Exemplo de configuração de VPN SSL thin-client (WebVPN) no ASA com ASDM

Contents

Introduction

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.

- **VPN SSL sem cliente (WebVPN)**—Fornece um cliente remoto que exige um navegador Web habilitado para SSL para acessar servidores Web HTTP ou HTTPS em uma rede local corporativa (LAN). Além disso, a VPN SSL sem cliente fornece acesso para a navegação de arquivos do Windows através do protocolo CIFS (Common Internet File System). O Outlook Web Access (OWA) é um exemplo de acesso HTTP.Consulte Exemplo de Configuração de VPN SSL Sem Clientes (WebVPN) no ASA para saber mais sobre a VPN SSL Sem Clientes.

- **Thin-Client SSL VPN (Port Forwarding)**—Fornece um cliente remoto que faz o download de um pequeno miniaplicativo baseado em Java e permite acesso seguro para aplicativos TCP (Transmission Control Protocol) que usam números de porta estáticos. Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), secure shell (ssh) e Telnet são exemplos de acesso seguro. Como os arquivos na máquina local mudam, os usuários devem ter privilégios administrativos locais para usar esse método. Esse método de VPN SSL não funciona com aplicativos que usam atribuições de porta dinâmicas, como alguns aplicativos de protocolo de transferência de arquivos (FTP).**Observação:** o User Datagram Protocol (UDP) não é suportado.
- **SSL VPN Client (Tunnel Mode)** — Faz download de um pequeno cliente para a estação de trabalho remota e permite acesso totalmente seguro aos recursos em uma rede corporativa interna. Você pode baixar permanentemente o SSL VPN Client (SVC) em uma estação de trabalho remota ou pode remover o cliente quando a sessão segura é fechada.Consulte Exemplo de Configuração de SSL VPN Client (SVC) no ASA com ASDM para saber mais sobre o SSL VPN Client.

Este documento demonstra uma configuração simples para o Thin-Client SSL VPN no Adaptive Security Appliance (ASA). A configuração permite que um usuário faça telnet com segurança para um roteador localizado no interior do ASA. A configuração neste documento é suportada para o ASA versão 7.x e posterior.

Prerequisites

Requirements

Antes de tentar esta configuração, verifique se você atende a estes requisitos para as estações cliente remotas:

- navegador da Web habilitado para SSL
- SUN Java JRE versão 1.4 ou posterior
- Cookies ativados
- Bloqueadores de pop-up desabilitados
- Privilégios administrativos locais (não obrigatórios, mas altamente sugeridos)

Observação: a versão mais recente do SUN Java JRE está disponível como download gratuito no site Java.

Componentes Utilizados

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

- Cisco Adaptive Security Appliance série 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Observação:** consulte Permitindo Acesso HTTPS para ASDM para permitir que o ASA seja configurado pelo ASDM.
- Software Cisco Adaptive Security Appliance versão 7.2(1)
- Cliente remoto do Microsoft Windows XP Professional (SP 2)

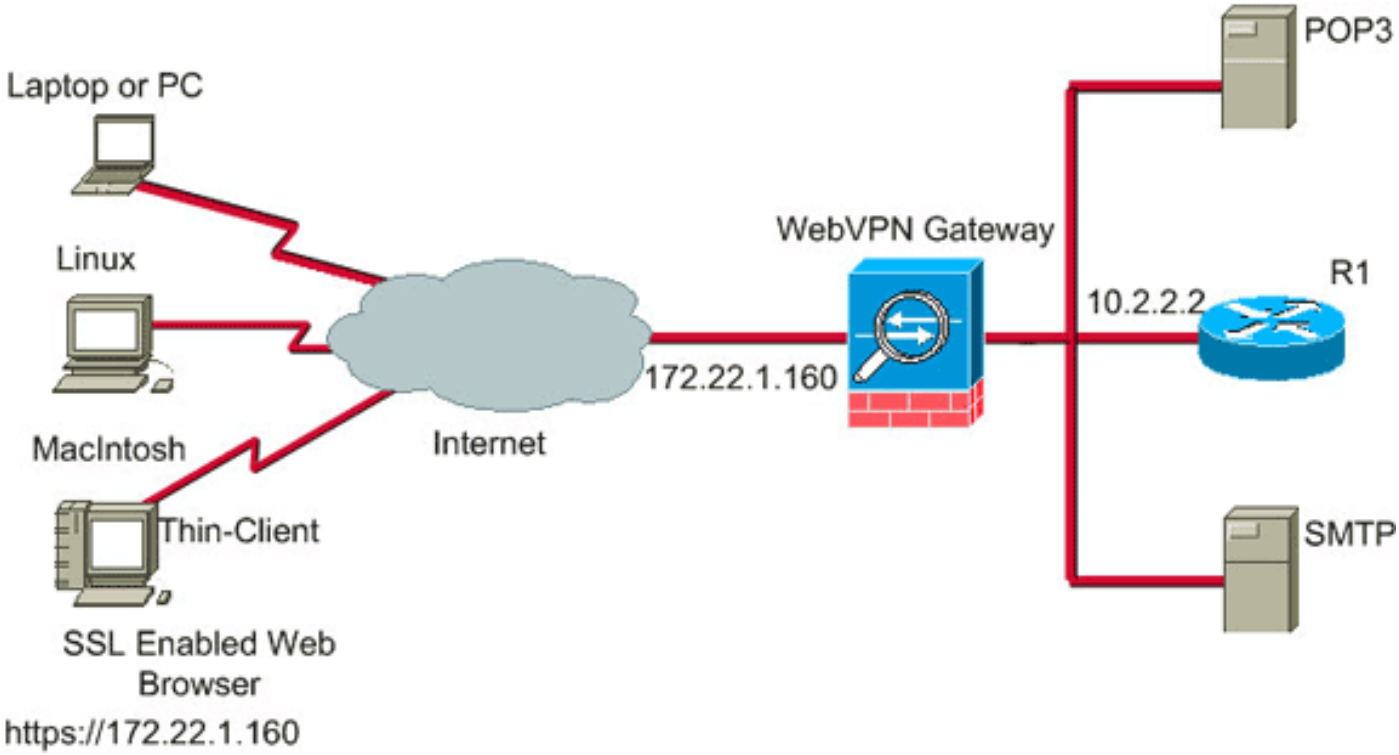
As informações neste documento foram desenvolvidas em um ambiente de laboratório. Todos os dispositivos usados neste documento foram redefinidos para sua configuração padrão. Se sua rede estiver ativa, certifique-se de que você entendeu o impacto potencial de qualquer comando. Todos os endereços IP usados nesta configuração foram selecionados de endereços RFC 1918

em um ambiente de laboratório; esses endereços IP não são roteáveis na Internet e são apenas para fins de teste.

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 faz o download de um pequeno miniaplicativo Java para a estação de trabalho. O cliente recebe uma lista de recursos pré-configurados.



Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

Para iniciar uma sessão, o cliente remoto abre um navegador SSL para a interface externa do ASA. Depois que a sessão é estabelecida, o usuário pode usar os parâmetros configurados no ASA para invocar qualquer Telnet ou acesso de aplicativo. O ASA faz o proxy da conexão segura e permite que o usuário acesse o dispositivo.

Observação: as listas de acesso de entrada não são necessárias para essas conexões porque o ASA já está ciente do que constitui uma sessão legal.

Configuração de VPN SSL Thin-Client usando ASDM

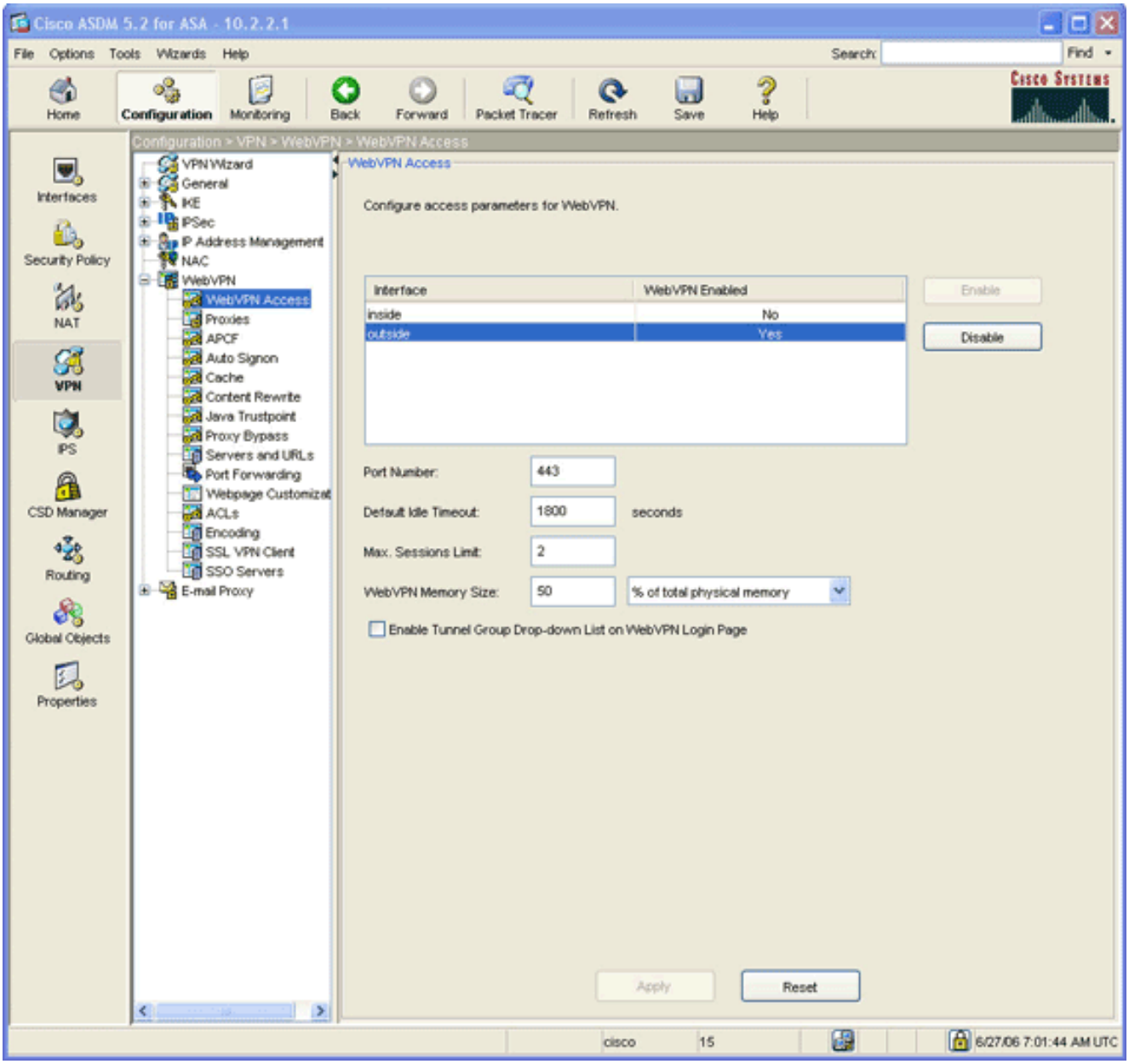
Para configurar o Thin-Client SSL VPN no ASA, faça o seguinte:

1. Habilitar WebVPN no ASA
2. Configurar características de encaminhamento de porta
3. Crie uma Política de Grupo e vincule-a à Lista de Encaminhamento de Portas (criada na Etapa 2)
4. Crie um Grupo de Túneis e vincule-o à Política de Grupo (criada na Etapa 3)
5. Crie um usuário e adicione esse usuário à política de grupo (criada na Etapa 3)

Etapa 1. Habilitar WebVPN no ASA

Para habilitar o WebVPN no ASA, faça o seguinte:

1. No aplicativo ASDM, clique em **Configuration** e em **VPN**.
2. Expanda **WebVPN** e escolha **WebVPN Access**.

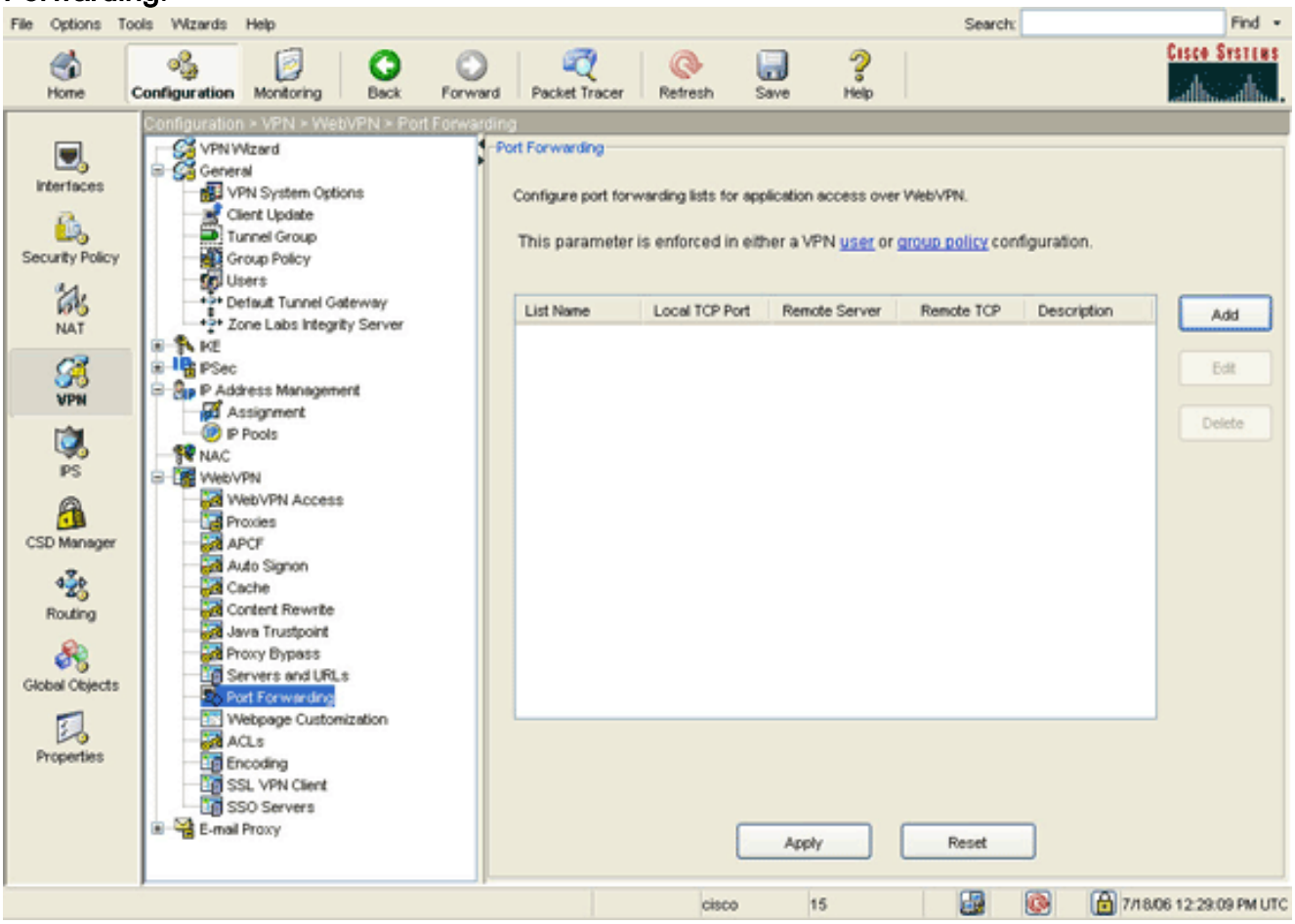


3. Realce a interface e clique em **Enable (Habilitar)**.
4. Clique em **Aplicar**, clique em **Salvar** e clique em **Sim** para aceitar as alterações.

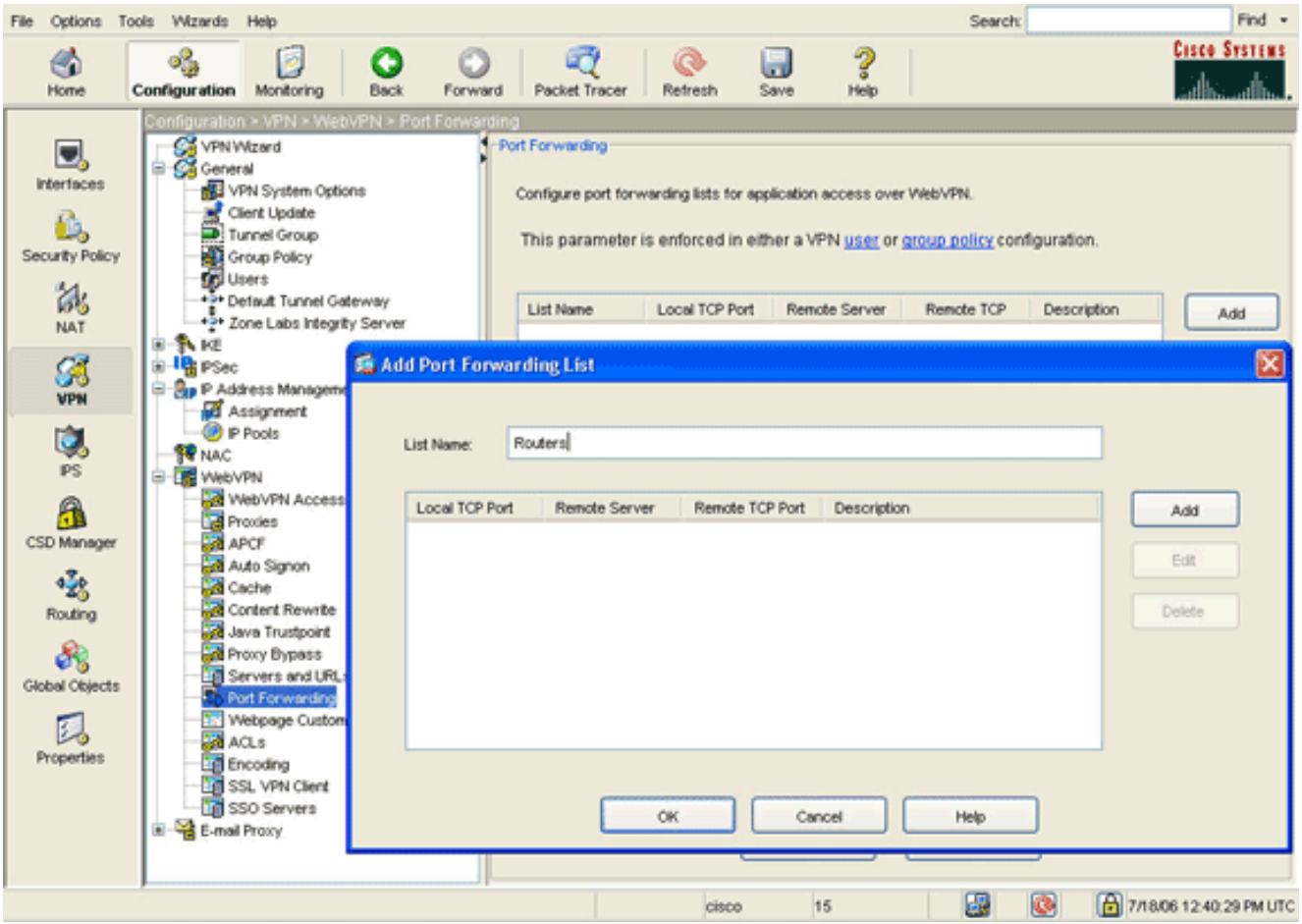
Etapa 2. Configurar características de encaminhamento de porta

Para configurar as características de encaminhamento de portas, faça o seguinte:

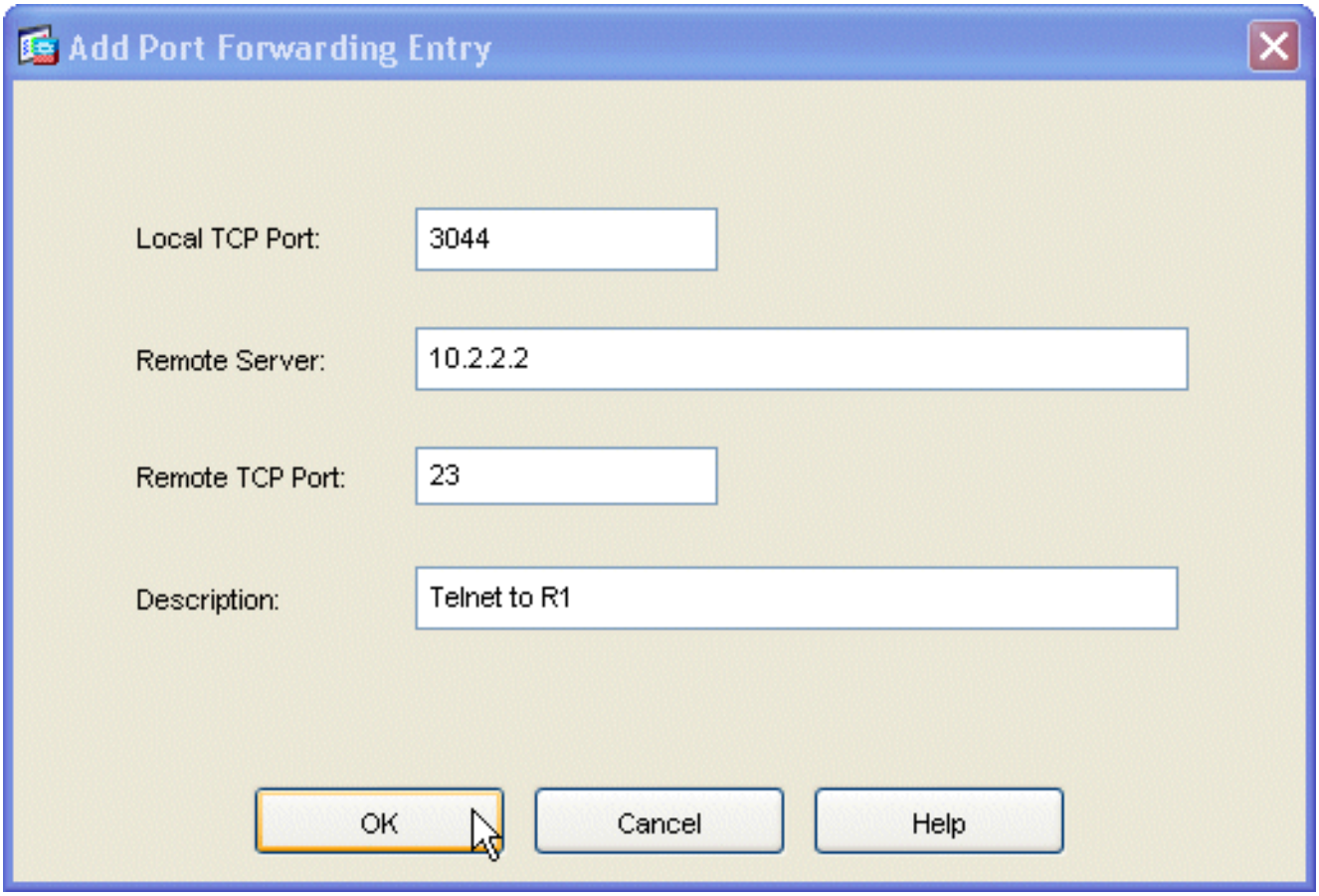
1. Expanda **WebVPN** e escolha **Port Forwarding**.



2. Clique no botão Adicionar.



3. Na caixa de diálogo Add Port Forwarding List (Adicionar lista de encaminhamento de portas), digite um nome de lista e clique em **Add**.A caixa de diálogo Add Port Forwarding Entry é
exibida.



4. Na caixa de diálogo Adicionar entrada de encaminhamento de porta, digite estas opções:No

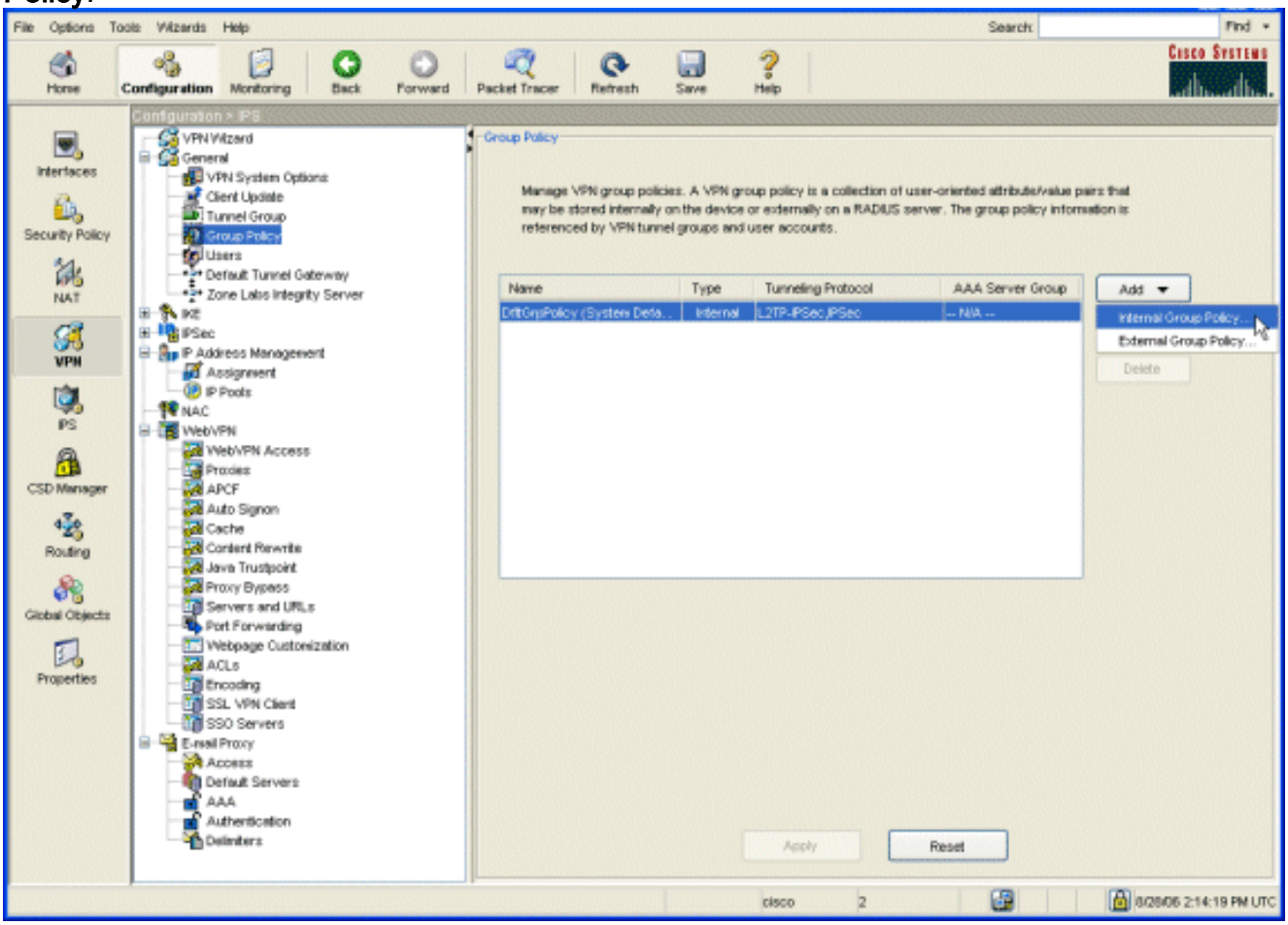
campo Porta TCP local, insira um número de porta ou aceite o valor padrão.O valor digitado pode ser qualquer número de 1024 a 65535.No campo Servidor remoto, insira um endereço IP.Este exemplo usa o endereço do roteador.No campo Remote TCP Port (Porta TCP remota), insira um número de porta.Este exemplo usa a porta 23.No campo Descrição, digite uma descrição e clique em **OK**.

