Exemplo de Configuração de VPN SSL Sem Clientes (WebVPN) no Cisco IOS com SDM

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Diagrama de Rede
Convenções
Tarefas de Pré-configuração
Configurar a WebVPN no Cisco IOS
Passo 1. Configurar o Gateway WebVPN
Passo 2. Configurar os Recursos Permitidos para o Grupo de Políticas
Passo 3. Configurar o Grupo de Políticas WebVPN e Selecionar os Recursos
Passo 4. Configurar o Contexto WebVPN
Passo 5. Configurar o Banco de Dados de Usuários e o Método de Autenticação
Resultados
Verificar
Procedimento
Comandos
Troubleshooting
Procedimento
Comandos
Informações Relacionadas

Introdução

As VPNs SSL sem clientes (WebVPN) permitem que um usuário acesse recursos de forma segura na LAN corporativa de qualquer lugar com um navegador Web habilitado para SSL. Primeiro, o usuário autentica com um gateway WebVPN que permitirá o seu acesso a recursos de rede pré-configurados. Os gateways WebVPN podem ser configurados no Roteadores do ® do Cisco IOS, nas ferramentas de segurança adaptáveis de Cisco (ASA), nos concentradores do Cisco VPN 3000, e no Módulo de serviços de Cisco WebVPN para os Catalyst 6500 e 7600 Router.

A tecnologia Virtual Private Network (VPN) Secure Socket Layer (SSL) pode ser configurada em dispositivos Cisco em três modos principais: VPN SSL Sem Clientes (WebVPN), VPN SSL Thin-Client (Encaminhamento de Portas), e Cliente VPN SSL (modo SVC). Este documento demonstra a configuração da WebVPN em Cisco IOS Routers.

Nota: Não altere o nome do domínio IP ou o nome de host do roteador, pois isso acionará uma regeneração do certificado autoassinado e substituirá o ponto de confiança configurado. A regeneração do certificado autoassinado utilizará problemas de conexão se o roteador tiver sido configurado para WebVPN. A WebVPN vincula o nome do ponto de confiança SSL à configuração de gateway WebVPN. Portanto, se um certificado autoassinado novo for emitido, o nome novo do ponto de confiança não corresponderá à configuração da WebVPN e os usuários não conseguirão conectar.

Nota: Se você executar o **comando ip https-secure server** em um roteador WebVPN que use um certificado autoassinado persistente, uma nova chave RSA será gerada e o certificado se tornará inválido. Um novo ponto de confiança será criado, o que quebra a WebVPN SSL. Se o roteador que usa o certificado autoassinado persistente reinicializar após você executar o **comando ip https-secure server**, o mesmo problema ocorrerá.

Consulte o Exemplo de Configuração do IOS da VPN SSL Thin-Client (WebVPN) com SDM para obter mais informações sobre a VPN SSL thin-client.

Consulte o Exemplo de Configuração de Cliente VPN SSL (SVC) no IOS com SDM para obter mais informações sobre o Cliente VPN SSL.

A VPN SSL pode ser executada nestas plataformas de Cisco Routers:

- Cisco 870, 1811, 1841, 2801, 2811, 2821 e 2851 Series Routers
- Cisco 3725, 3745, 3825, 3845, 7200 e 7301 Series Routers

Pré-requisitos

Requisitos

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

- Uma imagem avançada do Cisco IOS Software Release 12.4(6)T ou posterior
- Uma das plataformas de Cisco Routers listadas na Introdução

Componentes Utilizados

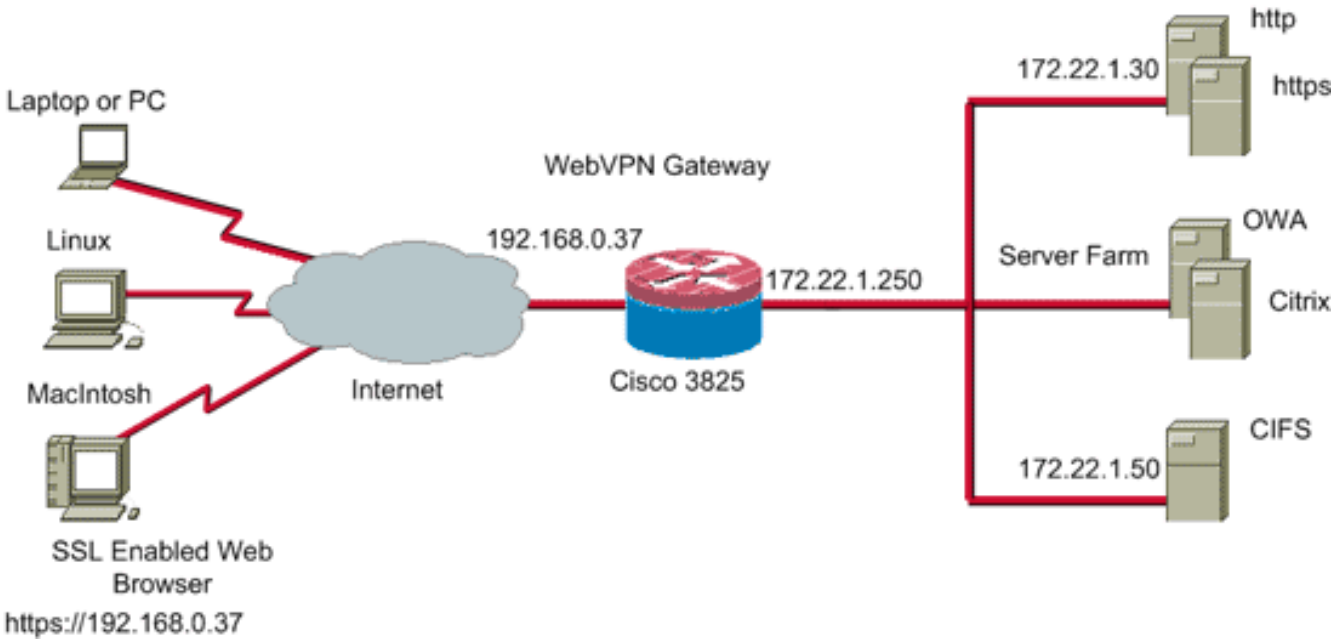
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 3825 Router
- Imagem do software Advanced Enterprise - Cisco IOS Software Release 12.4(9)T
- Cisco Router and Security Device Manager (SDM) - versão 2.3.1

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. Os endereços IP utilizados neste exemplo foram obtidos de endereços RFC 1918 que são privados e ilegais para uso na Internet.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Convenções

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

Tarefas de Pré-configuração

Antes de iniciar, execute estas tarefas:

1. Configure um nome de host e um nome de domínio.
2. Configure o roteador para SDM. A Cisco envia alguns roteadores com uma cópia pré-instalada do SDM.Se o Cisco SDM já não estiver carregado em seu roteador, você poderá obter uma cópia gratuita do software de Download de Software (somente clientes registrados). Você deve possuir uma conta CCO com um contrato de serviço. Para obter informações detalhadas sobre a instalação e a configuração do SDM, consulte Cisco Router and Security Device Manager.
3. Configure a data, a hora e o fuso horário corretos para seu roteador.

Configurar a WebVPN no Cisco IOS

Você pode ter mais de um gateway WebVPN associado a um dispositivo. Cada gateway WebVPN é vinculado somente a um endereço IP no roteador. Você pode criar mais de um contexto WebVPN para um gateway WebVPN específico. Para identificar contextos individuais, forneça cada contexto com um nome exclusivo. Um grupo de políticas pode ser associado somente a um contexto WebVPN. O grupo de políticas descreve quais recursos estão disponíveis em um contexto WebVPN específico.

Execute estes passos para configurar a WebVPN no Cisco IOS:

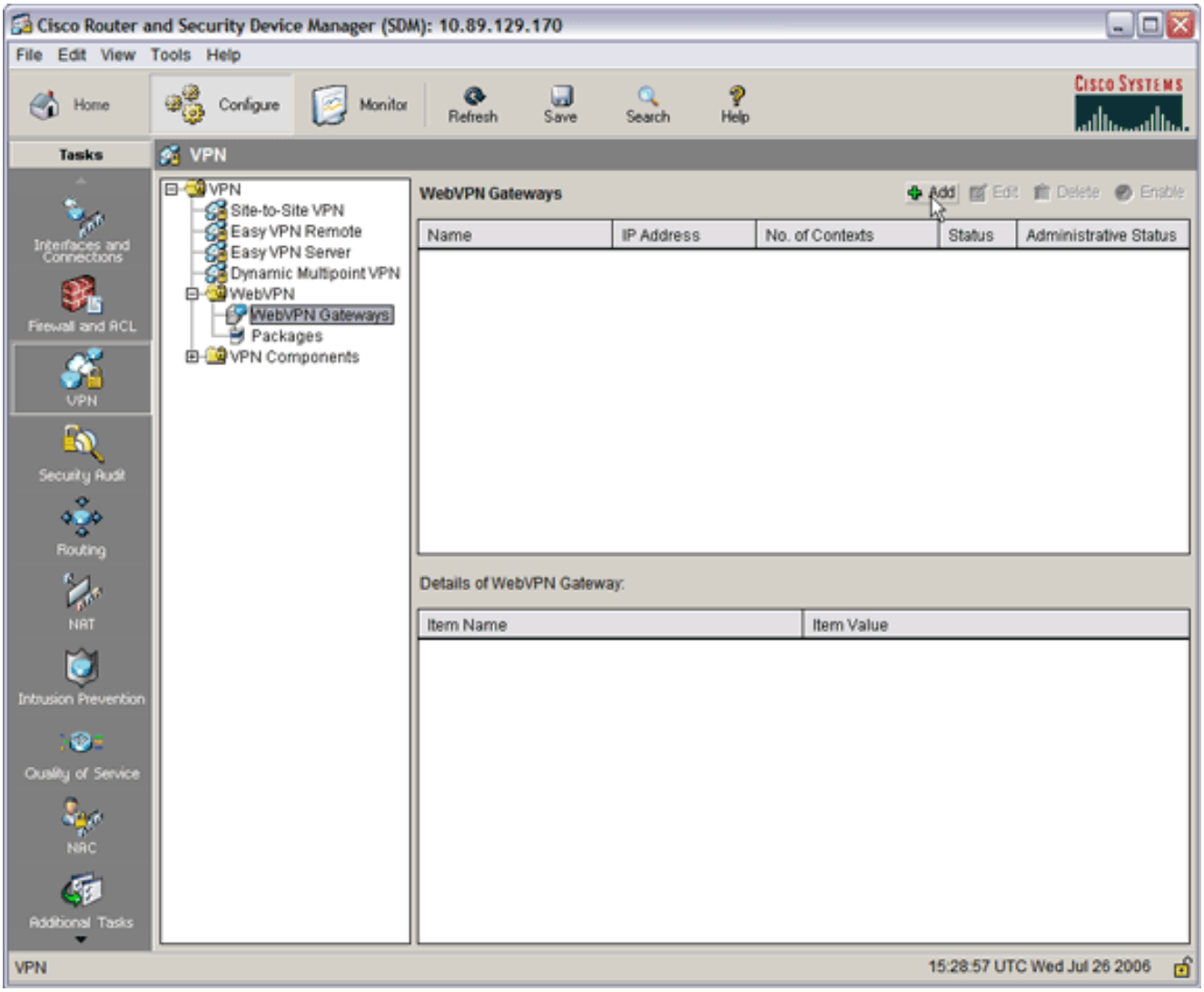
1. Configurar o Gateway WebVPN
2. Configurar os Recursos Permitidos o Grupo de Políticas
3. Configurar o Grupo de Políticas WebVPN e Selecionar os Recursos

