Cliente “liviano” SSL VPN (WebVPN) en el ASA con el ejemplo de la Configuración de ASDM

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Diagrama de la red
Convenciones
Antecedentes
Configuración VPN del cliente “liviano” SSL usando el ASDM
Paso 1. WebVPN del permiso en el ASA
Paso 2. Características de la expedición del puerto de la configuración
Paso 3. Cree una directiva del grupo y conéctela a la lista de la expedición del puerto
Paso 4. Cree a un grupo de túnel y conéctelo a la directiva del grupo
Paso 5. Cree a un usuario y agregue a ese usuario a la directiva del grupo
Configuración VPN del cliente “liviano” SSL usando el CLI
Verificación
Procedimiento
Comandos
Troubleshooting
¿Es el contacto SSL de proceso completa?
¿Es el cliente “liviano” SSL VPN funcional?
Comandos
Información Relacionada

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 a un cliente remoto que requiera a un buscador Web SSL-habilitado acceder a los servidores Web HTTP o HTTPS en un red de área local (LAN) corporativo. Además, el clientless SSL VPN proporciona el acceso para el archivo de Windows que hojea con el protocolo del Common Internet File System (CIFS). El Acceso Web de la perspectiva (OWA) es un acceso del ejemplo de HTTP.Refiera al clientless SSL VPN (WebVPN) en el ejemplo de configuración ASA para aprender más sobre el

clientless SSL VPN.

- **El cliente "liviano" SSL VPN (expedición del puerto)** — proporciona a un cliente remoto que descargue un pequeño applet de la Java basada y permite el acceso seguro para las aplicaciones del Transmission Control Protocol (TCP) que utilizan los números del puerto estático. El protocolo Post Office Protocol (POP3), el Simple Mail Transfer Protocol (SMTP), el Internet Message Access Protocol (IMAP), el Secure Shell (SSH), y Telnet son ejemplos del acceso seguro. Porque los archivos en la máquina local cambian, los usuarios deben tener privilegios administrativos locales de utilizar este método. Este método de SSL VPN no trabaja con las aplicaciones que utilizan las asignaciones de puerto dinámico, tales como algunas aplicaciones del File Transfer Protocol (FTP).**Nota:** El User Datagram Protocol (UDP) no se soporta.
- **Cliente VPN SSL (modo túnel)** — Descarga a un pequeño cliente a la estación de trabajo remota y permite el acceso seguro completo a los recursos en una red corporativa interna. Usted puede descargar permanentemente el (SVC) del cliente VPN SSL a una estación de trabajo remota, o usted puede quitar al cliente una vez que la sesión segura es cerrada.Refiera al (SVC) del cliente VPN SSL en el ASA con el ejemplo de la Configuración de ASDM para aprender más sobre el cliente VPN SSL.

Este documento demuestra una Configuración simple para el cliente "liviano" SSL VPN en el dispositivo de seguridad adaptante (ASA). La configuración permite a un usuario al telnet con seguridad a un router situado en el interior del ASA. La configuración en este documento se soporta para la Versión de ASA 7.x y posterior.

prerrequisitos

Requisitos

Antes de que usted intente esta configuración, asegúrese de que usted cumpla estos requisitos para las estaciones del cliente remoto:

- buscador Web SSL-habilitado
- Versión JRE 1.4 de las Javas del SOL o más adelante
- Cookie habilitados
- Moldes móviles inhabilitados
- Privilegios administrativos locales (no requeridos sino sugeridos fuertemente)

Nota: La última versión de las Javas JRE del SOL está disponible como descarga gratuita del sitio web de las Javas .

Componentes Utilizados

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

- 5510 Series adaptantes del dispositivo de seguridad de Cisco
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Nota:** Consulte Cómo Permitir el Acceso HTTPS para el ASDM para que el ASA sea configurado por el ASDM.
- Versión de software adaptante del dispositivo de seguridad de Cisco 7.2(1)
- Profesional del Microsoft Windows XP (cliente remoto SP 2)

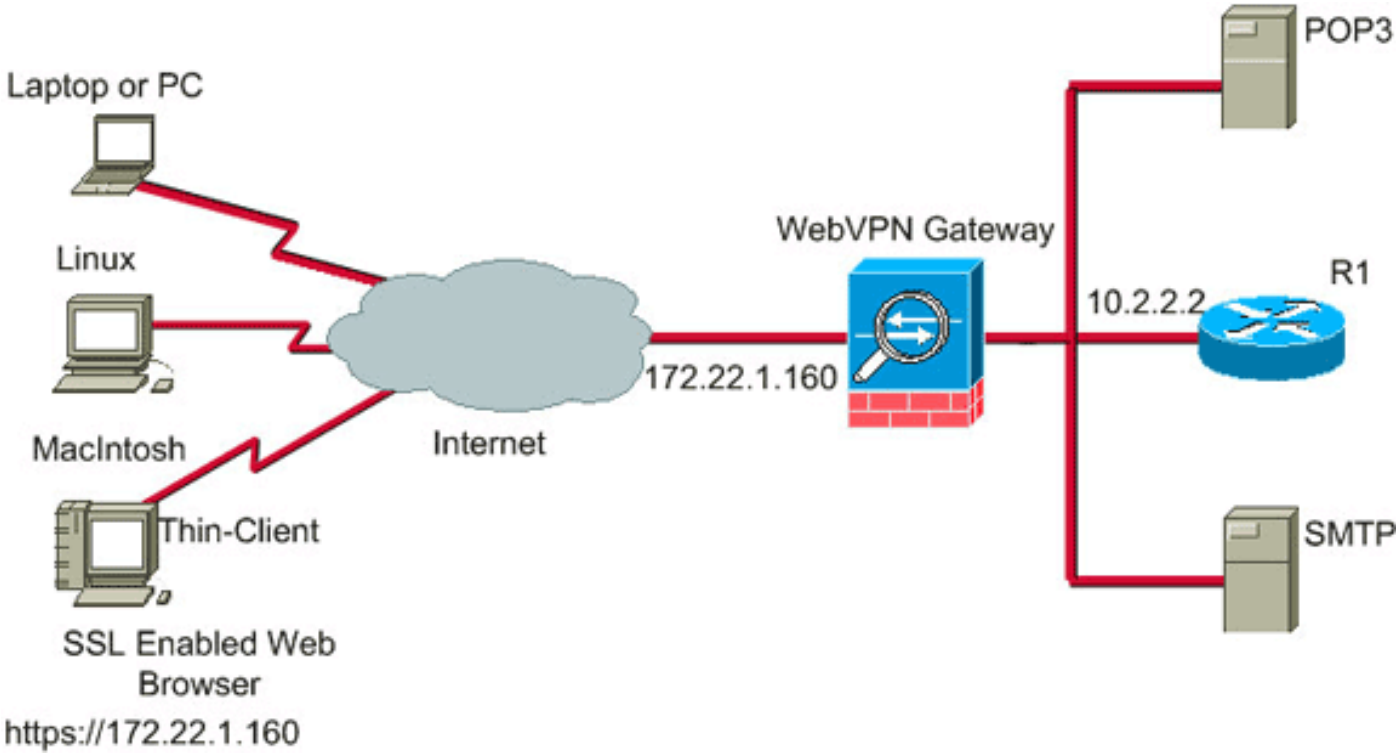
La información en este documento fue desarrollada en un ambiente de laboratorio. Todos los

dispositivos usados en este documento fueron reajustados a su configuración predeterminada. Si su red está viva, aseegurese le entender el impacto potencial del comando any. Todos los IP Addresses usados en esta configuración fueron seleccionados de los direccionamientos del RFC 1918 en un ambiente de laboratorio; estos IP Addresses no son routable en Internet y están para las para pruebas solamente.

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 los pequeños subprogramas java al puesto de trabajo. Presentan el cliente con una lista de recursos preconfigurados.



Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Antecedentes

Para comenzar una sesión, el cliente remoto abre a un navegador SSL en la interfaz exterior del ASA. Después de que se establezca la sesión, el usuario puede utilizar los parámetros configurados en el ASA para invocar cualquier Telnet o acceso de la aplicación. Los proxys ASA la conexión segura y permiten el acceso del usuario al dispositivo.

