Configurar CSD no Cisco IOS usando SDM

Contents

Introduction

Embora as sessões de uma VPN (Cisco WebVPN) Secure Sockets Layer (SSL) sejam seguras, o cliente pode ainda encontrar cookies, arquivos do navegador e anexos de e-mails que permanecem depois que a sessão é encerrada. O Cisco Secure Desktop (CSD) estende a segurança inerente das sessões de VPN SSL gravando dados de sessão em um formato criptografado para uma área de *cofre* especial do disco do cliente. Além disso, esses dados são removidos do disco quando a sessão de VPN SSL é encerrada. Este documento apresenta um exemplo de configuração para CSD em um roteador Cisco IOS®.

O CSD é compatível com as seguintes plataformas de dispositivos da Cisco:

- Cisco IOS Routers versão 12.4(6)T e posterior
- Cisco 870,1811,1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 e 730 roteadores1
- Cisco VPN 3000 Series Concentrators versão 4.7 e posterior
- Dispositivos de segurança Cisco ASA 5500 Series versão 7.1 e posterior
- Cisco WebVPN Services Module para Cisco Catalyst e Cisco 7600 Series versão 1.2 e posterior

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

Requisitos para o roteador Cisco IOS

- Roteador Cisco IOS com Imagem Avançada 12.4(6T) ou posterior
- Cisco Router Secure Device Manager (SDM) 2.3 ou superior
- Uma cópia do pacote CSD para IOS na sua estação de gerenciamento
- Um certificado ou autenticação digital autoassinado do roteador com uma autoridade de certificação (CA)**Observação:** sempre que usar certificados digitais, certifique-se de definir corretamente o nome do host, o nome do domínio e a data/hora/fuso horário do roteador.
- Uma senha secreta de ativação no roteador
- DNS ativado no roteador. Vários serviços WebVPN exigem que o DNS funcione corretamente.

Requisitos para computadores clientes

- Os clientes remotos devem ter privilégios administrativos locais; não é obrigatório, mas é altamente sugerido.
- Os clientes remotos devem ter Java Runtime Environment (JRE) versão 1.4 ou superior.
- Navegadores clientes remotos: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 ou Firefox 1.0
- Cookies ativados e pop-ups permitidos em clientes remotos

Componentes Utilizados

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

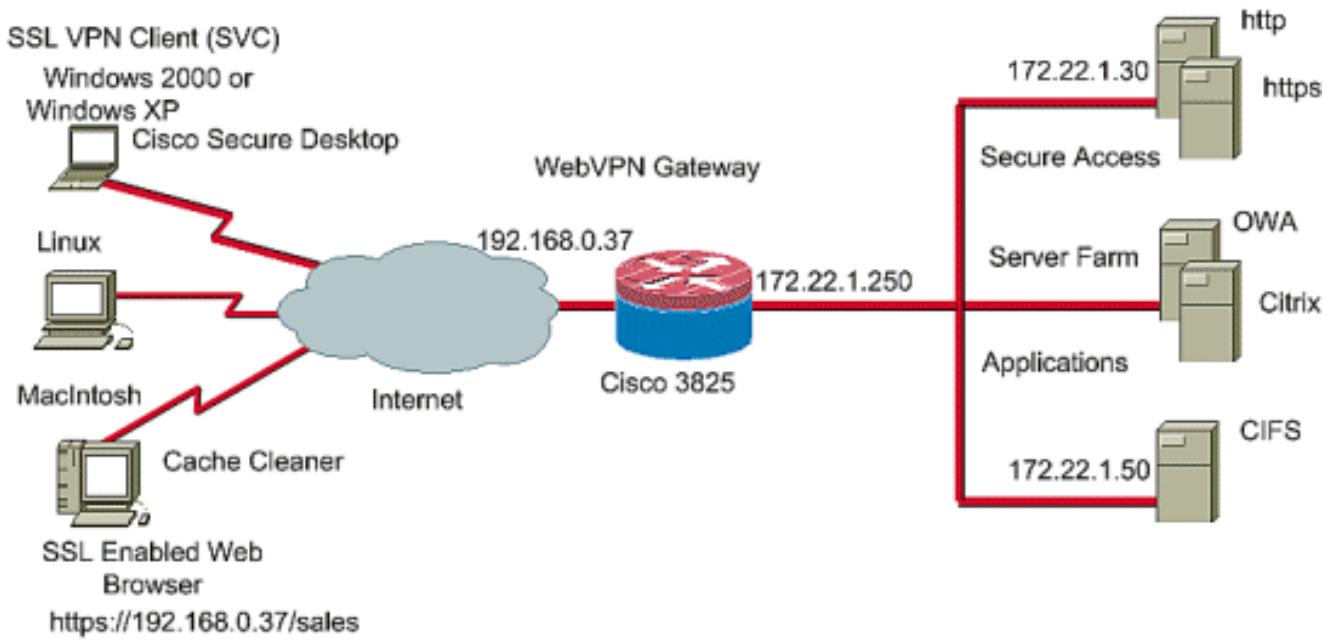
- Roteador Cisco IOS 3825 com versão 12.9(T)
- SDM versão 2.3.1

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). If your network is live, make sure that you understand the potential impact of any command.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Este exemplo usa um roteador Cisco 3825 Series para permitir acesso seguro à intranet da empresa. O roteador Cisco 3825 Series melhora a segurança das conexões VPN SSL com características e recursos de CSD configuráveis. Os clientes podem se conectar ao roteador habilitado para CSD por meio de um destes três métodos de VPN SSL: VPN SSL sem cliente (WebVPN), VPN SSL thin-client (Port-Forwarding) ou Cliente VPN SSL (SVC de tunelamento completo).



Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- Plataformas de roteador Cisco 870,1811,1841,2801,2811,2821 2851,3725,3745,3825,3845, 7200 e 73 01
- Cisco IOS Advanced Security Image versão 12.4(6)T e posterior

Conventions

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

Configurar

Um gateway WebVPN permite que um usuário se conecte ao roteador através de uma das tecnologias de VPN SSL. Somente um gateway WebVPN por endereço IP é permitido no dispositivo, embora mais de um contexto WebVPN possa ser conectado a um gateway WebVPN. Cada contexto é identificado por um nome exclusivo. As Políticas de Grupo identificam os recursos configurados disponíveis para um contexto WebVPN específico.

A configuração do CSD em um roteador IOS é realizada em duas fases:

Fase I: Prepare seu roteador para a configuração do CSD com o SDM

1. Configure um gateway WebVPN, contexto WebVPN e política de grupo .**Observação:** esta etapa é opcional e não é abordada com detalhes neste documento. Se você já configurou seu roteador para uma das tecnologias de VPN SSL, omita esta etapa.
2. Ative o CSD em um contexto WebVPN.

Fase II: Configure o CSD usando um navegador da Web.

1. Definir *Locais do Windows*.

2. Identificar critérios de localização .
3. Configurar os módulos e recursos de localização do Windows.
4. Configure os recursos do Windows CE, Macintosh e Linux.

Fase I: Prepare seu roteador para a configuração do CSD com o SDM.

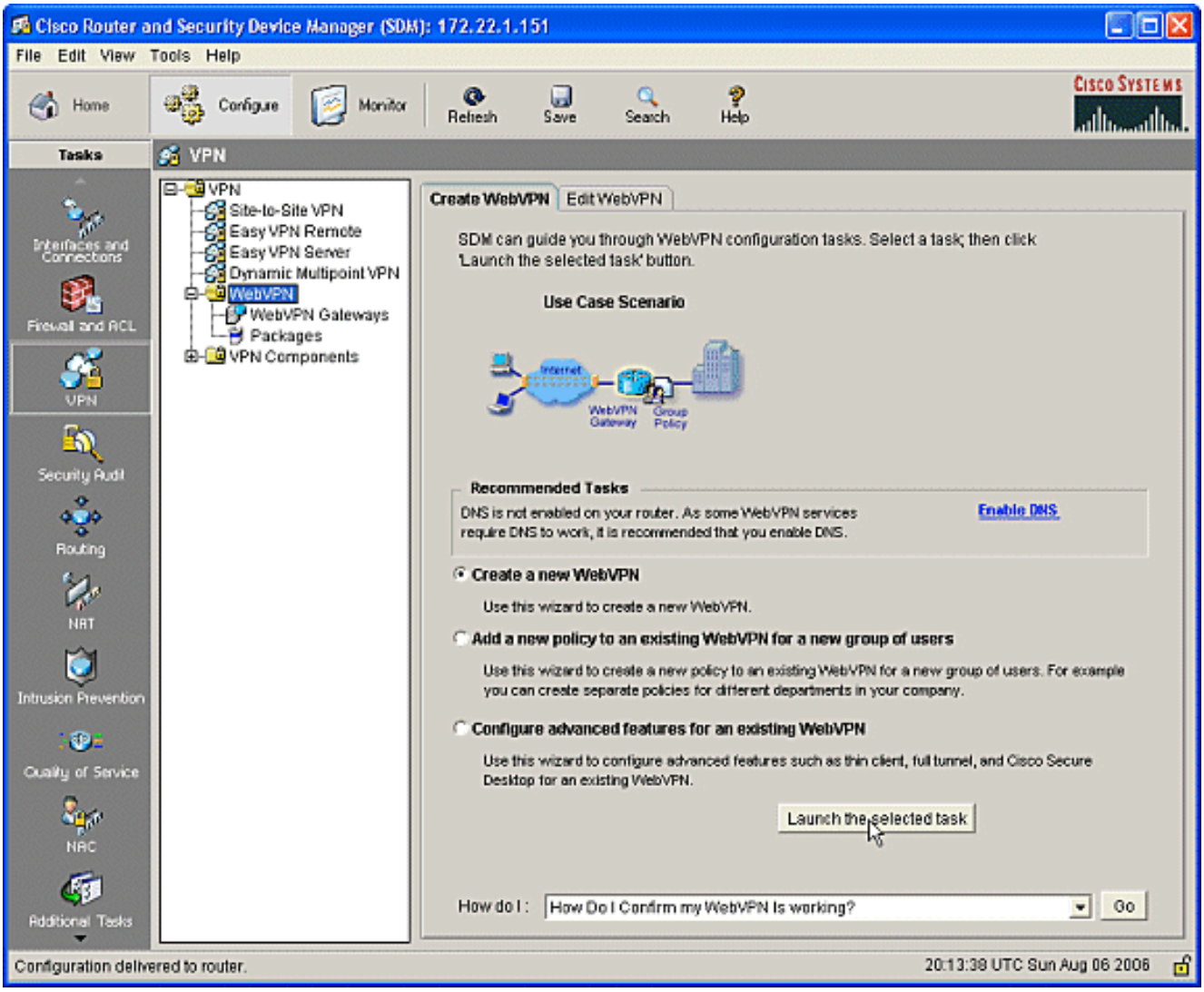
O CSD pode ser configurado com SDM ou pela interface de linha de comando (CLI). Essa configuração usa SDM e um navegador da Web.

Essas etapas são usadas para concluir a configuração do CSD no roteador do IOS.

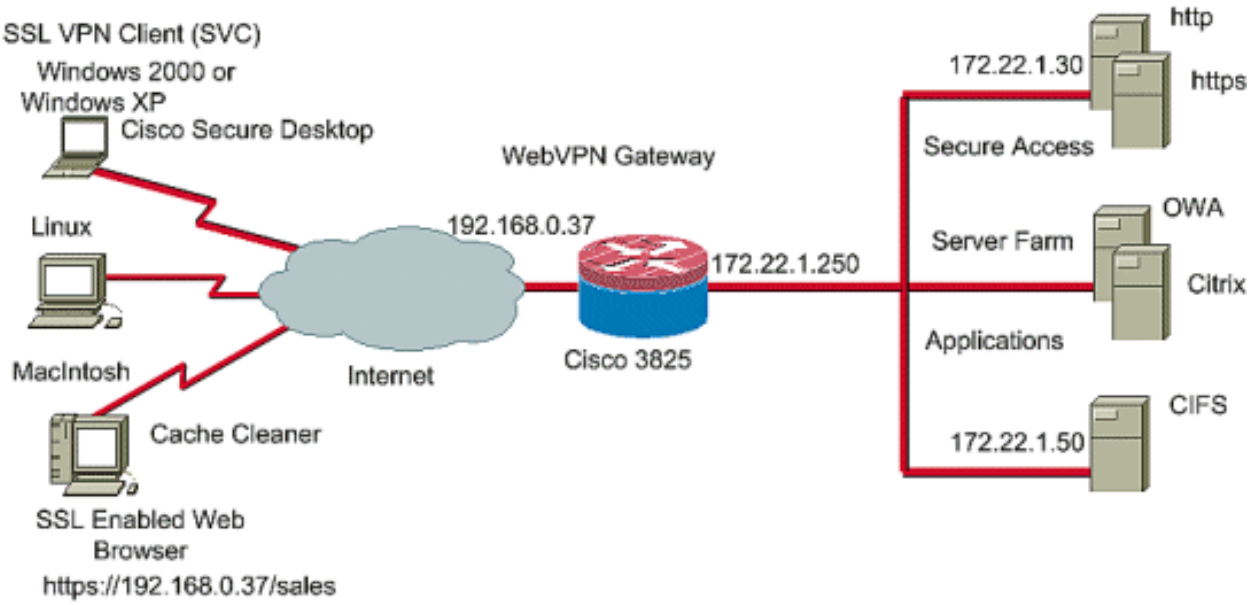
Fase I: Passo 1: Configure um gateway WebVPN, contexto WebVPN e política de grupo.

Você pode usar o WebVPN Wizard para realizar essa tarefa.

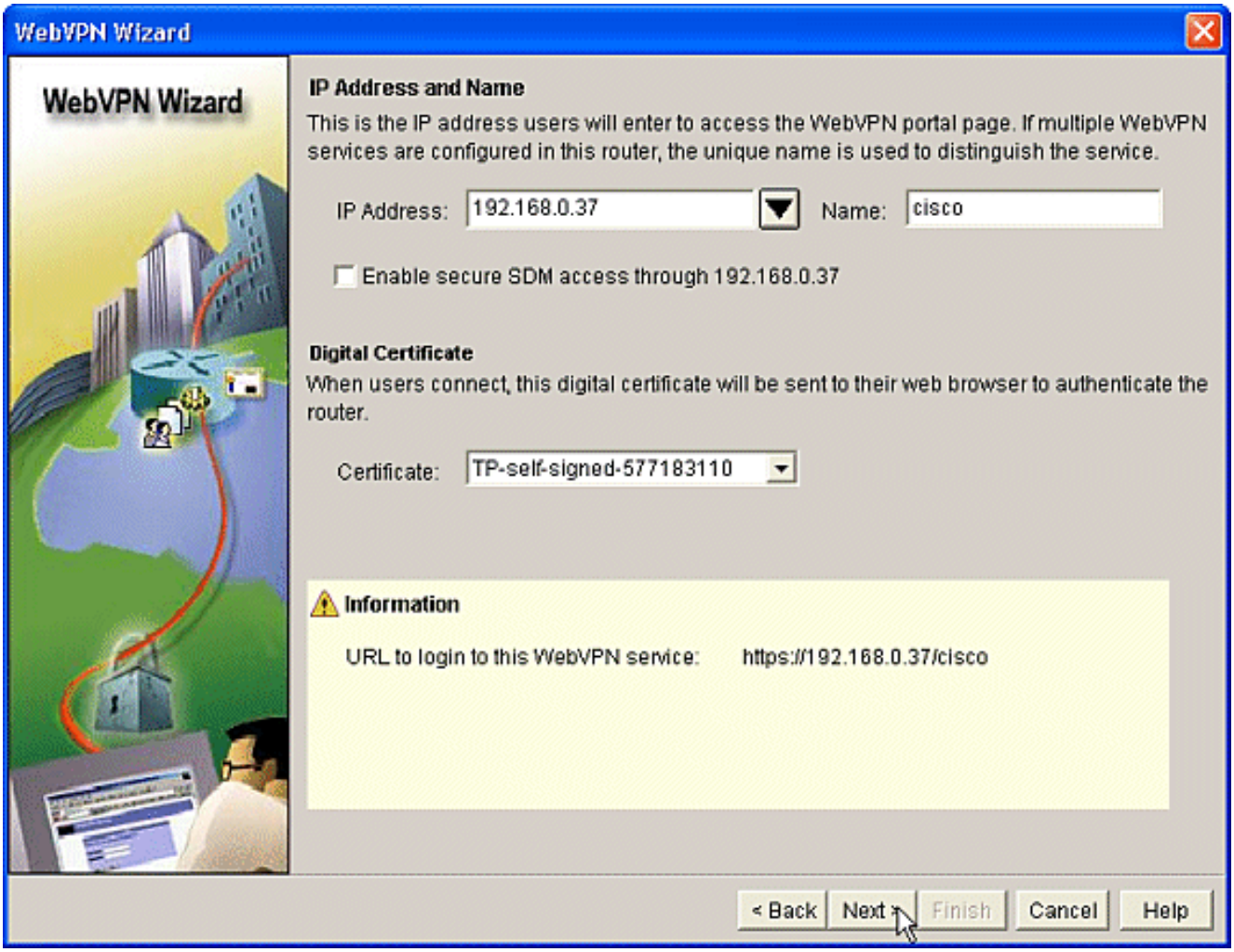
1. Abra o SDM e vá para **Configure > VPN > WebVPN**. Clique na guia **Create WebVPN** e marque o botão de opção **Create a new WebVPN**. Clique em **Iniciar a tarefa selecionada**.



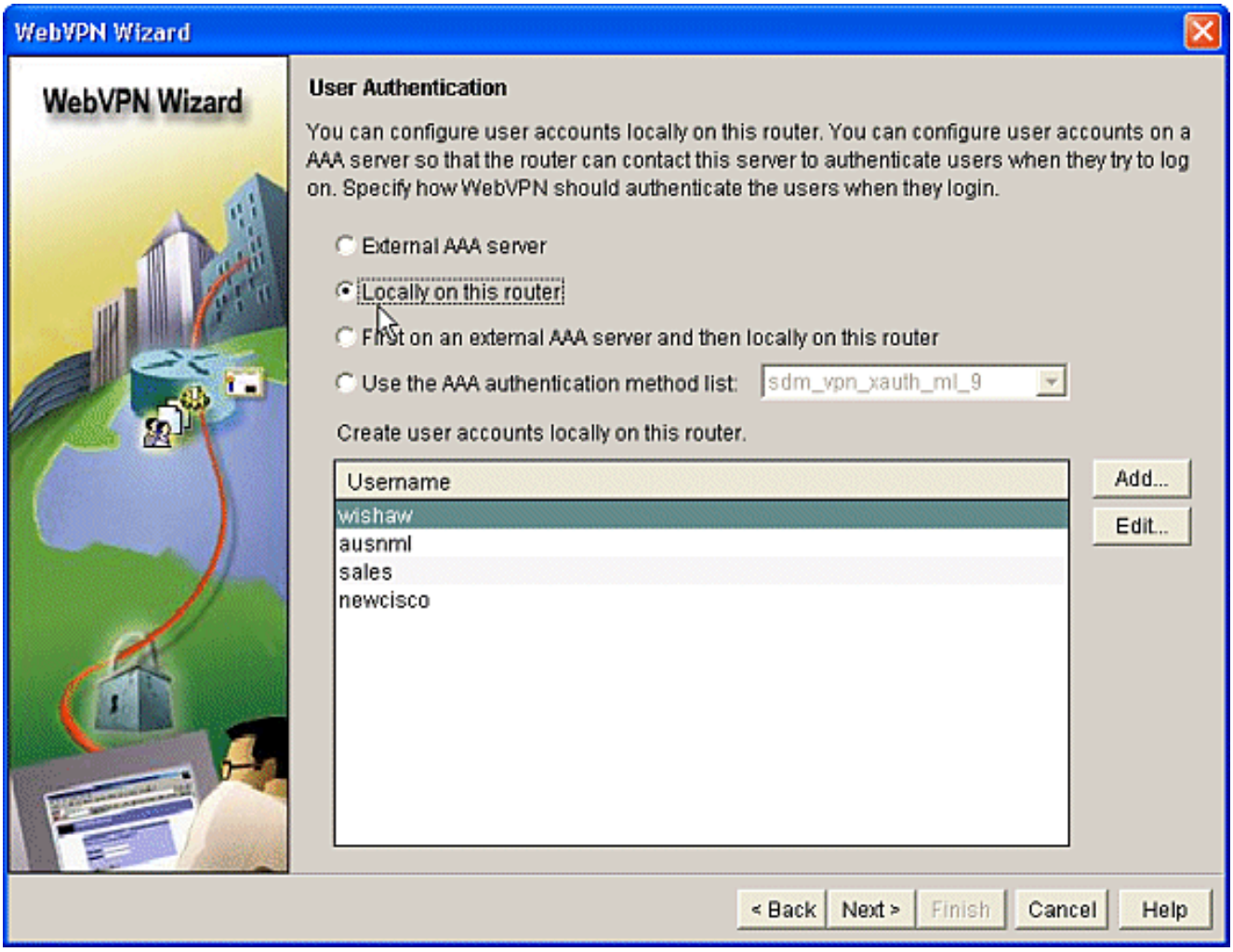
2. A tela WebVPN Wizard (Assistente de WebVPN) lista os parâmetros que você pode configurar. Clique em
Next.



