Ejemplo de Configuración de Thin-Client SSL VPN (WebVPN) en ASA con ASDM

Contenido

Introducción

La tecnología Thin-Client SSL VPN permite el acceso seguro a algunas aplicaciones que tengan puertos estáticos, como Telnet(23), SSH(22), POP3(110), IMAP4(143) y SMTP(25). Puede utilizar Thin-Client SSL VPN como una aplicación basada en el usuario, una aplicación basada en política, o ambas. Es decir, puede configurar el acceso según cada usuario o puede crear directivas de grupo en las cuales agrega uno o más usuarios.

- **Clientless SSL VPN (WebVPN)**: proporciona un cliente remoto que requiere un navegador web con SSL para acceder a servidores web HTTP o HTTPS en una red de área local (LAN) corporativa. Además, SSL VPN sin cliente proporciona acceso para la exploración de archivos de Windows a través del protocolo Common Internet File System (CIFS). Outlook Web Access (OWA) es un ejemplo de acceso HTTP.Consulte Ejemplo de Configuración de VPN SSL sin Cliente (WebVPN) en ASA para obtener más información sobre la VPN SSL sin

Cliente.

- **Thin-Client SSL VPN (Port Forwarding)**: proporciona un cliente remoto que descarga un pequeño applet basado en Java y permite el acceso seguro para aplicaciones de protocolo de control de transmisión (TCP) que utilizan números de puerto estáticos. El protocolo de oficina de correos (POP3), el protocolo simple de transferencia de correo (SMTP), el protocolo de acceso a mensajes de Internet (IMAP), el shell seguro (ssh) y Telnet son ejemplos de acceso seguro. Debido a que los archivos del equipo local cambian, los usuarios deben tener privilegios administrativos locales para utilizar este método. Este método de VPN SSL no funciona con aplicaciones que utilizan asignaciones de puertos dinámicos, como algunas aplicaciones de protocolo de transferencia de archivos (FTP).**Nota:** No se admite el protocolo de datagramas de usuario (UDP).
- **SSL VPN Client (Modo de túnel)**: descarga un cliente pequeño a la estación de trabajo remota y permite un acceso seguro completo a los recursos en una red corporativa interna. Puede descargar de forma permanente el SSL VPN Client (SVC) en una estación de trabajo remota o puede quitar el cliente una vez que se haya cerrado la sesión segura.Consulte Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM para obtener más información sobre SSL VPN Client.

Este documento muestra una configuración simple para Thin-Client SSL VPN en Adaptive Security Appliance (ASA). La configuración permite que un usuario telnet de forma segura a un router ubicado en el interior del ASA. La configuración de este documento es compatible con ASA versión 7.x y posteriores.

Prerequisites

Requirements

Antes de intentar esta configuración, asegúrese de cumplir con estos requisitos para las estaciones cliente remotas:

- Navegador web con SSL habilitado
- SUN Java JRE versión 1.4 o posterior
- Cookies activadas
- Bloqueadores emergentes deshabilitados
- Privilegios administrativos locales (no obligatorios pero muy recomendados)

Nota: La última versión de SUN Java JRE está disponible como descarga gratuita desde el sitio web de Java .

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Adaptive Security Appliance serie 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Nota:** Consulte Permiso de Acceso HTTPS para ASDM para permitir que el ASA sea configurado por el ASDM.
- Software Cisco Adaptive Security Appliance versión 7.2(1)
- Cliente remoto de Microsoft Windows XP Professional (SP 2)

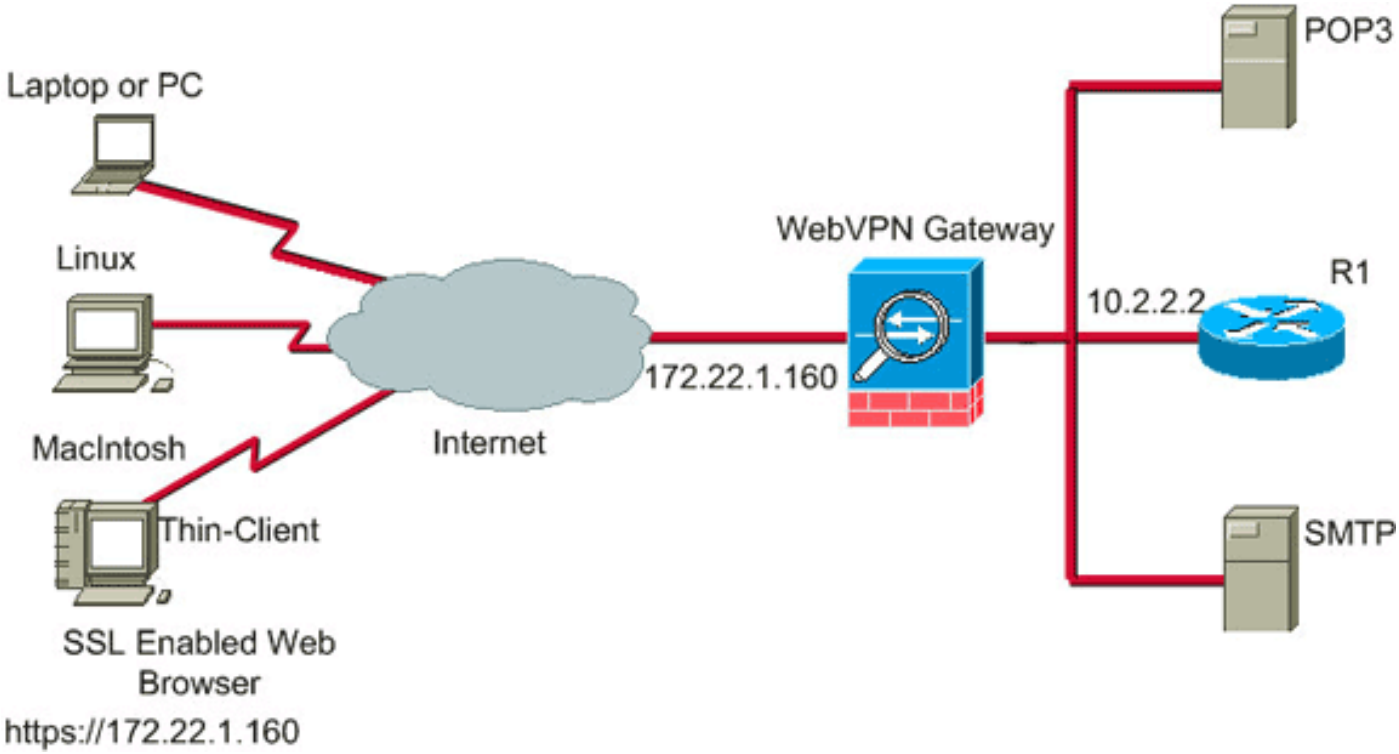
La información en este documento se desarrolló en un entorno de laboratorio. Todos los

dispositivos utilizados en este documento se restablecieron a su configuración predeterminada. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando. Todas las direcciones IP utilizadas en esta configuración se seleccionaron de las direcciones RFC 1918 en un entorno de laboratorio; estas direcciones IP no se pueden enrutar en Internet y se utilizan únicamente con fines de prueba.

Diagrama de la red

Este documento utiliza la configuración de red descrita en esta sección.

Cuando un cliente remoto inicia una sesión con el ASA, el cliente descarga un pequeño applet Java en la estación de trabajo. Se presenta al cliente una lista de recursos preconfigurados.



Convenciones

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

Antecedentes

Para iniciar una sesión, el cliente remoto abre un navegador SSL a la interfaz exterior del ASA. Después de establecer la sesión, el usuario puede utilizar los parámetros configurados en el ASA para invocar cualquier Telnet o acceso a la aplicación. El ASA proxies la conexión segura y permite al usuario acceder al dispositivo.

Nota: Las listas de acceso entrantes no son necesarias para estas conexiones porque el ASA ya es consciente de lo que constituye una sesión legal.

Configuración de Thin-Client SSL VPN con ASDM

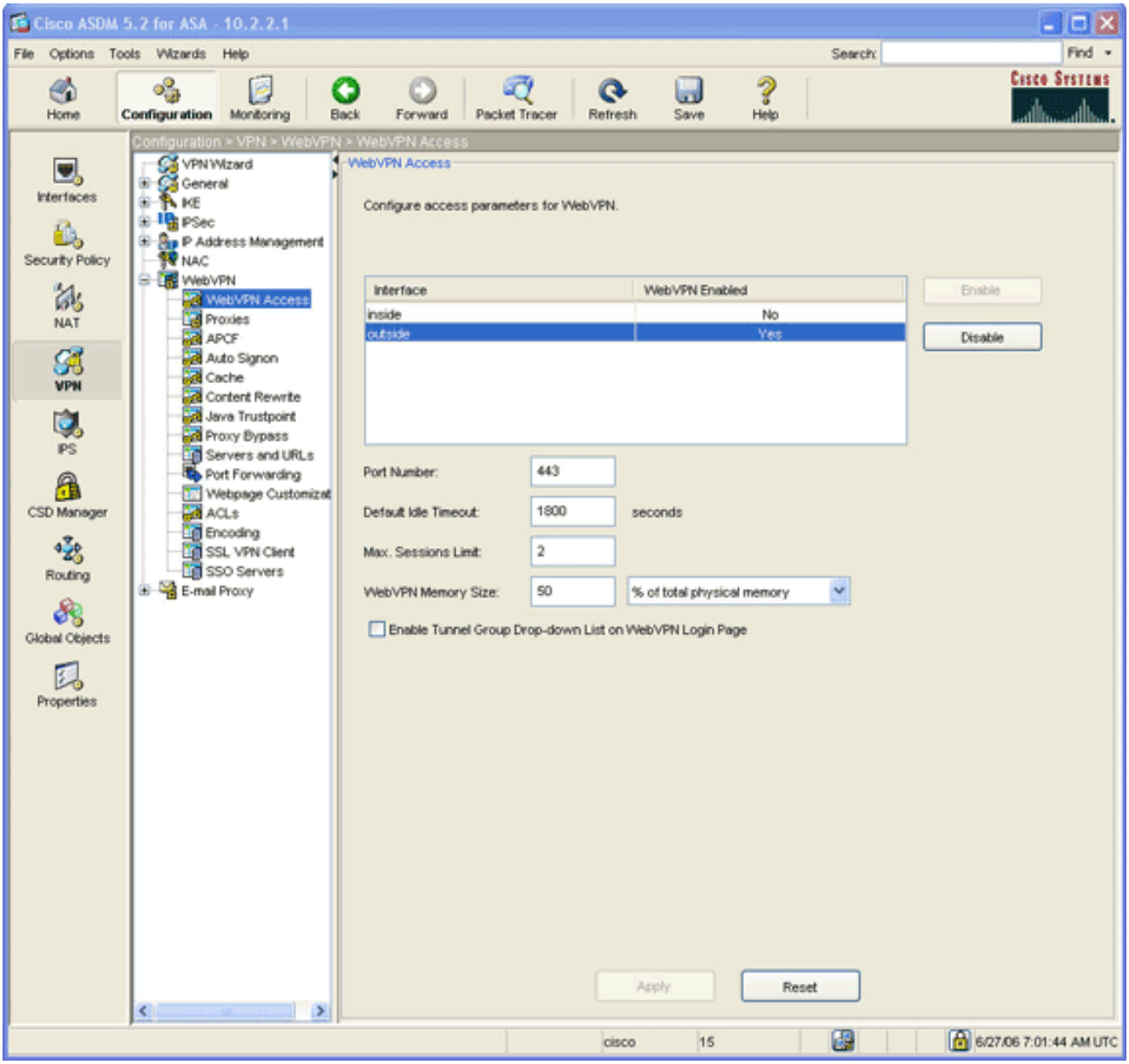
Para configurar Thin-Client SSL VPN en el ASA, complete estos pasos:

1. Habilitar WebVPN en ASA
2. Configurar las características de reenvío de puertos
3. Cree una política de grupo y enlaza esta a la lista de reenvío de puertos (creada en el paso 2)
4. Crear un grupo de túnel y enlazarlo a la política de grupo (creada en el paso 3)
5. Crear un usuario y agregar ese usuario a la directiva de grupo (creada en el paso 3)

Paso 1. Habilitar WebVPN en ASA

Para habilitar el WebVPN en el ASA, complete estos pasos:

1. Dentro de la aplicación ASDM, haga clic en **Configuration** y luego haga clic en **VPN**.
2. Expanda **WebVPN** y elija **Acceso WebVPN**.

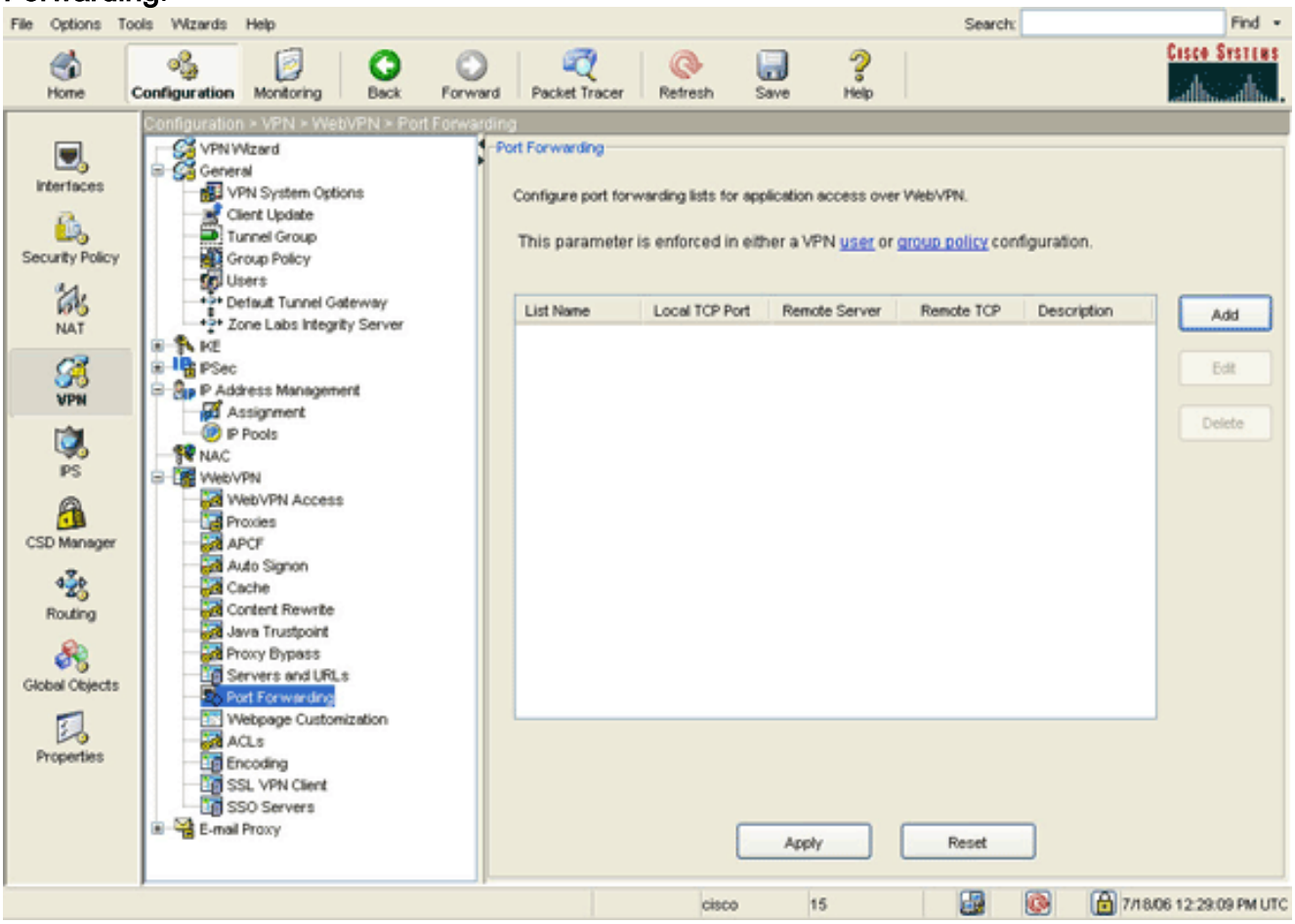


3. Resalte la interfaz y haga clic en **Enable**.
4. Haga clic en **Aplicar**, haga clic en **Guardar** y, a continuación, haga clic en **Sí** para aceptar los cambios.

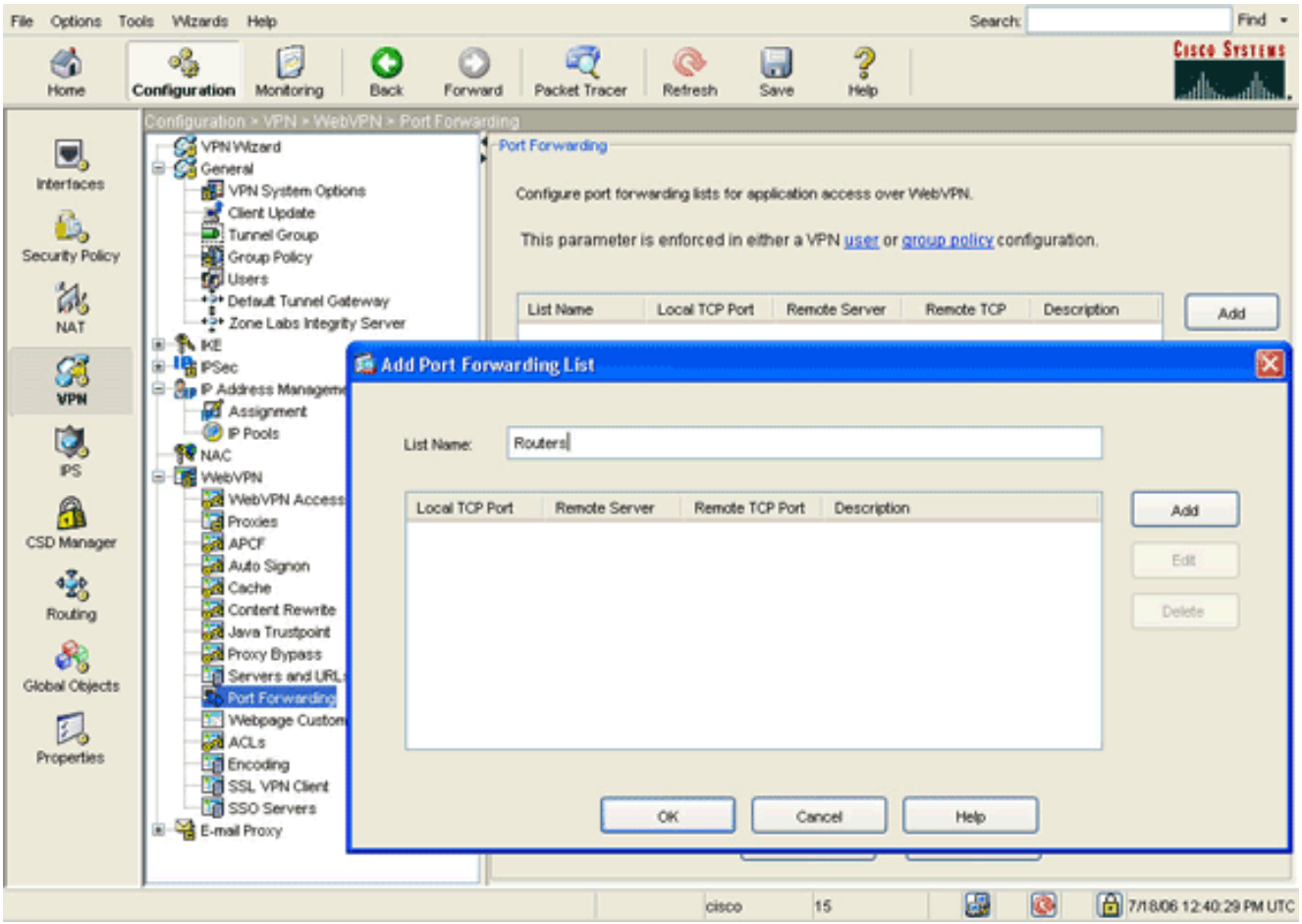
Paso 2. Configurar las características de reenvío de puertos