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

Configuración VPN del cliente “liviano” SSL usando el ASDM

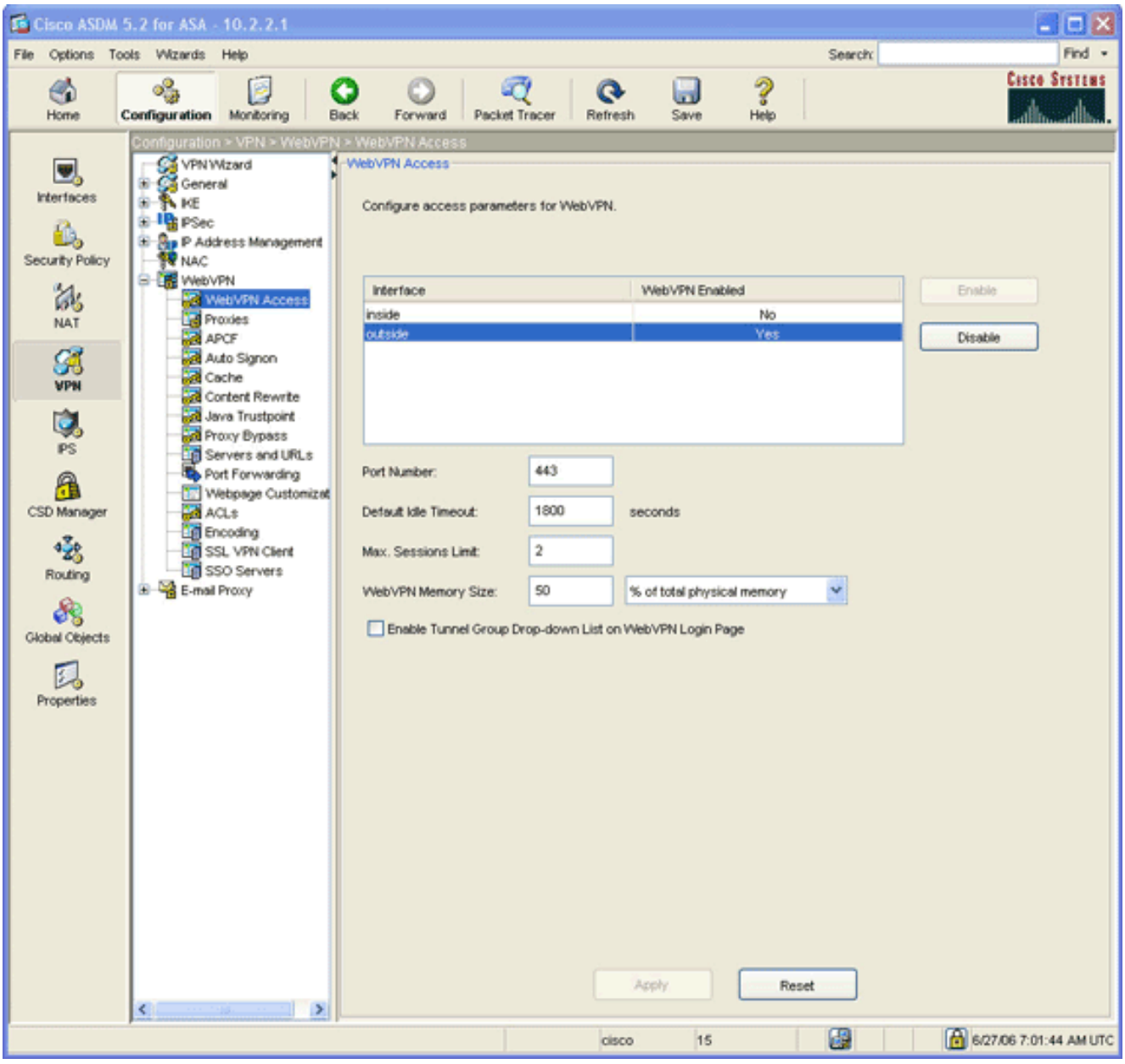
Para configurar al cliente “liviano” SSL VPN en el ASA, complete estos pasos:

1. Habilite el WebVPN en el ASA
2. Configure las características de la expedición del puerto
3. Cree una directiva del grupo y conéctela a la lista de la expedición del puerto (creada en el paso 2)
4. Cree a un grupo de túnel y conéctelo a la directiva del grupo (creada en el paso 3)
5. Cree a un usuario y agregue que usuario a la directiva del grupo (creada en el paso 3)

Paso 1. WebVPN del permiso en el ASA

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

1. Dentro de la aplicación ASDM, haga clic la **configuración**, y después haga clic el **VPN**.
2. Amplíe el **WebVPN**, y elija el **acceso del WebVPN**.

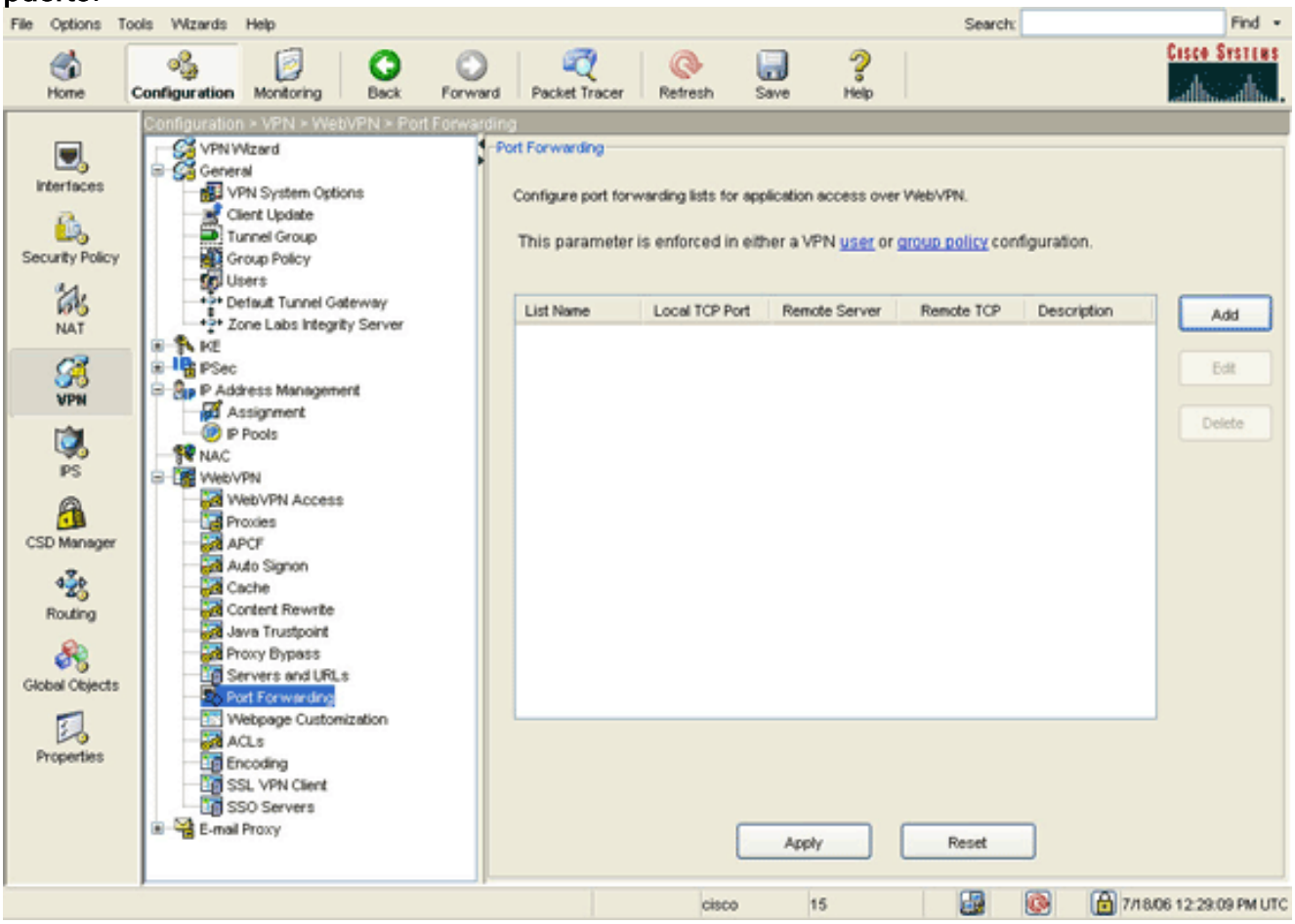


3. Resalte la interfaz, y haga clic el **permiso**.
4. El tecleo **se aplica**, hace clic la **salvaguardia**, y después hace clic **sí** para validar los cambios.

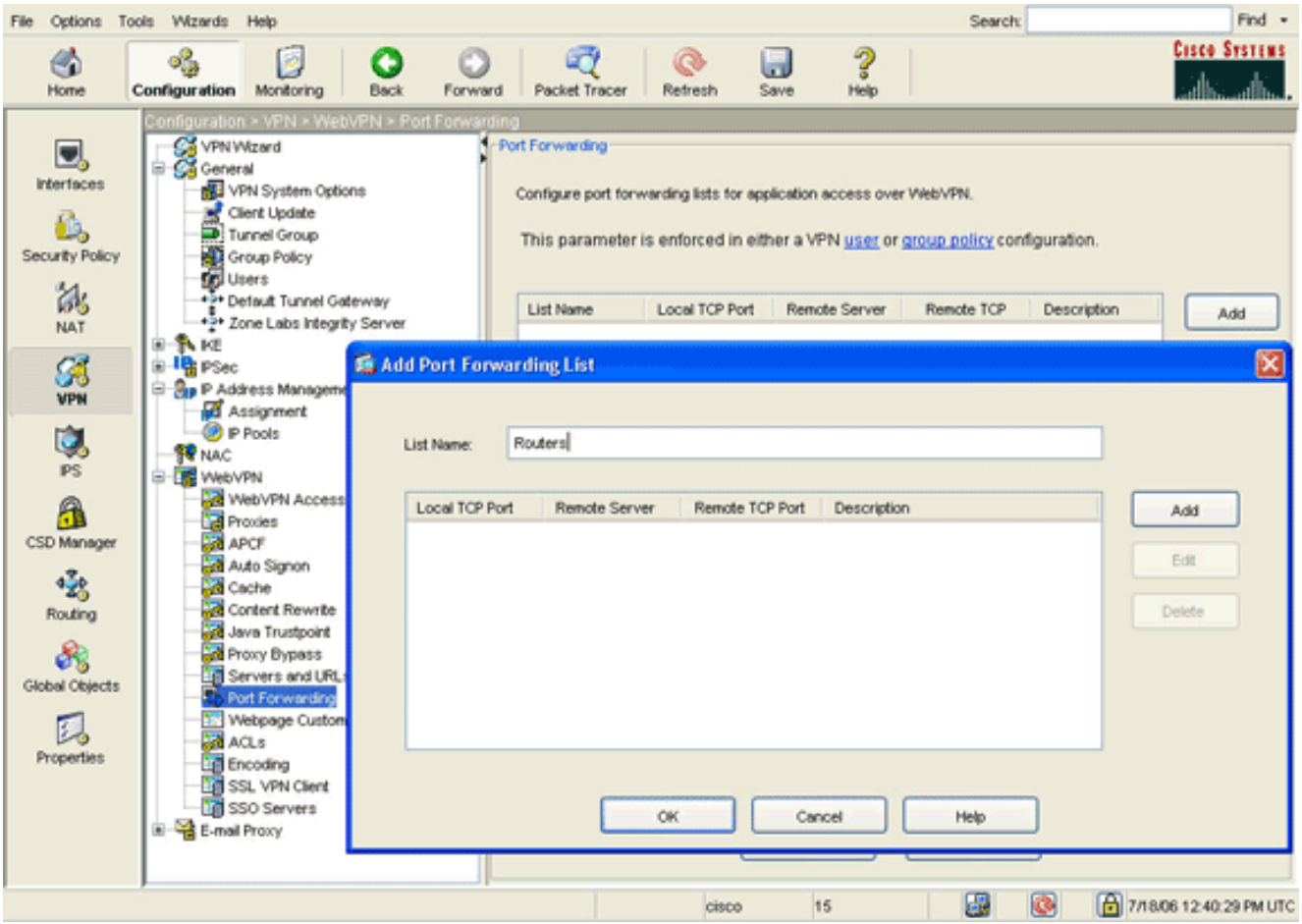
Paso 2. Características de la expedición del puerto de la configuración