4. Configurar o Contexto WebVPN
5. Configurar o Banco de Dados de Usuários e o Método de Autenticação

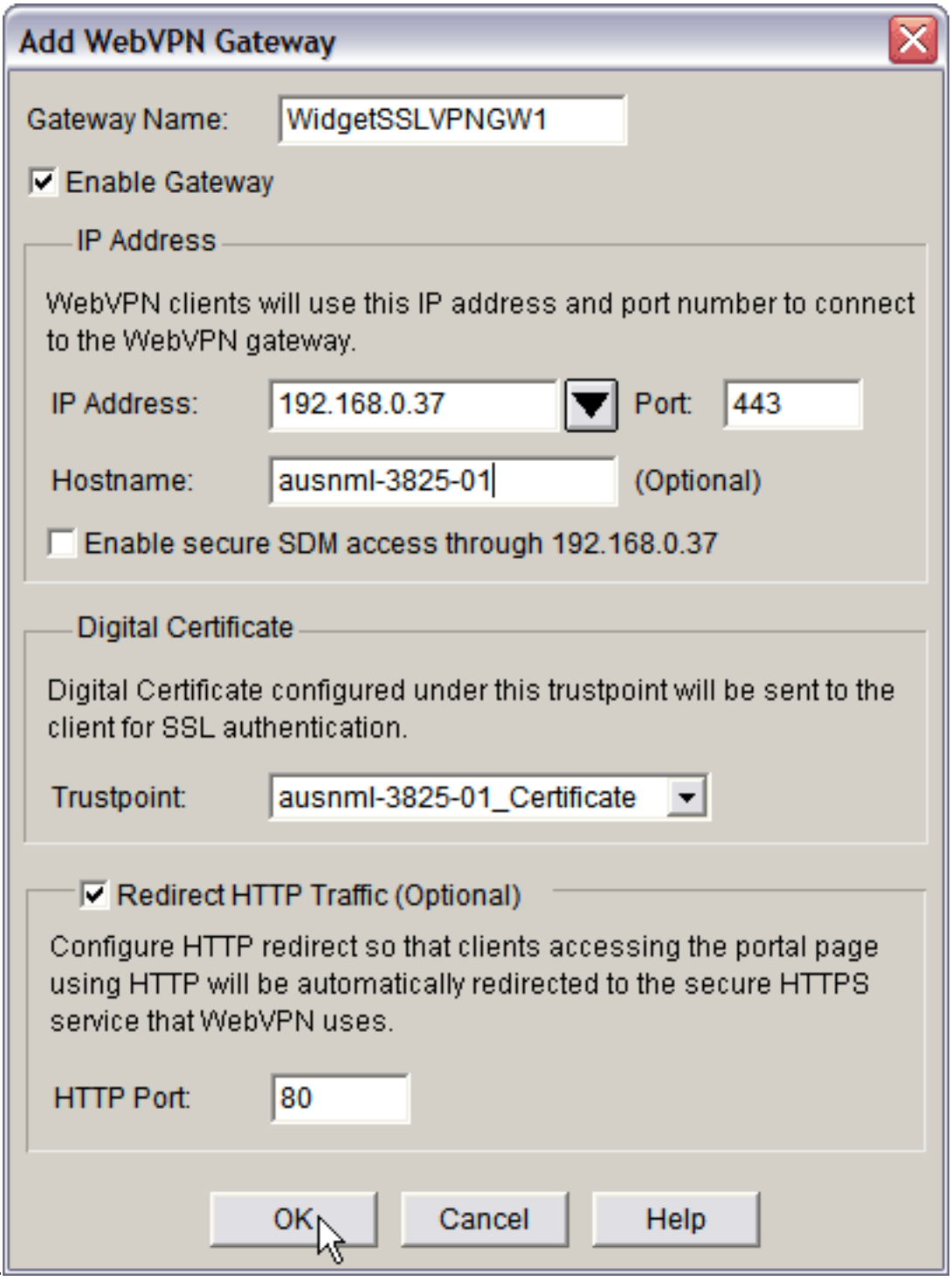
Passo 1. Configurar o Gateway WebVPN

Execute estes passos para configurar o Gateway WebVPN:

1. No aplicativo SDM, clique em **Configure** e em **VPN**.
2. Expanda **WebVPN**, e escolha **Gateways WebVPN**.



3. Clique em Add.A caixa de diálogo Add WebVPN Gateway é



exibida.

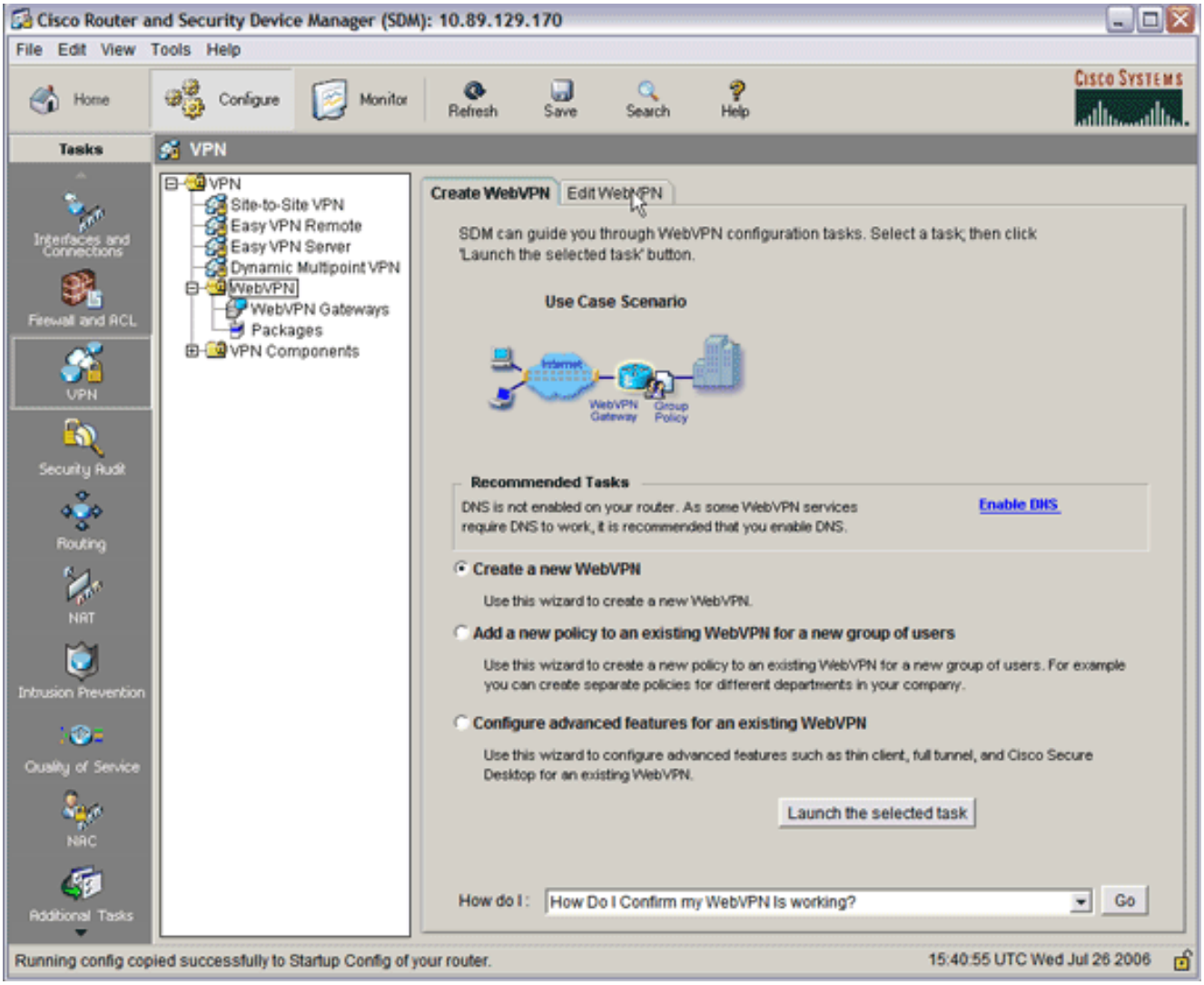
4. Insira valores nos campos Gateway Name e IP Address e marque a caixa de seleção **Enable Gateway**.
5. Marque a caixa de seleção **Redirect HTTP Traffic** e clique em **OK**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Passo 2. Configurar os Recursos Permitidos para o Grupo de Políticas