5. Clique em **OK** e em **Aplicar**.
6. Clique em **Save** e, em seguida, clique em **Yes para aceitar as alterações.**

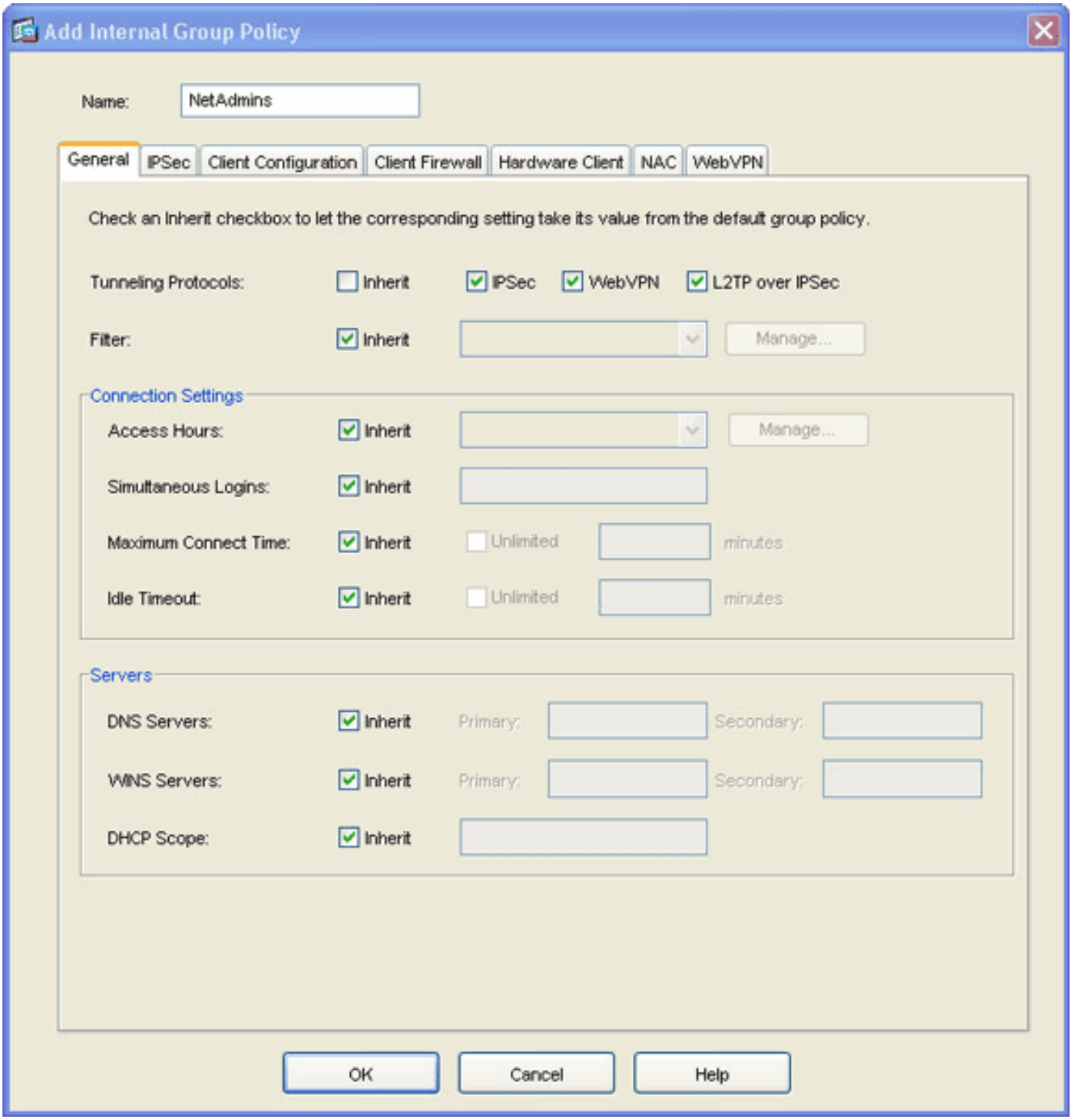
Etapa 3. Crie uma política de grupo e vincule-a à lista de encaminhamento de portas

Para criar uma política de grupo e vinculá-la à lista de encaminhamento de portas, faça o seguinte:

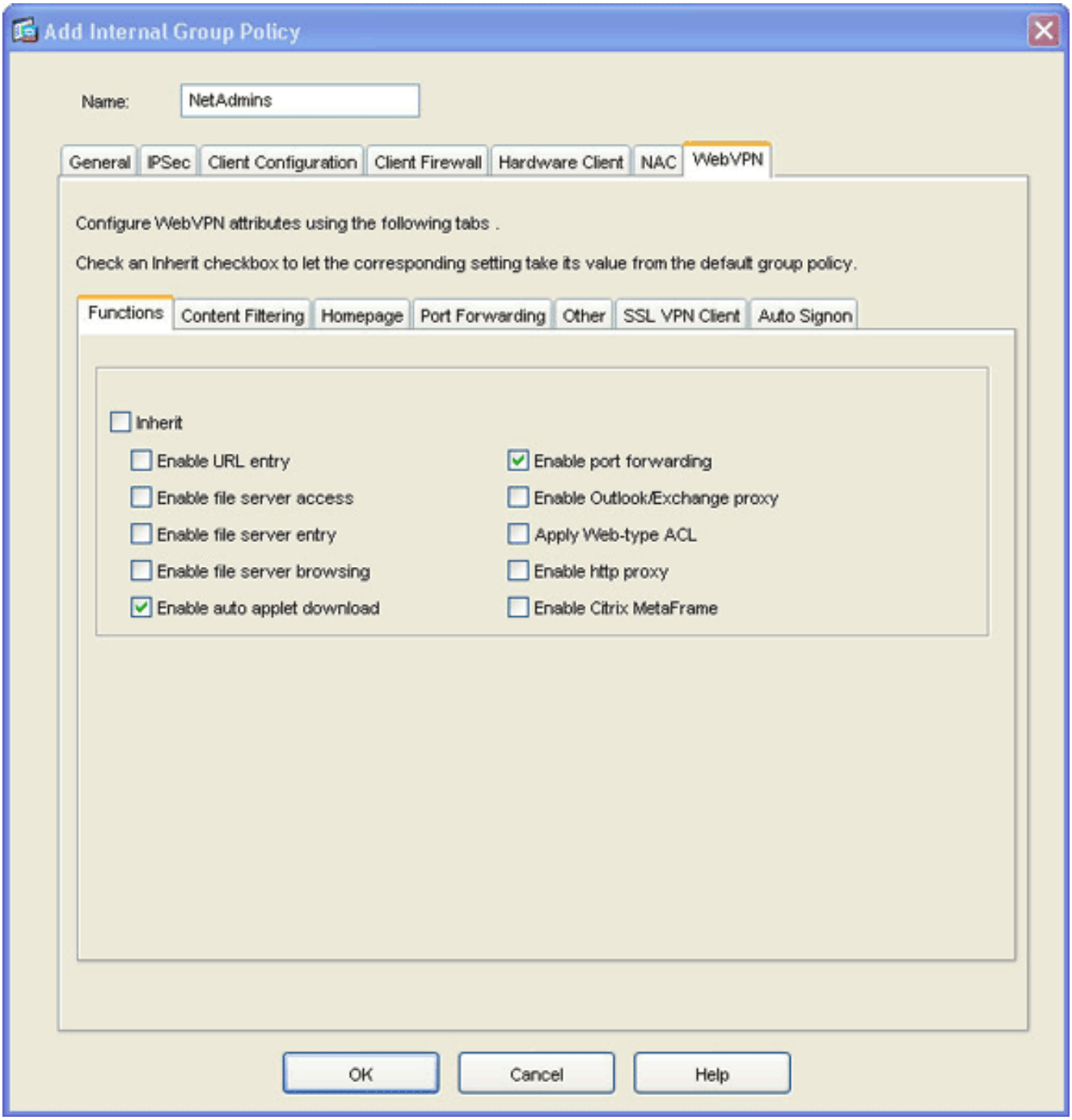
1. Expanda **General** e escolha **Group Policy**.



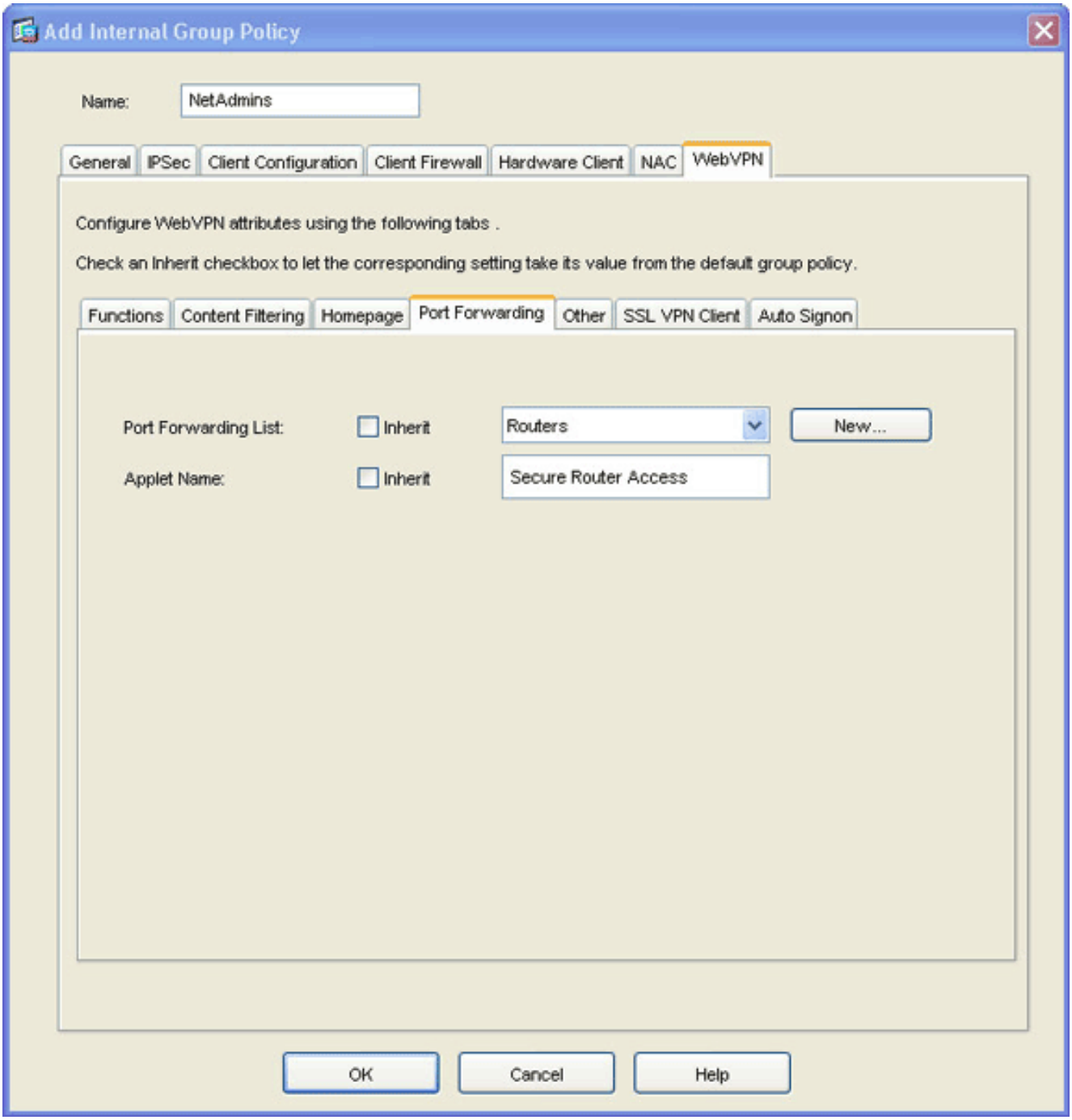
2. Clique em **Add** e escolha **Internal Group Policy**.A caixa de diálogo Add Internal Group Policy é
exibida.



