Thin-Client SSL VPN (WebVPN) on ASA with ASDM Configuration Example

Contents

Introduction

Thin-Client SSL VPN technology allows secure access for some applications that have static ports, such as Telnet(23), SSH(22), POP3(110), IMAP4(143) and SMTP(25). You can use the Thin-Client SSL VPN as a user-driven application, policy-driven application, or both. That is, you can configure access on a user by user basis or you can create Group Policies in which you add one or more users.

- **Clientless SSL VPN (WebVPN)**—Provides a remote client that requires an SSL-enabled Web browser to access HTTP or HTTPS Web servers on a corporate local-area network (LAN). In addition, clientless SSL VPN provides access for Windows file browsing through the Common Internet File System (CIFS) protocol. Outlook Web Access (OWA) is an example of HTTP access.Refer to Clientless SSL VPN (WebVPN) on ASA Configuration Example in order to learn more about the Clientless SSL VPN.

- **Thin-Client SSL VPN (Port Forwarding)**—Provides a remote client that downloads a small Java-based applet and allows secure access for Transmission Control Protocol (TCP) applications that use static port numbers. Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), secure shell (ssh), and Telnet are examples of secure access. Because files on the local machine change, users must have local administrative privileges to use this method. This method of SSL VPN does not work with applications that use dynamic port assignments, such as some file transfer protocol (FTP) applications.**Note:** User Datagram Protocol (UDP) is not supported.
- **SSL VPN Client (Tunnel Mode)**—Downloads a small client to the remote workstation and allows full secure access to resources on an internal corporate network. You can download permanently the SSL VPN Client (SVC) to a remote workstation, or you can remove the client once the secure session is closed.Refer to SSL VPN Client (SVC) on ASA with ASDM Configuration Example in order to learn more about the SSL VPN Client.

This document demonstrates a simple configuration for the Thin-Client SSL VPN on the Adaptive Security Appliance (ASA). The configuration allows a user to telnet securely to a router located on the inside of the ASA. The configuration in this document is supported for ASA version 7.x and later.

Prerequisites

Requirements

Before you attempt this configuration, ensure that you meet these requirements for the remote client stations:

- SSL-enabled Web browser
- SUN Java JRE version 1.4 or later
- Cookies enabled
- Popup blockers disabled
- Local Administrative privileges (not required but strongly suggested)

Note: The latest version of the SUN Java JRE is available as a free download from the Java Website .

Components Used

The information in this document is based on these software and hardware versions:

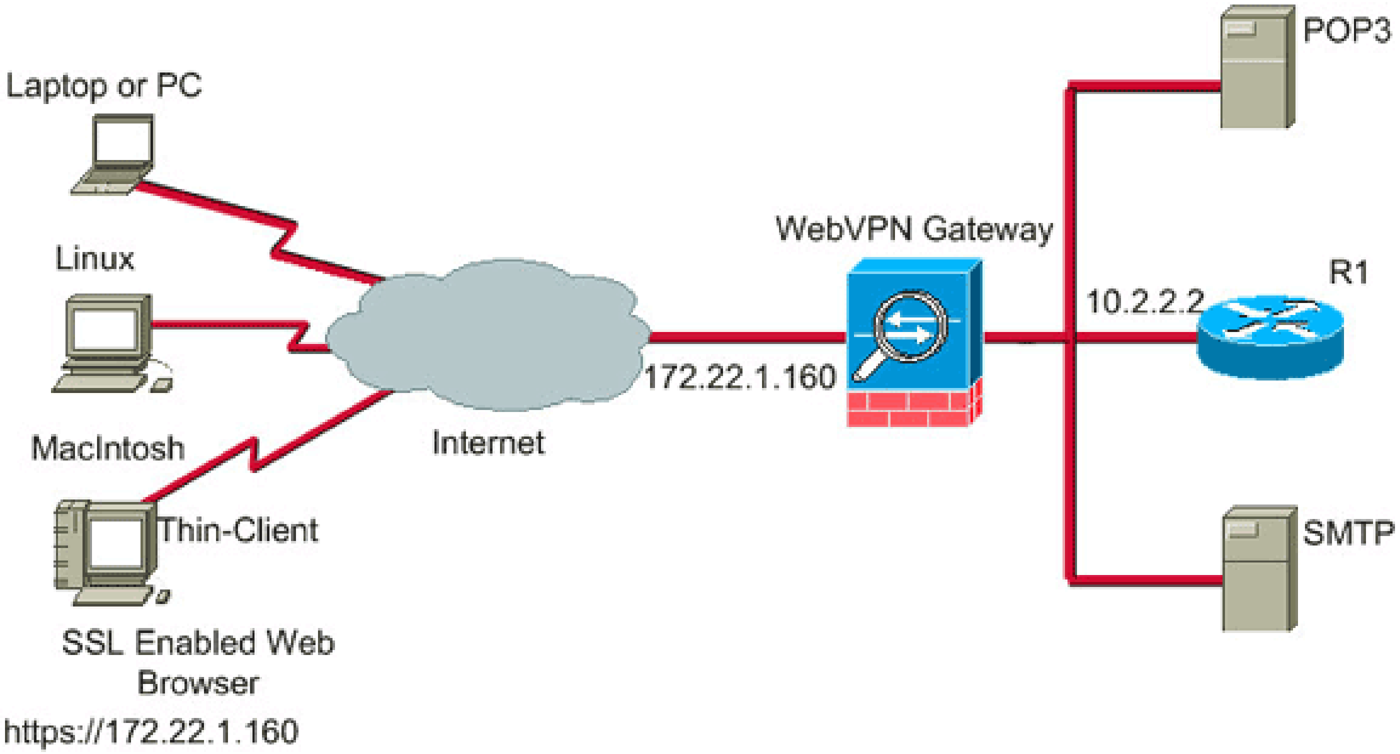
- Cisco Adaptive Security Appliance 5510 series
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Note:** Refer to Allowing HTTPS Access for ASDM in order to allow the ASA to be configured by the ASDM.
- Cisco Adaptive Security Appliance Software Version 7.2(1)
- Microsoft Windows XP Professional (SP 2) remote client

The information in this document was developed in a lab environment. All devices used in this document were reset to their default configuration. If your network is live, make sure you understand the potential impact of any command. All IP addresses used in this configuration were selected from RFC 1918 addresses in a lab environment; these IP addresses are not routable on the Internet and are for test purposes only.

Network Diagram

This document uses the network configuration described in this section.

When a remote client initiates a session with the ASA, the client downloads a small Java applet to the workstation. The client is presented with a list of preconfigured resources.



Conventions

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

Background Information

In order to start a session, the remote client opens an SSL browser to the outside interface of the ASA. After the session is established, the user can use the parameters configured on the ASA to invoke any Telnet or application access. The ASA proxies the secure connection and allows the user access to the device.

Note: Inbound access lists are not necessary for these connections because the ASA is already aware of what constitutes a legal session.

Thin-Client SSL VPN Configuration using ASDM

In order to configure Thin-Client SSL VPN on the ASA, complete these steps:

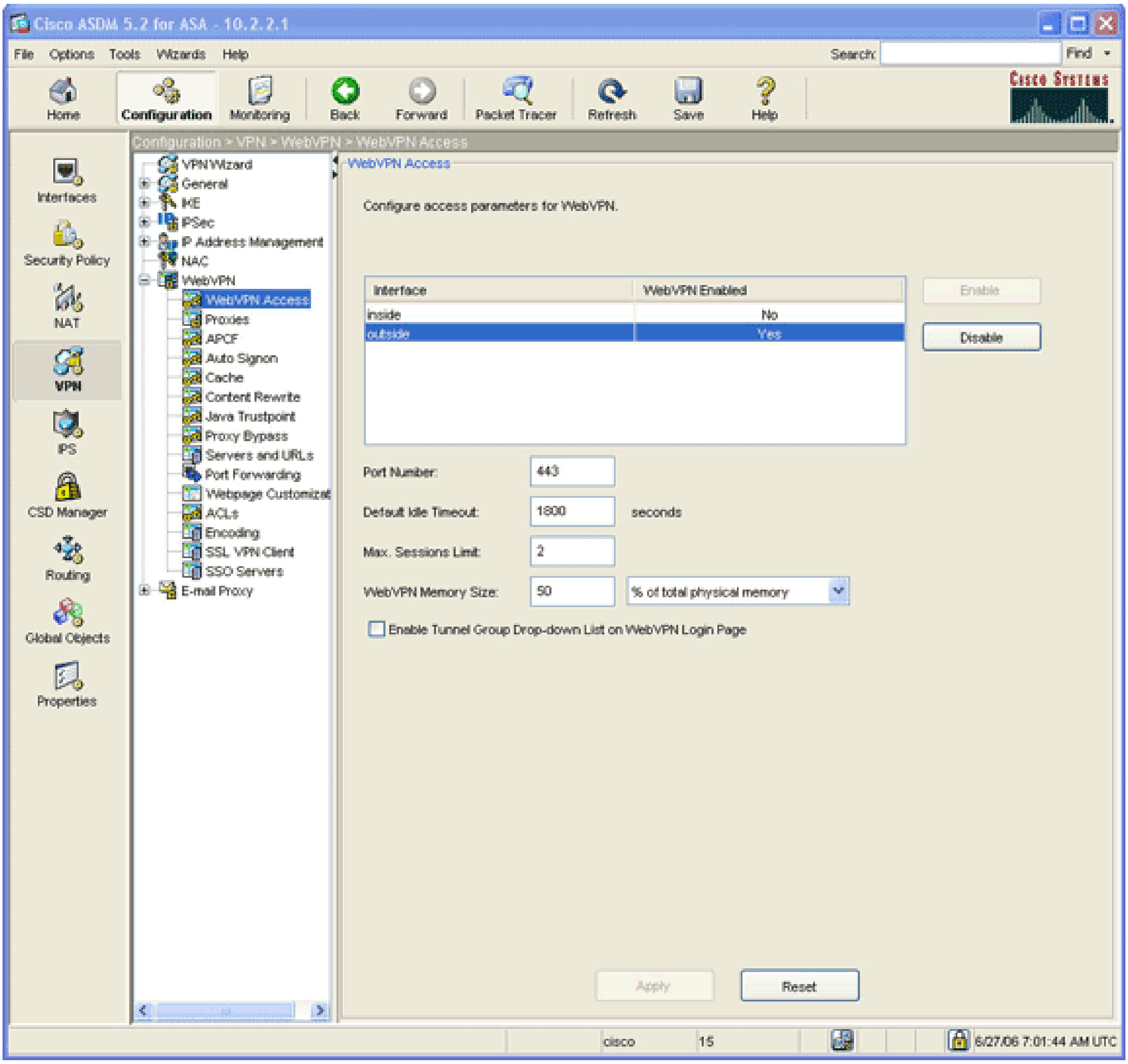
1. Enable WebVPN on the ASA
2. Configure Port Forwarding Characteristics
3. Create a Group Policy and Link it to the Port Forwarding List (created in Step 2)
4. Create a Tunnel Group and Link it to the Group Policy (created in Step 3)

5. Create a User and Add That User to the Group Policy (created in Step 3)

Step 1. Enable WebVPN on the ASA

In order to enable WebVPN on the ASA, complete these steps:

1. Within the ASDM application, click **Configuration**, and then click **VPN**.
2. Expand **WebVPN**, and choose **WebVPN Access**.