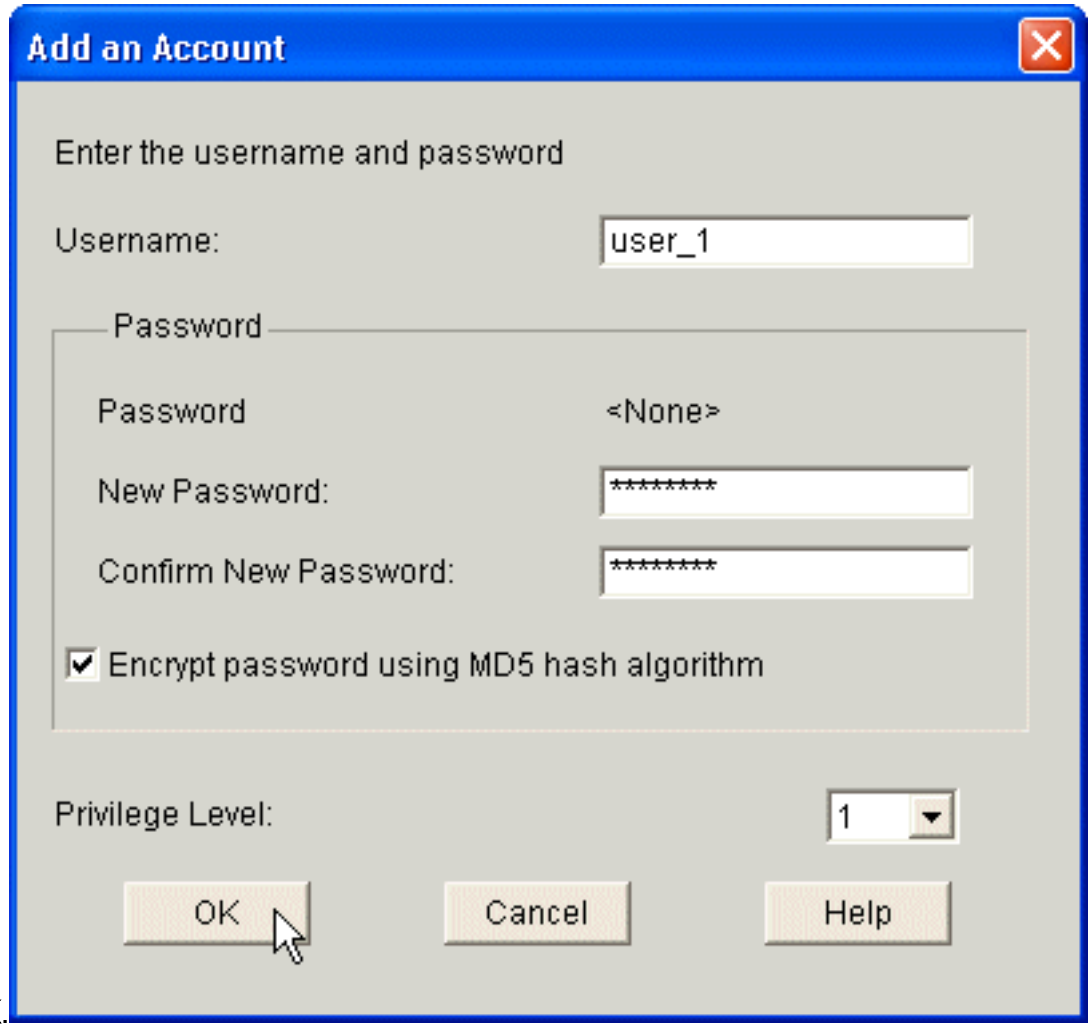
3. Insira o endereço IP do gateway WebVPN, um nome exclusivo para o serviço e informações de certificado digital. Clique em
Next.



4. As contas de usuário podem ser criadas para autenticação neste gateway WebVPN. Você pode usar contas locais ou contas criadas em um servidor externo de Autenticação, Autorização e Contabilidade (AAA). Este exemplo usa contas locais no roteador. Verifique o botão de opção **Localmente neste roteador** e clique em
Adicionar.

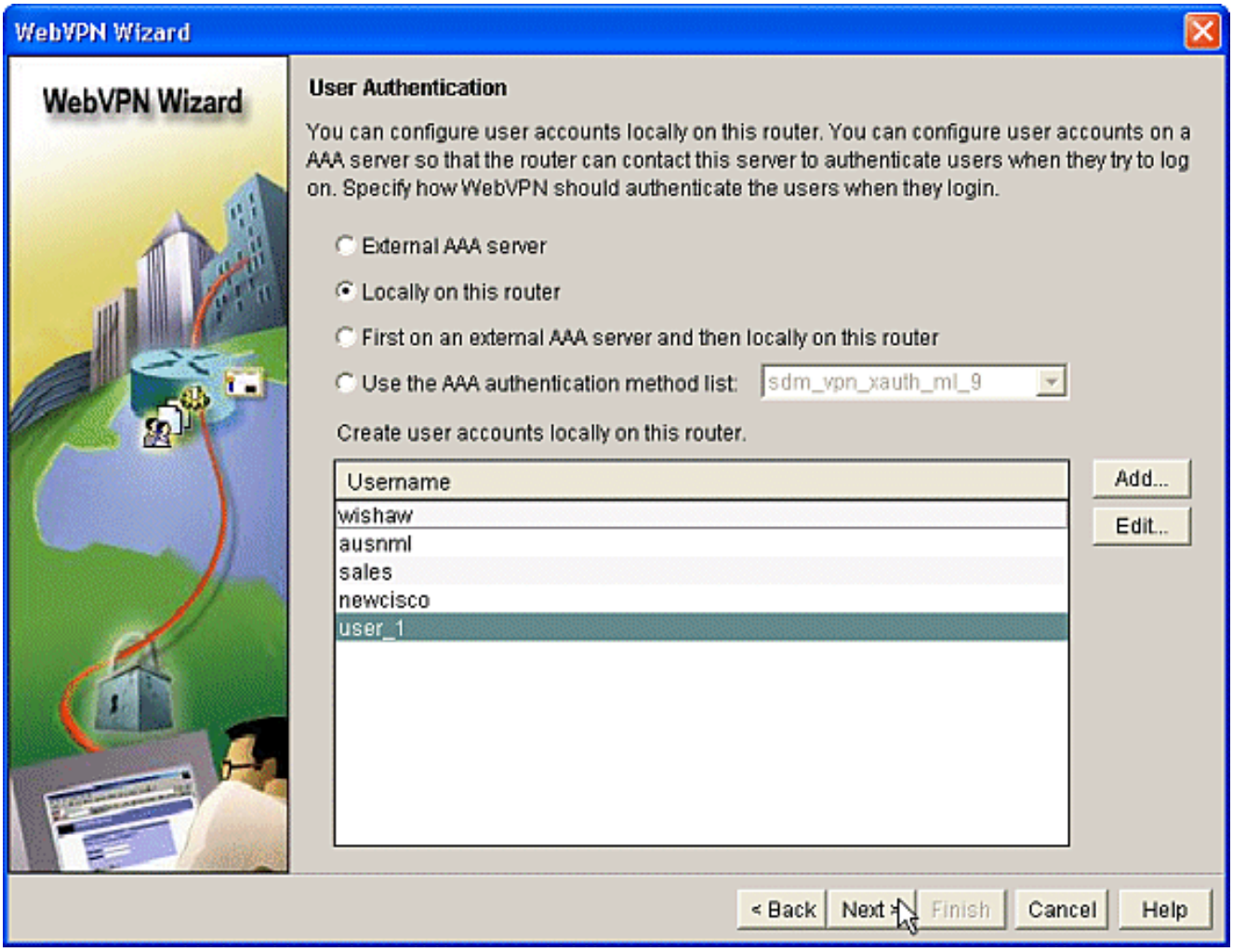


5. Insira as informações da conta do novo usuário na tela Adicionar uma conta e clique em

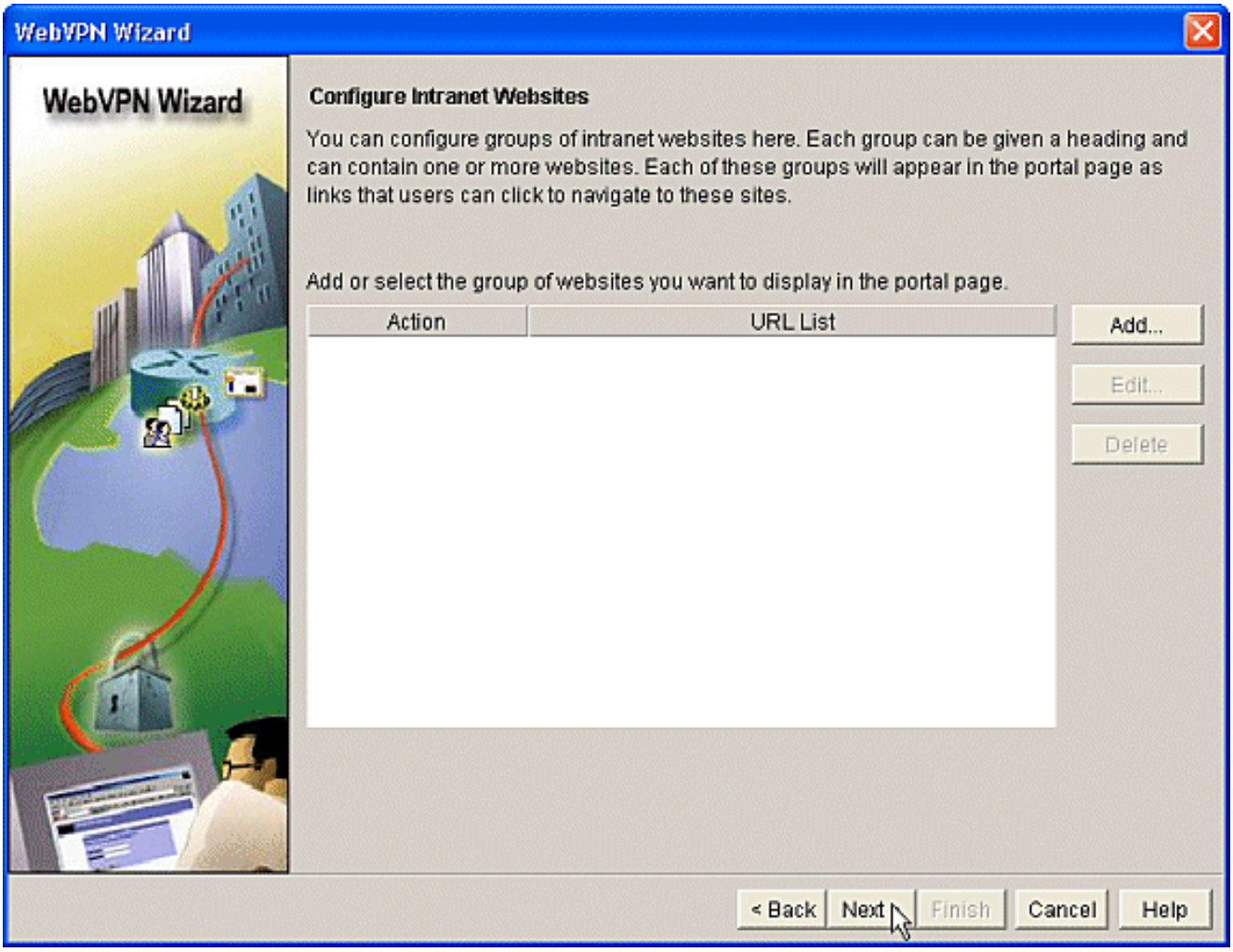


OK.

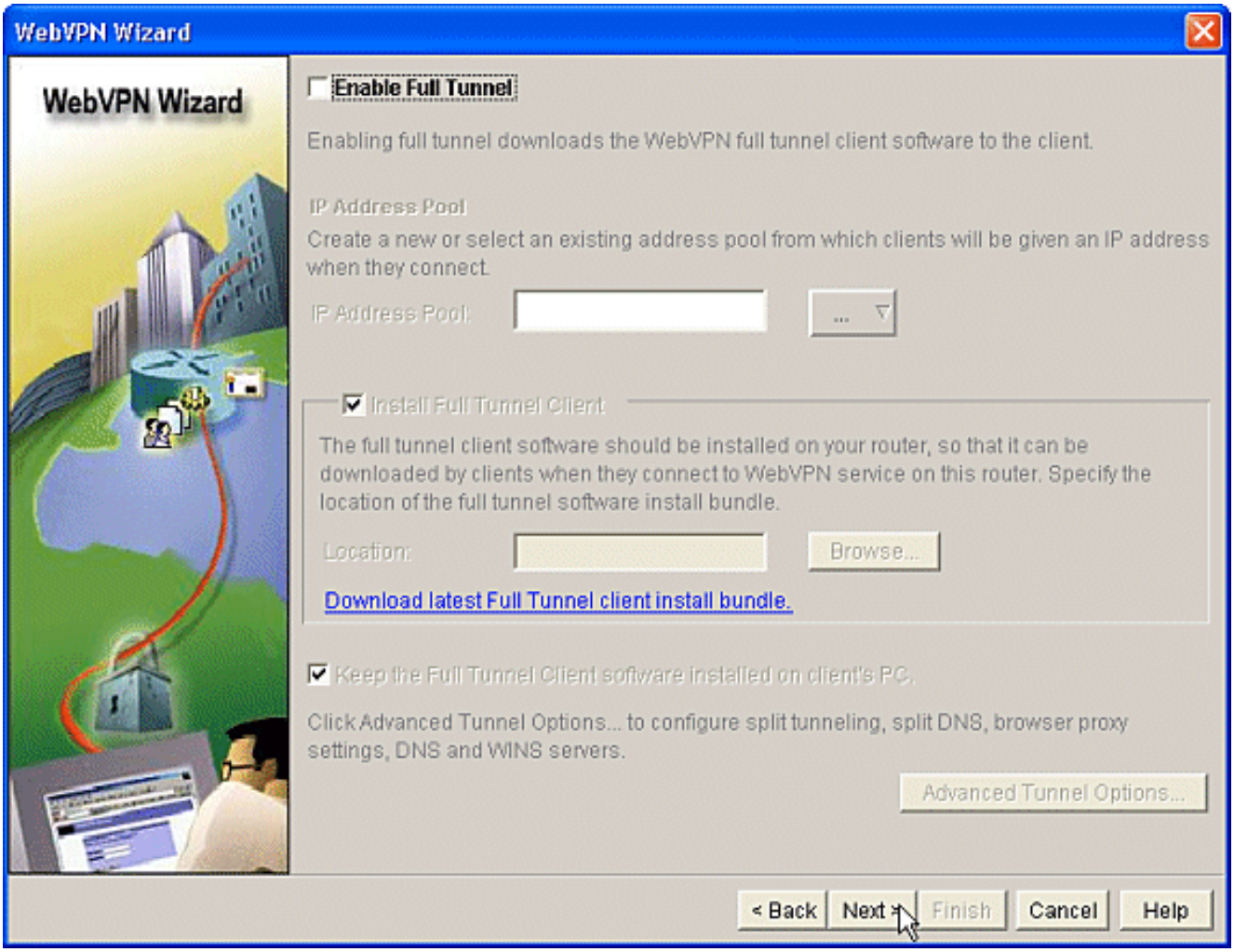
6. Depois de criar os seus utilizadores, clique em **Seguinte** na página Autenticação de Utilizador.



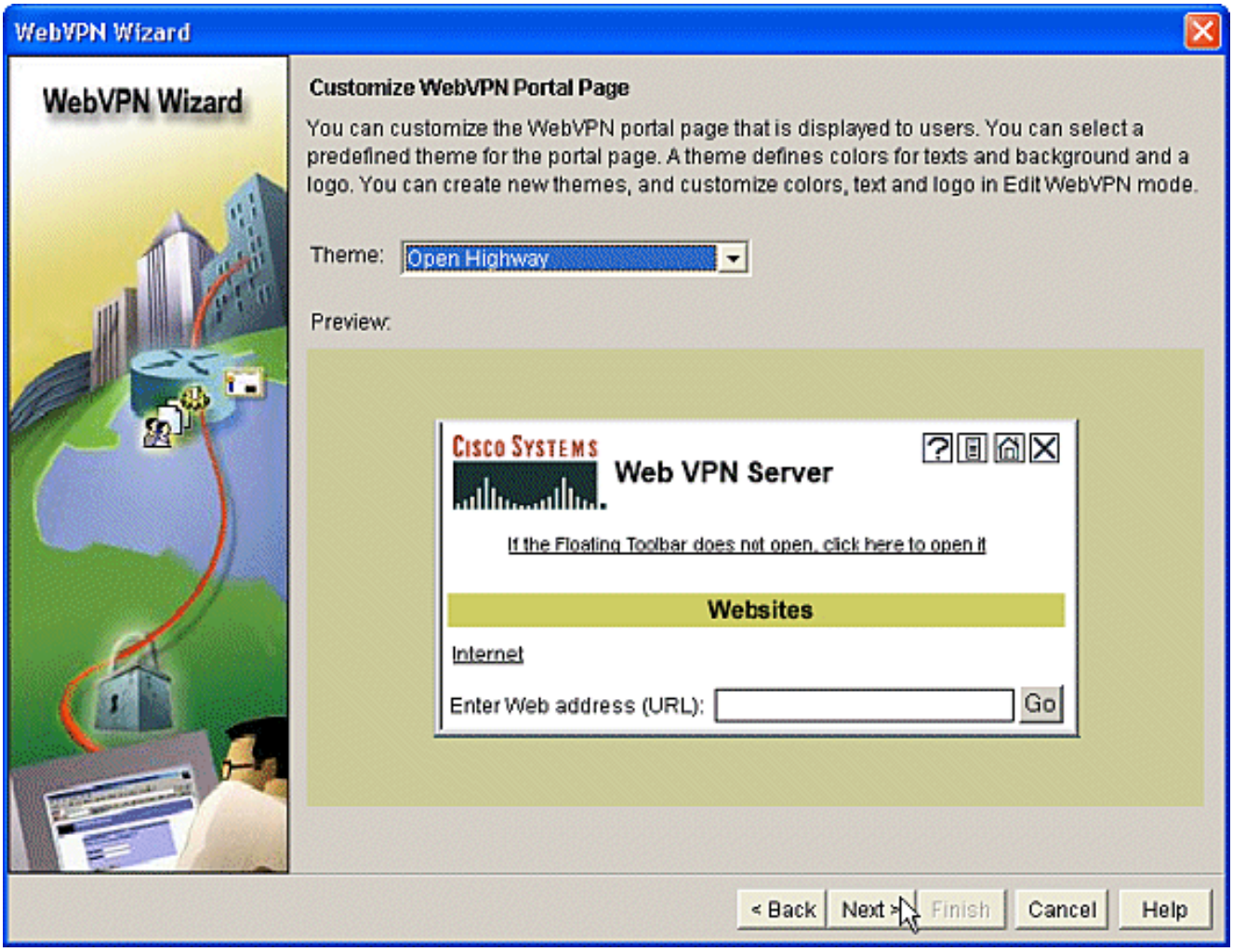
7. A tela Configurar sites da Intranet permite configurar o site disponível para os usuários do gateway WebVPN. Como o foco deste documento é a configuração do CSD, desconsidere esta página. Clique em
   Next.



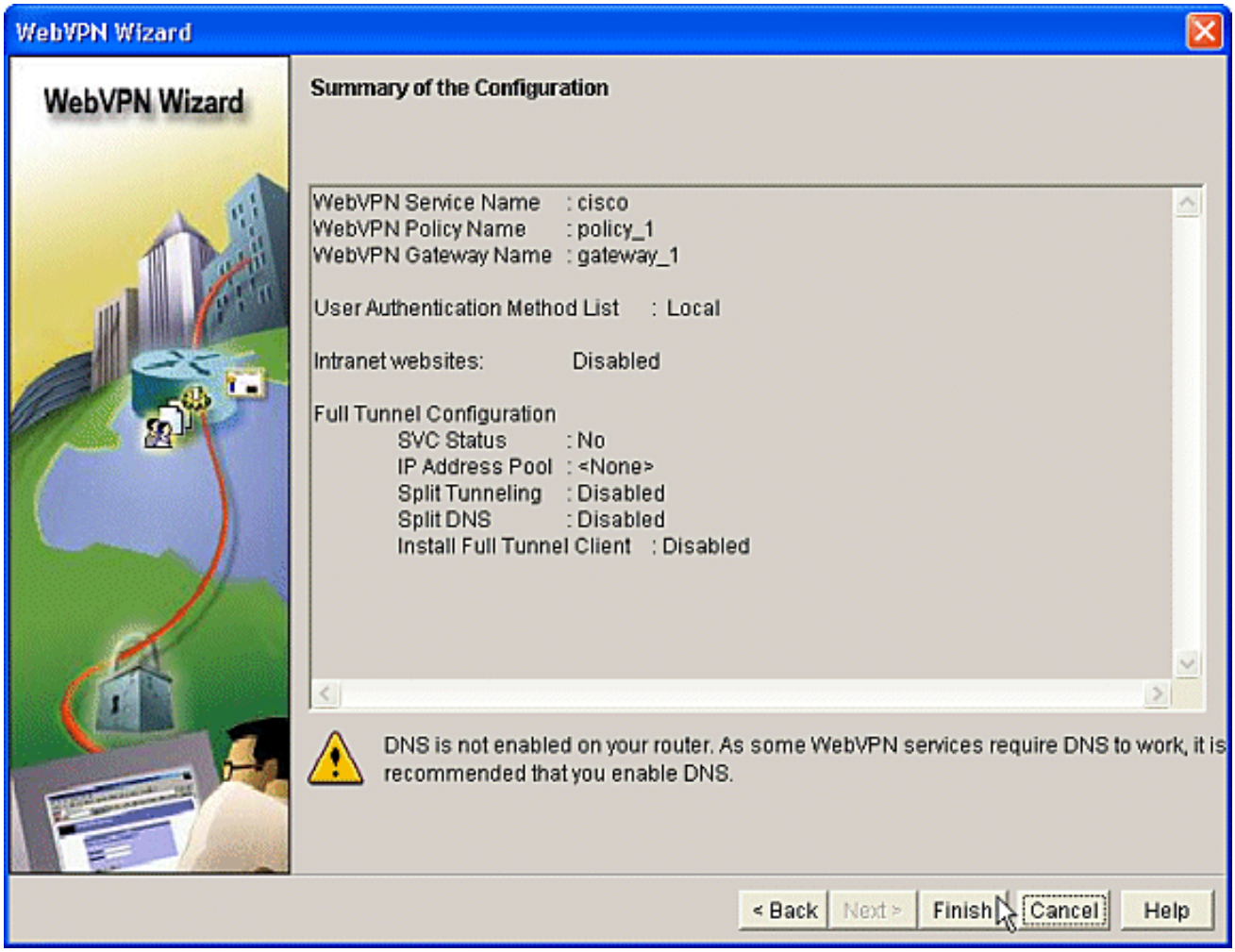
8. Embora a próxima tela do WebVPN Wizard permita que você opte por ativar o cliente VPN SSL de túnel completo, o foco deste documento é como habilitar o CSD. Desmarque **Enable Full Tunnel (Ativar túnel completo)** e clique em **Next (Avançar)**.