Para configurar las características de reenvío de puertos, complete estos pasos:

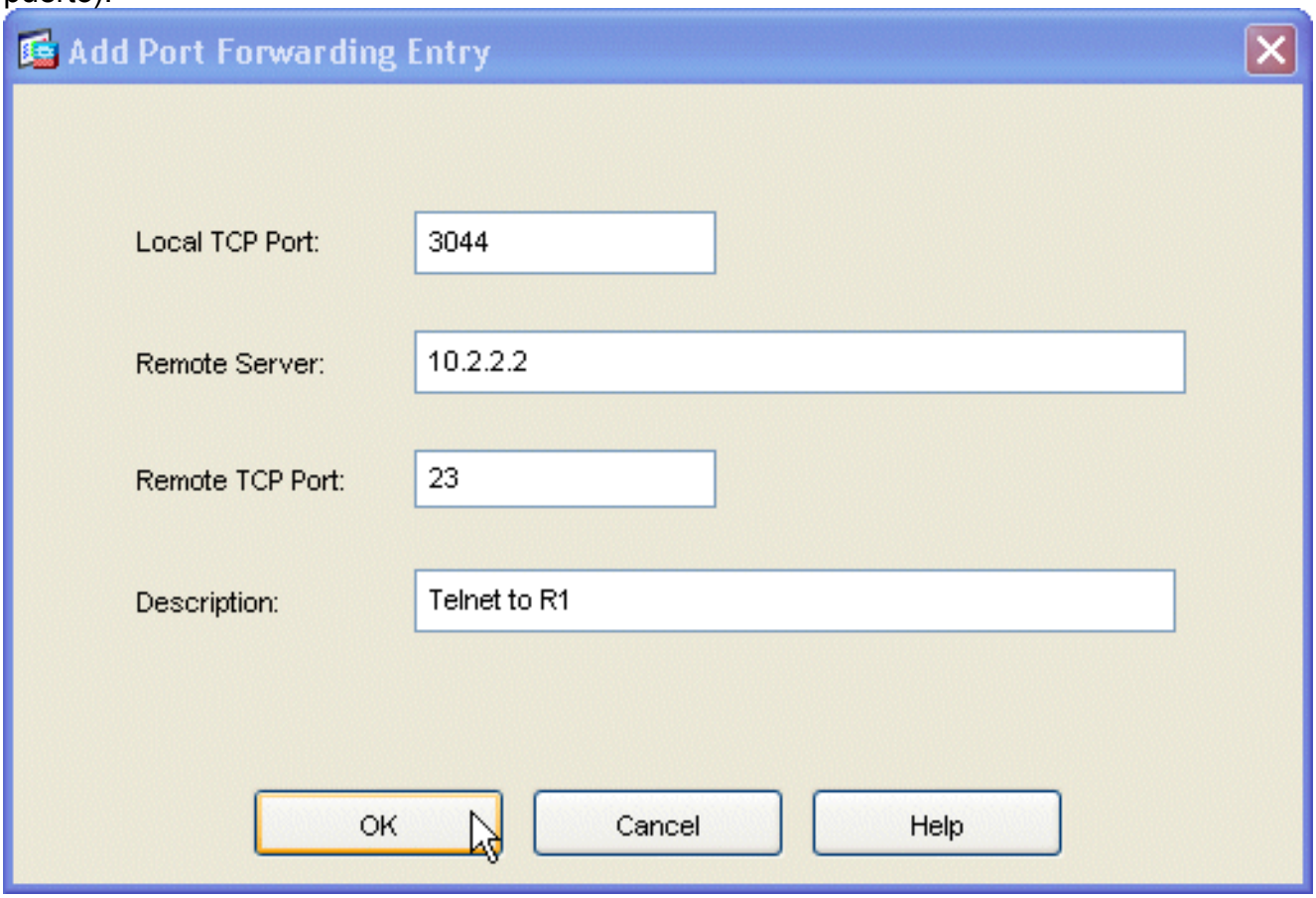
1. Expanda **WebVPN** y elija **Port Forwarding**.



2. 'Haga clic en el botón Add (Agregar).'



3. En el cuadro de diálogo Add Port Forwarding List (Agregar lista de reenvío de puertos), introduzca un nombre de lista y haga clic en **Add** (Agregar).Aparece el cuadro de diálogo Add Port Forwarding Entry (Agregar entrada de reenvío de puerto).



4. En el cuadro de diálogo Add Port Forwarding Entry (Agregar entrada de reenvío de puerto),

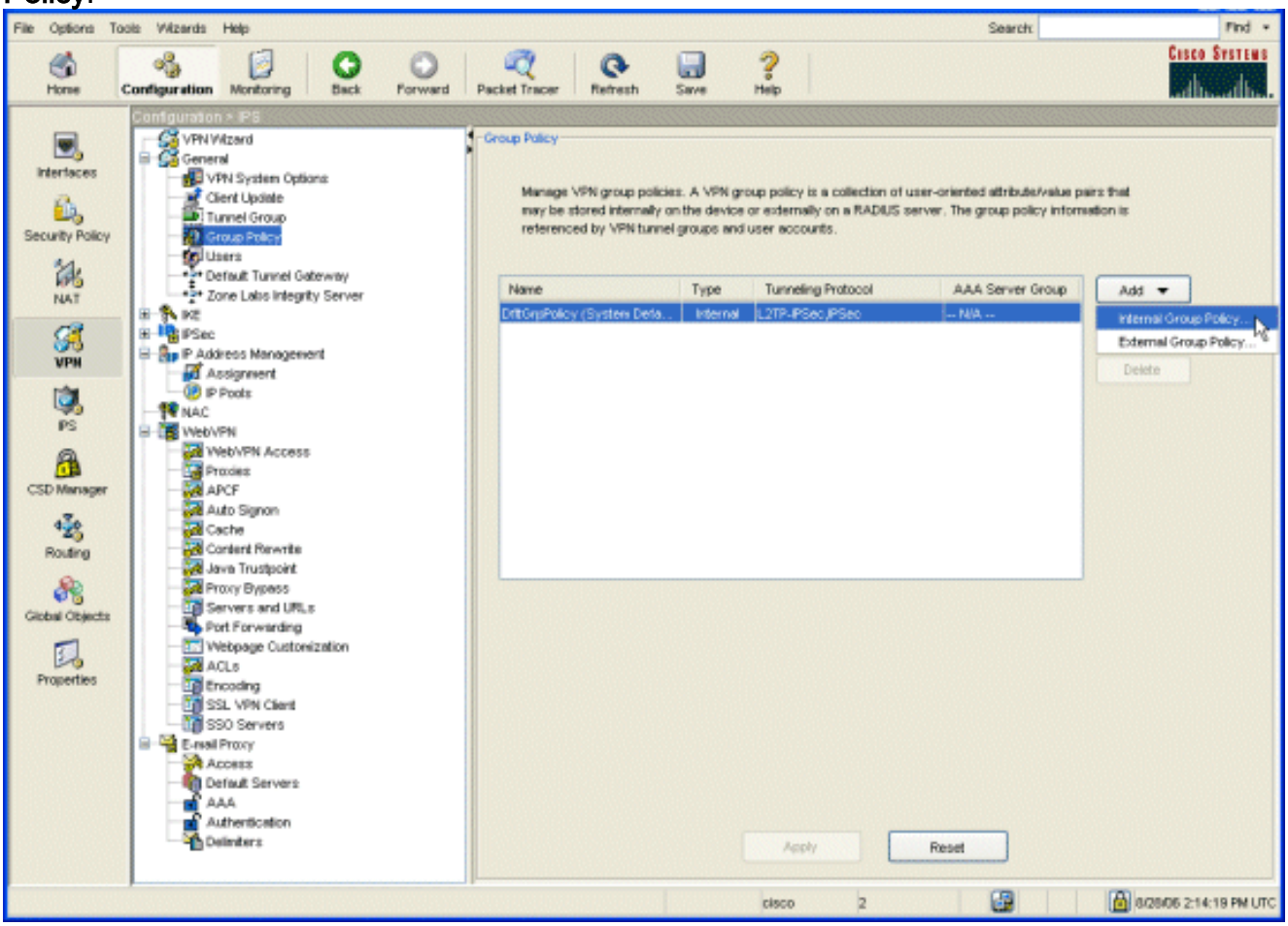
introduzca las siguientes opciones:En el campo Local TCP Port (Puerto TCP local), introduzca un número de puerto o acepte el valor predeterminado.El valor que introduzca puede ser cualquier número entre 1024 y 65535.En el campo Servidor remoto, introduzca una dirección IP.Este ejemplo utiliza la dirección del router.En el campo Puerto TCP remoto, introduzca un número de puerto.Este ejemplo utiliza el puerto 23.En el campo Descripción, introduzca una descripción y haga clic en **Aceptar**.

5. Haga clic en **Aceptar** y luego en **Aplicar**.
6. Haga clic en **Guardar** y, a continuación, haga clic en **Sí** para aceptar los cambios.