Cisco ASDM 5.2 for ASA - 10.2.2.1

Configuration > VPN > WebVPN > WebVPN Access

WebVPN Access

Configure access parameters for WebVPN.

Interface	WebVPN Enabled
inside	No
outside	Yes

Port Number: 443

Default Idle Timeout: 1800 seconds

Max. Sessions Limit: 2

WebVPN Memory Size: 50 % of total physical memory

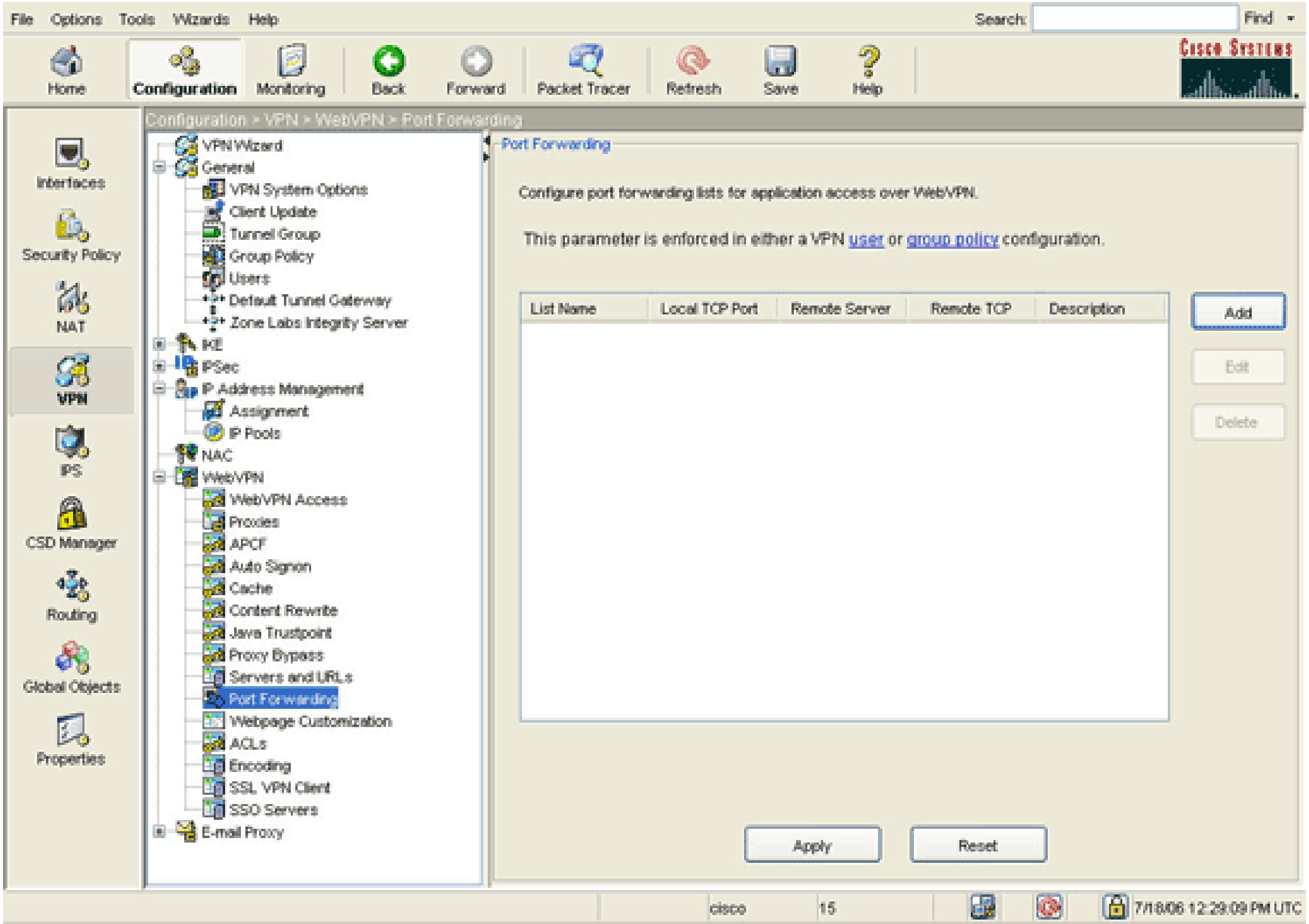
☐ Enable Tunnel Group Drop-down List on WebVPN Login Page

3. Highlight the interface, and click **Enable**.
4. Click **Apply**, click **Save**, and then click **Yes** to accept the changes.

Step 2. Configure Port Forwarding Characteristics

In order to configure port forwarding characteristics, complete these steps:

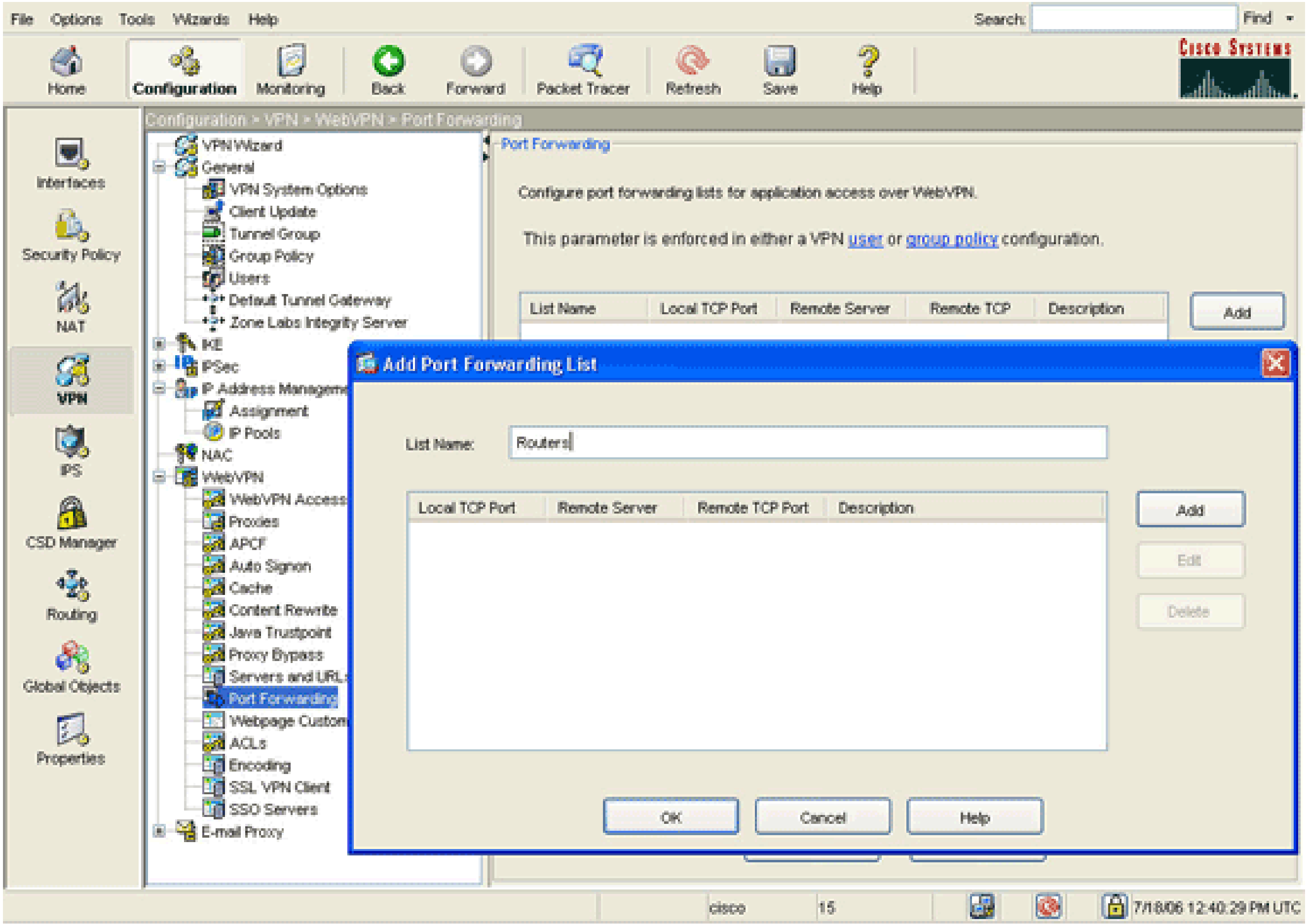
1. Expand **WebVPN**, and choose **Port Forwarding**.



Configure port forwarding lists for application access over WebVPN.

This parameter is enforced in either a VPN user or group policy configuration.

2. Click the **Add** button.



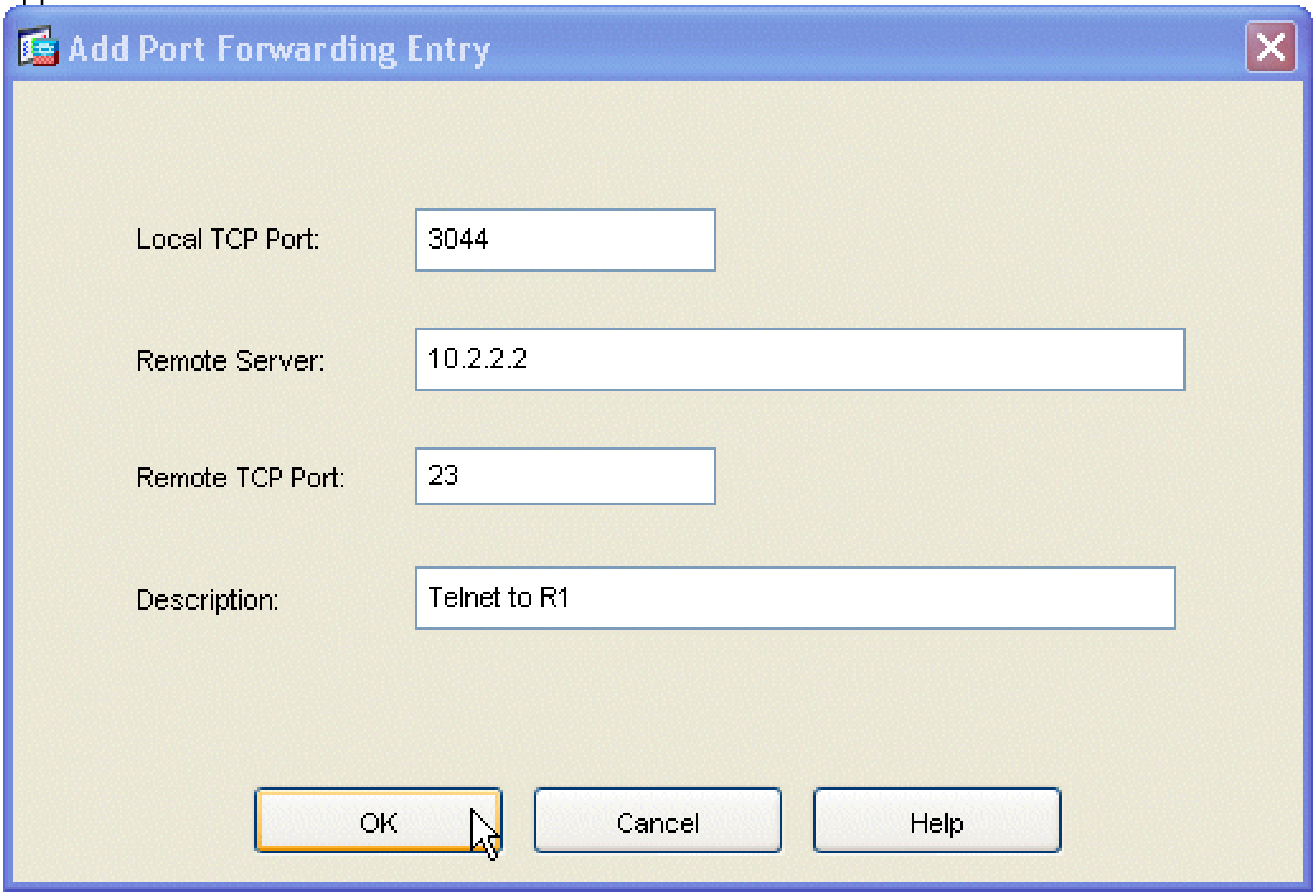
Configure port forwarding lists for application access over WebVPN.

