Beispiel einer Thin-Client SSL VPN (WebVPN)-Konfiguration für ASA mit ASDM

Inhalt

Einführung

Die Thin-Client SSL VPN-Technologie ermöglicht den sicheren Zugriff für einige Anwendungen mit statischen Ports, z. B. Telnet(23), SSH(22), POP3(110), IMAP4(143) und SMTP(25). Sie können das Thin-Client SSL VPN als benutzergesteuerte Anwendung, richtliniengesteuerte Anwendung oder beides verwenden. Das heißt, Sie können den Zugriff auf Benutzerbasis konfigurieren oder Gruppenrichtlinien erstellen, in denen Sie einen oder mehrere Benutzer hinzufügen.

- **Clientless SSL VPN (WebVPN)** - Stellt einen Remote-Client bereit, der einen SSL-fähigen Webbrowser für den Zugriff auf HTTP- oder HTTPS-Webserver in einem lokalen Unternehmensnetzwerk (LAN) benötigt. Darüber hinaus bietet Clientless-SSL-VPN Zugriff für das Durchsuchen von Windows-Dateien über das Common Internet File System (CIFS)-Protokoll. Outlook Web Access (OWA) ist ein Beispiel für den HTTP-Zugriff.Weitere Informationen zum Clientless-SSL-VPN (WebVPN) finden Sie im Konfigurationsbeispiel der

ASA.

- **Thin-Client SSL VPN (Port Forwarding)** - Bietet einen Remote-Client, der ein kleines, Java-basiertes Applet herunterlädt und sicheren Zugriff für TCP-Anwendungen (Transmission Control Protocol) ermöglicht, die statische Portnummern verwenden. Beispiele für sicheren Zugriff sind das Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Secure Shell (SSH) und Telnet. Da sich Dateien auf dem lokalen Computer ändern, müssen Benutzer über lokale Administratorberechtigungen verfügen, um diese Methode verwenden zu können. Diese SSL VPN-Methode funktioniert nicht mit Anwendungen, die dynamische Portzuweisungen verwenden, wie z. B. einige FTP-Anwendungen (File Transfer Protocol).**Hinweis:** User Datagram Protocol (UDP) wird nicht unterstützt.
- **SSL VPN Client (Tunnel-Modus)**: Lädt einen kleinen Client zur Remote-Workstation herunter und ermöglicht einen vollständigen sicheren Zugriff auf Ressourcen in einem internen Unternehmensnetzwerk. Sie können den SSL VPN Client (SVC) dauerhaft auf eine Remote-Workstation herunterladen oder den Client entfernen, wenn die sichere Sitzung beendet ist.Weitere Informationen zum SSL VPN-Client finden Sie unter SSL VPN Client (SVC) auf ASA mit ASDM Configuration Example.

Dieses Dokument zeigt eine einfache Konfiguration für das Thin-Client SSL VPN auf der Adaptive Security Appliance (ASA). Die Konfiguration ermöglicht es Benutzern, sicher Telnet zu einem Router in der ASA zu übertragen. Die Konfiguration in diesem Dokument wird für ASA 7.x und höher unterstützt.

Voraussetzungen

Anforderungen

Bevor Sie diese Konfiguration versuchen, stellen Sie sicher, dass Sie die folgenden Anforderungen für die Remote-Client-Stationen erfüllen:

- SSL-fähiger Webbrowser
- SUN Java JRE Version 1.4 oder höher
- Cookies aktiviert
- Popup-Blocker deaktiviert
- Lokale Administratorrechte (nicht erforderlich, aber dringend empfohlen)

Hinweis: Die neueste Version der SUN Java JRE steht als kostenloser Download von der Java-Website zur Verfügung.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

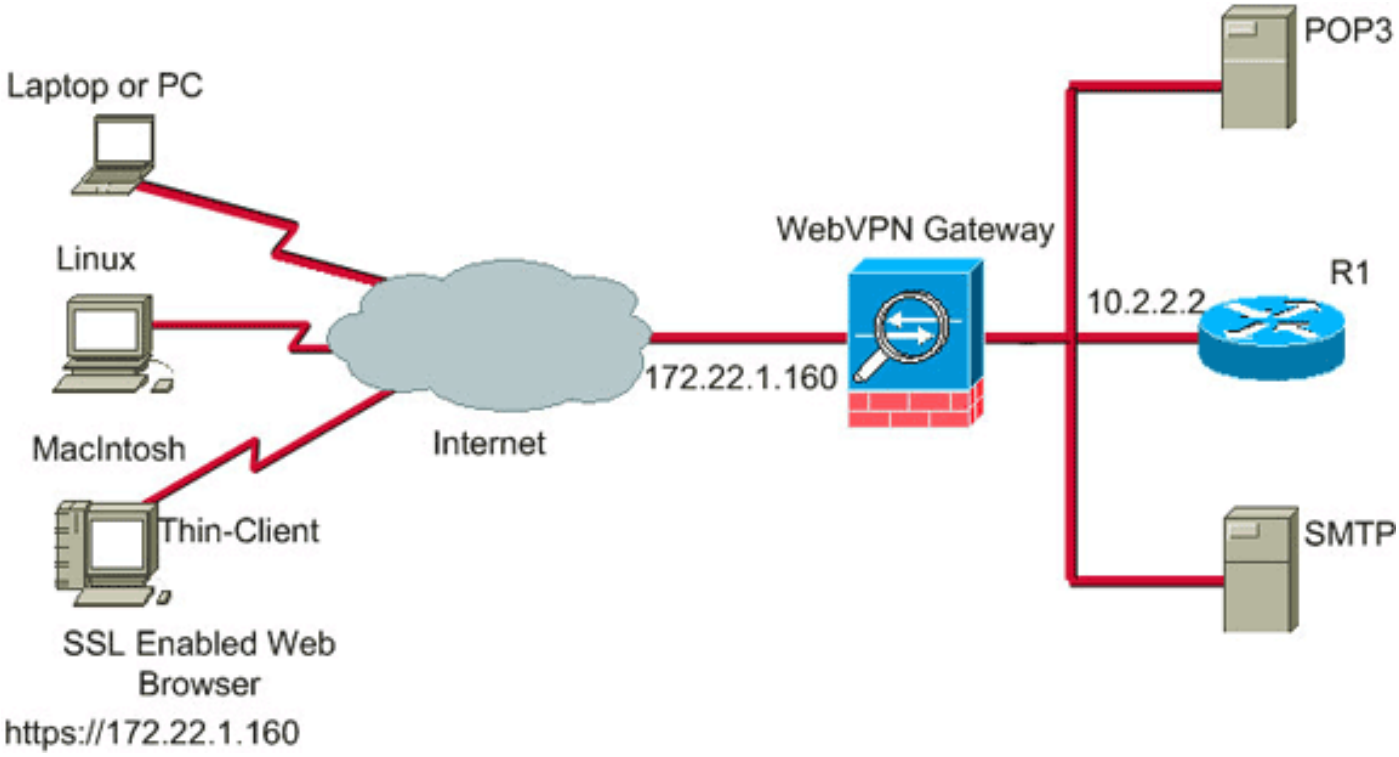
- Cisco Adaptive Security Appliance der Serie 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Hinweis:** Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.
- Cisco Adaptive Security Appliance Software Version 7.2(1)
- Remote-Client Microsoft Windows XP Professional (SP 2)