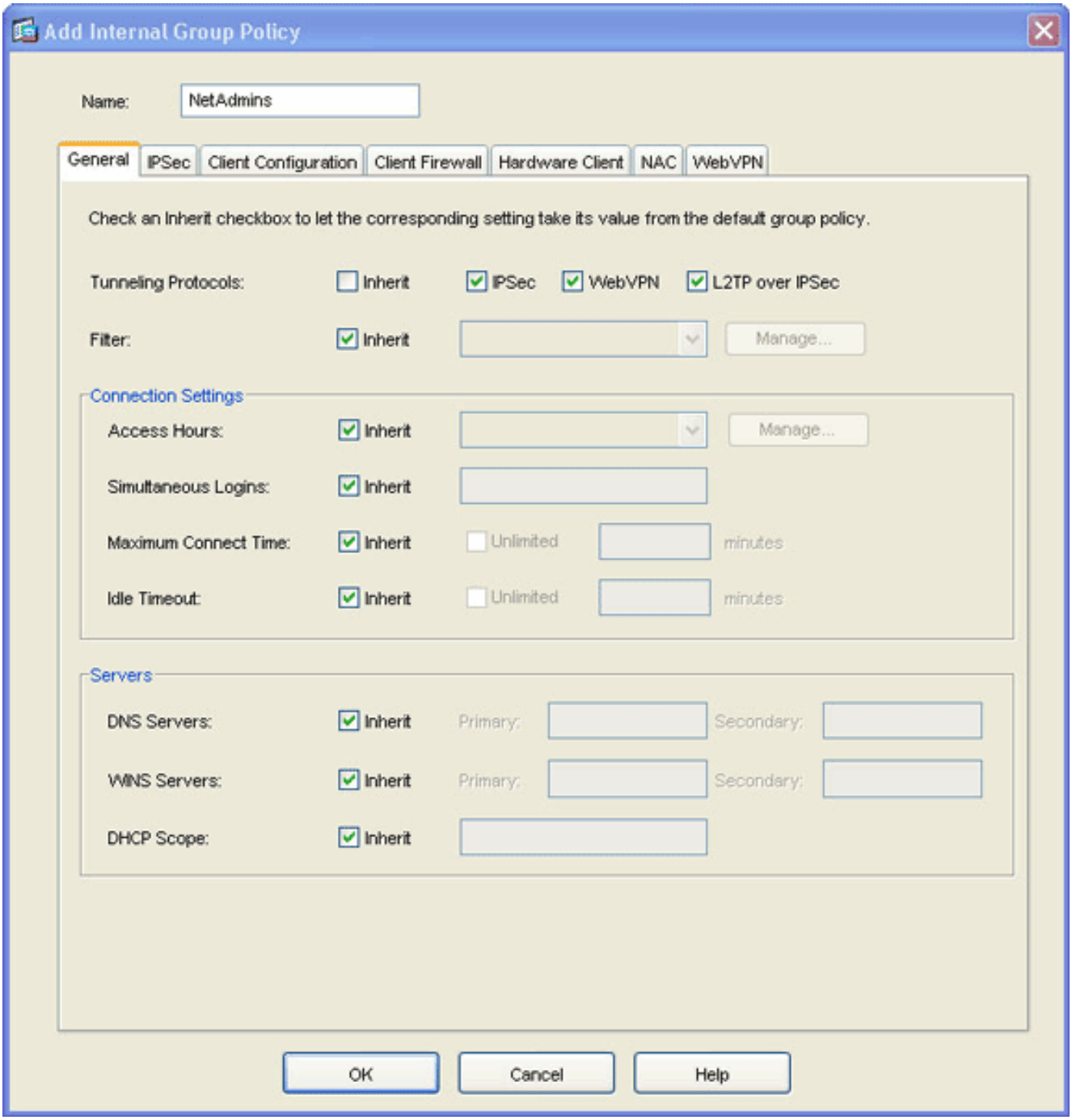
Paso 3. Crear una política de grupo y enlazarla a la lista de reenvío de puertos

Para crear una política de grupo y vincularla a la lista de reenvío de puertos, complete estos pasos:

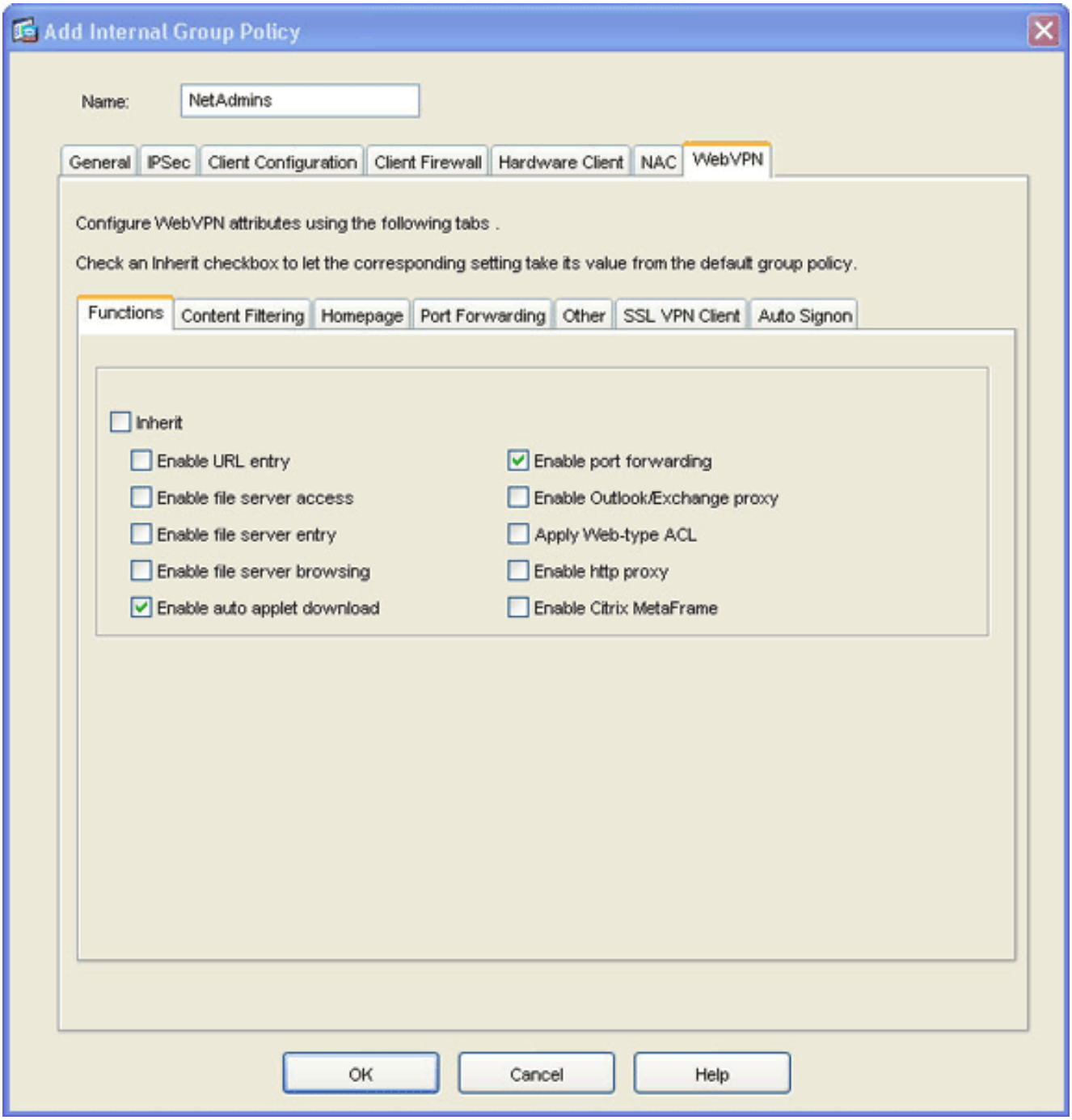
1. Expanda **General** y elija **Group Policy**.



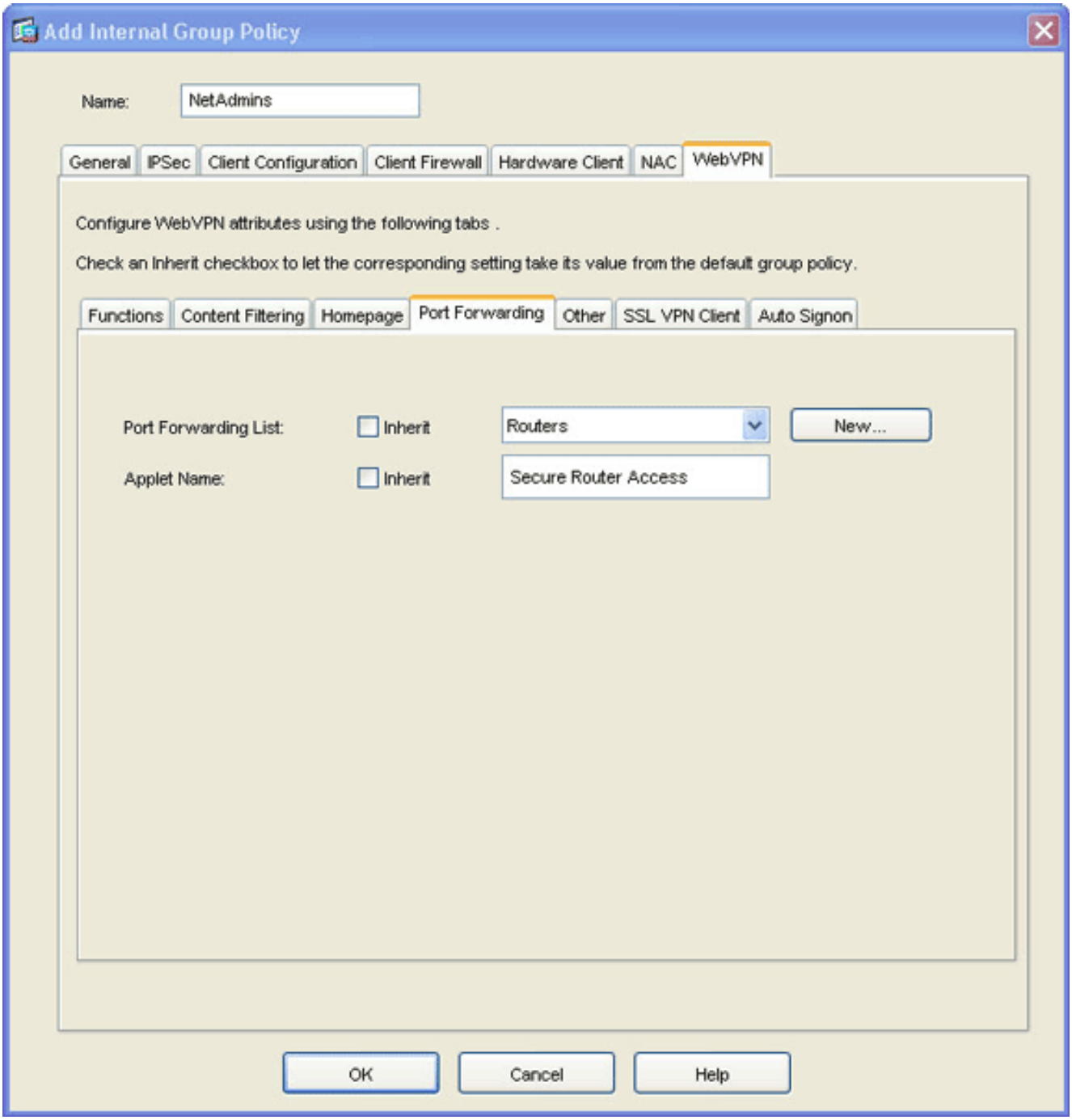
2. Haga clic en **Agregar** y elija **Directiva de grupo interna**.Aparecerá el cuadro de diálogo Agregar directiva de grupo interna.



