在 ASA 上用 ASDM 配置瘦客户端 SSL VPN (WebVPN) 的示例

目录

简介

通过瘦客户端 SSL VPN 技术，可以用安全方式访问某些具有 Telnet(23)、SSH(22)、POP3(110)、IMAP4(143) 和 SMTP(25) 等静态端口的应用程序。 可以使用瘦客户端 SSL VPN 作为用户驱动的应用程序和/或策略驱动的应用程序。即，可以按用户配置用户的访问权限，也可以创建组策略，从中添加一个或多个用户。

- **无客户端 SSL VPN (WebVPN) — 提供一个远程客户端，它要求通过启用了 SSL 的 Web 浏览器才能访问公司局域网 (LAN) 上的 HTTP 或 HTTPS Web 服务器。** 此外，利用无客户端 SSL VPN 还可以通过公用 Internet 文件系统 (CIFS) 协议浏览 Windows 文件。Outlook Web Access (OWA) 就是 HTTP 访问的一个示例。请参阅 ASA 上的无客户端 SSL VPN (WebVPN) 配置示例详细了解无客户端 SSL VPN。
- **瘦客户端 SSL VPN（端口转发）— 提供一个远程客户端，它下载基于 Java 的小程序，并允许**

以安全方式访问使用静态端口号的传输控制协议 (TCP) 应用程序。安全访问的示例包括邮局协议 (POP3)、简单邮件传输协议 (SMTP)、Internet 邮件访问协议 (IMAP)、安全 Shell (ssh) 和 Telnet。由于本地计算机上的文件发生更改，因此用户必须有本地管理权限才能使用此方法。这种 SSL VPN 方法不能与使用动态端口分配的应用程序（如某些文件传输协议 (FTP) 应用程序）配合工作。**注意：**不支持用户数据报协议(UDP)。

- **SSL VPN Client（隧道模式）— 向远程工作站下载一个小客户端，并允许以安全方式完全访问公司内部网络中的资源。**可以将 SSL VPN Client (SVC) 永久下载到远程工作站，也可以在安全会话关闭后删除该客户端。要详细了解 SSL VPN 客户端，请参阅在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例。

本文档演示自适应安全设备 (ASA) 上瘦客户端 SSL VPN 的简单配置。 通过该配置，用户可安全地 telnet 到位于 ASA 内部的路由器。ASA 7.x 版及更高版本支持本文档中的配置。

先决条件

要求

尝试进行此配置之前，请确保符合远程客户端站点的以下这些要求：

- 启用了 SSL 的 Web 浏览器
- SUN Java JRE 1.4 版或更高版本
- 启用了 Cookie
- 禁用了弹出窗口阻止程序
- 本地管理权限（并非必需，但强烈建议）

注意：SUN Java JRE的最新版本可从Java网站免费下载。

使用的组件

本文档中的信息基于以下软件和硬件版本：

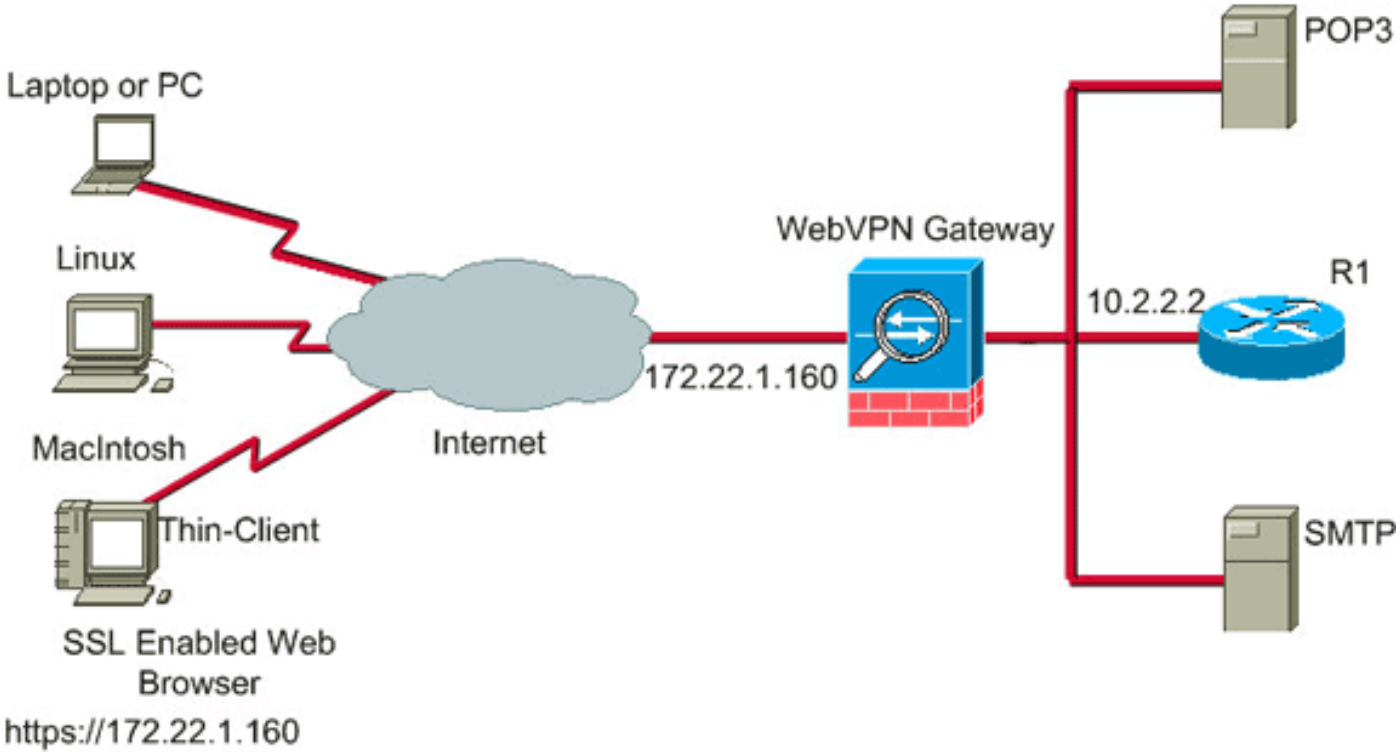
- Cisco 自适应安全设备 5510 系列
- Cisco 自适应安全设备管理器 (ASDM) 5.2(1)**注意：**请参阅允许ASDM的HTTPS访问，以便允许ASDM配置ASA。
- Cisco 自适应安全设备软件版本 7.2(1)
- Microsoft Windows XP Professional (SP 2) 远程客户端

本文档中的信息在实验室环境中形成。本文档中使用的所有设备都重置为其默认配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。此配置中使用的所有 IP 地址都是从实验室环境中的 RFC 1918 地址挑选而出的；这些 IP 地址在 Internet 上不可路由，仅做测试用途。

网络图

本文档使用此部分所述的网络配置。

远程客户端使用 ASA 启动会话时，客户端向工作站下载一个基于 Java 的小程序。为客户端提供了预先配置的资源的列表。



规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

背景信息

为了启动会话，远程客户端打开一个 SSL 浏览器，并进入 ASA 的外部接口。建立会话之后，用户可以使用在 ASA 上配置的参数调用任何 Telnet 或应用程序访问。ASA 作为安全连接的代理，允许用户访问设备。