This parameter is enforced in either a VPN user or group policy configuration.

List Name: Routers

3. In the Add Port Forwarding List dialog box, enter a list name, and click **Add**.The Add Port Forwarding Entry dialog box

appears.



Local TCP Port: 3044

Remote Server: 10.2.2.2

Remote TCP Port: 23

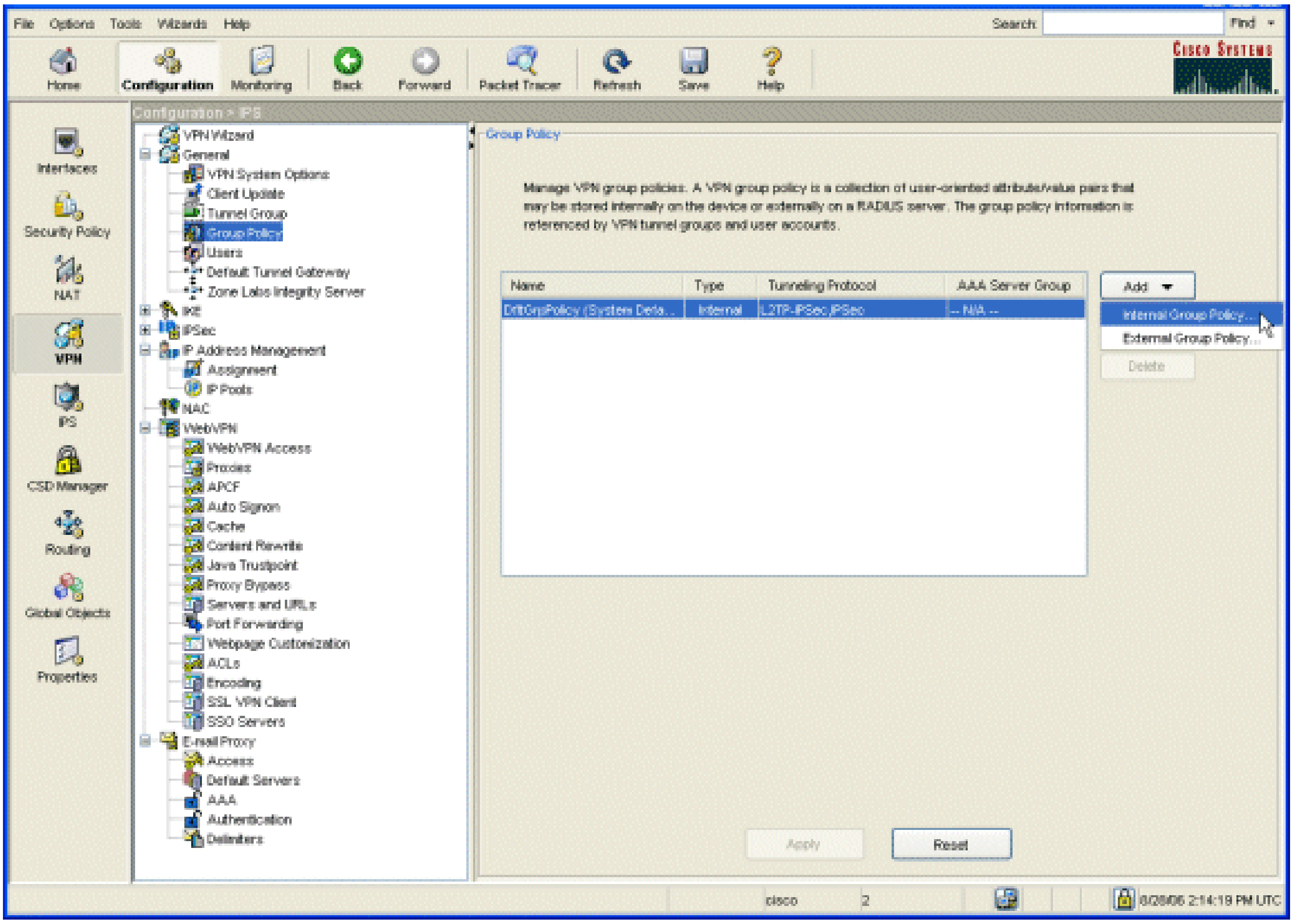
Description: Telnet to R1

4. In the Add Port Forwarding Entry dialog box, enter these options:In the Local TCP Port field, enter a port number or accept the default value.The value you enter can be any number from 1024 to 65535.In the Remote Server field, enter an IP address.This example uses the address of the router.In the Remote TCP Port field, enter a port number.This example uses port 23.In the Description field, enter a description, and click **OK**.
5. Click **OK**, and then click **Apply**.
6. Click **Save**, and then click **Yes** to accept the changes.

Step 3. Create a Group Policy and Link it to the Port Forwarding List

In order to create a group policy and link it to the port forwarding list, complete these steps:

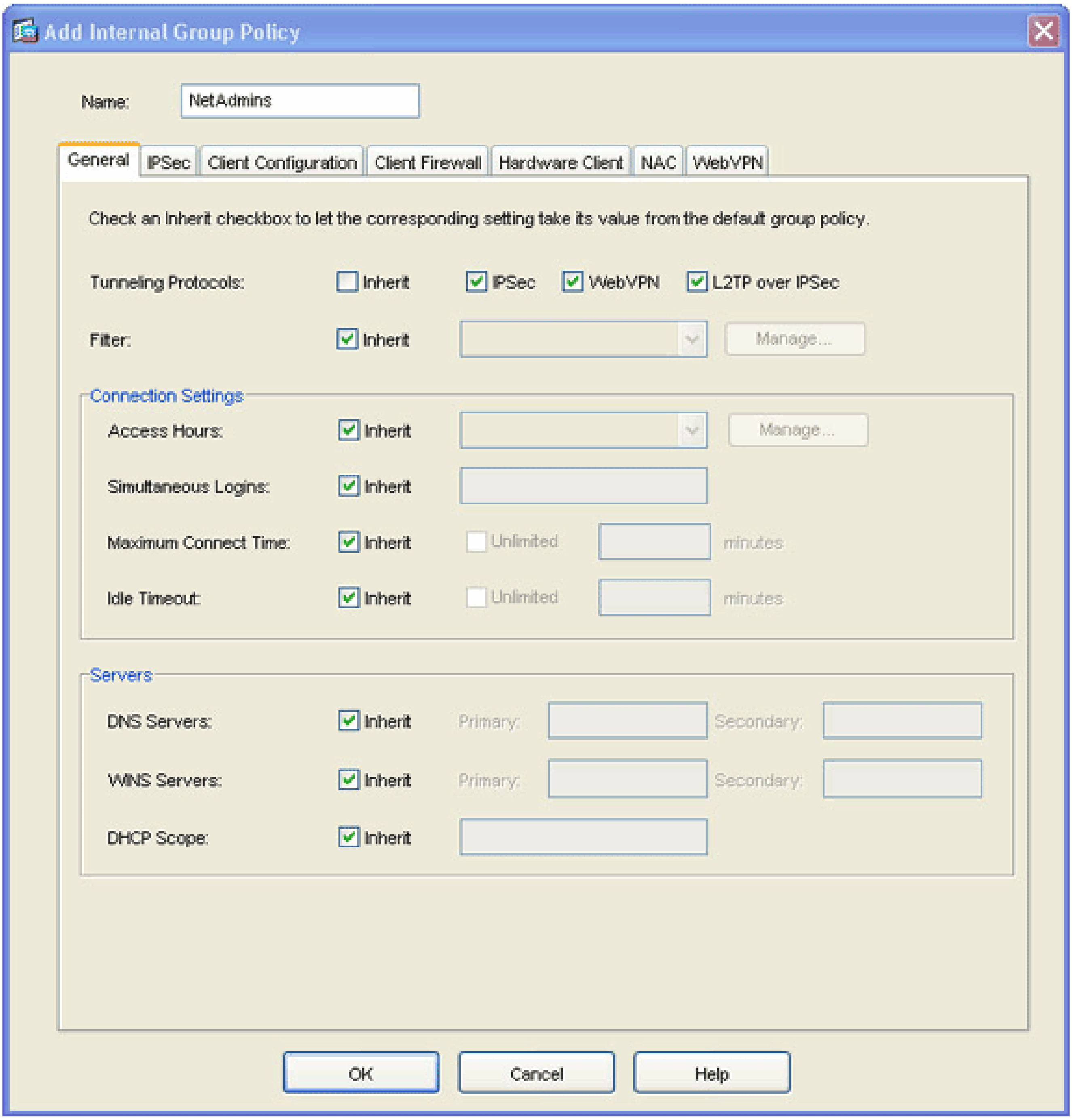
1. Expand **General**, and choose **Group Policy**.



Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	AAA Server Group
DfltGrpPolicy (System Defa...	Internal	L2TP-IPSec,IPSec	-- N/A --

2. Click **Add**, and choose **Internal Group Policy**.The Add Internal Group Policy dialog box appears.



Name: NetAdmins

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: □ Inherit ☑ IPSec ☑ WebVPN ☑ L2TP over IPSec

Filter: ☑ Inherit

Connection Settings

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

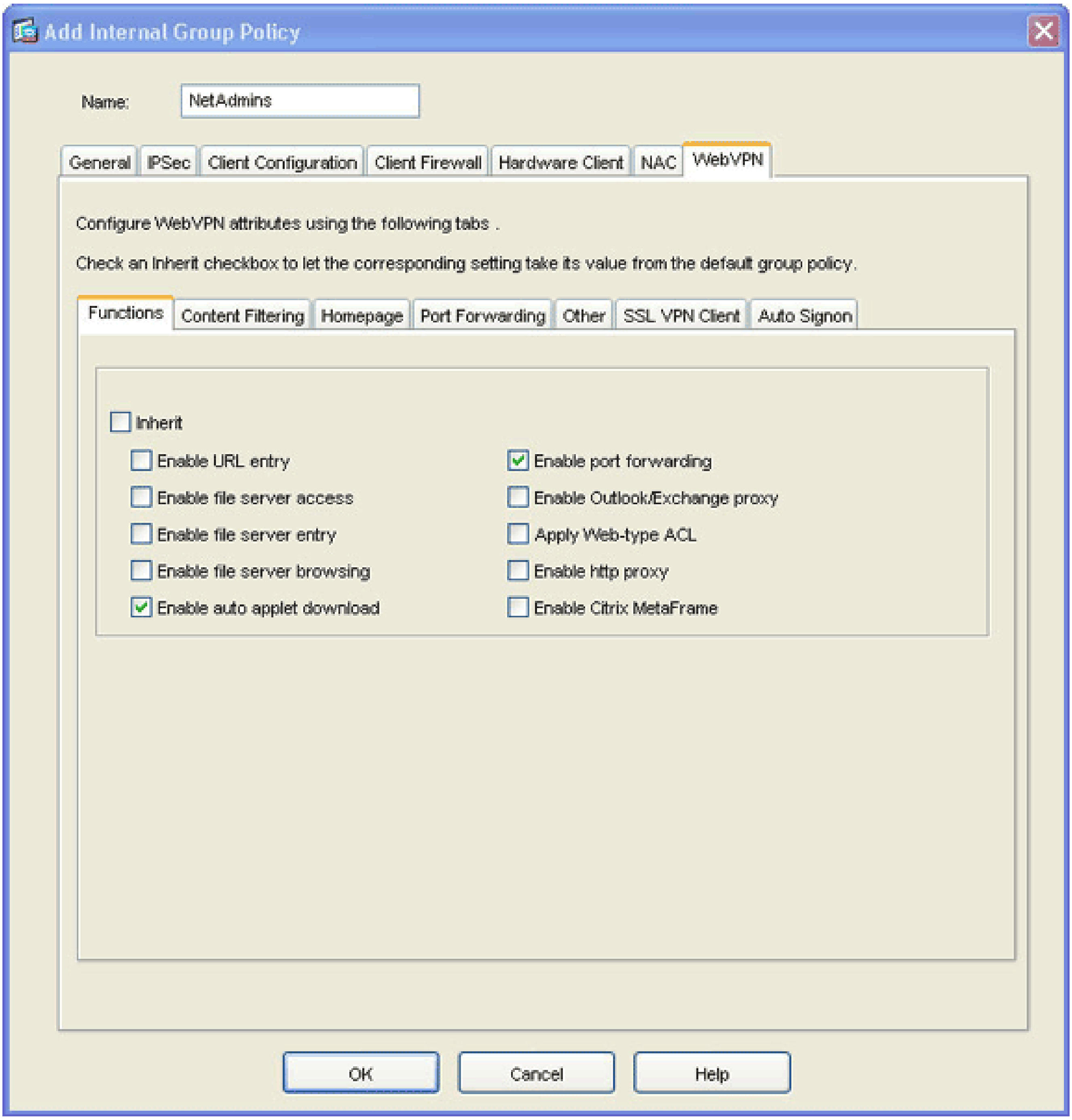
Servers

DNS Servers: ☑ Inherit Primary: Secondary:

WINS Servers: ☑ Inherit Primary: Secondary:

DHCP Scope: ☑ Inherit

3. Enter a name or accept the default group policy name.
4. Uncheck the Tunneling Protocols **Inherit** check box, and check the **WebVPN** check box.
5. Click the **WebVPN** tab located at the top of dialog box, and then click the **Functions** tab.
6. Uncheck the **Inherit** check box, and check the **Enable auto applet download** and **Enable port forwarding** check boxes as shown in this image:



Name: NetAdmins

Configure WebVPN attributes using the following tabs .

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

□ Inherit

□ Enable URL entry

□ Enable file server access

□ Enable file server entry

□ Enable file server browsing

☑ Enable auto applet download

☑ Enable port forwarding

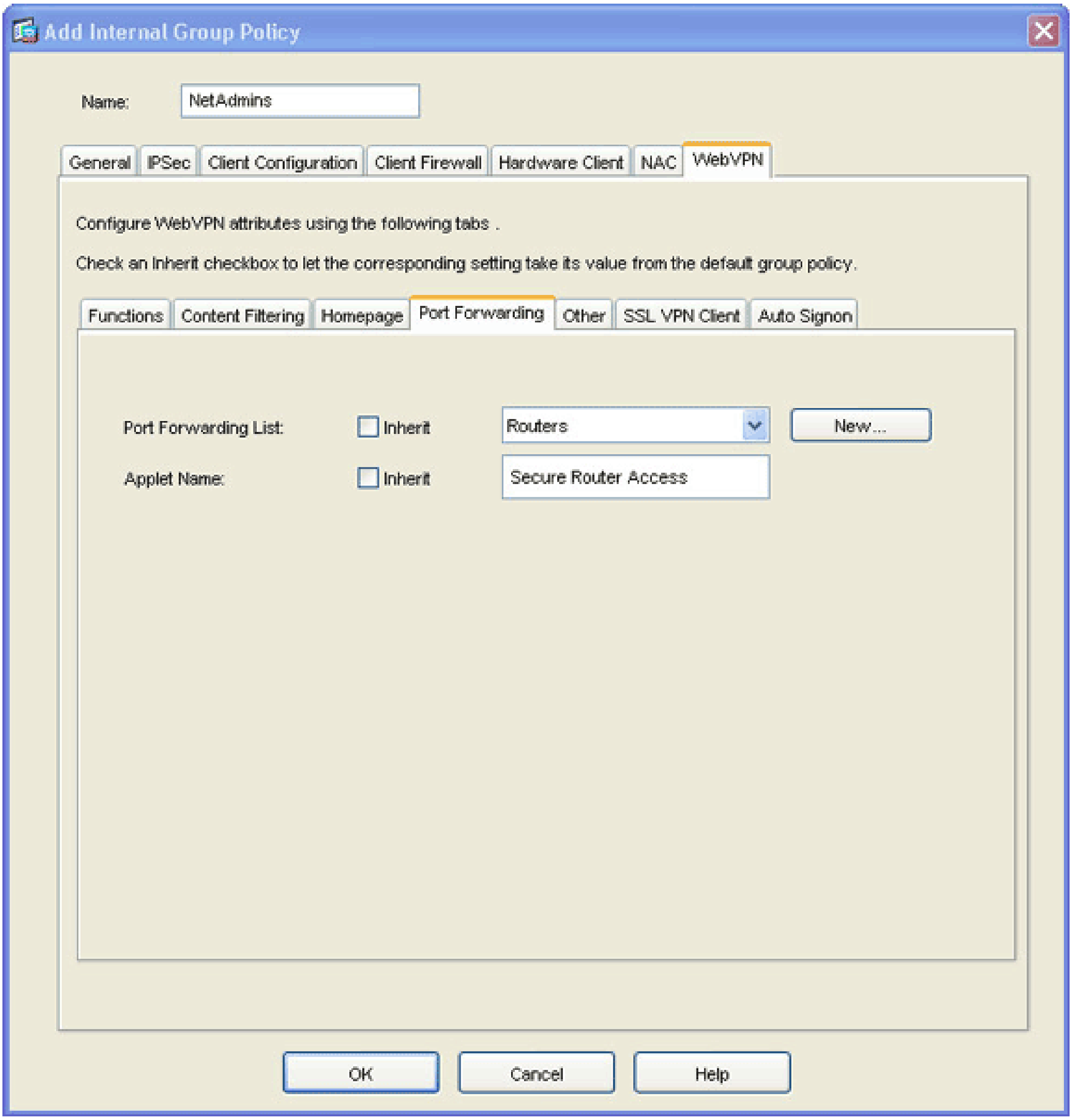
□ Enable Outlook/Exchange proxy

□ Apply Web-type ACL

□ Enable http proxy

□ Enable Citrix MetaFrame

7. Also within the WebVPN tab, click the **Port Forwarding** tab, and uncheck the Port Forwarding List **Inherit** check box.



Add Internal Group Policy

Name: NetAdmins

Configure WebVPN attributes using the following tabs .

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Port Forwarding List: □ Inherit Routers

Applet Name: □ Inherit Secure Router Access

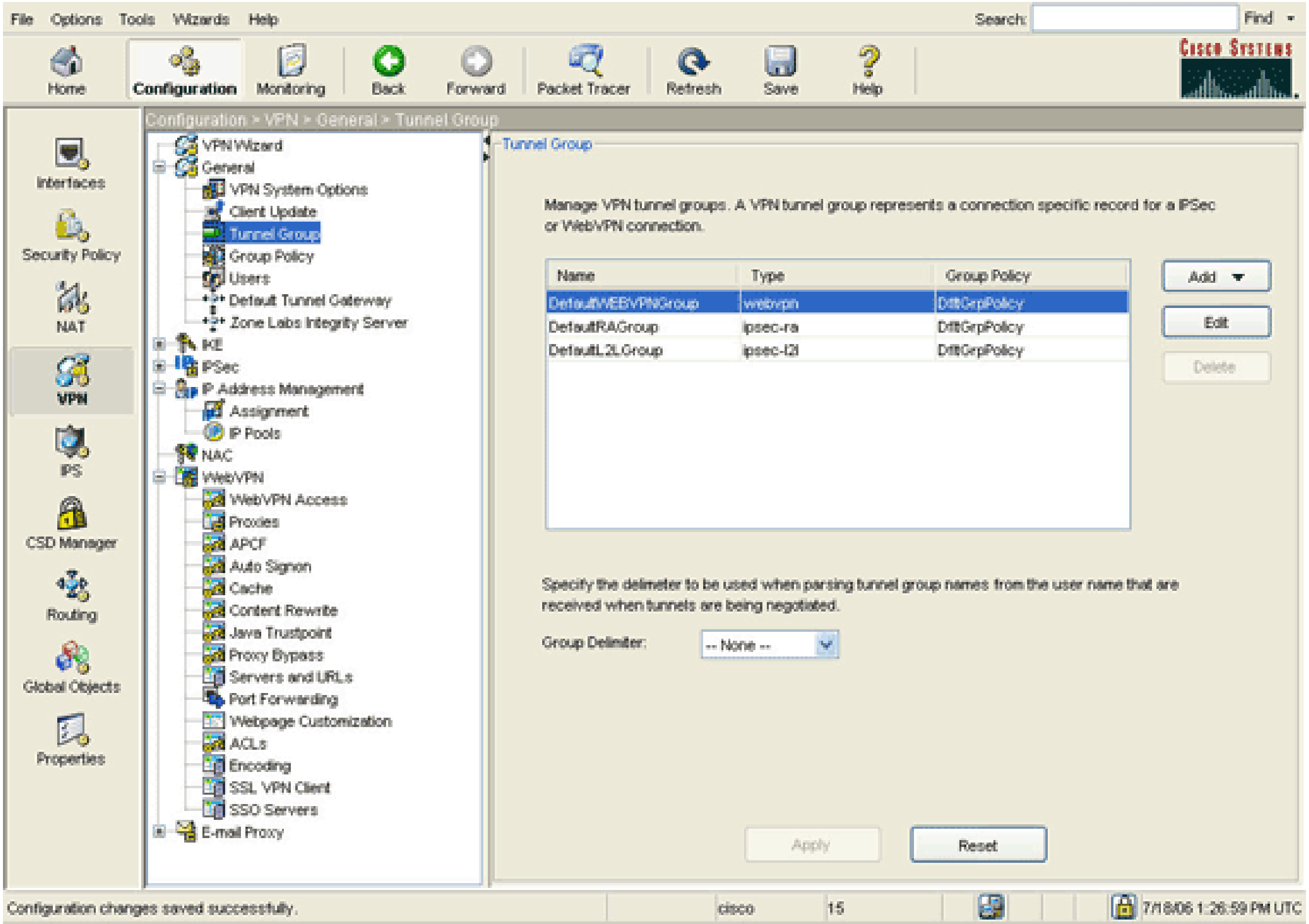
8. Click the **Port Forwarding List** drop-down arrow, and choose the port forwarding list you created in Step 2.
9. Uncheck the Applet Name **Inherit** check box, and change the name in the text field.The client displays the Applet Name on connection.
10. Click **OK**, and then click **Apply**.
11. Click **Save**, and then click **Yes** to accept the changes.