3. Insira um nome ou aceite o nome padrão da política de grupo.
4. Desmarque a caixa de seleção Tunneling Protocols **Inherit** e marque a caixa de seleção **WebVPN**.
5. Clique na guia **WebVPN** localizada na parte superior da caixa de diálogo e clique na guia **Functions**.
6. Desmarque a caixa de seleção **Inherit** e marque as caixas de seleção **Enable auto applet download** e **Enable port forwarding** como mostrado nesta imagem:



7. Além disso, na guia WebVPN, clique na caixa de seleção **Port Forwarding** (Encaminhamento de portas) e desmarque a opção Port Forwarding List **Inherit (Herdar lista de encaminhamento de portas)**.



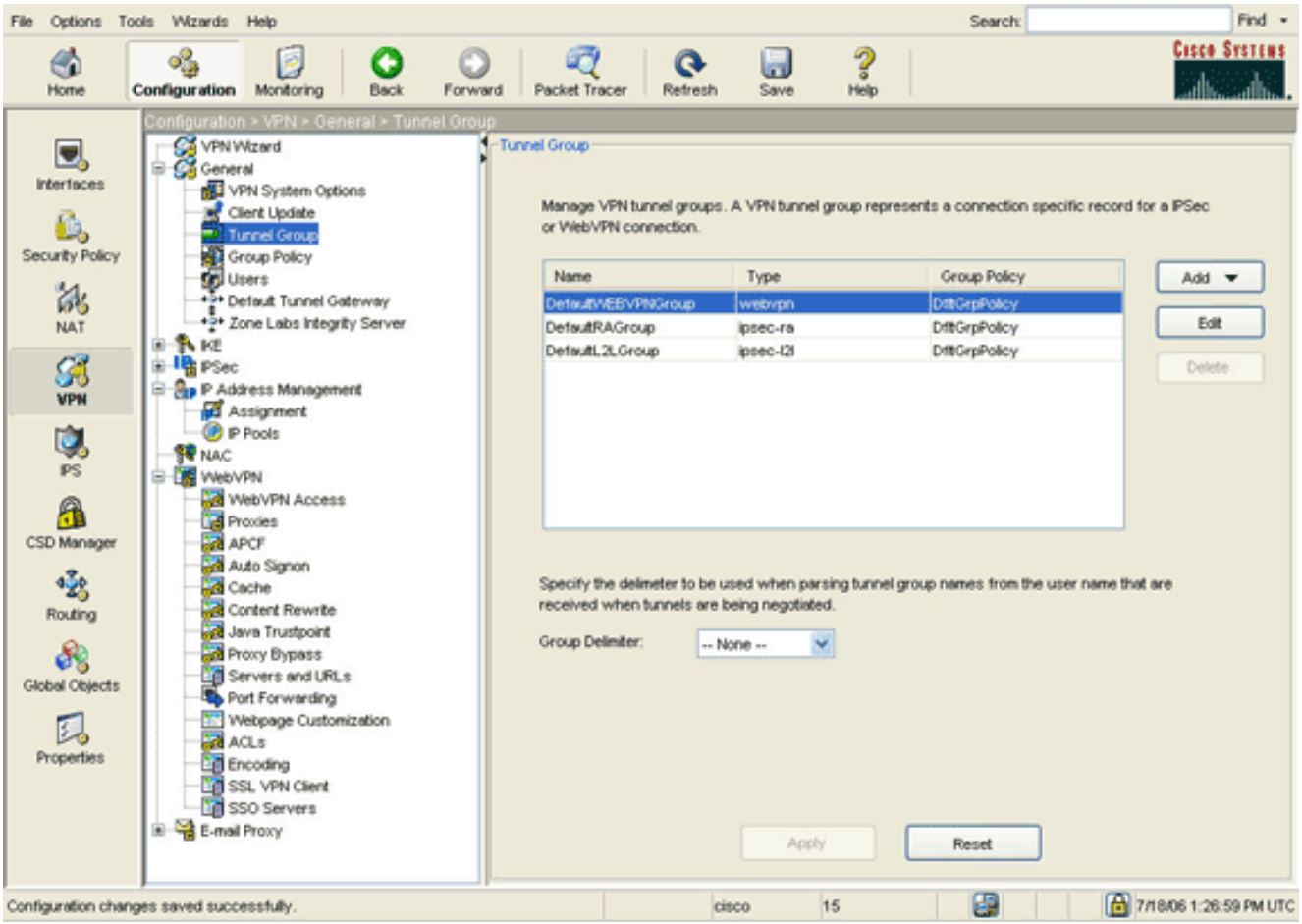
8. Clique na seta suspensa **Lista de encaminhamento de portas** e escolha a lista de encaminhamento de portas que você criou na Etapa 2.
9. Desmarque a caixa de seleção Nome do miniaplicativo **Herdar** e altere o nome no campo de texto.O cliente exibe o nome do miniaplicativo na conexão.
10. Clique em **OK** e em **Aplicar**.
11. Clique em **Save** e, em seguida, clique em **Yes para aceitar as alterações.**

Etapa 4. Crie um grupo de túnel e vincule-o à política de grupo

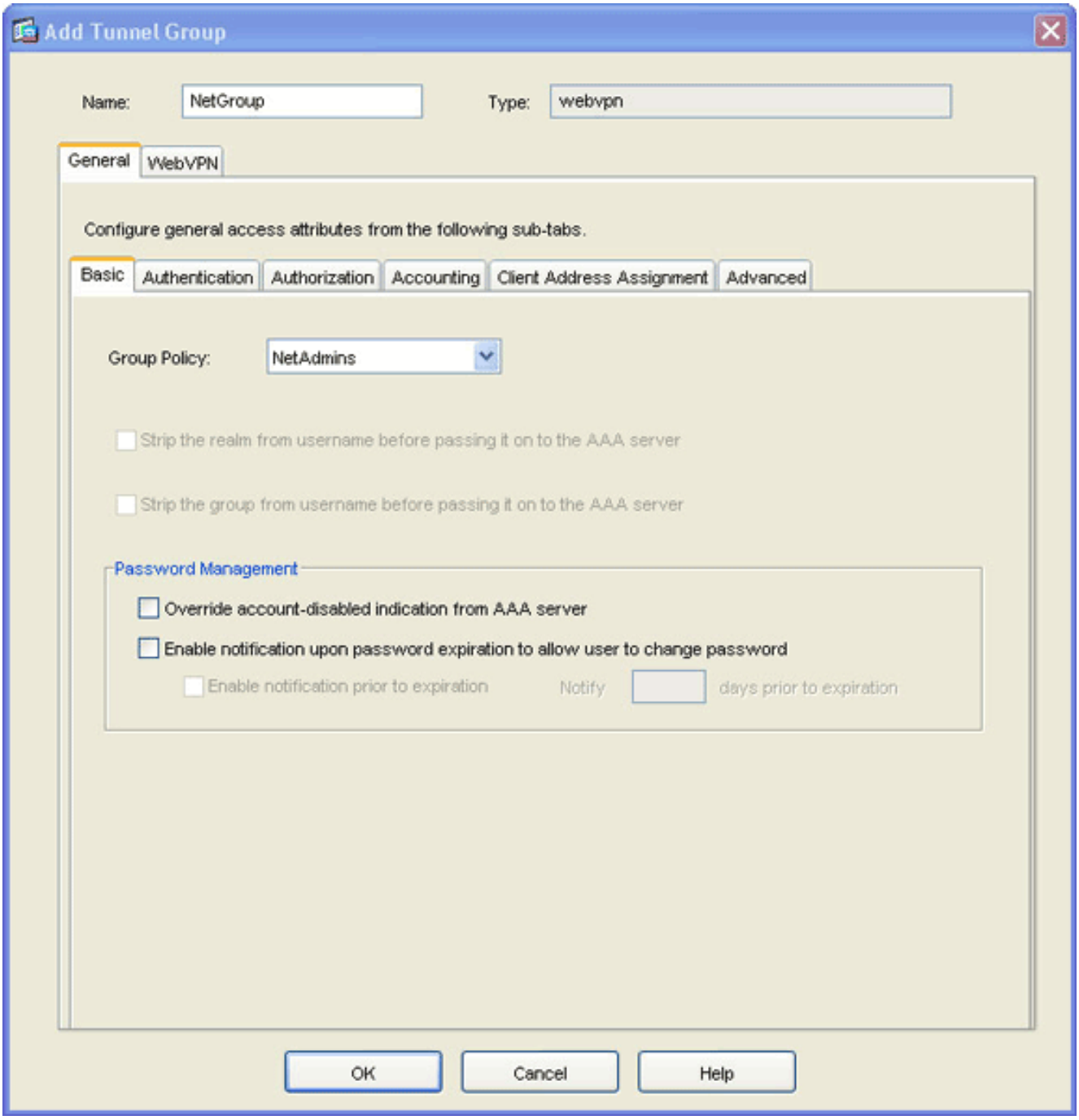
Você pode editar o grupo de túneis *DefaultWebVPNGroup* padrão ou criar um novo grupo de túneis.

Para criar um novo grupo de túneis, faça o seguinte:

1. Expanda **General** e escolha **Tunnel Group**.



2. Clique em **Add** e escolha **WebVPN Access**.A caixa de diálogo Add Tunnel Group (Adicionar grupo de túnel) é
exibida.

