Ejemplo de Configuración de ASA con WebVPN y Single Sign-on con ASDM y NTLMv1

Contenido

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) para pasar automáticamente credenciales de login de usuario WebVPN, así como la autenticación secundaria, a los servidores que requieren validación de login adicional respecto a Windows Active Directory que ejecuta NT LAN Manager versión 1 (NTLMv1). Esta función se conoce como Inicio único de sesión (SSO). Proporciona a los links configurados para un grupo WebVPN específico la capacidad de pasar esta información de autenticación de usuarios, eliminando así las indicaciones de autenticación múltiples. Esta función también se puede utilizar en el nivel global o en el nivel de configuración de usuarios.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Asegúrese de que el NTLMv1 y los permisos de Windows para los usuarios de VPN de la blanco estén configurados. Consulte su documentación de Microsoft para más información sobre los derechos de acceso del Dominio de Windows.

Componentes Utilizados

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

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Servicios de Internet Information Server de Microsoft (IIS)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

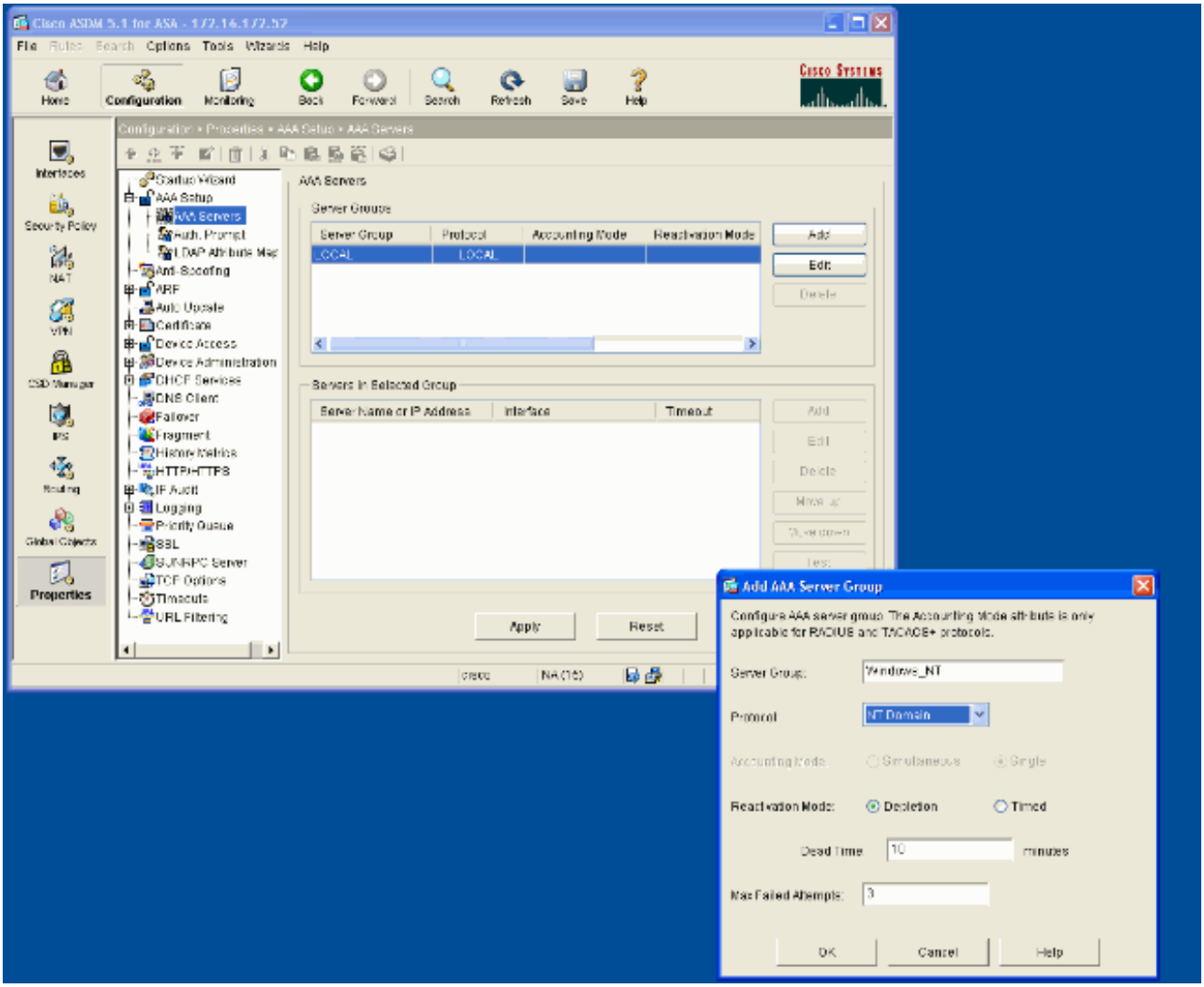
En esta sección, le presentan con la información para configurar el ASA como servidor WebVPN con el SSO.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

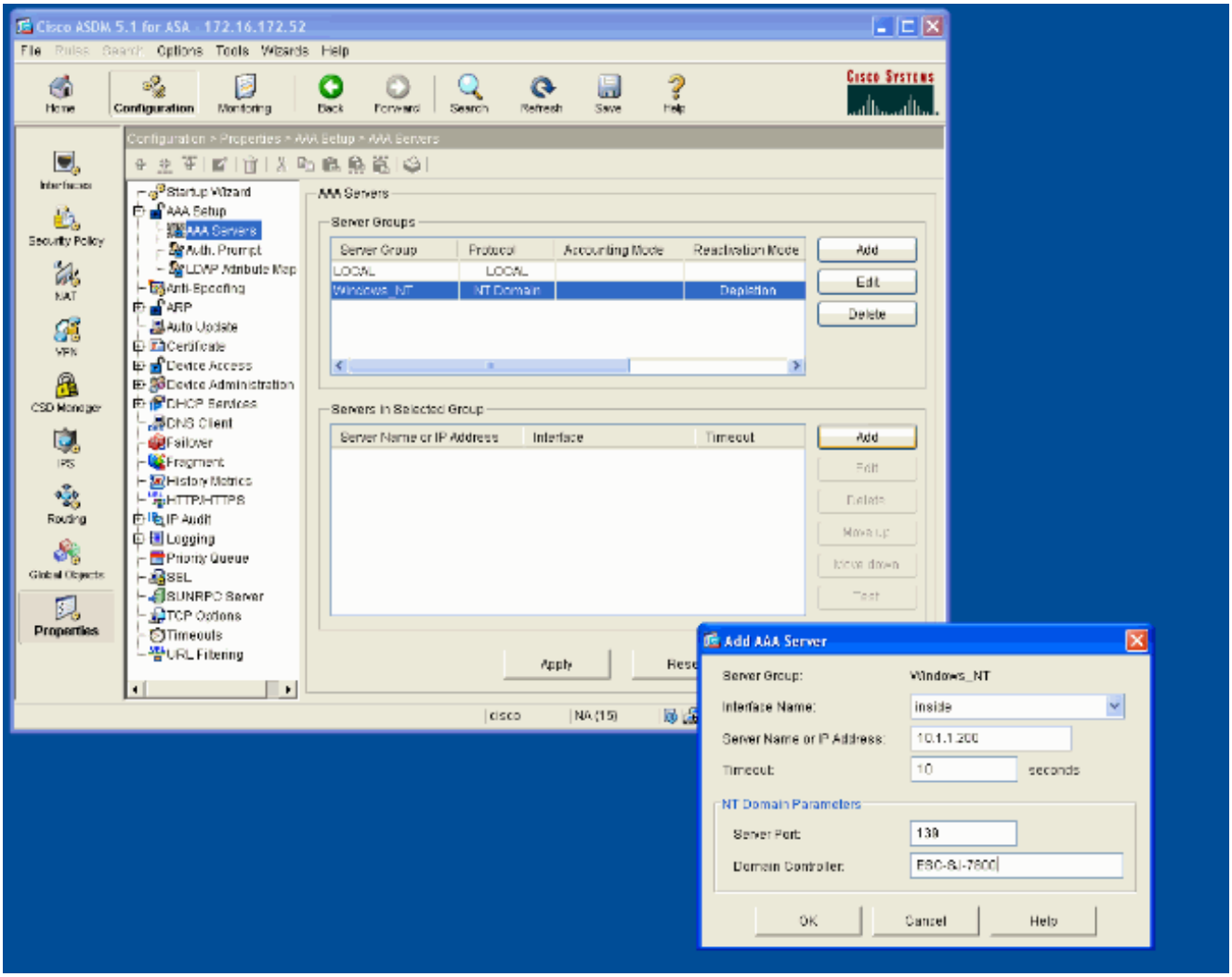
Agregue a un servidor de AAA para la autenticación del Dominio de Windows

Complete estos pasos para configurar el ASA para utilizar un controlador de dominio para la autenticación.