Die Informationen in diesem Dokument wurden in einer Laborumgebung entwickelt. Alle in diesem Dokument verwendeten Geräte wurden auf ihre Standardkonfiguration zurückgesetzt. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen. Alle in dieser Konfiguration verwendeten IP-Adressen wurden in einer Laborumgebung aus RFC 1918-Adressen ausgewählt. Diese IP-Adressen sind nicht im Internet routbar und dienen nur zu Testzwecken.

Netzwerkdiagramm

In diesem Dokument wird die in diesem Abschnitt beschriebene Netzwerkkonfiguration verwendet.

Wenn ein Remote-Client eine Sitzung mit der ASA initiiert, lädt der Client ein kleines Java-Applet auf die Workstation. Dem Client wird eine Liste vorkonfigurierter Ressourcen angezeigt.



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen

Um eine Sitzung zu starten, öffnet der Remote-Client einen SSL-Browser zur externen Schnittstelle der ASA. Nach Einrichtung der Sitzung kann der Benutzer die auf der ASA konfigurierten Parameter verwenden, um Telnet- oder Anwendungszugriff aufzurufen. Die ASA stellt die sichere Verbindung her und ermöglicht dem Benutzer den Zugriff auf das Gerät.

Hinweis: Eingehende Zugriffslisten sind für diese Verbindungen nicht erforderlich, da die ASA bereits weiß, was eine rechtliche Sitzung darstellt.

SSL-VPN-Konfiguration mit Thin-Client unter Verwendung von

ASDM

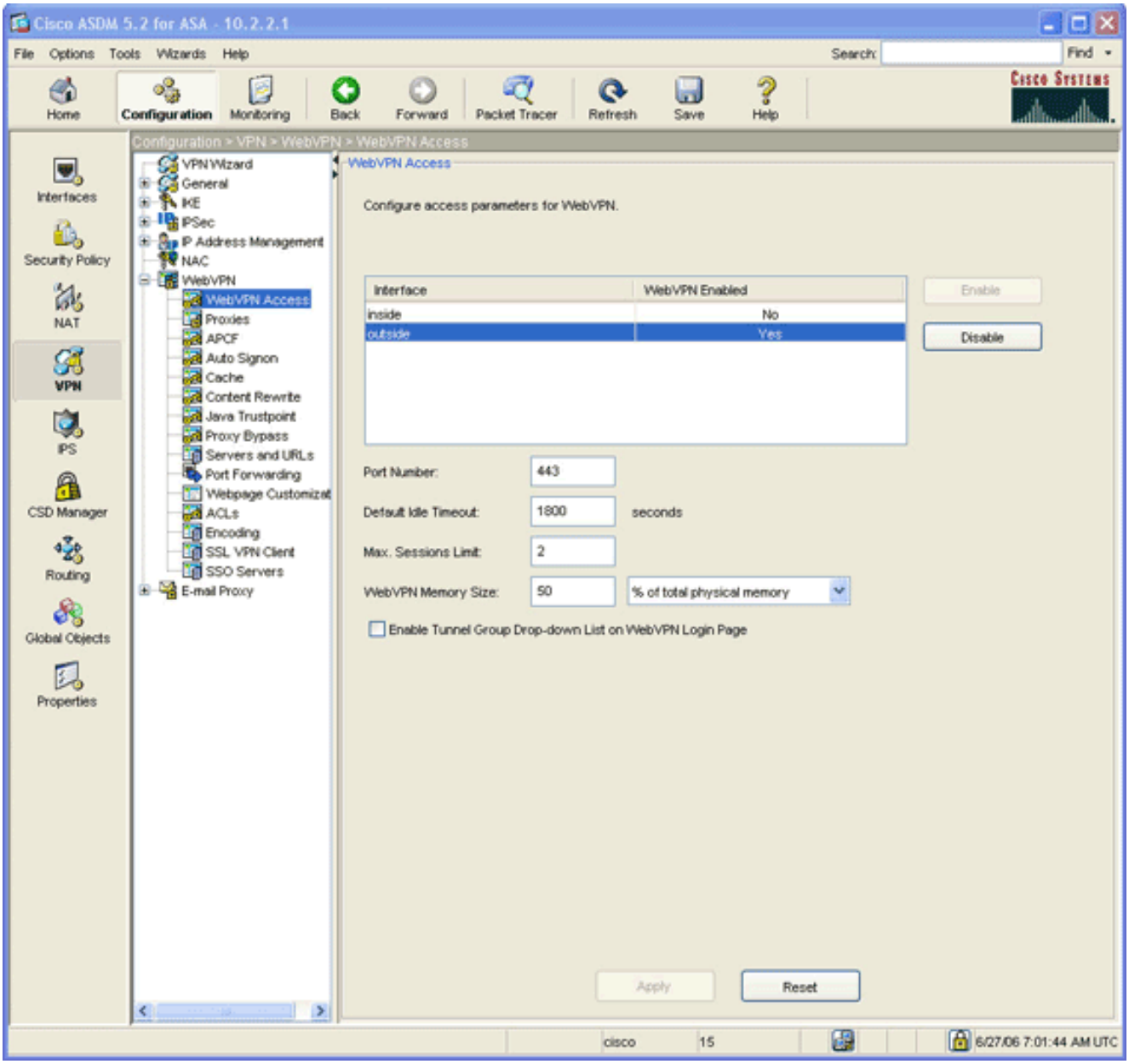
Gehen Sie wie folgt vor, um Thin-Client SSL VPN auf der ASA zu konfigurieren:

1. Aktivierung von WebVPN auf der ASA
2. Konfigurieren von Port Forwarding-Eigenschaften
3. Erstellen einer Gruppenrichtlinie und Verknüpfen Sie diese mit der Portweiterleitungsliste (erstellt in Schritt 2)
4. Erstellen einer Tunnelgruppe und Verknüpfen Sie diese mit der Gruppenrichtlinie (erstellt in Schritt 3)
5. Erstellen eines Benutzers und Hinzufügen dieses Benutzers zur Gruppenrichtlinie (erstellt in Schritt 3)

Schritt 1: Aktivierung von WebVPN auf der ASA

Gehen Sie wie folgt vor, um WebVPN auf der ASA zu aktivieren:

1. Klicken Sie in der ASDM-Anwendung auf **Konfiguration** und dann auf **VPN**.
2. Erweitern Sie **WebVPN**, und wählen Sie **WebVPN Access aus**.

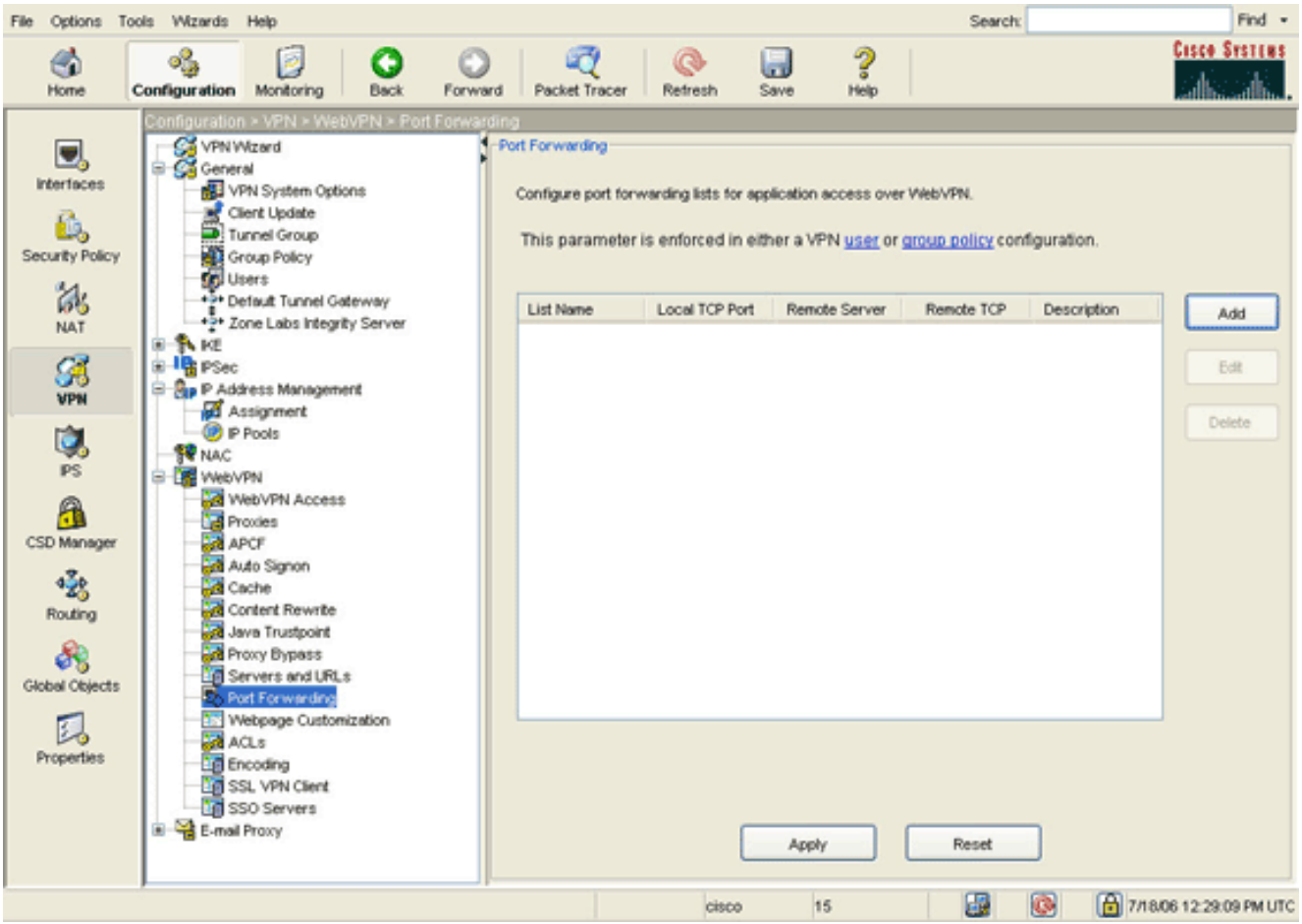


3. Markieren Sie die Schnittstelle, und klicken Sie auf **Aktivieren**.
4. Klicken Sie auf **Übernehmen**, klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