9. Você pode personalizar a aparência da página do portal WebVPN para os usuários. Nesse caso, a aparência padrão é aceita. Clique em
Next.



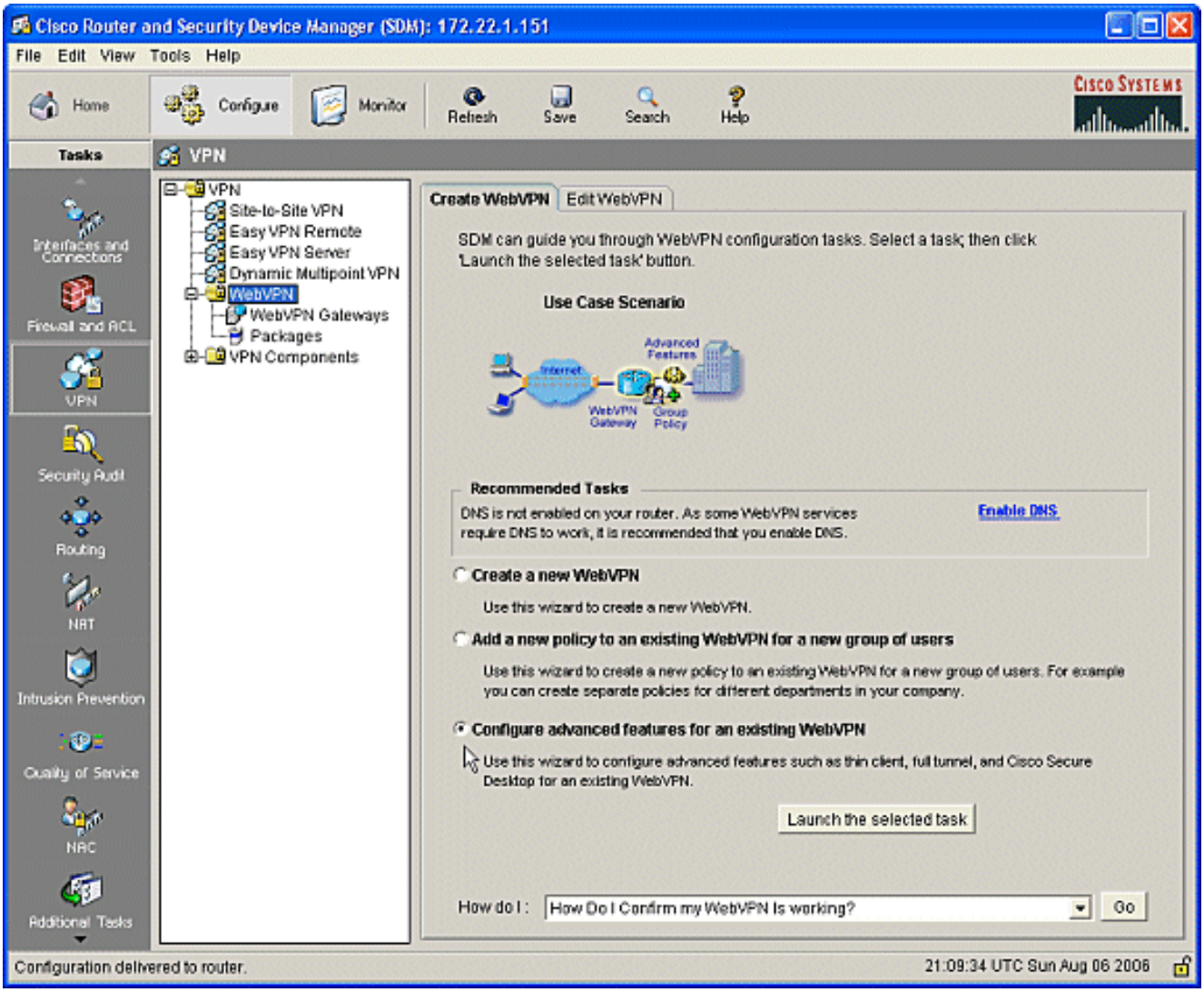
10. O Assistente exibe a última tela nesta série. Ele mostra um resumo da configuração para o gateway WebVPN. Clique em **Finish** e, quando solicitado, clique em **OK**.



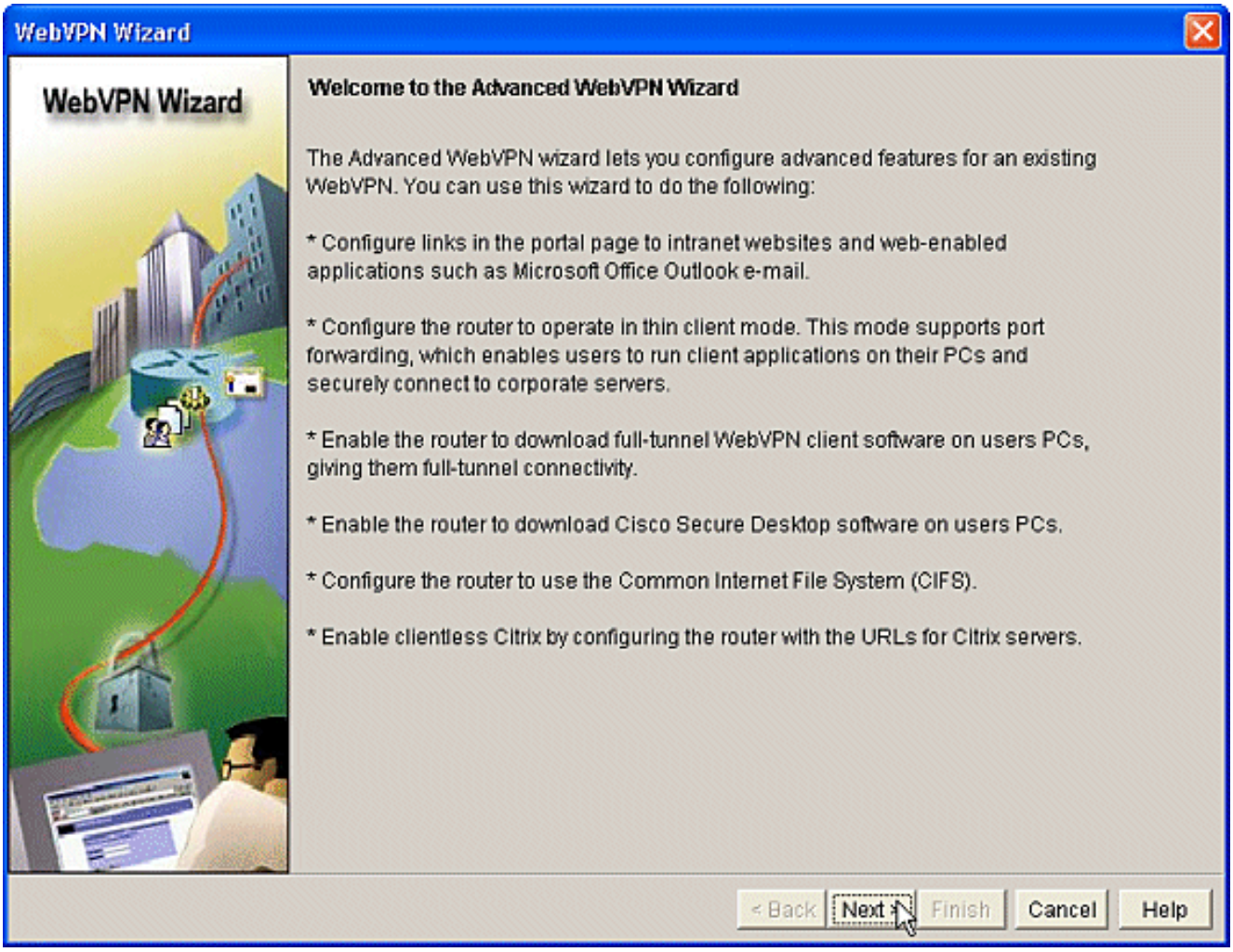
Fase I: Passo 2: Habilitar CSD em um contexto WebVPN.

Use o WebVPN Wizard para habilitar o CSD em um contexto WebVPN.

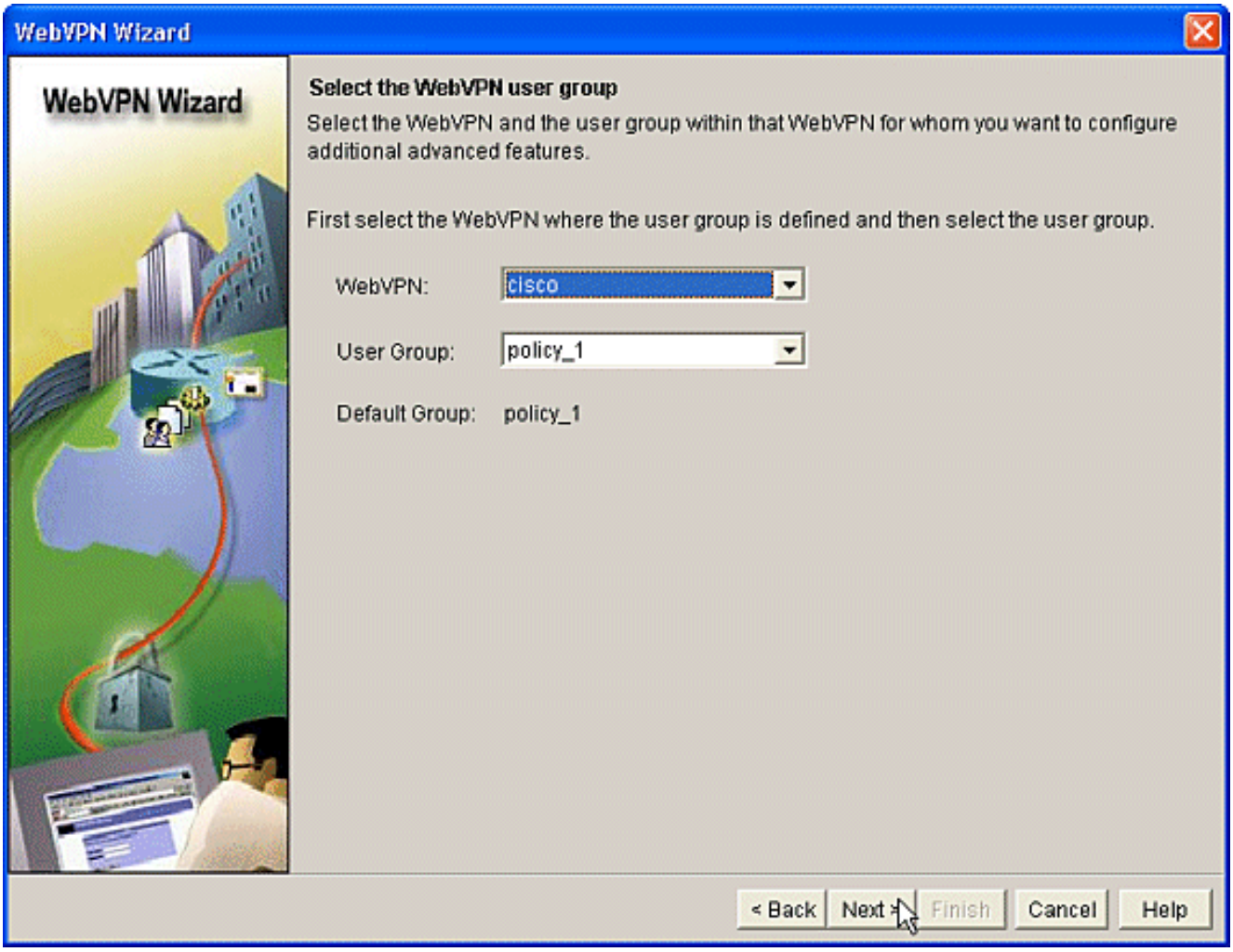
1. Use os recursos avançados do WebVPN Wizard para habilitar o CSD para o contexto recém-criado. O Assistente oferece a oportunidade de instalar o pacote CSD se ele ainda não estiver instalado.No SDM, clique na guia **Configurar**.No painel de navegação, clique em **VPN > WebVPN**.Clique na guia **Create WebVPN (Criar WebVPN).**Verifique o botão de opção **Configurar recursos avançados para um WebVPN existente**.Clique no botão **Iniciar a tarefa selecionada**.



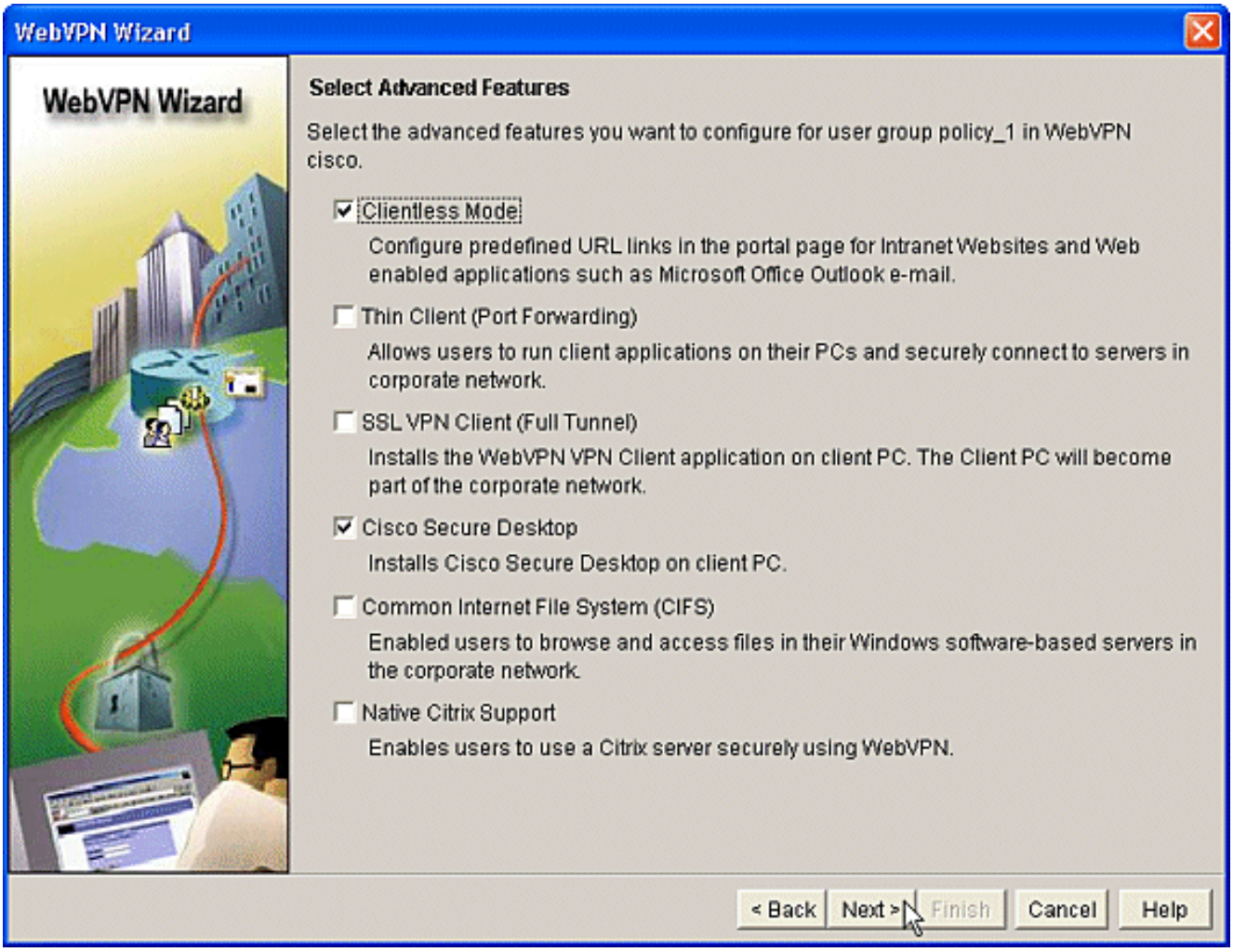
2. A página de boas-vindas do Assistente WebVPN Avançado é exibida. Clique em Next.



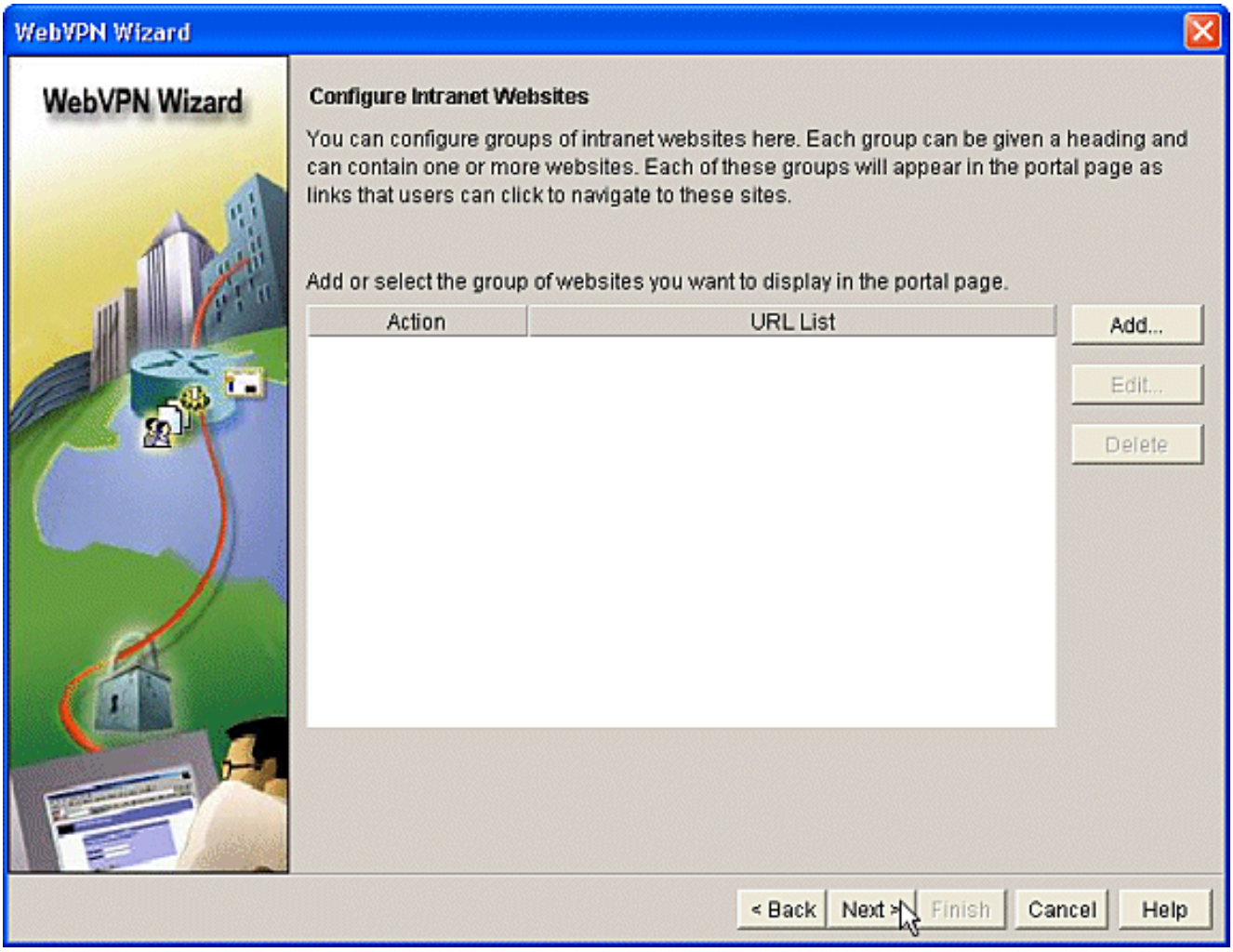
3. Escolha o WebVPN e o grupo de usuários nas caixas suspensas dos campos. Os recursos do Advanced WebVPN Wizard serão aplicados às suas opções. Clique em Next.



4. A tela Selecionar recursos avançados permite escolher entre as tecnologias listadas.Verifique o **Cisco Secure Desktop**.Neste exemplo, a escolha é **Modo sem cliente**.Se você escolher qualquer uma das outras tecnologias listadas, janelas adicionais serão abertas para permitir a entrada de informações relacionadas.Clique no botão **Avançar**.