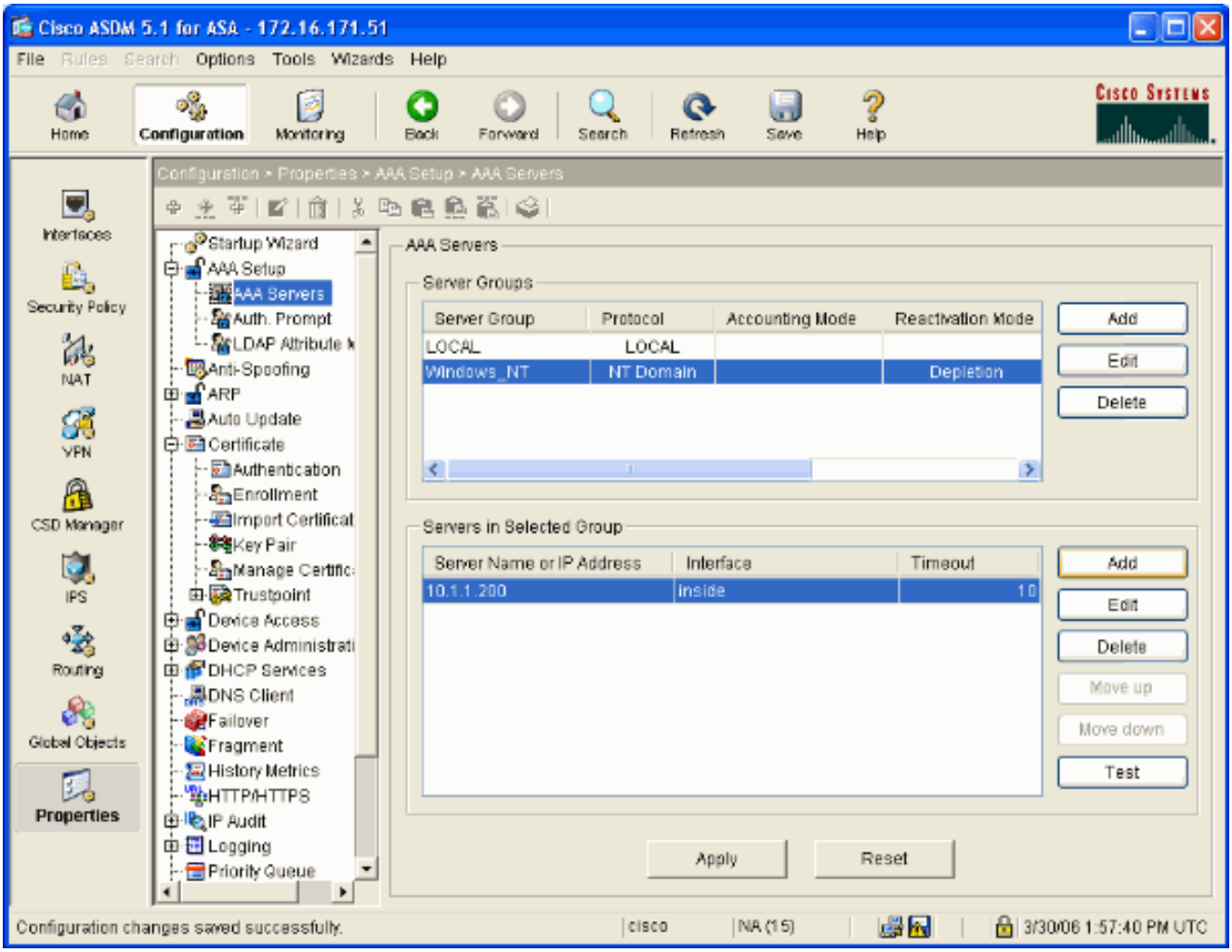
1. Seleccione la **configuración > las propiedades >AAA ponen >AAA los servidores** y el haga click en Add Proporcione un nombre para el grupo de servidores, tal como Windows_NT, y elija el **dominio de NT** como el
protocolo.



2. Agregue a un Servidor Windows.Seleccione el grupo creado recientemente y el haga click en Add Seleccione la interfaz donde se localiza el servidor y ingrese el IP Address y el nombre del controlador de dominio. Esté seguro que el nombre del controlador de dominio está ingresado en todas las letras mayúsculas. Haga Click en OK cuando le hacen.



Esta ventana muestra la configuración AAA completada:

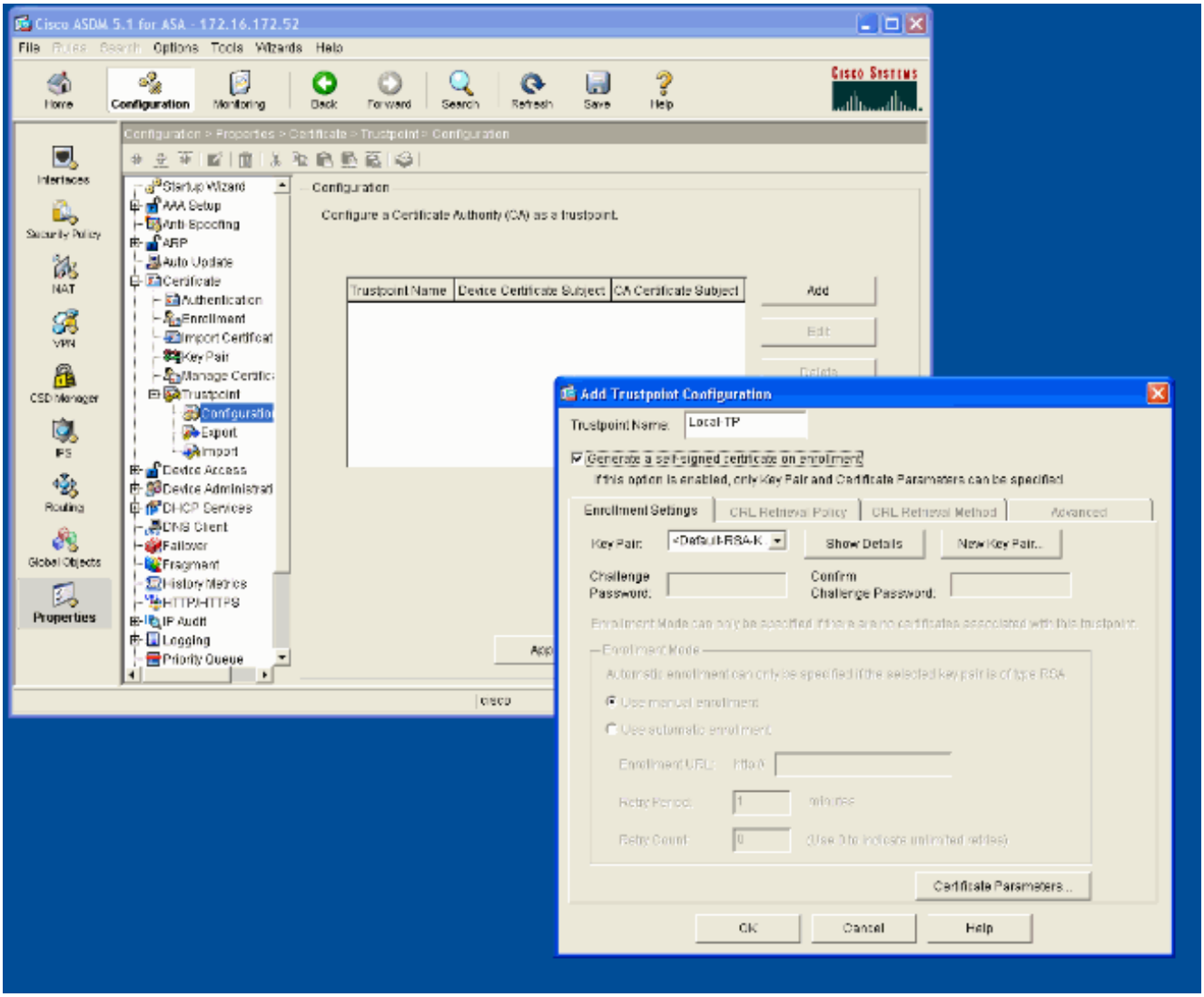


Cree un certificado autofirmado

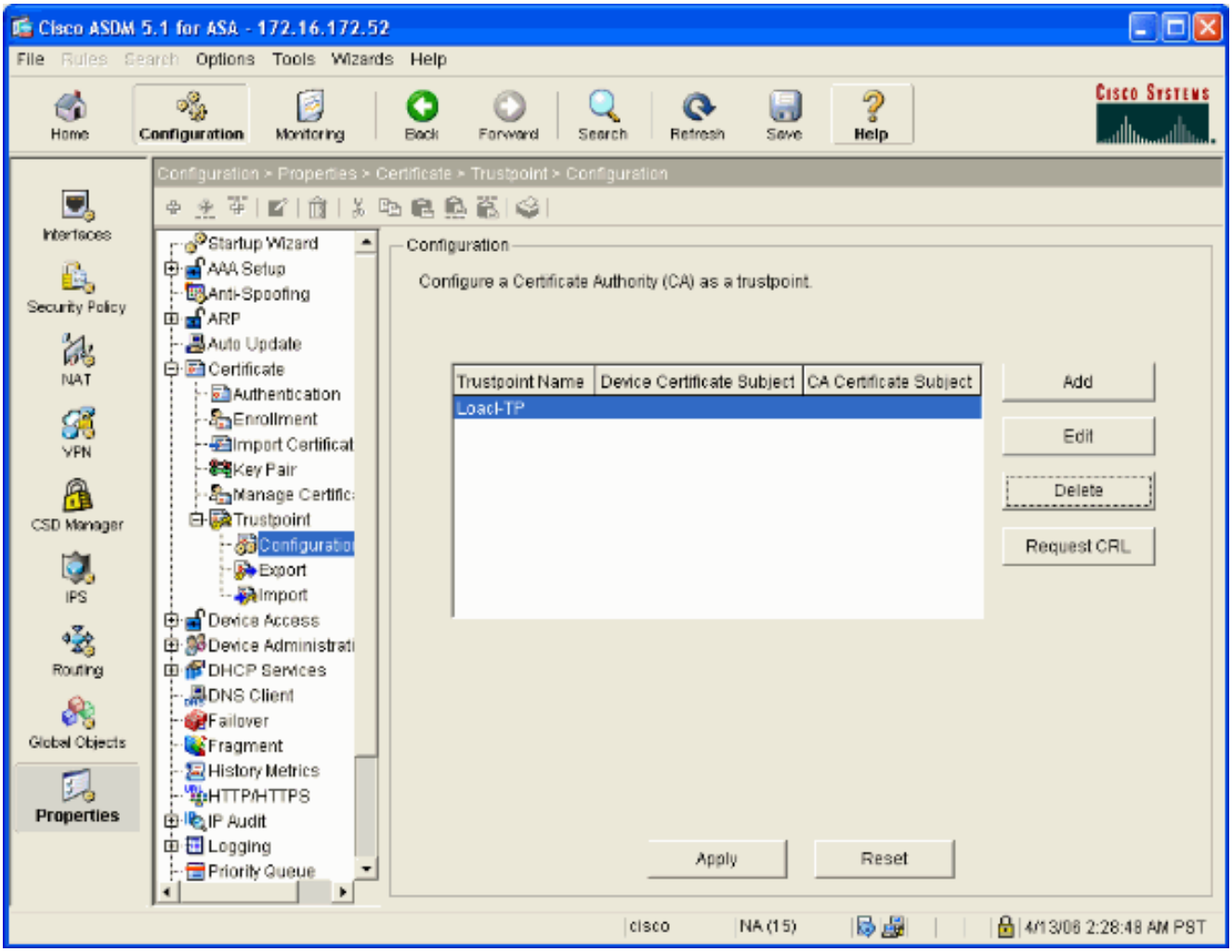
Complete estos pasos para configurar el ASA para utilizar un certificado autofirmado.