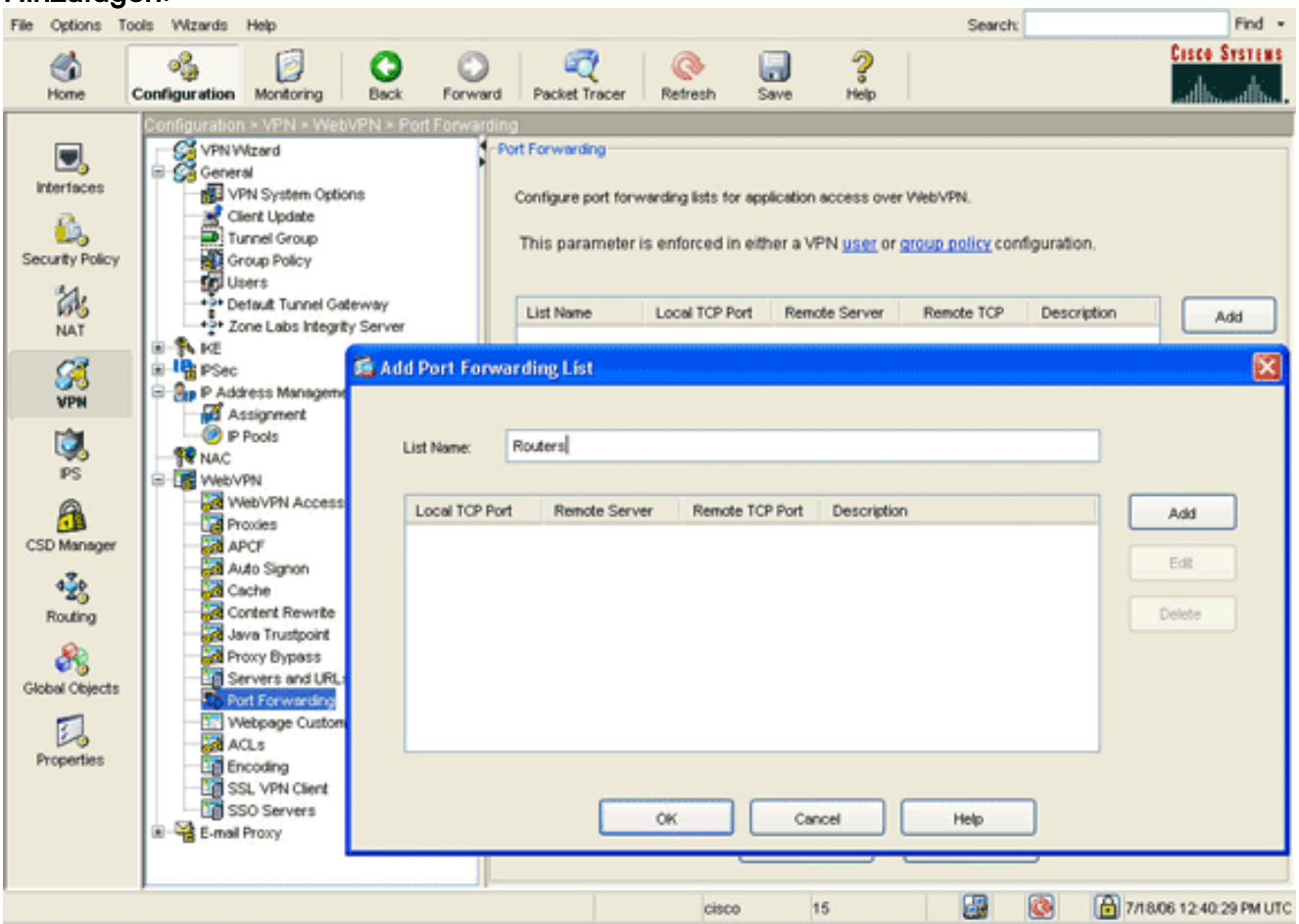
Schritt 2: Konfigurieren von Port Forwarding-Eigenschaften

Gehen Sie wie folgt vor, um die Eigenschaften der Port-Weiterleitung zu konfigurieren:

1. Erweitern Sie **WebVPN**, und wählen Sie **Port Forwarding aus**.

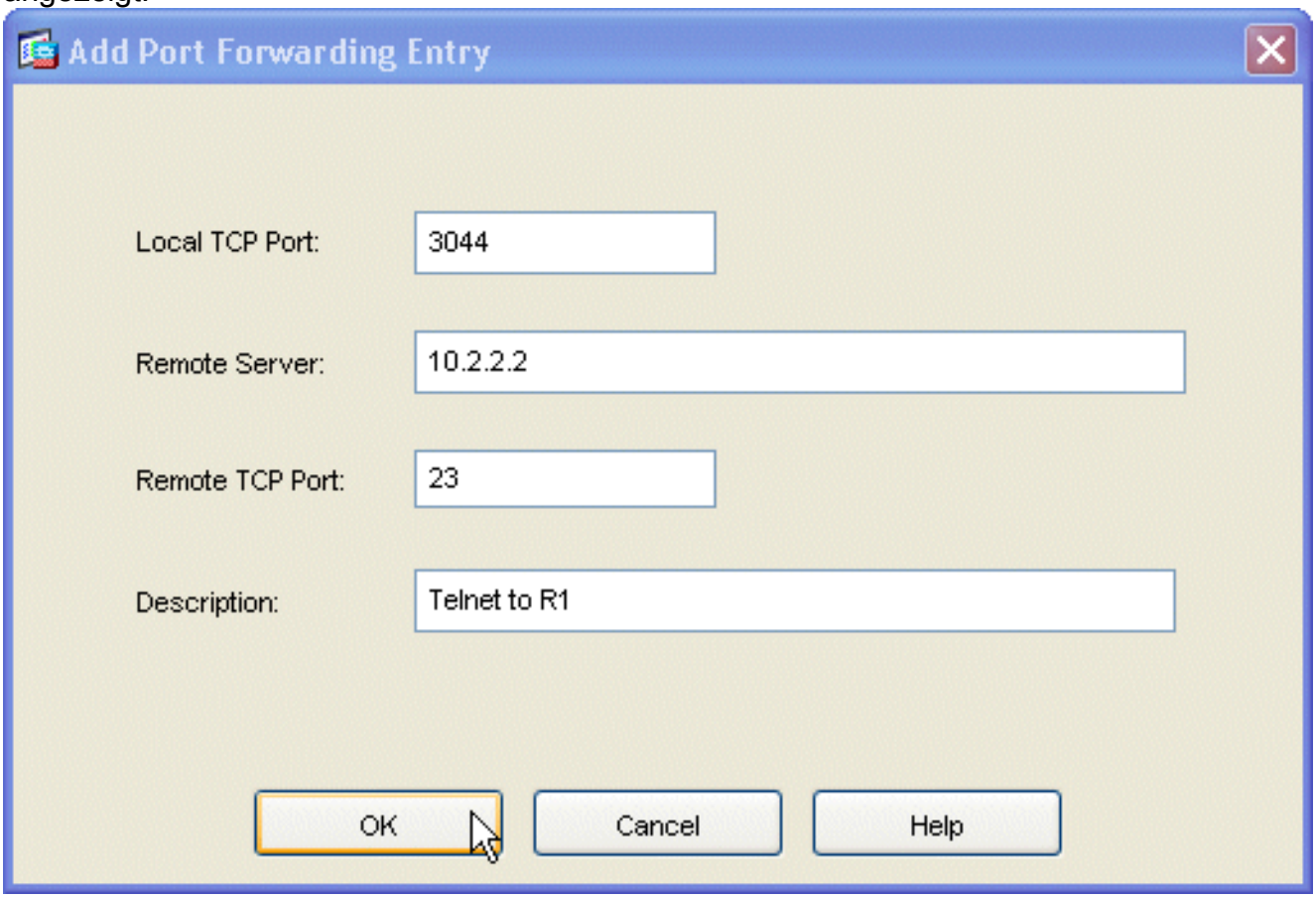


2. Klicken Sie auf die Schaltfläche **Hinzufügen**.



3. Geben Sie im Dialogfeld "Portweiterleitungsliste hinzufügen" einen Listennamen ein, und klicken Sie auf **Hinzufügen**.Das Dialogfeld Port Forwarding Entry (Port-Weiterleitungseintrag

hinzufügen) wird angezeigt.

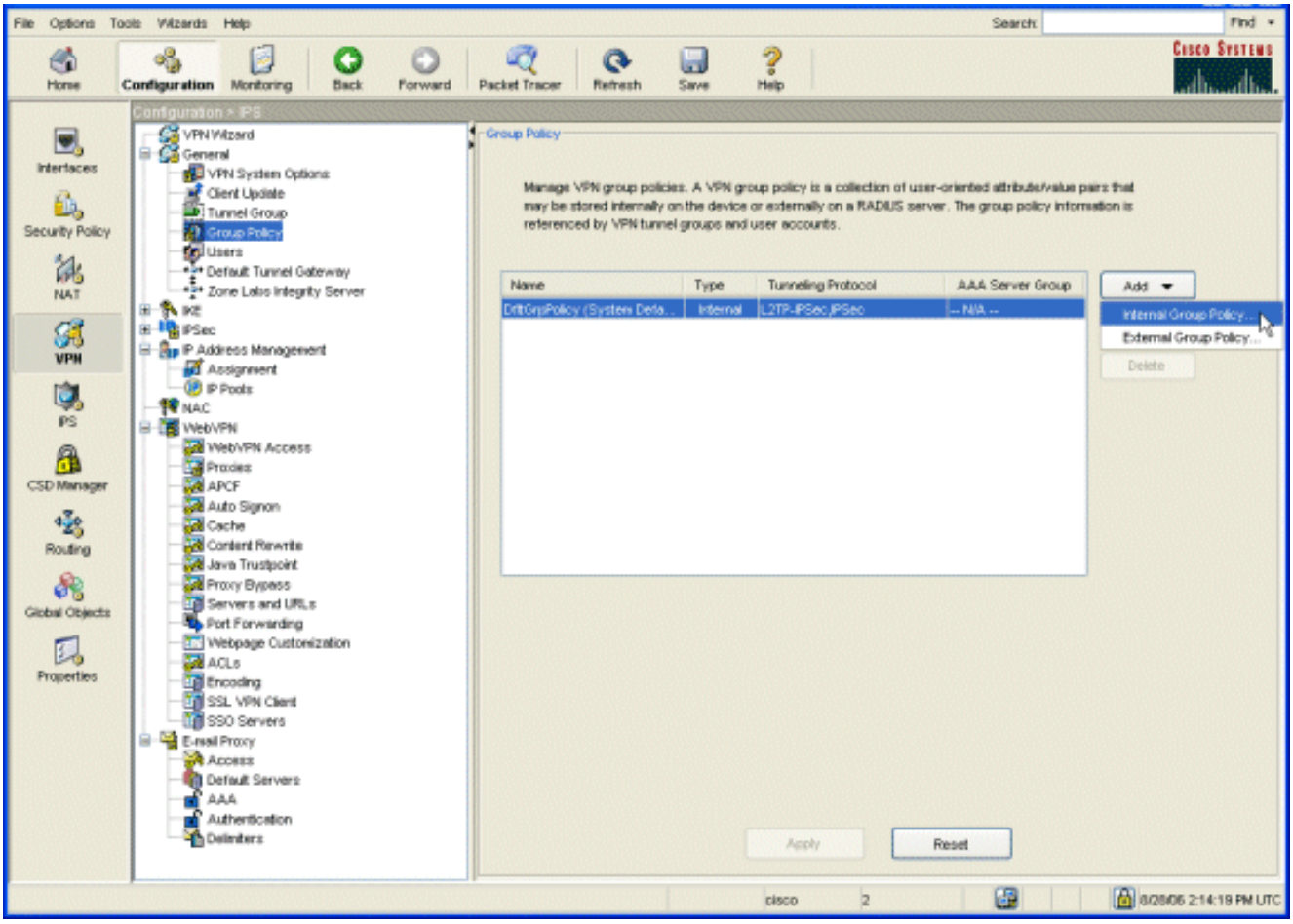


4. Geben Sie im Dialogfeld Add Port Forwarding Entry (Port-Weiterleitungseintrag hinzufügen) die folgenden Optionen ein:Geben Sie im Feld Local TCP Port (Lokaler TCP-Port) eine Portnummer ein, oder akzeptieren Sie den Standardwert.Beim eingegebenen Wert kann es sich um eine beliebige Zahl zwischen 1024 und 65535 handeln.Geben Sie im Feld Remote Server (Remote-Server) eine IP-Adresse ein.In diesem Beispiel wird die Adresse des Routers verwendet.Geben Sie im Feld Remote TCP Port (Remote-TCP-Port) eine Portnummer ein.In diesem Beispiel wird Port 23 verwendet.Geben Sie im Feld Beschreibung eine Beschreibung ein, und klicken Sie auf **OK**.
5. Klicken Sie auf **OK** und dann auf **Übernehmen**.
6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