3. Introduzca un nombre o acepte el nombre predeterminado de la política de grupo.
4. Desmarque la casilla de verificación Tunneling Protocols **Inherit** y marque la **WebVPN**.
5. Haga clic en la ficha **WebVPN** situada en la parte superior del cuadro de diálogo y, a continuación, haga clic en la ficha **Funciones**.
6. Desactive la casilla de verificación **Heredar** y active las casillas de verificación **Habilitar descarga automática de applet** y **Habilitar reenvío de puerto**, como se muestra en esta imagen:



7. También dentro de la ficha WebVPN, haga clic en la ficha **Port Forwarding** y desmarque la **casilla de verificación Inherit** de la **Lista de** Reenvío de Puertos.



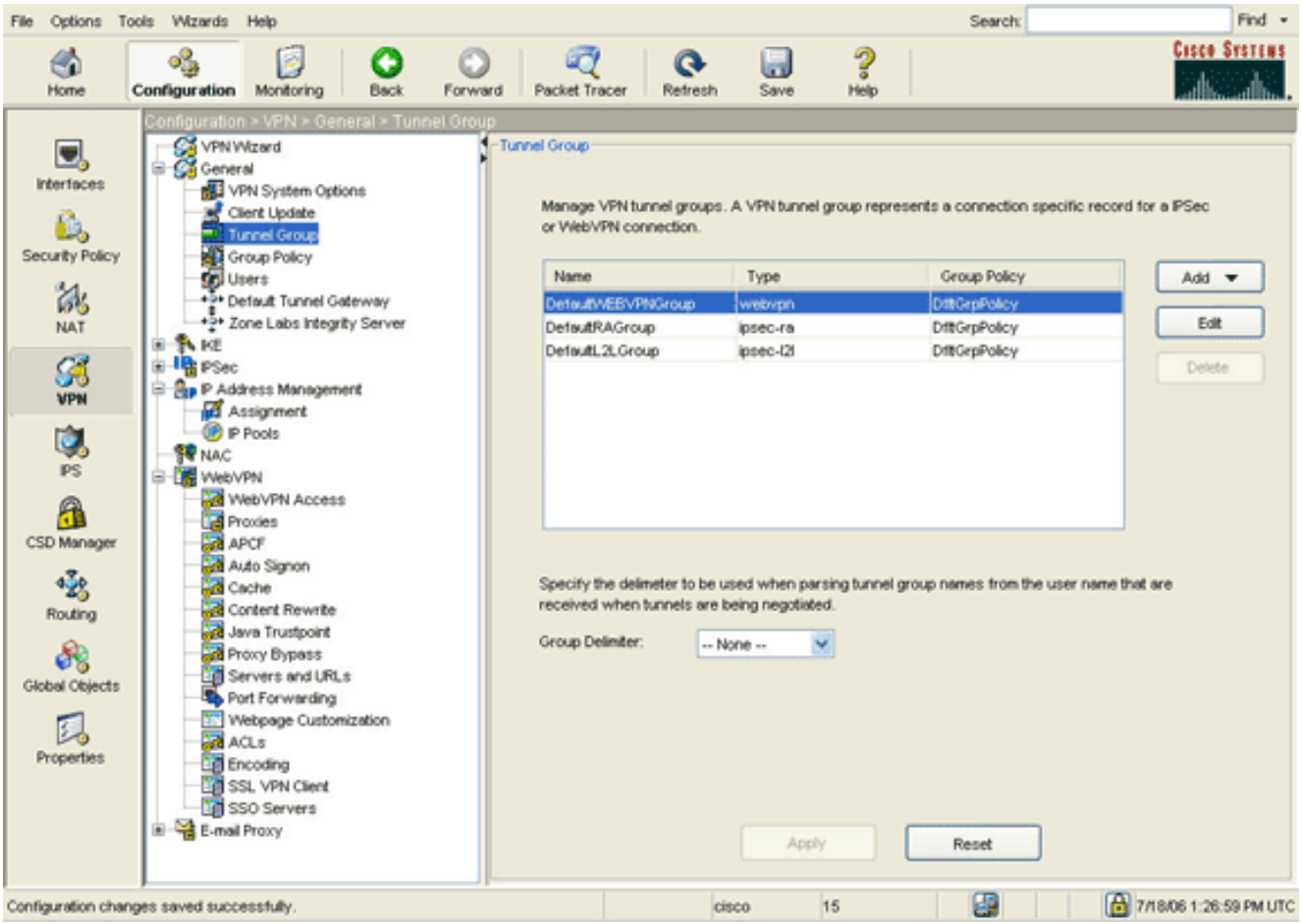
8. Haga clic en la flecha desplegable **Lista de reenvío de puertos** y elija la lista de reenvío de puertos que creó en el Paso 2.
9. Desmarque la casilla de verificación Heredar nombre de miniaplicación y cambie el nombre en el campo de texto.El cliente muestra el Applet Name en la conexión.
10. Haga clic en **Aceptar** y luego en **Aplicar**.
11. Haga clic en **Guardar** y, a continuación, haga clic en **Sí** para aceptar los cambios.

Paso 4. Crear un grupo de túnel y enlazarlo a la política de grupo

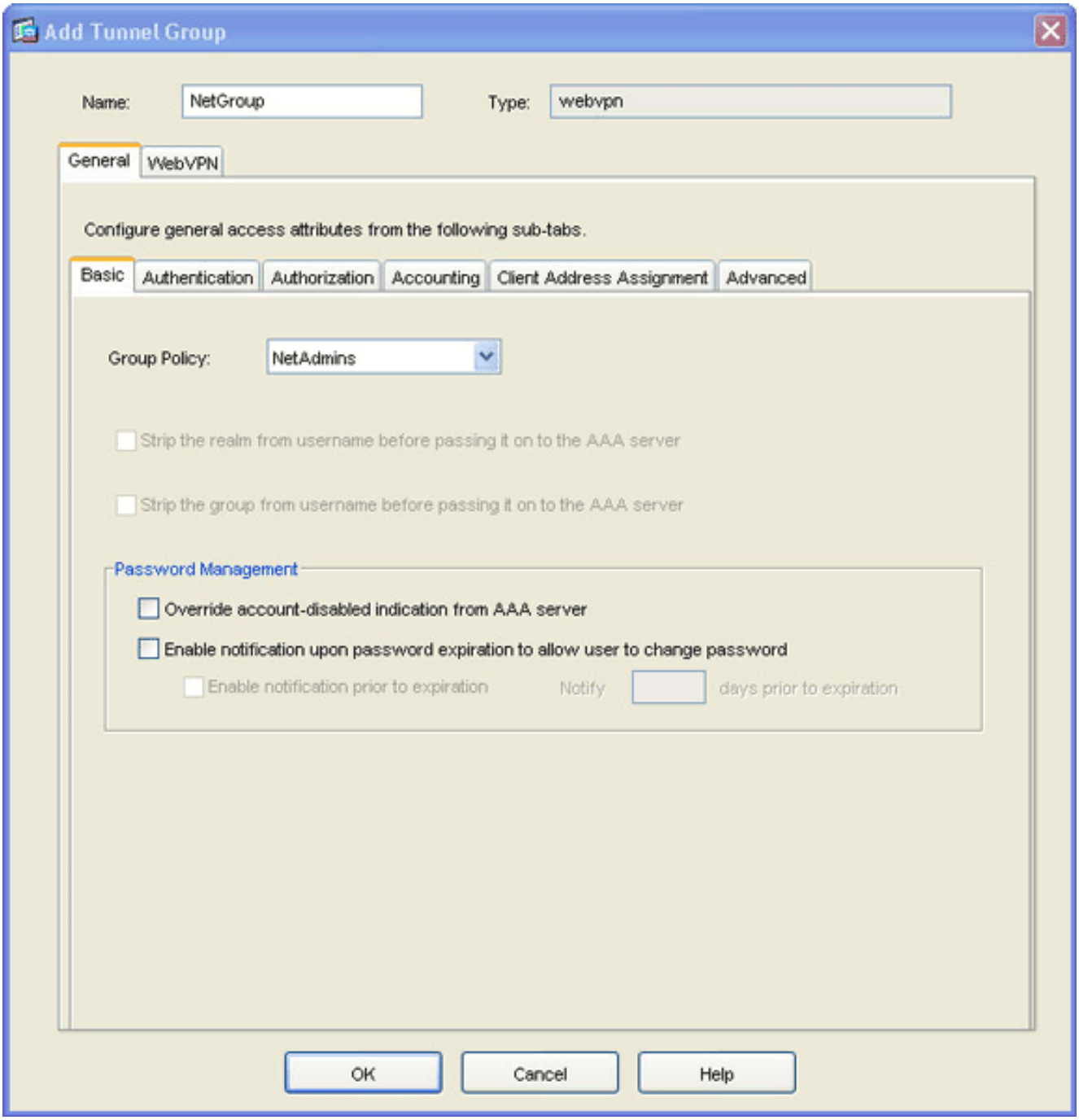
Puede editar el grupo de túnel *DefaultWebVPNGroup* predeterminado o crear un nuevo grupo de túnel.