Nota: En este ejemplo un certificado autofirmado se utiliza para la simplicidad. Para otras opciones de la inscripción del certificado, tales como alistar con un Certificate Authority externo, refiera a configurar los Certificados.

1. Seleccione la **configuración > las propiedades > el certificado > el trustpoint > la configuración** y el haga click en Add
2. En la ventana que aparece ingrese un nombre del trustpoint tal como Local-TP y control **generan un certificado autofirmado en la inscripción**. Las otras opciones se pueden dejar con sus configuraciones predeterminadas. Haga Click en OK cuando le hacen.



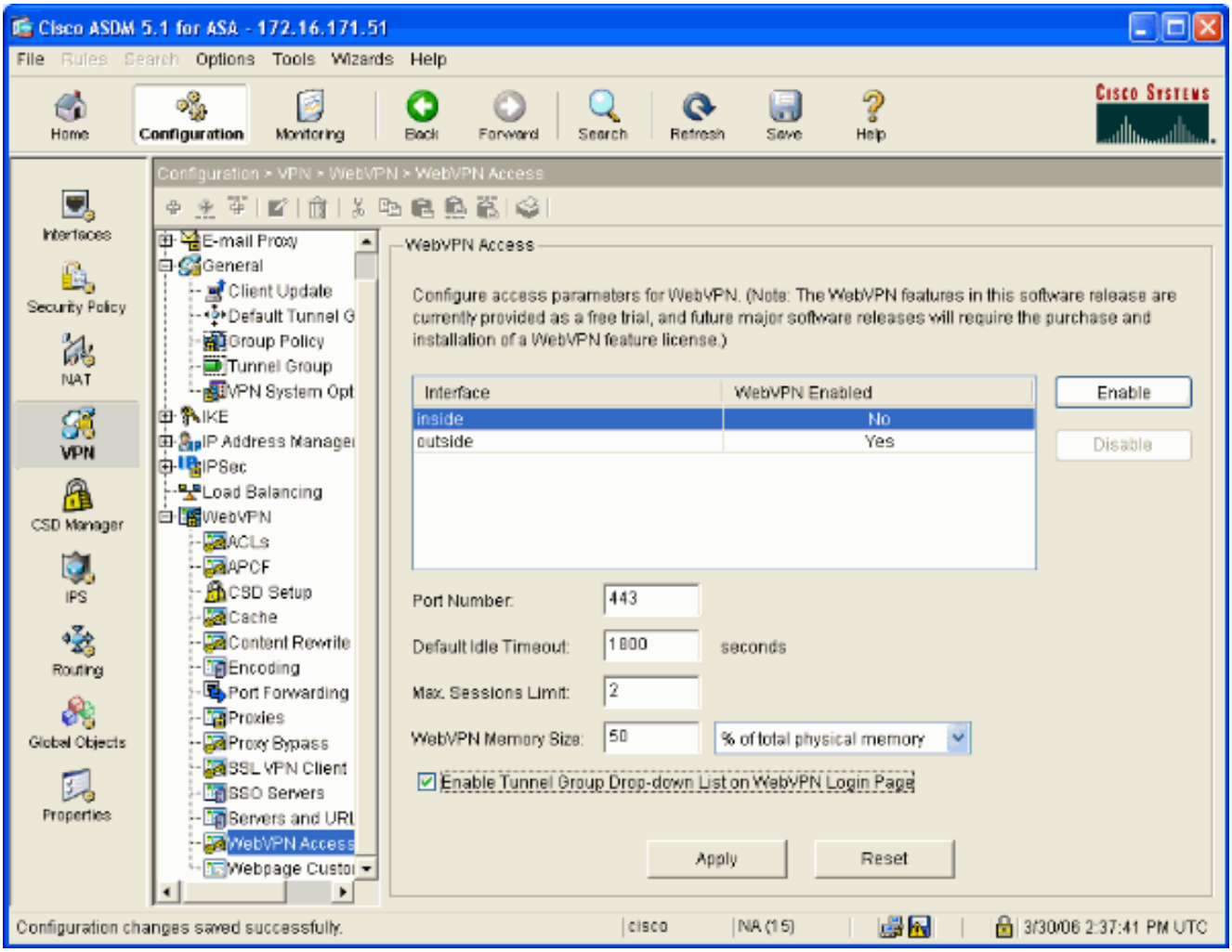
Esta ventana muestra la configuración completada del trustpoint:



WebVPN del permiso en la interfaz exterior

Complete estos pasos para permitir que los usuarios fuera de su red conecten usando el WebVPN.

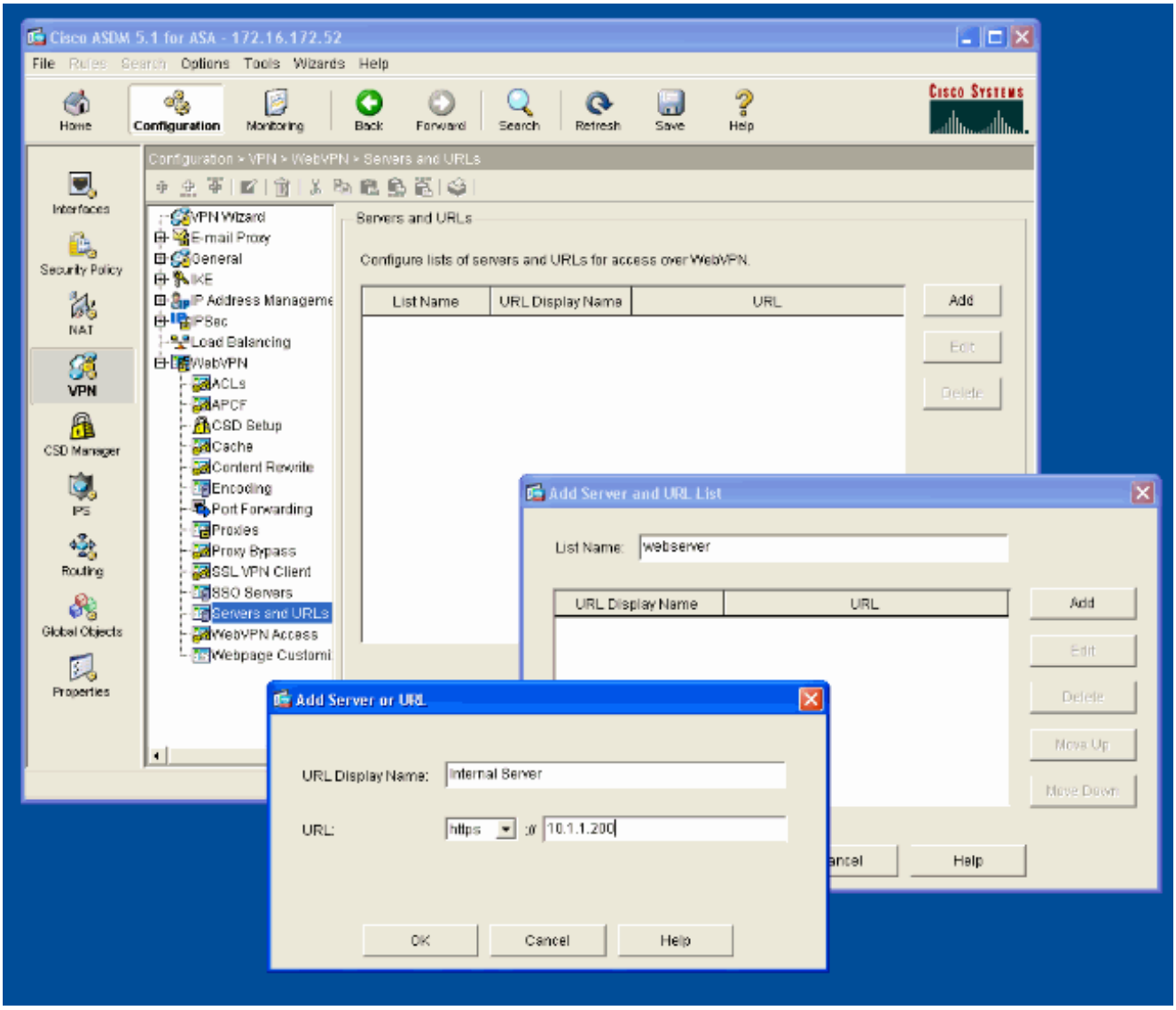
1. Seleccione la **configuración > el VPN > el WebVPN > el acceso del WebVPN**.
2. Seleccione la interfaz deseada, haga clic el **permiso**, y marque la **lista desplegable del grupo de túnel del permiso en la página de registro del WebVPN.Nota:** Si la misma interfaz se utiliza para el WebVPN y el acceso del ASDM, usted debe cambiar el puerto predeterminado para el acceso del ASDM del puerto 80 a un nuevo puerto tal como 8080. Esto se hace bajo la **configuración > las propiedades > acceso del dispositivo > HTTPS/ASDM.Nota:** Usted puede reorientar automáticamente a un usuario al puerto 443 en caso que un usuario navegue a **http:// <ip_address>** en vez de **https:// <ip_address>**. Seleccione la **configuración > las propiedades > el HTTP/HTTPS**, elija la interfaz deseada, el tecleo **edita** y selecto **reoriente el HTTP al HTTPS**.