注意： 不必对这些连接建立入站访问列表，因为 ASA 已了解构成合法会话的内容。

使用 ASDM 配置瘦客户端 SSL VPN

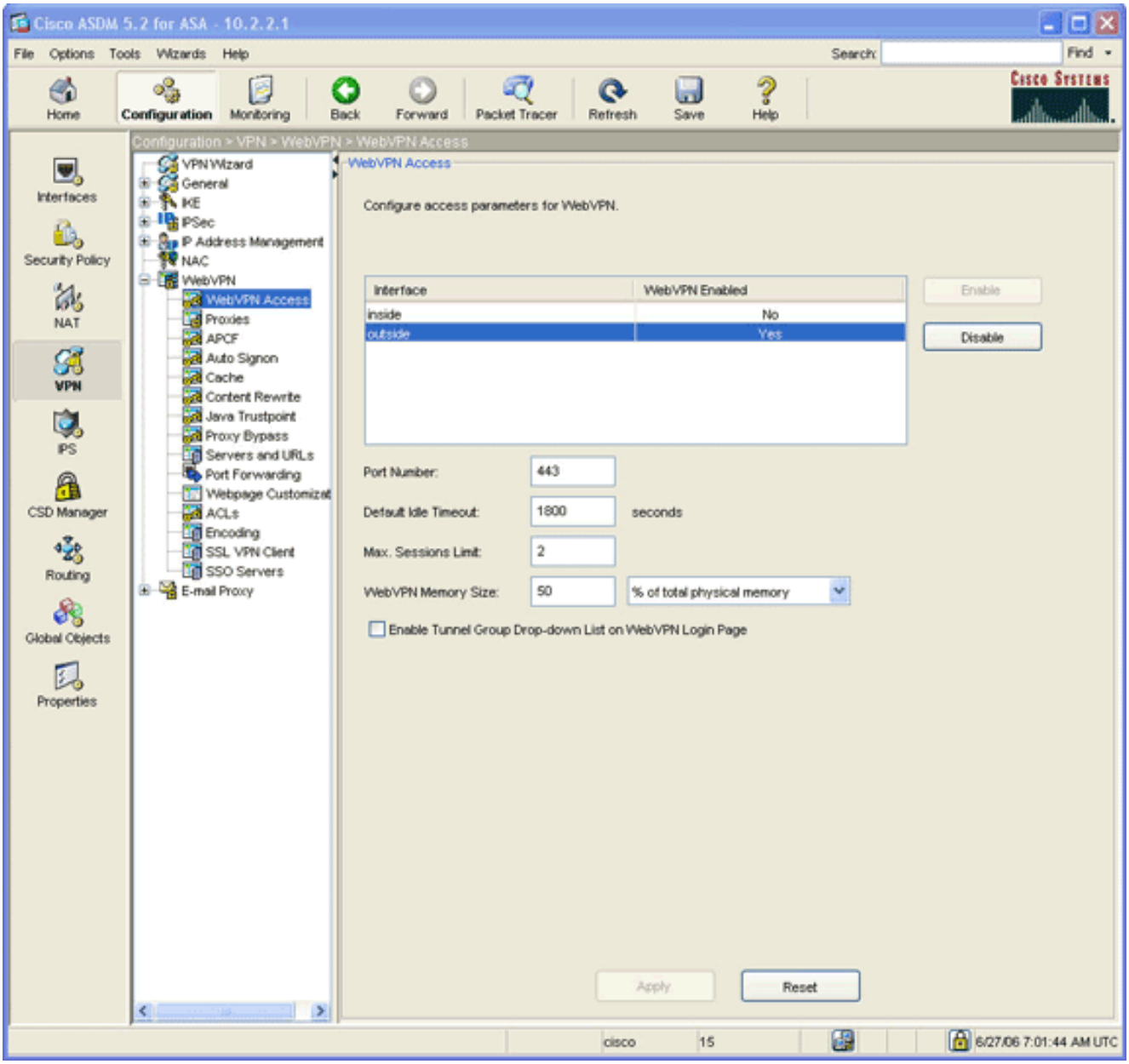
要在 ASA 上配置瘦客户端 SSL VPN，请完成以下这些步骤：

1. 在 ASA 上启用 WebVPN
2. 配置端口转发特性
3. 创建组策略并将其与端口转发列表关联（在第 2 步中创建端口转发列表）
4. 创建隧道组并将其与组策略关联（在第 3 步中创建组策略）
5. 创建用户并将该用户添加到组策略中（在第 3 步中创建组策略）

第 1 步. 在 ASA 上启用 WebVPN

要在 ASA 上启用 WebVPN，请完成以下这些步骤：

1. 在 ASDM 应用程序中，单击 **Configuration**，然后单击 VPN。
2. 展开 **WebVPN**，然后选择 WebVPN Access。

