Thin client SSL VPN (WebVPN) no ASA com exemplo da configuração ASDM

Índice

Introdução

A tecnologia de Thin-Client SSL VPN permite um acesso seguro para aplicativos que têm portas estáticas, como Telnet(23), SSH(22), POP3(110), IMAP4(143) e SMTP(25). É possível usar a Thin-Client SSL VPN como um aplicativo executado por usuário, aplicativo executado por políticas ou ambos. Isto é, você pode configurar o acesso em uma base de usuário por usuário ou criar Políticas de Grupo nas quais adicionará um ou mais usuários.

- **Sem clientes SSL VPN (WebVPN)** — Fornece um cliente remoto que exija um navegador da Web SSL-permitido alcançar servidores de Web HTTP ou HTTPS em uma rede de área local (LAN) corporativa. Além, os sem clientes SSL VPN fornecem o acesso para o arquivo de Windows que consulta com o protocolo do Common Internet File System (CIFS). O acesso à Web da probabilidade (OWA) é um acesso do exemplo de HTTP.Refira os sem clientes SSL VPN (WebVPN) no exemplo de configuração ASA a fim aprender mais sobre os sem clientes

SSL VPN.

- **O thin client SSL VPN (transmissão da porta)** — fornece um cliente remoto que transfira um applet com base em Java pequeno e permite o acesso seguro para os aplicativos do Transmission Control Protocol (TCP) que usam números de porta estática. O protocolo Post Office Protocol (POP3), o Simple Mail Transfer Protocol (SMTP), o Internet Message Access Protocol (IMAP), o Shell Seguro (ssh), e o telnet são exemplos do acesso seguro. Porque os arquivos na máquina local mudam, os usuários devem ter privilégios administrativos locais usar este método. Este método de SSL VPN não trabalha com aplicativos que usam atribuições de porta dinâmica, tais como alguns aplicativos do File Transfer Protocol (FTP).**Nota:** O User Datagram Protocol (UDP) não é apoiado.
- **Cliente VPN SSL (modo de túnel)** — Transfere um cliente pequeno à estação de trabalho remota e permite o acesso seguro completo aos recursos em uma rede corporativa interna. Você pode transferir permanentemente o cliente VPN SSL (SVC) a uma estação de trabalho remota, ou você pode remover o cliente uma vez que a sessão segura é fechada.Refira o cliente VPN SSL (SVC) no ASA com exemplo da configuração ASDM a fim aprender mais sobre o cliente VPN SSL.

Este documento demonstra uma configuração simples para o thin client SSL VPN na ferramenta de segurança adaptável (ASA). A configuração permite um usuário ao telnet firmemente a um roteador situado no interior do ASA. A configuração neste documento é apoiada para a versão ASA 7.x e mais tarde.

Pré-requisitos

Requisitos

Antes que você tente esta configuração, assegure-se de que você cumpra estas exigências para as estações do cliente remoto:

- navegador da Web SSL-permitido
- Versão JRE 1.4 das Javas do SOL ou mais atrasado
- Cookie permitidos
- Construtores emergentes desabilitados
- Privilégios administrativos locais (não exigidos mas sugeridos fortemente)

Nota: A versão a mais atrasada das Javas JRE do SOL está disponível como um download livre do Web site das Javas .

Componentes Utilizados

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

- 5510 Series adaptável da ferramenta de segurança de Cisco
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Nota:** Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.
- Versão de software adaptável da ferramenta de segurança de Cisco 7.2(1)
- Cliente remoto do profissional do Microsoft Windows XP (SP2)

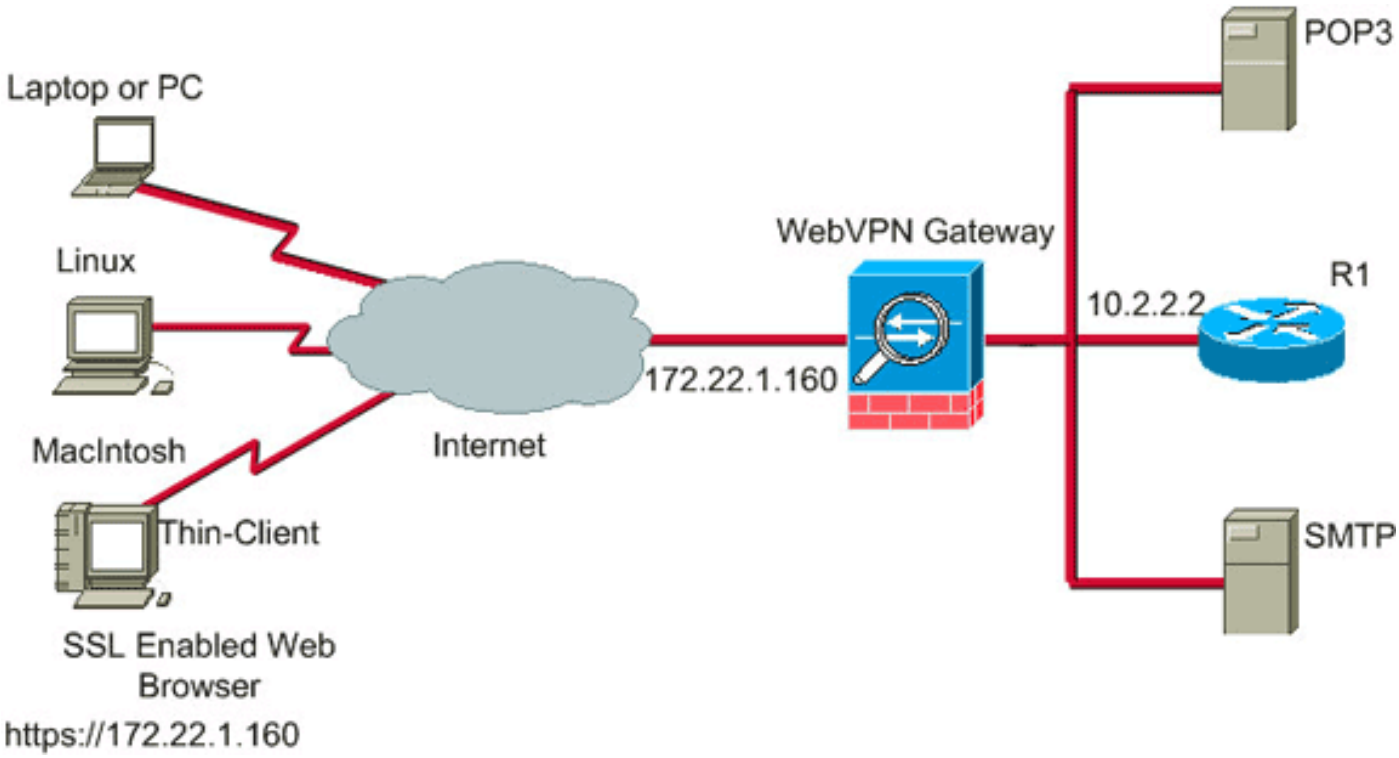
A informação neste documento foi desenvolvida em um ambiente de laboratório. Todos os dispositivos usados neste documento foram restaurados a sua configuração padrão. Se sua rede está viva, certifique-se de você compreender o impacto potencial do comando any. Todos os

endereços IP de Um ou Mais Servidores Cisco ICM NT usados nesta configuração foram selecionados dos endereços do RFC 1918 em um ambiente de laboratório; estes endereços IP de Um ou Mais Servidores Cisco ICM NT não são roteável no Internet e são para propósitos de teste somente.

Diagrama de Rede

Este documento usa a configuração de rede descrita nesta seção.

Quando um cliente remoto inicia uma sessão com o ASA, o cliente transfere um Java applet pequeno à estação de trabalho. O cliente é presentado com uma lista de recursos preconfigured.



Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

A fim começar uma sessão, o cliente remoto abre um navegador SSL à interface externa do ASA. Depois que a sessão é estabelecida, o usuário pode usar os parâmetros configurados no ASA para invocar todo o telnet ou acesso de aplicativo. Os proxys ASA a conexão segura e permitem o acesso de usuário ao dispositivo.

Nota: As listas de acessos de entrada não são necessárias para estas conexões porque o ASA está já ciente do que constitui uma sessão legal.

Configuração de VPN do thin client SSL usando o ASDM

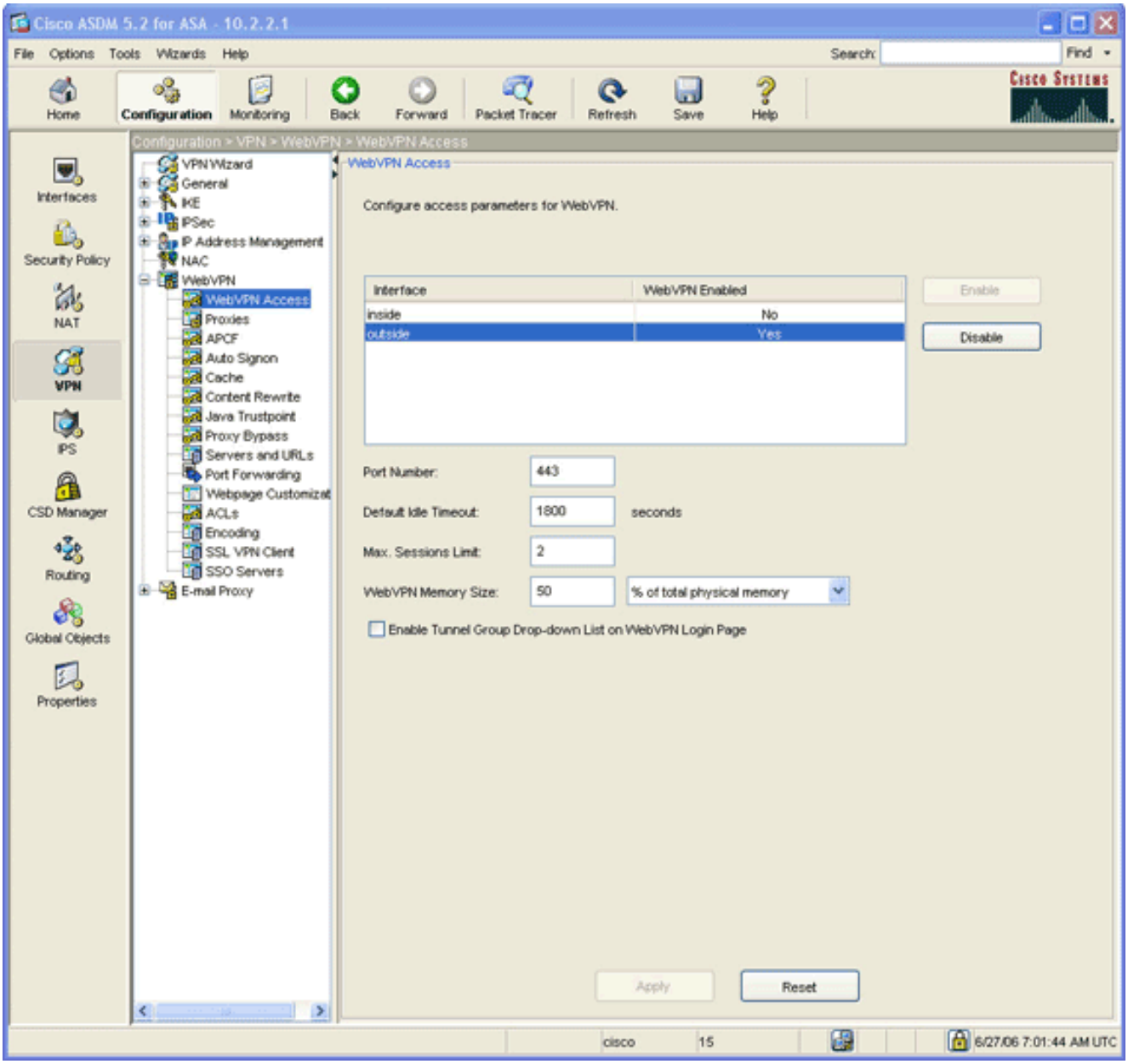
A fim configurar o thin client SSL VPN no ASA, termine estas etapas:

1. Permita o WebVPN no ASA
2. Configurar características da transmissão da porta
3. Crie uma política do grupo e ligue-a à lista da transmissão da porta (criada em etapa 2)
4. Crie um grupo de túneis e ligue-o à política do grupo (criada em etapa 3)
5. Crie um usuário e adicionar-lo que usuário à política do grupo (criada em etapa 3)

Etapa 1. Permita o WebVPN no ASA

A fim permitir o WebVPN no ASA, termine estas etapas:

1. Dentro do aplicativo ASDM, clique a **configuração**, e clique então o **VPN**.
2. Expanda o **WebVPN**, e escolha o **acesso WebVPN**.

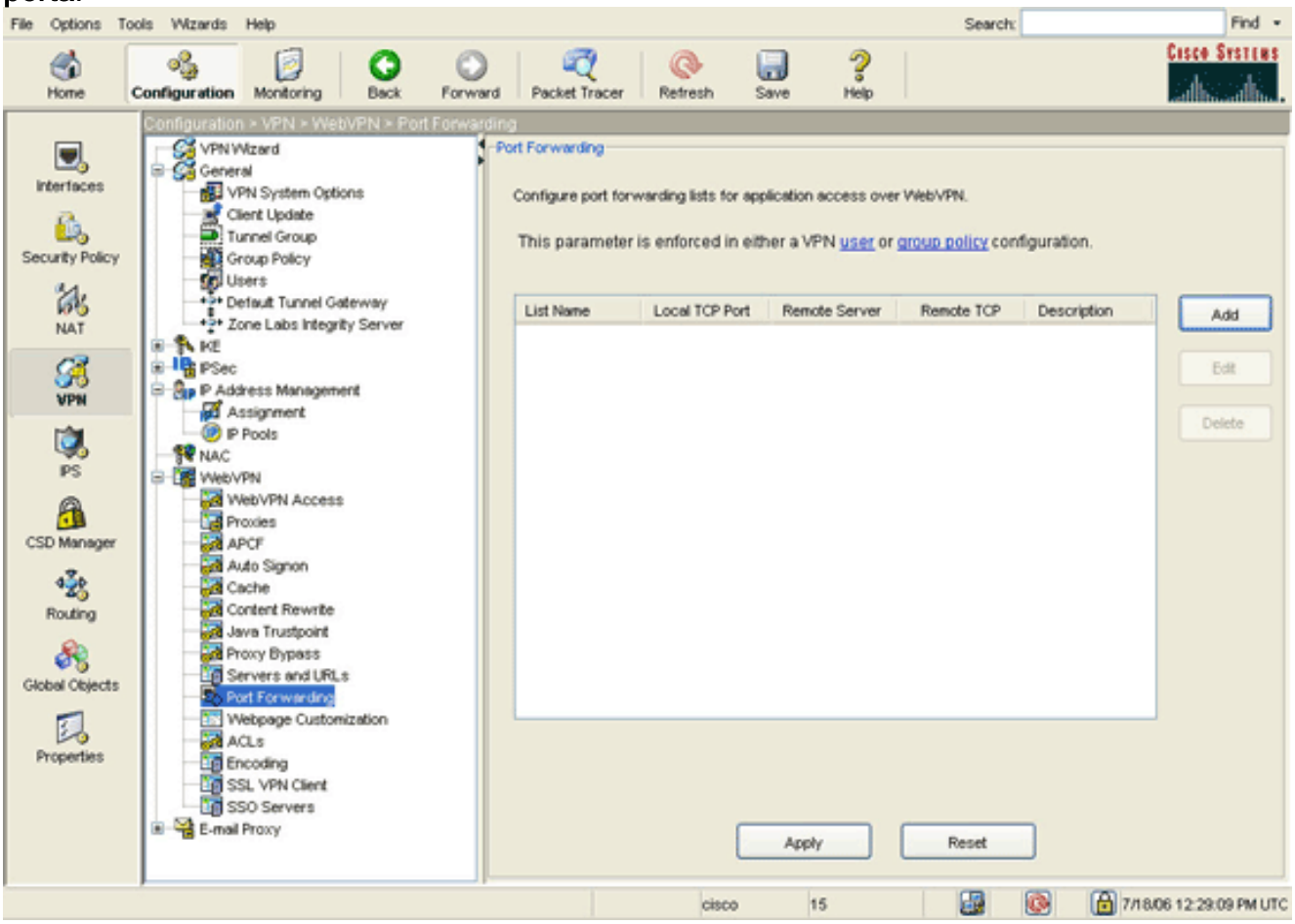


3. Destaque a relação, e o clique **permite**.
4. O clique **aplica-se**, clica-se a **salvaguarda**, e clica-se então **sim** para aceitar as mudanças.

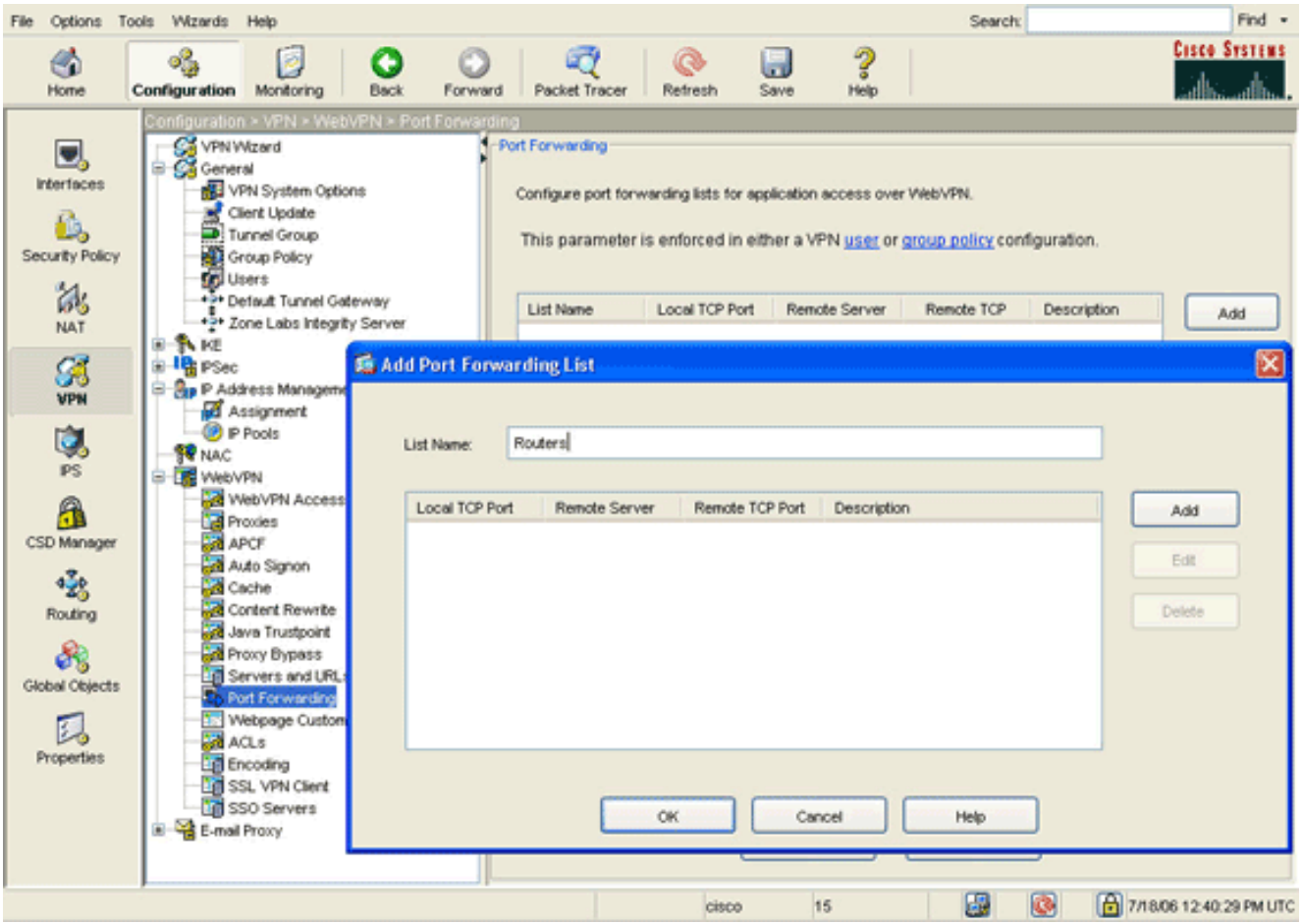
Etapa 2. Configurar características da transmissão da porta