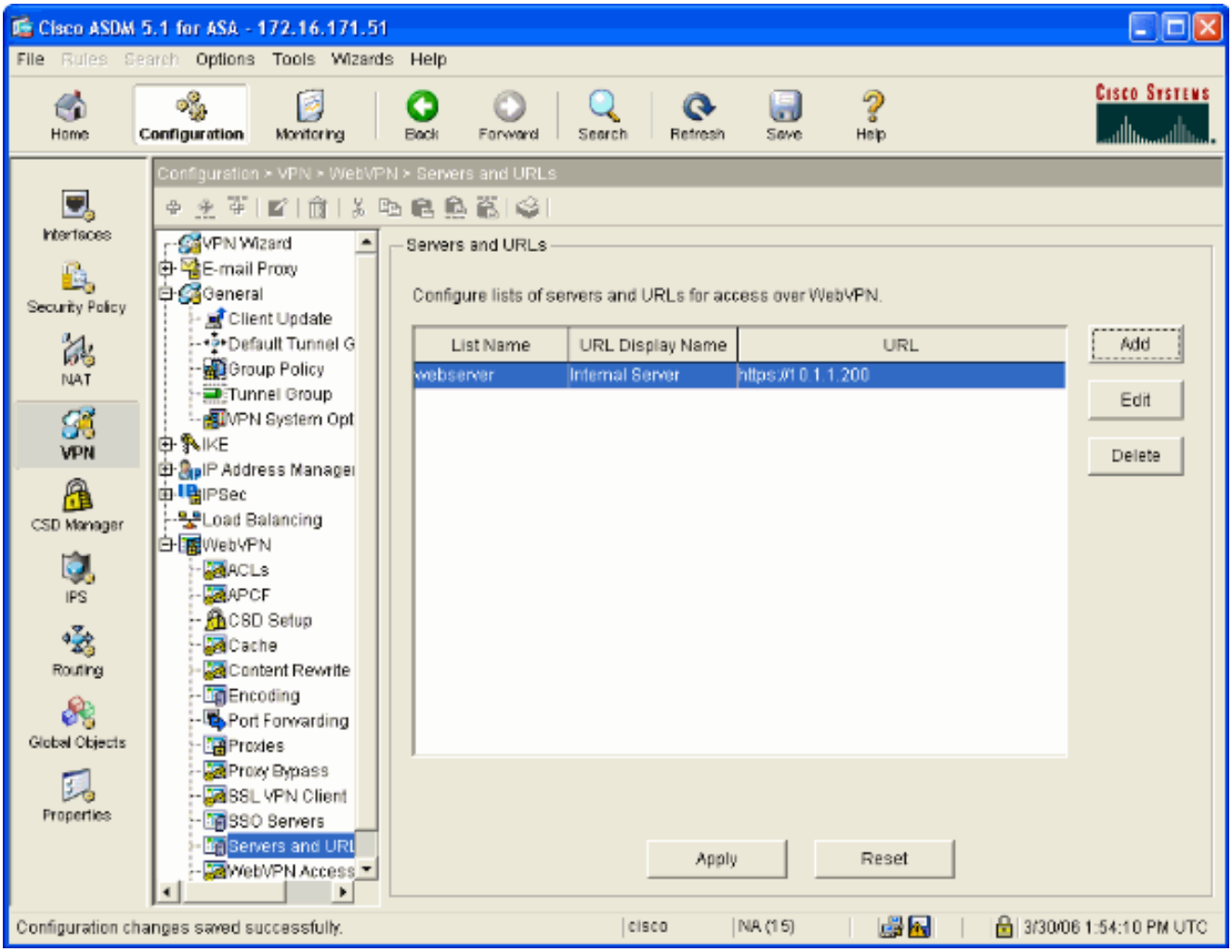
Configure una lista url para sus servidores internos

Complete estos pasos para crear una lista que contenga los servidores para los cuales usted quiere conceder su acceso de usuarios de WebVPN.

1. Seleccione la **configuración > VPN > WebVPN > los servidores y los URL** y haga click en Add
2. Ingrese un nombre para la lista url. Este nombre no es visible a los usuarios finales. Haga clic en Add (Agregar).
3. Ingrese el nombre de la visualización URL pues debe ser visualizado a los usuarios. Ingrese la información del URL del servidor. Éste debe ser cómo usted accede normalmente el servidor.



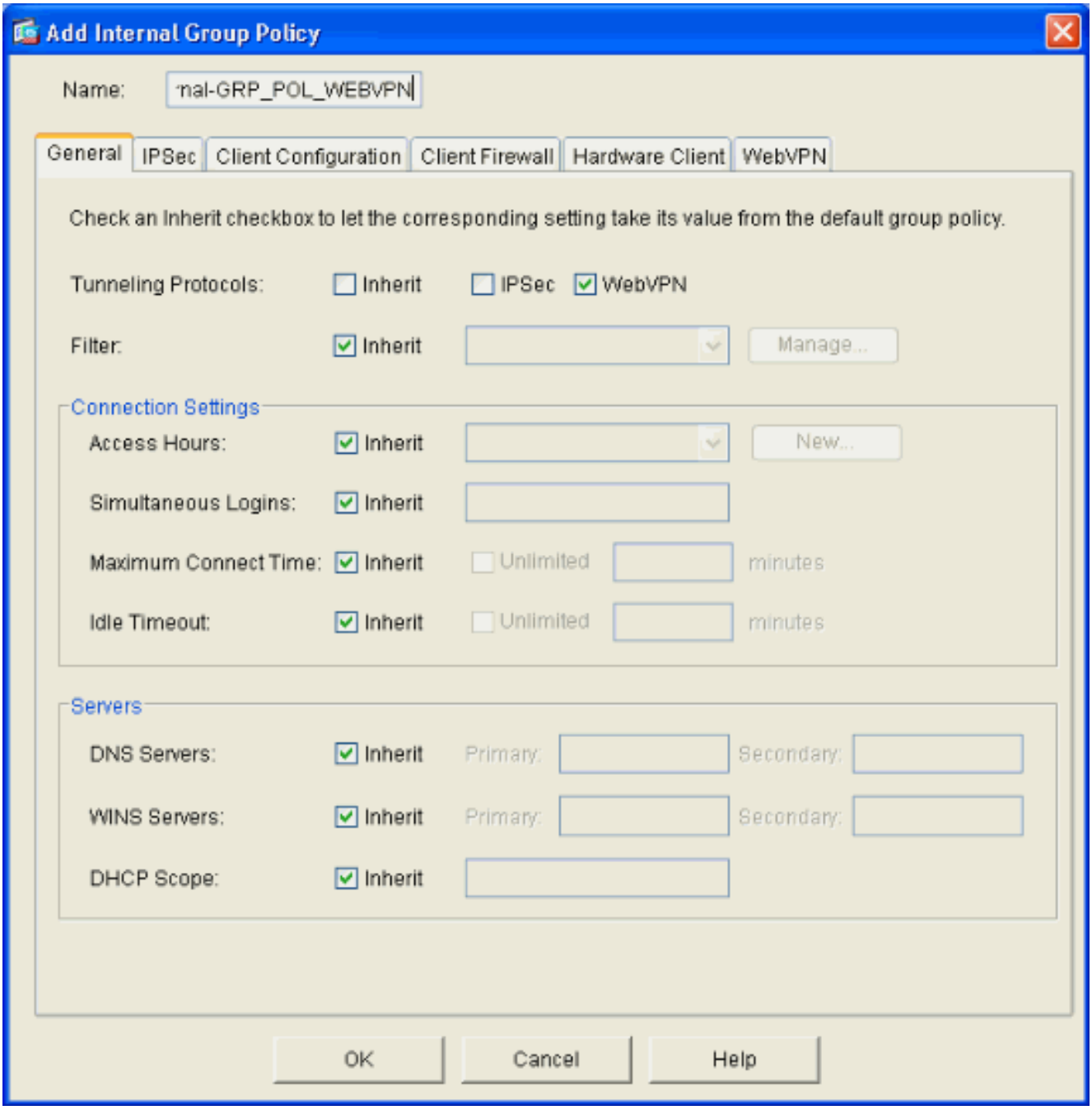
4. El Haga Click en OK, **AUTORIZACIÓN**, y entonces **se aplica**.