Para configurar las características de la expedición del puerto, complete estos pasos:

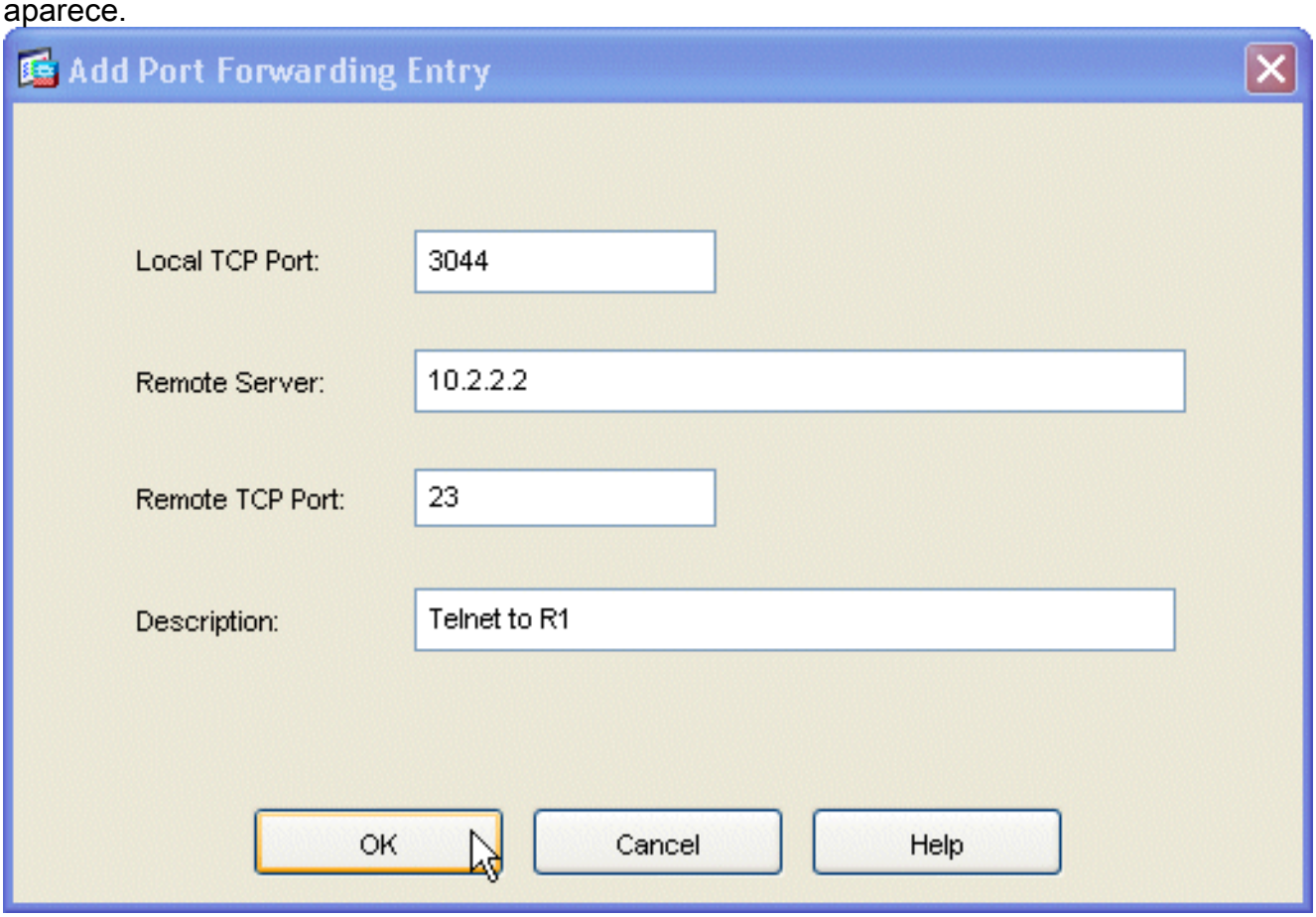
1. Amplíe el **WebVPN**, y elija la **expedición del puerto**.



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



3. En el cuadro de diálogo de la lista de la expedición del puerto del agregar, ingrese un nombre de la lista, y el haga click en AddEl cuadro de diálogo de la entrada de reenvío del puerto del agregar
aparece.



4. En el cuadro de diálogo de la entrada de reenvío del puerto del agregar, ingrese estas

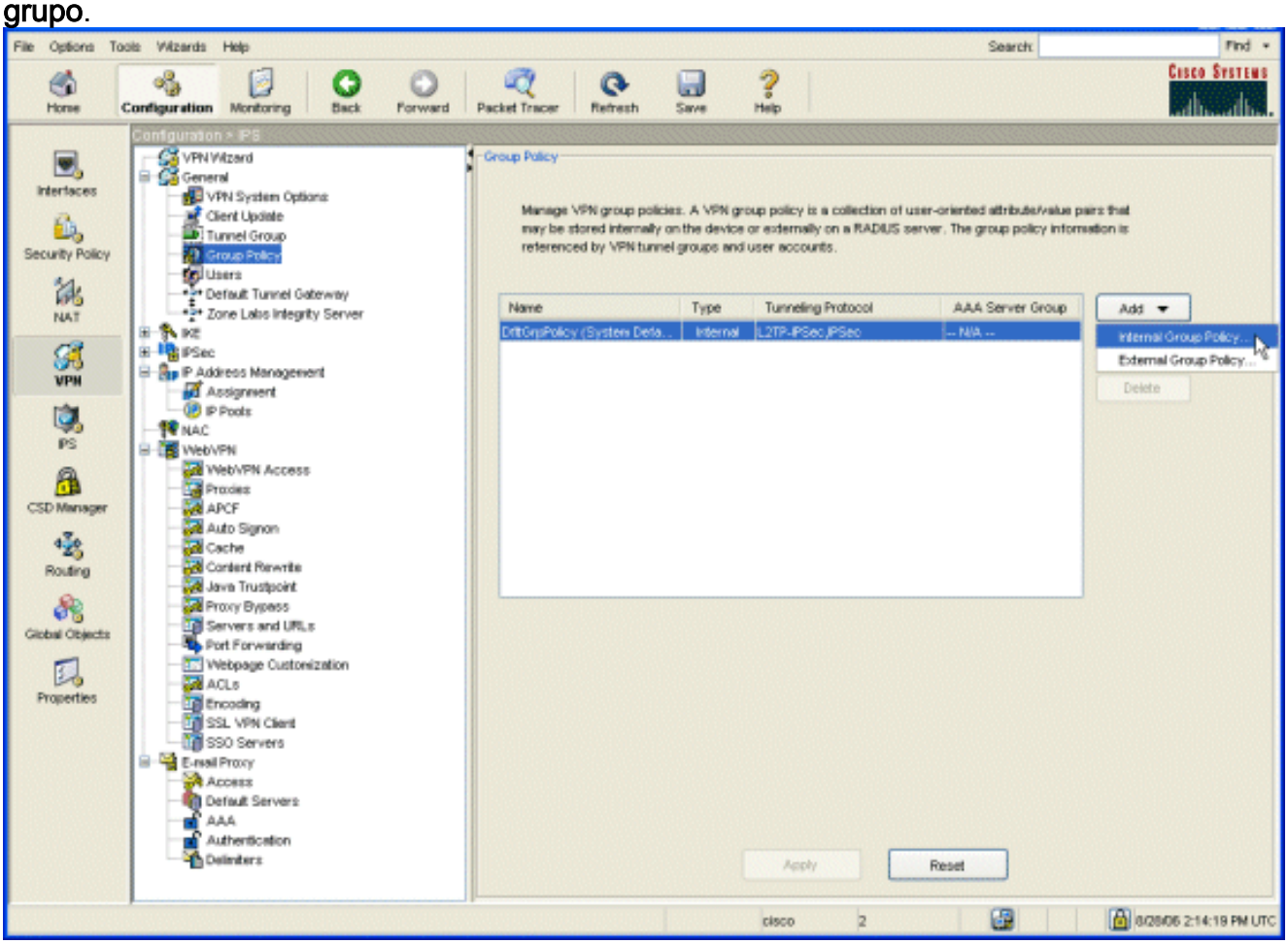
opciones:En el campo de puerto TCP local, ingrese un número del puerto o valide el valor predeterminado.El valor que usted ingresa puede ser cualquier número a partir de 1024 a 65535.En el campo del servidor remoto, ingrese un IP Address.Este ejemplo utiliza el direccionamiento del router.En el campo de puerto TCP alejado, ingrese un número del puerto.Este ejemplo utiliza el puerto 23.En el campo Description (Descripción), ingrese una descripción, y haga clic la **AUTORIZACIÓN**.