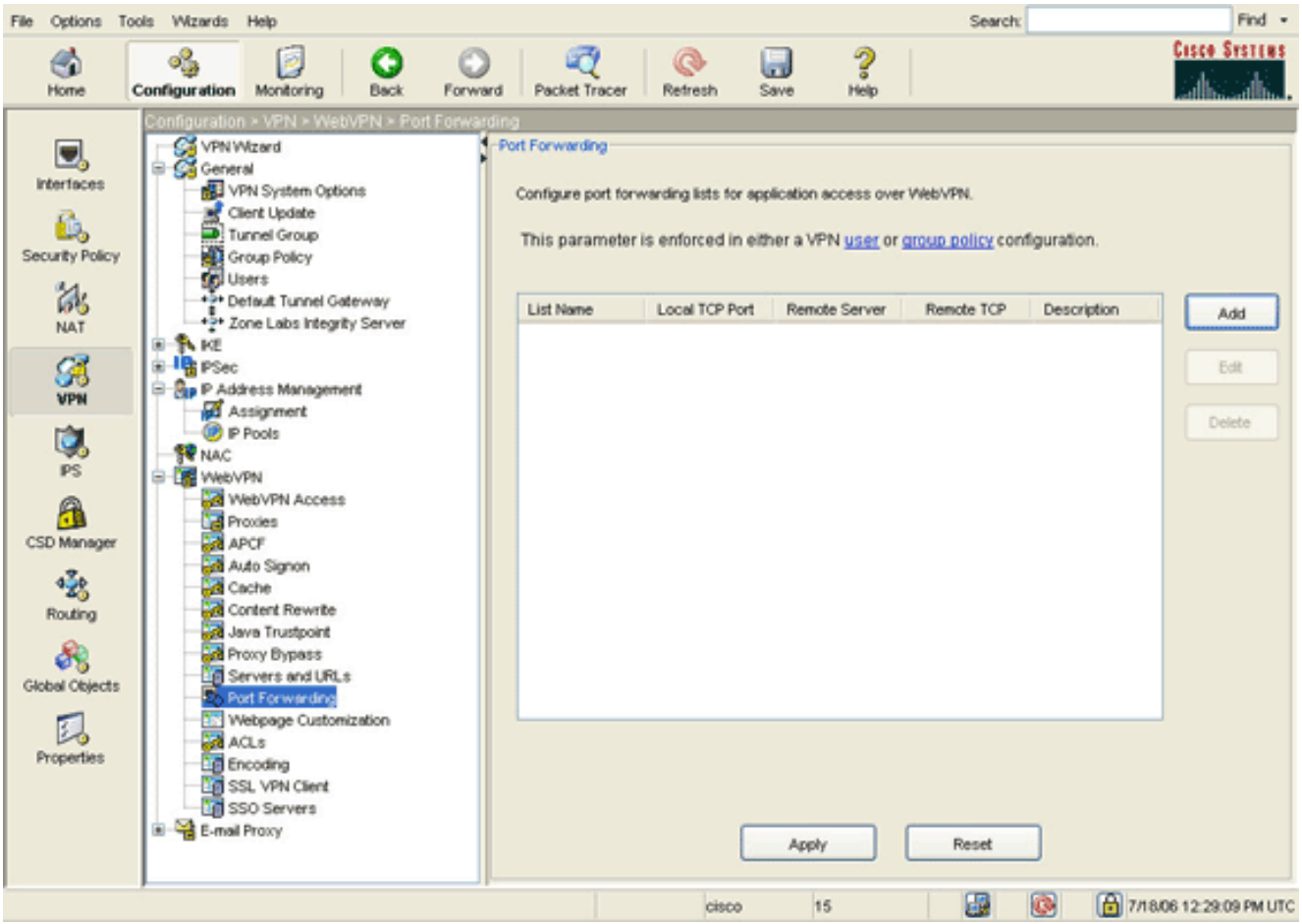


3. 突出显示接口，然后单击 **Enable**。
4. 单击 **Apply**，单击 Save，然后单击 Yes 接受更改。

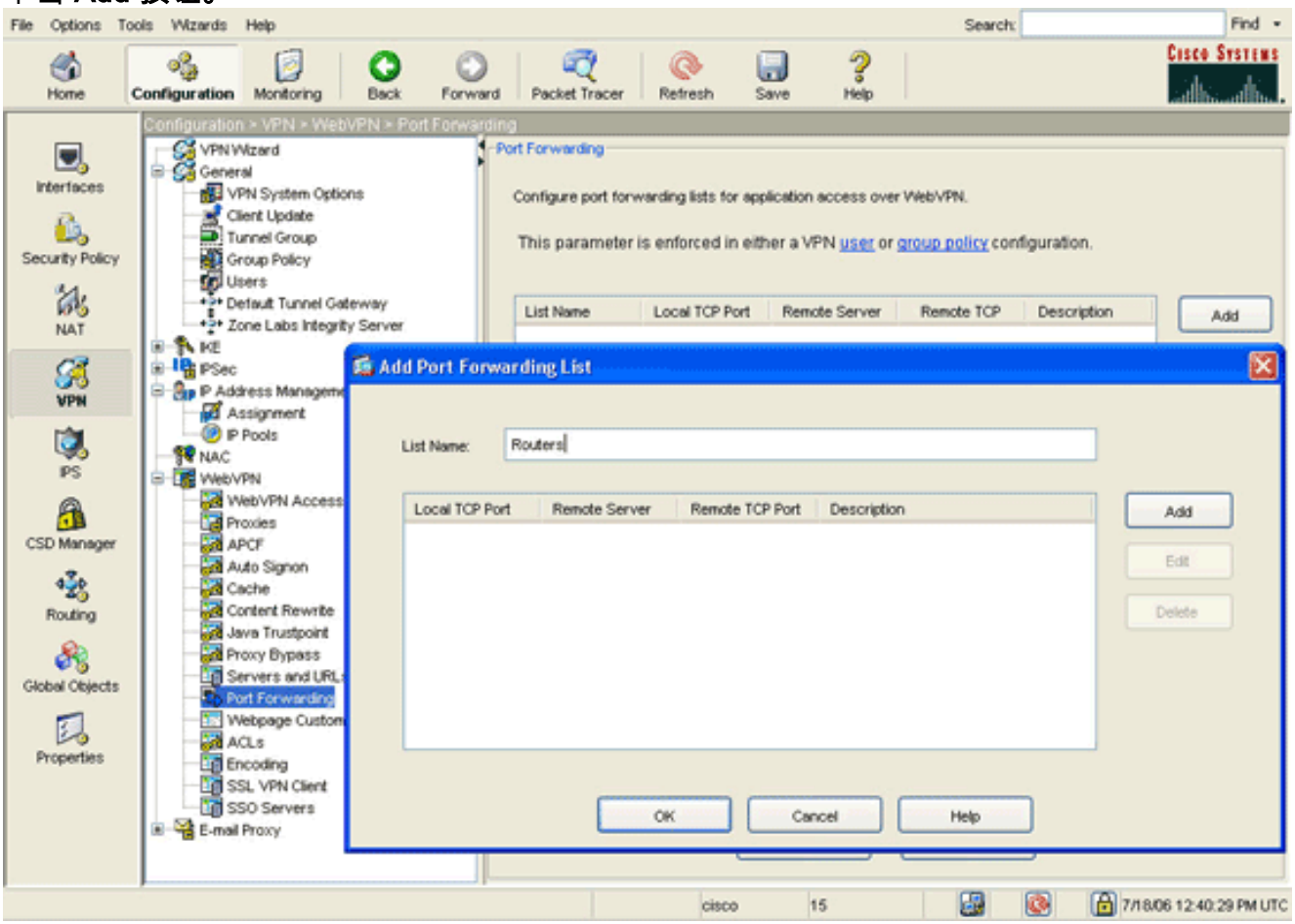
第 2 步. 配置端口转发特性

要配置端口转发特性，请完成以下这些步骤：

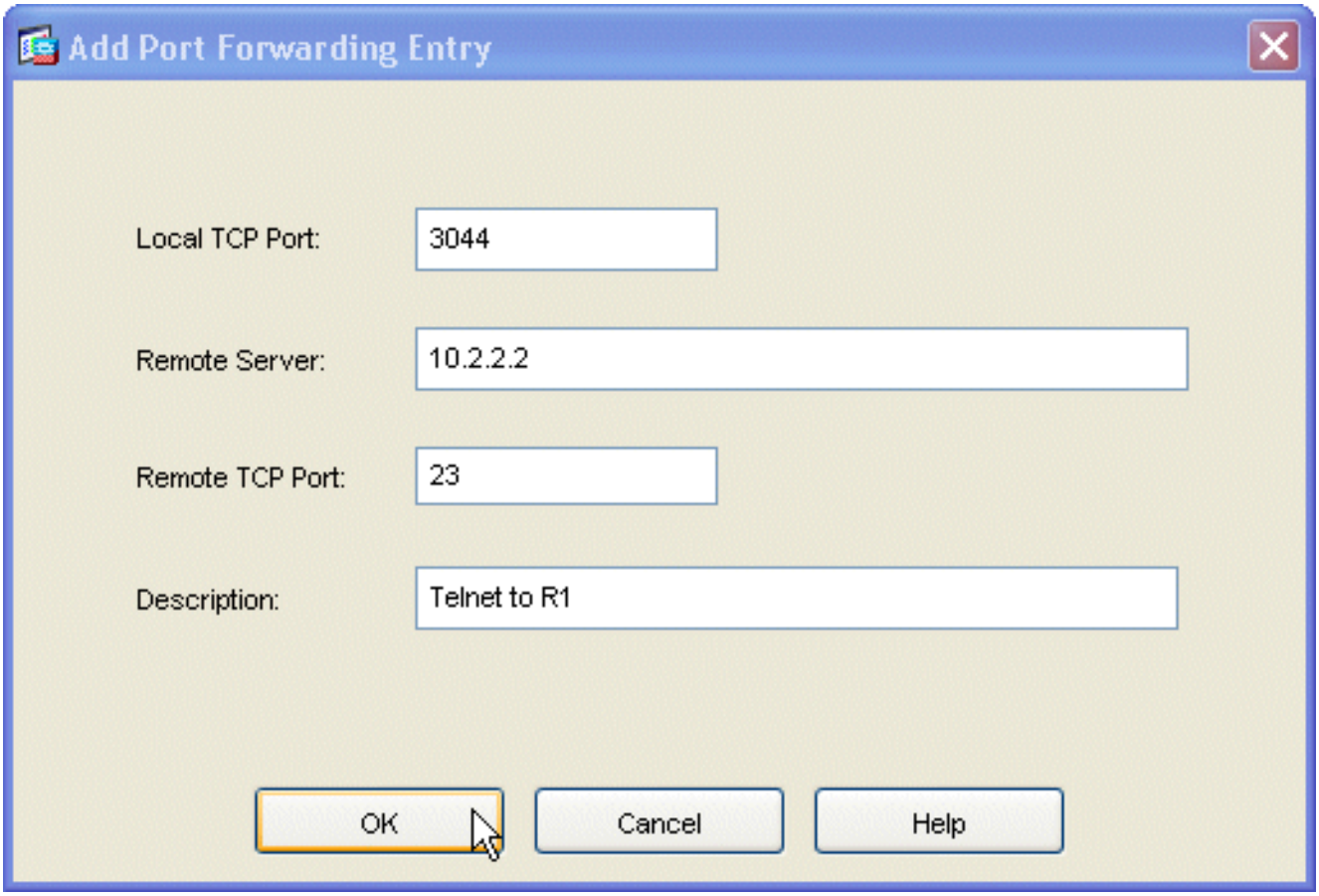
1. 展开 **WebVPN**，然后选择 Port Forwarding。



2. 单击 **Add 按钮。**



3. 在 Add Port Forwarding List 对话框中，输入列表名称，然后单击 **Add**。此时出现 Add Port Forwarding Entry 对话框。

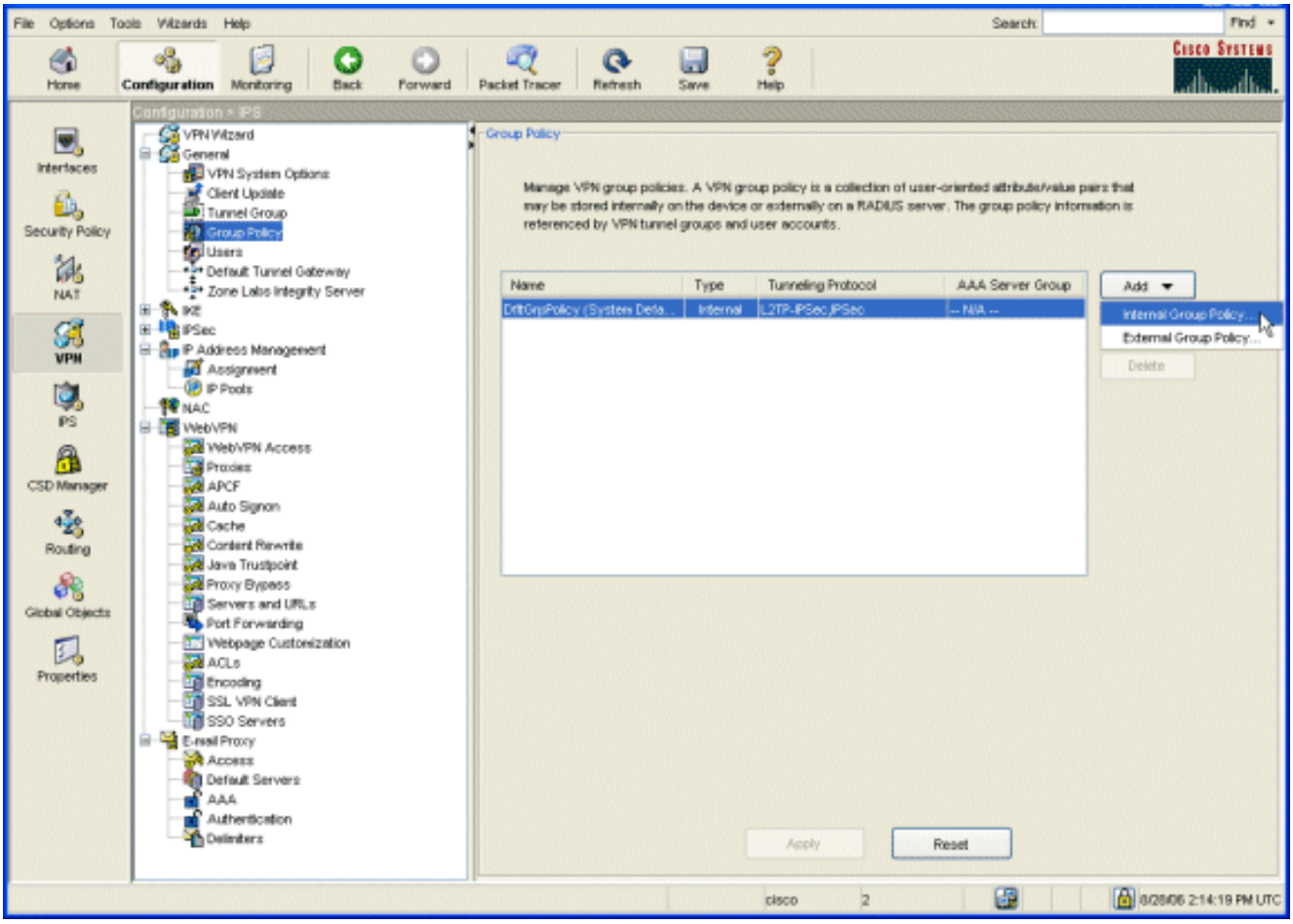


4. 在 Add Port Forwarding Entry 对话框中，输入以下这些选项：在 Local TCP Port 字段中，输入端口号或接受默认值。输入的值可以是从 1024 到 65535 的任何一个数字。在 Remote Server 字段中，输入 IP 地址。本示例使用路由器的地址。在 Remote TCP Port 字段中，输入端口号。本示例使用端口 23。在 Description 字段中，输入说明，然后单击 **OK**。
5. 单击 **OK**，然后单击 Apply。
6. 单击 **Save**，然后单击 Yes 接受更改。