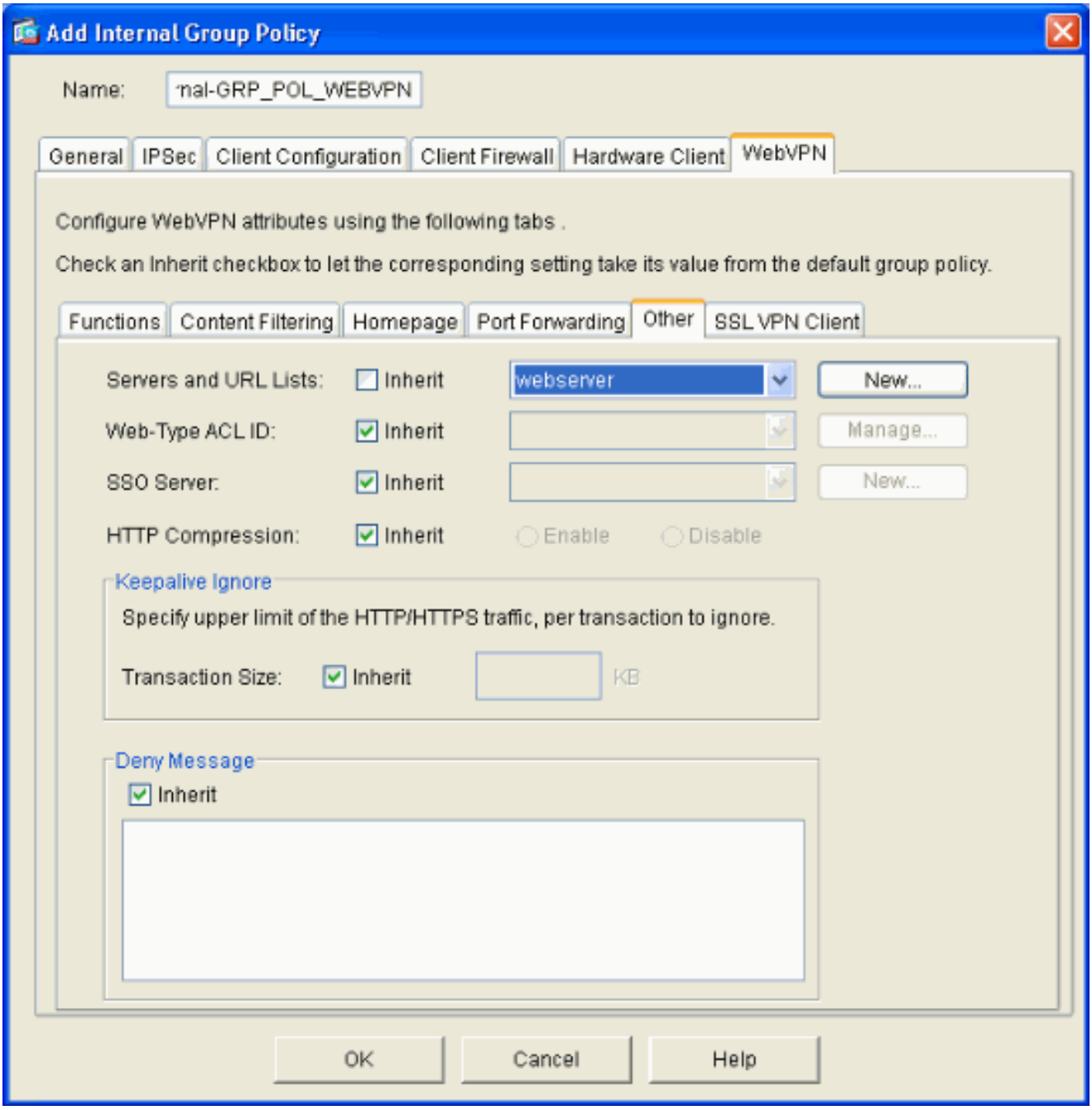
Configure un Internal group policy (política grupal interna)

Complete estos pasos para configurar una directiva del grupo para sus usuarios de WebVPN.

1. Seleccione la **configuración > el VPN > la directiva del general > del grupo**, el tecleo **agrega**, y selecciona el **Internal group policy (política grupal interna)**.
2. En la ficha general, especifique un nombre de la directiva, tal como Internal-Group_POL_WEBVPN. Entonces desmarque **heredan** al lado de los protocolos de túneles y del **WebVPN del**
   control.



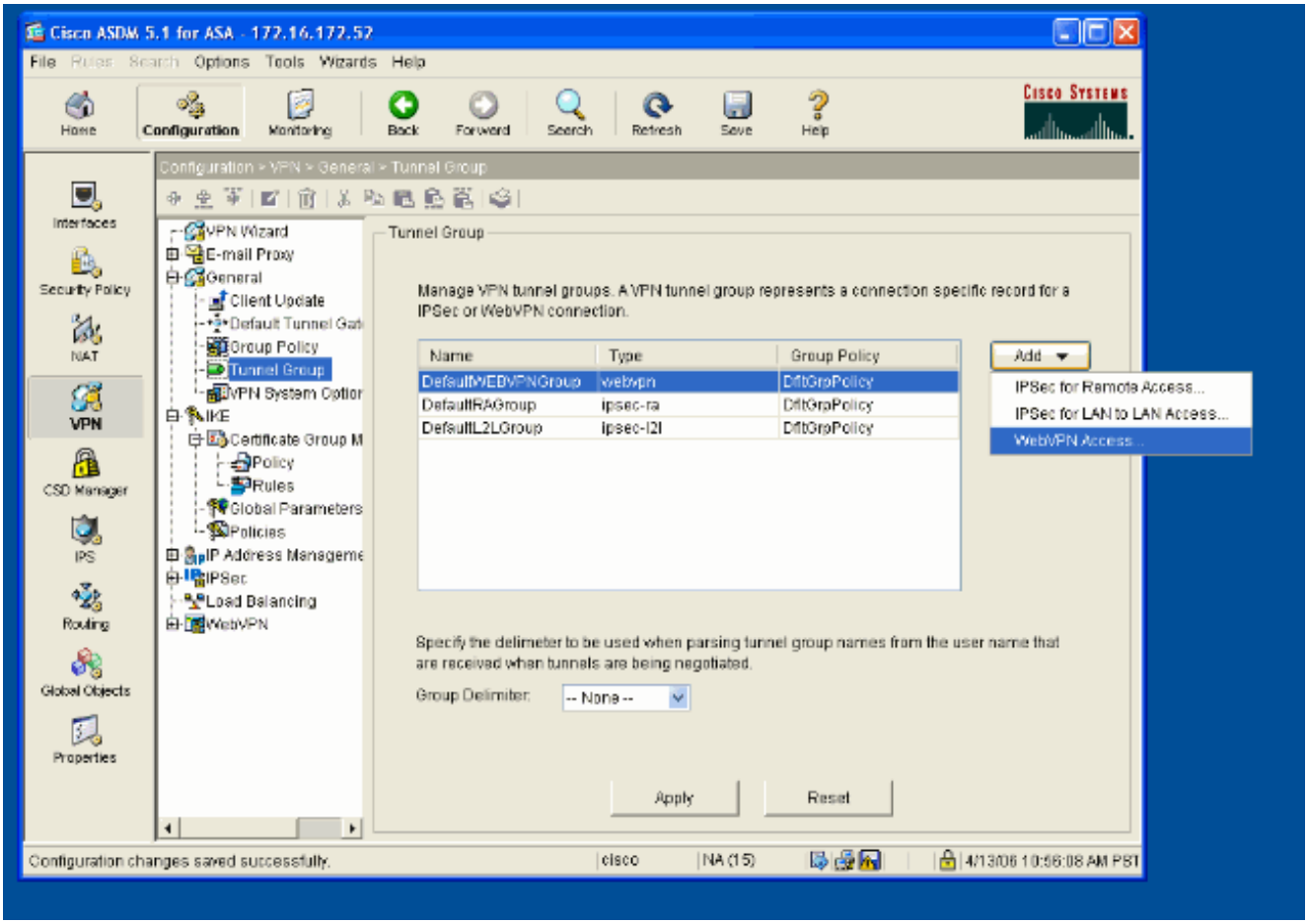
3. En la lengueta del WebVPN seleccione la **otra sub-**lengueta. Desmarque **heredan** al lado de los servidores y de las listas url y seleccionan la lista url que usted configuró de la lista desplegable. Haga Click en OK cuando le
hacen.