5. El Haga Click en OK, y entonces hace clic **se aplica**.
6. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

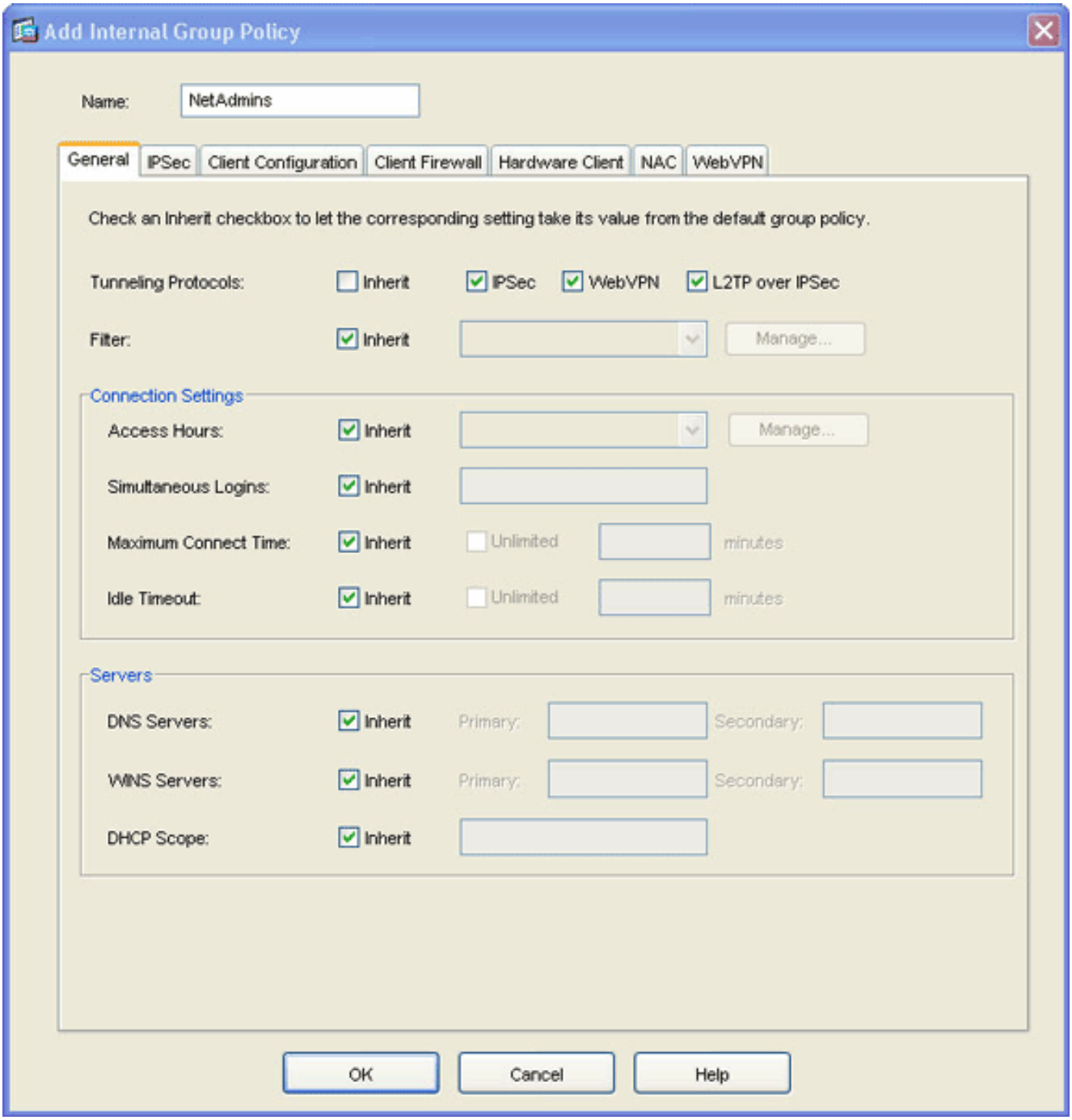
Paso 3. Cree una directiva del grupo y conéctela a la lista de la expedición del puerto

Para crear una directiva del grupo y conectarla a la lista de la expedición del puerto, complete estos pasos:

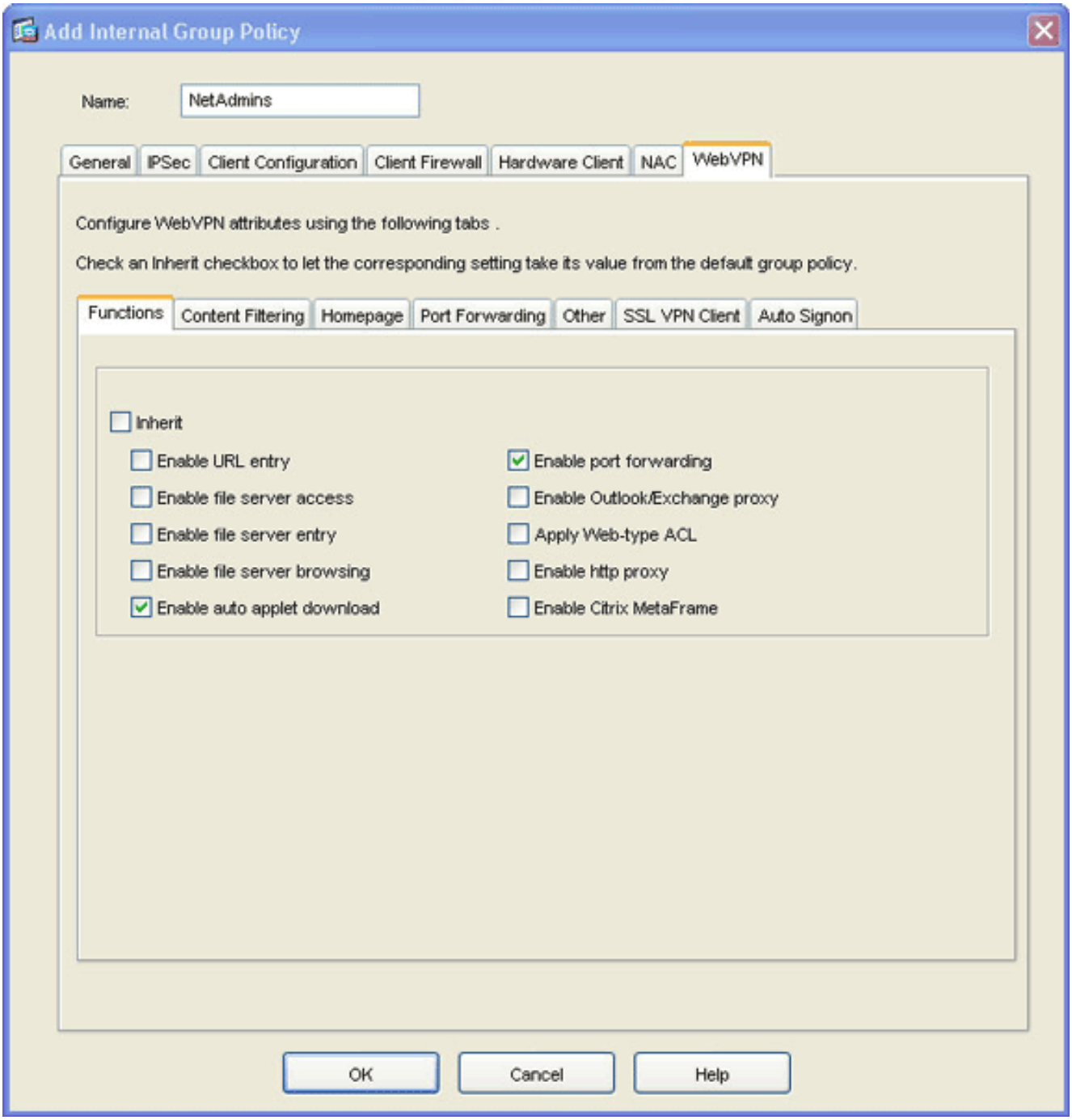
1. Amplíe al **general**, y elija la **directiva del grupo**.



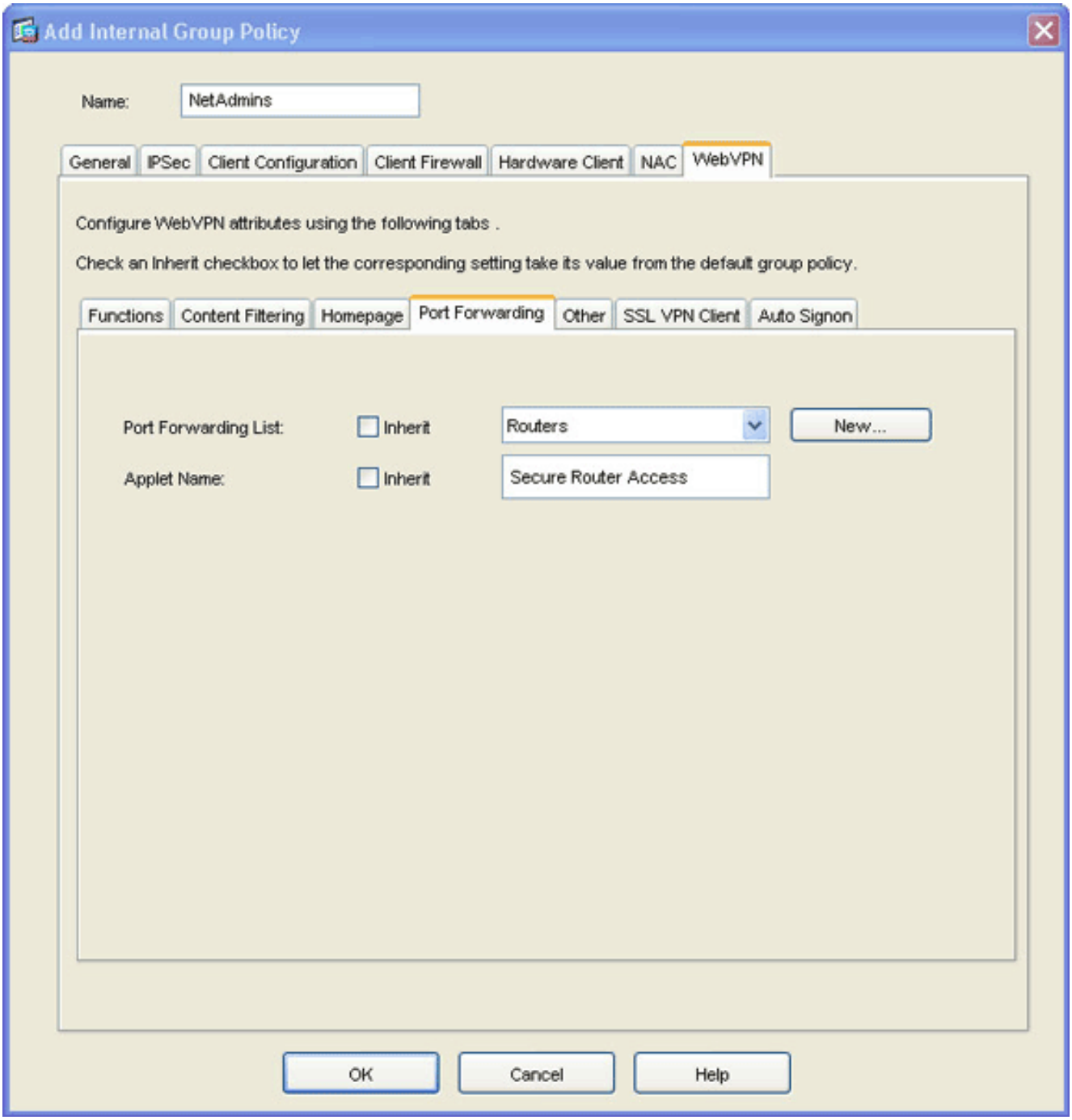
2. El tecleo **agrega**, y elige el **Internal group policy (política grupal interna)**.El cuadro de diálogo del Internal group policy (política grupal interna) del agregar aparece.