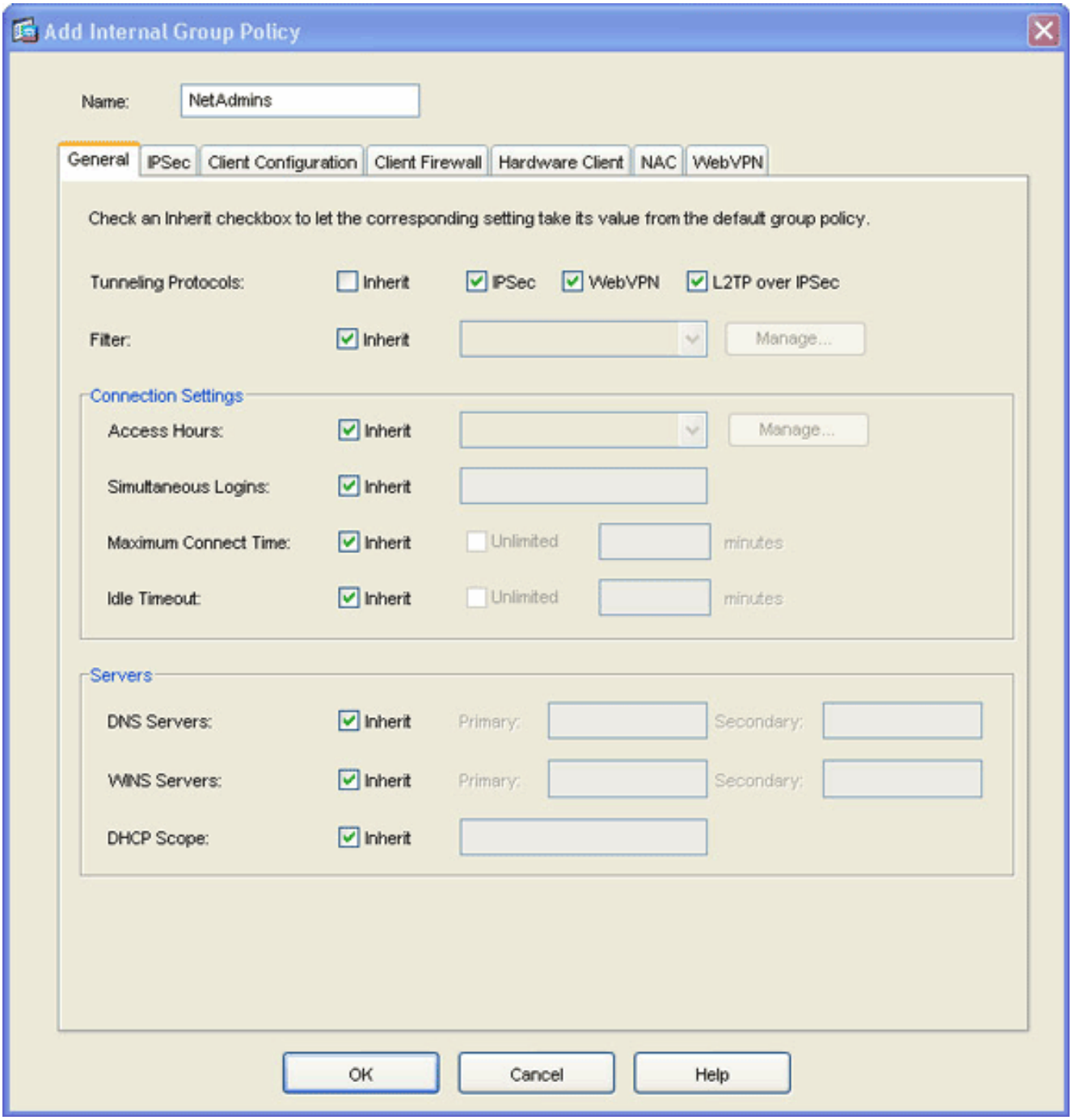
第 3 步. 创建组策略并将其与端口转发列表链接

要创建组策略并将其与端口转发列表链接，请完成以下这些步骤：

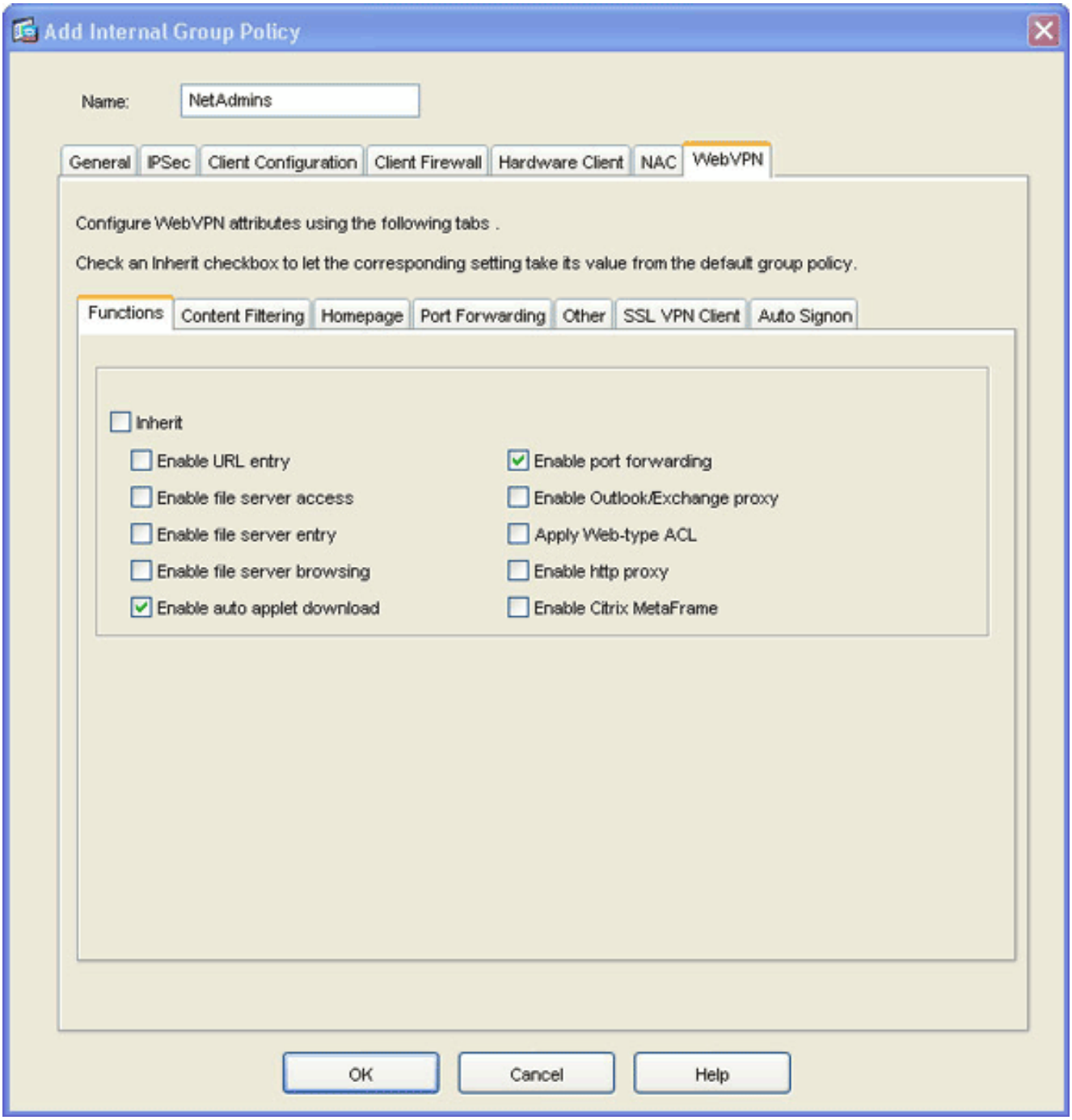
1. 展开 **General**，然后选择 Group Policy。



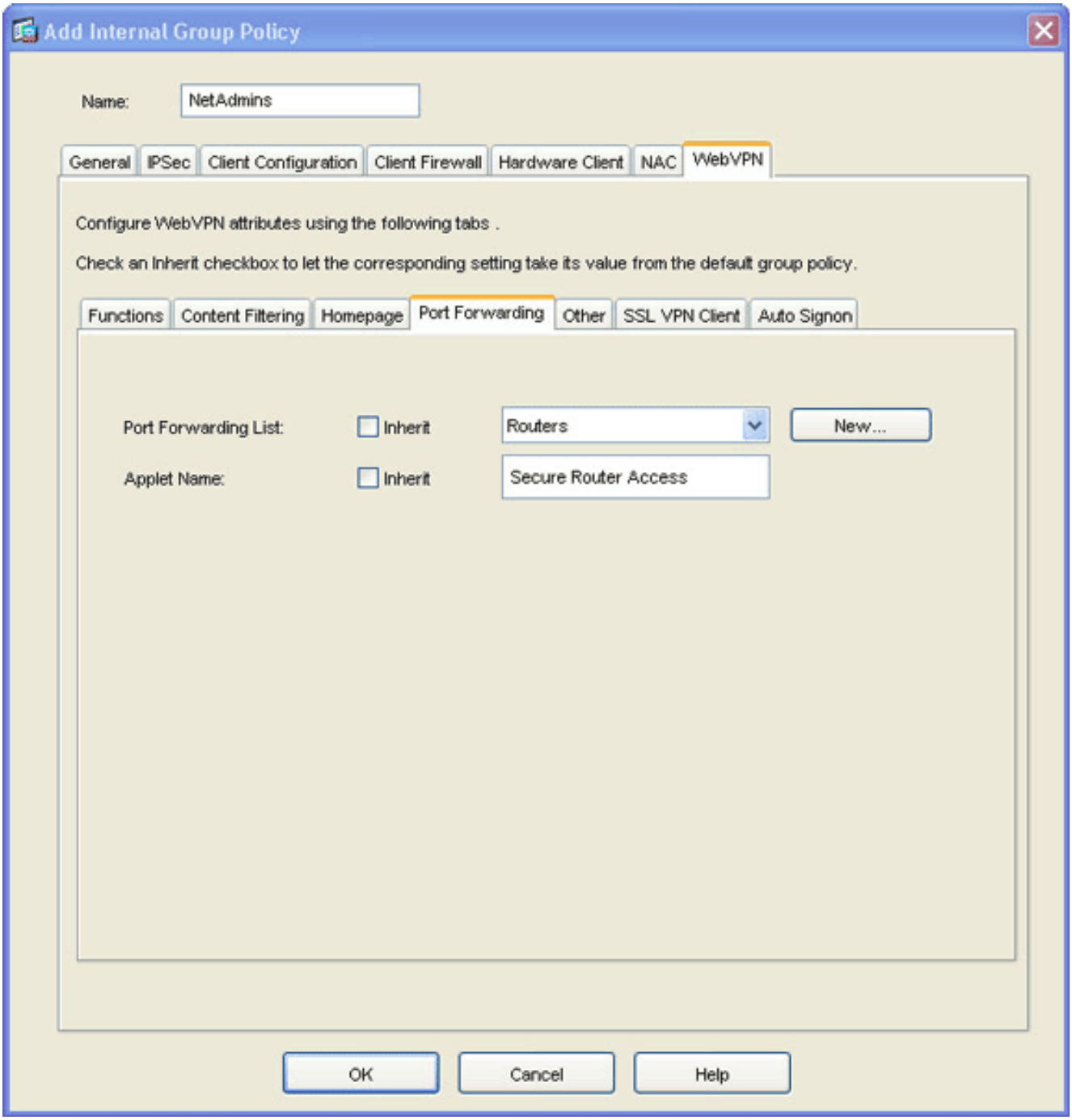
2. 单击 **Add**，然后选择 Internal Group Policy。此时出现 Add Internal Group Policy 对话框。