Para crear un nuevo grupo de túnel, complete estos pasos:

1. Expanda **General** y elija **Grupo de Túnel**.



2. Haga clic en **Add**, y elija **WebVPN Access**.Aparecerá el cuadro de diálogo Agregar grupo de túnel.

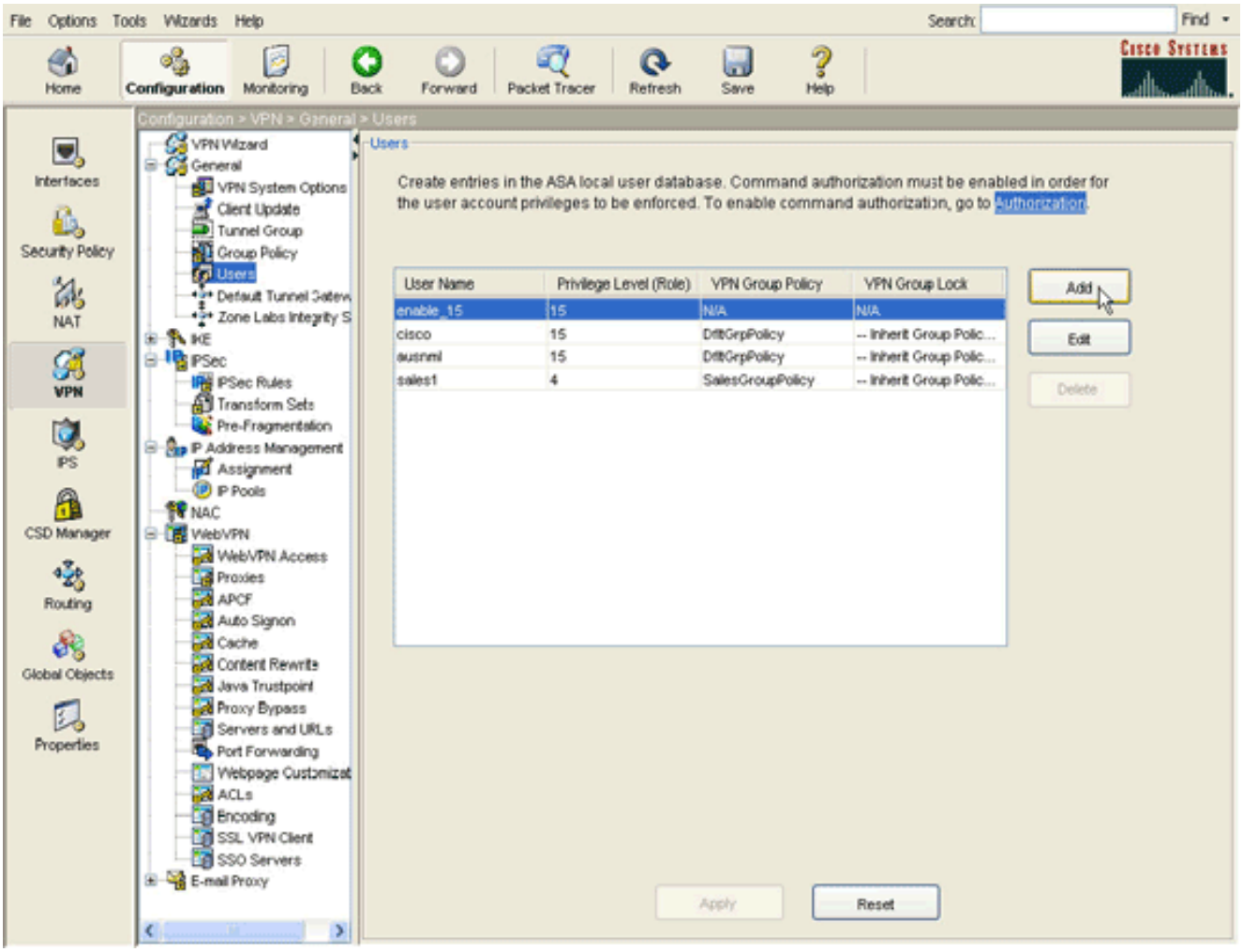


3. Introduzca un nombre en el campo Nombre.
4. Haga clic en la flecha desplegable **Política de grupo** y elija la política de grupo que creó en el Paso 3.
5. Haga clic en **Aceptar** y luego en **Aplicar**.
6. Haga clic en **Guardar** y, a continuación, haga clic en **Sí** para aceptar los cambios.Las características del grupo de túnel, la política de grupo y el reenvío de puertos están ahora enlazadas.

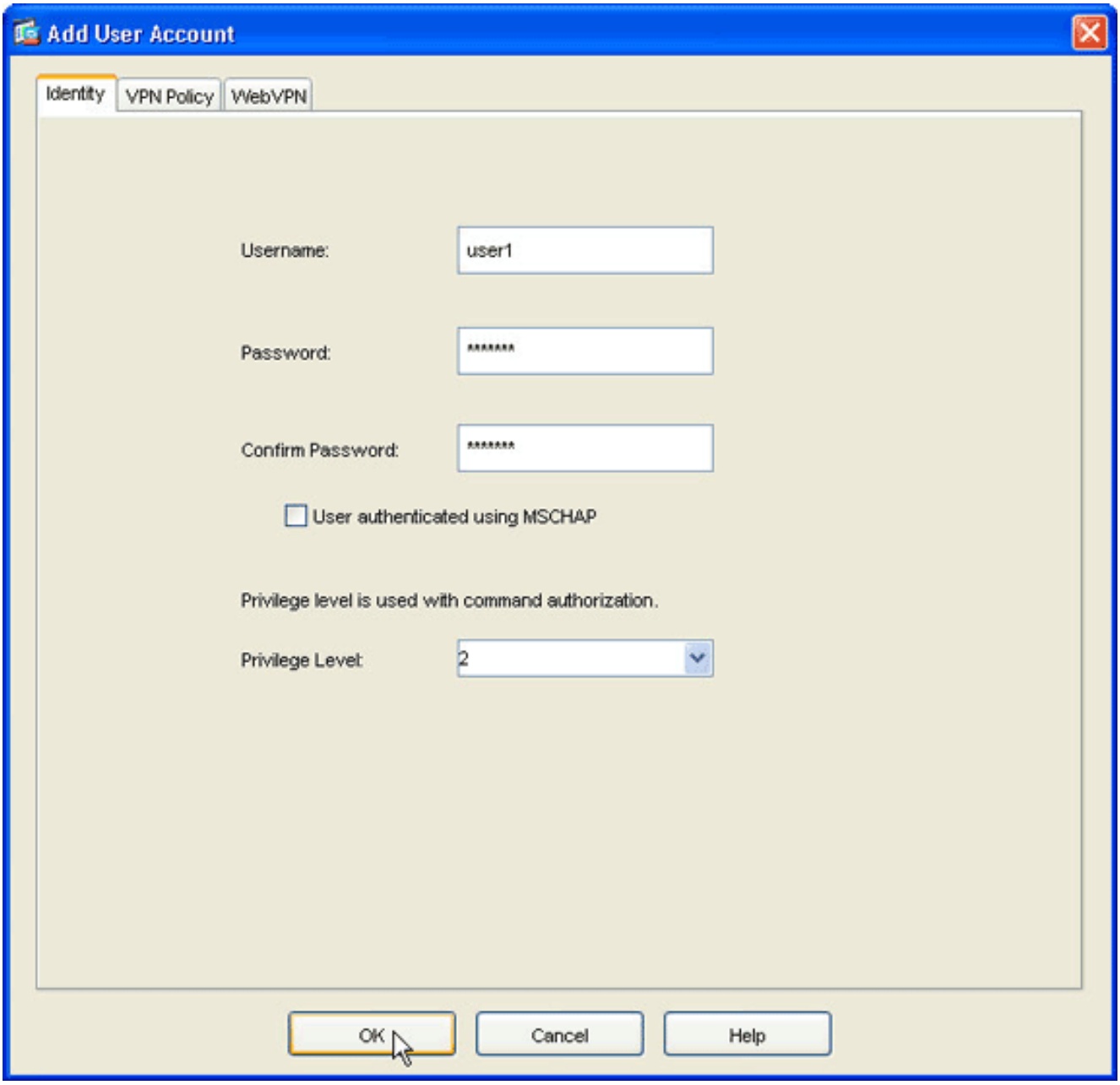
Paso 5. Crear un usuario y agregarlo a la directiva de grupo

Para crear un usuario y agregarlo a la política de grupo, complete estos pasos:

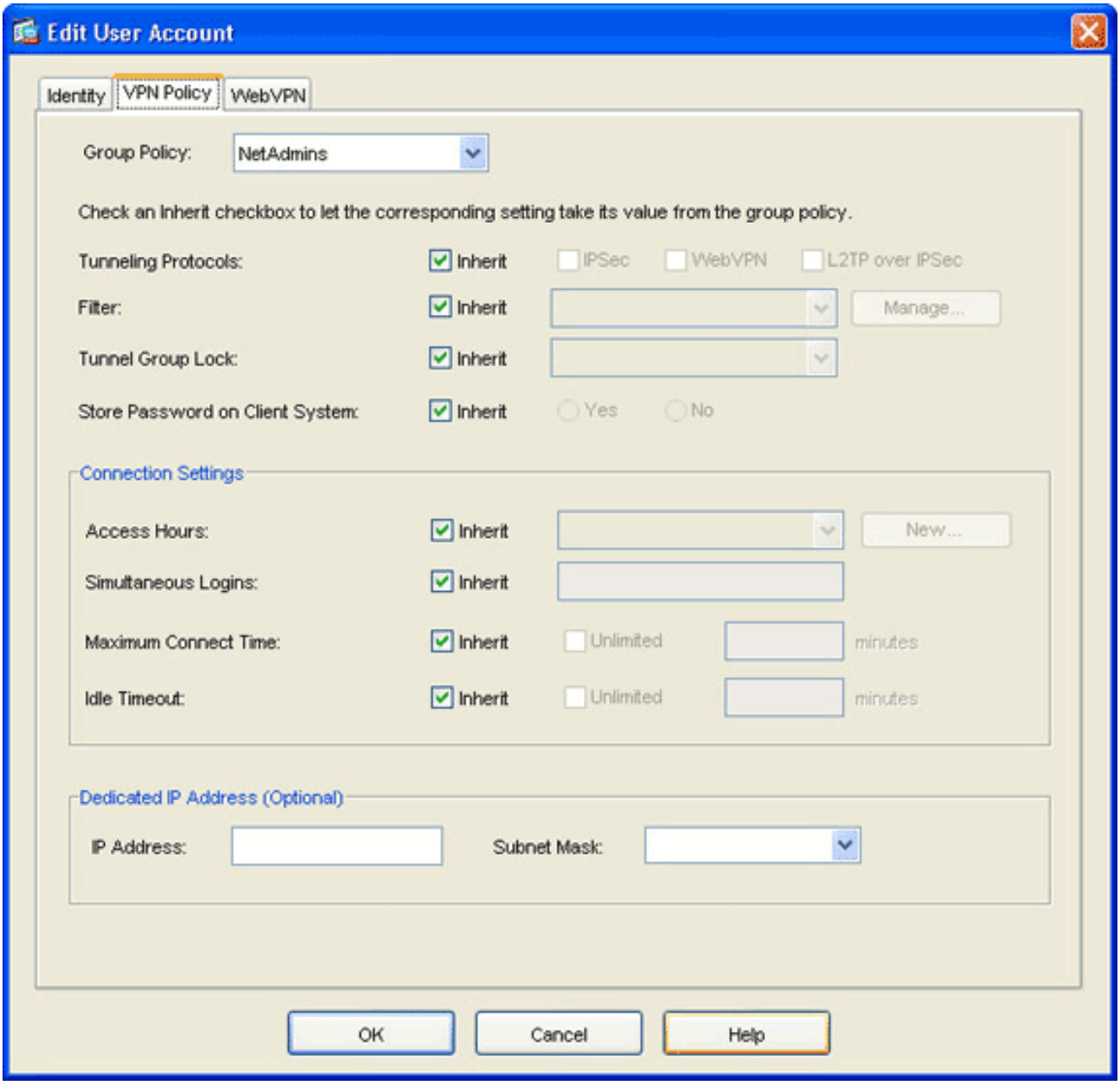
1. Expanda **General** y elija **Usuarios**.