3. Ingrese un nombre o valide el nombre de la directiva del grupo predeterminado.
4. Desmarque los protocolos de túneles **heredan la** casilla de verificación, y marcan la casilla de verificación del **WebVPN**.
5. Haga clic la lengueta del **WebVPN** situada en la cima del cuadro de diálogo, y después haga clic la lengueta de las **funciones**.
6. Desmarque la casilla de verificación de la **herencia**, y marque la **descarga auto del applet del permiso** y **habilite las** casillas de verificación de la **expedición del puerto** tal y como se muestra en de esta
imagen:



7. También dentro de la lengueta del WebVPN, haga clic la lengueta de **expedición del puerto**, y desmarque la lista de la expedición del puerto **heredan la** casilla de verificación.



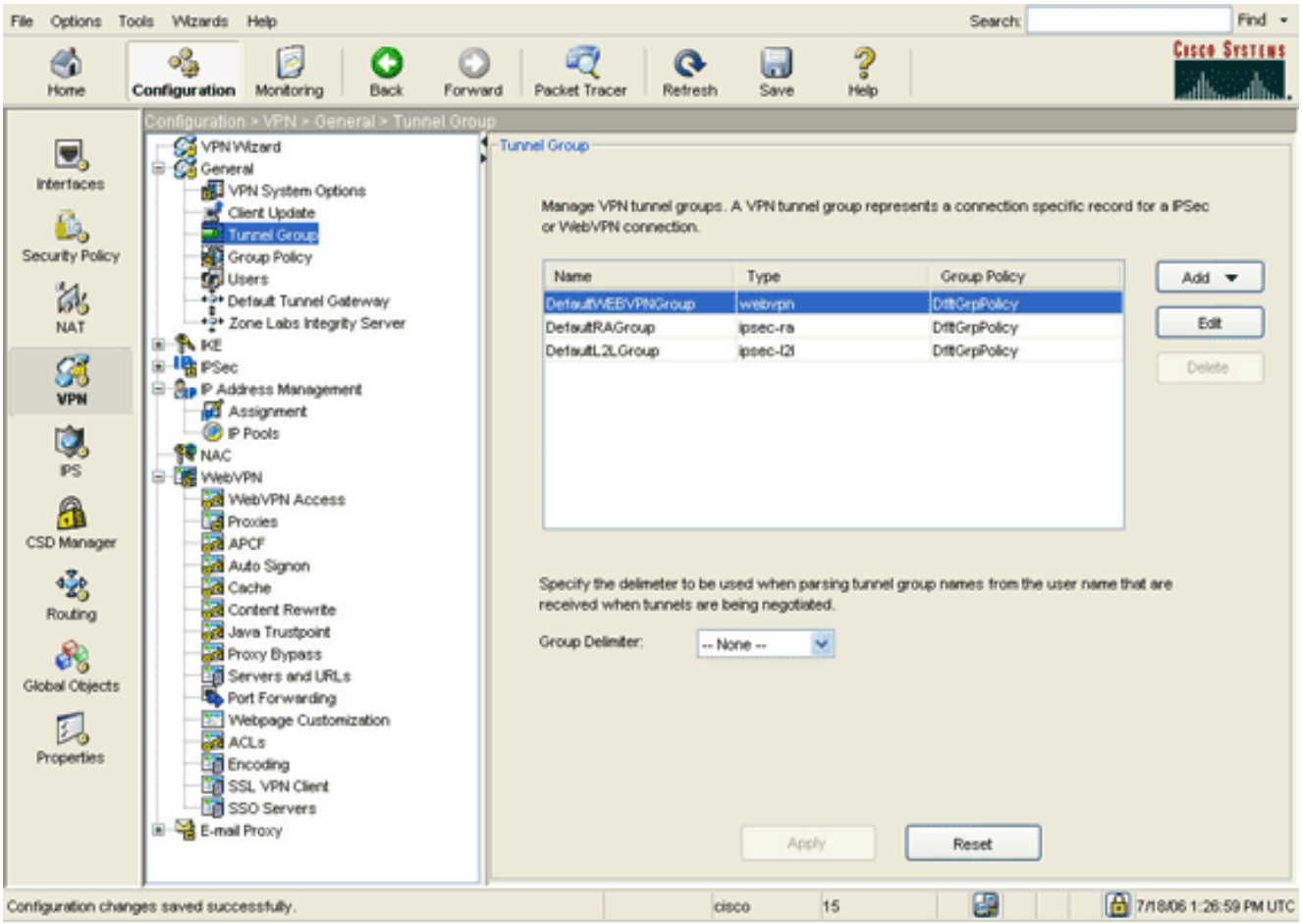
8. Haga clic la flecha desplegable de la **lista de la expedición del puerto**, y elija la lista de la expedición del puerto que usted creó en el paso 2.
9. Desmarque el nombre del applet **heredan la** casilla de verificación, y cambian el nombre en el campo de texto.El cliente visualiza el nombre del applet en la conexión.
10. El Haga Click en OK, y entonces hace clic **se aplica**.
11. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Paso 4. Cree a un grupo de túnel y conéctelo a la directiva del grupo

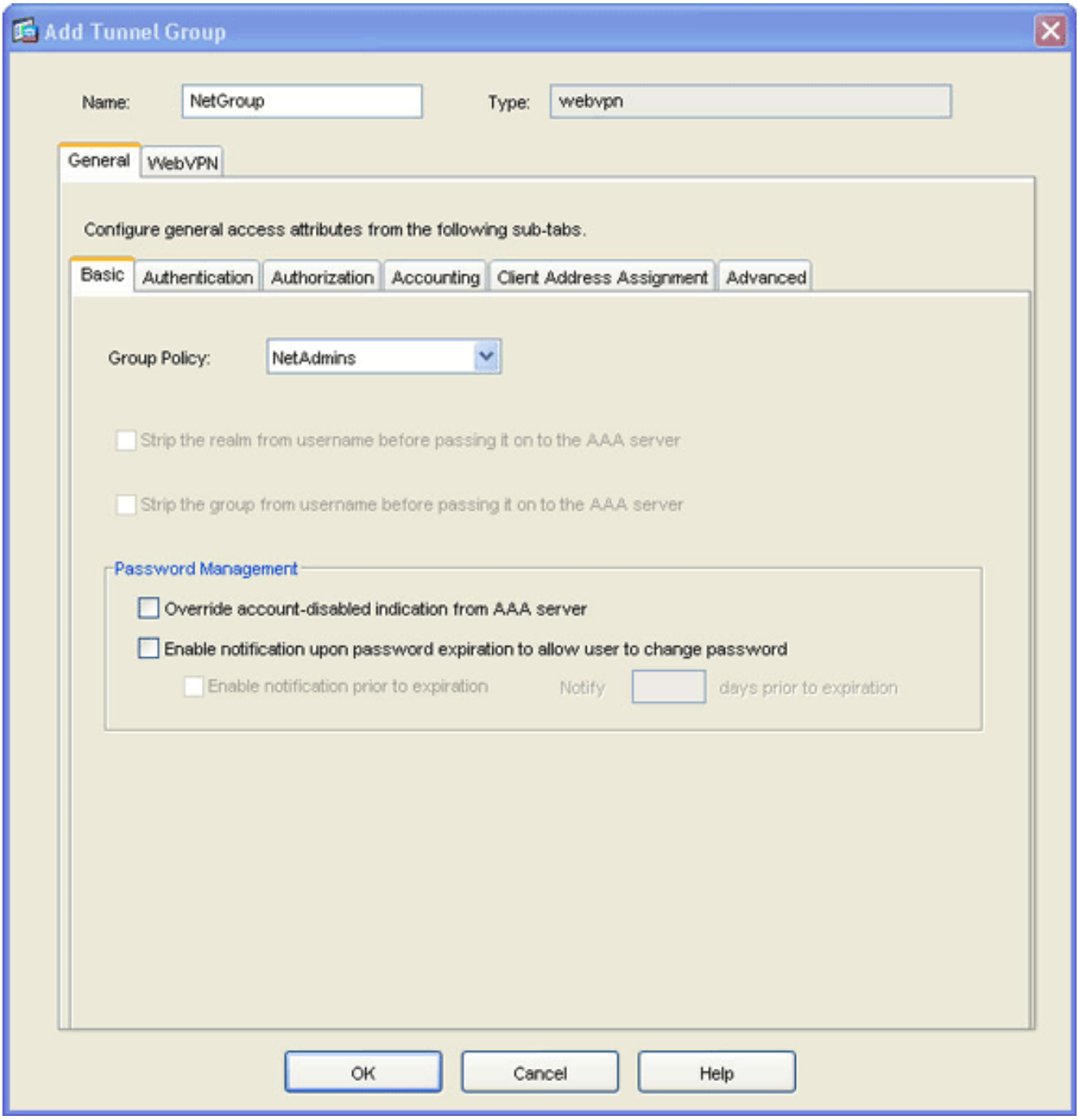
Usted puede editar al grupo de túnel predeterminado de *DefaultWebVPNGroup* o crear a un nuevo grupo de túnel.