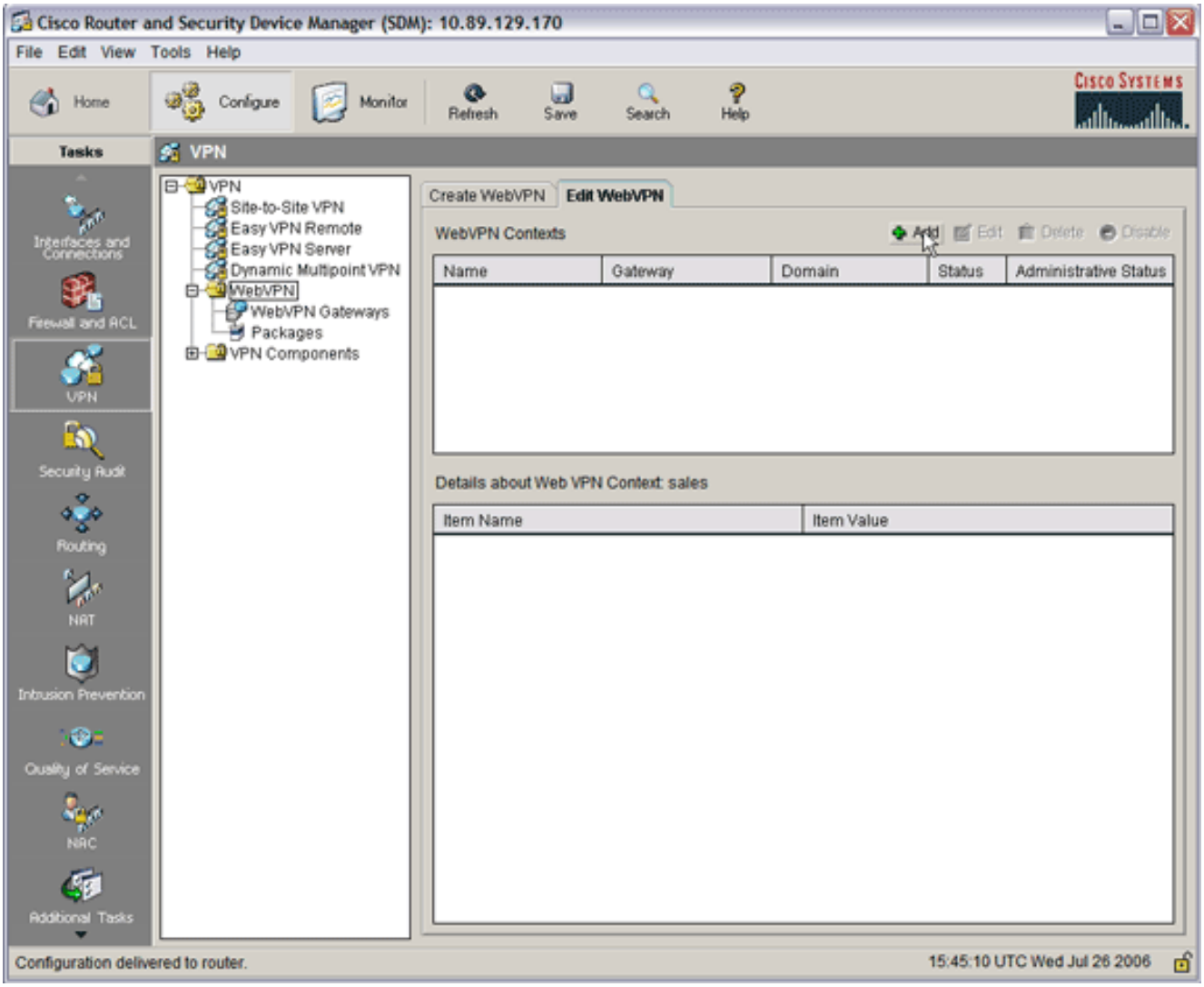
Para facilitar adicionar recursos a um grupo de políticas, você pode configurar os recursos antes de criar o grupo de políticas.

Execute estes passos para configurar os recursos permitidos o grupo de políticas:

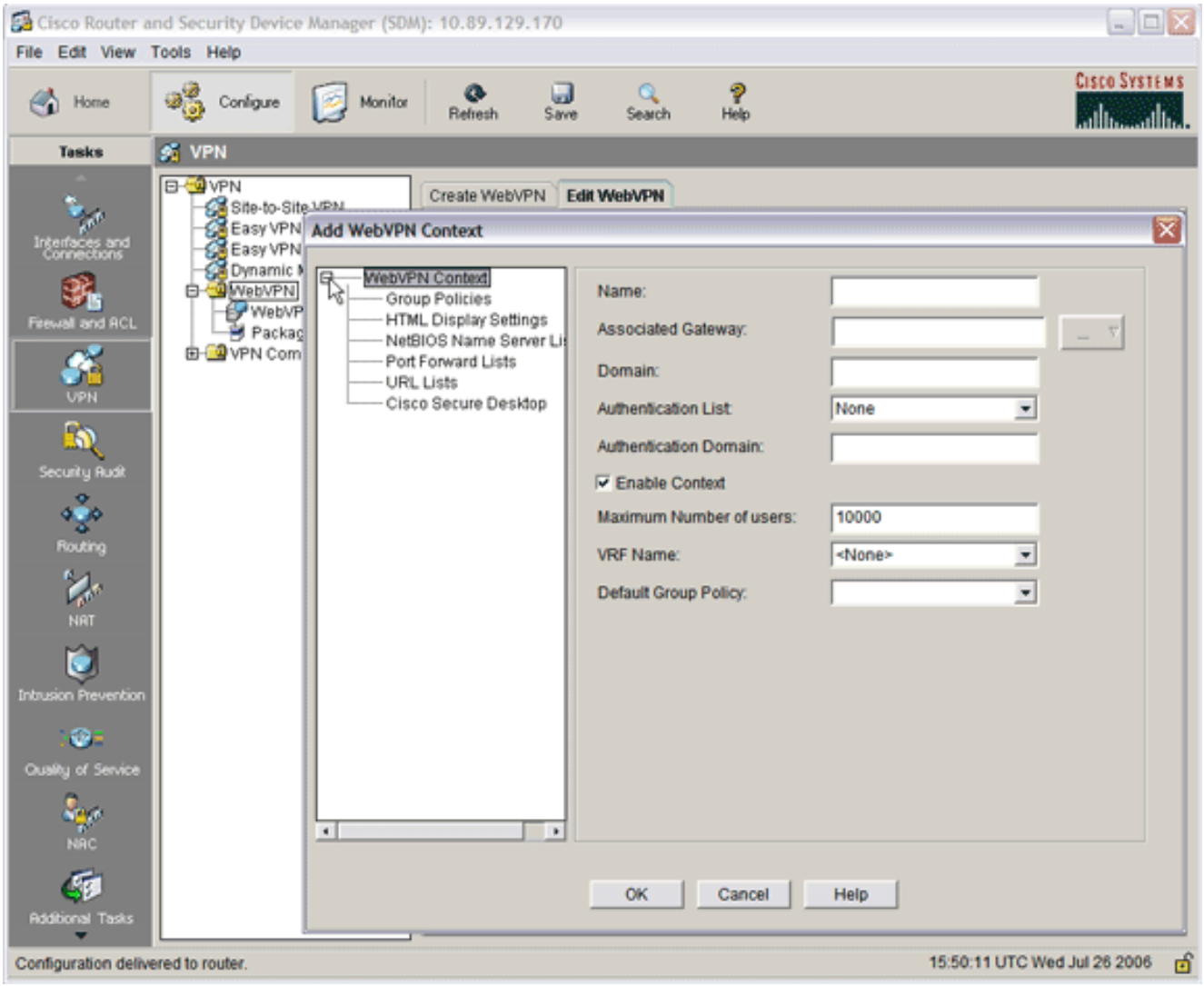
1. Clique em **Configure** e clique em **VPN**.



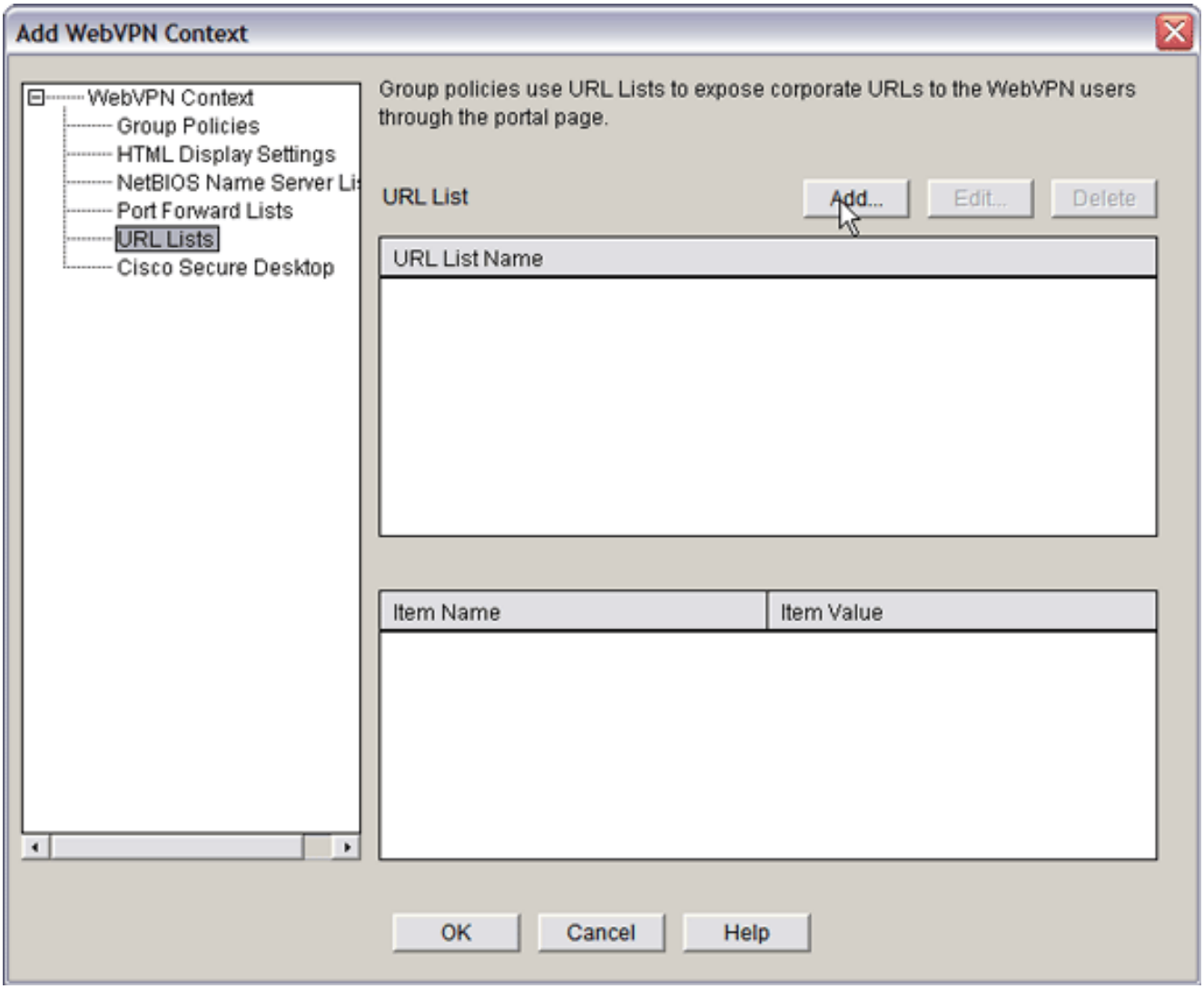
2. Escolha **WebVPN** e clique na guia **Edit WebVPN**.**Nota:** A WebVPN permite que você configure acesso para HTTP, HTTPS, navegação de arquivos do Windows através do protocolo Common Internet File System (CIFS) e
Citrix.