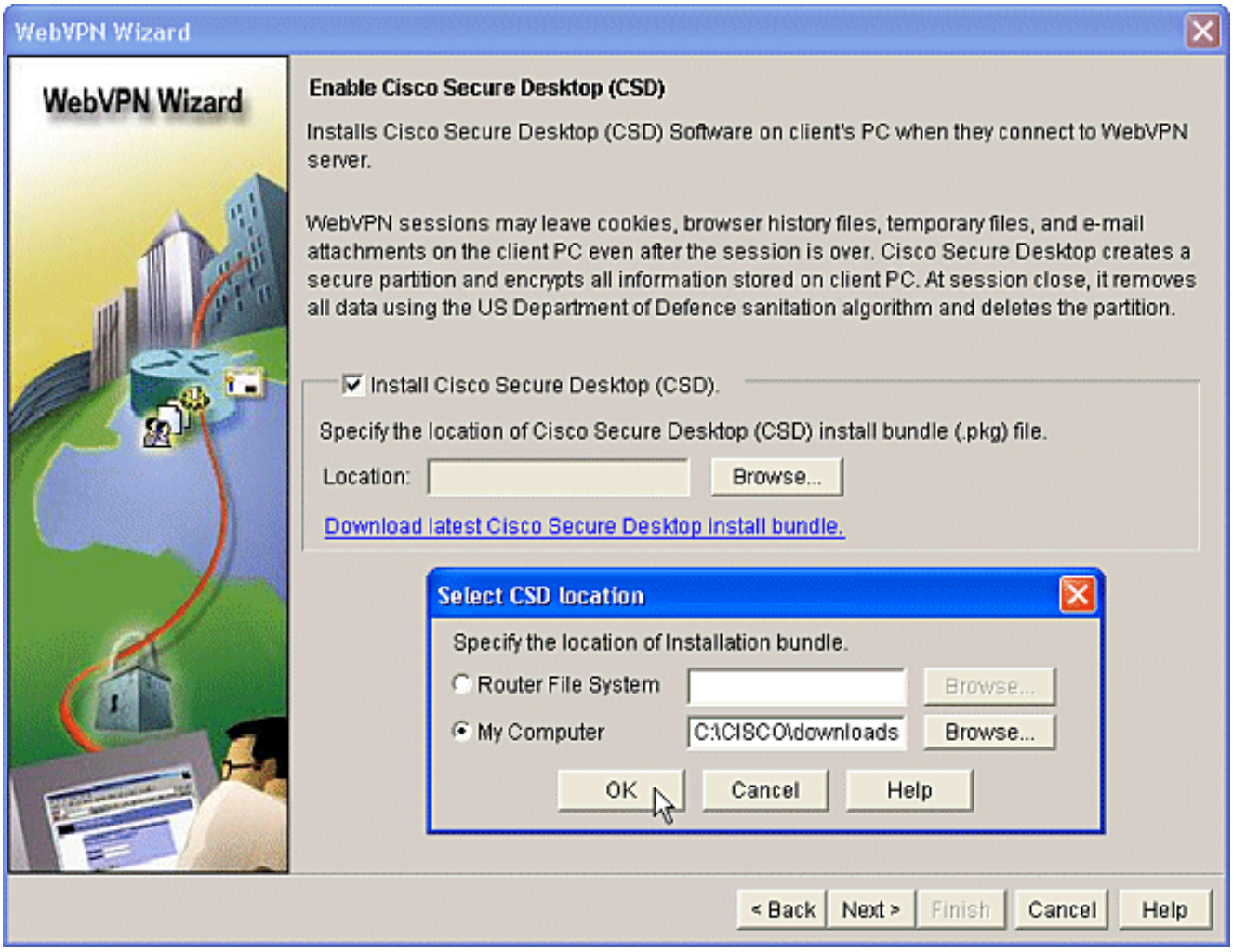


5. A tela Configurar sites da Intranet permite configurar os recursos do site que você deseja que estejam disponíveis para os usuários. Você pode adicionar os sites internos da empresa, como o Outlook Web Access
(OWA).



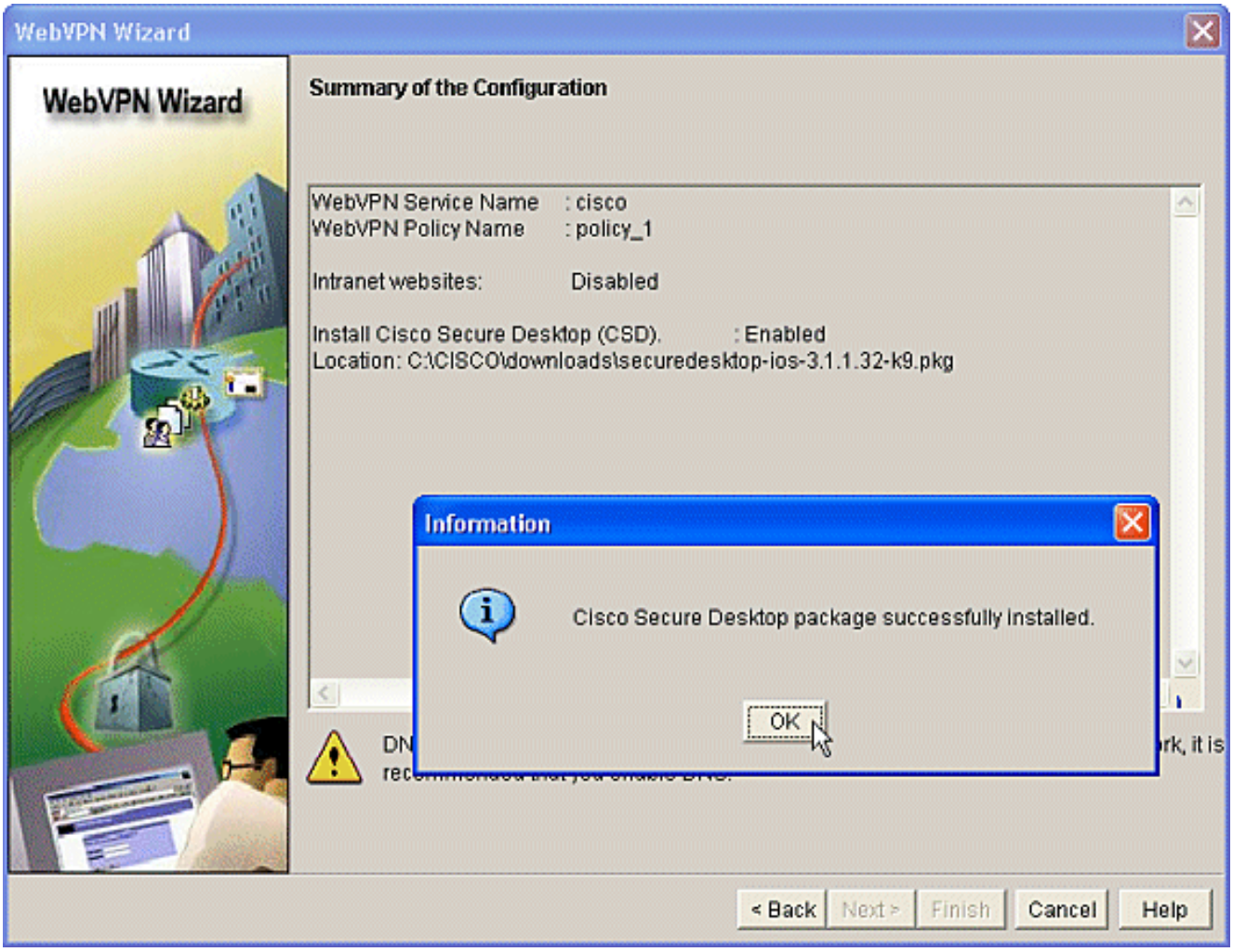
6. Na tela Habilitar Cisco Secure Desktop (CSD), você tem a oportunidade de habilitar o CSD para esse contexto. Marque a caixa ao lado de **Install Cisco Secure Desktop (CSD)** e clique em
Browse.

7. Na área Selecionar local do CSD, marque **Meu computador**.Clique no botão **Procurar**.Escolha o arquivo do pacote do CSD IOS na sua estação de trabalho de gerenciamento.Clique na tecla OK.Clique no botão **Avançar**.



8. A tela Resumo da configuração é exibida. Clique no botão **Concluir**.

9. Clique em **OK** quando vir que o arquivo do pacote CSD foi instalado com êxito.



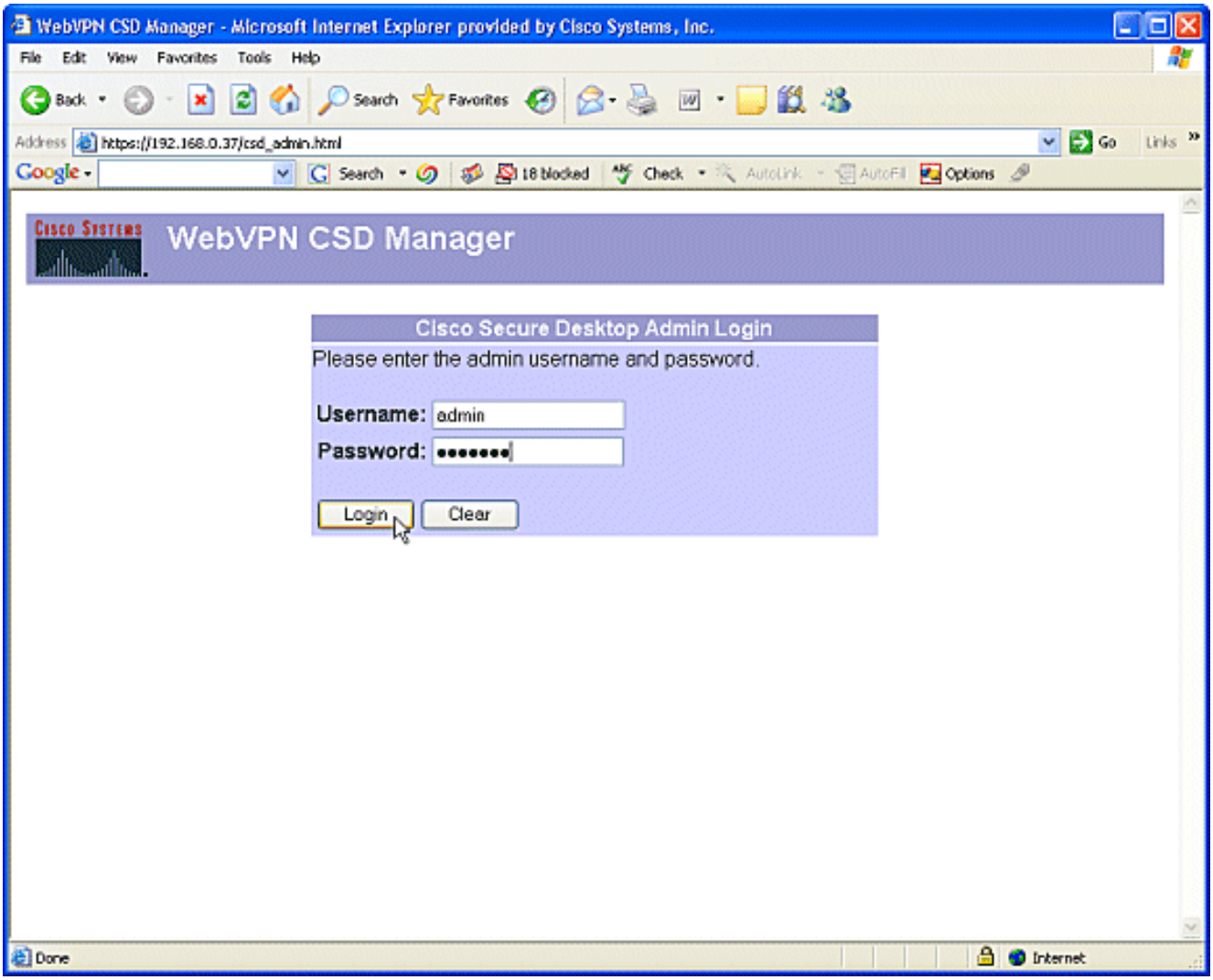
Fase II: Configure o CSD usando um navegador da Web.

Essas etapas são usadas para concluir a configuração do CSD no seu navegador da Web.

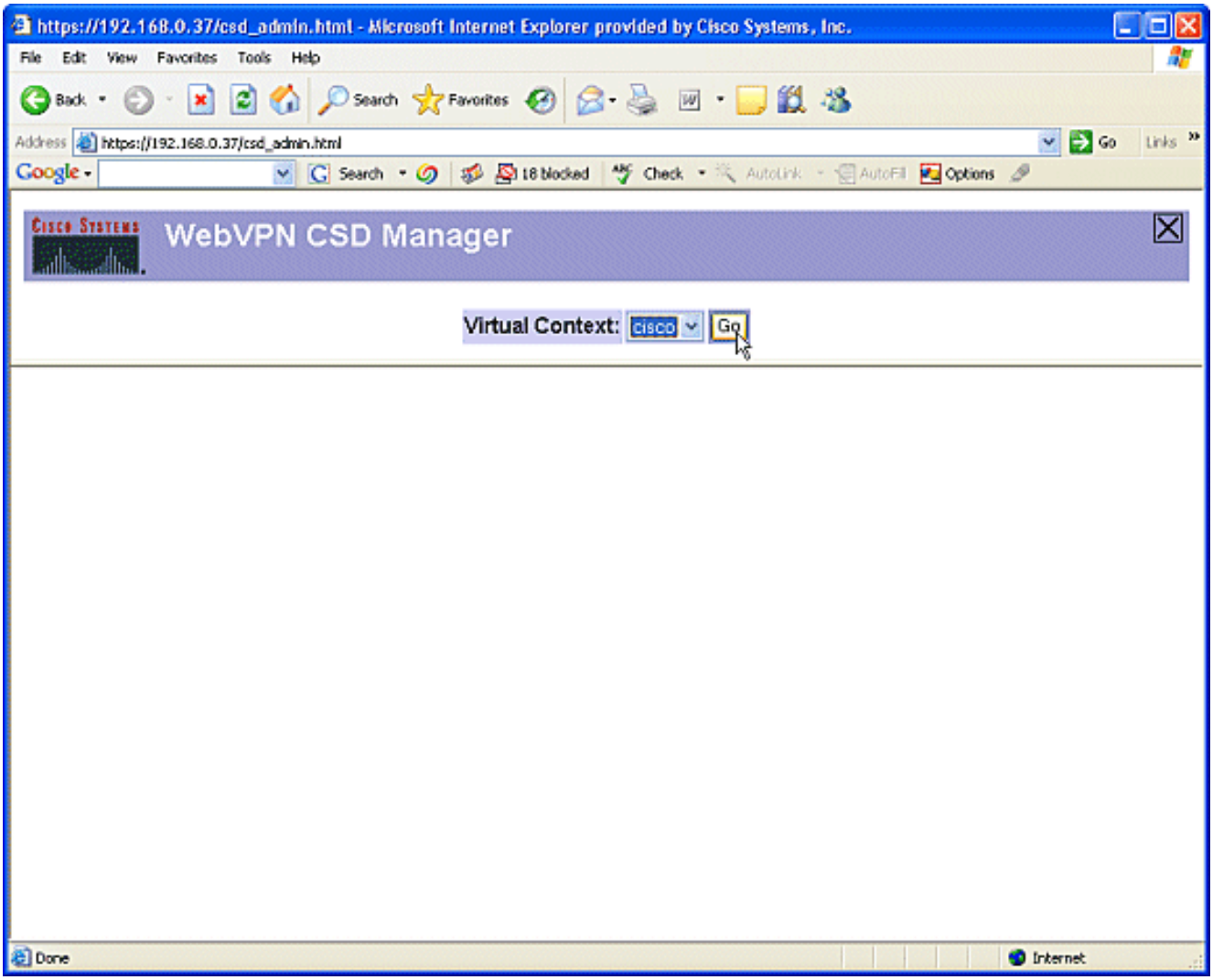
Fase II: Passo 1: Definir locais do Windows.

Defina os locais do Windows.

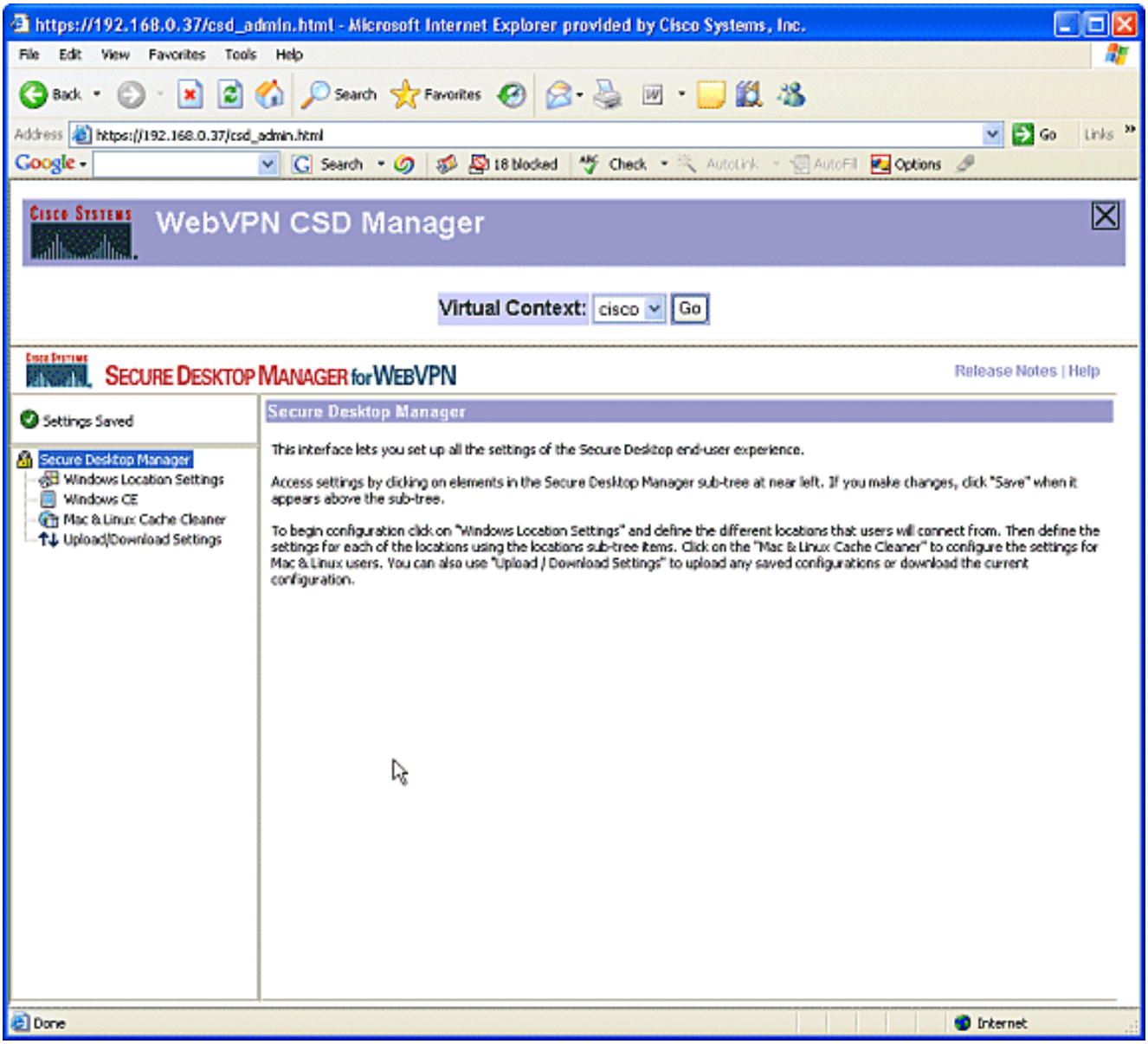
1. Abra o navegador da Web em **https://WebVPNgateway_IP Address/csd_admin.html**, por exemplo, **https:/192.168.0.37/csd_admin.html**.
2. Digite o nome de usuário **admin**.Digite a senha, que é o segredo de ativação do roteador.Clique em
   login.



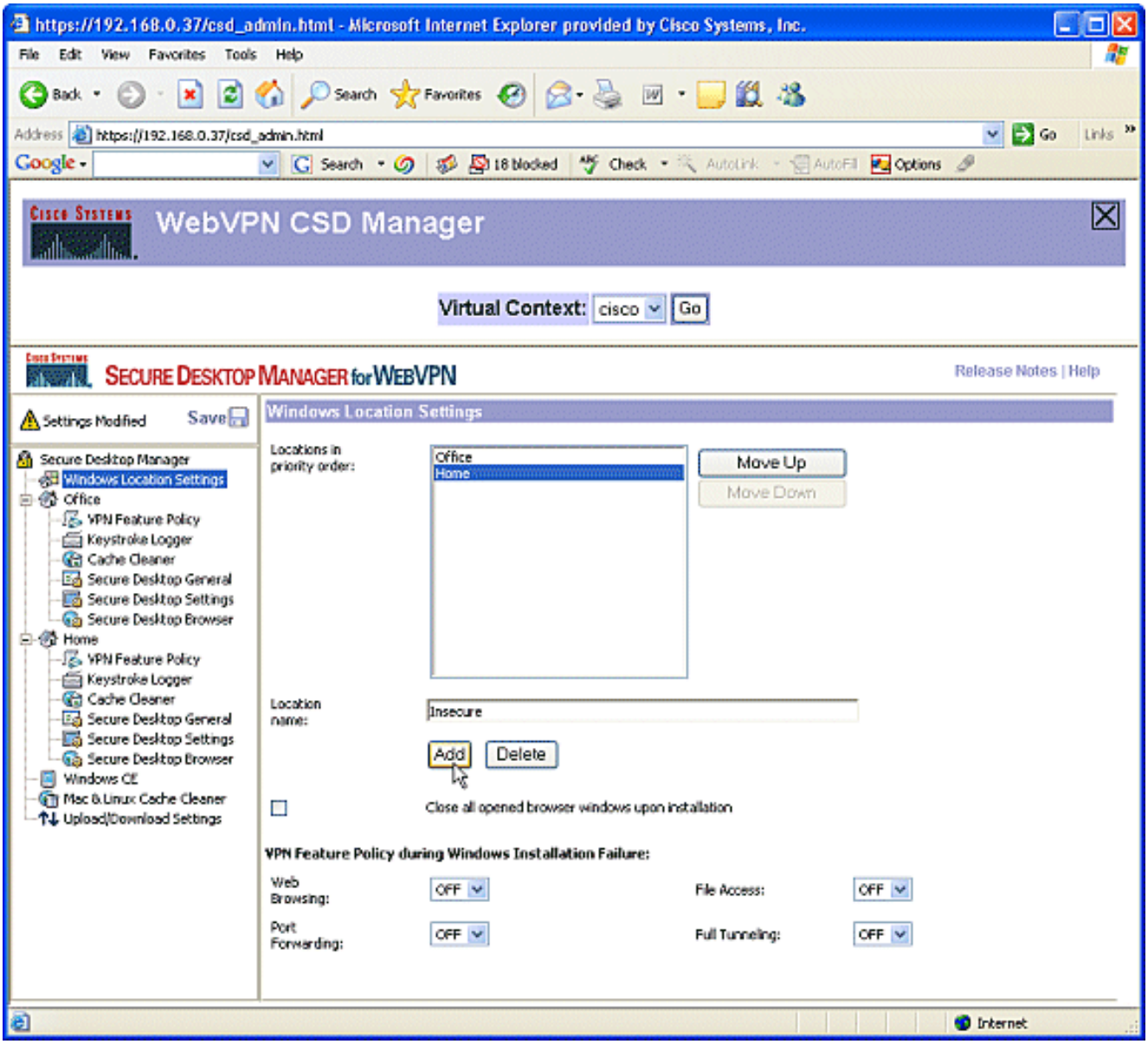
3. Aceite o certificado oferecido pelo roteador, escolha o contexto na caixa suspensa e clique em
   Ir.