A fim configurar características da transmissão da porta, termine estas etapas:

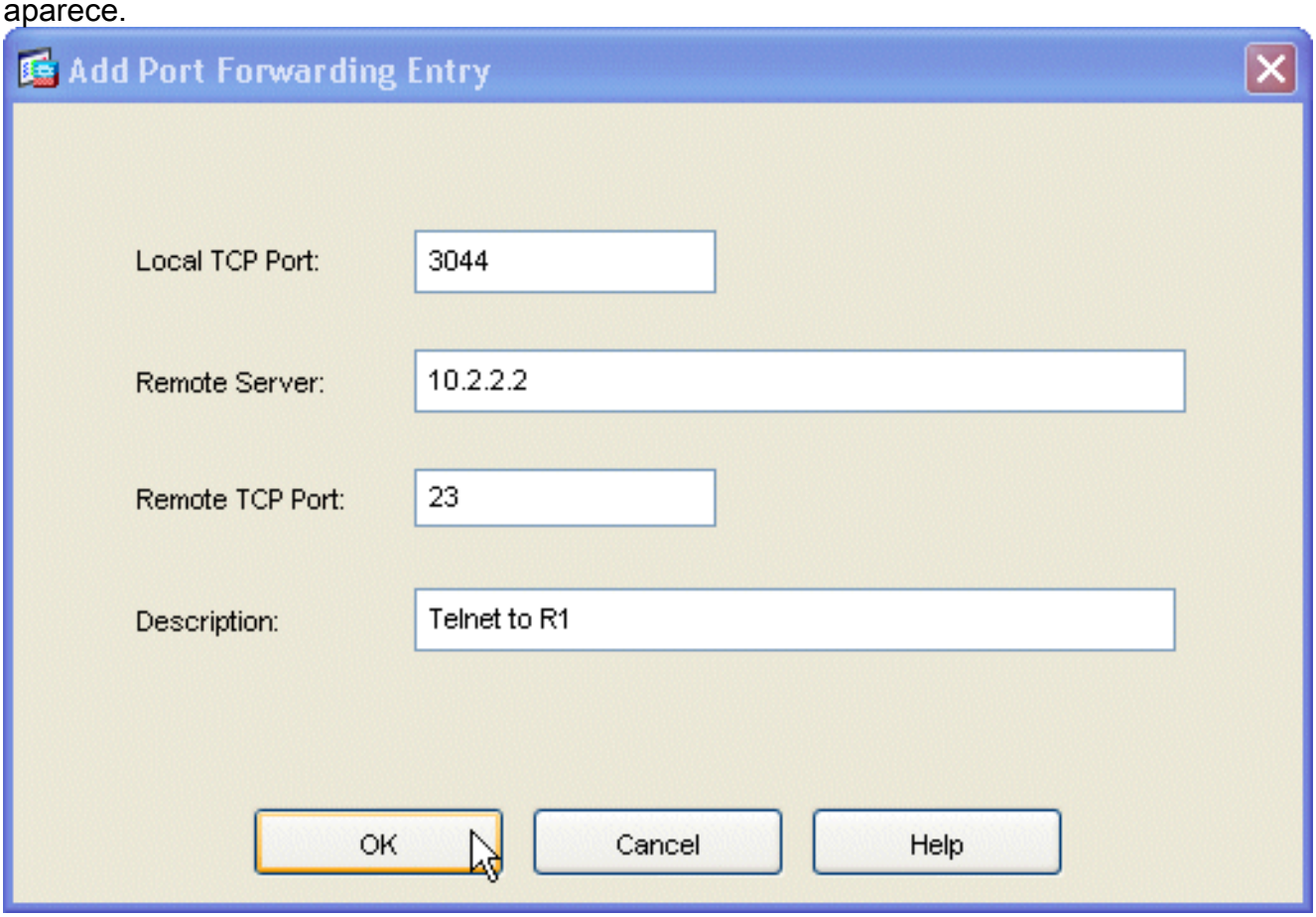
1. Expanda o **WebVPN**, e escolha a **transmissão da porta**.



2. Clique no botão Adicionar.



3. Na caixa de diálogo da lista da transmissão da porta adicionar, dê entrada com um nome de lista, e o clique **adiciona**.A caixa de diálogo da entrada de encaminhamento da porta adicionar
aparece.



4. Na caixa de diálogo da entrada de encaminhamento da porta adicionar, incorpore estas

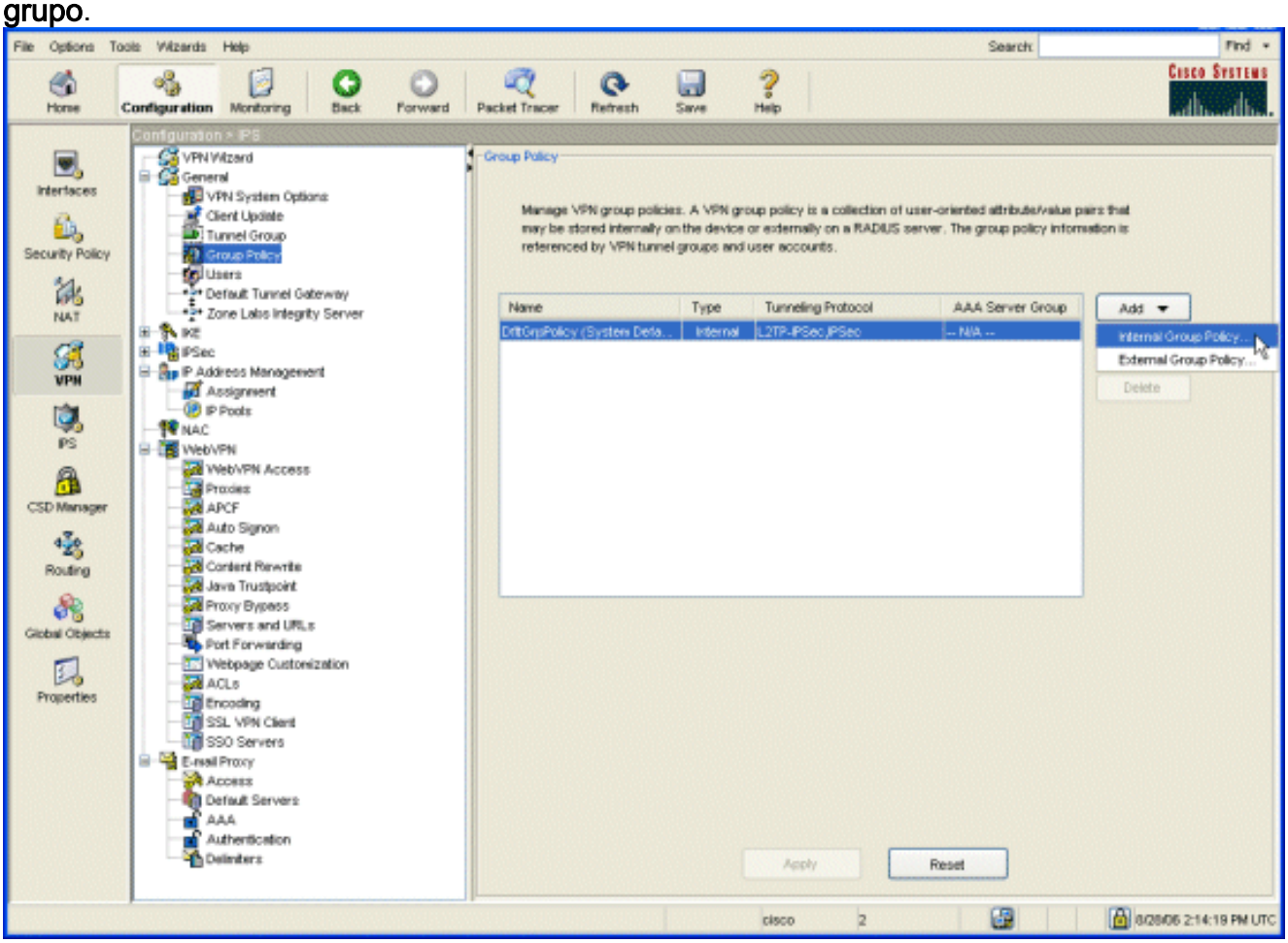
opções:No campo de porta TCP local, entre em um número de porta ou aceite o valor padrão.O valor que você incorpora pode ser todo o número desde 1024 a 65535.No campo do servidor remoto, incorpore um endereço IP de Um ou Mais Servidores Cisco ICM NT.Este exemplo usa o endereço do roteador.No campo de porta TCP remoto, entre em um número de porta.Este exemplo usa a porta 23.No campo de descrição, incorpore uma descrição, e clique a **APROVAÇÃO**.

5. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

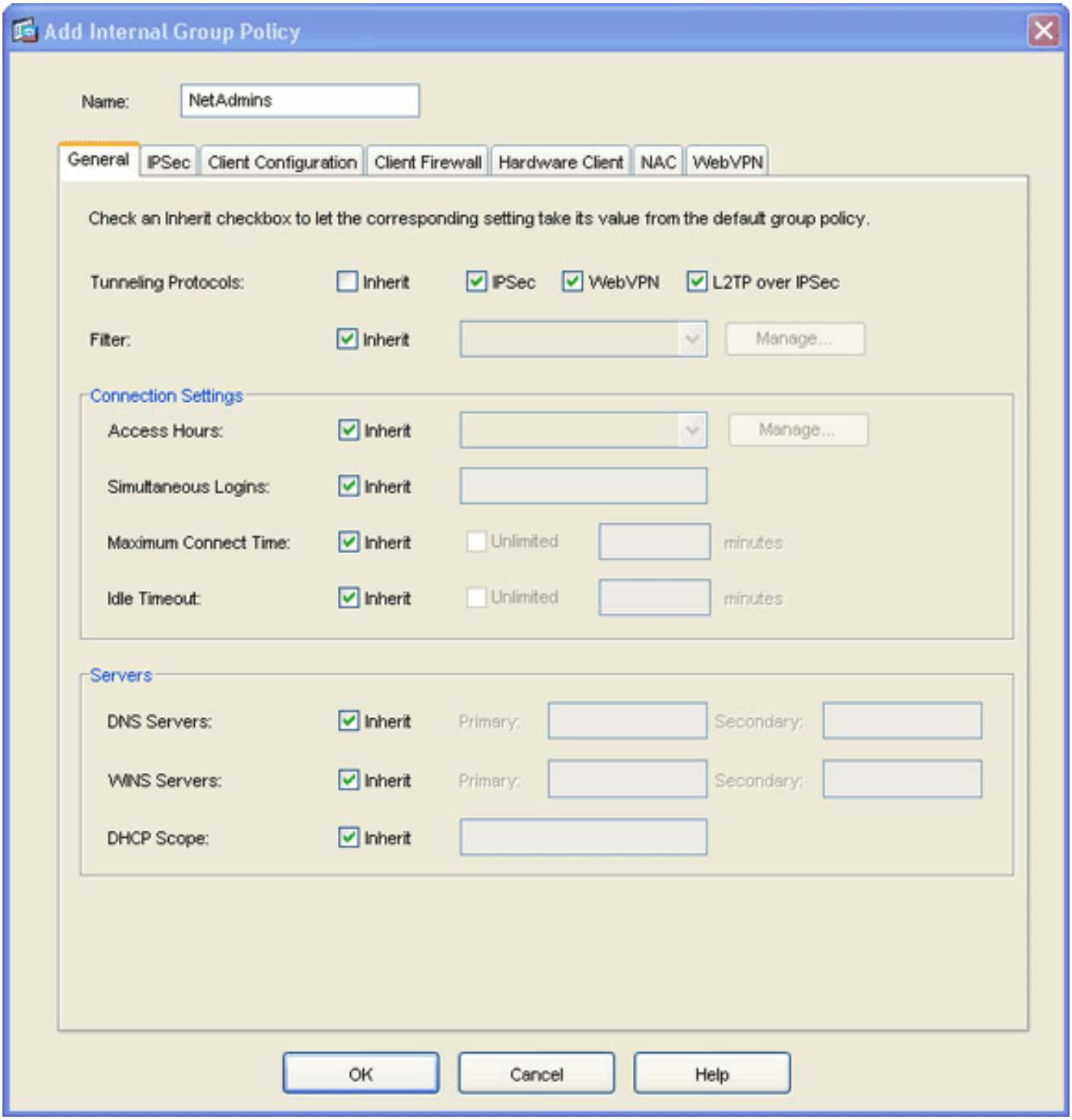
Etapa 3. Crie uma política do grupo e ligue-a à lista da transmissão da porta

A fim criar uma política do grupo e ligá-la à lista da transmissão da porta, termine estas etapas:

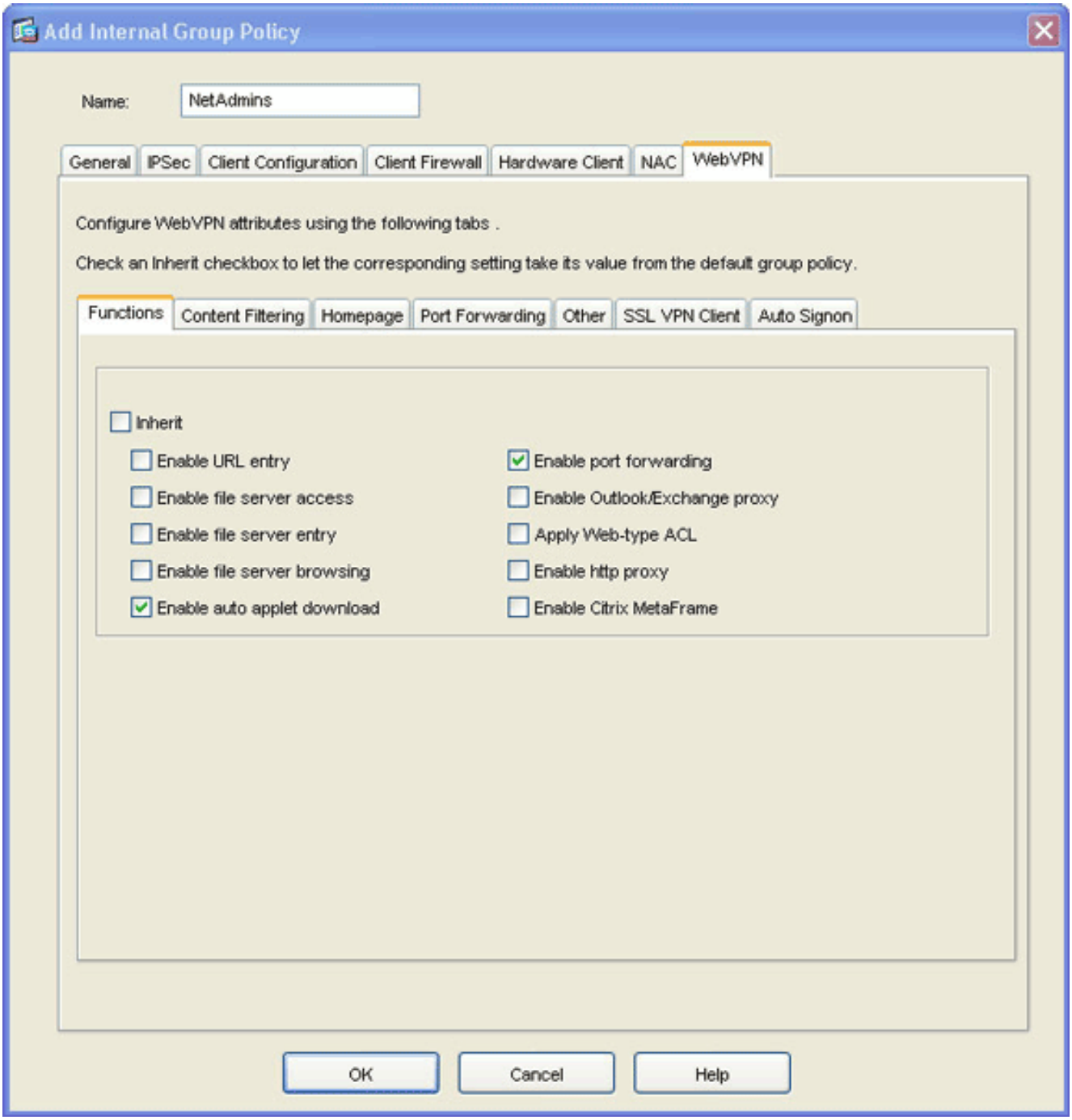
1. Expanda o **general**, e escolha a **política do grupo**.



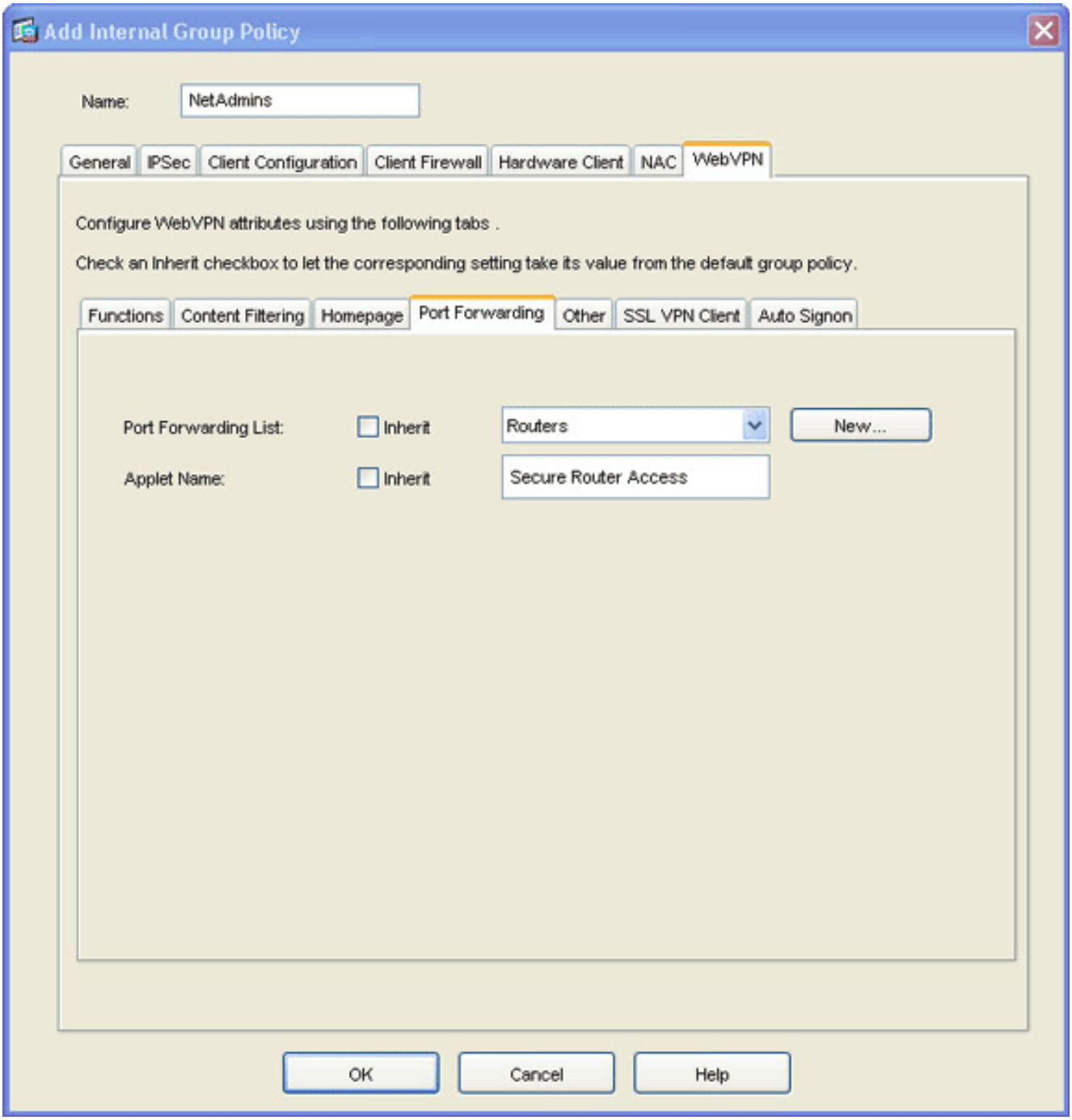
2. O clique **adiciona**, e escolhe a **Política interna de grupo**.A caixa de diálogo da Política interna de grupo adicionar aparece.