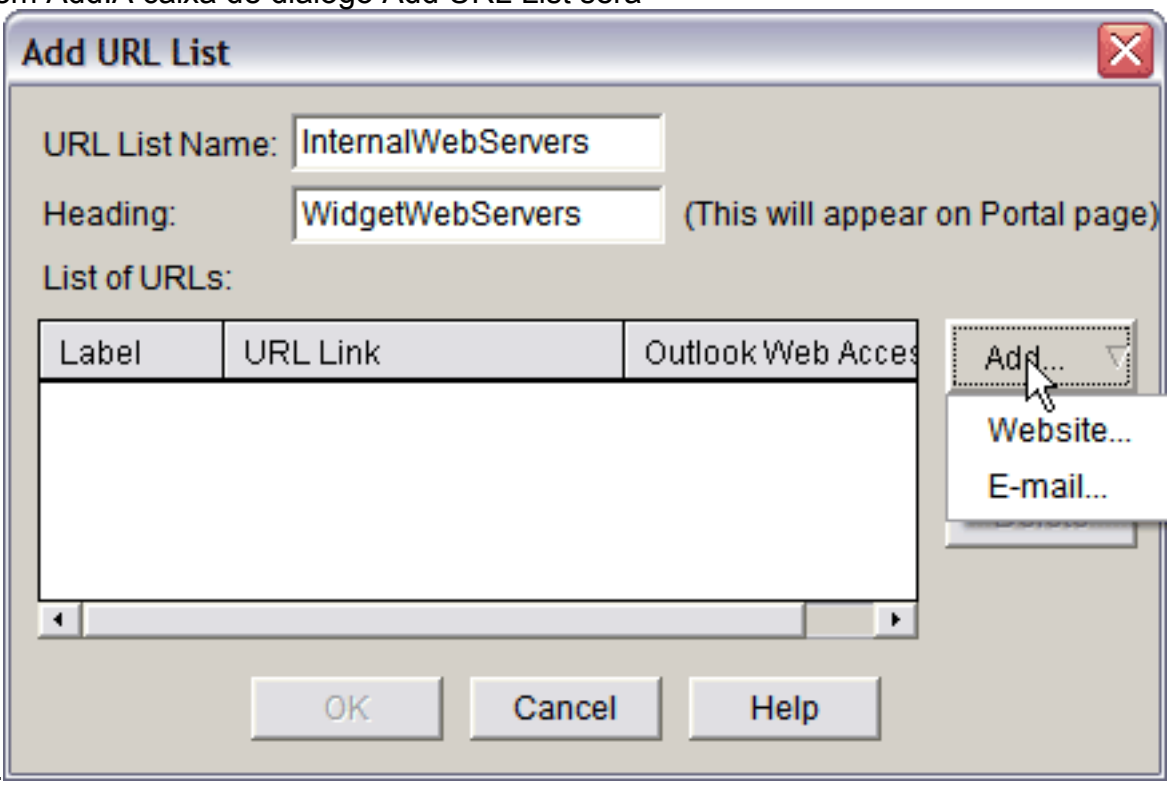
3. Clique em Add.A caixa de diálogo Add WebVPN Context é exibida.



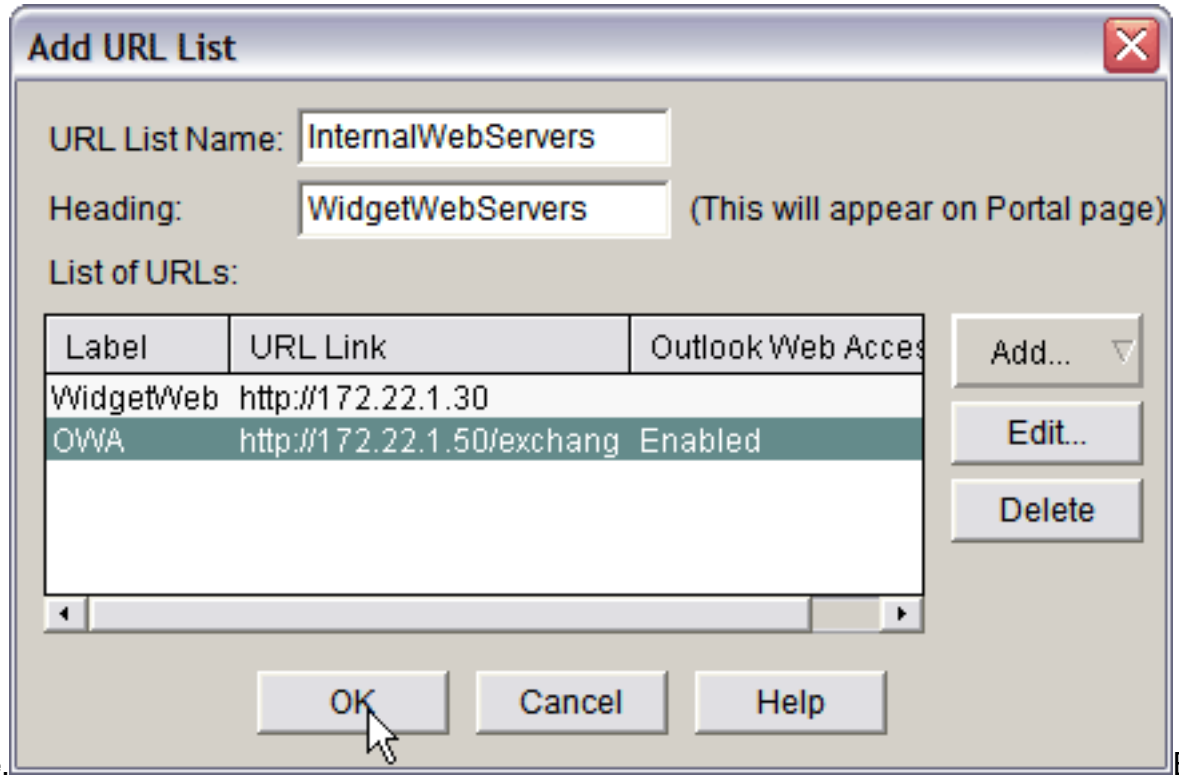
4. Expanda **WebVPN Context** e escolha **URL Lists**.