3. 输入名称或接受默认组策略名称。
4. 取消选中 Tunneling Protocols 的 **Inherit** 复选框，然后选中 WebVPN 复选框。
5. 单击位于对话框顶部的 **WebVPN 选项卡，然后单击 Functions 选项卡。**
6. 取消选中 **Inherit 复选框，然后选中 Enable auto applet download 和 Enable port forwarding 复选框，如下图所示**
   ：



7. 此外，在 WebVPN 选项卡中，单击 **Port Forwarding 选项卡，然后取消选中 Port Forwarding List 的 Inherit 复选框。**



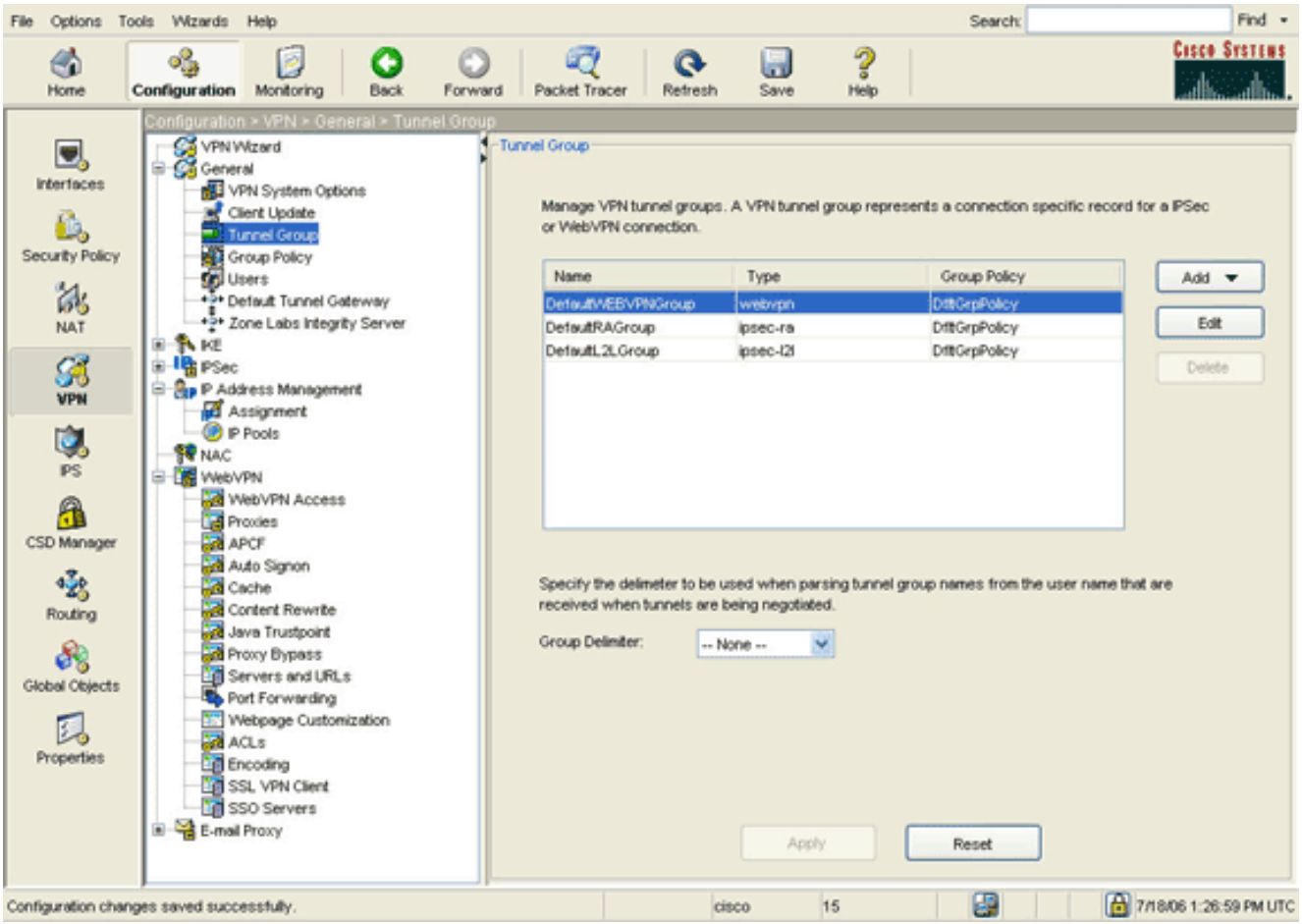
8. 单击 **Port Forwarding List 下拉箭头，然后选择在**第 2 步中创建的端口转发列表。
9. 取消选中 Applet Name 的 **Inherit 复选框，然后更改文本字段中的名称。**客户端将在连接上显示该小程序名称。
10. 单击 **OK**，然后单击 Apply。
11. 单击 **Save**，然后单击 Yes 接受更改。

第 4 步. 创建隧道组并将其与组策略链接

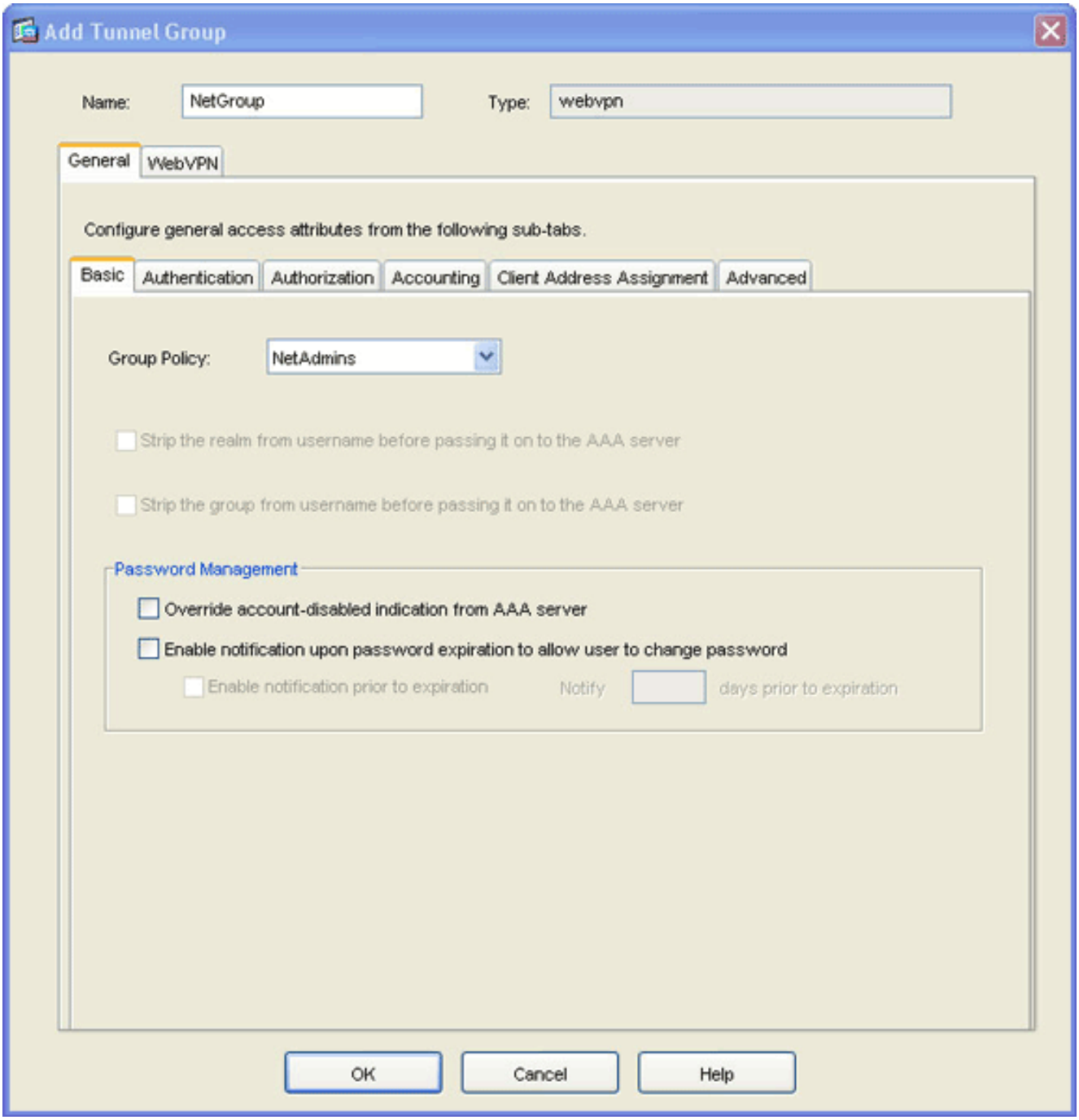
可以编辑默认的 *DefaultWebVPNGroup 隧道组或创建新隧道组。*