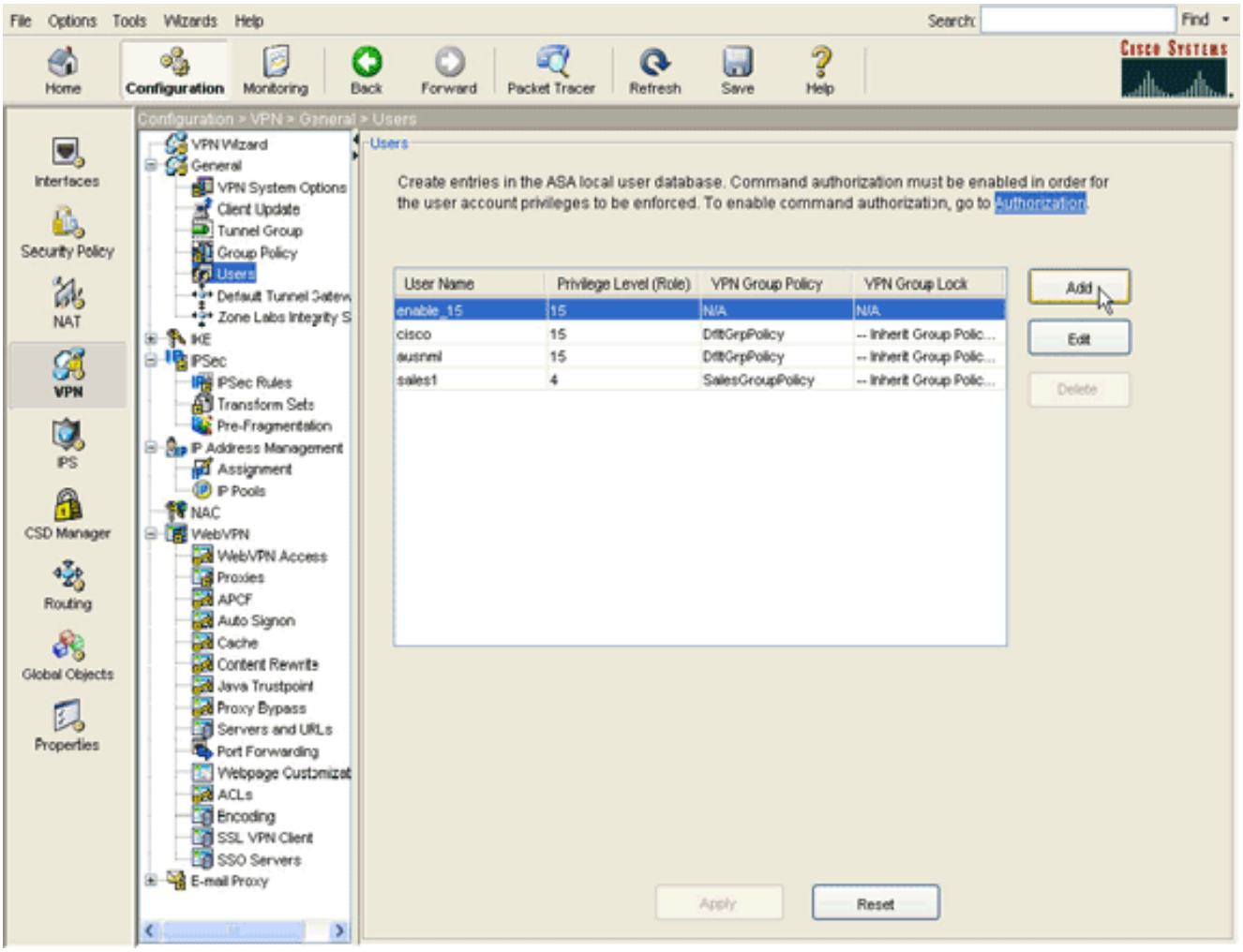


3. Digite um nome no campo Nome.
4. Clique na seta suspensa **Política de grupo** e escolha a política de grupo criada na Etapa 3.
5. Clique em **OK** e em **Aplicar**.
6. Clique em **Save** e, em seguida, clique em **Yes para aceitar as alterações.**O grupo de túneis, a política de grupo e as características de encaminhamento de portas agora estão vinculadas.

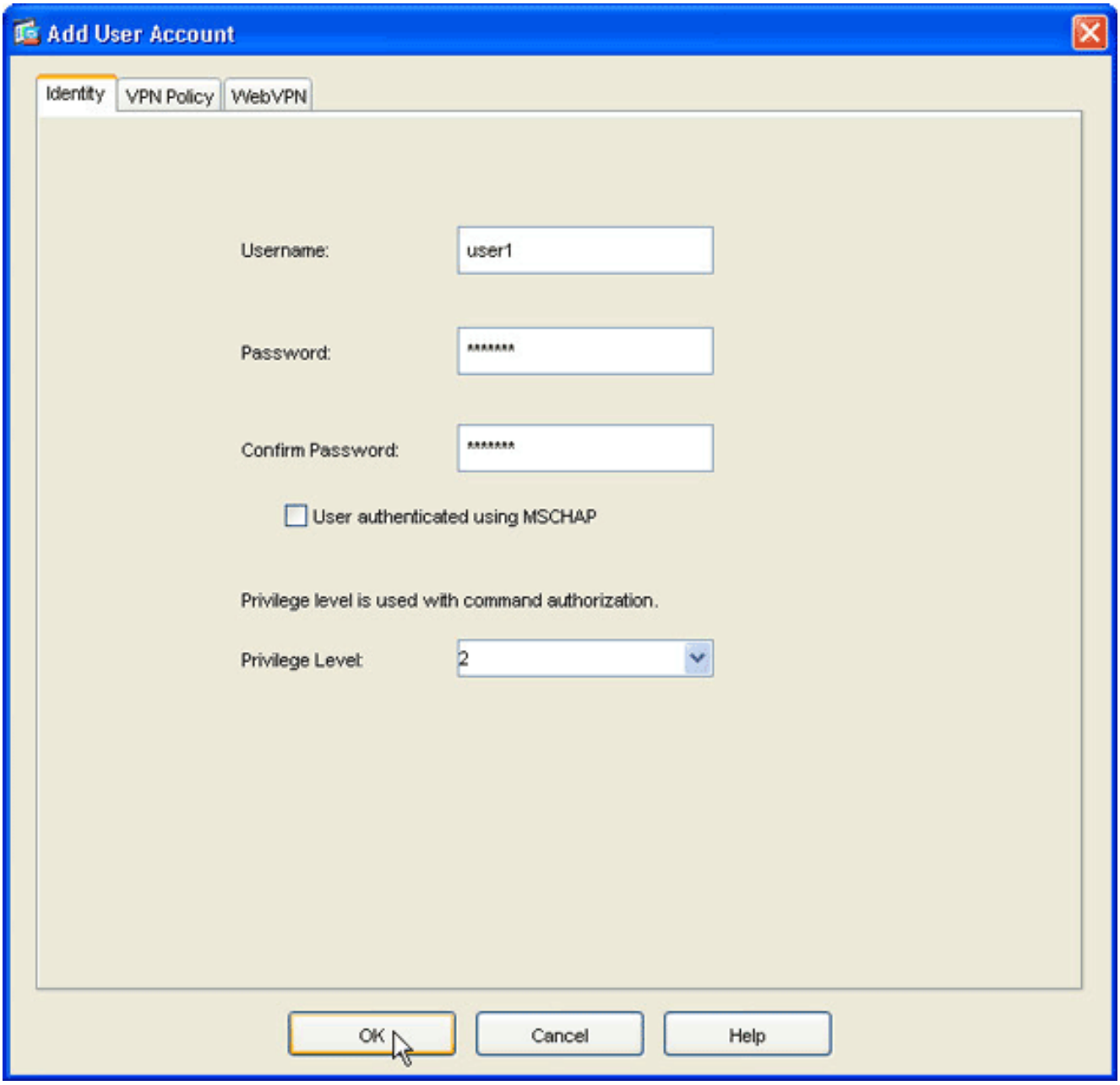
Etapa 5. Crie um usuário e adicione esse usuário à política de grupo

Para criar um usuário e adicioná-lo à política de grupo, faça o seguinte:

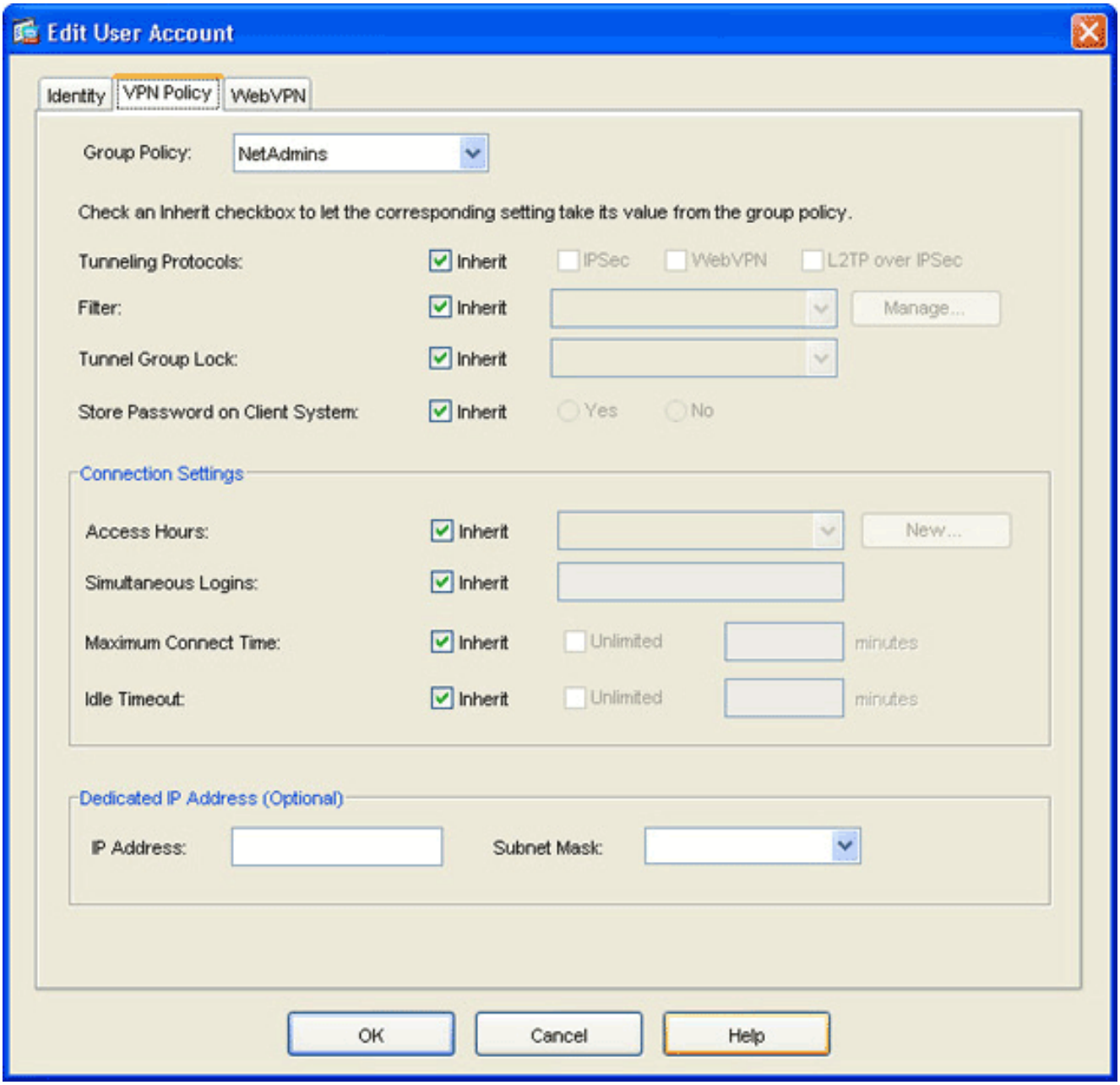
1. Expanda **General** e escolha **Users**.



2. Clique no botão Adicionar.A caixa de diálogo Adicionar conta de usuário é exibida.



3. Insira valores para o nome de usuário, senha e informações de privilégio e clique na guia **Política de VPN**.



4. Clique na seta suspensa **Política de grupo** e escolha a política de grupo criada na Etapa 3.Este usuário herda as características e políticas do WebVPN da política de grupo selecionada.
5. Clique em **OK** e em **Aplicar**.
6. Clique em **Salvar** e em **Sim** para aceitar as alterações.