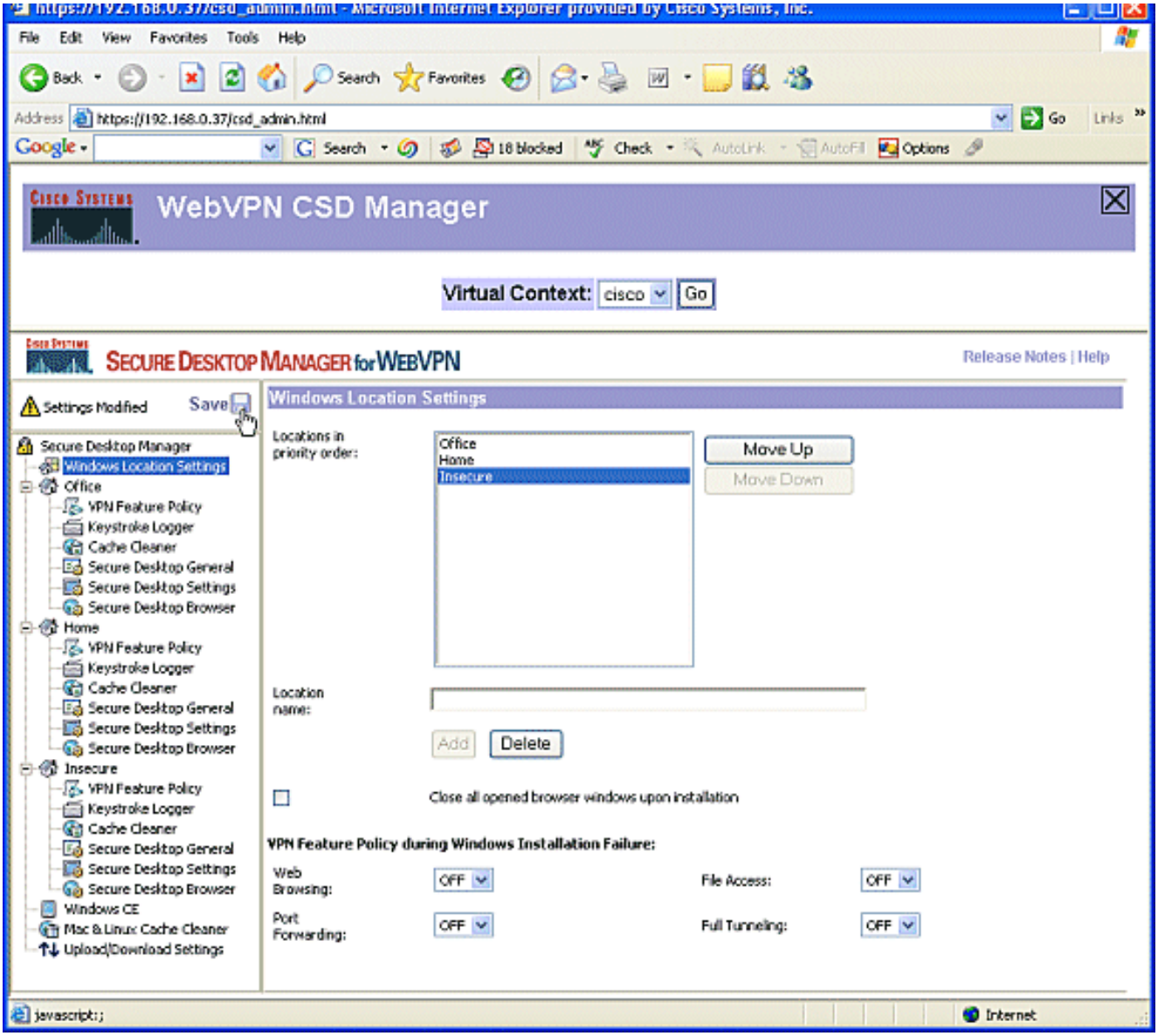
4. O Secure Desktop Manager para WebVPN é aberto.



5. No painel esquerdo, escolha **Configurações de local do Windows**.Coloque o cursor na caixa ao lado de Nome do local e insira um nome de local.Clique em Add.Neste exemplo, três nomes de local são mostrados: Office, Home e Insecure. Cada vez que um novo local é adicionado, o painel esquerdo se expande com os parâmetros configuráveis para esse local.



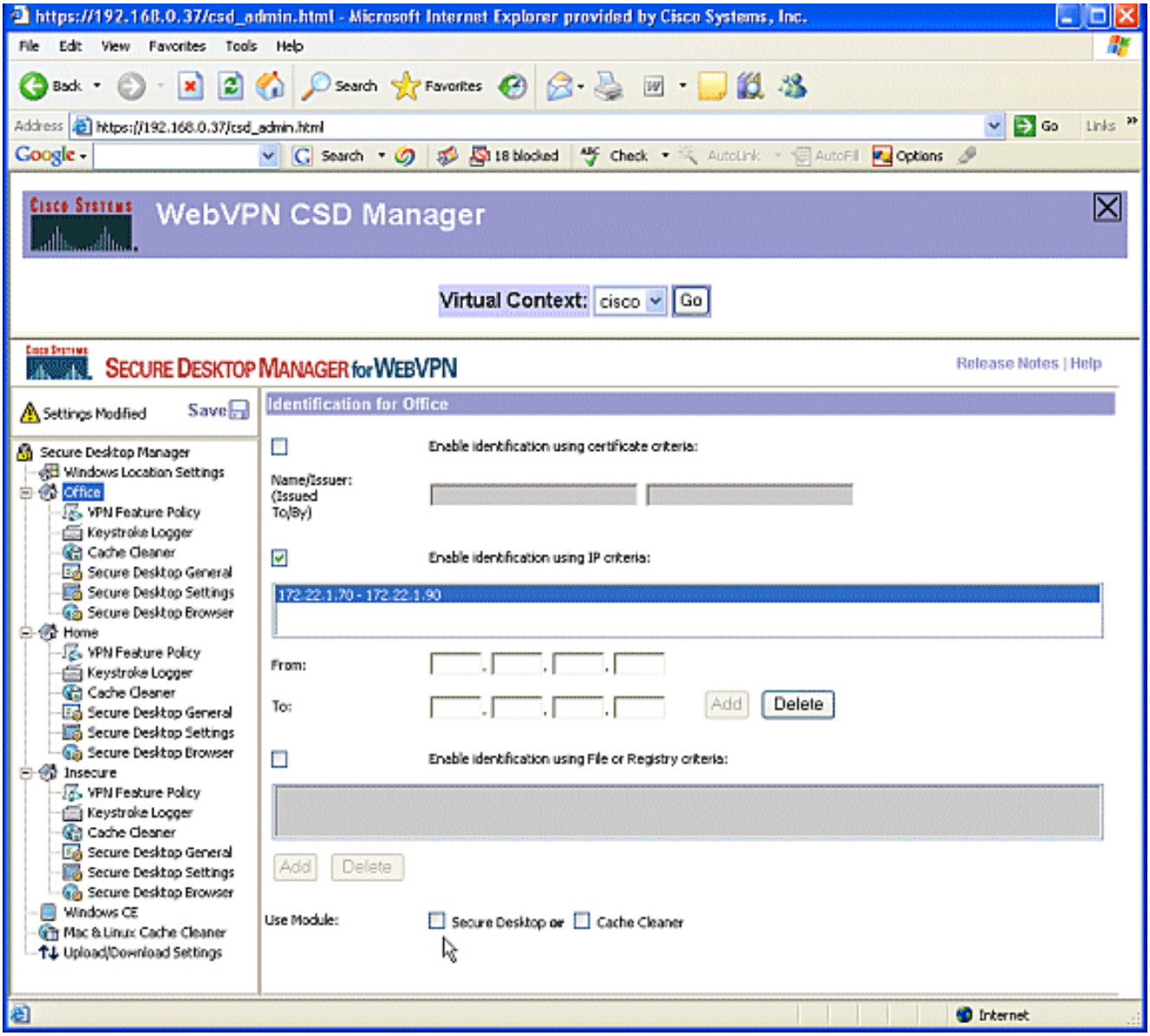
6. Depois de criar os locais do Windows, clique em **Salvar** na parte superior do painel esquerdo.**Observação:** salve suas configurações com frequência porque suas configurações serão perdidas se você for desconectado do navegador da Web.



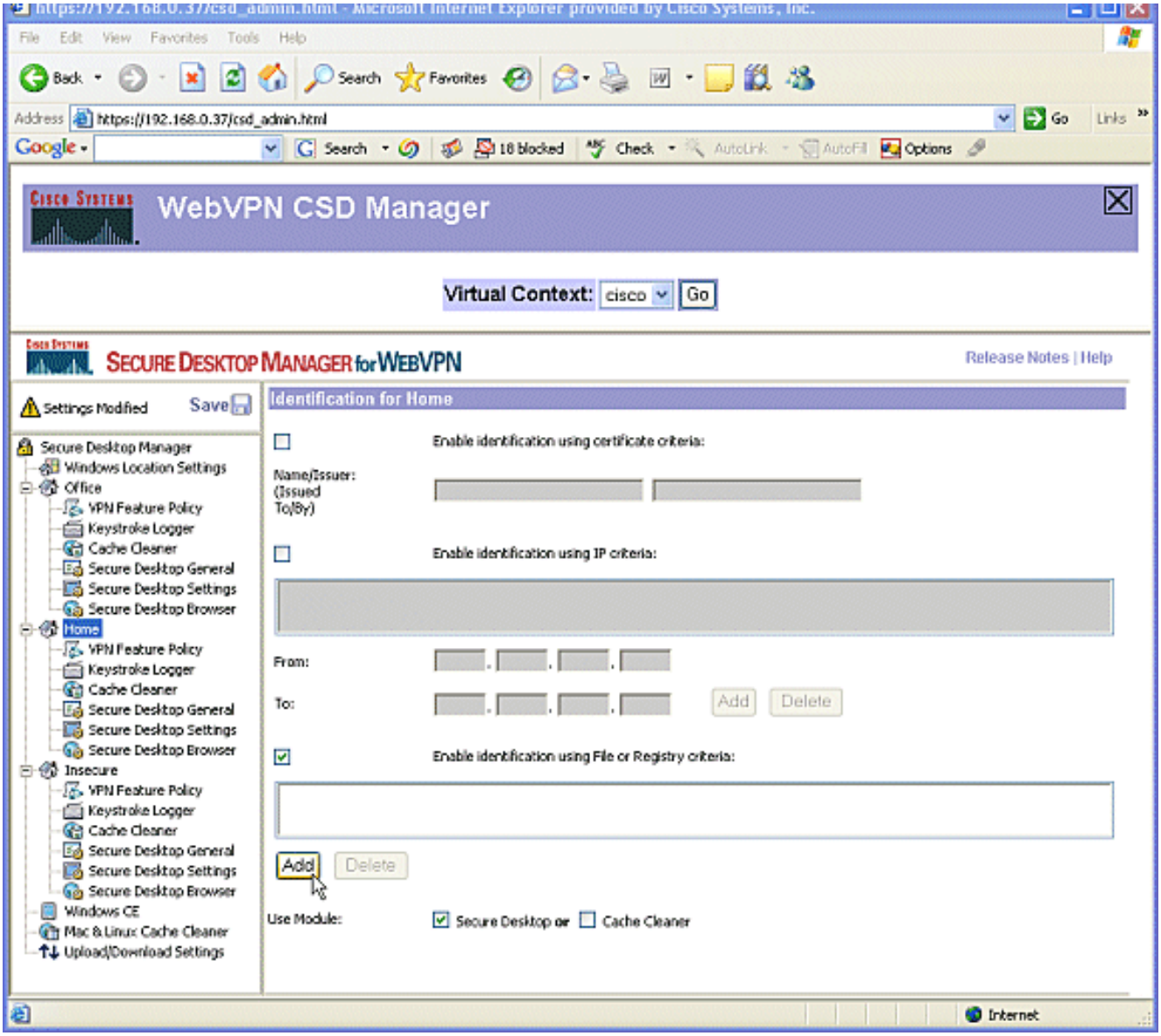
Fase II: Passo 2: Identificar critérios de localização

Para distinguir entre locais do Windows, atribua critérios específicos a cada local. Isso permite que a CSD determine quais de seus recursos aplicar a um local específico do Windows.

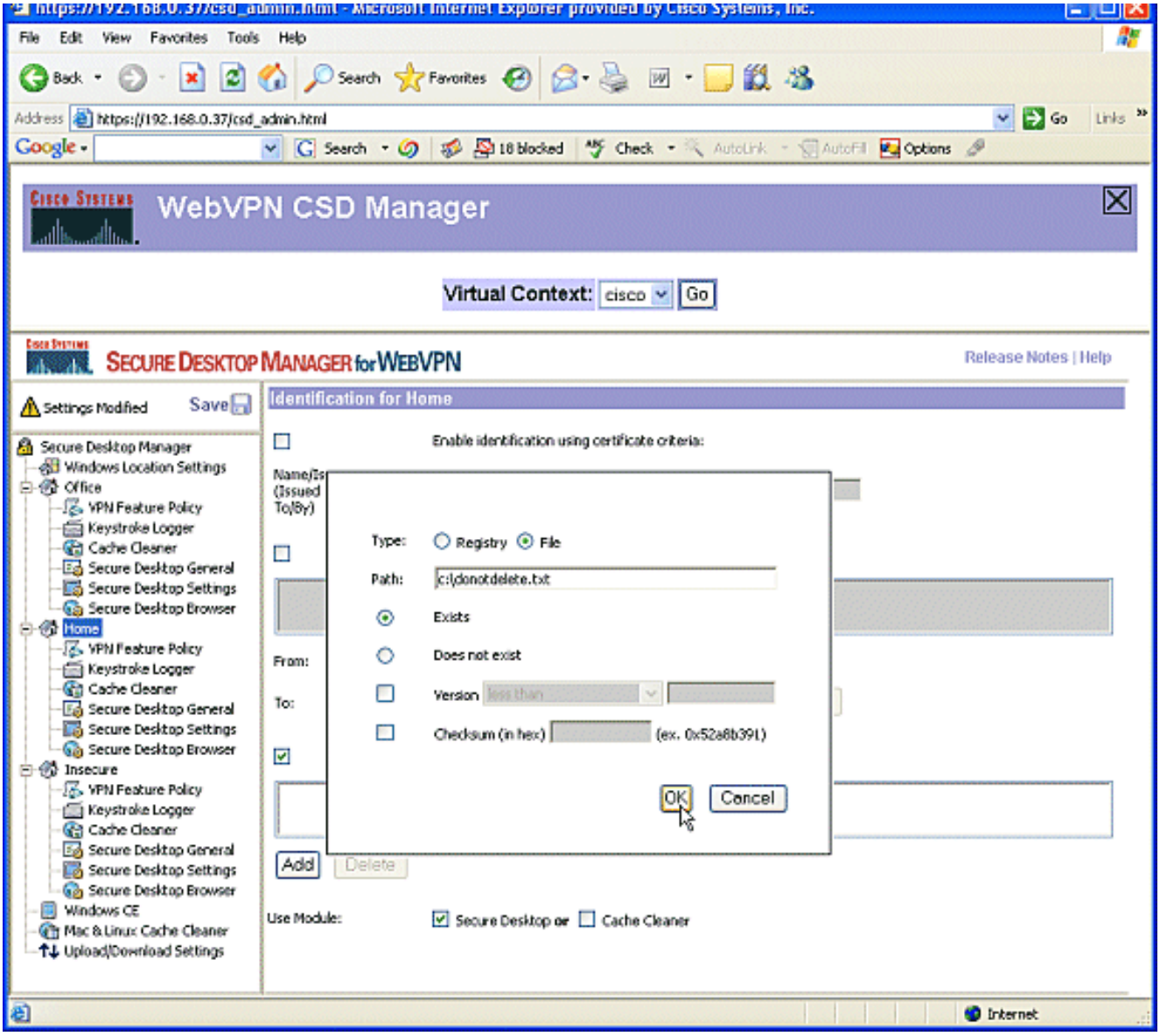
1. No painel esquerdo, clique em **Office**.Você pode identificar um local do Windows com critérios de certificado, critérios de IP, um arquivo ou critérios de registro. Você também pode escolher o Secure Desktop ou o Cache Cleaner para esses clientes. Como esses usuários são funcionários internos do escritório, identifique-os com critérios de IP.Insira os intervalos de endereços IP nas caixas **De** e **Para**.Clique em Add. Desmarque **Usar módulo: Desktop seguro**.Quando solicitado, clique em **Salvar** e clique em **OK**.



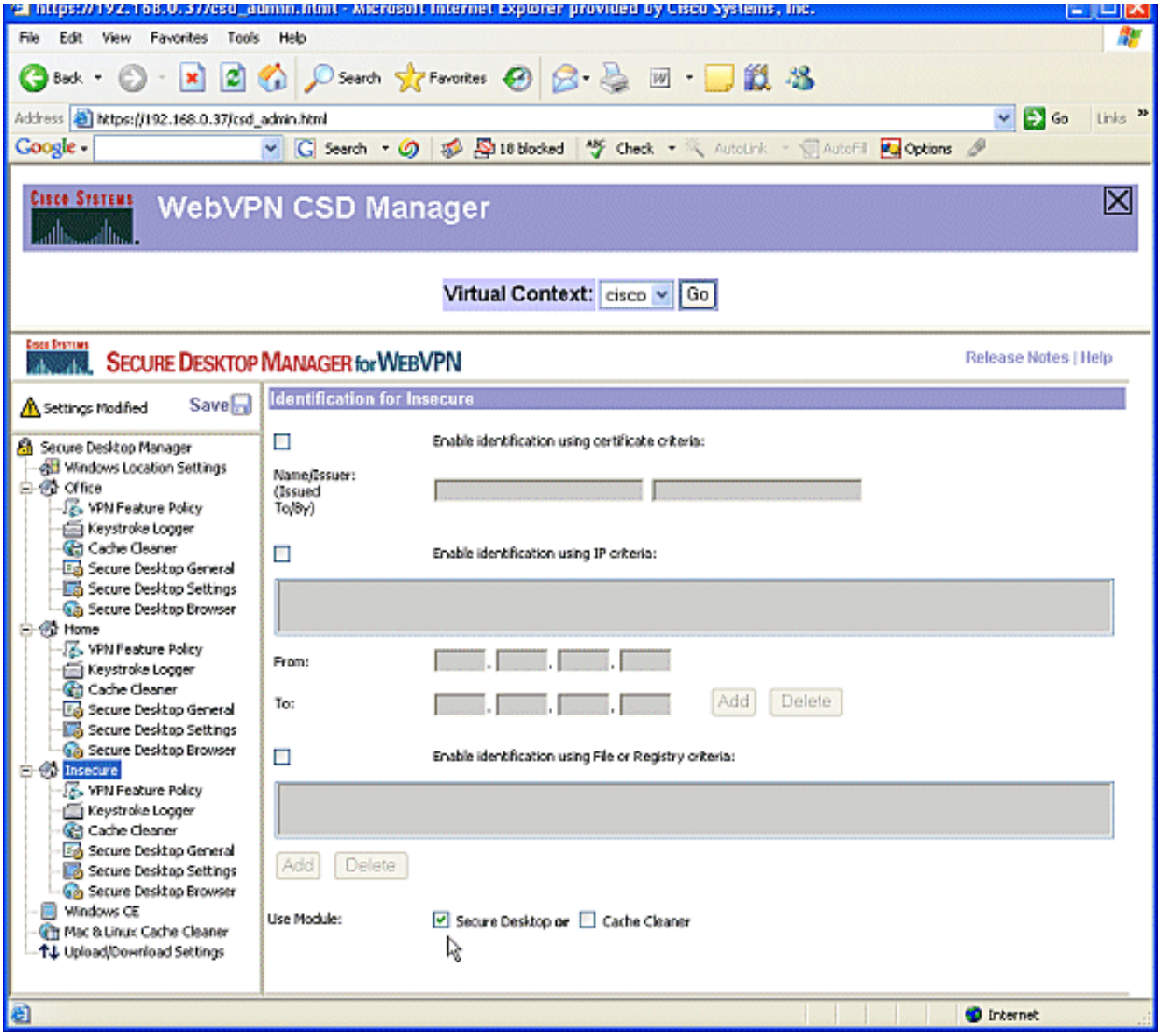
2. No painel esquerdo, clique na segunda opção Configuração de local do Windows **Home**.Certifique-se de **usar o módulo: Área de trabalho segura** marcada.Será distribuído um arquivo que identifica esses clientes. Você pode optar por distribuir certificados e/ou critérios de registro para esses usuários.Marque **Habilitar identificação usando os critérios de Arquivo ou Registro**.Clique em
Add.



3. Na caixa de diálogo, escolha **Arquivo** e digite o caminho para o arquivo.Este arquivo deve ser distribuído para todos os seus clientes domésticos.Verifique se o botão de opção **existe**.Quando solicitado, clique em **OK** e em **Salvar**.



