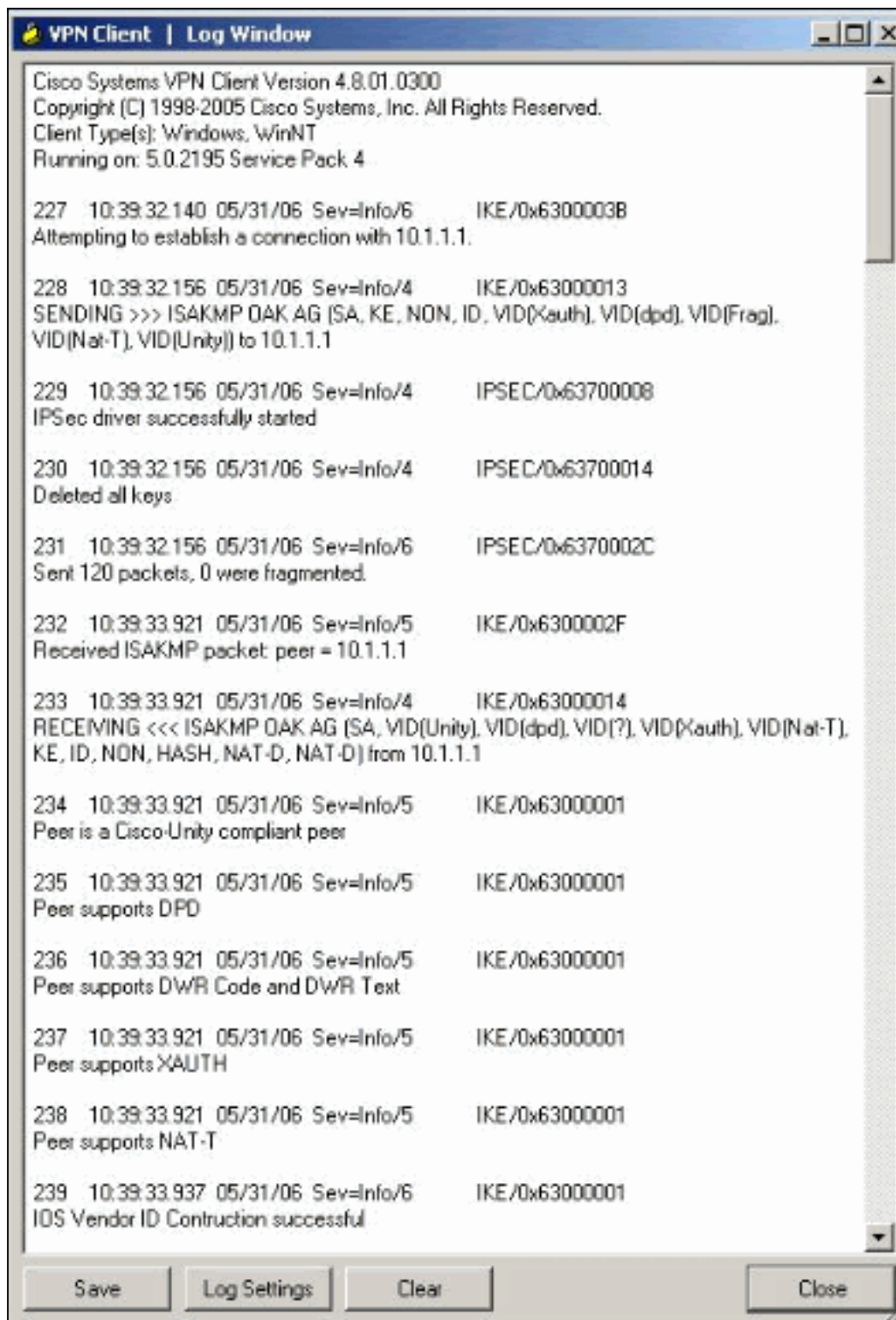
6. Selecione o log > as configurações de registro para permitir os níveis do log no Cisco VPN





Client.

7. Seleccione o **log** > o **log Windows** para ver as entradas de registro no Cisco VPN



Client.

## [Informações Relacionadas](#)

- [Transferindo e instalando Roteador Cisco e Security Device Manager](#)
- [Página de Suporte do Cisco VPN Client](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)