Step 4. Create a Tunnel Group and Link it to the Group Policy

You can edit the default *DefaultWebVPNGroup* tunnel group or create a new tunnel group.

In order to create a new tunnel group, complete these steps:

1. Expand **General**, and choose **Tunnel Group**.



Configuration > VPN > General > Tunnel Group

Tunnel Group

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection.

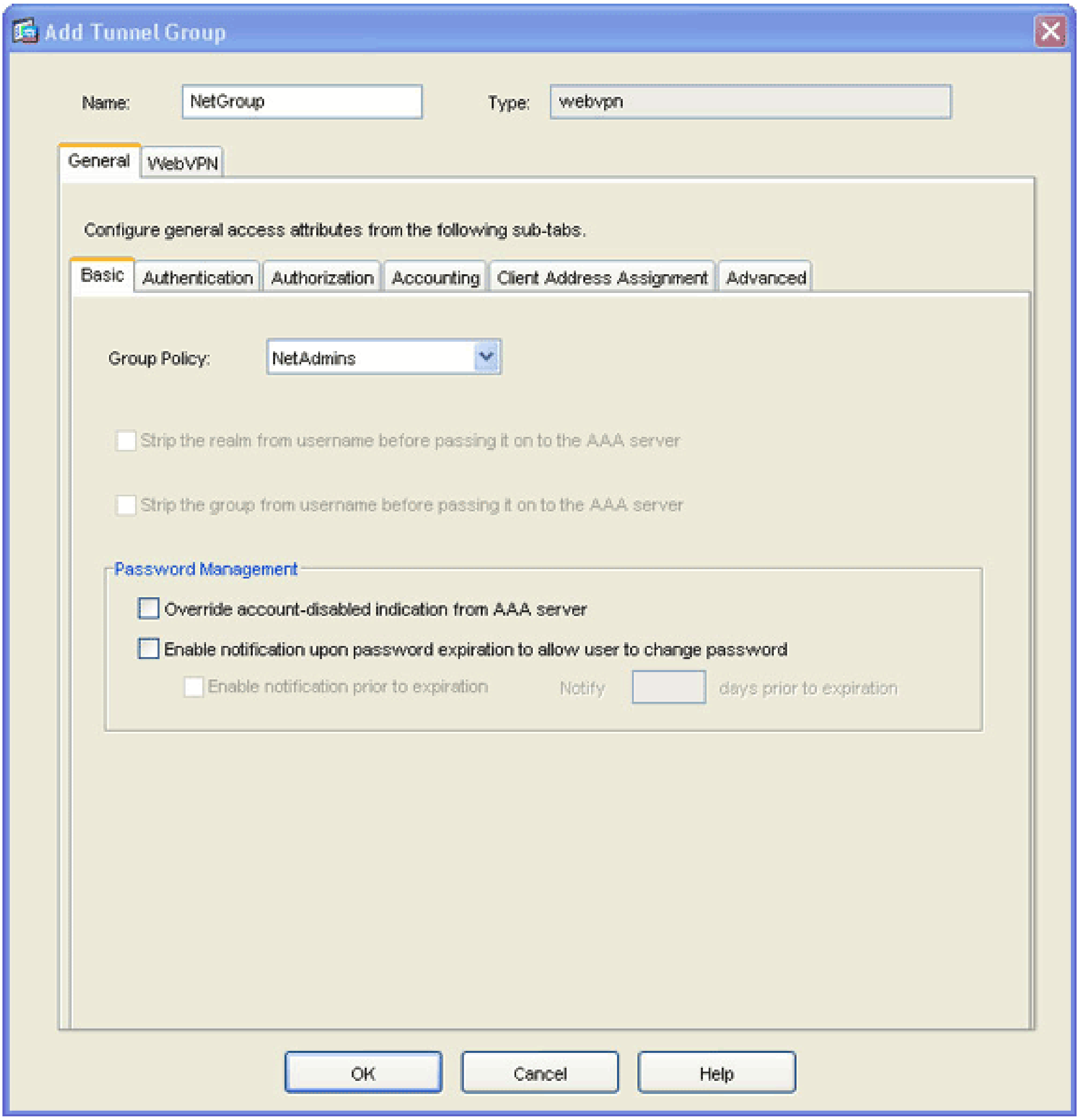
Name	Type	Group Policy
DefaultWEBVPNGroup	webvpn	DfltGrpPolicy
DefaultRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

Specify the delimeter to be used when parsing tunnel group names from the user name that are received when tunnels are being negotiated.

Group Delimiter: -- None --

Configuration changes saved successfully. cisco 15 7/18/06 1:26:59 PM UTC

2. Click **Add**, and choose **WebVPN Access**.The Add Tunnel Group dialog box appears.



Name: NetGroup

Type: webvpn

Configure general access attributes from the following sub-tabs.

Group Policy: NetAdmins

□ Strip the realm from username before passing it on to the AAA server

□ Strip the group from username before passing it on to the AAA server

Password Management

□ Override account-disabled indication from AAA server

□ Enable notification upon password expiration to allow user to change password

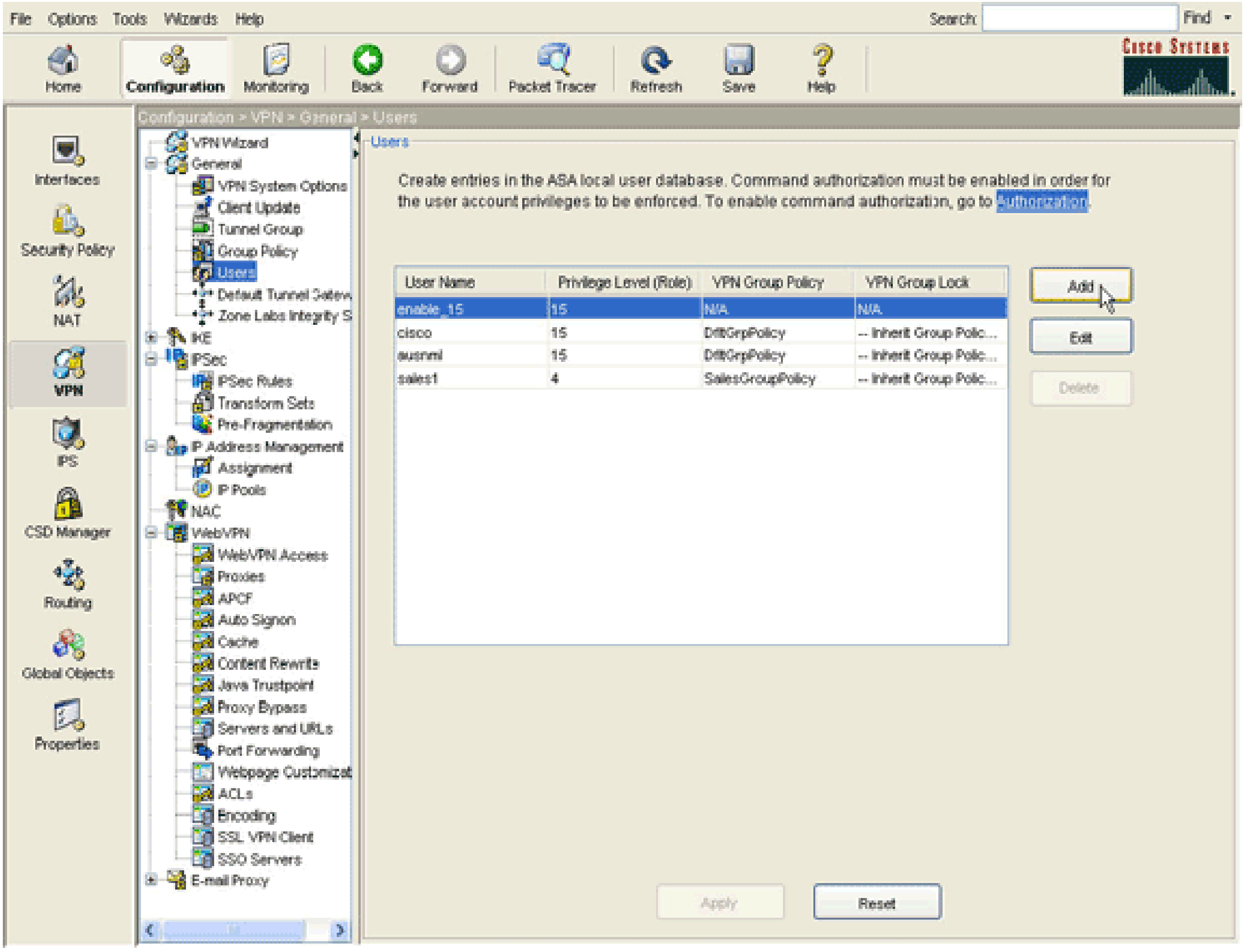
□ Enable notification prior to expiration Notify days prior to expiration

3. Enter a name in the Name field.
4. Click the **Group Policy** drop-down arrow, and choose the group policy you created in Step 3.
5. Click **OK**, and then click **Apply**.
6. Click **Save**, and then click **Yes** to accept the changes.The tunnel group, group policy, and port forwarding characteristics are now linked.