2. ‘Haga clic en el botón Add (Agregar).’Aparecerá el cuadro de diálogo Agregar cuenta de usuario.



3. Ingrese los valores para la información de nombre de usuario, contraseña y privilegio, y luego haga clic en la pestaña **Política de VPN**.



4. Haga clic en la flecha desplegable **Política de grupo** y elija la política de grupo que creó en el Paso 3.Este usuario hereda las características y políticas de WebVPN de la política de grupo seleccionada.
5. Haga clic en **Aceptar** y luego en **Aplicar**.
6. Haga clic en **Guardar** y, a continuación, **Sí** para aceptar los cambios.

Configuración de Thin-Client SSL VPN con 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
```

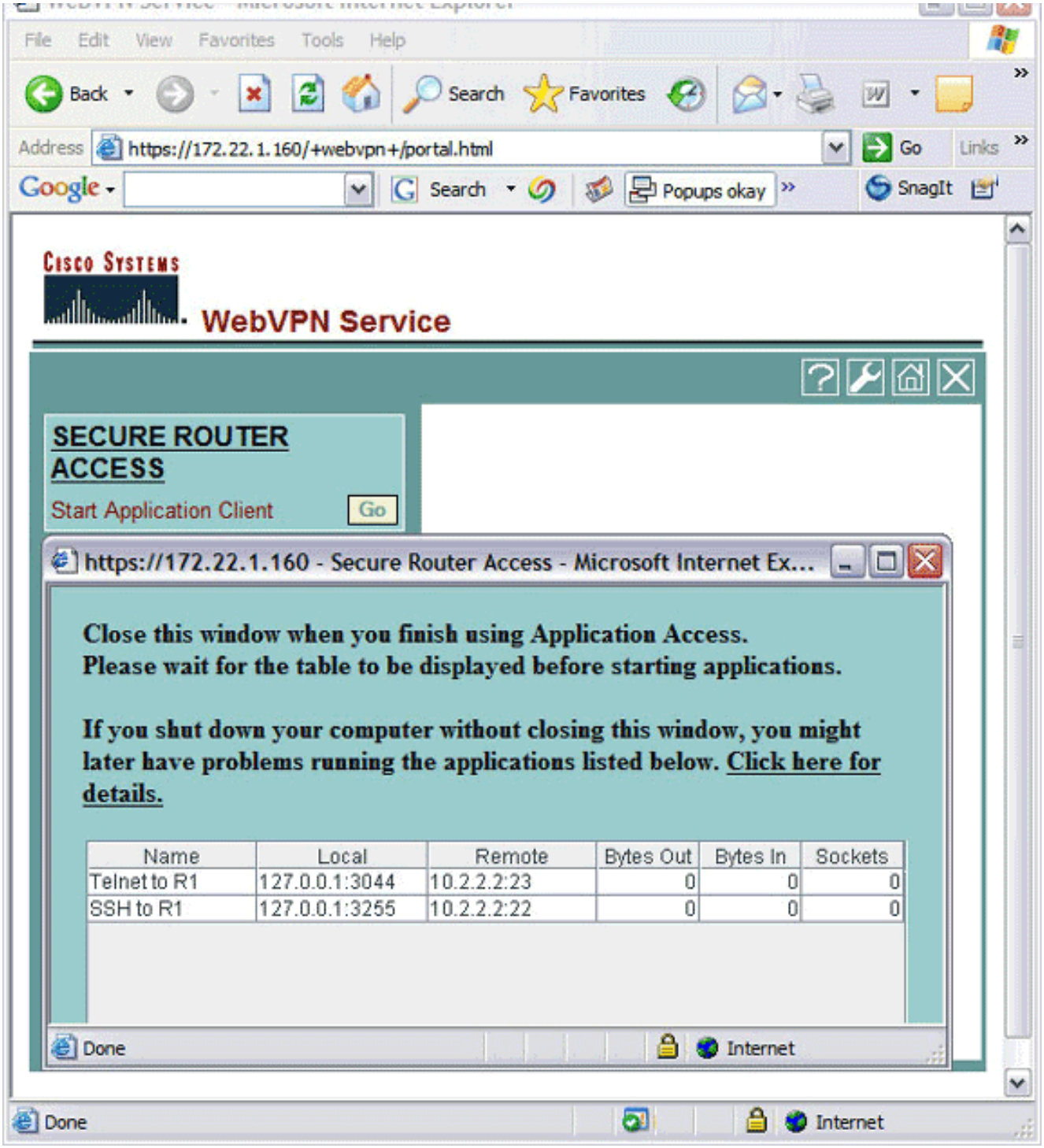
Verificación

Utilice esta sección para verificar que su configuración funciona correctamente.

Procedimiento

Este procedimiento describe cómo determinar la validez de la configuración y cómo probarla.

1. Desde una estación de trabajo cliente, ingrese **https:// *outside_ASA_IP Address*** ; donde *outside_ASA_IPAddress* es la URL SSL del ASA.Cuando se acepta el certificado digital y se autentica al usuario, aparece la página Web Servicio WebVPN.

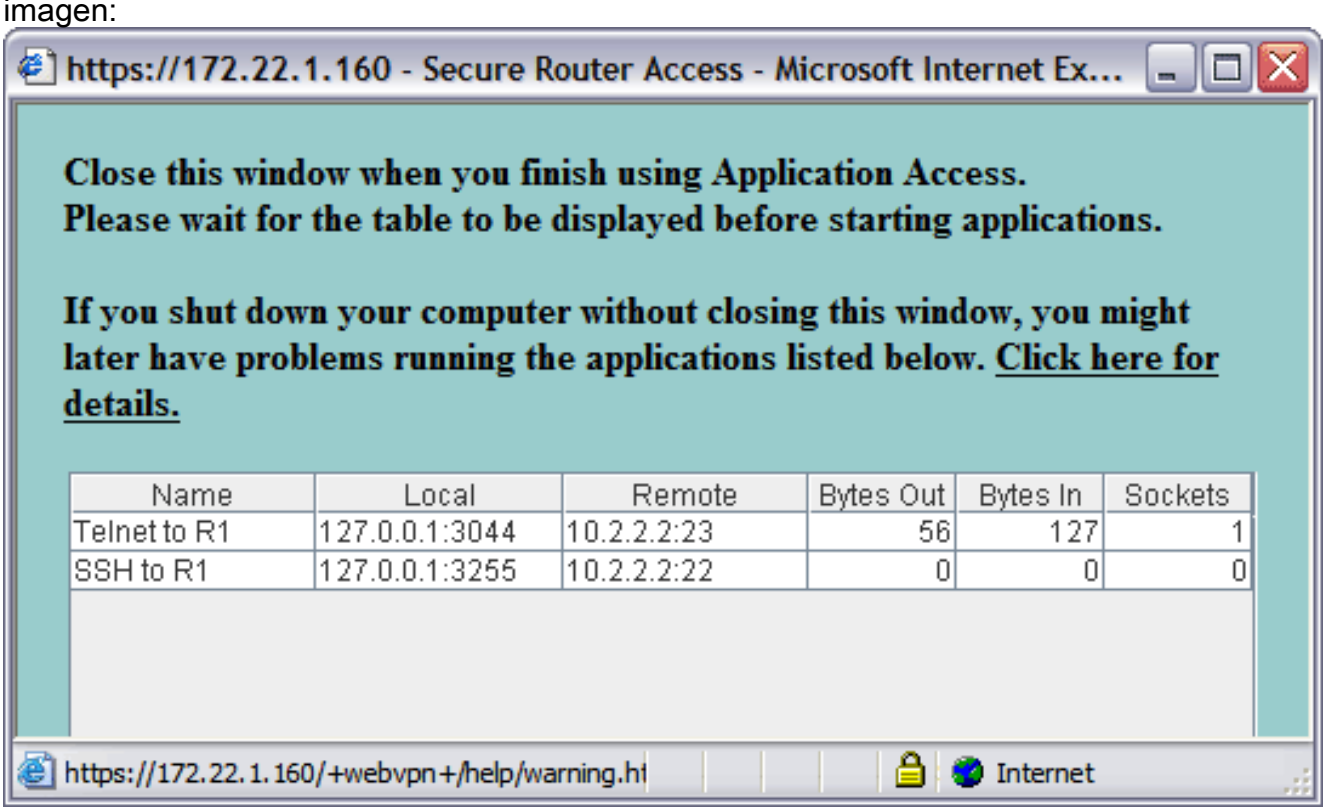


La dirección y la información de puerto necesarias para acceder a la aplicación aparecen en la columna local. Las columnas Bytes de salida y Bytes de entrada no muestran actividad porque la aplicación no se ha invocado en este momento.

2. Utilice el mensaje DOS u otra aplicación Telnet para iniciar una sesión Telnet.
3. En el símbolo del sistema, ingrese **telnet 127.0.0.1 3044**.**Nota:** Este comando proporciona un ejemplo de cómo obtener acceso al puerto local que se muestra en la imagen de la página Web del servicio WebVPN en este documento. *El comando no incluye dos puntos (:).* Escriba el comando como se describe en este documento.El ASA recibe el comando sobre la sesión segura y, como almacena un mapa de la información, el ASA sabe inmediatamente abrir la sesión Telnet segura al dispositivo