Configuração de VPN SSL Thin-Client usando 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
```

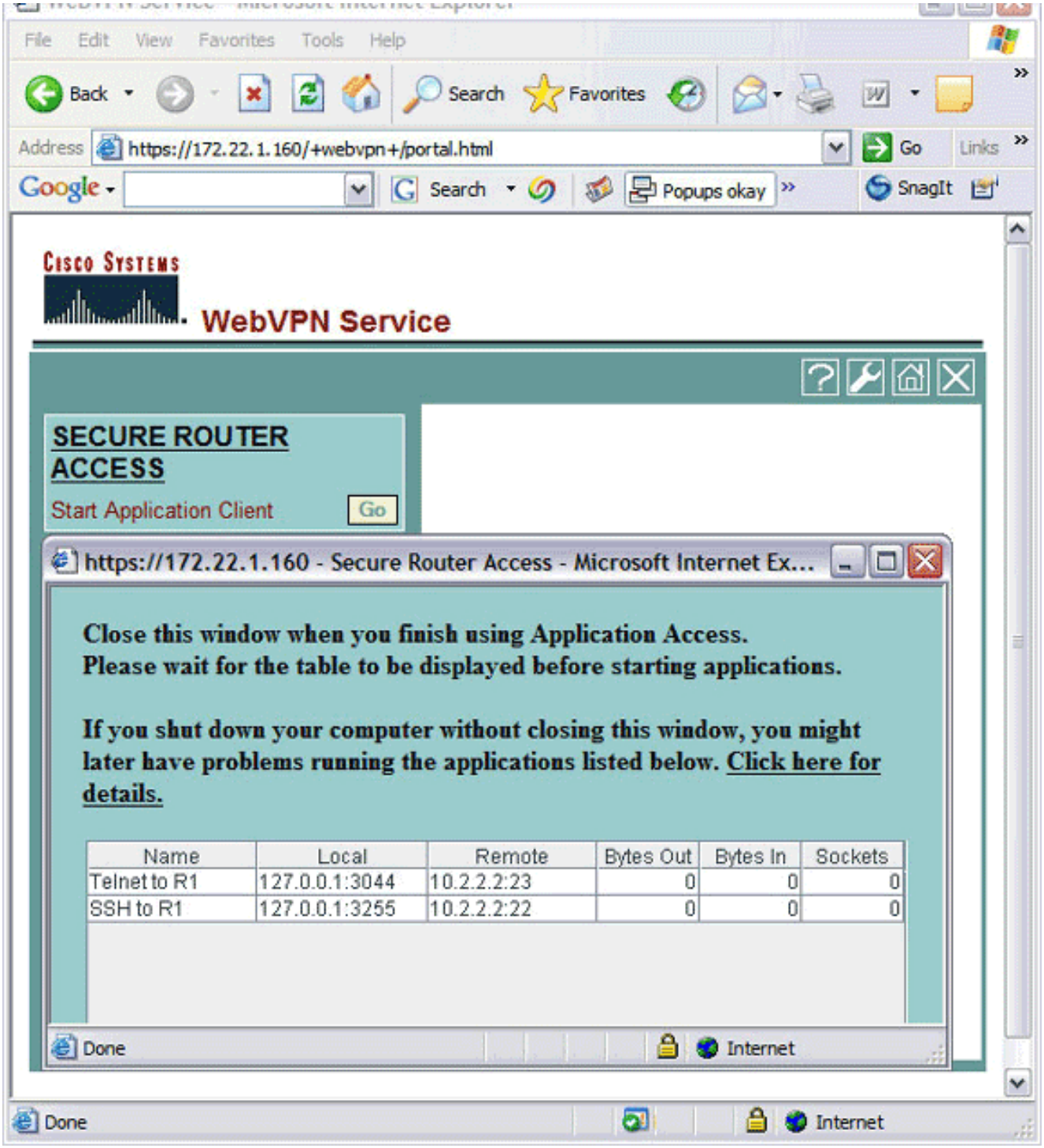
Verificar

Use esta seção para verificar se sua configuração funciona corretamente.

Procedimento

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

1. Em uma estação de trabalho cliente, digite **https:// *outside_ASA_IP Address*** ; onde *outside_ASA_IPAaddress* é a URL SSL do ASA.Quando o certificado digital for aceito e o usuário for autenticado, a página Web do WebVPN Service será exibida.

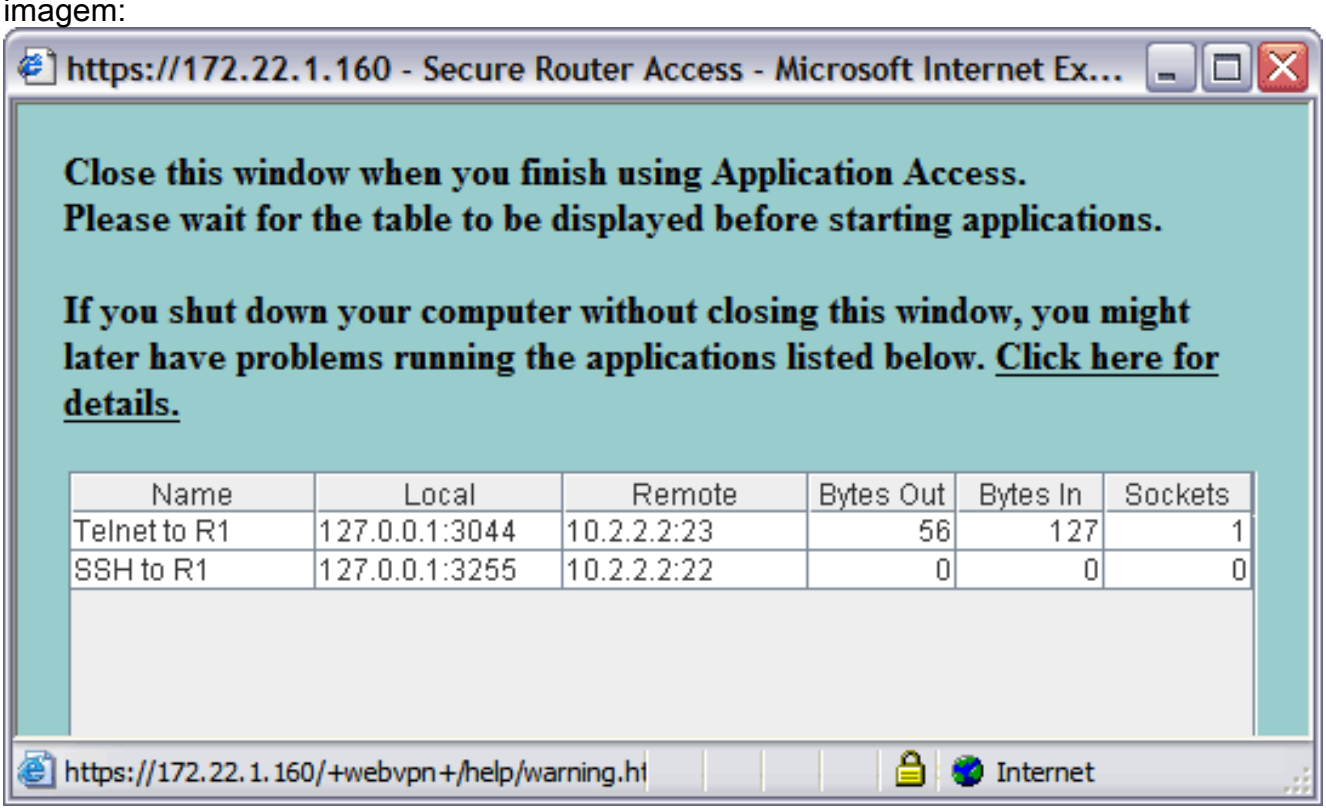


As informações de endereço e porta necessárias para acessar o aplicativo são exibidas na coluna local. As colunas Bytes Out e Bytes In não exibem nenhuma atividade porque o aplicativo não foi chamado no momento.

2. Use o prompt do DOS ou outro aplicativo Telnet para iniciar uma sessão Telnet.
3. No prompt de comando, digite **telnet 127.0.0.1 3044**.**Observação:** esse comando fornece um exemplo de como obter acesso à porta local exibida na imagem da página Web do WebVPN Service neste documento. *O comando não inclui dois-pontos (:).* Digite o comando conforme descrito neste documento.O ASA recebe o comando pela sessão segura e, como armazena um mapa das informações, o ASA sabe imediatamente para abrir a sessão Telnet segura para o dispositivo
mapeado.

Quando você digitar seu nome de usuário e senha, o acesso ao dispositivo estará concluído.

4. Para verificar o acesso ao dispositivo, verifique as colunas Bytes Out e Bytes In como mostrado nesta
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.

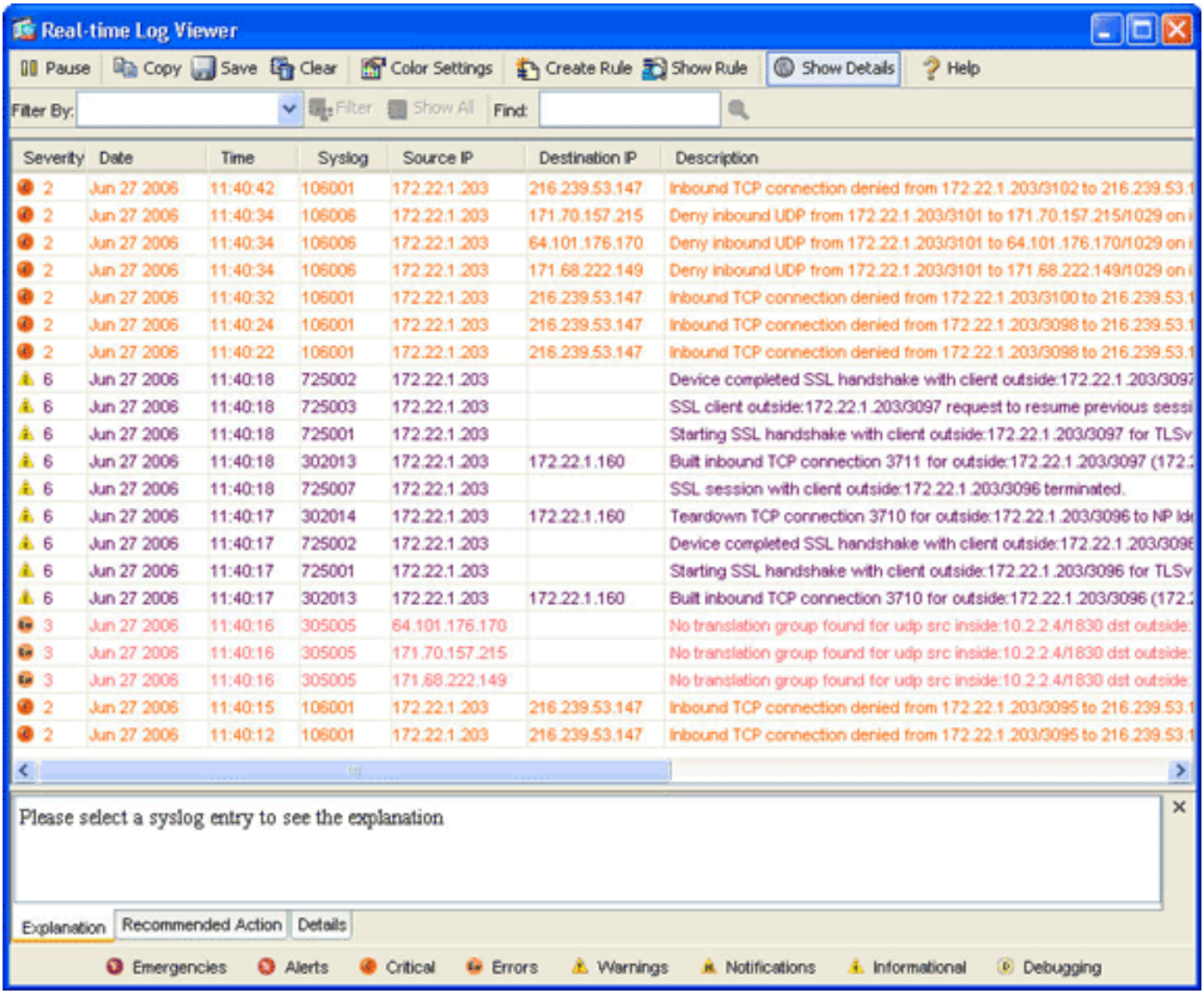
Observação: a Output Interpreter Tool (somente clientes registrados) (OIT) suporta determinados comandos **show**. Use a OIT para exibir uma análise da saída do comando show.

Troubleshoot

Use esta seção para resolver problemas de configuração.

O processo de handshake SSL está concluído?

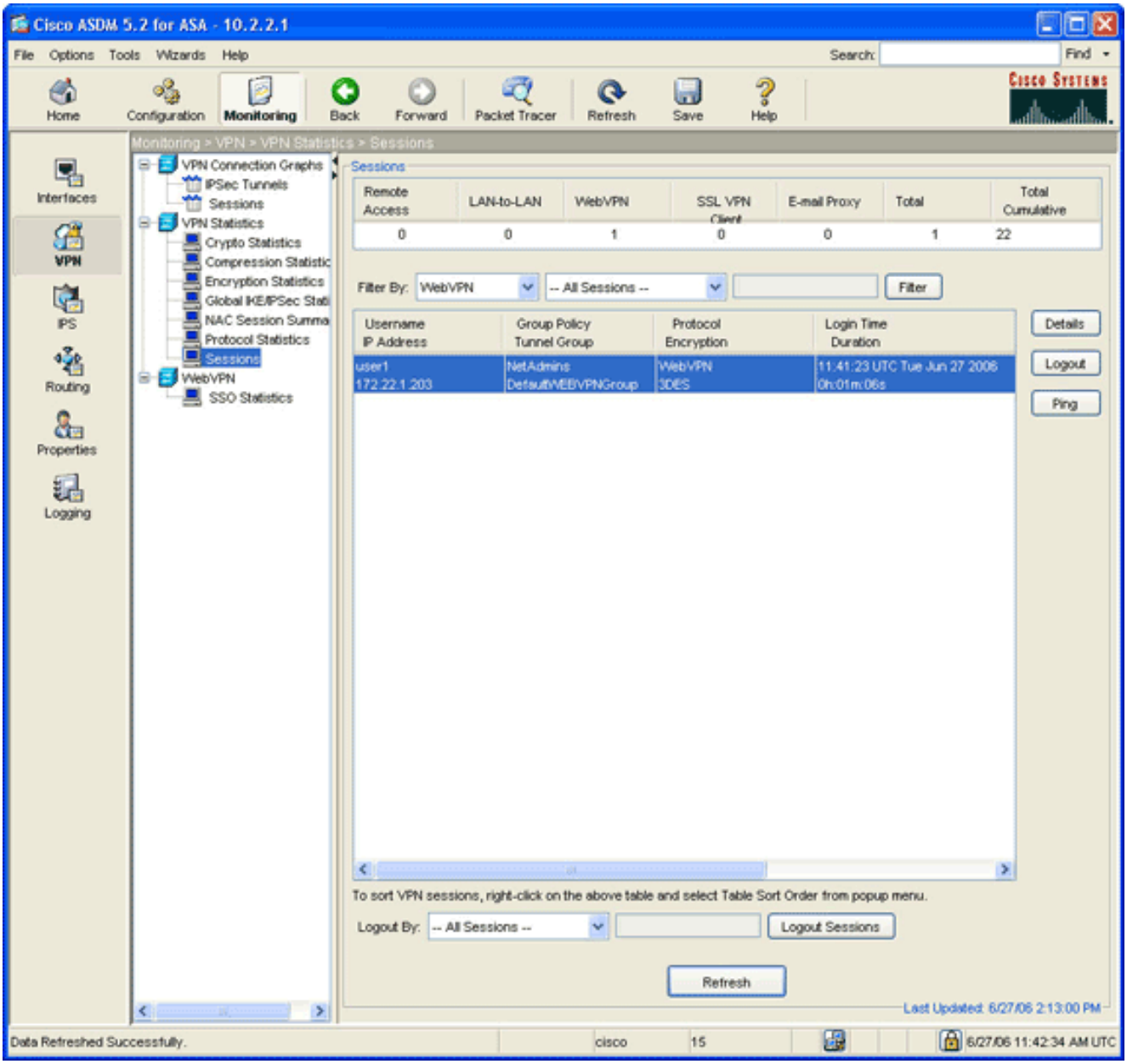
Depois de se conectar ao ASA, verifique se o registro em tempo real mostra a conclusão do handshake SSL.



O Thin Client da VPN SSL está funcionando?

Para verificar se o Thin-Client de VPN SSL está funcionando, faça o seguinte:

1. Clique em **Monitoring** e, em seguida, clique em **VPN**.
2. Expanda **VPN Statistics** e clique em **Sessions**.Sua sessão SSL VPN Thin-Client deve aparecer na lista de sessões. Certifique-se de filtrar por WebVPN conforme mostrado nesta imagem:



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.

Informações Relacionadas

- Exemplo de configuração de VPN SSL sem cliente (WebVPN) no ASA
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- ASA com WebVPN e logon único usando o exemplo de configuração de ASDM e NTLMv1
- Suporte Técnico e Documentação - Cisco Systems