5. Clique em Add.A caixa de diálogo Add URL List será exibida.

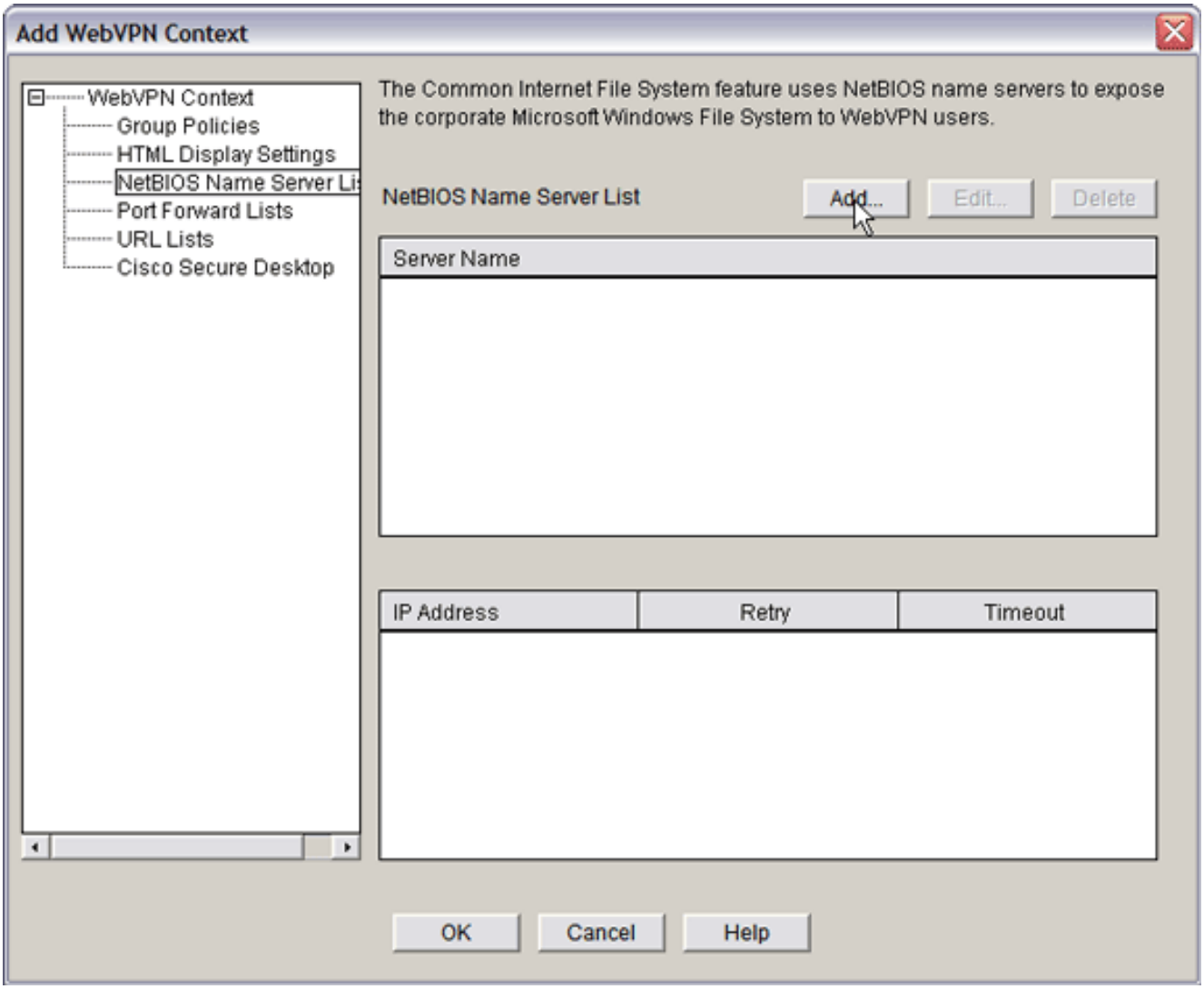


6. Insira valores nos campos URL List Name e Heading.
7. Clique em **Add** e escolha

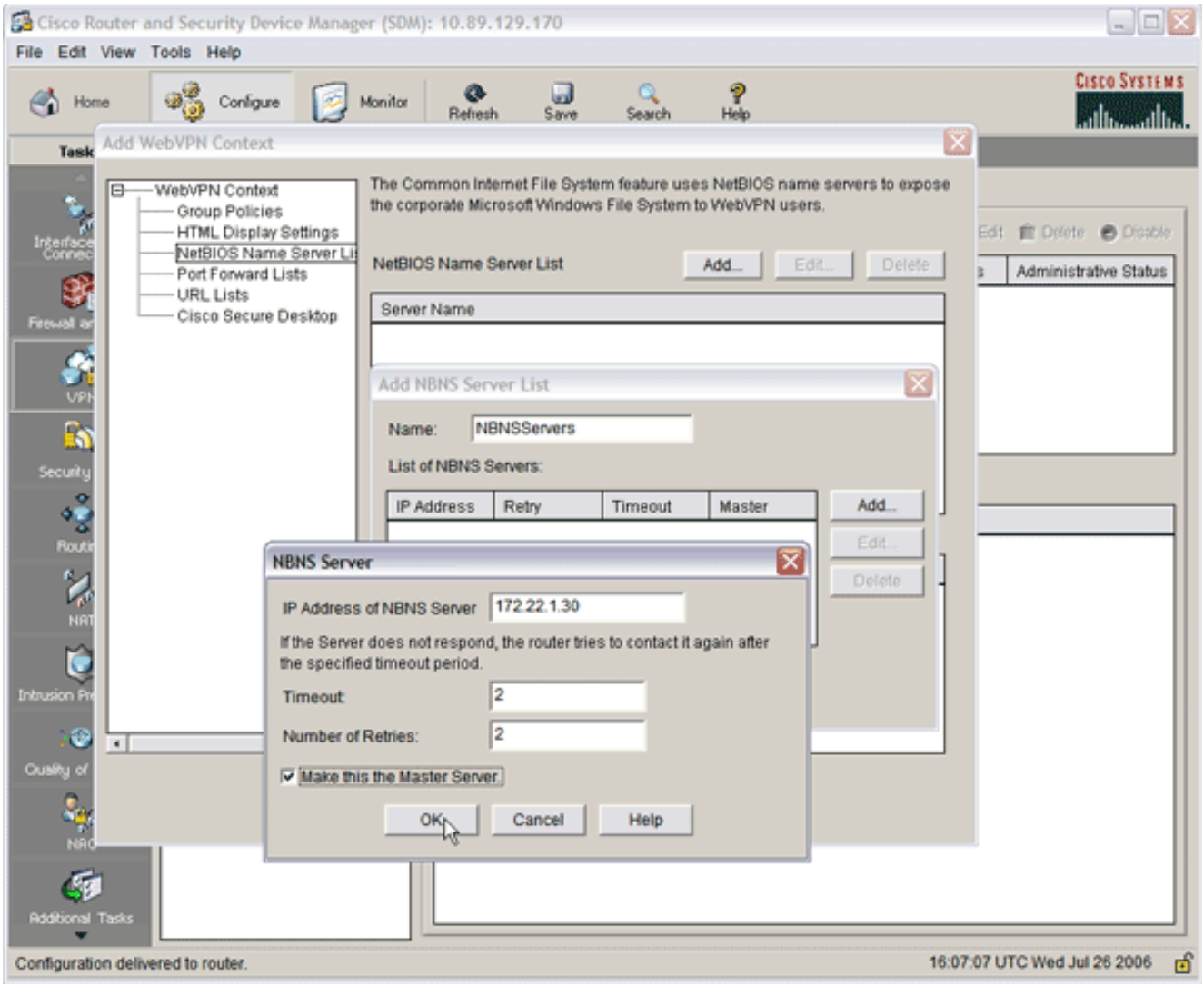


Website.E sta lista contém todos os servidores Web HTTP e HTTPS que você deseja disponibilizar para esta conexão WebVPN.

8. Para adicionar acesso ao Outlook Web Access (OWA), clique em **Add**, escolha **E-mail** e clique em **OK** após preencher todos os campos desejados.
9. Para permitir a navegação de arquivos do Windows através do CIFS, você pode designar um servidor NetBIOS Name Service (NBNS) e configurar os compartilhamentos apropriados no domínio do Windows em ordem.Na lista WebVPN Context, escolha **NetBIOS Name Server**
Lists.



Clique em Add.A caixa de diálogo Add NBNS Server List é exibida.Insira um nome para a lista e clique em **Add**.A caixa de diálogo NBNS Server será exibida.

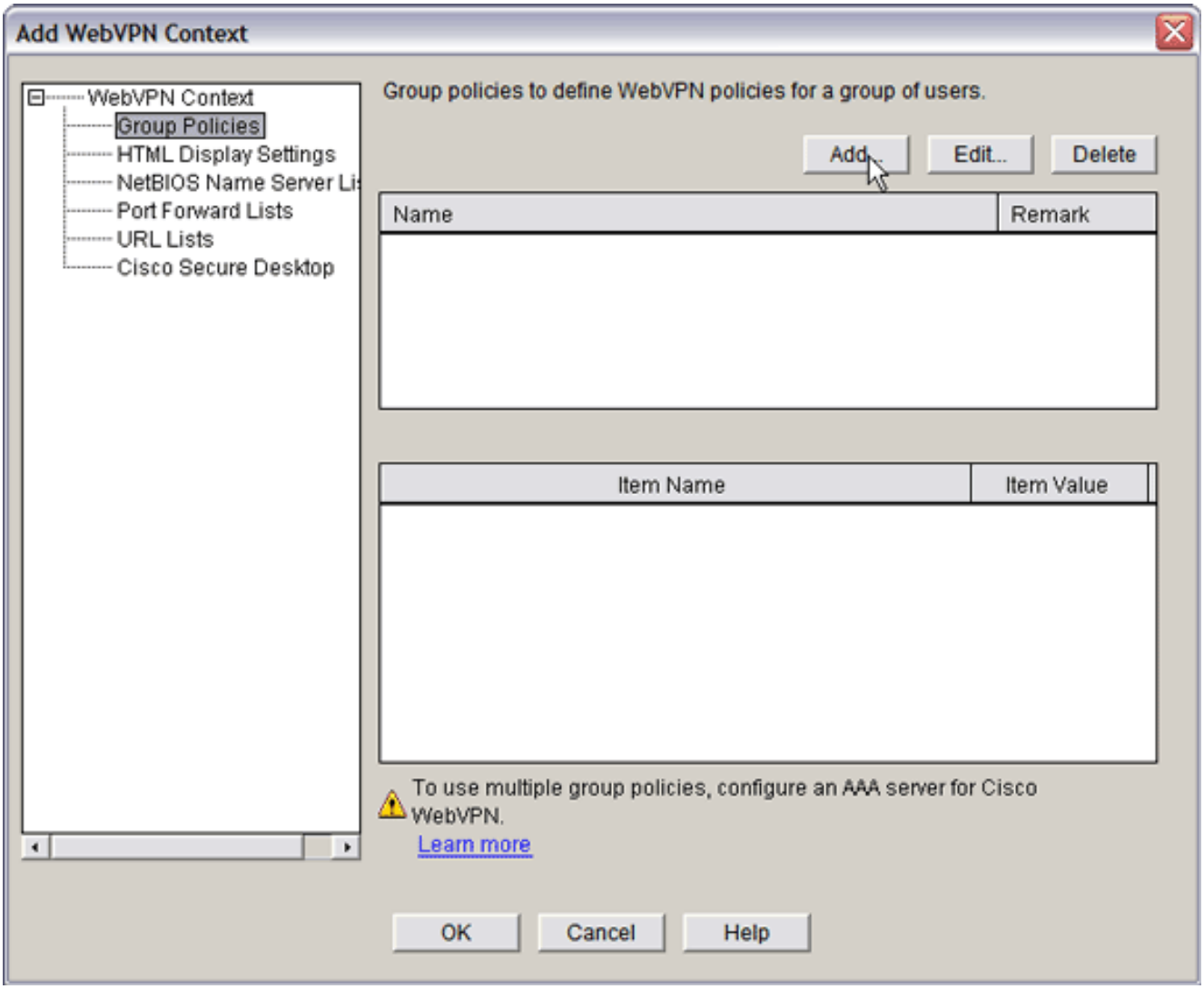


Se aplicável, marque a caixa de seleção **Make This the Master Server**.Clique em **OK** e, em seguida, clique em **OK**.