Step 5. Create a User and Add That User to the Group Policy

In order to create a user and add that user to the group policy, complete these steps:

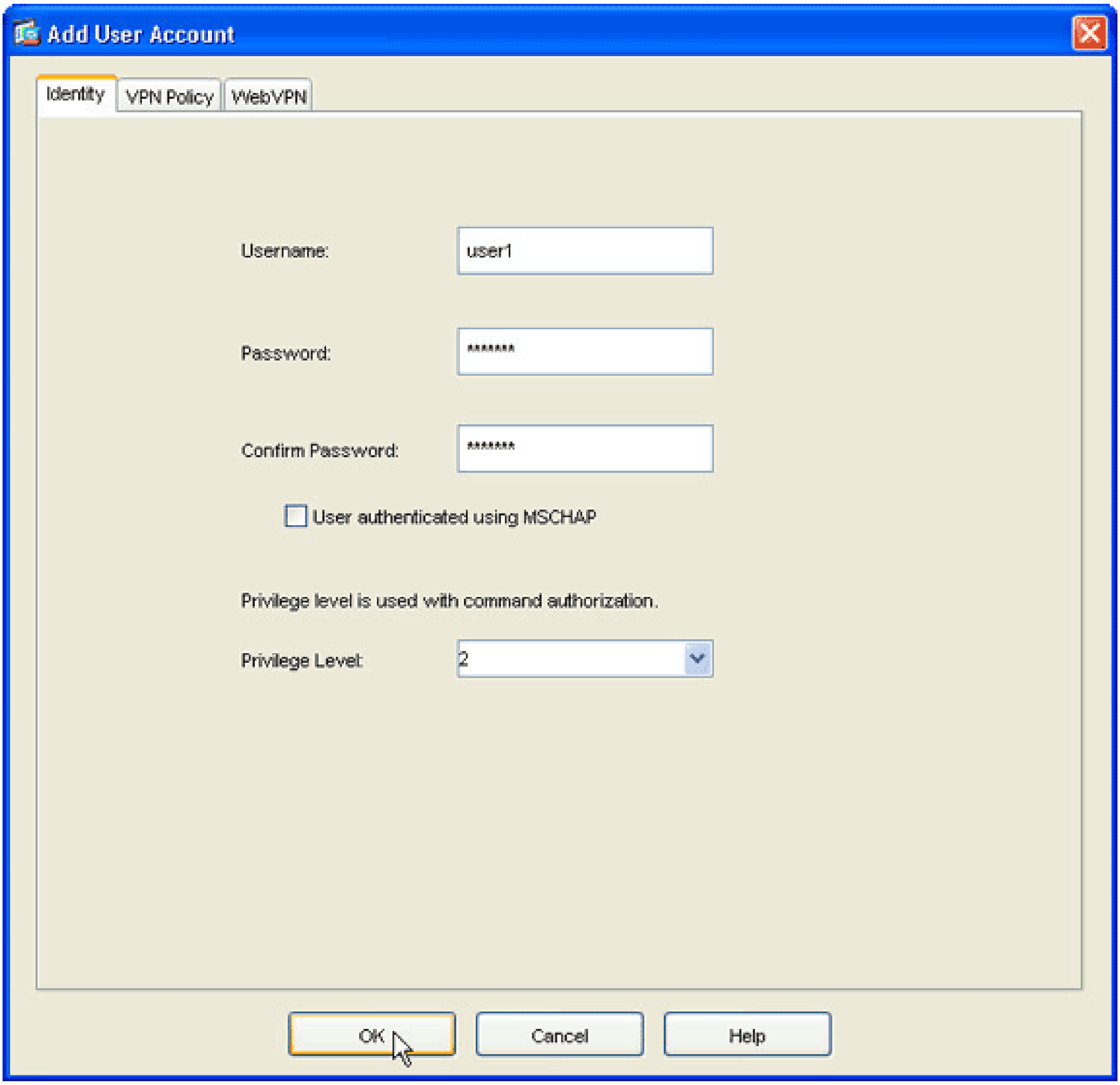
1. Expand **General**, and choose **Users**.



Create entries in the ASA local user database. Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.

User Name	Privilege Level (Role)	VPN Group Policy	VPN Group Lock
enable_15	15	N/A	N/A
cisco	15	DfltGrpPolicy	-- Inherit Group Polic...
ausnml	15	DfltGrpPolicy	-- Inherit Group Polic...
sales1	4	SalesGroupPolicy	-- Inherit Group Polic...

2. Click the **Add** button.The Add User Account dialog box appears.



Username: user1

Password: *******

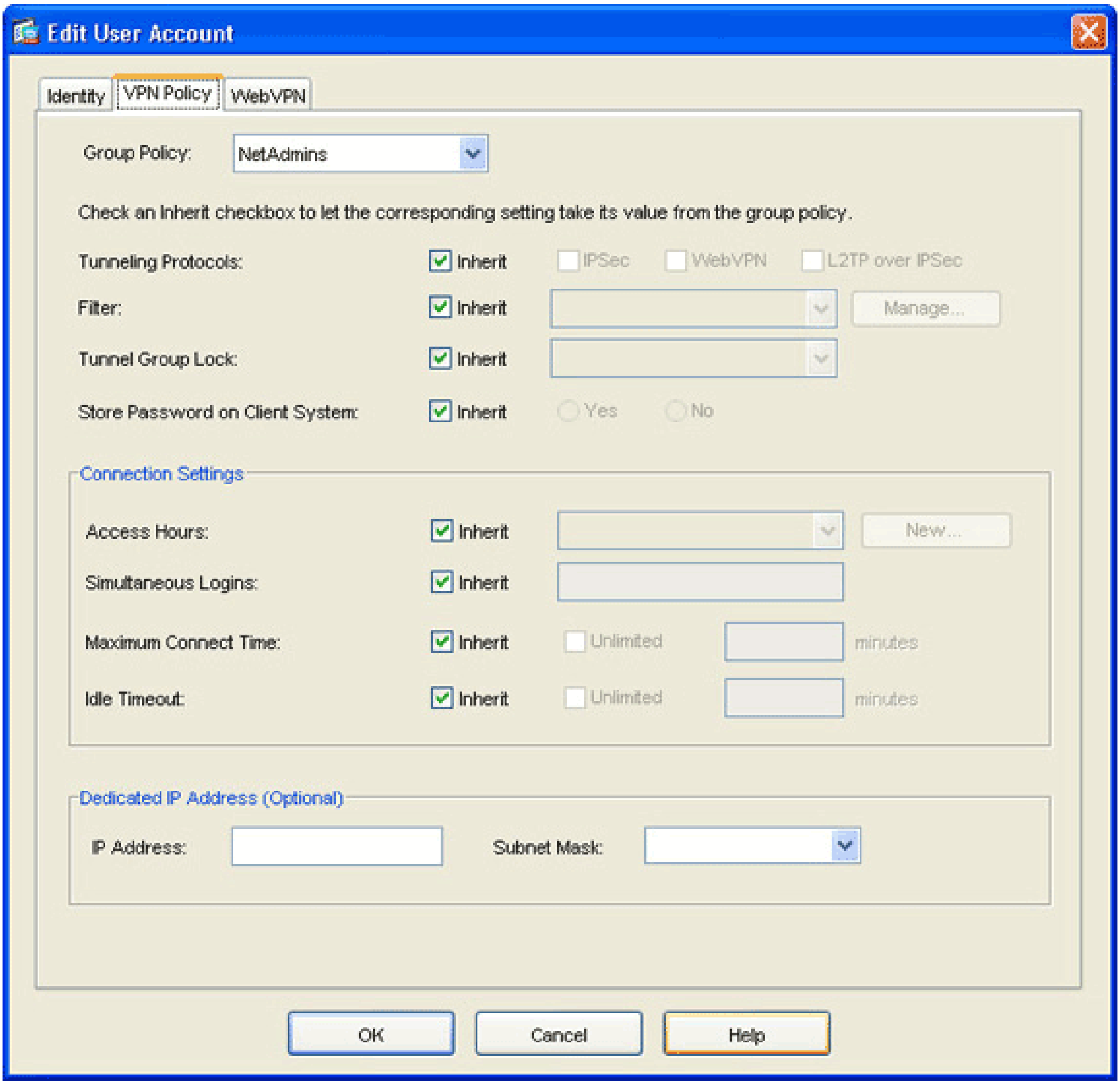
Confirm Password: *******

□ User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

3. Enter values for the username, password, and privilege information, and then click the **VPN Policy** tab.



Edit User Account

Identity | VPN Policy | WebVPN

Group Policy: NetAdmins

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

Tunneling Protocols: ☑ Inherit □ IPSec □ WebVPN □ L2TP over IPSec

Filter: ☑ Inherit

Tunnel Group Lock: ☑ Inherit

Store Password on Client System: ☑ Inherit ○ Yes ○ No

Connection Settings

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

Dedicated IP Address (Optional)

IP Address:

Subnet Mask:

4. Click the **Group Policy** drop-down arrow, and choose the group policy you created in Step 3.This user inherits the WebVPN characteristics and policies of the selected group policy.
5. Click **OK**, and then click **Apply**.
6. Click **Save**, and then **Yes** to accept the changes.