asignado.

Cuando introduzca su nombre de usuario y contraseña, el acceso al dispositivo se habrá completado.

4. Para verificar el acceso al dispositivo, verifique las columnas Bytes Out y Bytes In como se muestra en esta
imagen:



Comandos

Varios **comandos show se asocian a WebVPN.** Puede ejecutar estos comandos en command-line interface (CLI) para mostrar las estadísticas y otra información. Para obtener información detallada sobre los **comandos show, consulte** Verificar la Configuración WebVPN.

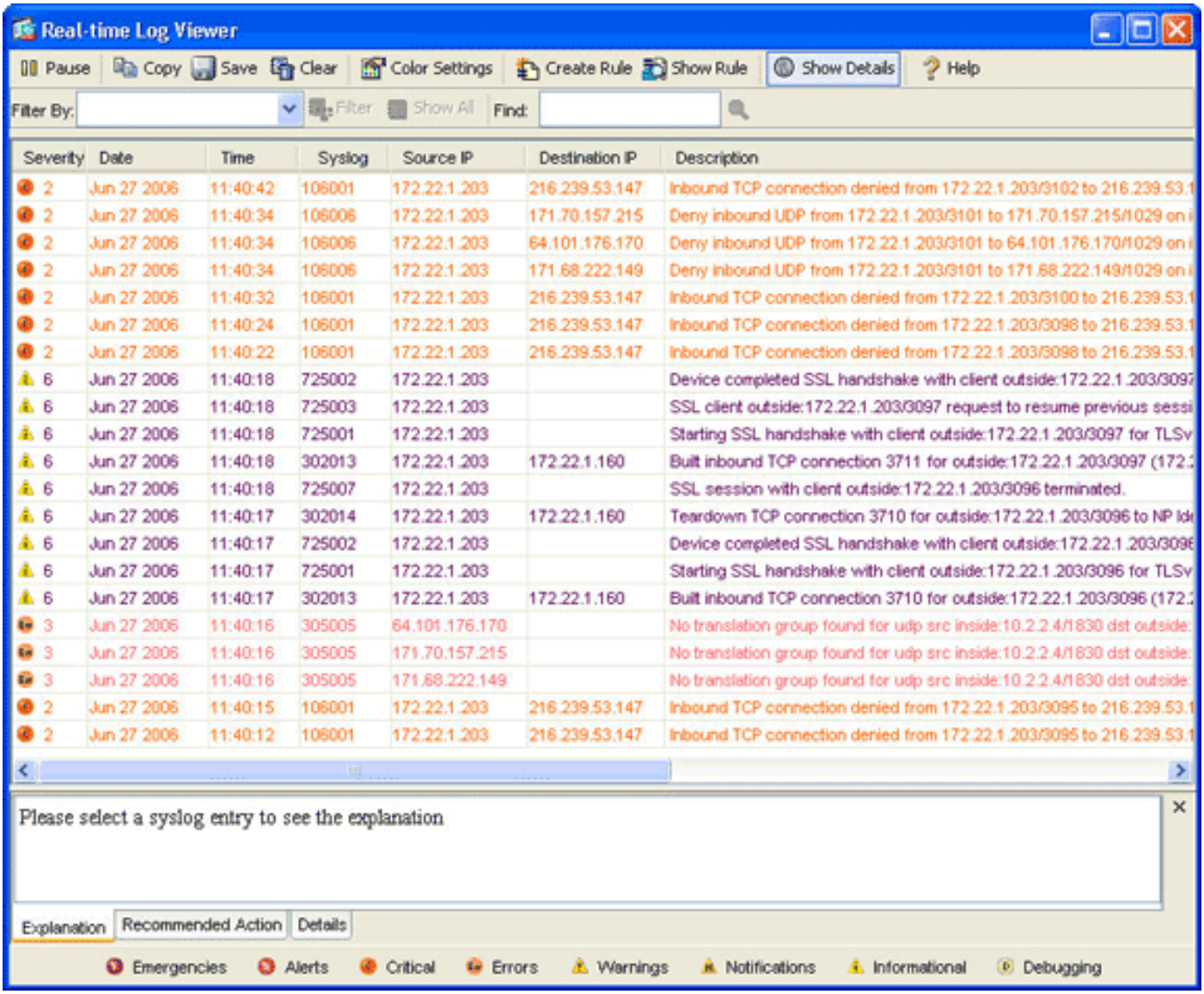
Nota: La Herramienta Output Interpreter (sólo clientes registrados) (OIT) admite determinados comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshoot

Use esta sección para resolver problemas de configuración.

¿Ha finalizado el proceso de intercambio de señales SSL?

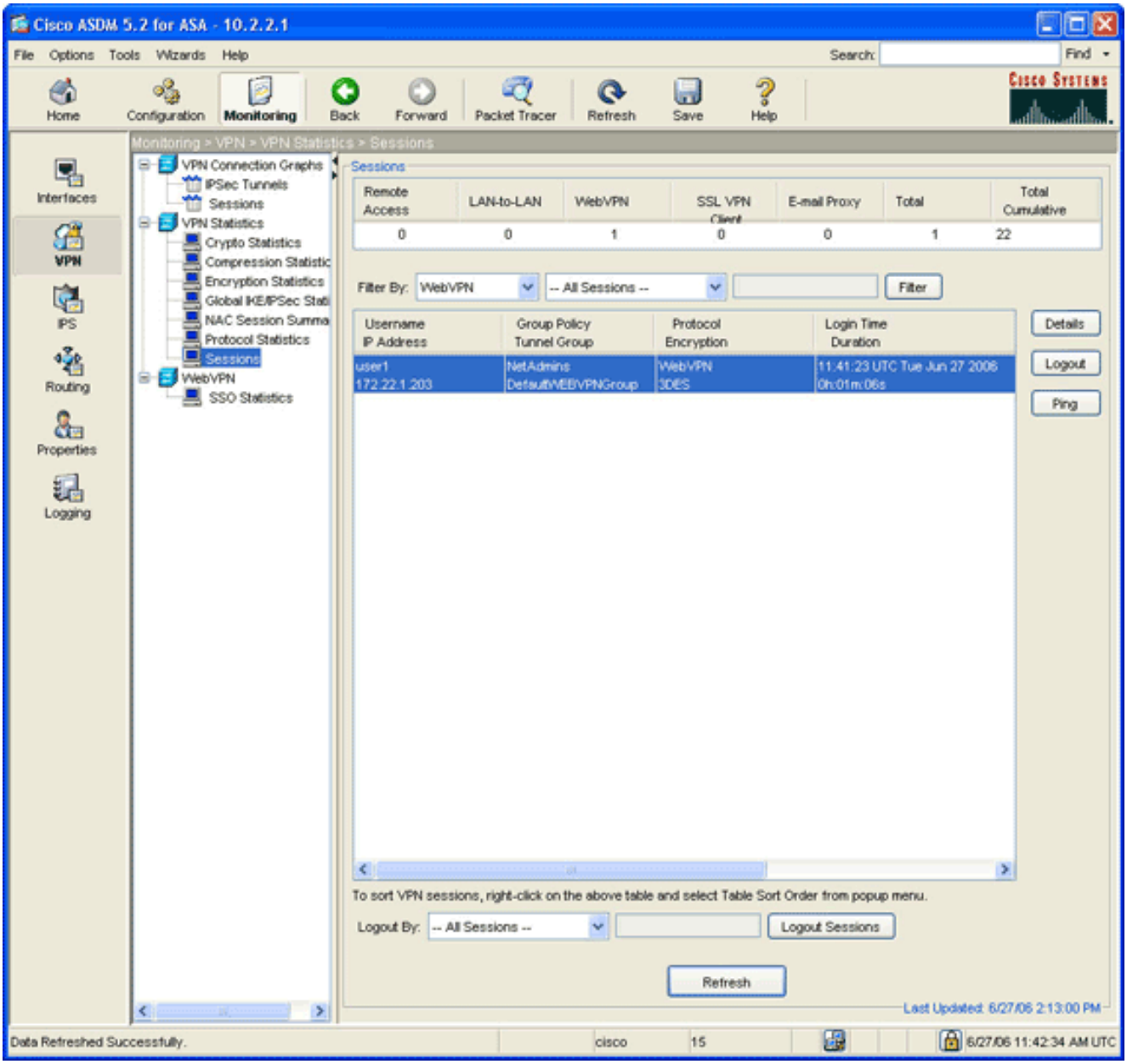
Una vez que se conecte al ASA, verifique si el registro en tiempo real muestra la finalización del intercambio de señales SSL.



¿Funciona el SSL VPN Thin-Client?

Para verificar que el SSL VPN Thin-Client funcione, complete estos pasos:

1. Haga clic en **Monitoring** y luego en **VPN**.
2. Expanda **Estadísticas de VPN** y haga clic en **Sesiones**.Su sesión de SSL VPN Thin-Client debe aparecer en la lista de sesiones. Asegúrese de filtrar por WebVPN como se muestra en esta
   imagen:



Comandos

Varios **comandos debug se asocian a WebVPN.** Para obtener información detallada sobre estos comandos, consulte Uso de los Comandos Debug de WebVPN.

Nota: El uso de los comandos **debug** puede afectar negativamente a su dispositivo Cisco. Antes de que utilice los **comandos debug, consulte** Información Importante sobre los Comandos Debug.

Información Relacionada

- Ejemplo de Configuración de Clientless SSL VPN (WebVPN) en ASA
- Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM
- Cisco ASA 5500 Series Adaptive Security Appliances
- Ejemplo de Configuración de ASA con WebVPN y Single Sign-on con ASDM y NTLMv1
- Soporte Técnico y Documentación - Cisco Systems