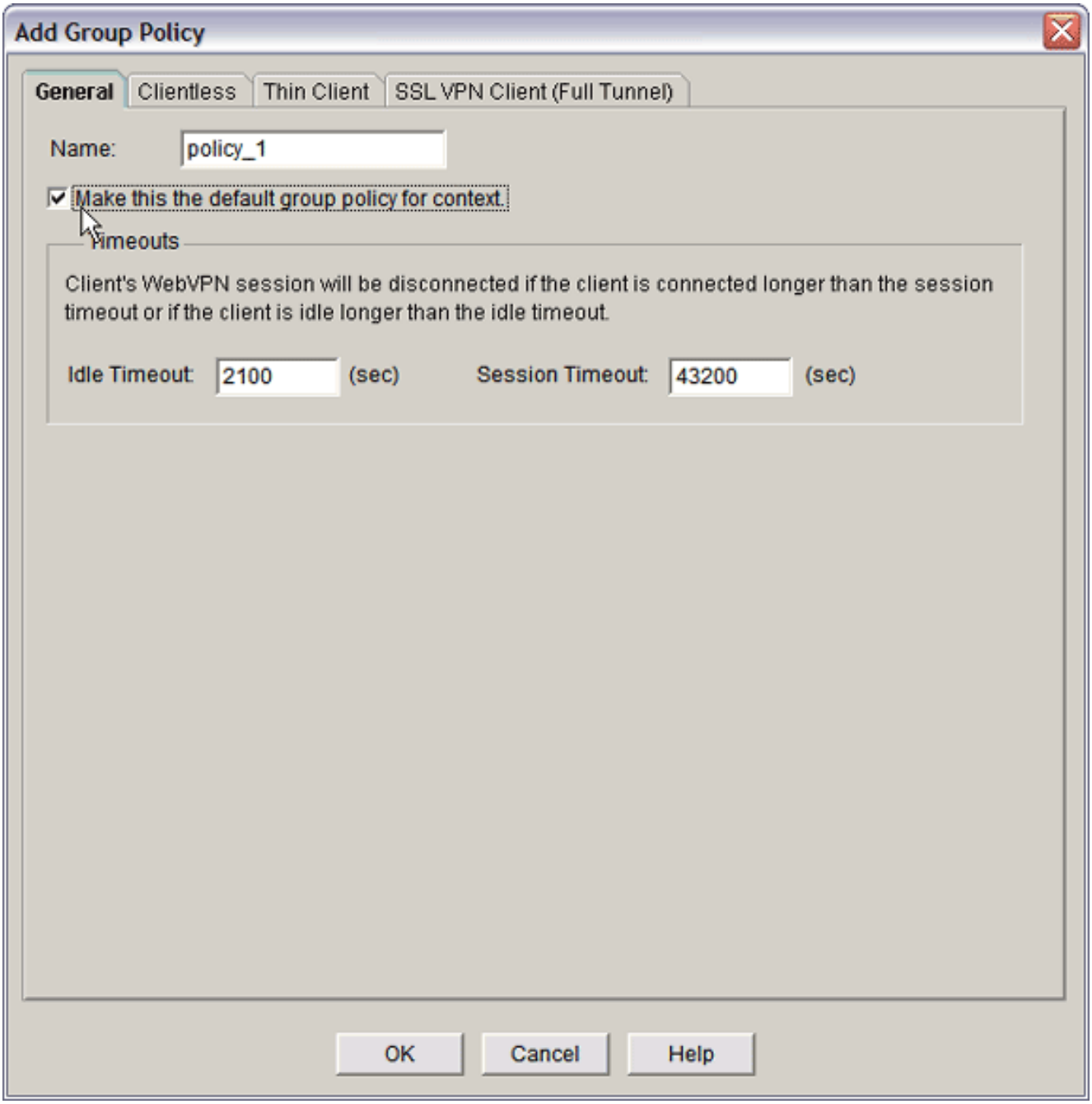
Passo 3. Configurar o Grupo de Políticas WebVPN e Selecionar os Recursos

Execute estes passos para configurar o grupo de políticas WebVPN e selecionar os recursos:

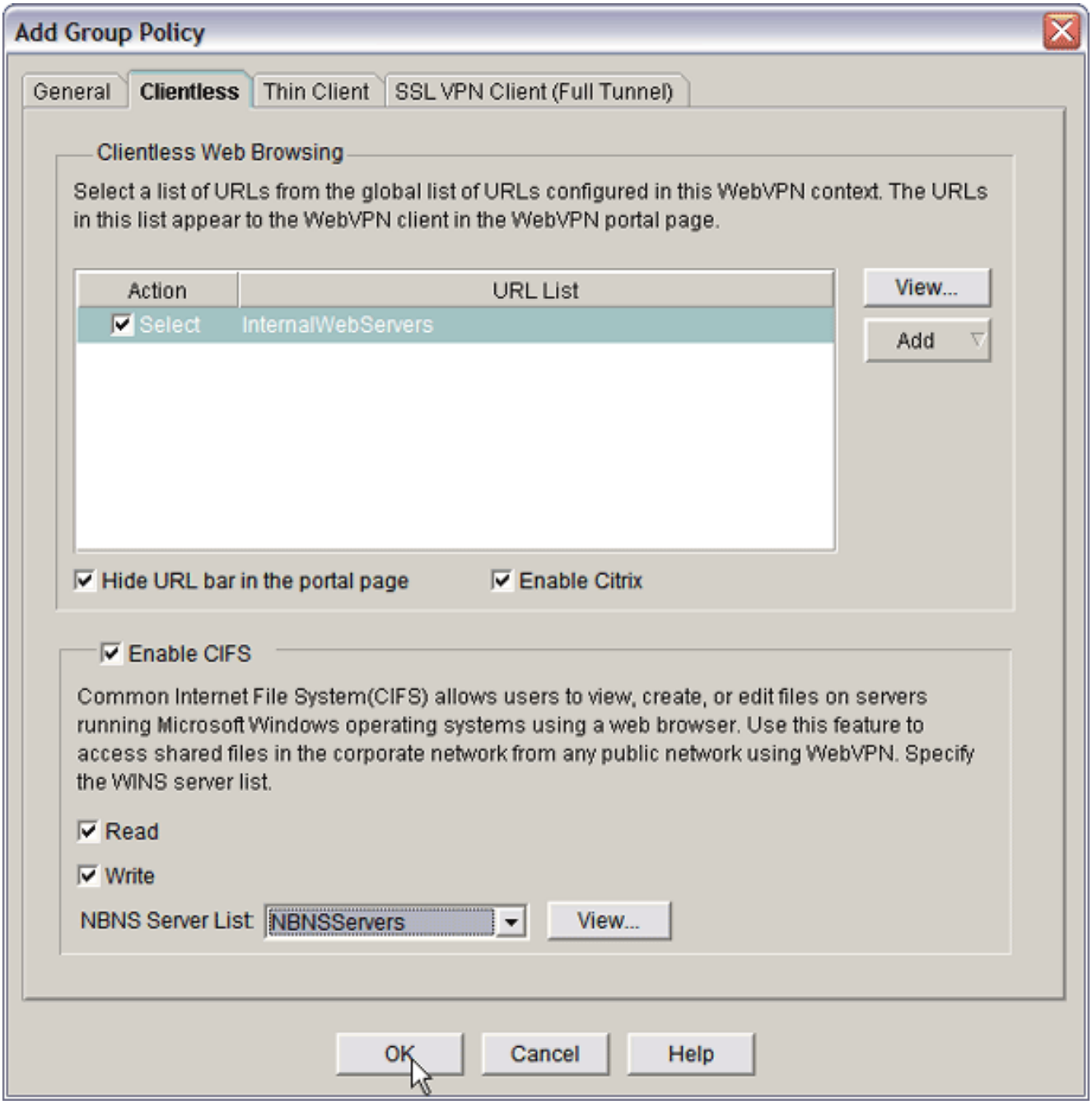
1. Clique em **Configure** e clique em **VPN**.
2. Expanda **WebVPN** e escolha **WebVPN Context**.



3. Escolha **Group Policies** e o clique em **Add**.A caixa de diálogo Add Group Policy é exibida.



4. Insira um nome para a nova política e selecione **Make this the default group policy para a** caixa de seleção de **contexto**.
5. Clique na guia **Clientless** localizada na parte superior da caixa de diálogo.