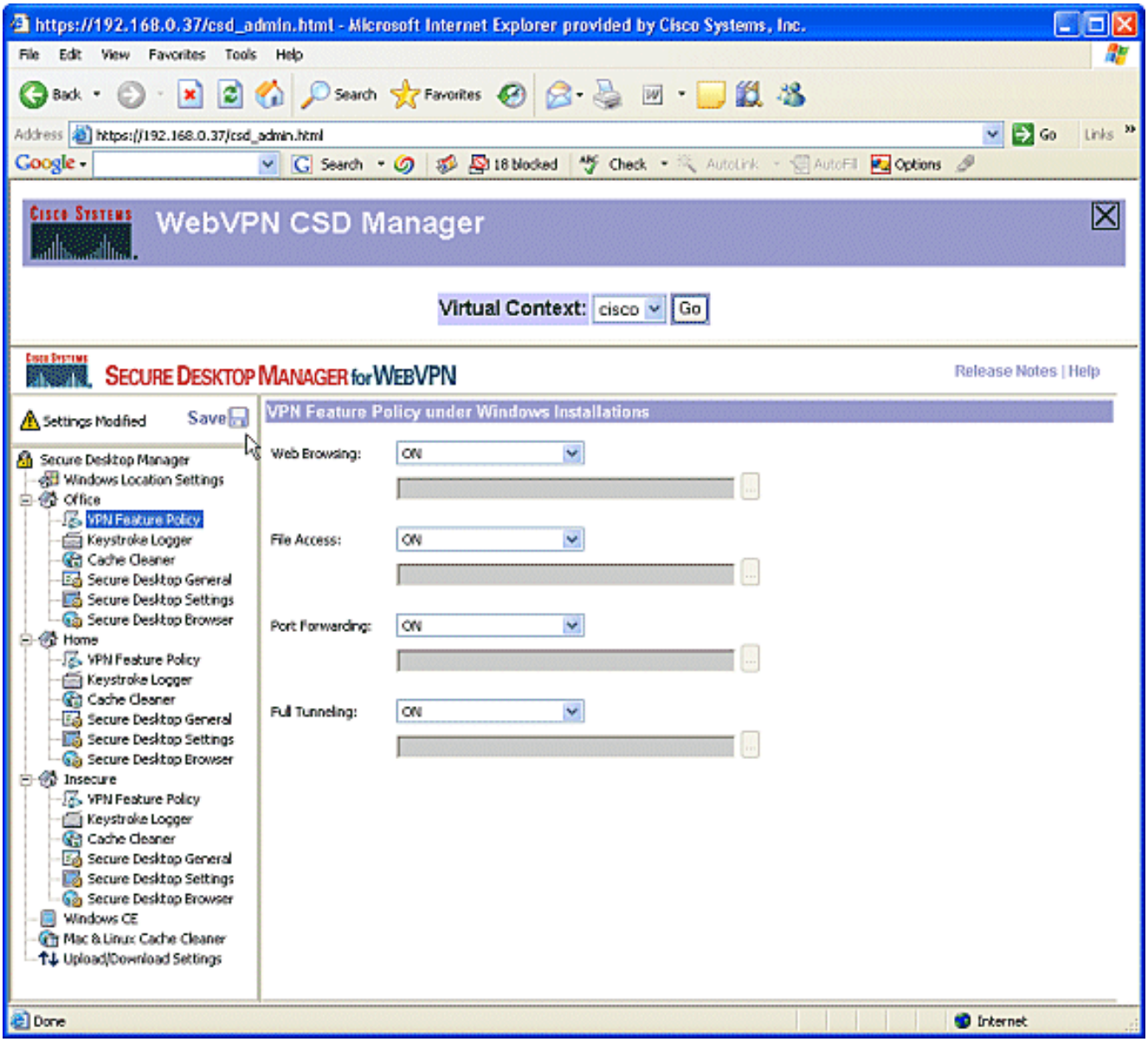
4. Para configurar a identificação de locais **inseguros**, simplesmente não aplique nenhum critério de identificação.Clique em **Insecure** no painel esquerdo.Deixe todos os critérios desmarcados.Marque **o módulo de uso: Desktop seguro**.Quando solicitado, clique em **Salvar** e clique em
OK.



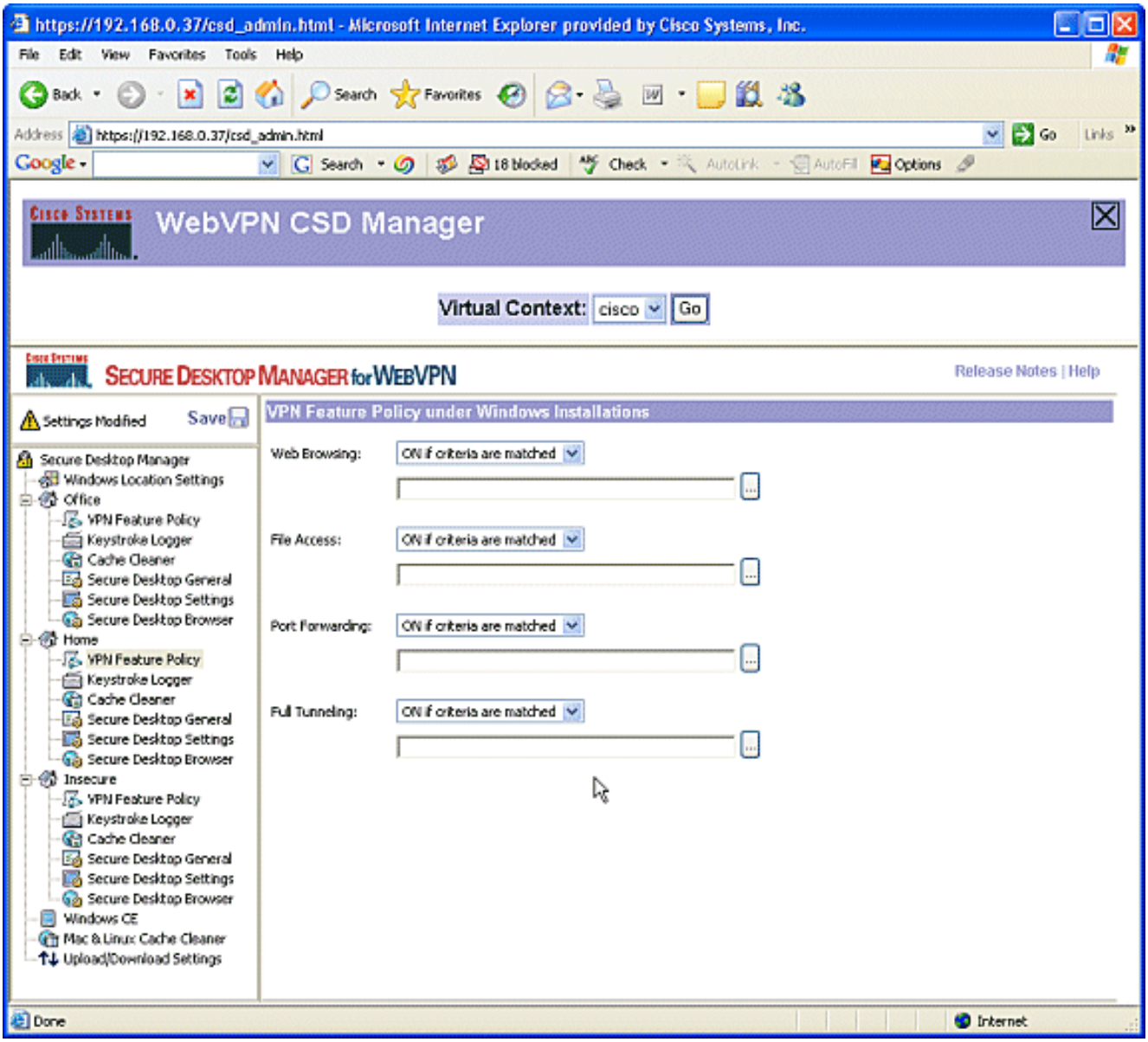
Fase II: Passo 3: Configurar módulos e recursos de localização do Windows.

Configure os recursos do CSD para cada local do Windows.

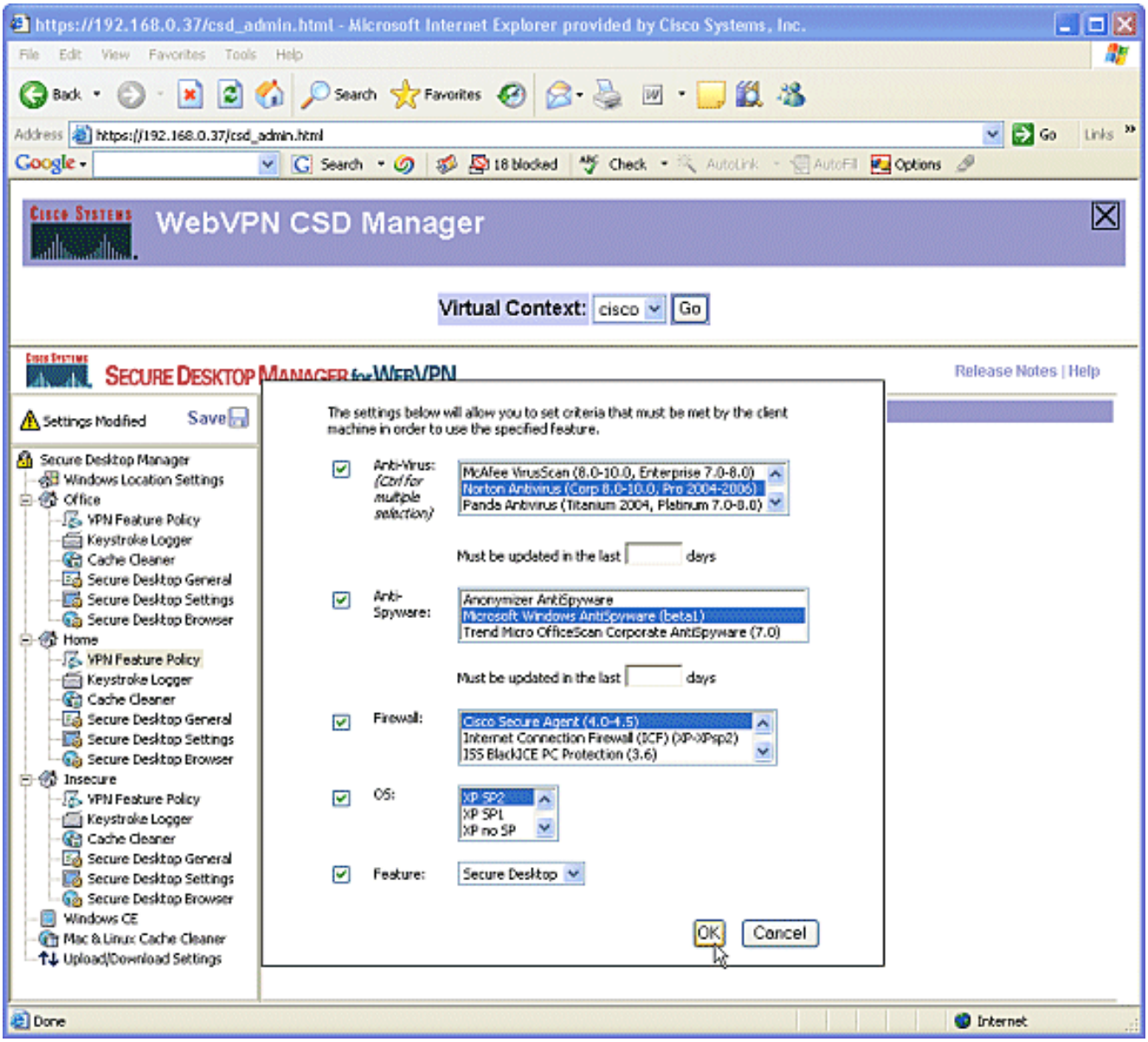
1. Em **Office**, clique em **VPN Feature Policy**. Como esses são clientes internos confiáveis, o CSD e o Cache Cleaner não foram habilitados. Nenhum dos outros parâmetros está disponível.



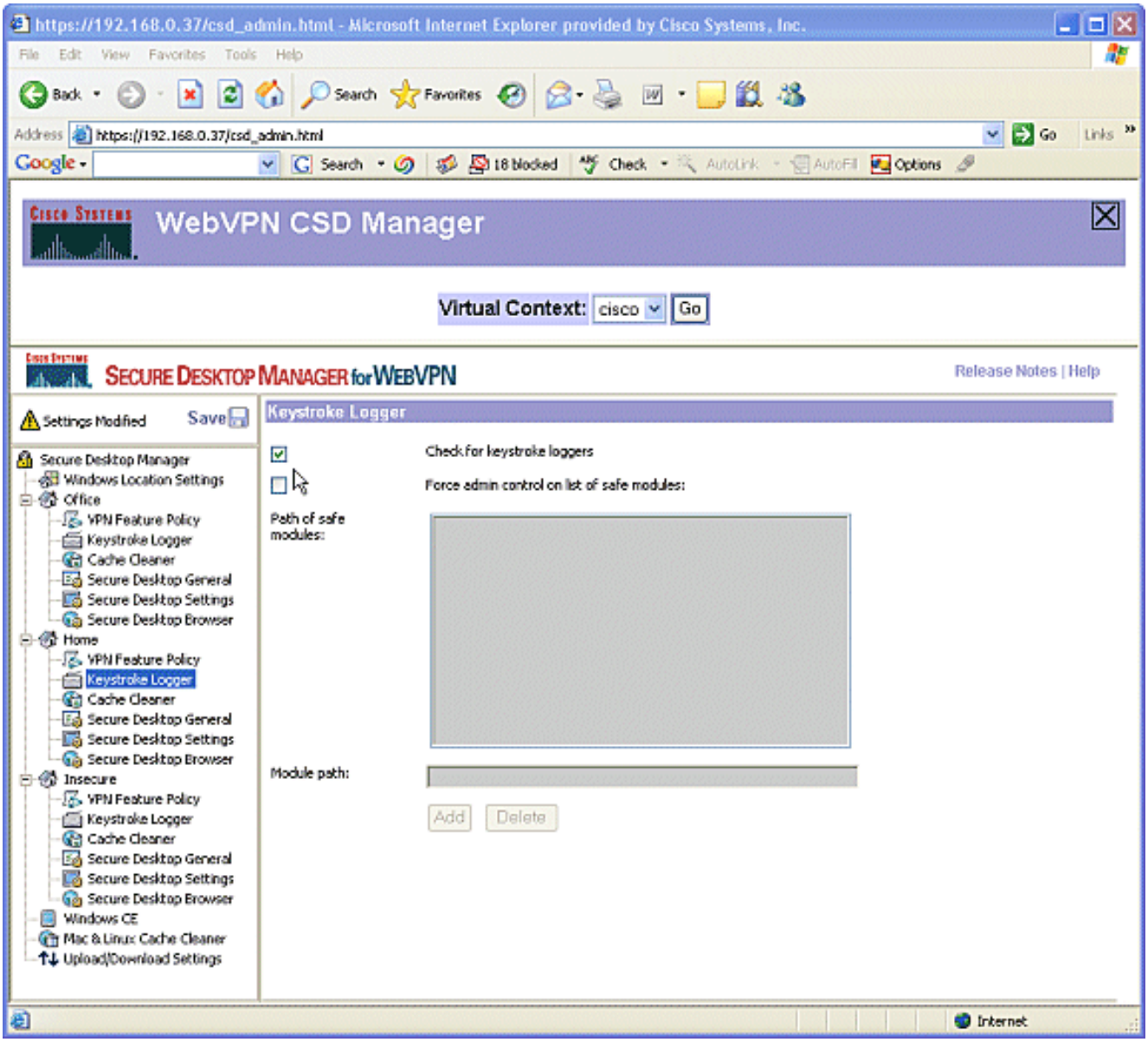
2. Ligue os recursos conforme mostrado.No painel esquerdo, escolha **Política de recursos de VPN** em **Início**.Os usuários domésticos terão acesso à LAN corporativa se os clientes atenderem a determinados critérios.Em cada método de acesso, escolha **ON se os critérios forem correspondentes**.



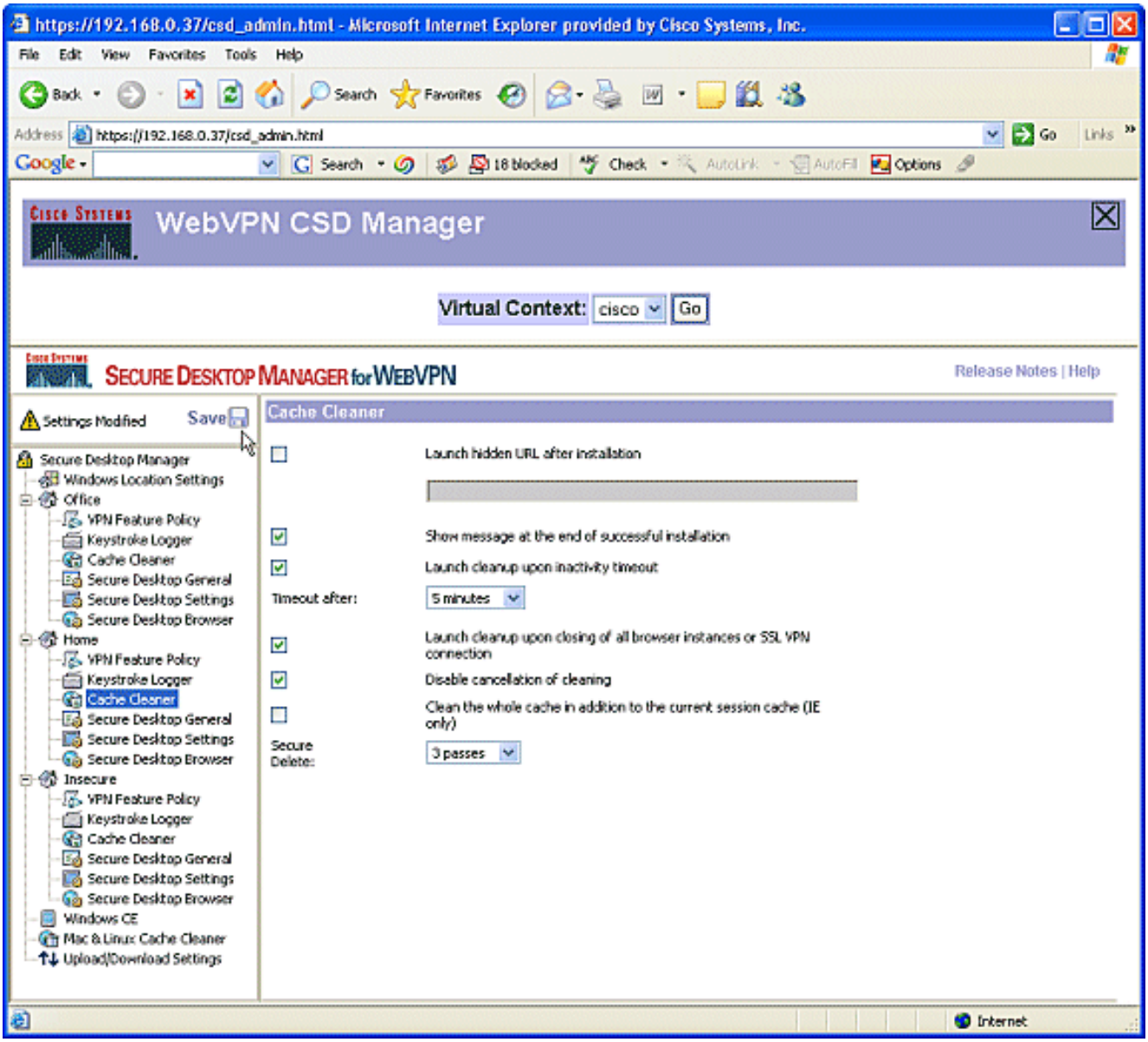
3. Para Navegação na Web, clique no botão de reticências e escolha os critérios que devem ser correspondentes. Clique em **OK** na caixa de diálogo.