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

1. Amplíe al **general**, y elija al **grupo de túnel**.



2. El tecleo **agrega**, y elige el **acceso del WebVPN**.El cuadro de diálogo del grupo de túnel del agregar
aparece.

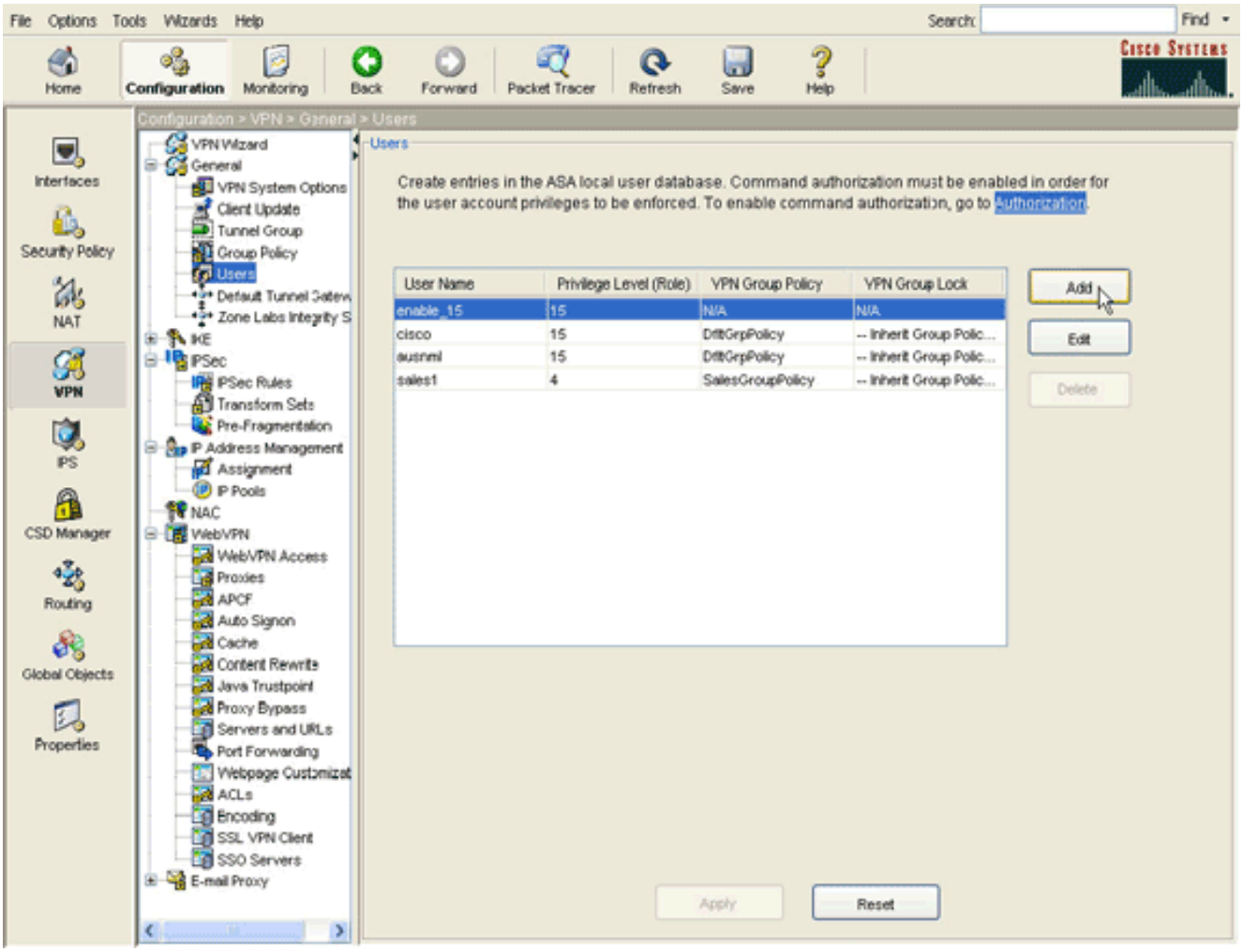


3. Ingrese un nombre en el campo de nombre.
4. Haga clic la flecha desplegable de la **directiva del grupo**, y elija la directiva del grupo que usted creó en el paso 3.
5. El Haga Click en OK, y entonces hace clic **se aplica**.
6. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.Ahora conectan al grupo de túnel, la directiva del grupo, y las características de la expedición del puerto.

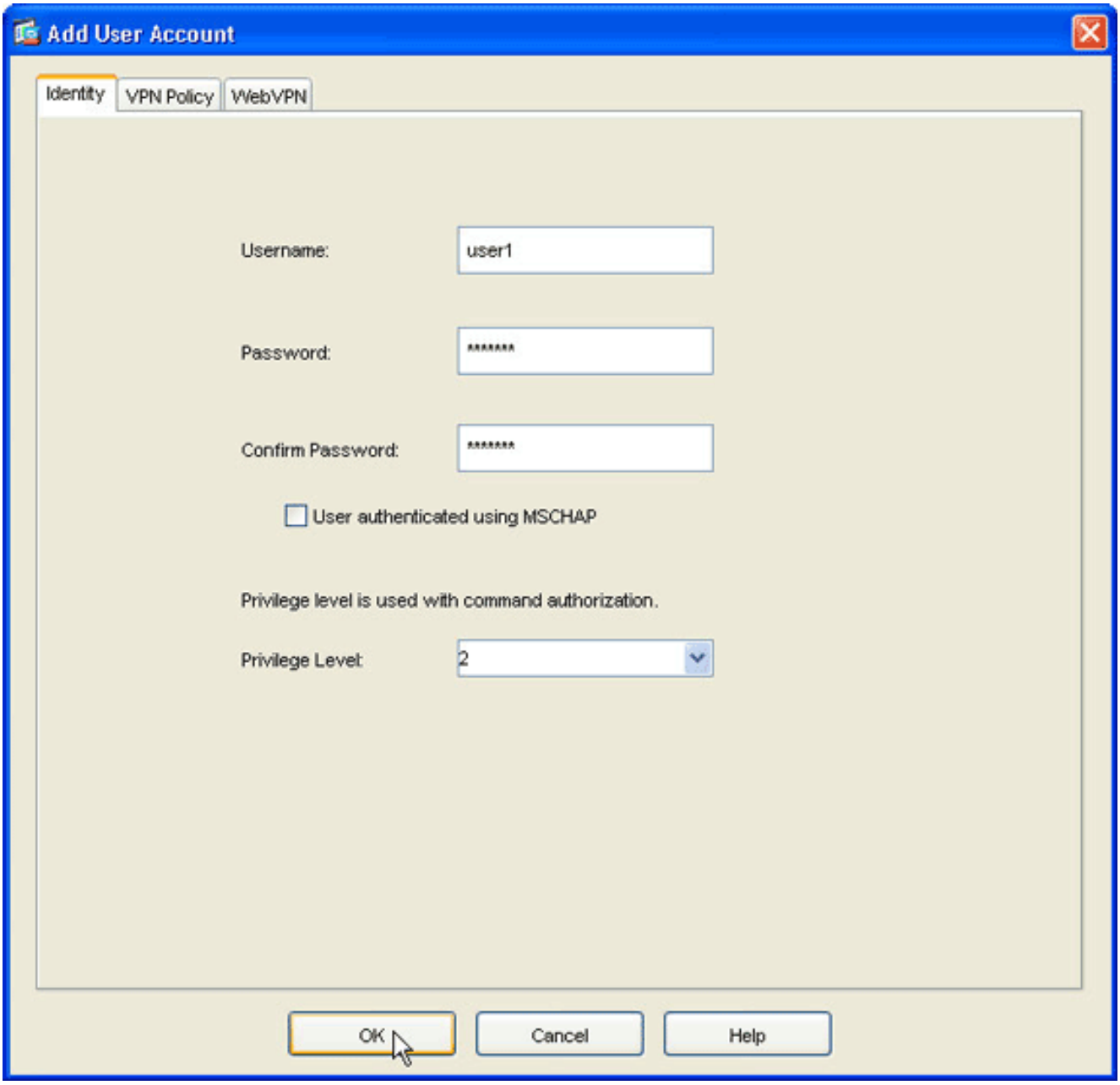
Paso 5. Cree a un usuario y agregue a ese usuario a la directiva del grupo

Para crear a un usuario y agregar a ese usuario a la directiva del grupo, complete estos pasos:

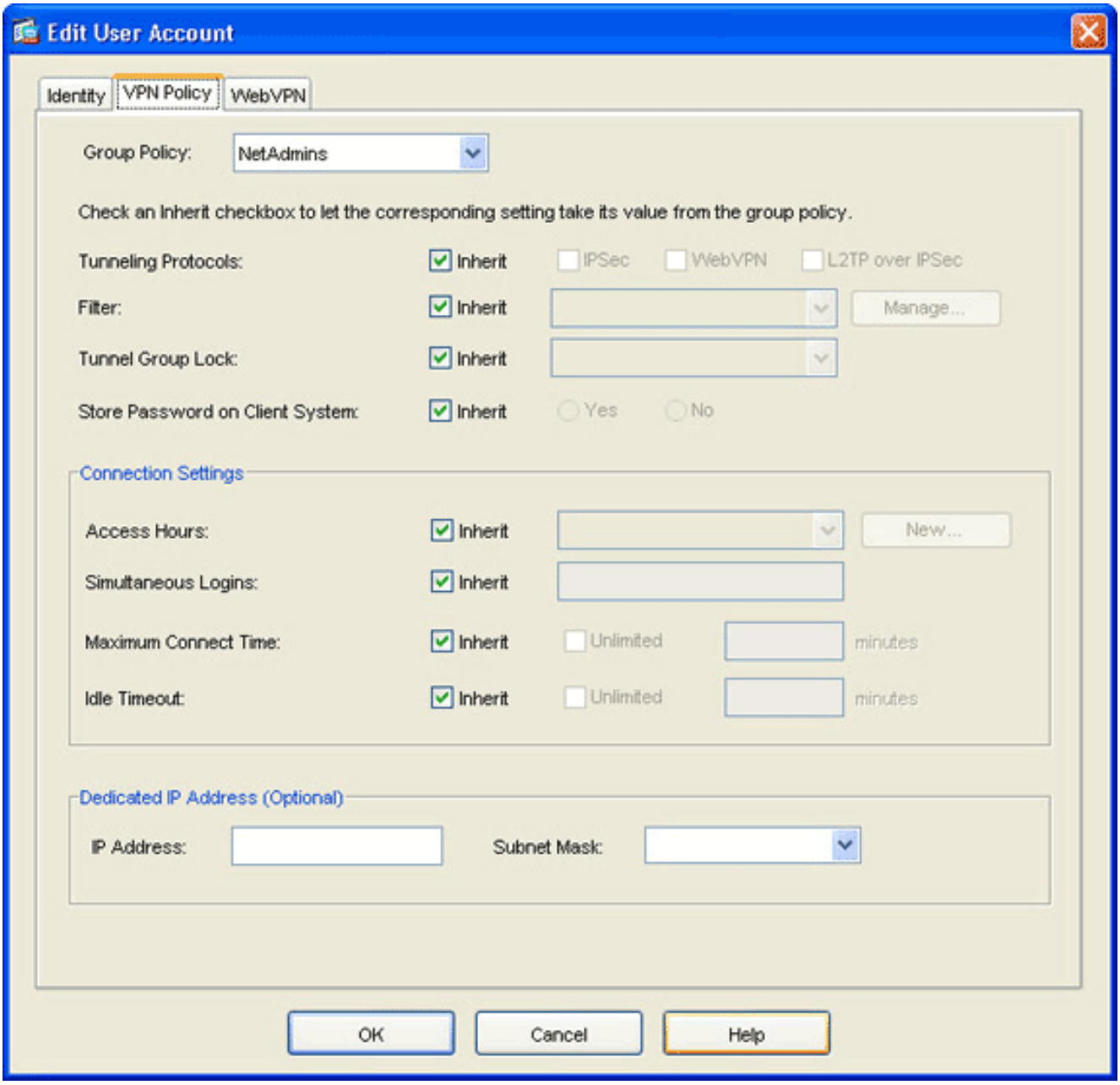
1. Amplíe al **general**, y elija a los **usuarios**.



2. ‘Haga clic en el botón Add (Agregar).’El cuadro de diálogo de la cuenta de usuario del agregar
aparece.



3. Ingrese los valores para el nombre de usuario, la contraseña, y la información del privilegio, y después haga clic la lengueta de la **política del VPN**.



4. Haga clic la flecha desplegable de la **directiva del grupo**, y elija la directiva del grupo que usted creó en el paso 3.Este usuario hereda las características del WebVPN y las directivas de la directiva seleccionada del grupo.
5. El Haga Click en OK, y entonces hace clic **se aplica**.
6. **Salvaguardia del** tecleo, y entonces validar **sí los** cambios.