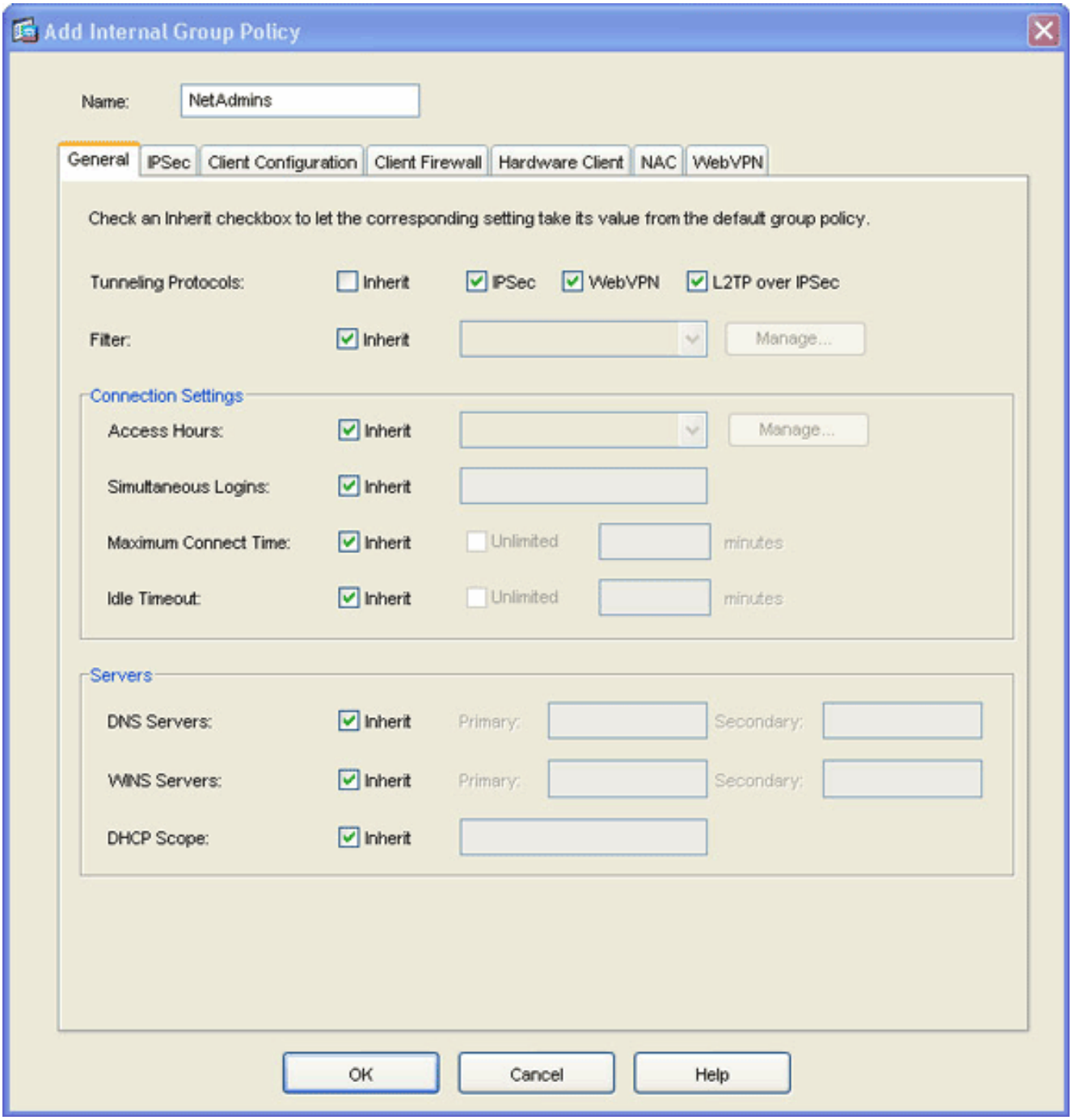
Schritt 3: Erstellen einer Gruppenrichtlinie und Verknüpfen Sie diese mit der Port Forwarding List

Gehen Sie wie folgt vor, um eine Gruppenrichtlinie zu erstellen und mit der Port Forwarding-Liste zu verknüpfen:

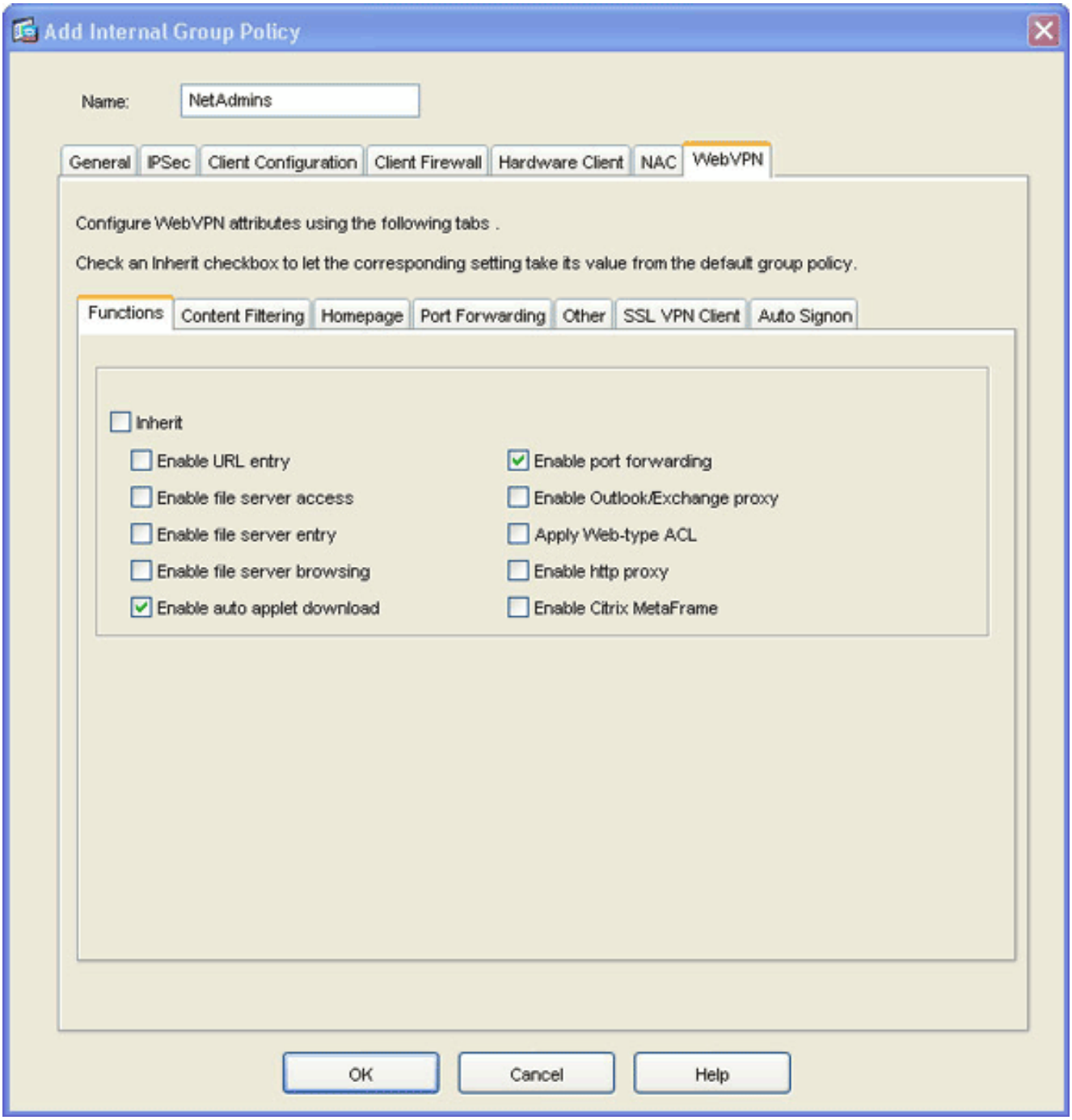
1. Erweitern Sie **Allgemein**, und wählen Sie **Gruppenrichtlinie aus**.



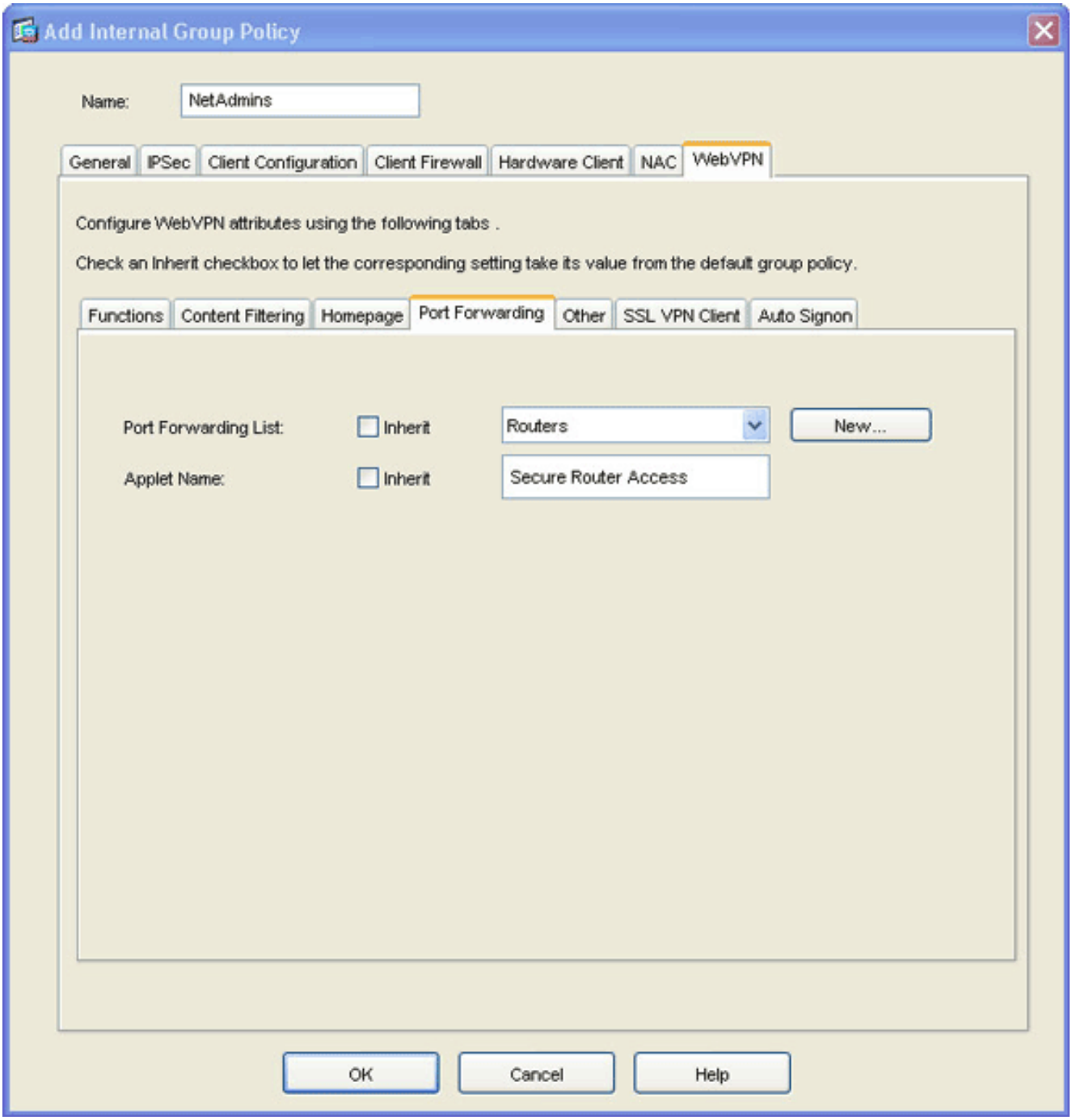
2. Klicken Sie auf **Hinzufügen**, und wählen Sie **Interne Gruppenrichtlinie aus**.Das Dialogfeld Interne Gruppenrichtlinie hinzufügen wird angezeigt.