3. Dê entrada com um nome ou aceite o nome da política do grupo padrão.
4. Desmarcar os protocolos de tunelamento **herdam a** caixa de verificação, e verificam a caixa de verificação **WebVPN**.
5. Clique a aba **WebVPN** situada na parte superior da caixa de diálogo, e clique então a aba das **funções**.
6. Desmarcar a caixa de verificação **herdar**, e verifique **transferência do applet da possibilidade a auto** e **permita** caixas de seleção da **transmissão da porta** segundo as indicações desta imagem:



7. Igualmente dentro da aba WebVPN, clique a aba de **transmissão da porta**, e desmarcar a lista da transmissão da porta **herdam a** caixa de verificação.



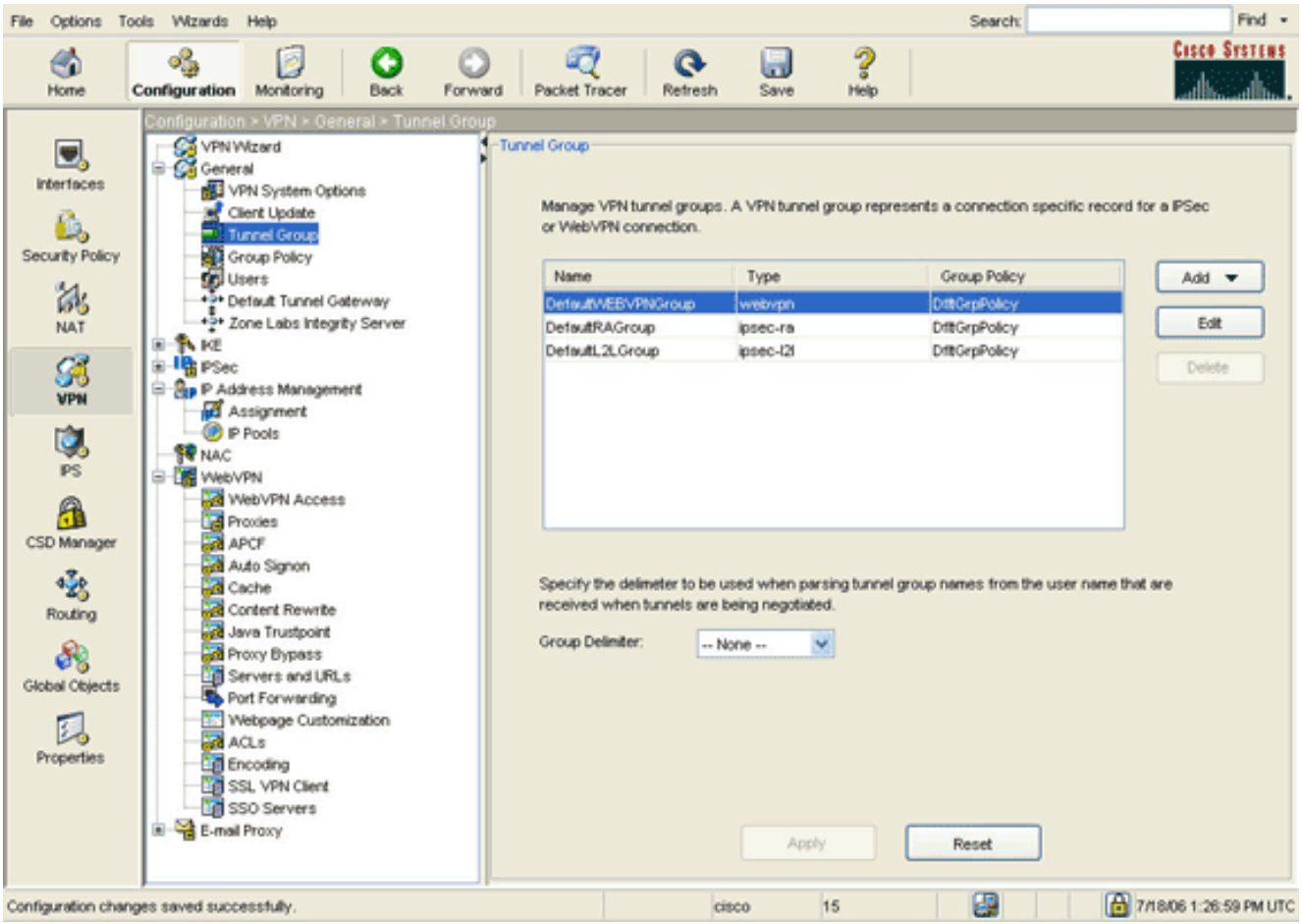
8. Clique a seta da gota-para baixo da **lista da transmissão da porta**, e escolha a lista que da transmissão da porta você criou em etapa 2.
9. Desmarcar o nome do applet **herdam a** caixa de verificação, e mudam o nome no campo de texto.O cliente indica o nome do applet na conexão.
10. **A APROVAÇÃO do** clique, e clica então **aplica-se**.
11. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Etapa 4. Crie um grupo de túneis e ligue-o à política do grupo

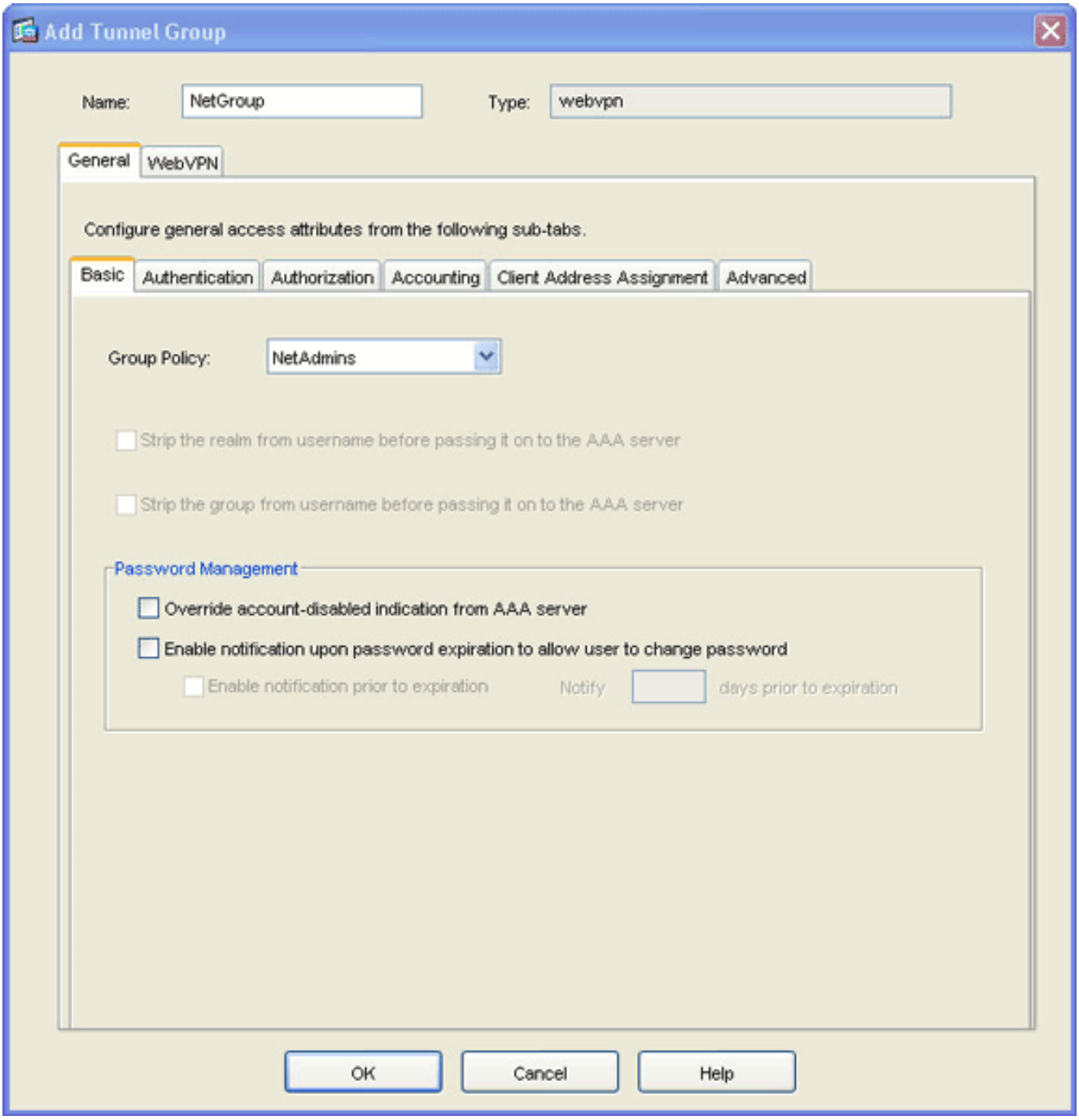
Você pode editar o grupo de túneis de *DefaultWebVPNGroup do* padrão ou criar um grupo de túneis novo.