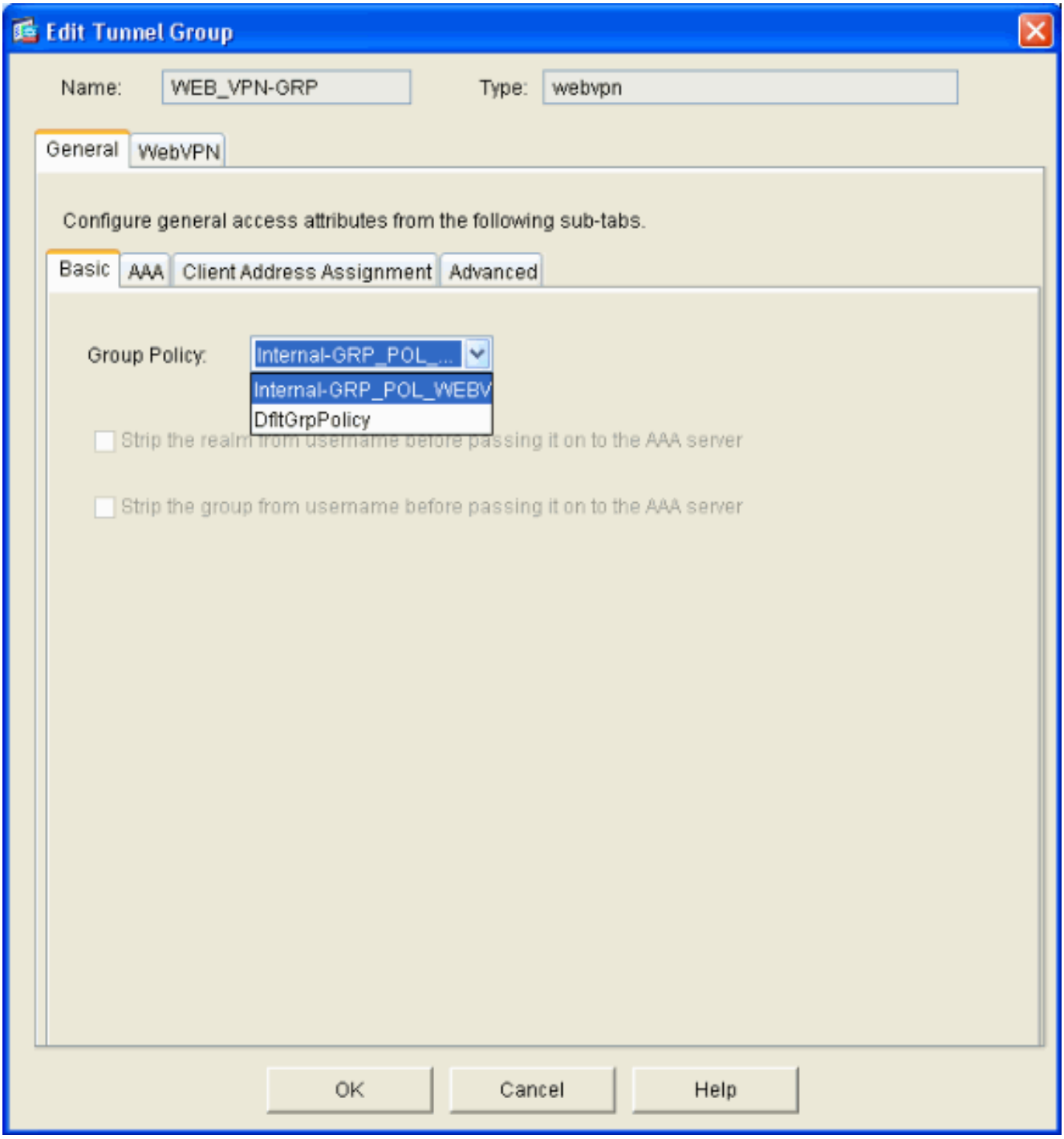
Configure a un grupo de túnel

Complete estos pasos para configurar a un grupo de túnel para sus usuarios de WebVPN.

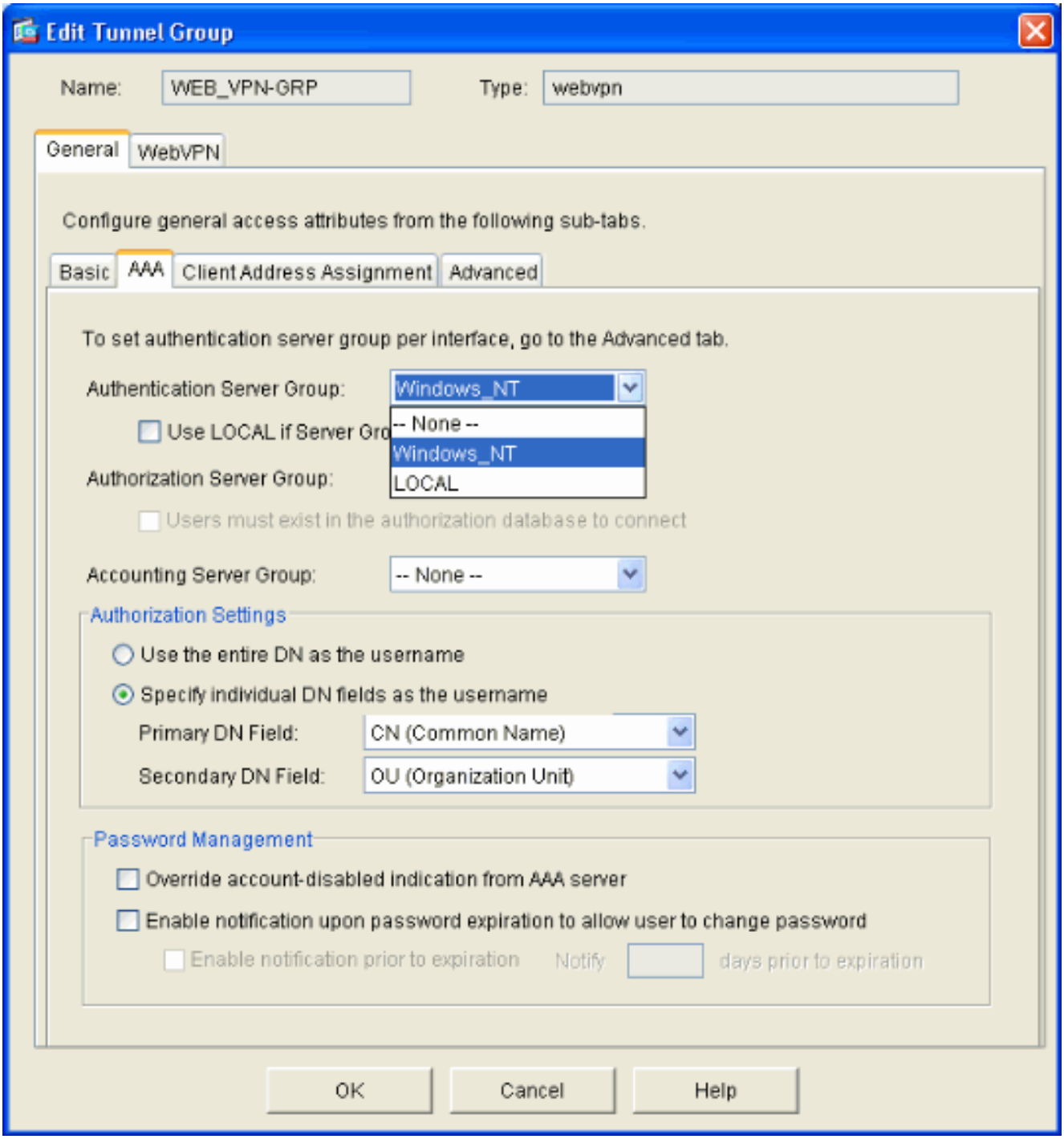
1. Seleccione la **configuración > el VPN > el general > al grupo de túnel**, el tecleo **agrega** y **acceso** selecto del **WebVPN...**



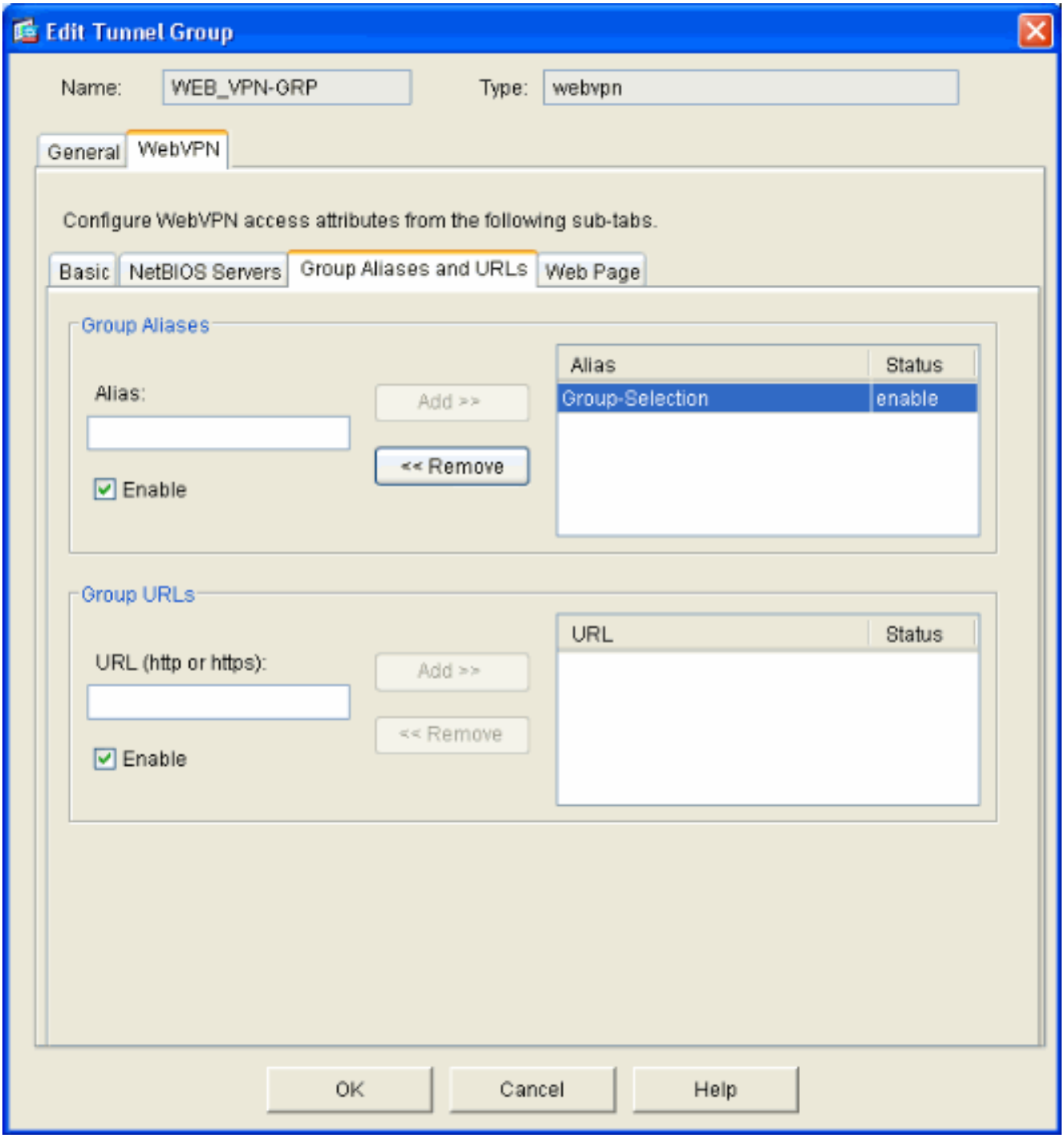
2. Ingrese un nombre para el grupo de túnel, tal como WEB_VPN-GRP. En la lengueta básica seleccione la directiva del grupo que usted creó y verifiquela que el Tipo de grupo es **webvpn**.