Configuración VPN del cliente “liviano” SSL usando el 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
```

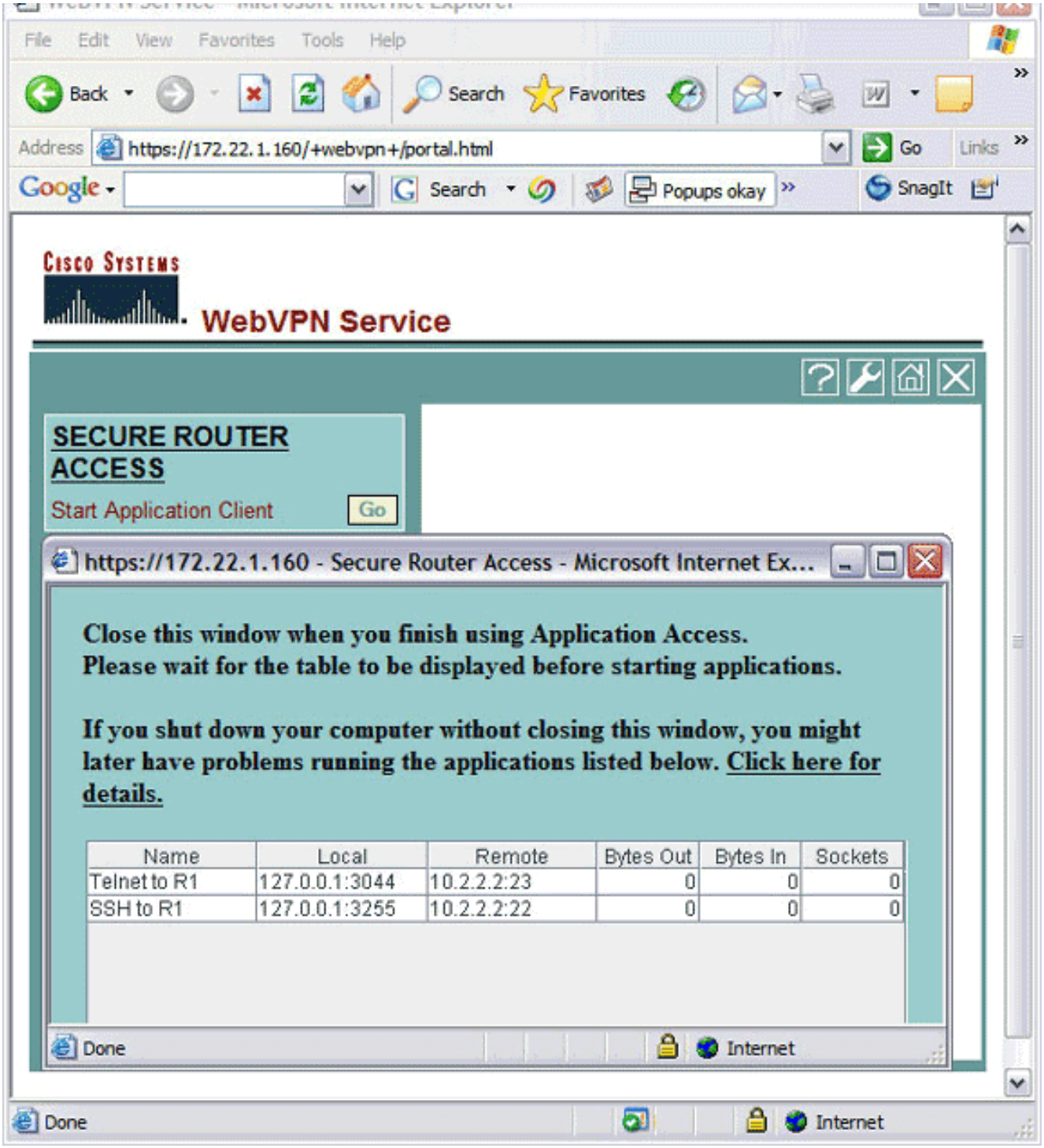
Verificación

Utilice esta sección para verificar que su configuración trabaja correctamente.

Procedimiento

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

1. De una estación de trabajo del cliente, ingrese el ***direccionamiento del outside_ASA_IP de*** **https://**; donde están el SSL los *outside_ASA_IPAddress* URL del ASA.Una vez que se valida el certificado digital, y autentican al usuario, la página web del servicio del WebVPN aparece.

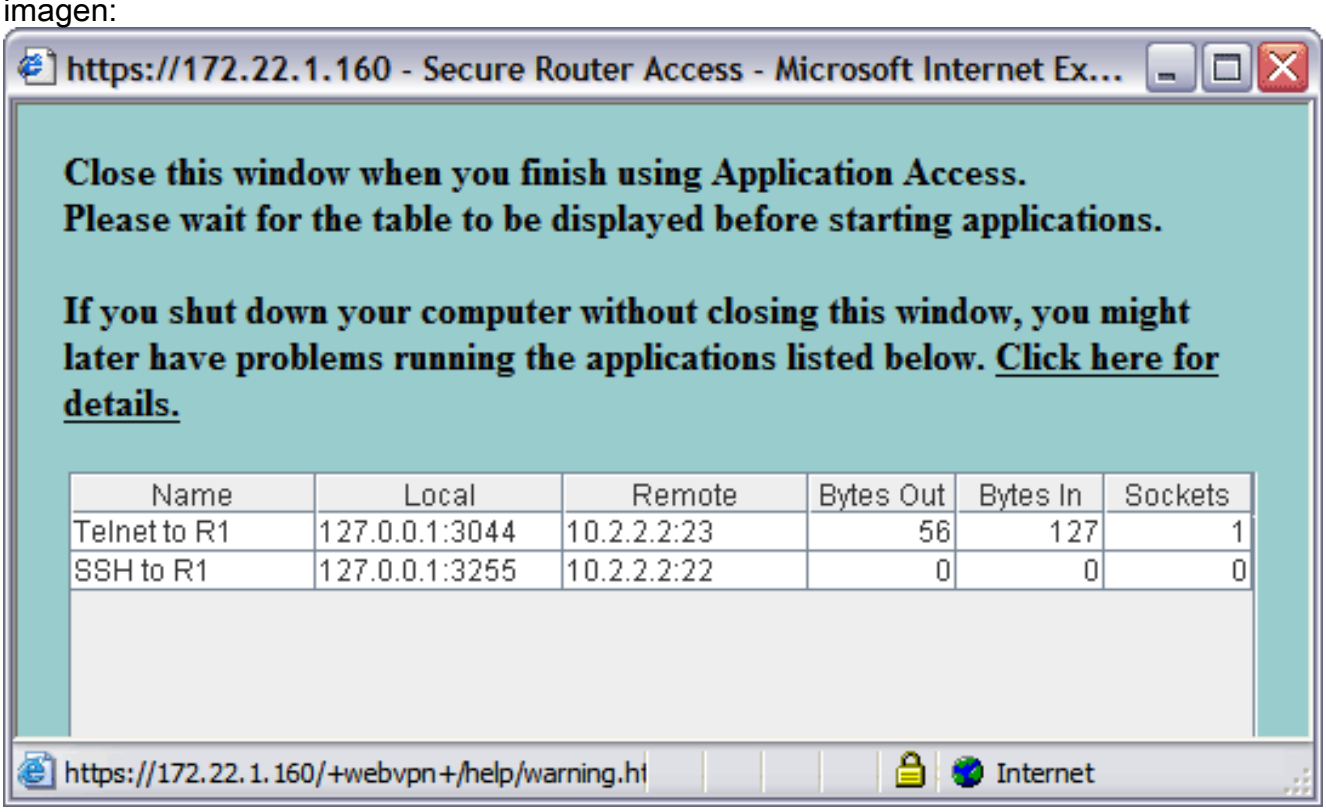


El direccionamiento y la información de puerto requeridos para acceder la aplicación aparece en la columna local. Los bytes hacia fuera y los bytes en las columnas no visualizan ninguna actividad porque la aplicación no se ha invocado ahora.

2. Utilice el prompt DOS o la otra aplicación Telnet de comenzar a una sesión telnet.
3. En el comando prompt, ingrese **telnet 127.0.0.1 3044**.**Nota:** Este comando proporciona un ejemplo de cómo acceder al puerto local visualizado en la imagen de la página web del servicio del WebVPN en este documento. *El comando no incluye los dos puntos (:).* Teclee el comando según lo descrito en este documento.El ASA recibe el comando sobre la sesión segura, y porque salva una correspondencia de la información, el ASA sabe inmediatamente para abrir la sesión de Telnet segura en el dispositivo
asociado.

Una vez que usted ingresa su nombre de usuario y contraseña, el acceso al dispositivo es completo.

4. Para verificar el acceso al dispositivo, marque los bytes hacia fuera y los bytes en las columnas tal y como se muestra en de 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.

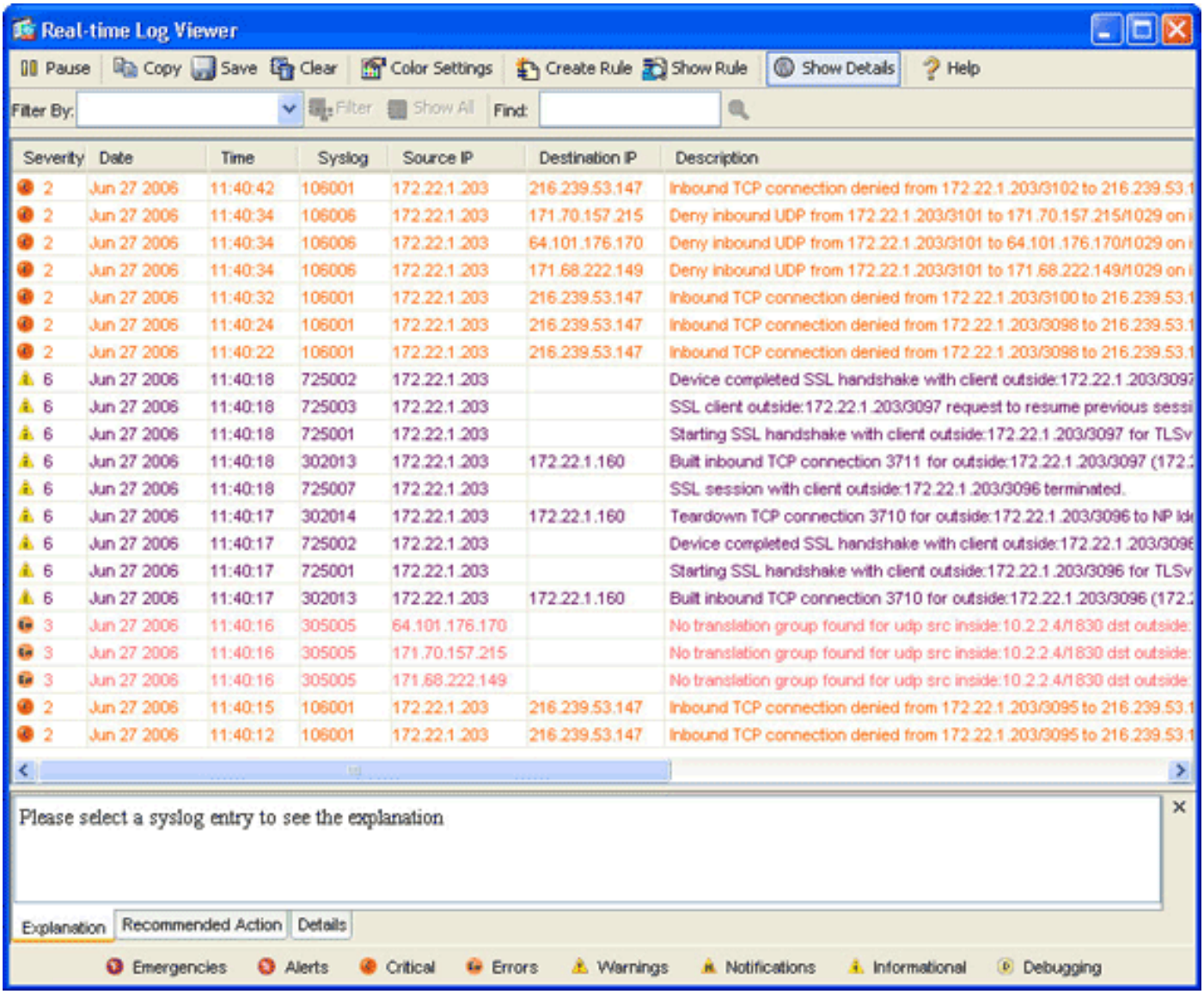
Nota: La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

Use esta sección para resolver problemas de configuración.

¿Es el contacto SSL de proceso completa?

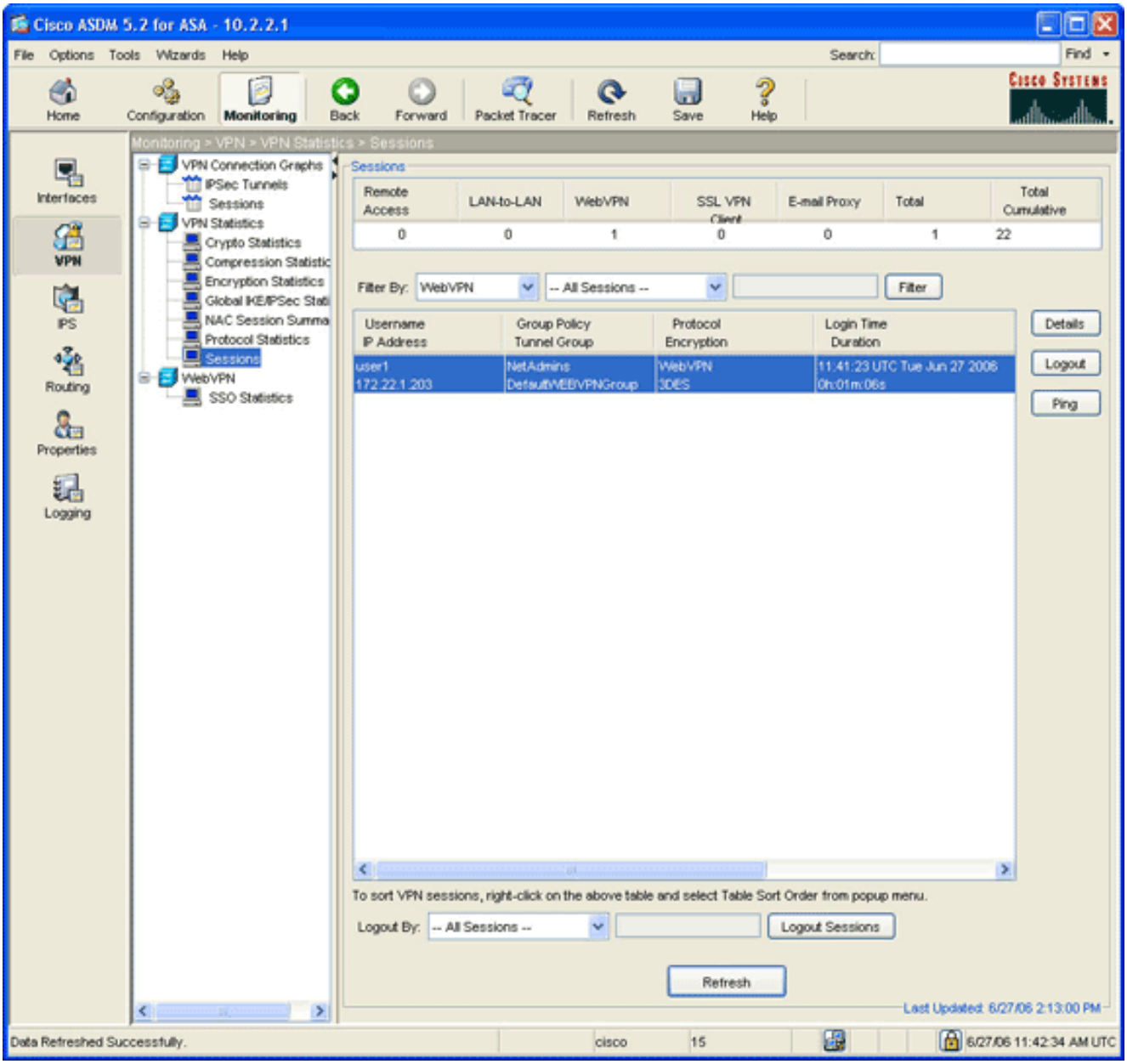
Una vez que usted conecta con el ASA, marque si el registro en tiempo real muestra la realización del contacto SSL.



¿Es el cliente “liviano” SSL VPN funcional?

Para verificar que el cliente “liviano” SSL VPN sea funcional, complete estos pasos:

1. Haga clic la **supervisión**, y después haga clic el **VPN**.
2. Amplíe los **VPN statistics (Estadísticas de la VPN)**, y haga clic las **sesiones**.Su sesión de cliente “liviano” SSL VPN debe aparecer en la lista de las sesiones. Esté seguro de filtrar por el WebVPN tal y como se muestra en de 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 su dispositivo de Cisco. Antes de que utilice los **comandos debug**, consulte Información Importante sobre los Comandos Debug.

Información Relacionada

- Clientless SSL VPN (WebVPN) en el ejemplo de configuración 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