A fim criar um grupo de túneis novo, termine estas etapas:

1. Expanda o **general**, e escolha o **grupo de túneis**.



2. O clique **adiciona**, e escolhe o **acesso WebVPN**.A caixa de diálogo do grupo de túneis adicionar
aparece.

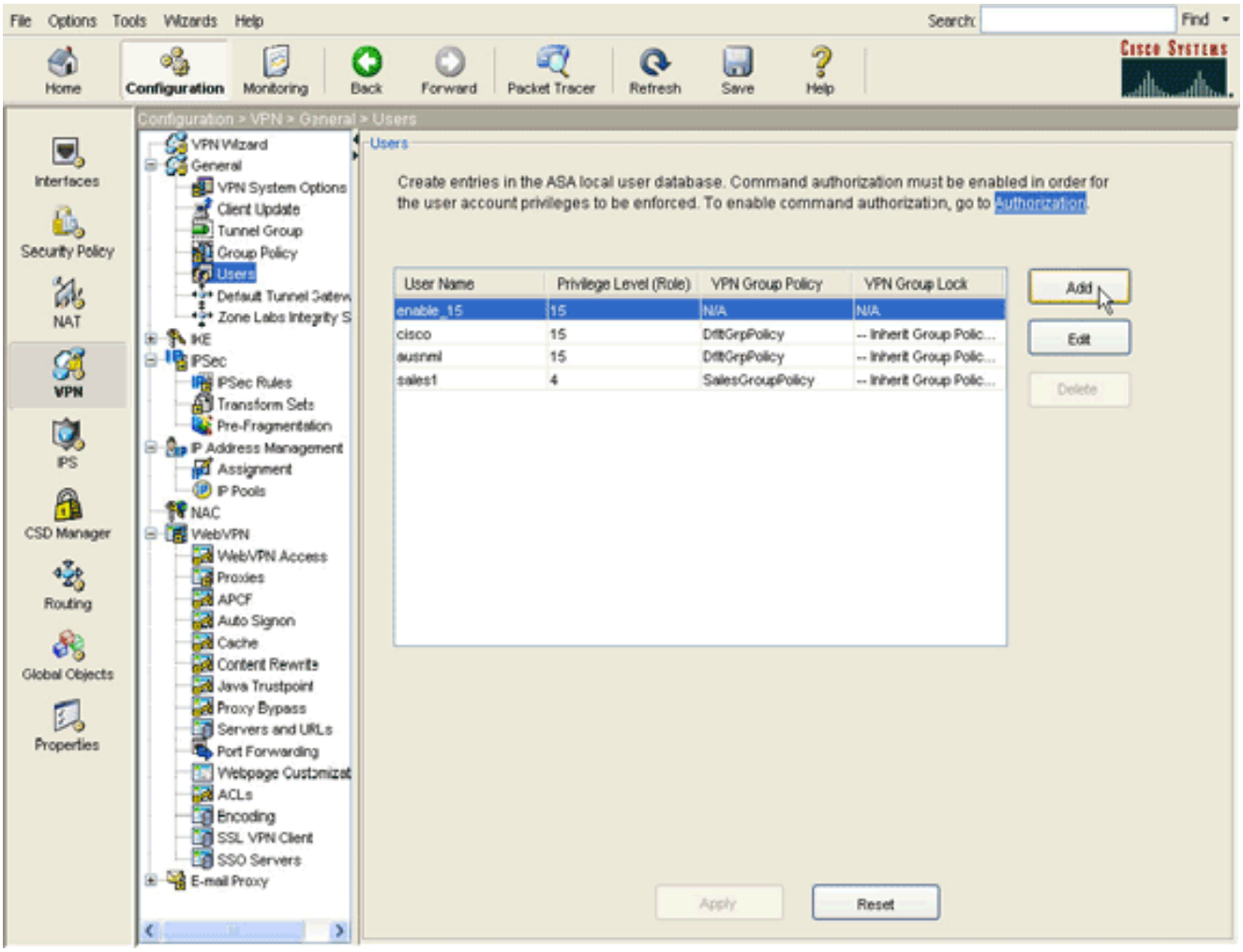


3. Dê entrada com um nome no campo de nome.
4. Clique a seta da gota-para baixo da **política do grupo**, e escolha a política que do grupo você criou em etapa 3.
5. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.O grupo de túneis, a política do grupo, e as características da transmissão da porta são ligados agora.

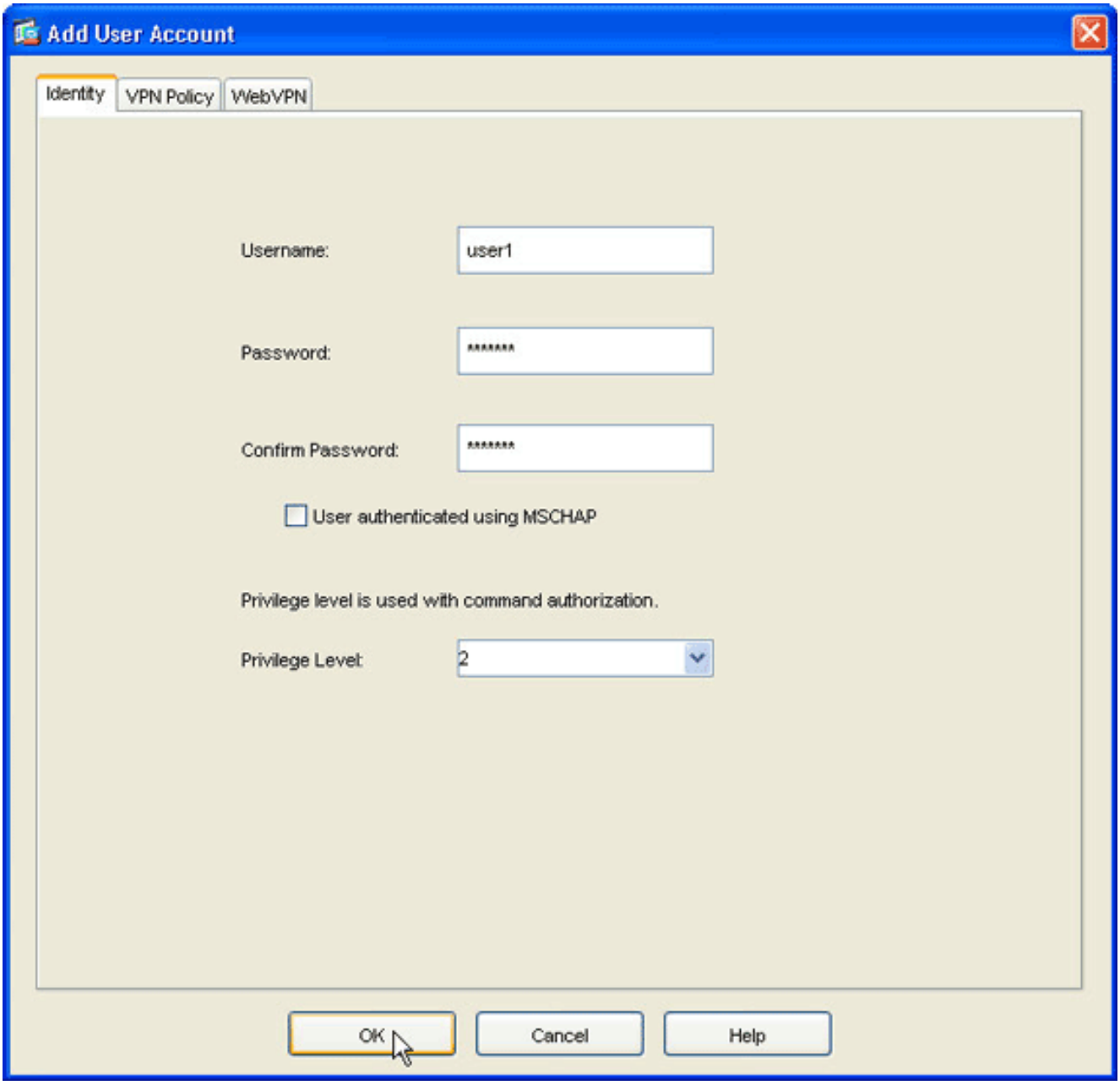
Etapa 5. Crie um usuário e adicionar esse usuário à política do grupo

A fim criar um usuário e adicionar esse usuário à política do grupo, termine estas etapas:

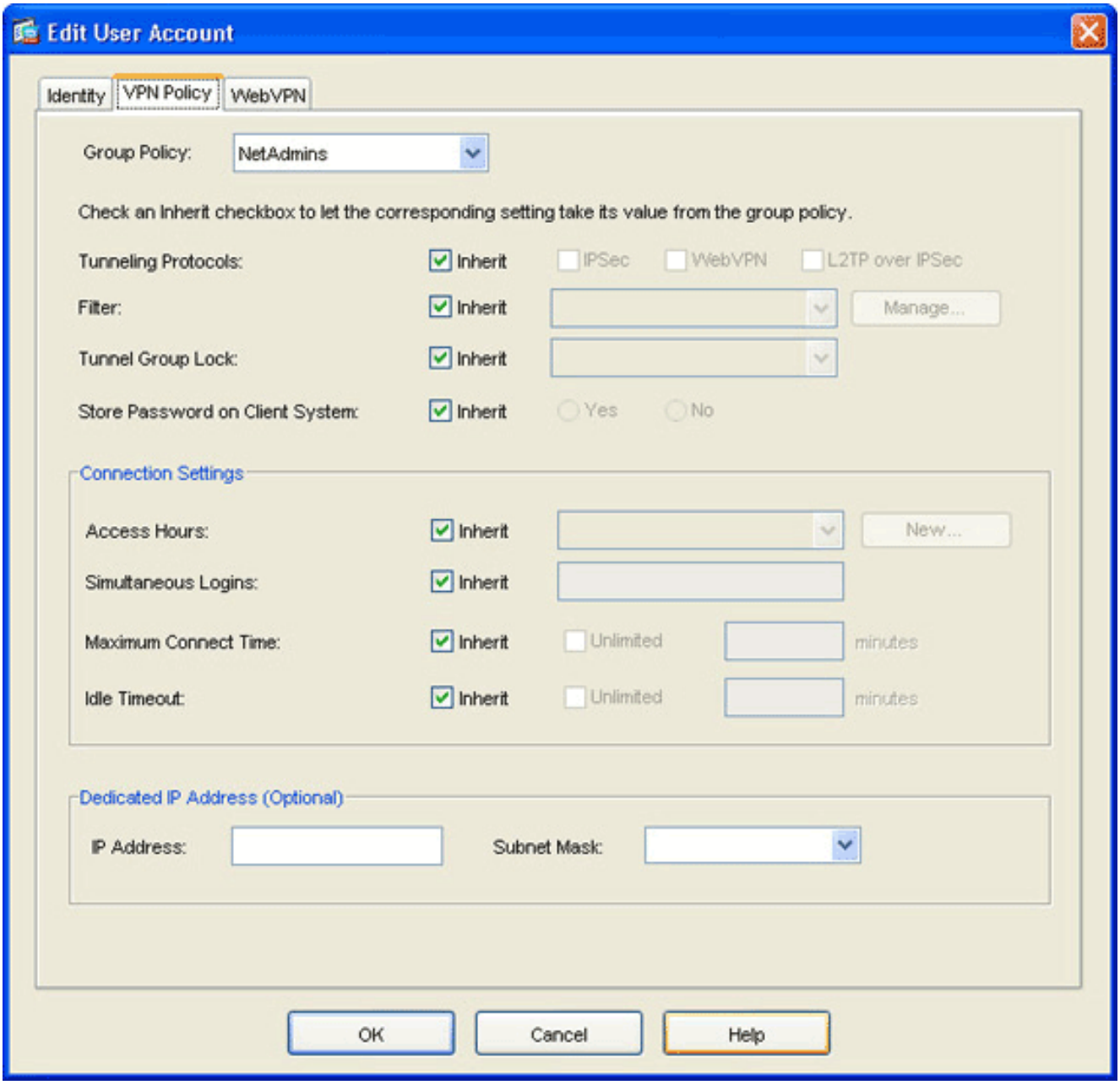
1. Expanda o **general**, e escolha **usuários**.