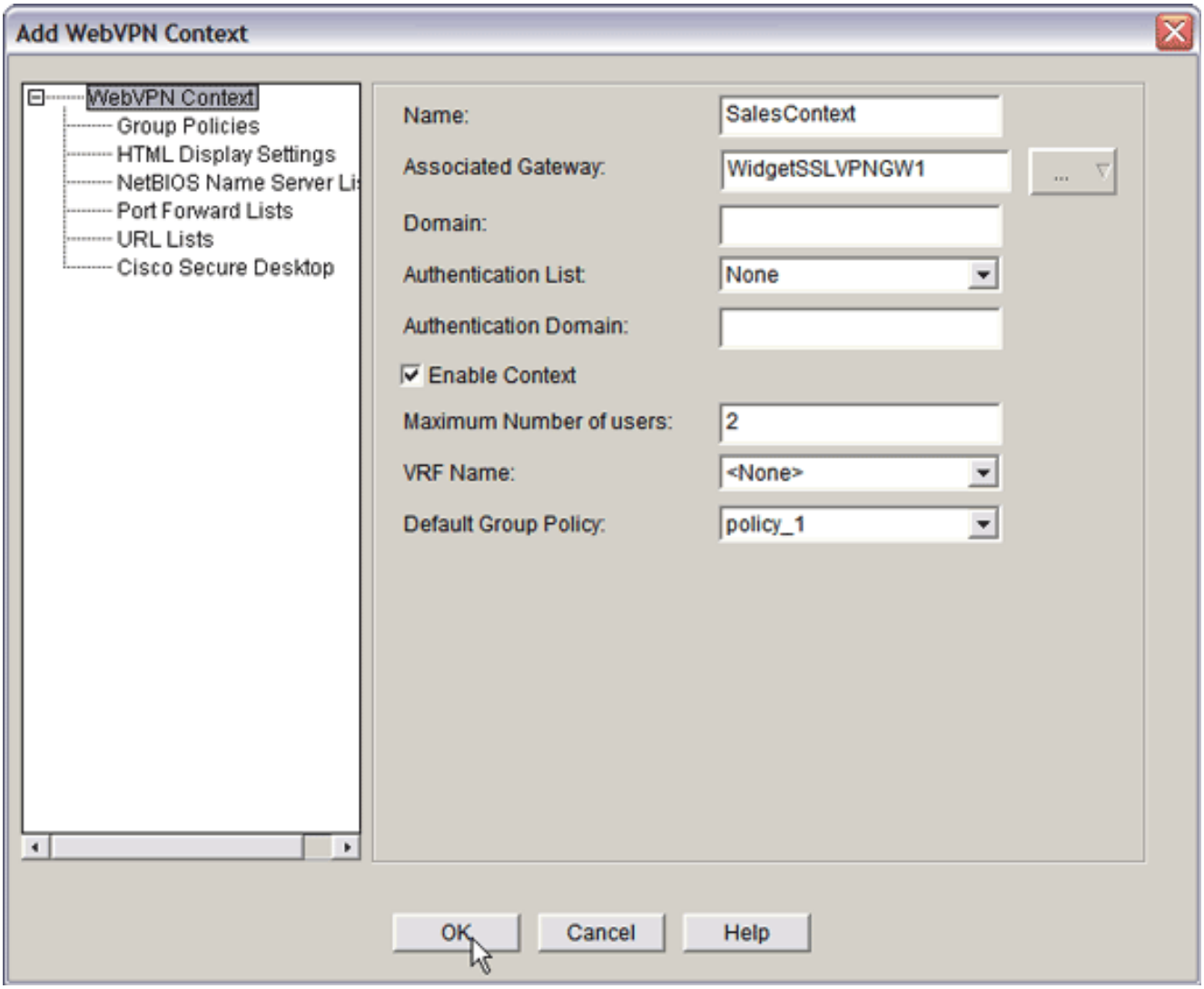


6. Marque a caixa de seleção **Select** para a URL List desejada.
7. Se seus clientes usam clientes Citrix que precisam de acesso a servidores Citrix, marque a caixa de seleção **Enable Citrix**.
8. Marque as caixas de seleção **Enable CIFS**, **Read** e **Write** .
9. Clique na seta suspensa **NBNS Server Lista**, e escolha a lista de servidores NBNS que você criou para a navegação de arquivos do Windows no Passo 2.
10. Clique em **OK**.

Passo 4. Configurar o Contexto WebVPN

Para vincular gateway WebVPN, política do grupos e recursos, você deve configurar o contexto WebVPN. Para configurar o contexto WebVPN, execute estes passos:

1. Escolha **WebVPN Context** e insira um nome para o contexto.



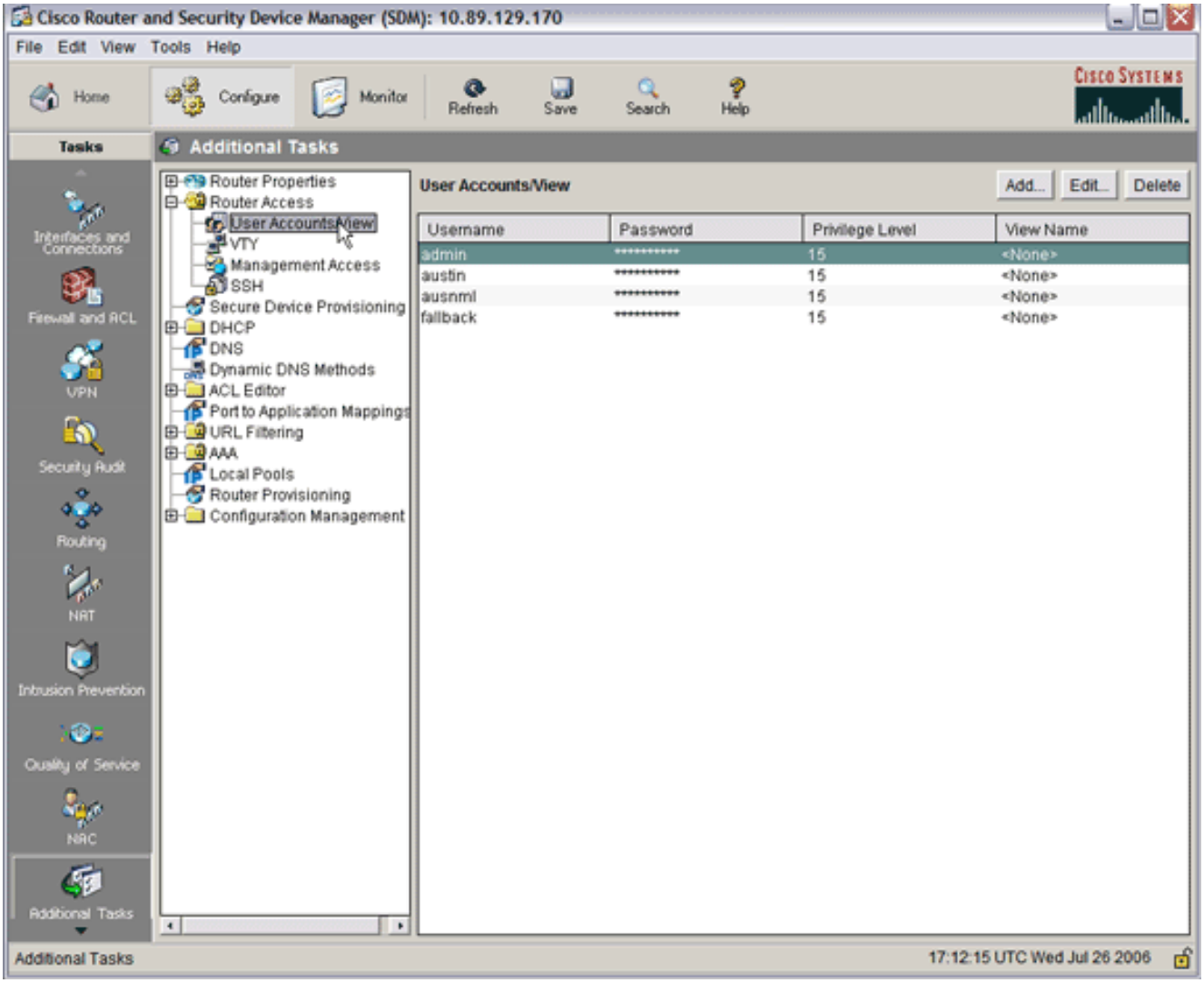
2. Clique na seta suspensa de Associates Gateway e escolha um gateway associado.
3. Se você pretende criar mais de um contexto, insira um nome exclusivo no campo Domain para identificar este contexto. Se você deixar o campo Domain em branco, os usuários deverão acessar a WebVPN com **https://EndereçoIP**. Se você inserir um nome de domínio (por exemplo, *Vendas*), os usuários deverão conectar com **https://EndereçoIP/Vendas**.
4. Marque a caixa de seleção **Enable Context**.
5. No campo Maximum Number of Users, insira o número máximo de usuários permitido pela licença de dispositivos.
6. Clique na seta suspensa **Default Group policy** e selecione a política de grupo a ser associada a este contexto.
7. Clique em **OK** e, em seguida, clique em **OK**.

Passo 5. Configurar o Banco de Dados de Usuários e o Método de Autenticação

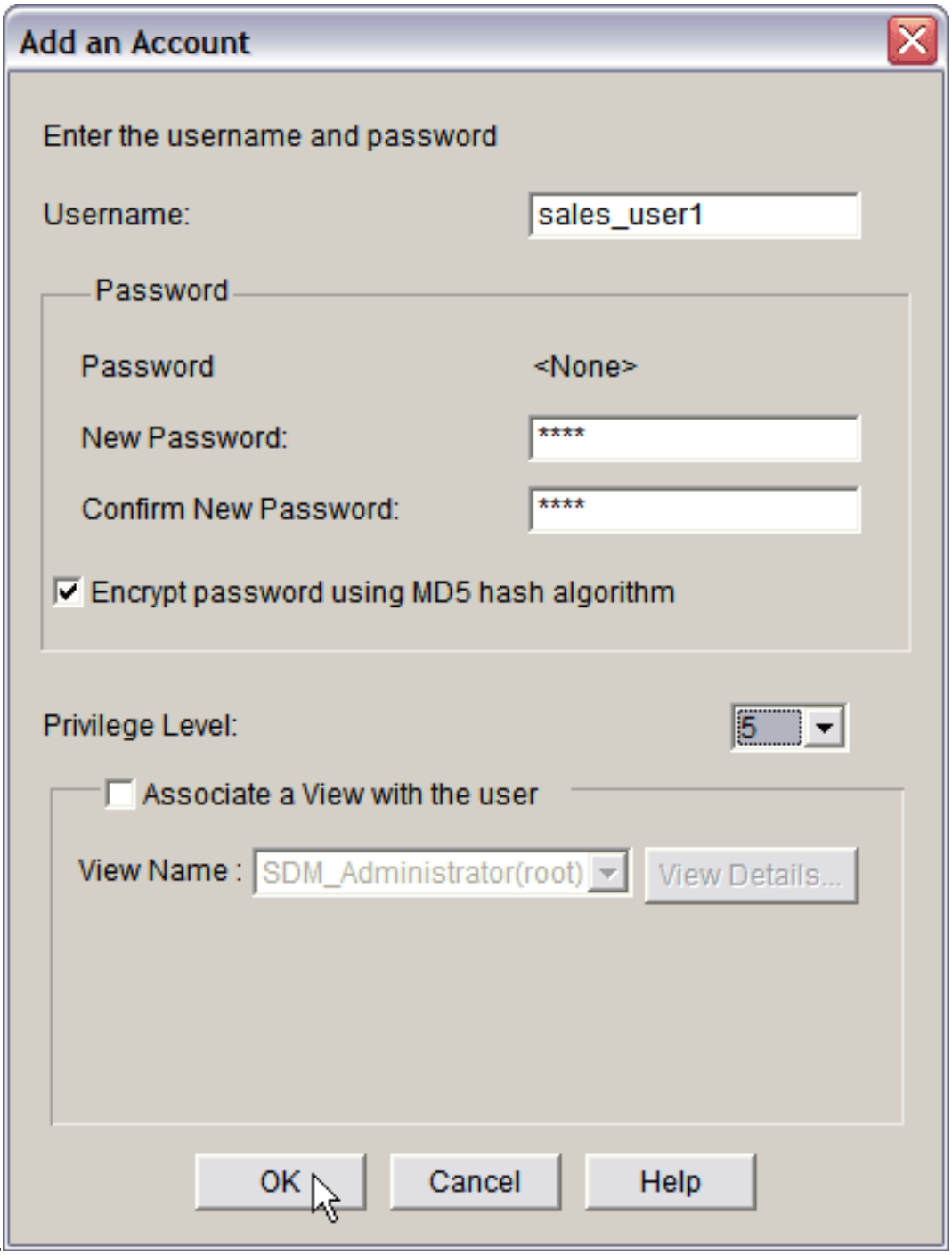
Você pode configurar sessões VPN SSL Sem Clientes (WebVPN) para autenticar com o Radius, o Cisco AAA Server ou um banco de dados local. Este exemplo usa um banco de dados local.