3. Vaya a la lengueta AAA.Para el grupo de servidor de autenticación, elija al grupo que usted configuró para habilitar la autenticación del NTLMv1 con su controlador de dominio.**Opcional:** Marque el **LOCAL del uso si el grupo de servidores no puede** habilitar el uso de la base de datos de usuarios locales en caso que el grupo configurado AAA falle. Esto puede ayudarle a resolver problemas en otro
momento.



4. Vaya a la lengueta del WebVPN y después vaya a la sub-lengueta de los **alias y URL del grupo**.
5. Ingrese un alias bajo los alias y el haga click en Add del grupo Este alias aparece en la lista desplegable presentada a los usuarios de WebVPN en el login.



6. Haga clic en OK y en **Apply**.

Auto-anuncio del comienzo de las emisiones de la configuración para un servidor

Switch a la línea de comando para habilitar el SSO para sus servidores internos.

Nota: Este paso no se puede completar en el ASDM y debe ser realizado usando la línea de comando. Refiera a acceder la interfaz de la línea de comandos para más información.

Utilice el **comando auto-signon** de especificar al recurso de red, tal como un servidor, que usted quiere dar su acceso de usuarios a. Una dirección IP del servidor único se configura aquí, pero un rango de red tal como **10.1.1.0 /24** puede también ser especificado. Refiera al comando auto-signon para más información.

```
ASA>enable ASA#configure terminal ASA(config)#webvpn ASA(config-webpvn)#auto-signon allow ip
10.1.1.200 255.255.255.255 auth-type ntlm ASA(config-webvpn)#quit ASA(config)#exit ASA#write
```

memory

En esta salida de ejemplo, configuran al **comando auto-signon** para el WebVPN global. Este comando se puede también utilizar en el modo de la configuración de grupo del WebVPN o el modo de configuración del nombre de usuario de WebVPN. El uso de este comando en el modo de la configuración de grupo del WebVPN lo limita a un grupo determinado. Asimismo, el uso de este comando en el modo de configuración del nombre de usuario de WebVPN lo limita a un usuario individual. Refiera al comando auto-signon para más información.

Configuración final de ASA

Este documento usa esta configuración:

Versión de ASA 7.1(1)

```
ASA#show running-config : Saved : ASA Version 7.1(1) !
terminal width 200 hostname ASA domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface GigabitEthernet0/0 nameif outside security-
level 0 ip address 172.16.171.51 255.255.255.0 !
interface GigabitEthernet0/1 nameif inside security-
level 100 ip address 10.1.1.1 255.255.255.0 ! interface
GigabitEthernet0/2 shutdown no nameif no security-level
no ip address ! interface GigabitEthernet0/3 shutdown no
nameif no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
cisco.com pager lines 24 mtu inside 1500 mtu outside
1500 no failover asdm image disk0:/asdm512.bin no asdm
history enable arp timeout 14400 route outside 0.0.0.0
0.0.0.0 172.16.171.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute !---
AAA server configuration aaa-server Windows_NT protocol
nt aaa-server Windows_NT host 10.1.1.200 nt-auth-domain-
controller ESC-SJ-7800 !--- Internal group policy
configuration group-policy Internal-GRP_POL_WEBVPN
internal group-policy Internal-GRP_POL_WEBVPN attributes
vpn-tunnel-protocol webvpn webvpn url-list value
webserver username cisco password Q/odgwmtmVIw4Dcm
encrypted privilege 15 aaa authentication http console
LOCAL aaa authentication ssh console LOCAL aaa
authentication enable console LOCAL http server enable
8181 http 0.0.0.0 0.0.0.0 outside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !---
Trustpoint/certificate configuration crypto ca
trustpoint Local-TP enrollment self crl configure crypto
ca certificate chain Local-TP certificate 31 308201b0
30820119 a0030201 02020131 300d0609 2a864886 f70d0101
04050030 1e311c30 1a06092a 864886f7 0d010902 160d4153
412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334
3930345a 170d3136 30333237 31333439 30345a30 1e311c30
1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e
636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d
00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a
1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434
561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404
9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17
```

```
68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3
776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06
092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544
59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d
3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b
af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de
775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a
f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c
quit !--- Tunnel group configuration tunnel-group
WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP
general-attributes authentication-server-group
Windows_NT default-group-policy Internal-GRP_POL_WEBVPN
tunnel-group WEB_VPN-GRP webvpn-attributes group-alias
Group-Selection enable telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
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 Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6 : end
```

Verificación

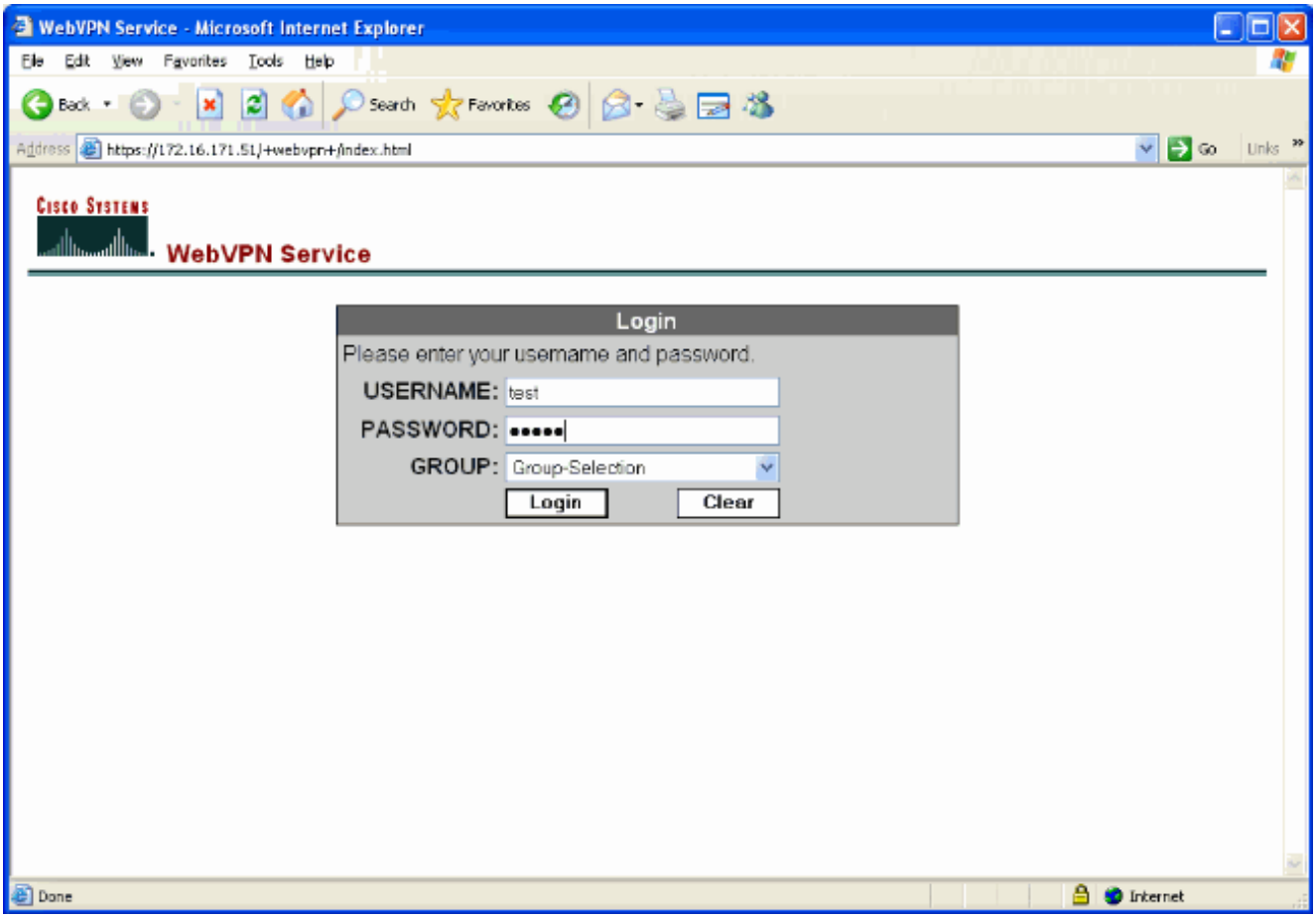
Use esta sección para confirmar que su configuración funciona correctamente.

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.