2. Clique no botão Adicionar.A caixa de diálogo da conta de usuário adicionar aparece.



3. Incorpore valores para o username, a senha, e a informação do privilégio, e clique então a aba da **política de VPN**.



4. Clique a seta da gota-para baixo da **política do grupo**, e escolha a política que do grupo você criou em etapa 3.Este usuário herda as características WebVPN e as políticas da política selecionada do grupo.
5. **A APROVAÇÃO do** clique, e clica então **aplica-se**.
6. **Salvaguarda do** clique, e para aceitar então **sim as** mudanças.

Configuração de VPN do thin client SSL usando o CLI

ASA
ASA Version 7.2(1) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0

```
!--- Output truncated port-forward portforward 3044
10.2.2.2 telnet Telnet to R1 !--- Configure the set of
applications that WebVPN users !--- can access over
forwarded TCP ports group-policy NetAdmins internal !--
- Create a new group policy for enabling WebVPN access
group-policy NetAdmins attributes vpn-tunnel-protocol
IPSec l2tp-ipsec webvpn !--- Configure group policy
attributes webvpn functions port-forward auto-download
!--- Configure group policies for WebVPN port-forward
value portforward !--- Configure port-forward to enable
WebVPN application access !--- for the new group policy
port-forward-name value Secure Router Access !---
Configure the display name that identifies TCP port !--
- forwarding to end users username user1 password
tJsDL6po9m1UFs.h encrypted username user1 attributes
vpn-group-policy NetAdmins !--- Create and add User(s)
to the new group policy http server enable http 0.0.0.0
0.0.0.0 DMZ no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart tunnel-group NetGroup type
webvpn tunnel-group NetGroup general-attributes
default-group-policy NetAdmins !--- Create a new tunnel
group and link it to the group policy telnet timeout 5
ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp
inspect sip inspect xdmcp ! service-policy
global_policy global webvpn enable outside !--- Enable
Web VPN on Outside interface port-forward portforward
3044 10.2.2.2 telnet Telnet to R1 prompt hostname
context
```

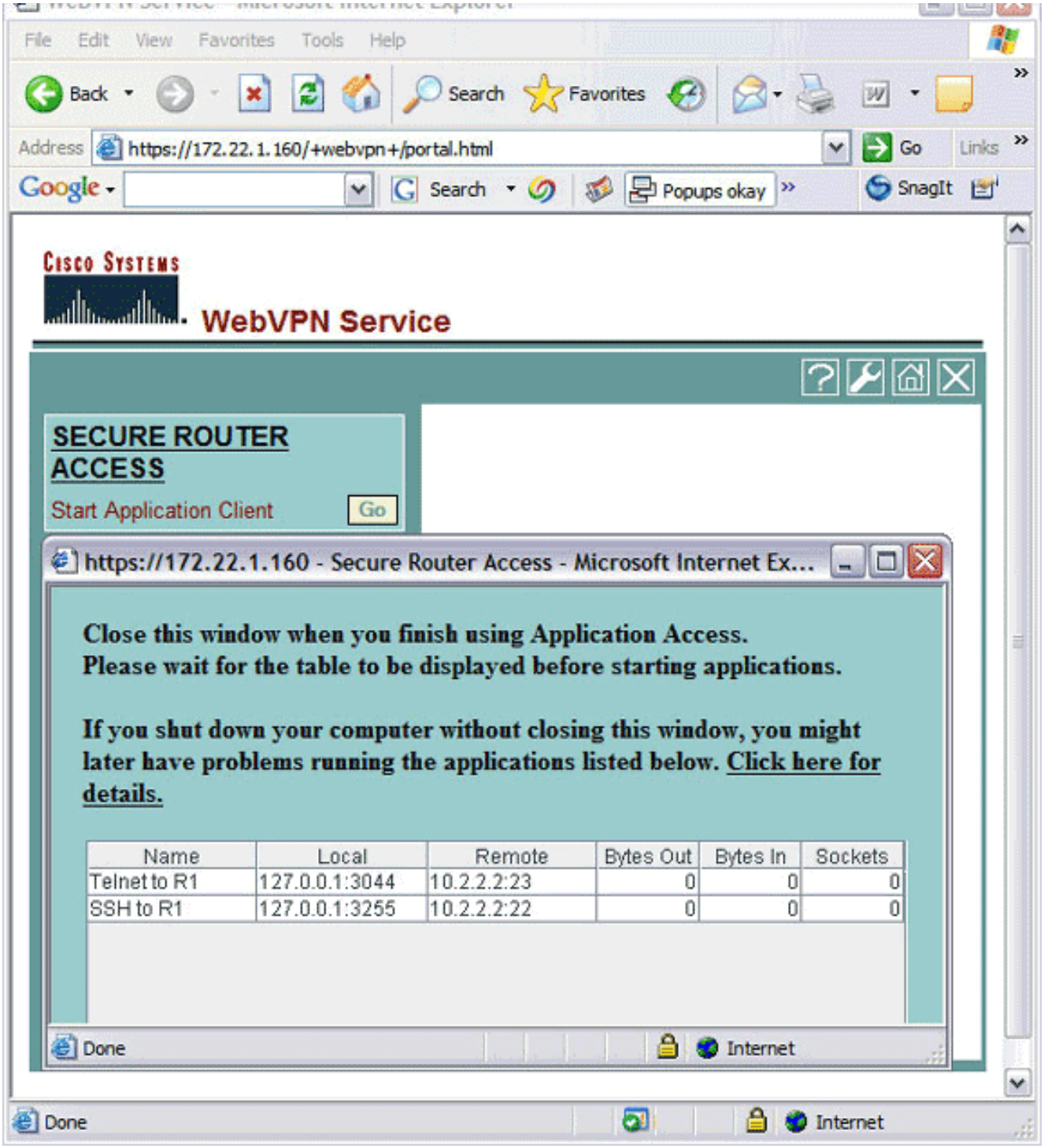
Verificar

Use esta seção para verificar que sua configuração trabalha corretamente.

Procedimento

Este procedimento descreve como determinar a validez da configuração e como testar a configuração.

1. De uma estação de trabalho cliente, incorpore o ***endereço do outside_ASA_IP de*** **https://**; onde os *outside_ASA_IPAddress* são o SSL URL do ASA.Uma vez que o certificado digital está aceitado, e o usuário está autenticado, o página da web do serviço WebVPN publica-se.

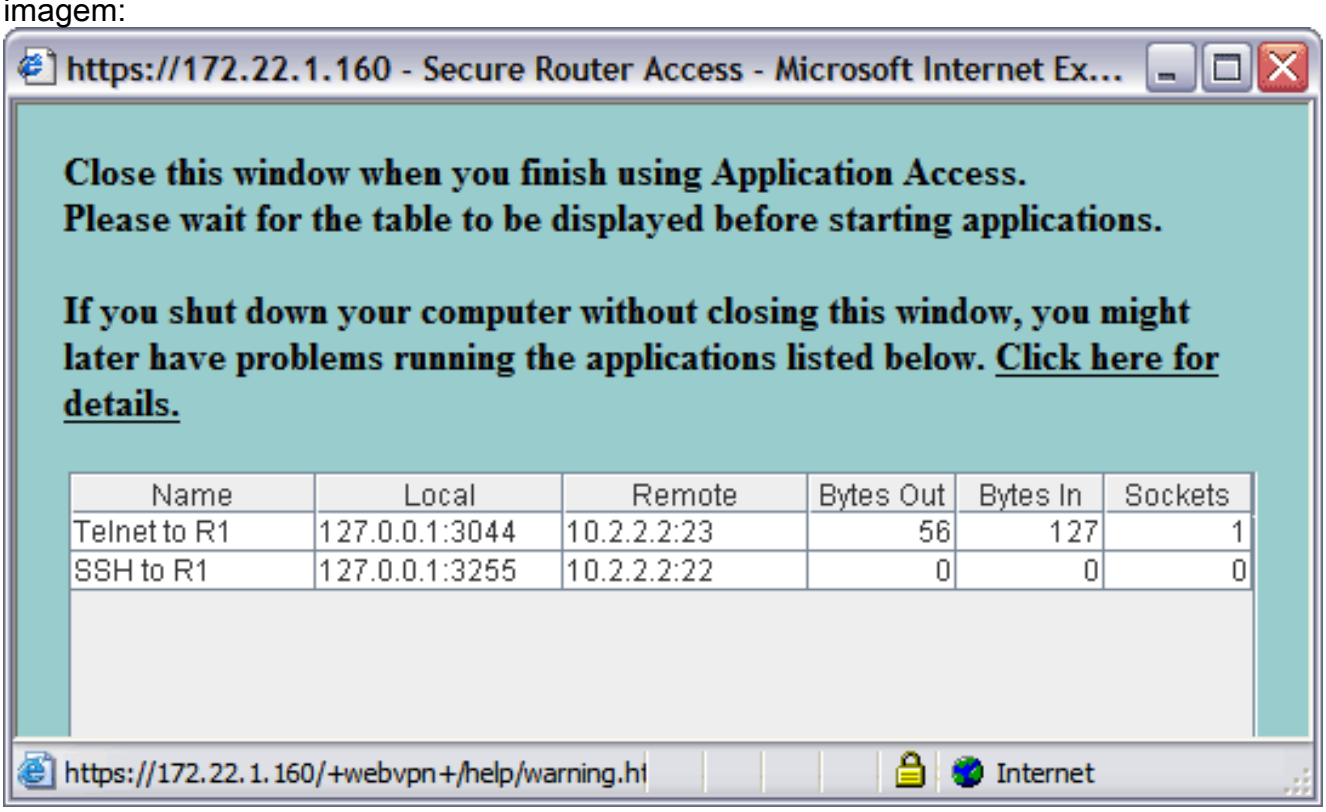


O endereço e a informação de porta exigidos para alcançar o aplicativo aparecem na coluna local. Os bytes para fora e os bytes nas colunas não indicam nenhuma atividade porque o aplicativo não foi invocado neste tempo.