Execute estes passos para configurar o banco de dados de usuários e o método de autenticação:

1. Clique em **Configuration** e em **Additional Tasks**.
2. Expanda **Router Access** e escolha **User Accounts/View**.



3. Clique no botão Adicionar.A caixa de diálogo Add an Account é



exibida.

4. Insira uma conta de usuário e uma senha.
5. Clique em **OK** e, em seguida, clique em **OK**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Resultados

O ASDM cria estas configurações de linha de comando:

ausnml-3825-01
Building configuration... Current configuration : 4190 bytes ! ! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by ausnml ! NVRAM config last updated at 17:22:31 UTC Wed Jul 26 2006 by ausnml

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 29312730 2506092A 864886F7 0D010902
16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63
6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
31303130 30303030 305A3029 31273025 06092A86 4886F70D
01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363
6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B
E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093
C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B
09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3
78307630 0F060355 1D130101 FF040530 030101FF 30230603
551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E
63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D
0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D
4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4
2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6
7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6
5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC
55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920
88A8A55E quit username admin privilege 15 secret 5
$1$jm6N$2xNfhupbAinq3BQZMRzrW0 username ausnml privilege
```

```
15 password 7 15071F5A5D292421 username fallback
privilege 15 password 7 08345818501A0A12 username austin
privilege 15 secret 5 $1$3xFv$W0YUsKDx1adDc.cVQF2Ei0
username sales_user1 privilege 5 secret 5
$1$2/SX$ep4fsCpodeyKaRji2mJkX/ ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http timeout-policy idle 600
life 86400 requests 100 ! control-plane ! line con 0
stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-
timeout 40 0 privilege level 15 password 7
071A351A170A1600 transport input telnet ssh line vty 5
15 exec-timeout 40 0 password 7 001107505D580403
transport input telnet ssh ! scheduler allocate 20000
1000 ! !--- WebVPN Gateway webvpn gateway
WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address
192.168.0.37 port 443 http-redirect port 80 ssl
trustpoint ausnml-3825-01_Certificate inservice ! webvpn
context SalesContext ssl authenticate verify all ! !---
Identify resources for the SSL VPN session url-list
"InternalWebServers" heading "WidgetWebServers" url-text
"WidgetWeb" url-value "http://172.22.1.30" url-text
"OWA" url-value "http://172.22.1.50/exchange" ! nbns-
list NBNSServers nbns-server 172.22.1.30 ! !--- Identify
the policy which controls the resources available policy
group policy_1 url-list "InternalWebServers" nbns-list
"NBNSServers" functions file-access functions file-
browse functions file-entry hide-url-bar citrix enabled
default-group-policy policy_1 gateway WidgetSSLVPNGW1
max-users 2 inservice ! end
```

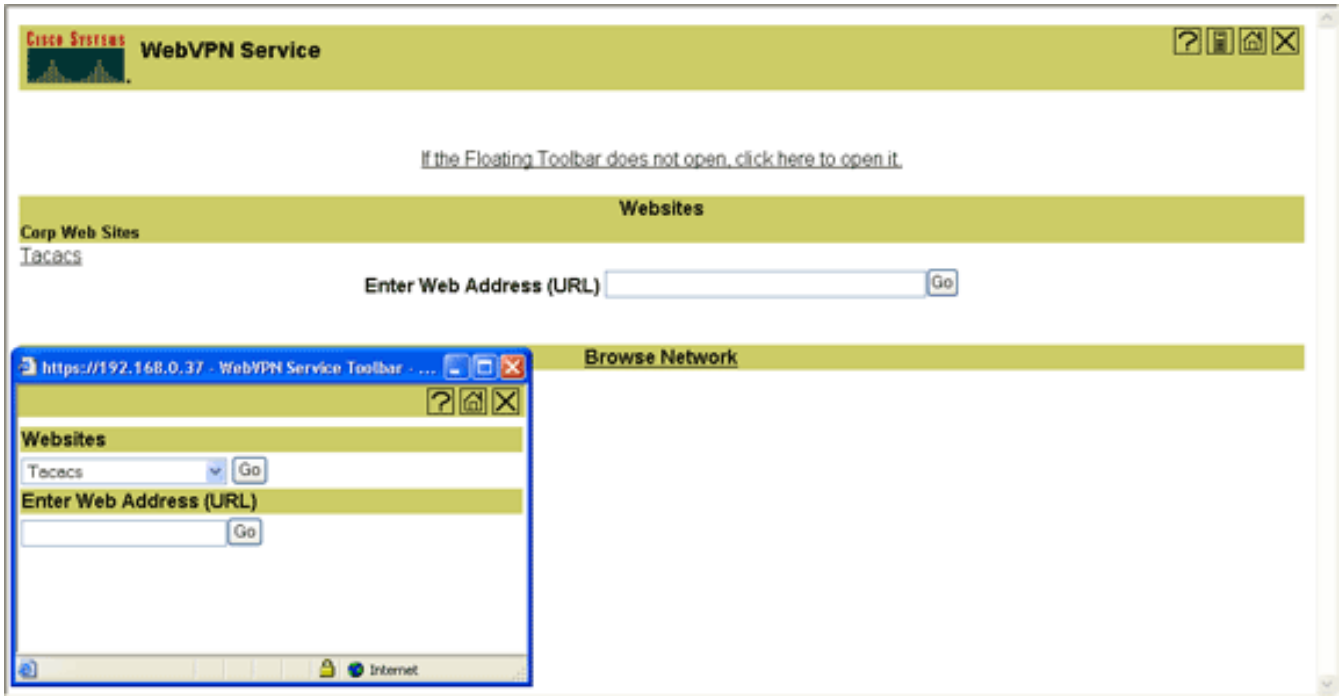
Verificar

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

Procedimento

Execute estes procedimentos para confirmar se a sua configuração está funcionando corretamente:

- Teste sua configuração com um usuário. Insira **https://WebVPN_Gateway_Endereço_IP em um** navegador da Web com SSL habilitado; onde *WebVPN_Gateway_Endereço_IP* é o endereço IP do serviço WebVPN. Após você aceitar o certificado e inserir um nome de usuário e uma senha, uma tela semelhante a esta imagem deverá ser exibida.



- Verifique a sessão VPN SSL. No aplicativo SDM, clique no botão **Monitor** e, em seguida, clique em **VPN Status**. Expanda **WebVPN (All Contexts)**, expanda o contexto apropriado e escolha **Users**.
- Verifique as mensagens de erro. No aplicativo SDM, clique no botão **Monitor**, clique em **Logging** e clique na guia **Syslog**.
- Consulte a configuração running para o dispositivo. No aplicativo SDM, clique no **botão Configure** e clique em **Additional Tasks**. Expanda **Configuration Management** e escolha **Config Editor**.

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.

Nota: 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.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Nota: Não interrompa o comando **Copy File to Server** ou navegue para uma janela diferente enquanto a cópia estiver em andamento. A interrupção da operação pode fazer com que um arquivo incompleto seja salvo no servidor.

Nota: Os usuários podem carregar e baixar os novos arquivos usando o cliente WebVPN, mas o usuário não pode substituir os arquivos no Common Internet File System (CIFS) na WebVPN usando o comando **Copy File to Server**. O usuário recebe esta mensagem quando ele tenta substituir um arquivo no servidor:

```
Unable to add the file
```

Procedimento

Execute estes passos para fazer troubleshoot da sua configuração:

1. Certifique-se de que os clientes desabilitem bloqueadores de pop-up.
2. Certifique-se de que os clientes possuam cookies habilitados.
3. Certifique-se de que os clientes usem os navegadores da Web Netscape, Internet Explorer, Firefox ou Mozilla.

Comandos

Vários **comandos debug** estão associados ao WebVPN. Consulte Usando Comandos de Depuração da WebVPN para obter informações detalhadas sobre esses comandos.

Nota: O uso de **comandos debug** pode afetar negativamente seu dispositivo Cisco. Antes de utilizar **comandos debug**, consulte Informações Importantes sobre Comandos Debug.

Informações Relacionadas

- Cisco IOS SSLVPN
- Perguntas e Respostas sobre a VPN SSL do Cisco IOS
- Exemplo de Configuração de VPN SSL com Thin-Client (WebVPN) no Cisco IOS com SDM
- Exemplo de Configuração de Cliente VPN SSL (SVC) no IOS com SDM
- Suporte Técnico e Documentação - Cisco Systems