要创建新隧道组，请完成以下这些步骤：

1. 展开 **General**，然后选择 Tunnel Group。



2. 单击 **Add**，然后选择 WebVPN Access。此时出现 Add Tunnel Group 对话框。

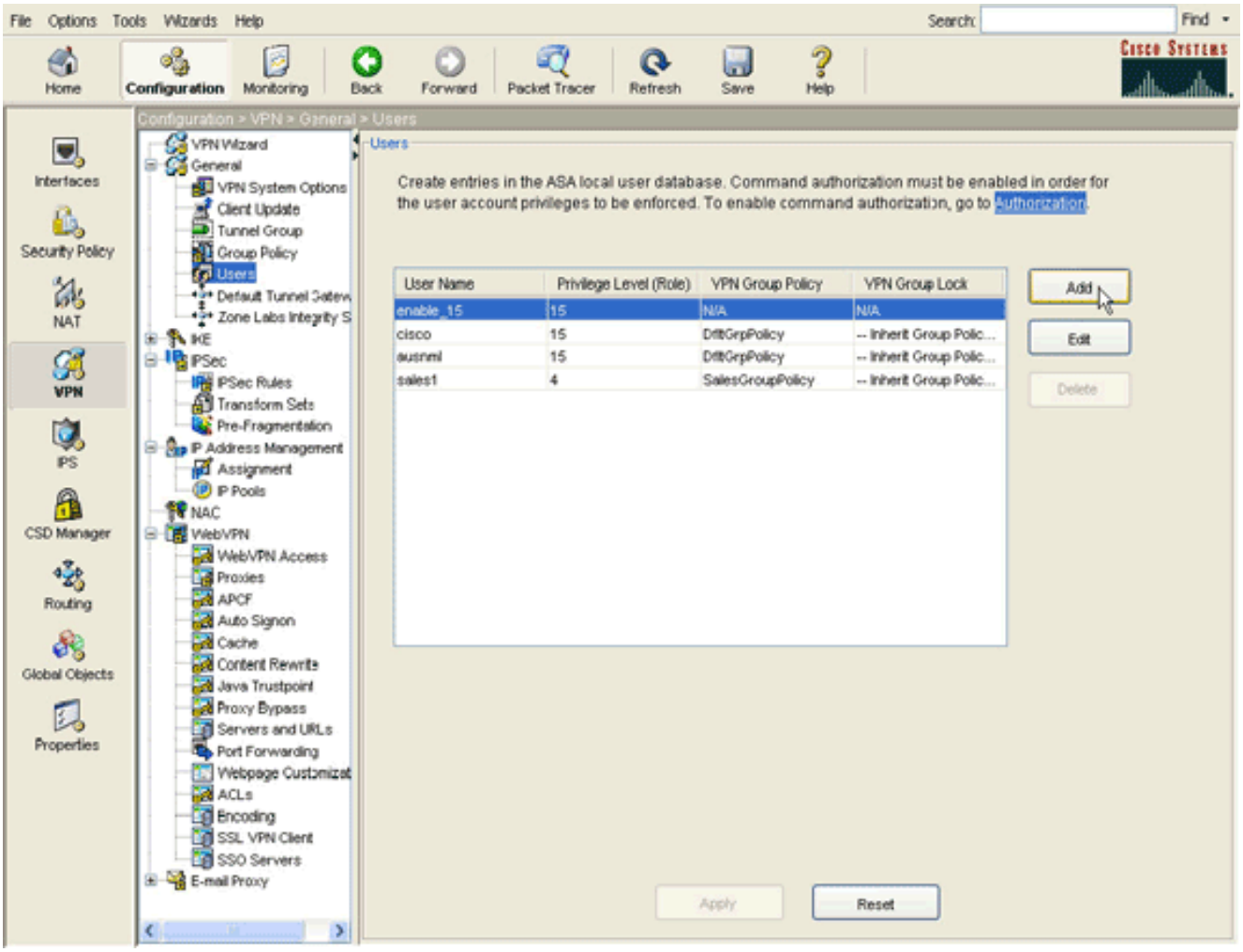


3. 在 Name 字段中输入名称。
4. 单击 **Group Policy 下拉箭头，然后选择在**第 3 步中创建的组策略。
5. 单击 **OK**，然后单击 Apply。
6. 单击 **Save**，然后单击 Yes 接受更改。现在隧道组、组策略和端口转发特性即相关联。