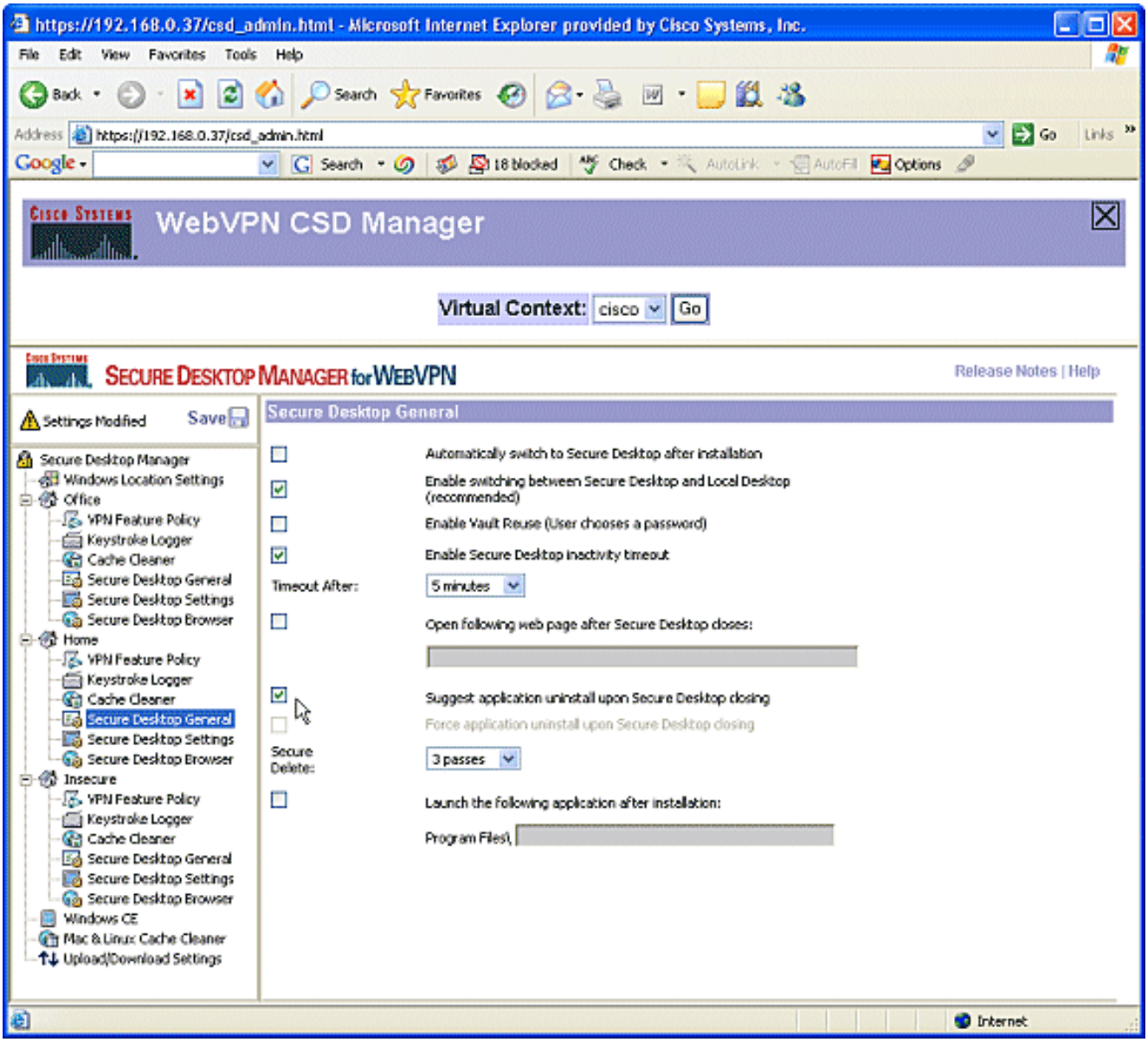
4. Você pode configurar os outros métodos de acesso de maneira semelhante.Em **Início**, escolha **Logger de pressionamento de tecla**.Coloque uma marca de seleção ao lado de **Verificar se há registradores de pressionamento de tecla**.Quando solicitado, clique em **Salvar** e clique em
OK.



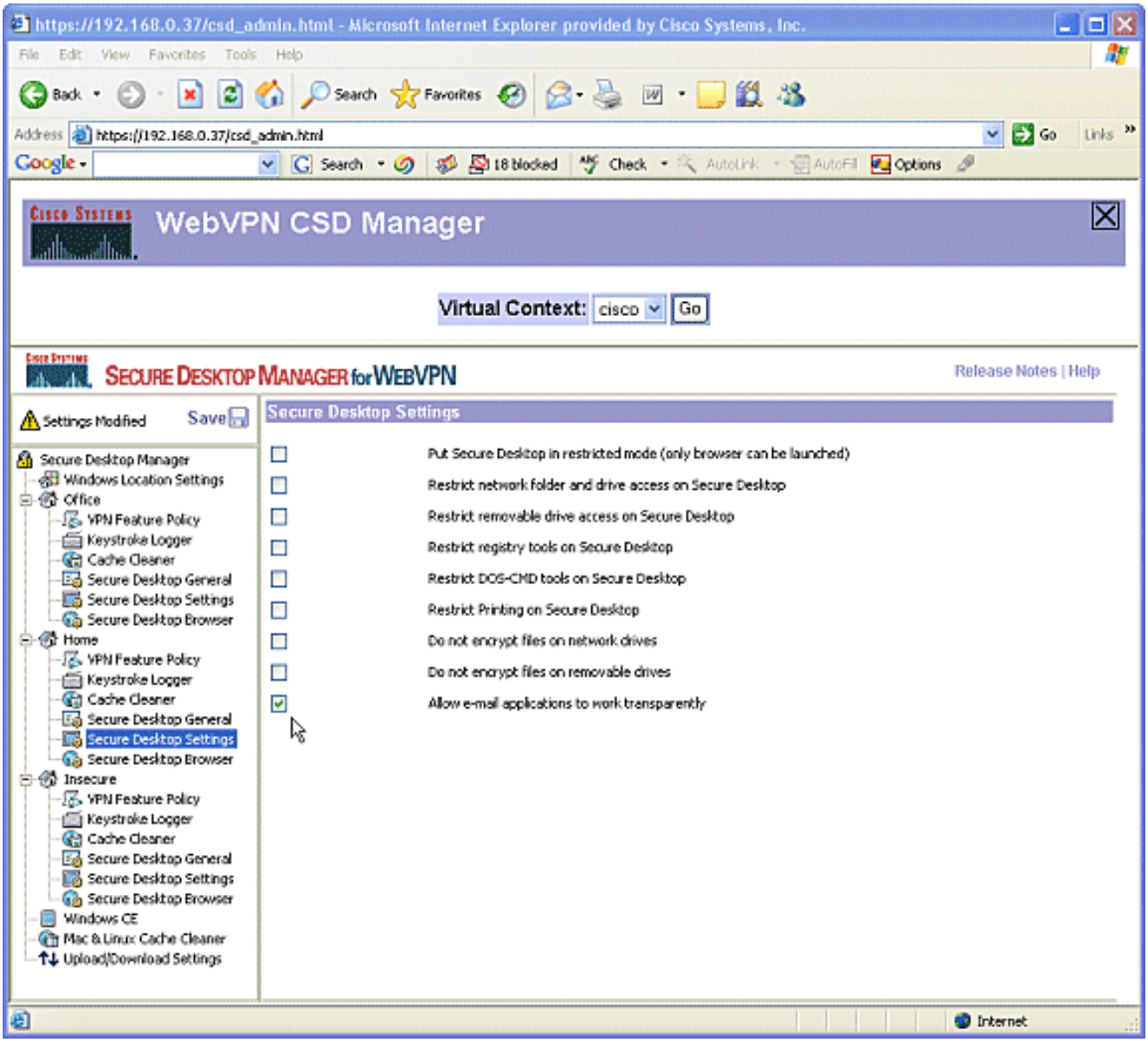
5. No local das janelas Home, escolha **Cache Cleaner**. Deixe as configurações padrão como mostrado na captura de
tela.



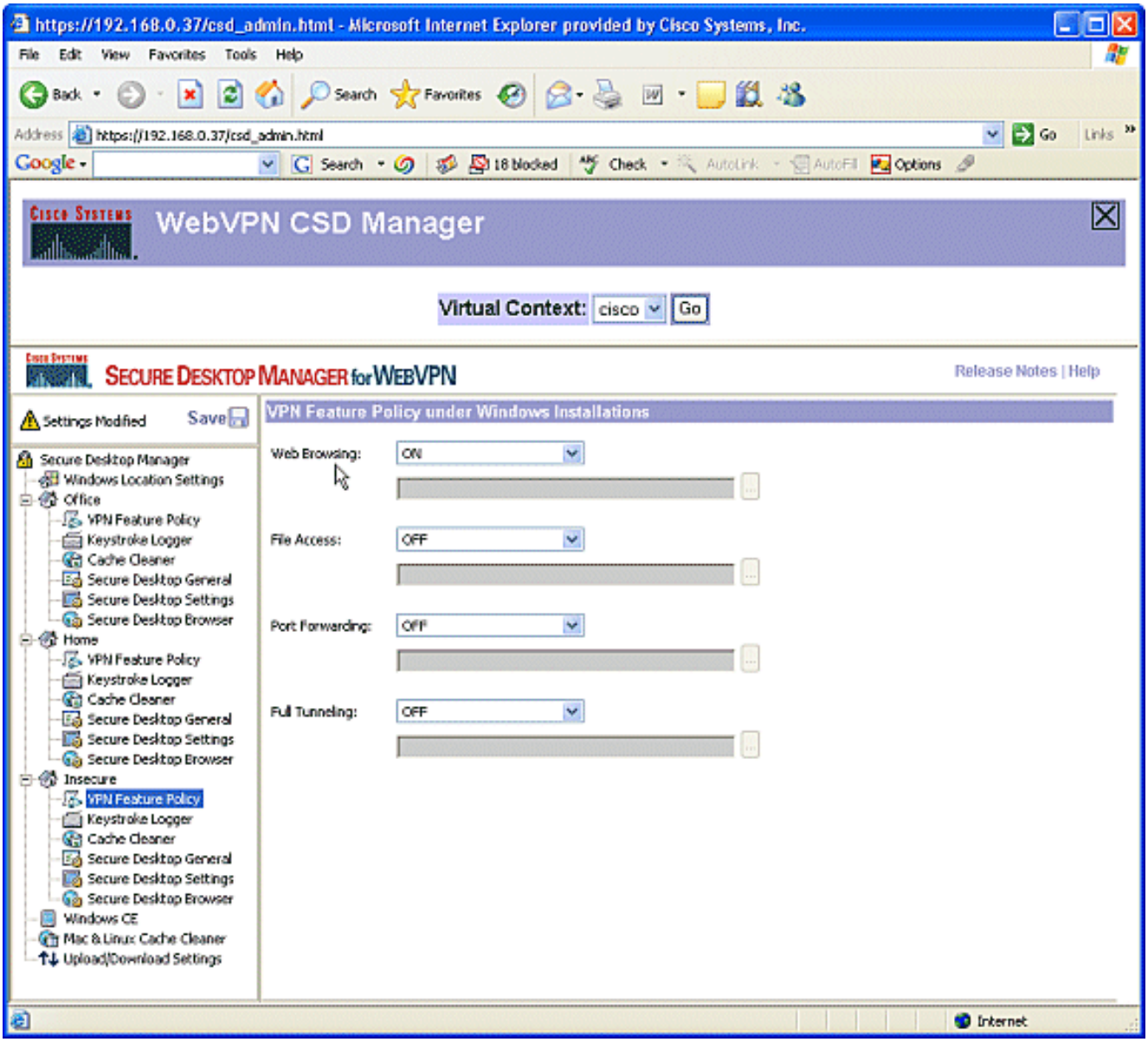
6. Em Home (Casa), escolha **Secure Desktop General**. Marque **Sugerir desinstalação do aplicativo ao fechar o Secure Desktop**. Deixe todos os outros parâmetros com suas configurações padrão, conforme mostrado na captura de tela.



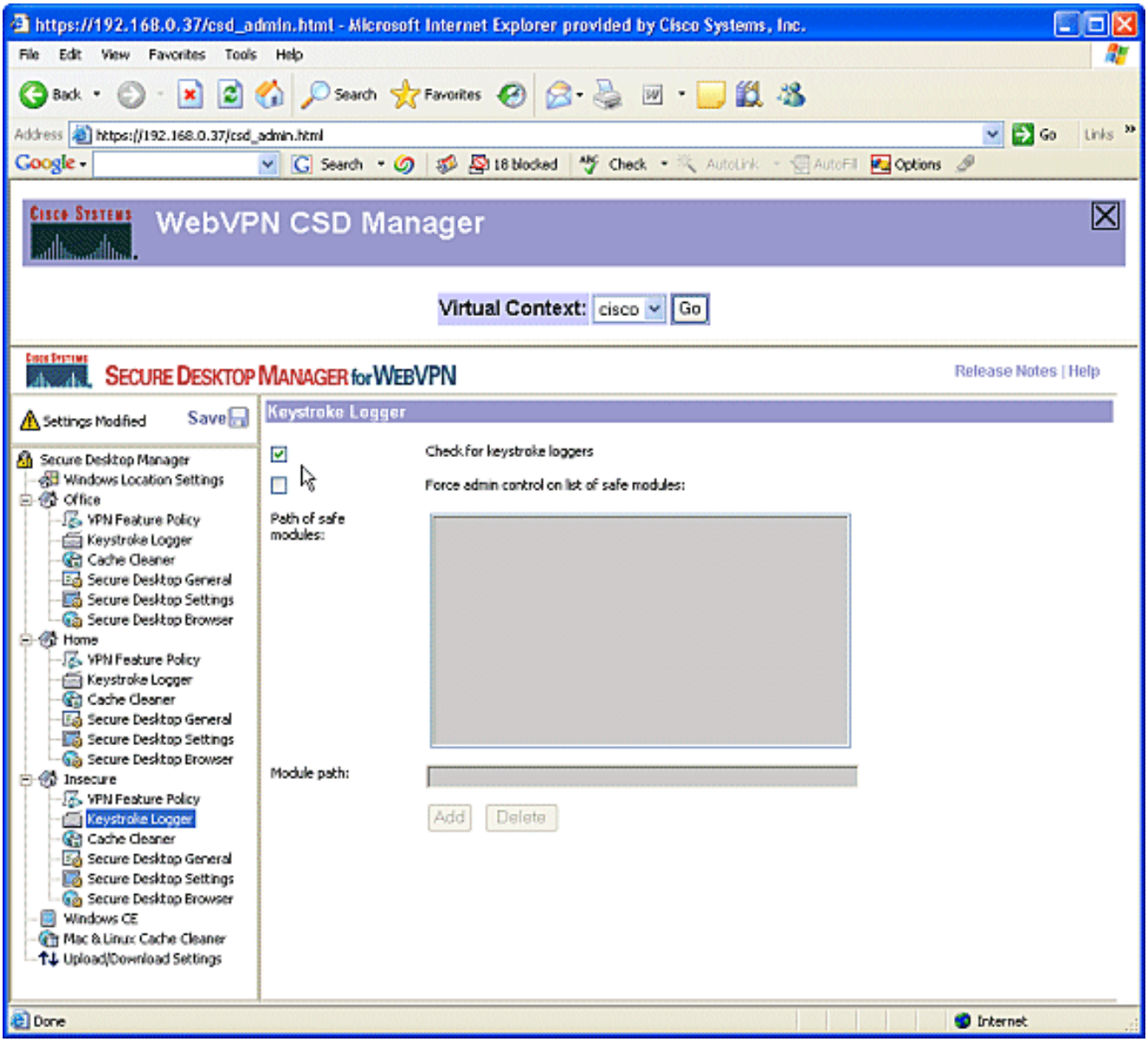
7. Para Configurações seguras da área de trabalho em Casa, escolha **Permitir que aplicativos de e-mail funcionem de forma transparente**. Quando solicitado, clique em **Salvar** e clique em **OK**.



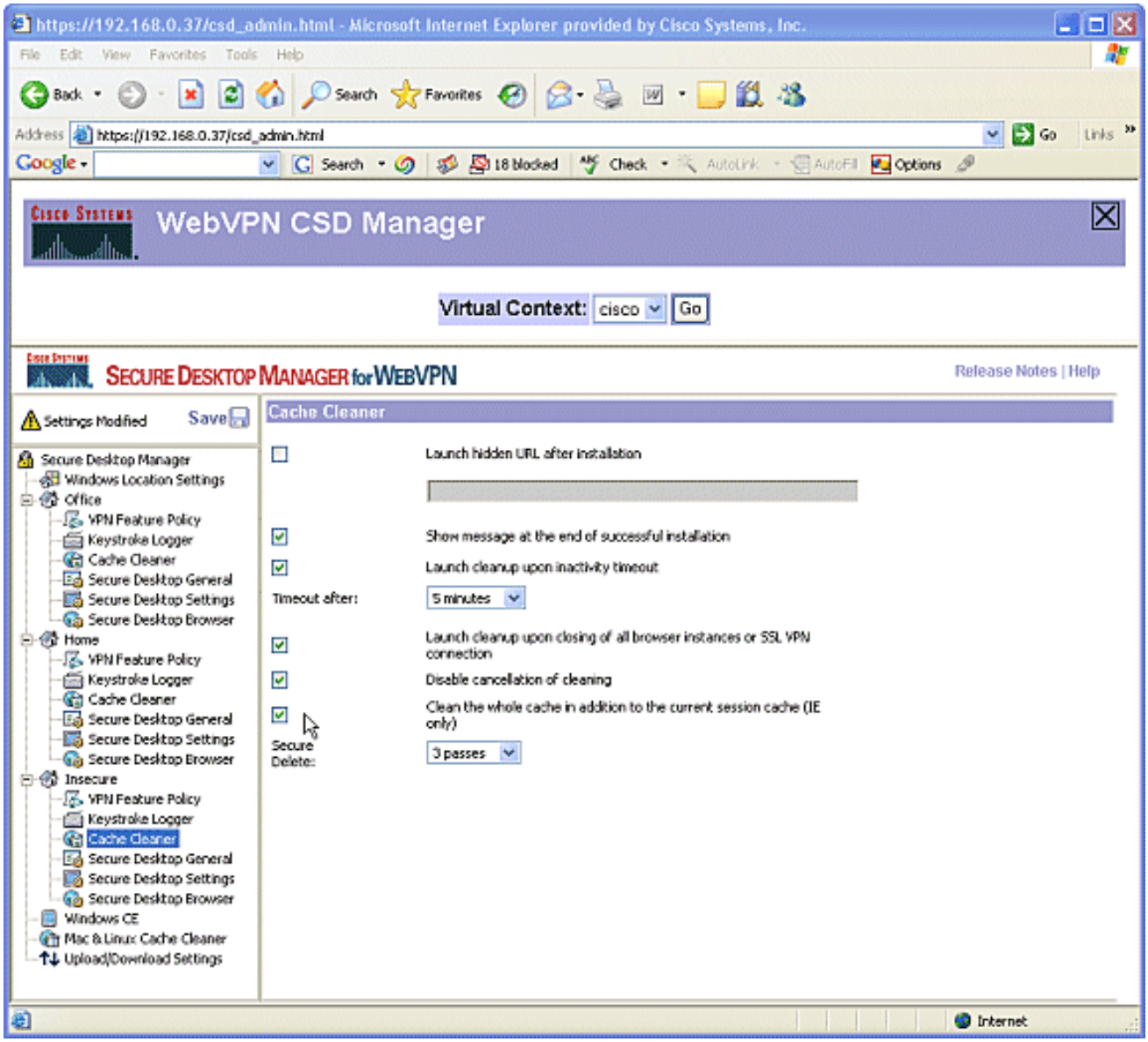
8. A configuração do **navegador de desktop seguro** depende se você deseja ou não que esses usuários acessem um site da empresa com favoritos pré-configurados.Em Inseguro, escolha **Política de recursos de VPN**.Como não são usuários confiáveis, permita somente a navegação na Web.Escolha **ON** no menu suspenso para **Navegação na Web**.Todos os outros acessos estão definidos como **DESLIGADO**.



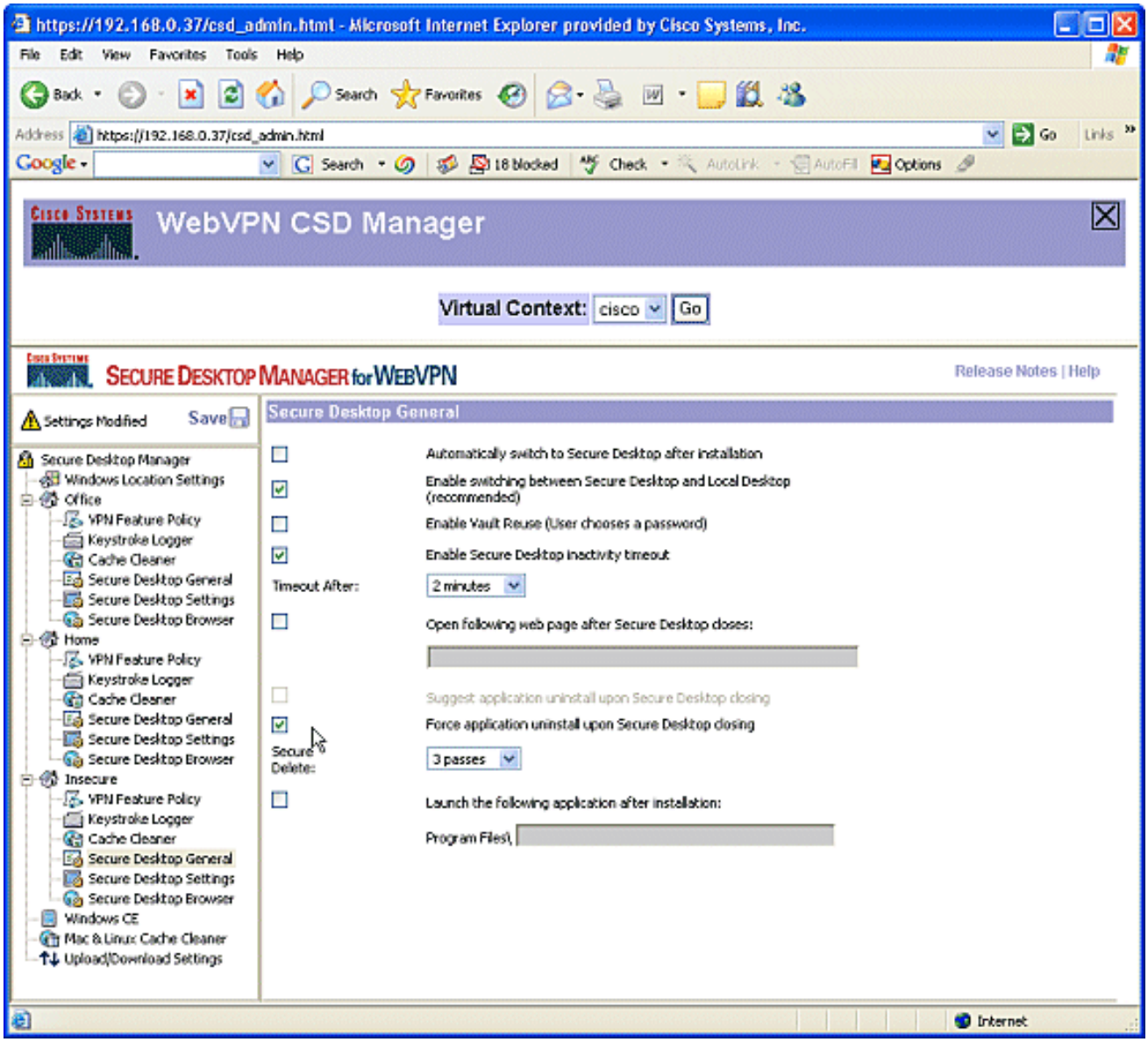
9. Marque a caixa de seleção **Verificar se há registros de pressionamento de tecla**.