Thin-Client SSL VPN Configuration using 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
```

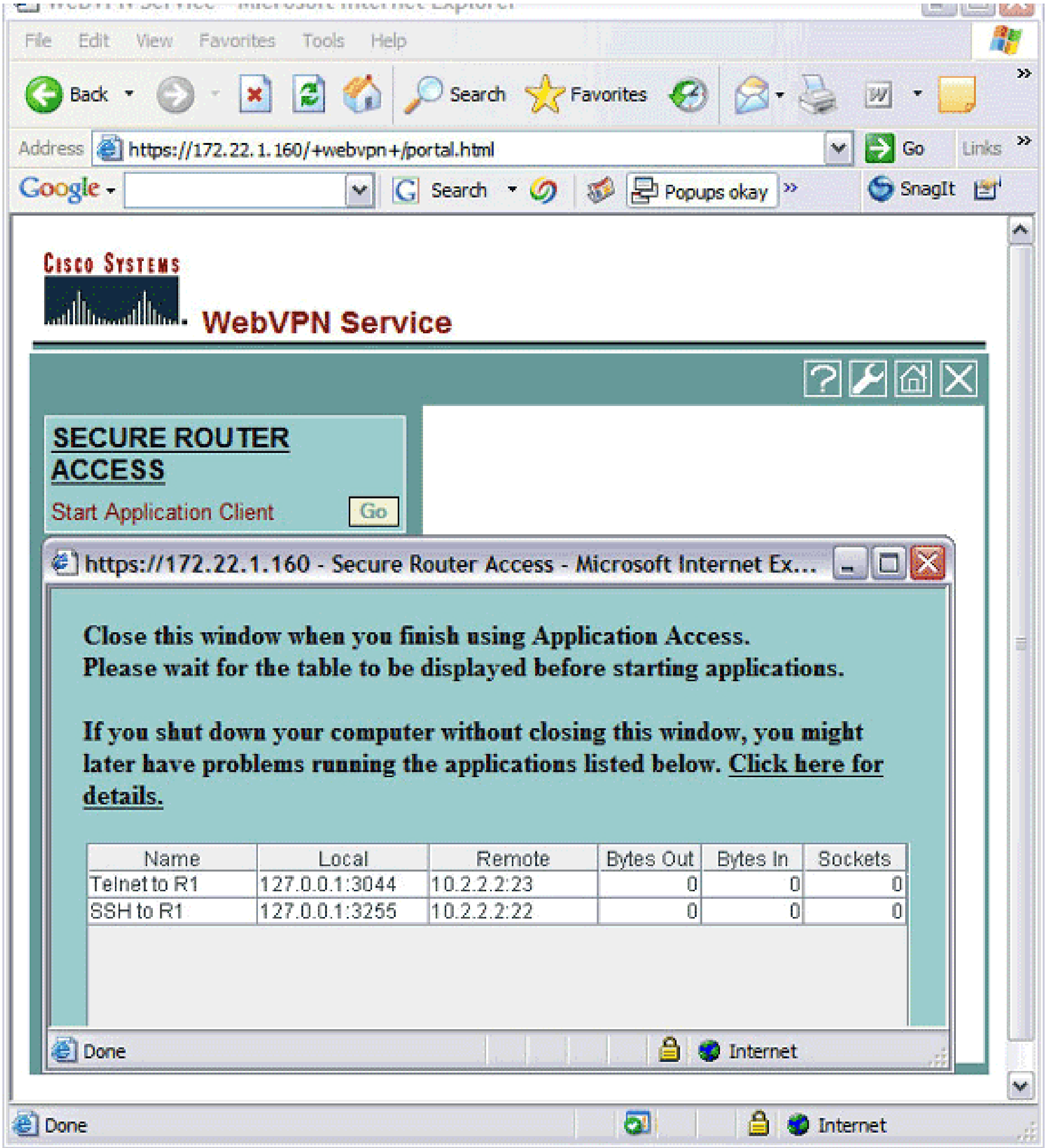
Verify

Use this section to verify that your configuration works properly.

Procedure

This procedure describes how to determine the validity of the configuration and how to test the configuration.

1. From a client workstation, enter **https://*outside_ASA_IP Address*** ; where *outside_ASA_IPAddress* is the SSL URL of the ASA.Once the digital certificate is accepted, and the user is authenticated, the WebVPN Service Web page appears.



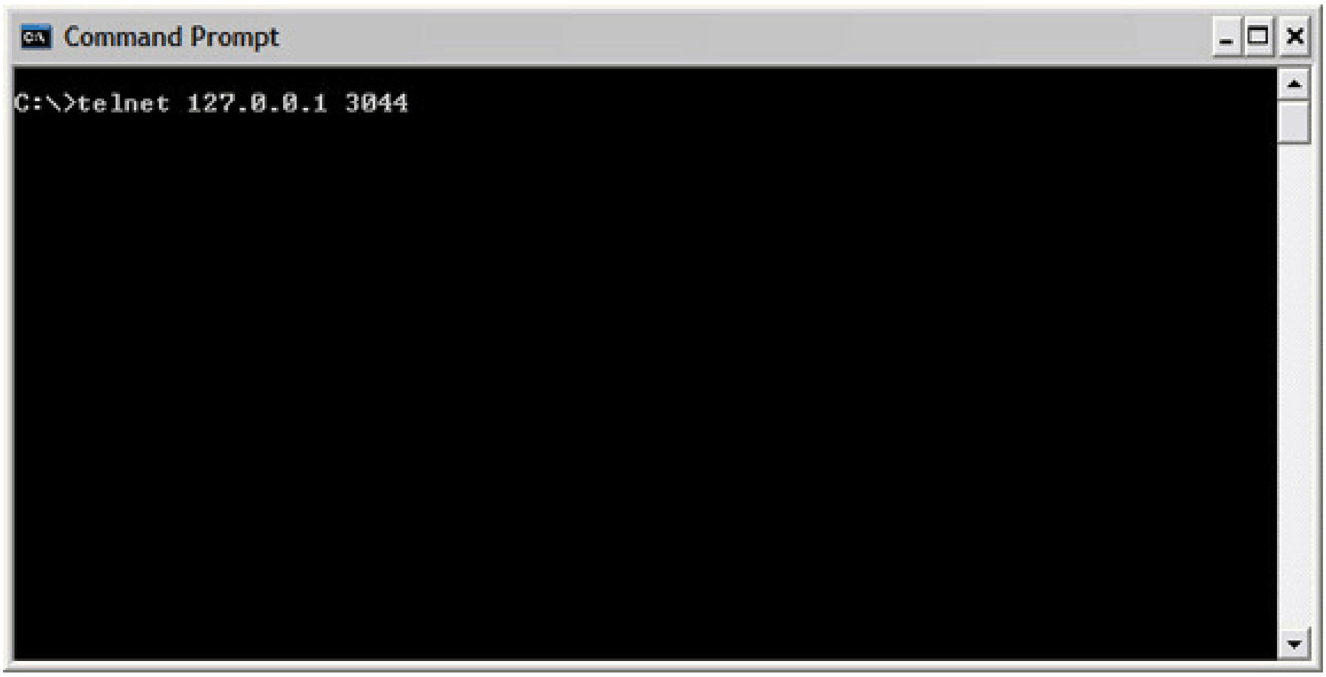
Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.

Name	Local	Remote	Bytes Out	Bytes In	Sockets
Telnet to R1	127.0.0.1:3044	10.2.2.2:23	0	0	0
SSH to R1	127.0.0.1:3255	10.2.2.2:22	0	0	0

The address and port information required to access the application appears in the local column. The Bytes Out and Bytes In columns display no activity because the application has not been invoked at this time.

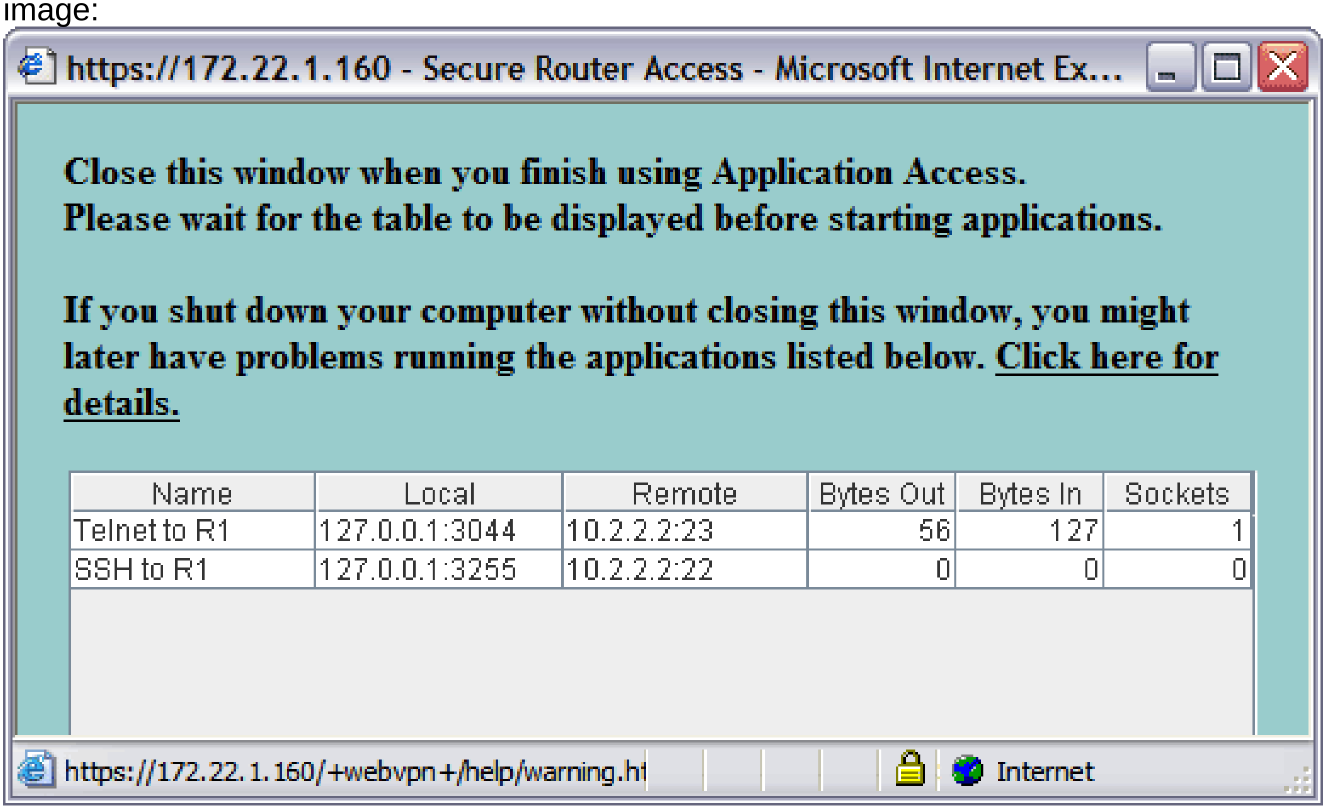
2. Use the DOS prompt or other Telnet application to start a Telnet session.
3. At the command prompt, enter **telnet 127.0.0.1 3044**.**Note:** This command provides an example of how to gain access to the local port displayed in the WebVPN Service Web page image in this document. *The command does not include a colon (:).* Type the command as described in this document.The ASA receives the command over the secure session, and because it stores a map of the information, the ASA knows immediately to open the secure Telnet session to the mapped
device.