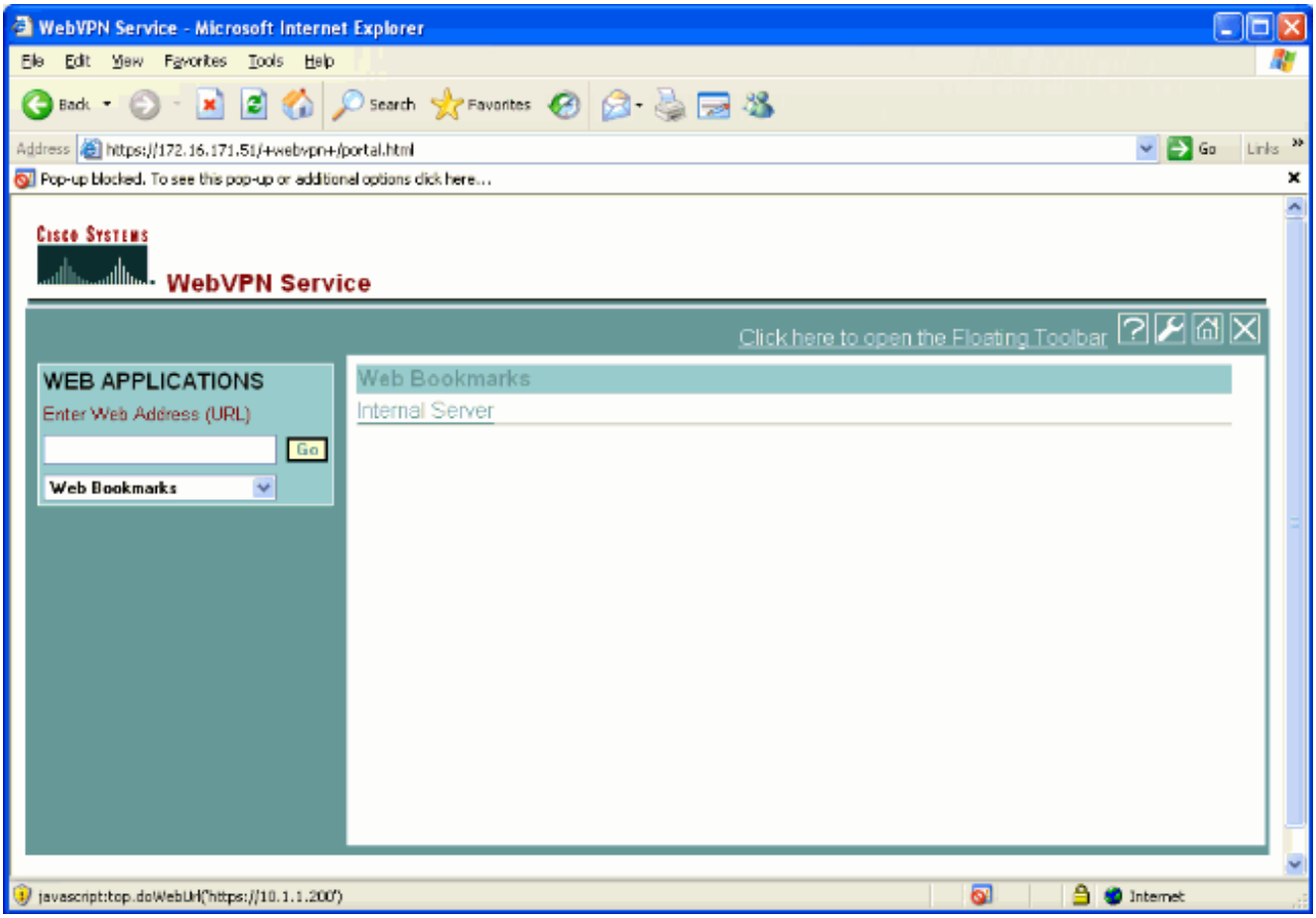
Pruebe un login del WebVPN

Inicie sesión como usuario para probar su configuración.

1. Intente iniciar sesión al ASA con la información del usuario de su dominio de NT. Seleccione al grupo alias configurado en el paso 5 debajo configuran a un grupo de túnel.

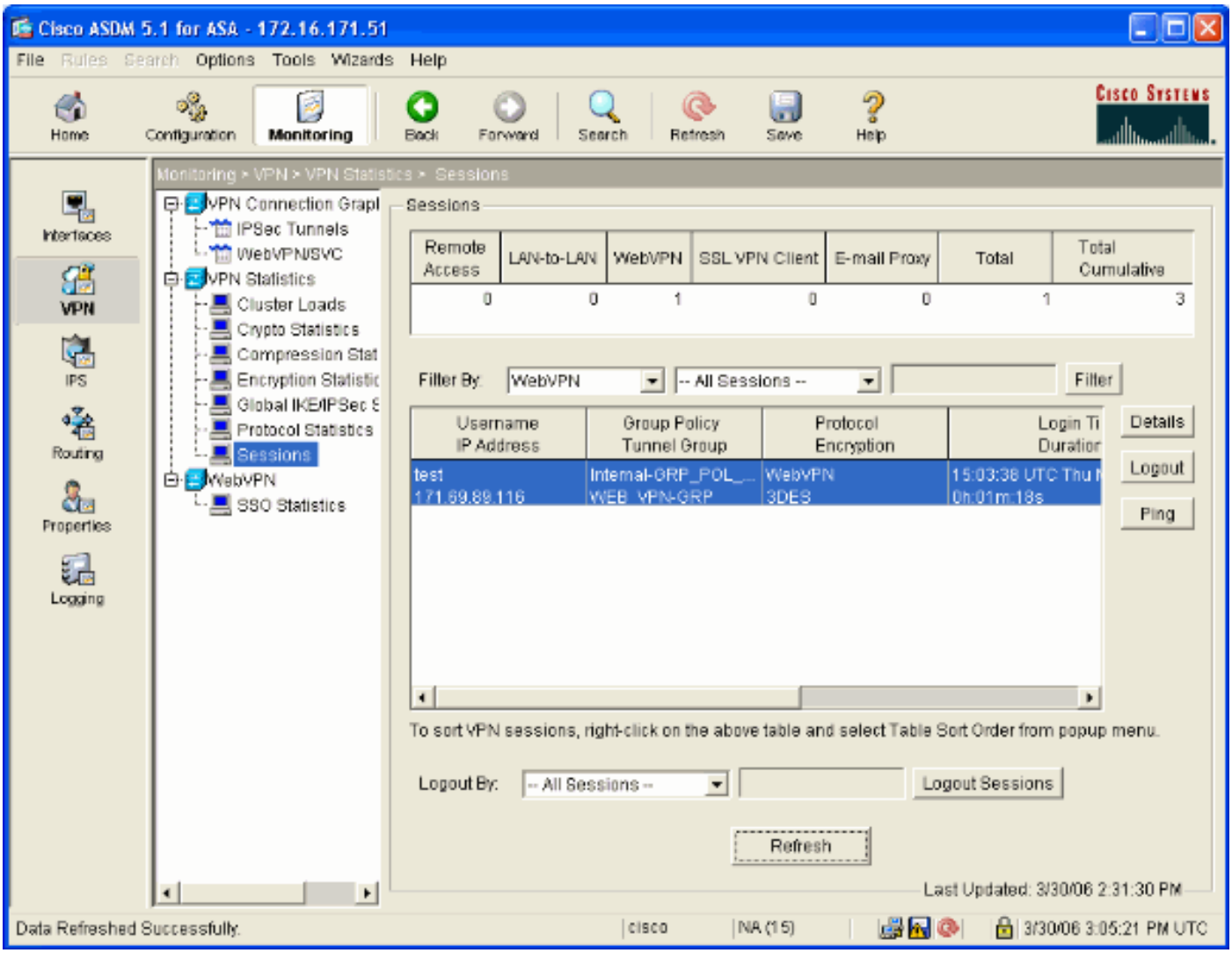


2. Busque los links configurados a los servidores internos. Haga clic en el link para verificar.



Sesiones de monitoreo

Seleccione la **supervisión > el VPN > los VPN statistics (Estadísticas de la VPN) > las sesiones** y busque a una sesión WebVPN que pertenezca al grupo configurado en este documento.



Haga el debug de a una sesión WebVPN

Esta salida es un debug de la muestra de una sesión WebVPN exitosa.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

```
ASA#debug webvpn 255 INFO: debug webvpn enabled at level 255 ASA# ASA#
webvpn_portal.c:ewaFormServe_webvpn_login[1570] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286] WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782] !--- Begin AAA WebVPN: calling AAA with
ewsContext (78986968) and nh (78960800)! WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422] WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095] WebVPN: user: (test) authenticated. !--- End
AAA webvpn_auth.c:http_webvpn_auth_accept[2093] webvpn_session.c:http_webvpn_create_session[159]
webvpn_session.c:http_webvpn_find_session[136] WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136] webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202] traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421] webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
```

```
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. !--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Si la casilla desplegable del grupo no está presente en la página de registro del WebVPN, esté seguro que usted ha completado el paso 2 bajo el WebVPN del permiso en la interfaz exterior y el paso 5 debajo configura a un grupo de túnel. Si estos pasos no se completan y el descenso-abajo falta, la autenticación baja bajo grupo predeterminado y falla probablemente.
- Aunque usted no pueda asignar los derechos de acceso al usuario en el ASDM o en el ASA, usted puede restringir a los usuarios con los derechos de acceso de Microsoft Windows en su controlador de dominio. Agregue los permisos necesarios del grupo de NT para la página web que el usuario autentica a. Una vez los registros de usuario en el WebVPN con los permisos del grupo, acceso a las páginas especificadas se conceden o se niegan por consiguiente. El ASA actúa solamente como host de la autenticación de representación en nombre del controlador de dominio y todas las comunicaciones aquí son NTLMv1.
- Usted no puede configurar el SSO para Sharepoint sobre el WebVPN porque el servidor de Sharepoint no soporta la autenticación basada las formas. Como consecuencia, los marcadores con el poste o el procedimiento plug-in del poste son no corresponde aquí.

Información Relacionada

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Soporte Técnico y Documentación - Cisco Systems**