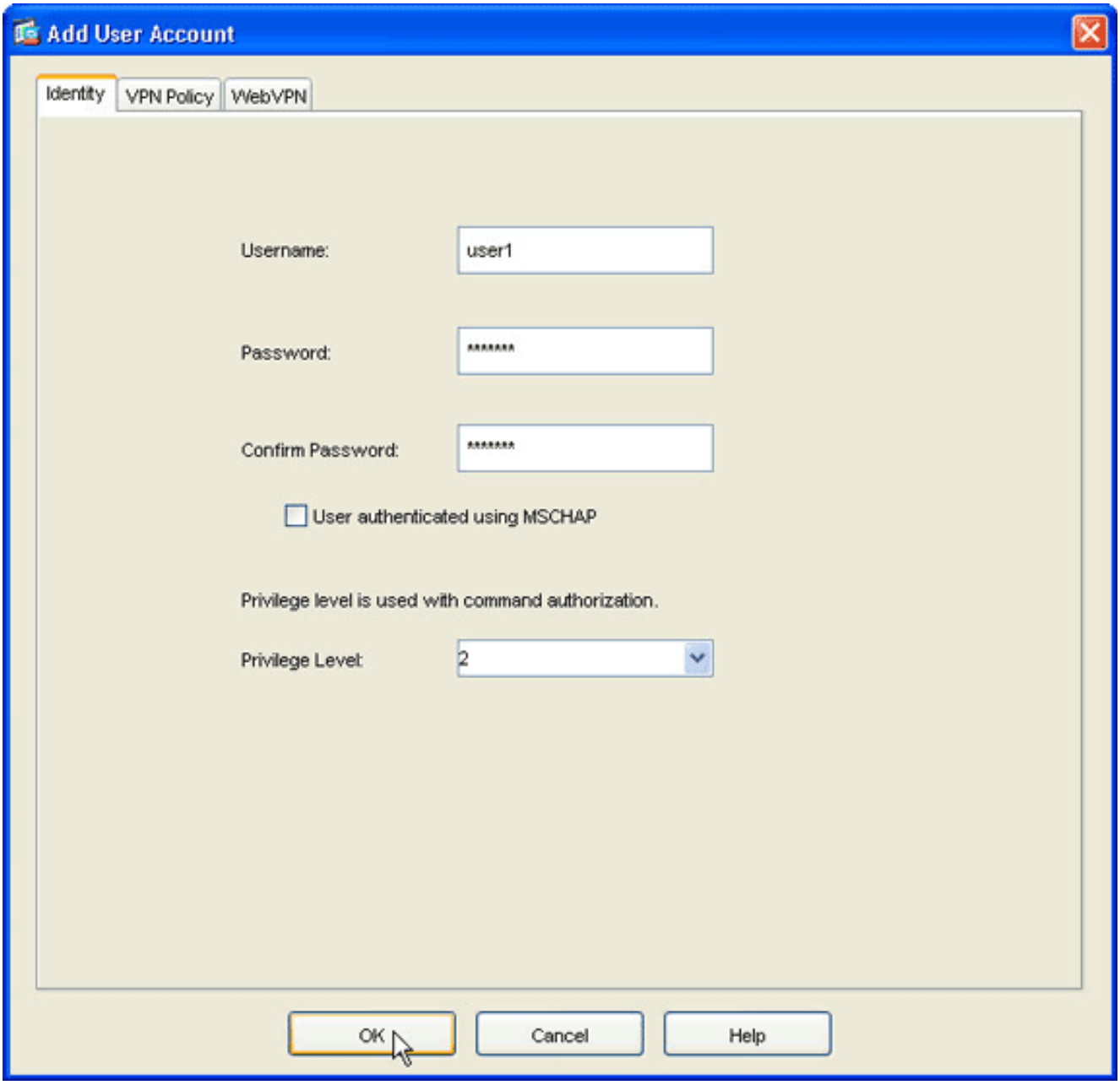
第 5 步. 创建用户并将该用户添加到组策略中

要创建用户并将该用户添加到组策略中，请完成以下这些步骤：

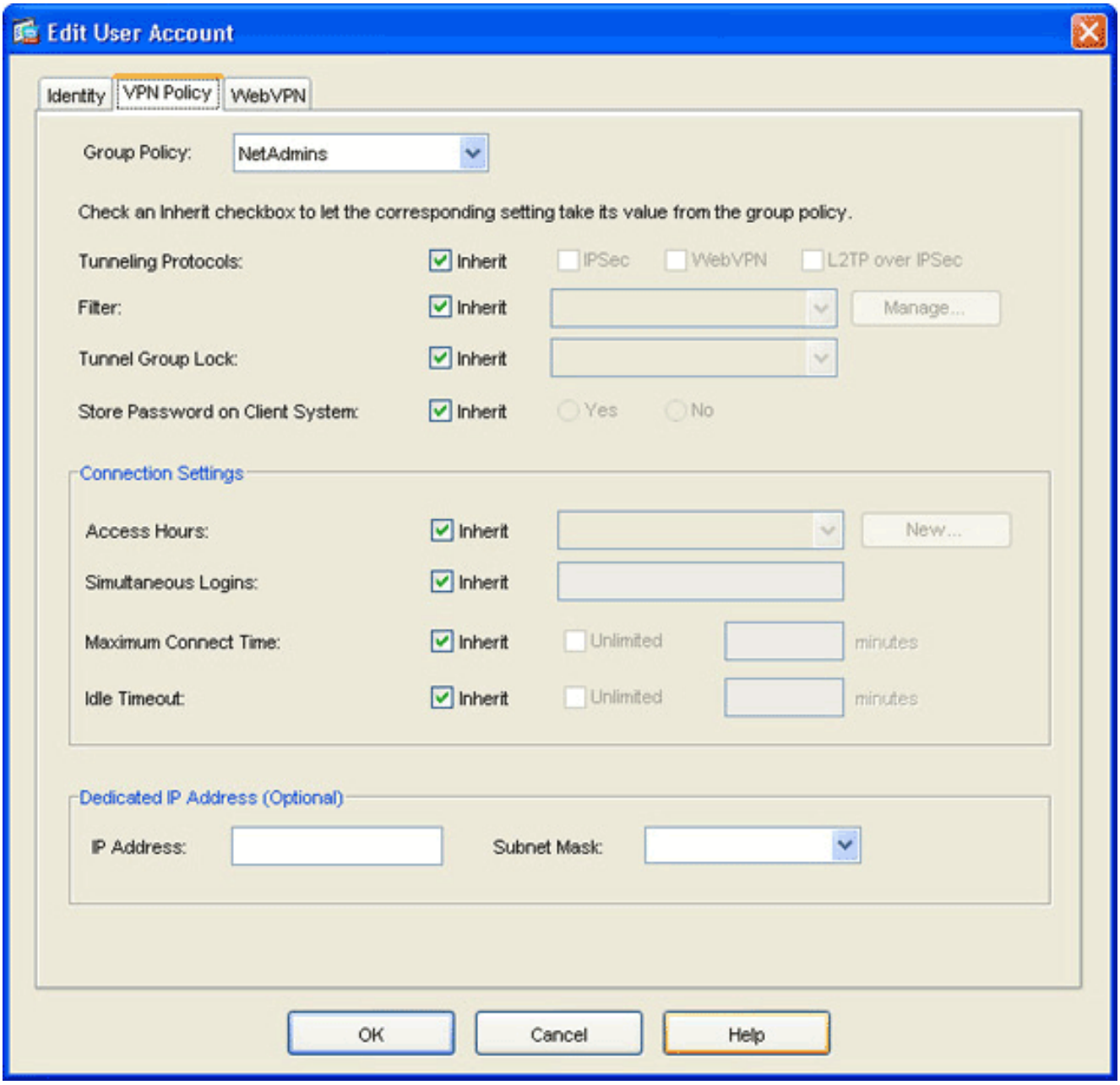
1. 展开 **General**，然后选择 Users。



2. 单击 **Add 按钮。**此时出现 Add User Account 对话框。



3. 输入用户名、口令和权限信息的值，然后单击 **VPN Policy 选项卡。**



4. 单击 **Group Policy 下拉箭头，然后选择在**第 3 步中创建的组策略。此用户将继承所选组策略的 WebVPN 特性和策略。
5. 单击 **OK**，然后单击 Apply。
6. 单击 **Save**，然后单击 Yes 接受更改。