```
C:\>telnet 127.0.0.1 3044
```

Once you enter your username and password, access to the device is complete.

4. In order to verify access to the device, check the Bytes Out and Bytes In columns as shown in this image:


https://172.22.1.160 - Secure Router Access - Microsoft Internet Ex...
https://172.22.1.160/+webvpn+/help/warning.ht
Internet

Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.

Name	Local	Remote	Bytes Out	Bytes In	Sockets
Telnet to R1	127.0.0.1:3044	10.2.2.2:23	56	127	1
SSH to R1	127.0.0.1:3255	10.2.2.2:22	0	0	0

Commands

Several **show** commands are associated with WebVPN. You can execute these commands at the command-line interface (CLI) to show statistics and other information. For detailed information about **show** commands, refer to Verifying WebVPN Configuration.

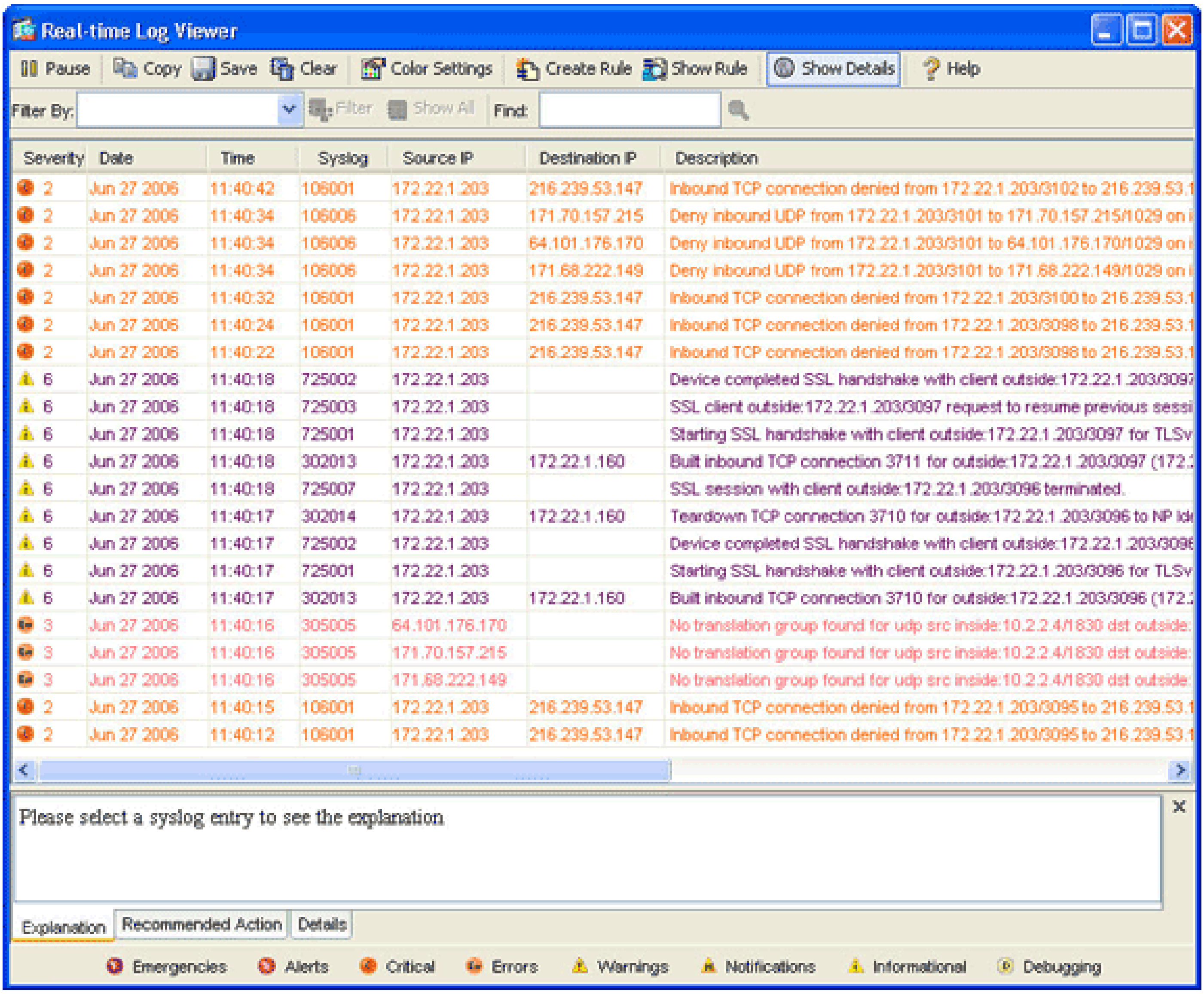
Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

Use this section to troubleshoot your configuration.

Is the SSL handshake process complete?

Once you connect to the ASA, check if the real-time log shows the completion of the SSL handshake.



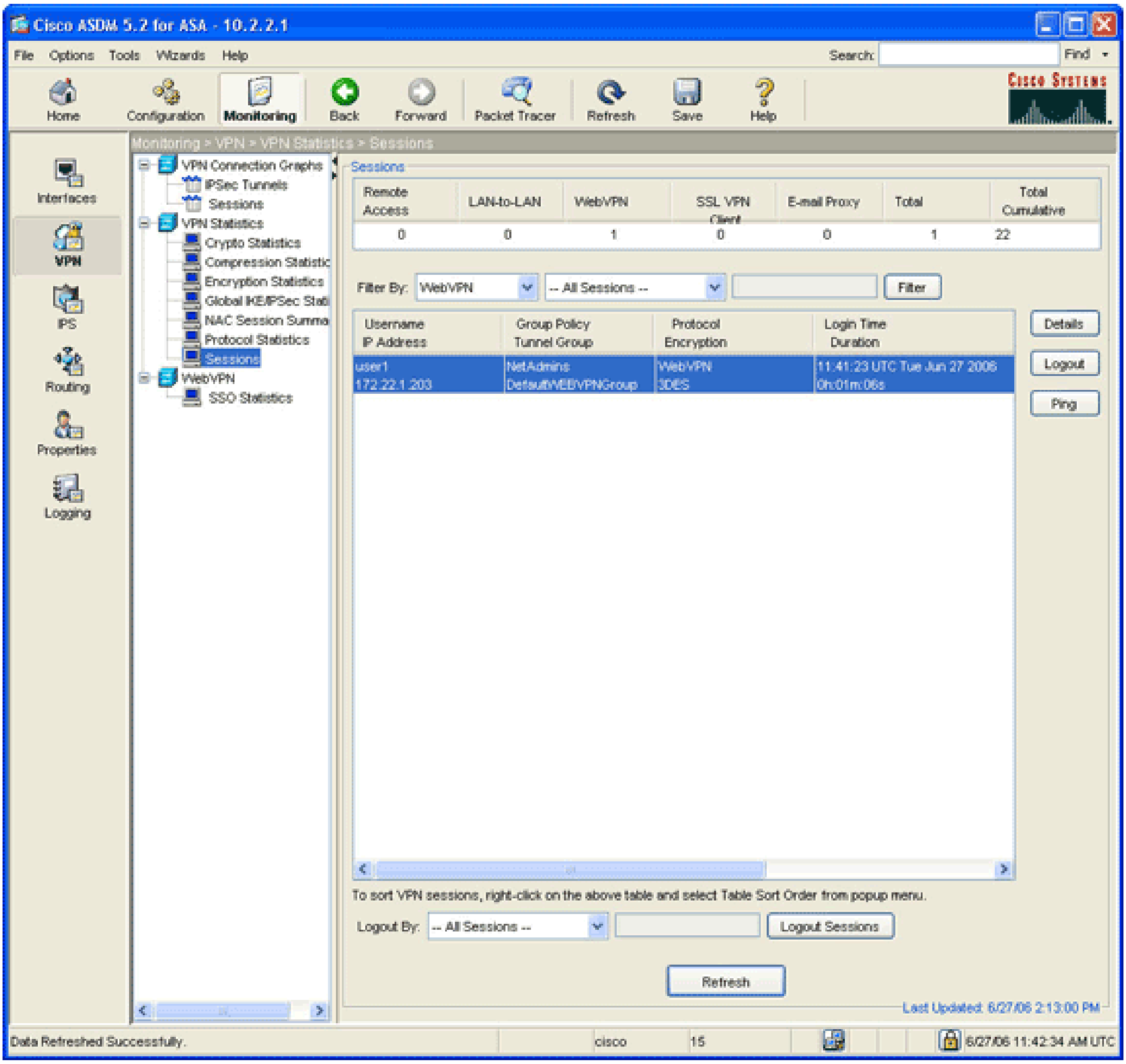
Severity	Date	Time	Syslog	Source IP	Destination IP	Description
2	Jun 27 2006	11:40:42	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3102 to 216.239.53.1
2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.70.157.215	Deny inbound UDP from 172.22.1.203/3101 to 171.70.157.215/1029 on i
2	Jun 27 2006	11:40:34	106006	172.22.1.203	64.101.176.170	Deny inbound UDP from 172.22.1.203/3101 to 64.101.176.170/1029 on i
2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.68.222.149	Deny inbound UDP from 172.22.1.203/3101 to 171.68.222.149/1029 on i
2	Jun 27 2006	11:40:32	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3100 to 216.239.53.1
2	Jun 27 2006	11:40:24	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.1
2	Jun 27 2006	11:40:22	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.1
6	Jun 27 2006	11:40:18	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/3097
6	Jun 27 2006	11:40:18	725003	172.22.1.203		SSL client outside:172.22.1.203/3097 request to resume previous sessi
6	Jun 27 2006	11:40:18	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3097 for TLSv
6	Jun 27 2006	11:40:18	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3711 for outside:172.22.1.203/3097 (172.2
6	Jun 27 2006	11:40:18	725007	172.22.1.203		SSL session with client outside:172.22.1.203/3096 terminated.
6	Jun 27 2006	11:40:17	302014	172.22.1.203	172.22.1.160	Teardown TCP connection 3710 for outside:172.22.1.203/3096 to NP Ide
6	Jun 27 2006	11:40:17	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/3096
6	Jun 27 2006	11:40:17	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3096 for TLSv
6	Jun 27 2006	11:40:17	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3710 for outside:172.22.1.203/3096 (172.2
3	Jun 27 2006	11:40:16	305005	64.101.176.170		No translation group found for udp src inside:10.2.2.4/1830 dst outside:
3	Jun 27 2006	11:40:16	305005	171.70.157.215		No translation group found for udp src inside:10.2.2.4/1830 dst outside:
3	Jun 27 2006	11:40:16	305005	171.68.222.149		No translation group found for udp src inside:10.2.2.4/1830 dst outside:
2	Jun 27 2006	11:40:15	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.1
2	Jun 27 2006	11:40:12	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.1

Please select a syslog entry to see the explanation

Is the SSL VPN Thin-Client functional?

In order to verify that the SSL VPN Thin-Client is functional, complete these steps:

1. Click **Monitoring**, and then click **VPN**.
2. Expand **VPN Statistics**, and click **Sessions**.Your SSL VPN Thin-Client session should appear in the sessions list. Be sure to filter by WebVPN as shown in this image:



Monitoring > VPN > VPN Statistics > Sessions

Sessions

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	1	0	0	1	22

Filter By: WebVPN | -- All Sessions -- | Filter

Username IP Address	Group Policy Tunnel Group	Protocol Encryption	Login Time Duration
user1 172.22.1.203	NetAdmins DefaultWEBVPNGroup	WebVPN 3DES	11:41:23 UTC Tue Jun 27 2006 0h:01m:06s

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions -- | Logout Sessions

Last Updated: 6/27/06 2:13:00 PM

Data Refreshed Successfully. | cisco | 15 | 6/27/06 11:42:34 AM UTC

Commands

Several **debug** commands are associated with WebVPN. For detailed information about these commands, refer to Using WebVPN Debug Commands.

Note: The use of **debug** commands can adversely impact your Cisco device. Before you use **debug** commands, refer to Important Information on Debug Commands.

Related Information

- Clientless SSL VPN (WebVPN) on ASA Configuration Example
- SSL VPN Client (SVC) on ASA with ASDM Configuration Example
- Cisco ASA 5500 Series Adaptive Security Appliances
- ASA with WebVPN and Single Sign-on using ASDM and NTLMv1 Configuration Example
- Technical Support & Documentation - Cisco Systems