2. Use o prompt do DOS ou o outro aplicativo Telnet começar uma sessão de Telnet.
3. No comando prompt, entre no **telnet 127.0.0.1 3044**.**Nota:** Este comando fornece um exemplo de como aceder à porta local indicada na imagem do página da web do serviço WebVPN neste documento. *O comando não inclui uns dois pontos (:).* Datilografe o comando como descrito neste documento.O ASA recebe o comando sobre a sessão segura, e porque armazena um mapa da informação, o ASA sabe imediatamente para abrir a sessão de telnet segura ao dispositivo
traçado.

Uma vez que você incorpora seu nome de usuário e senha, o acesso ao dispositivo está completo.

4. A fim verificar o acesso ao dispositivo, verifique os bytes para fora e bytes nas colunas segundo as indicações desta
imagem:



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

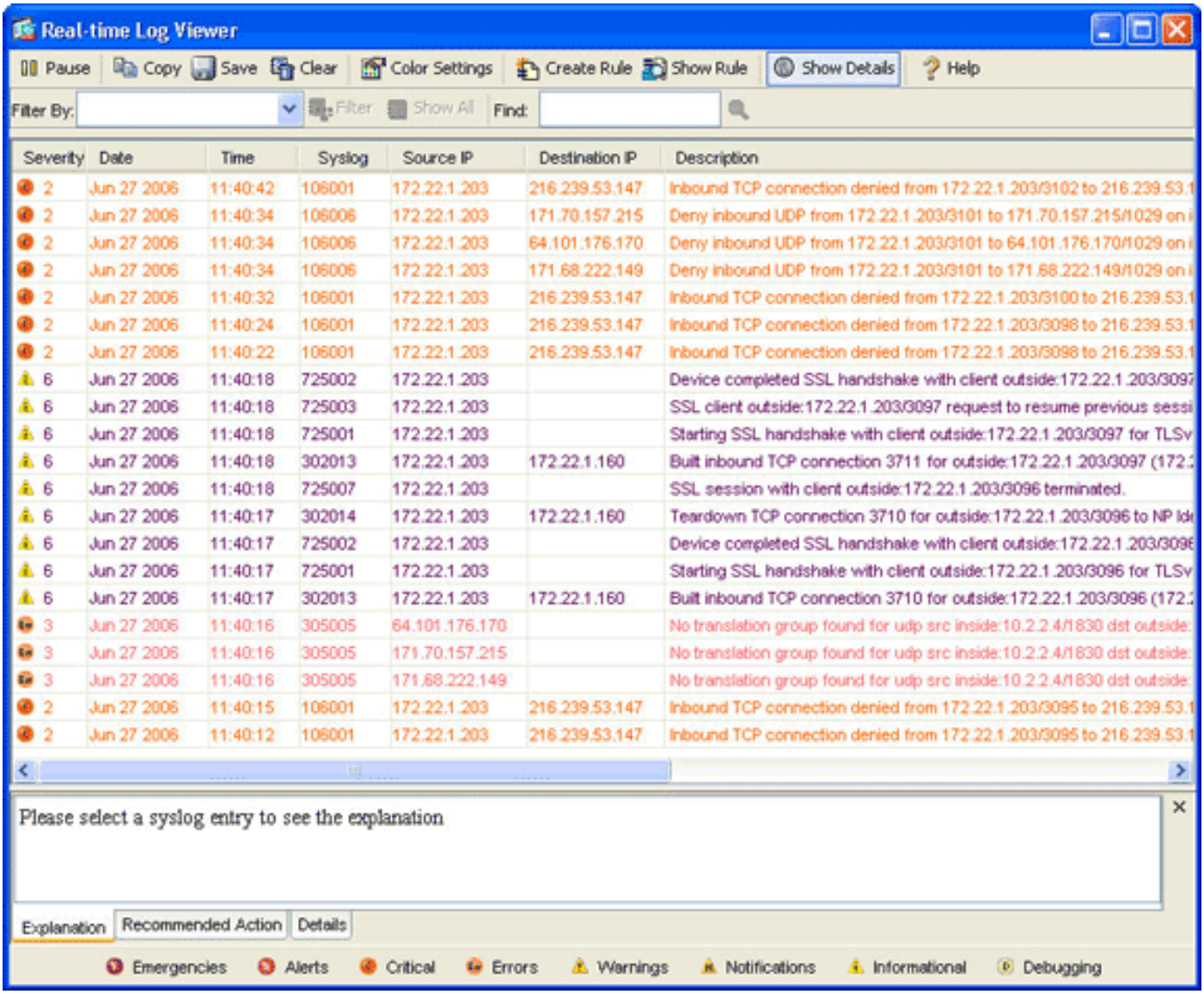
comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Está o processo da saudação de SSL completo?

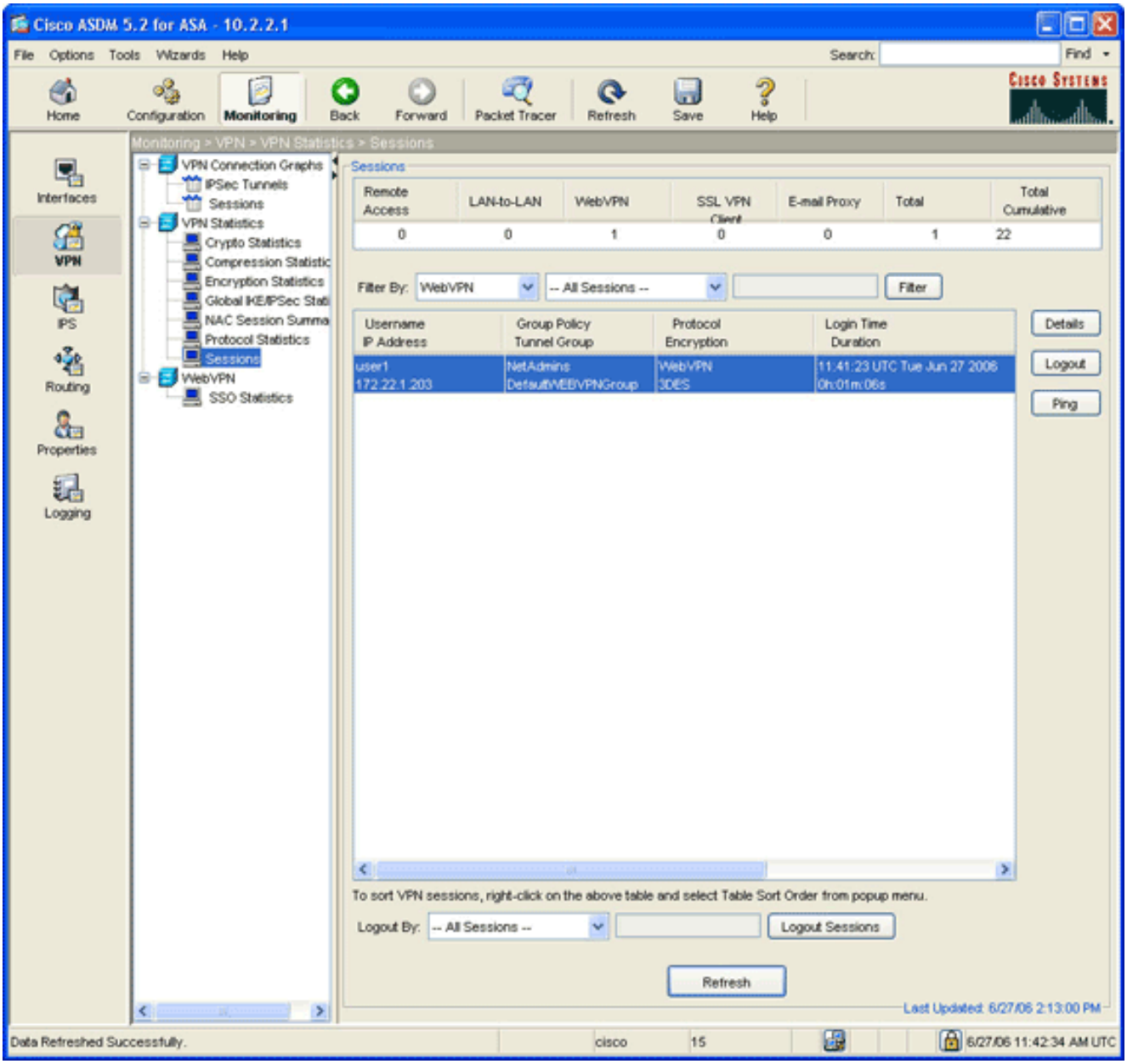
Uma vez que você conecta ao ASA, verifique se o log do tempo real mostra a conclusão da saudação de SSL.



É o thin client SSL VPN funcional?

A fim verificar que o thin client SSL VPN é funcional, termine estas etapas:

1. Clique a **monitoração**, e clique então o **VPN**.
2. Expanda **estatísticas de VPN**, e clique **sessões**.Sua sessão de thin client SSL VPN deve aparecer na lista das sessões. Seja certo filtrar pelo WebVPN segundo as indicações desta imagem:



Comandos

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

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

- Sem clientes SSL VPN (WebVPN) no exemplo de configuração ASA
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Cisco ASA 5500 Series Adaptive Security Appliances
- O ASA com WebVPN e escolhe Sinal-em usar o exemplo de configuração ASDM e NTLMv1
- Suporte Técnico e Documentação - Cisco Systems