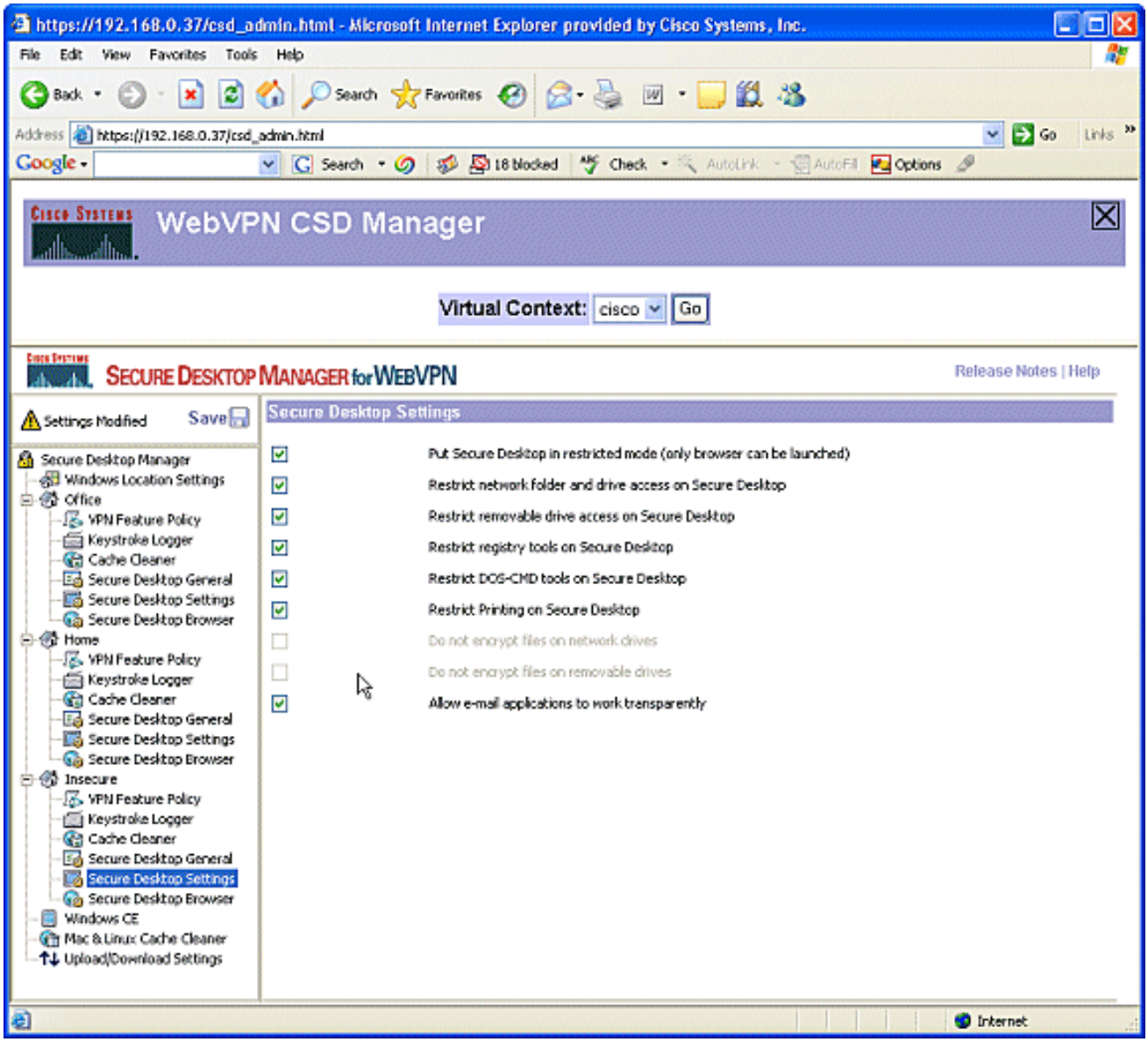
10. Configure o Cache Cleaner para Inseguro.Marque a caixa de seleção **Limpar o cache inteiro além do cache de sessão atual (somente IE)**.Deixe as outras configurações em seus padrões.



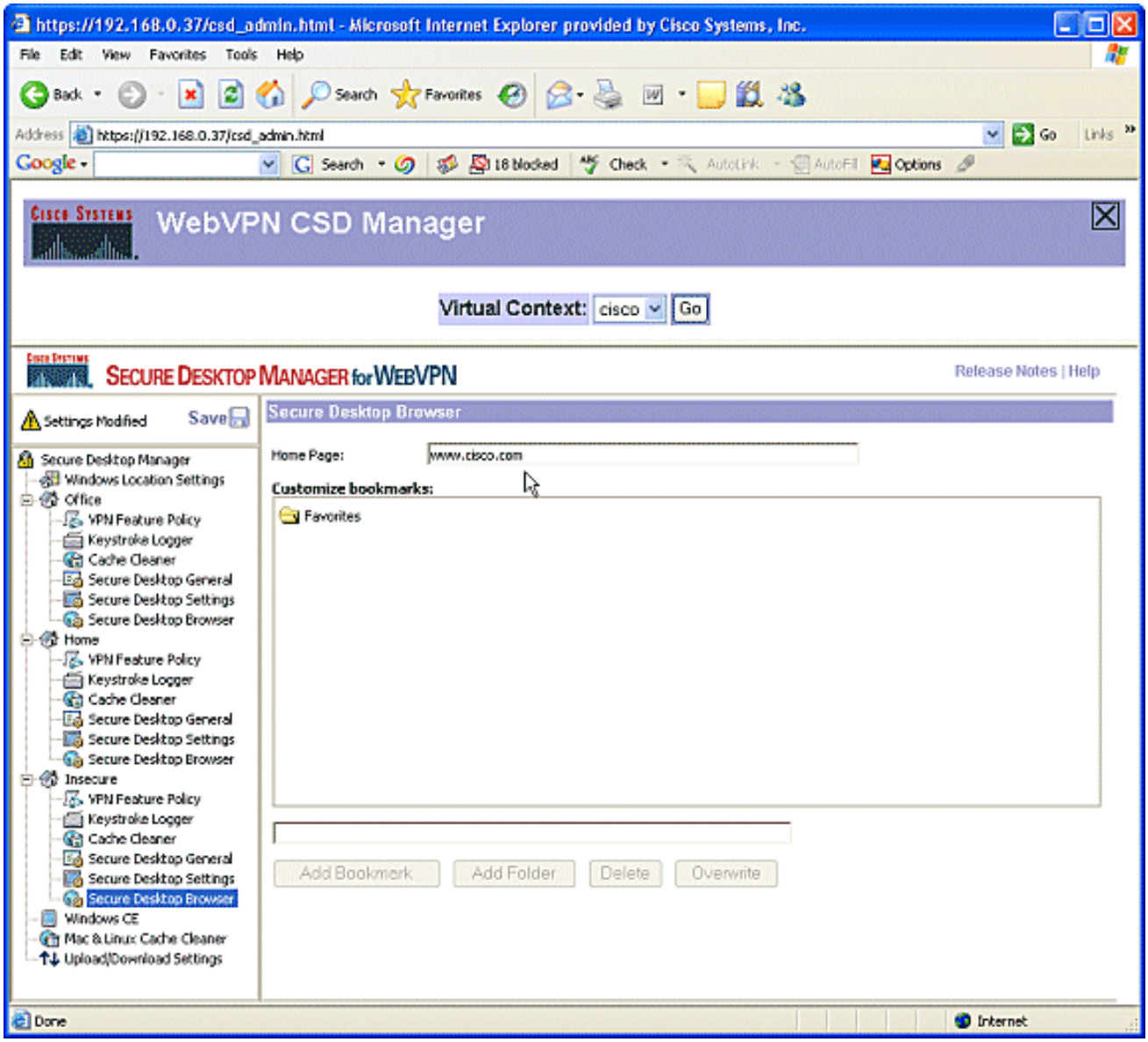
11. Em Insecure, escolha **Secure Desktop General**.Reduza o tempo limite de inatividade para 2 minutos.Marque a caixa de seleção **Forçar desinstalação do aplicativo ao fechar o Secure Desktop**.



12. Escolha **Configurações de desktop seguras** em Inseguro e defina configurações muito restritivas como
mostrado.



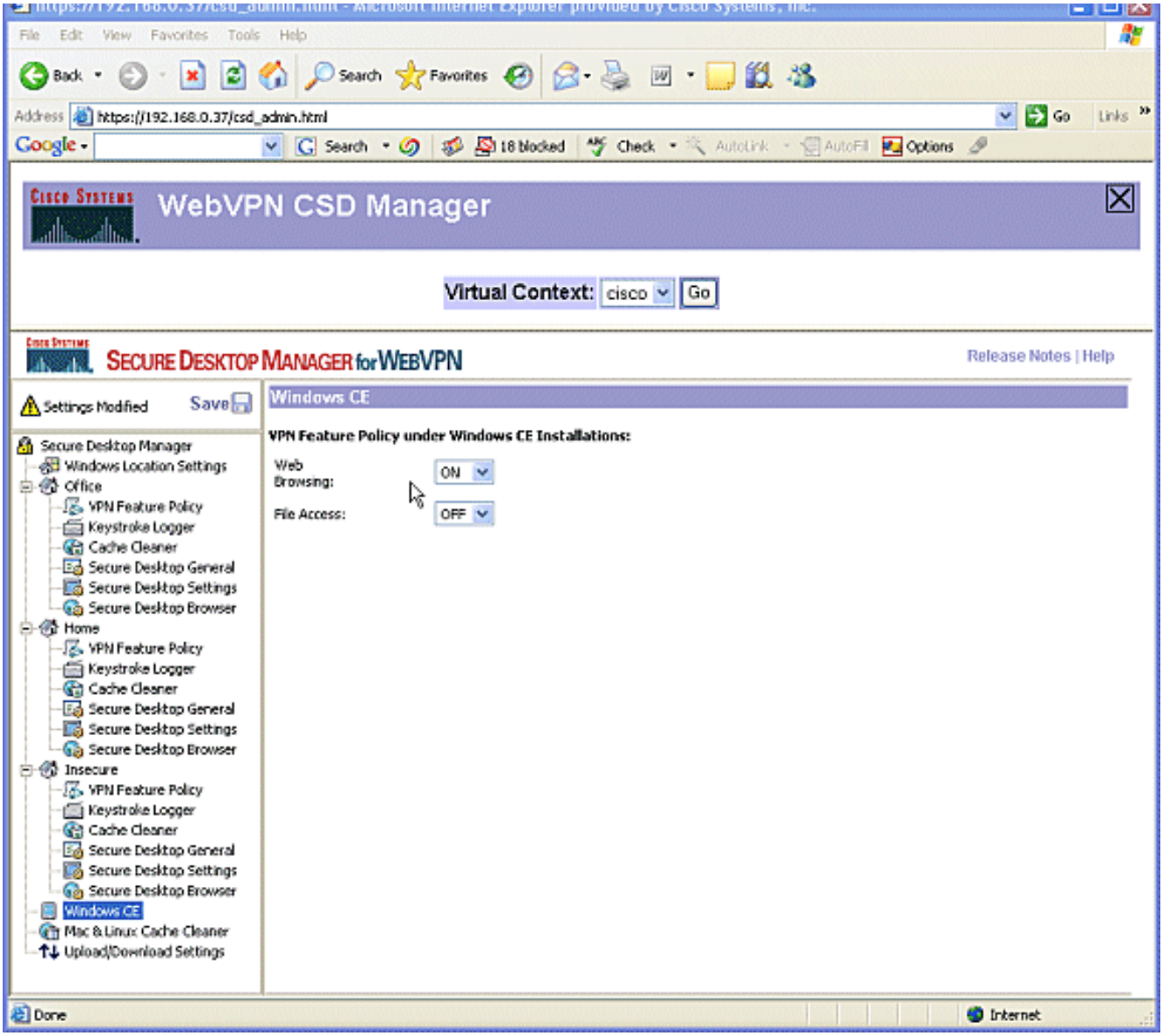
13. Escolha **Navegador de desktop seguro**. No campo Página inicial, digite o site para o qual esses clientes serão direcionados para sua página inicial.



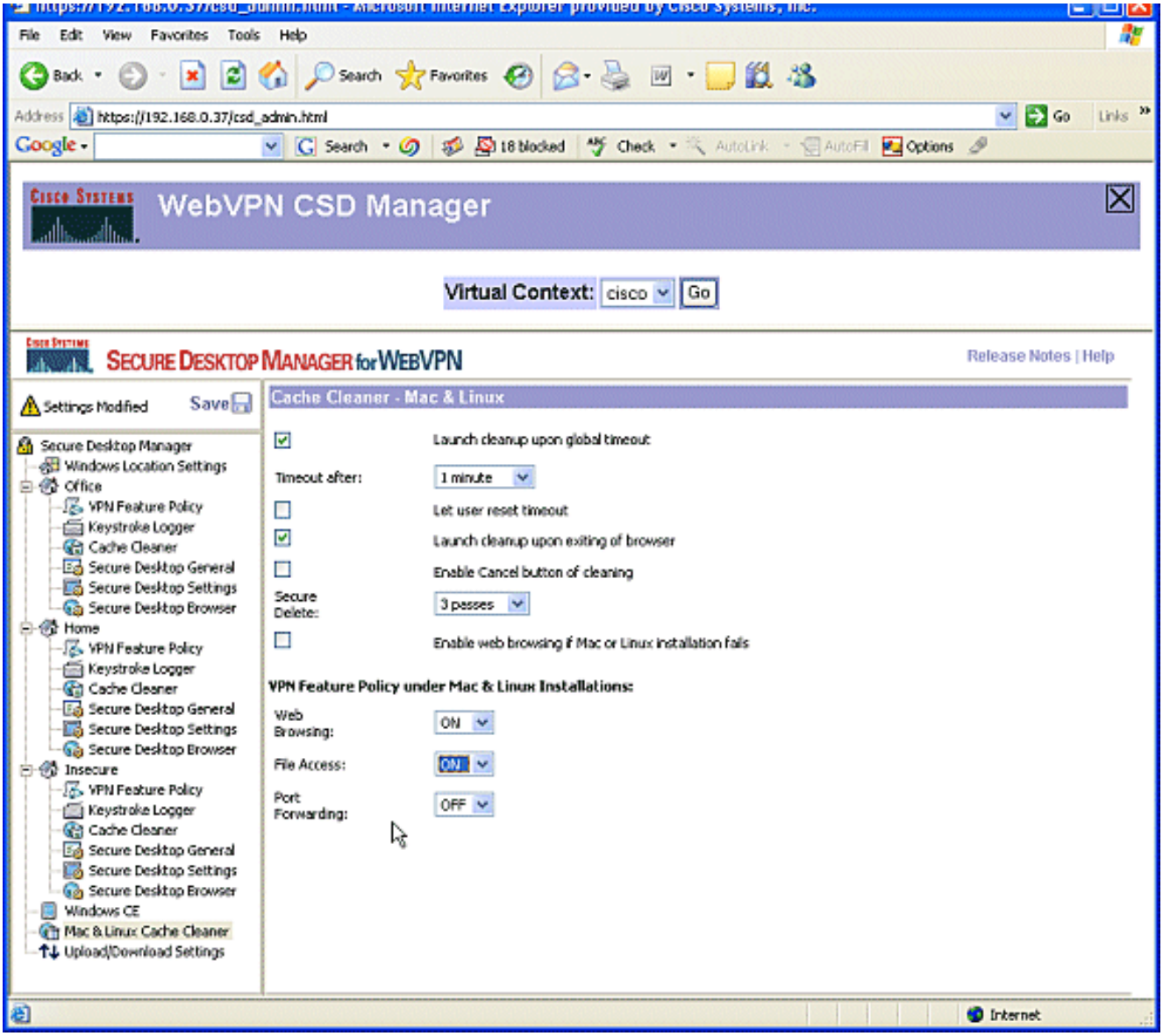
Fase II: Passo 4: Configure os recursos do Windows CE, Macintosh e Linux.

Configure os recursos do CSD para Windows CE, Macintosh e Linux.

1. Escolha **Windows CE** em Secure Desktop Manager. O Windows CE tem recursos VPN limitados. Ative **a navegação na Web**.



2. Escolha **Limpeza de Cache Mac & Linux**.Os sistemas operacionais Macintosh e Linux têm acesso apenas aos aspectos mais limpos do cache do CSD. Configure-os conforme mostrado no gráfico.Quando solicitado, clique em **Salvar** e clique em **OK**.

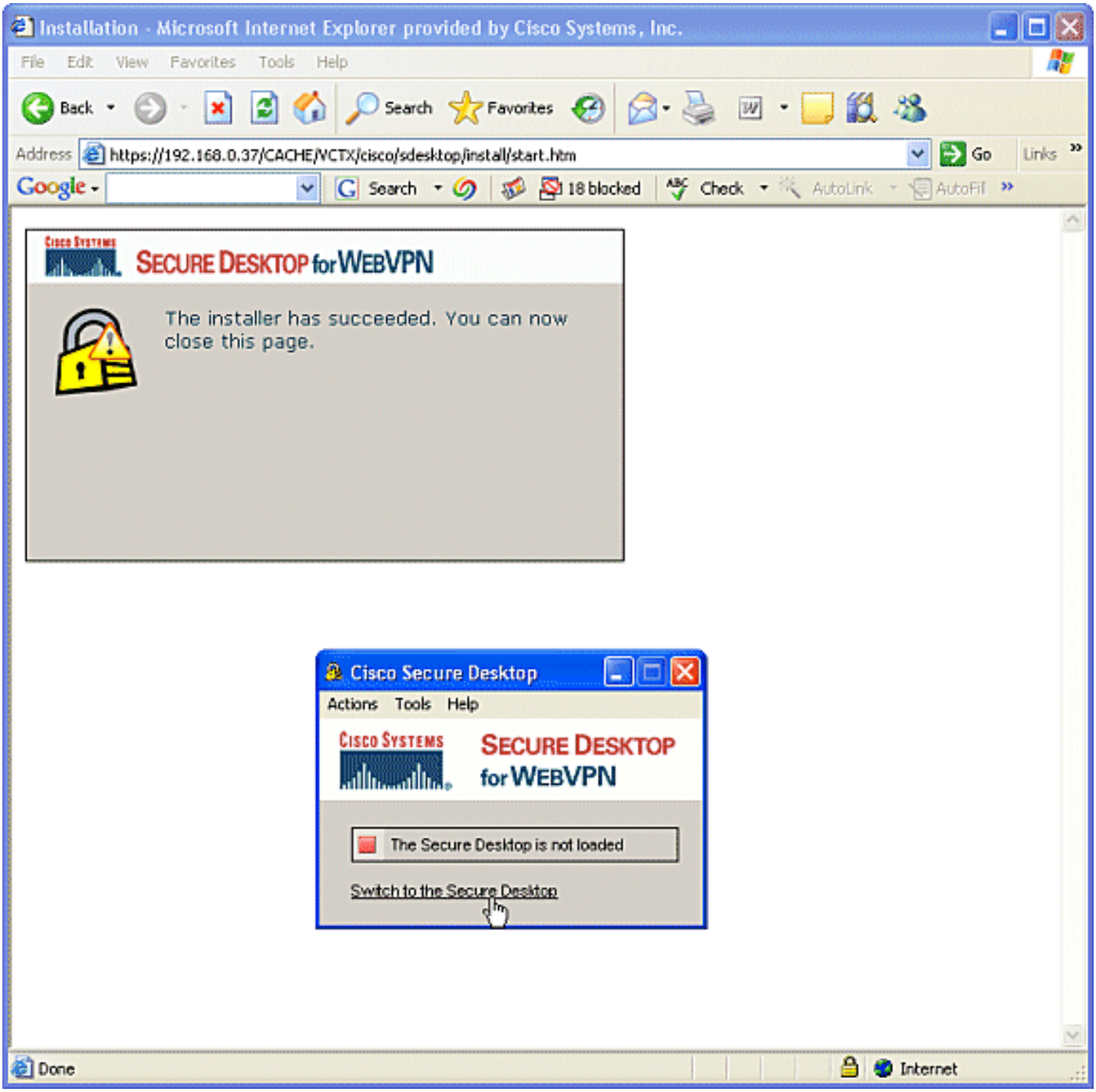


Verificar

Testar a Operação da CDT

Teste a operação do CSD conectando-se ao gateway WebVPN com um navegador habilitado para SSL no endereço **https://WebVPN_Gateway_IP**.

Observação: lembre-se de usar o nome exclusivo do contexto se você criou contextos WebVPN diferentes, por exemplo, **https://192.168.0.37/cisco**.



Comandos

Vários **comandos show estão associados ao WebVPN.** Você pode executar estes comandos na interface de linha de comando (CLI) para mostrar estatísticas e outras informações. Para obter informações detalhadas sobre os **comandos show, consulte** Verificação da Configuração do WebVPN.

Observação: o CLI Analyzer (somente clientes registrados) suporta determinados comandos **show**. Use o Analisador CLI para exibir uma análise da saída do comando **show**.

Troubleshoot

Comandos

Vários **comandos debug estão associados ao WebVPN.** Para obter informações detalhadas sobre estes comandos, consulte Uso de Comandos de Depuração do WebVPN.

Observação: o uso de comandos **debug** pode afetar adversamente seu dispositivo Cisco. Antes de utilizar **comandos debug, consulte** Informações Importantes sobre Comandos Debug.

Para obter mais informações sobre os comandos **clear**, consulte Utilização de comandos WebVPN Clear.

Informações Relacionadas

- Guia de Implantação de WebVPN e Convergência DMVPN
- SSL VPN - WebVPN
- Cisco IOS SSLVPN
- Suporte Técnico e Documentação - Cisco Systems