使用 CLI 配置瘦客户端 SSL VPN

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
```

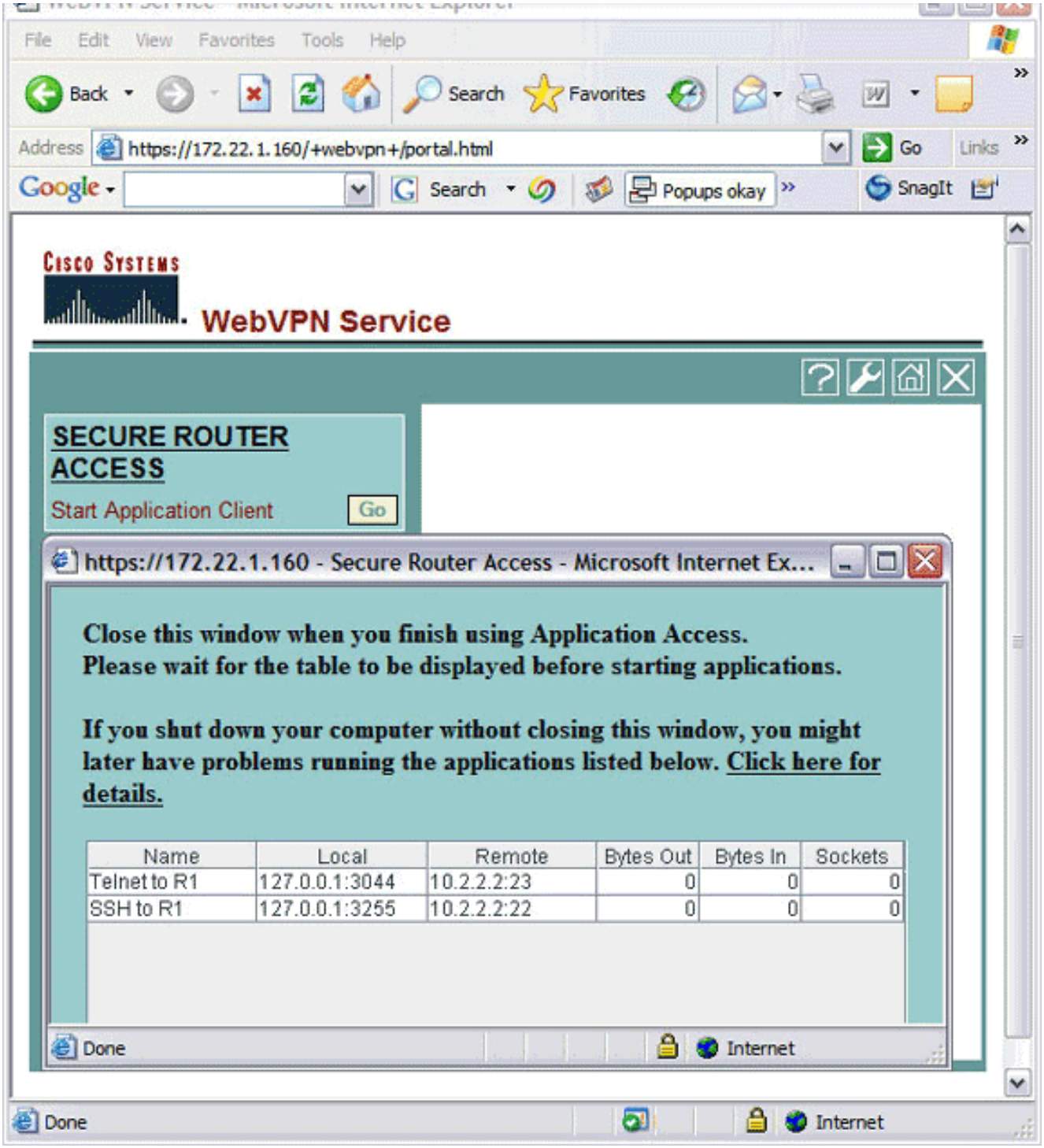
验证

使用本部分可确认配置能否正常运行。

步骤

本过程介绍如何确定配置的有效性以及如何测试配置。

1. 从客户端工作站中，输入 **https://outside_ASA_IP Address**；其中 *outside_ASA_IP Address 是 ASA 的 SSL URL*。接受数字证书，并验证用户身份后，将出现 WebVPN Service 网页。

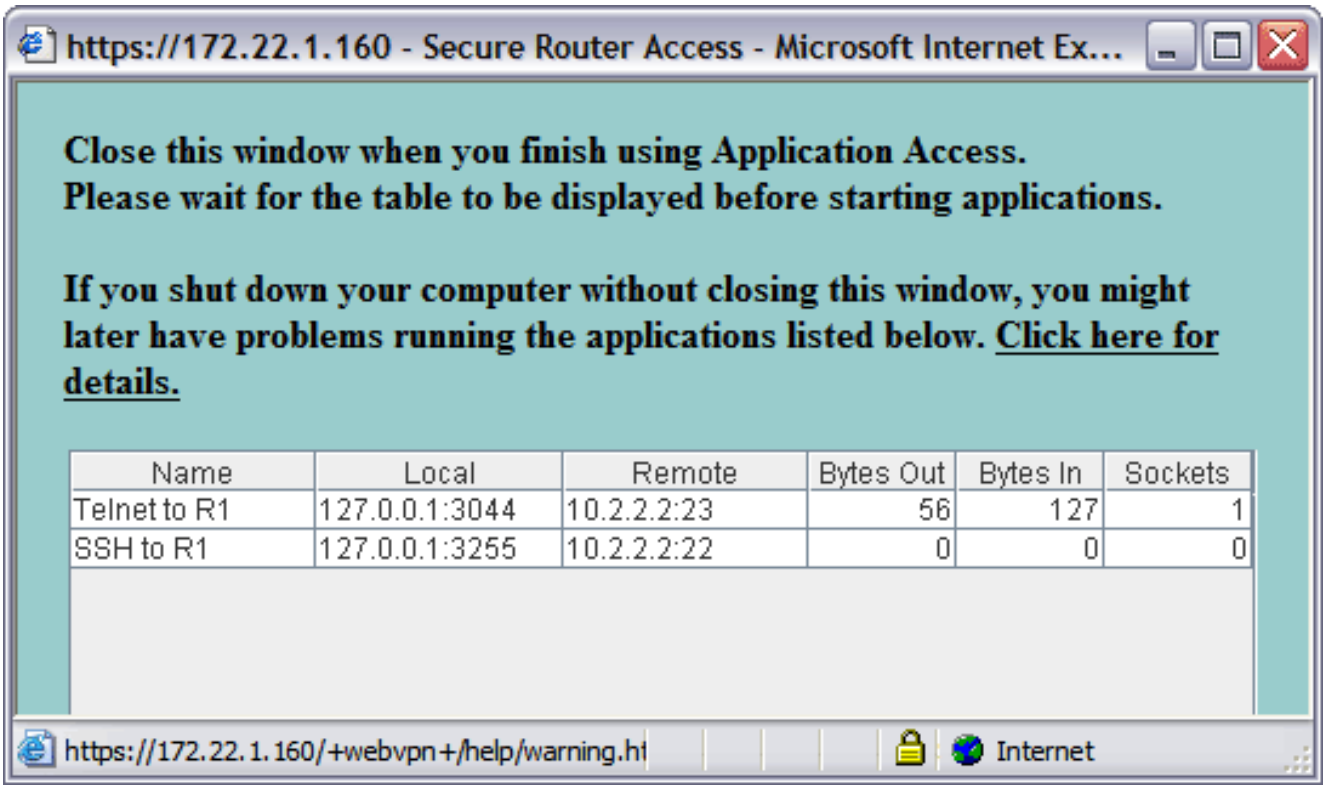


Local 列中显示访问应用程序所需的地址和端口信息。Bytes Out 和 Bytes In 列不显示任何活动，因为此时尚未调用应用程序。

2. 使用 DOS 提示符或其他 Telnet 应用程序启动 Telnet 会话。
3. 在命令提示符下，输入 **telnet 127.0.0.1 3044**。**注意**：此命令提供了如何访问本文档中WebVPN服务网页图像中显示的本地端口的示例。*命令不含冒号 (:)*。 键入本文档中所述的命令。ASA 通过安全会话接收命令，并且由于它存储信息的映射，因此 ASA 立即了解要打开安全 Telnet 会话，连接所映射的设备。

输入用户名和口令后，即完成对设备的访问。

4. 要验证对设备的访问，请检查 Bytes Out 和 Bytes In 列，如下图所示：



命令

有若干 **show 命令与 WebVPN 关联。**可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其他信息。有关 **show 命令的详细信息，请参阅**验证 WebVPN 配置。

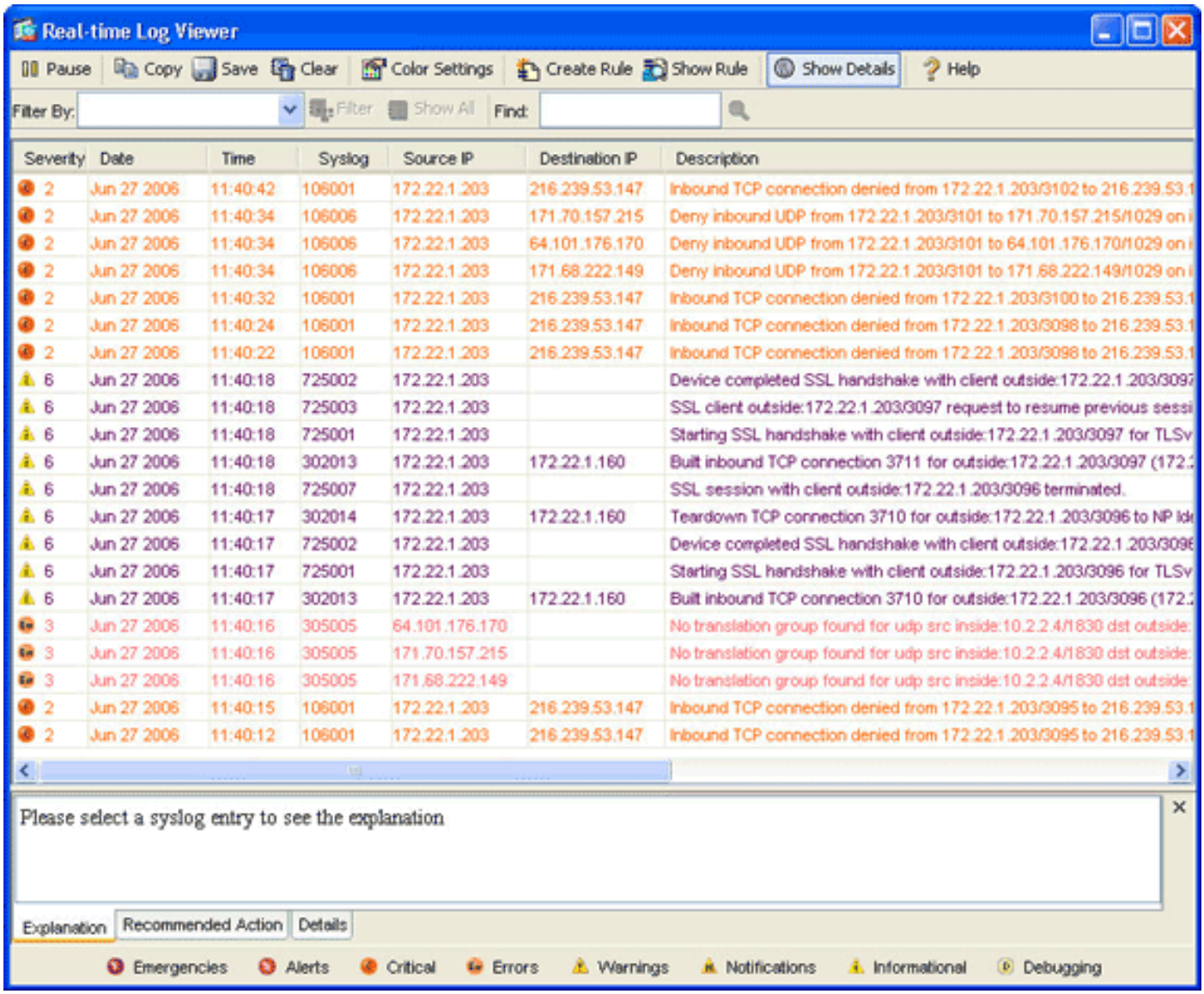
注意：输出解释器工具(仅注册客户)(OIT)支持某些**show**命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

使用本部分可排除配置故障。

SSL 握手过程是否完成？

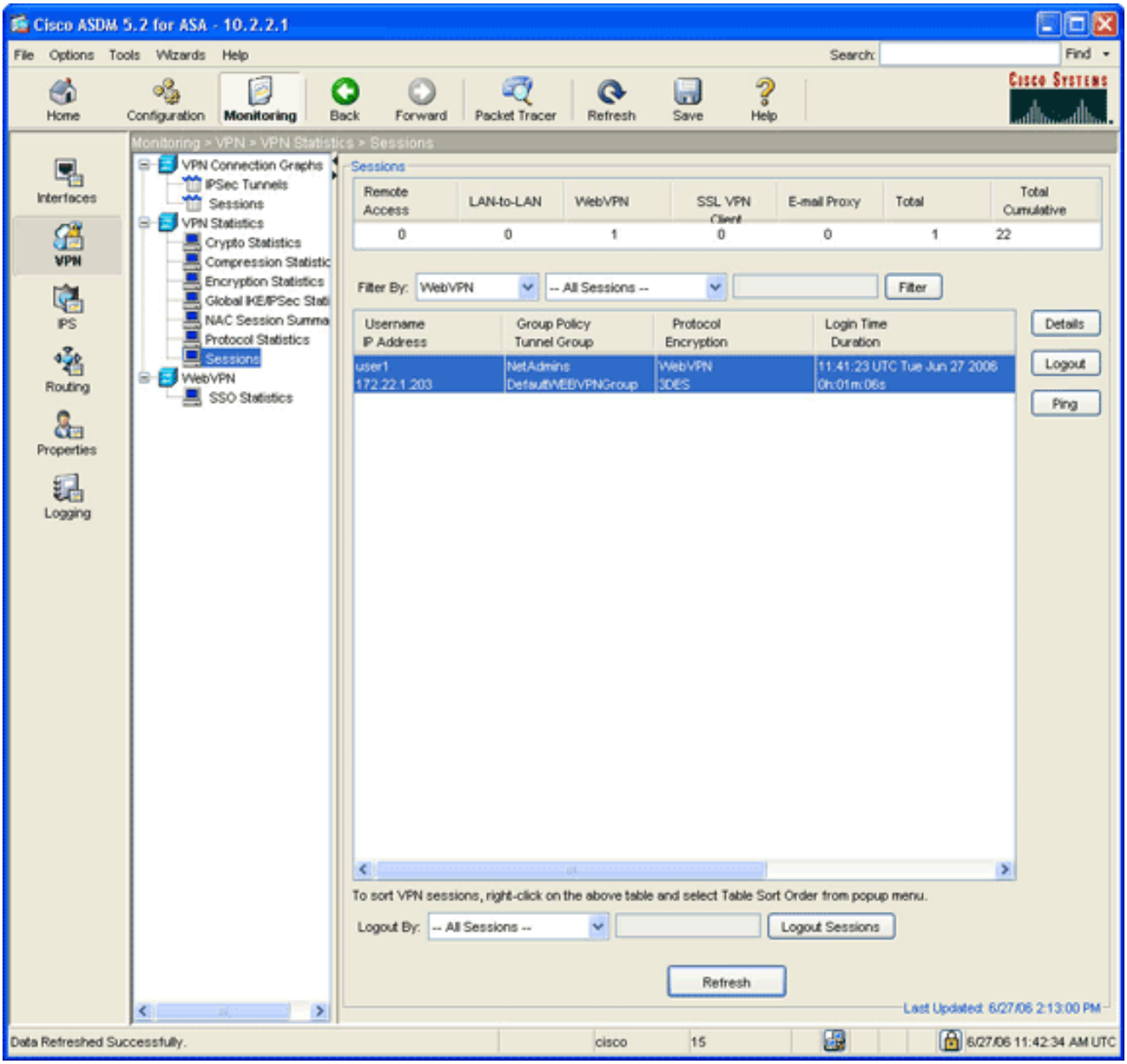
连接到 ASA 后，请检查实时日志是否显示 SSL 握手完成。



SSL VPN 瘦客户端是否运行正常？

要验证 SSL VPN 瘦客户端是否运行正常，请完成以下这些步骤：

1. 单击 **Monitoring**，然后单击 VPN。
2. 展开 **VPN Statistics**，然后单击 Sessions。会话列表中应显示 SSL VPN 瘦客户端会话。确保按 WebVPN 过滤，如下图所示
   ：



命令

有若干 **debug 命令与 WebVPN 关联。**有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。

注意：使用debug命令可能会对Cisco设备造成负面影响。使用 debug 命令之前，请参阅**有关 Debug 命令的重要信息。**

相关信息

- ASA 上的无客户端 SSL VPN (WebVPN) 配置示例
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- Cisco ASA 5500 系列自适应安全设备
- 使用 ASDM 和 NTLMv1 配置具有 WebVPN 和单点登录的 ASA 示例
- 技术支持和文档 - Cisco Systems