3. Geben Sie einen Namen ein, oder akzeptieren Sie den Standardnamen der Gruppenrichtlinie.
4. Deaktivieren Sie das Kontrollkästchen **Tunneling Protocols Inherit** (Tunneling-Protokolle erben), und aktivieren Sie das **WebVPN**-Kontrollkästchen.
5. Klicken Sie auf die Registerkarte **WebVPN** oben im Dialogfeld, und klicken Sie dann auf die Registerkarte **Funktionen**.
6. Deaktivieren Sie das Kontrollkästchen **Erben**, und aktivieren Sie die Kontrollkästchen **Auto Applet Download** und **Enable Port Forwarding** aktivieren, wie in diesem Bild gezeigt:



7. Klicken Sie auch auf der Registerkarte WebVPN auf die Registerkarte **Port Forwarding** (**Portweiterleitung**), und deaktivieren Sie das Kontrollkästchen Port Forwarding List **Inherit (Portweiterleitungsliste vererben)**.



8. Klicken Sie auf den Pfeil des Dropdown-Menüs **Portweiterleitungsliste**, und wählen Sie die in Schritt 2 erstellte Liste für die Portweiterleitung aus.
9. Deaktivieren Sie das Kontrollkästchen **Erben von** Applet-Name, und ändern Sie den Namen im Textfeld.Der Client zeigt den Applet-Namen bei der Verbindung an.
10. Klicken Sie auf **OK** und dann auf **Übernehmen**.
11. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

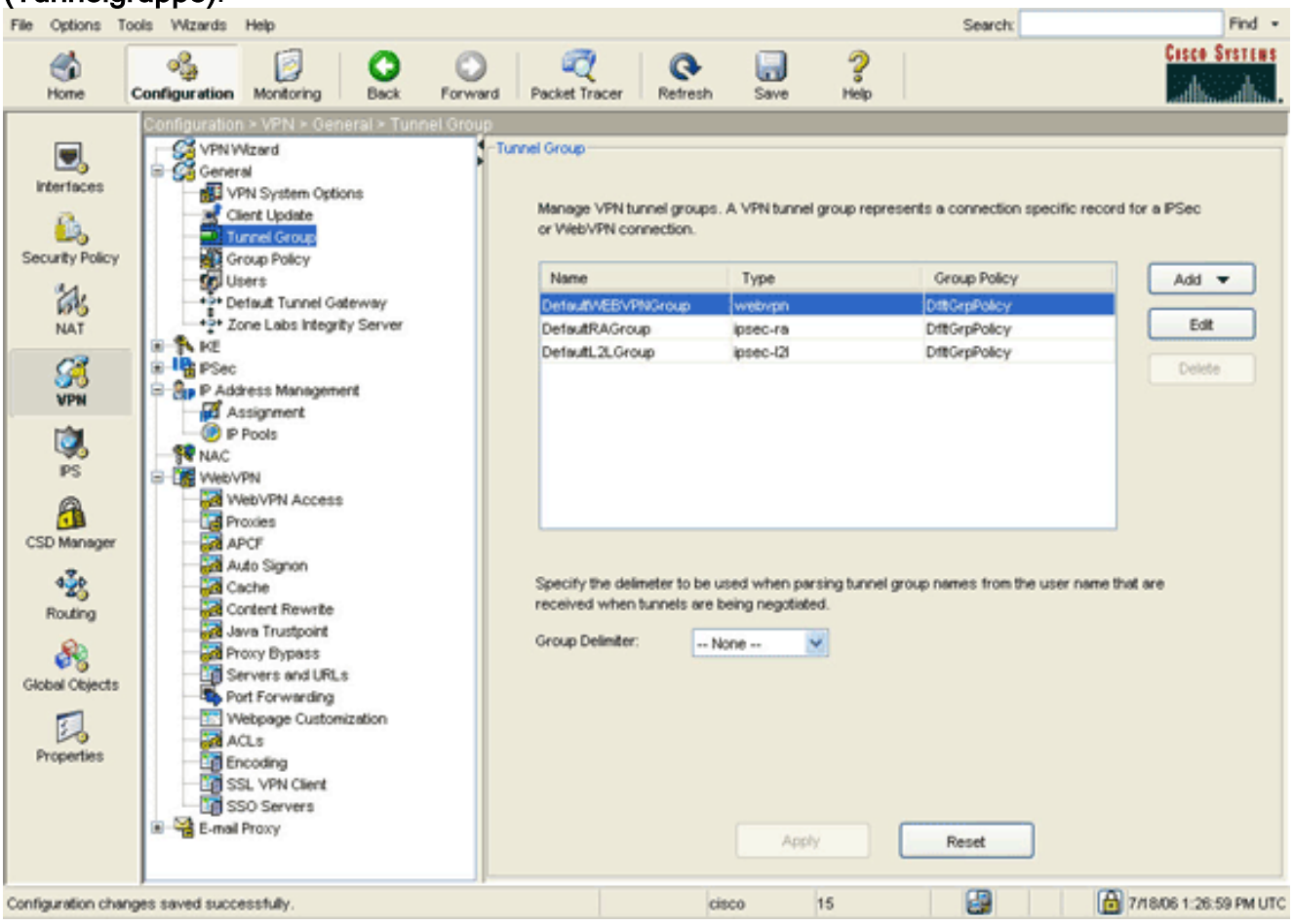
Schritt 4: Erstellen einer Tunnelgruppe und Verknüpfen Sie diese mit der Gruppenrichtlinie

Sie können die Standard-*DefaultWebVPNGroup*-Tunnelgruppe bearbeiten oder eine neue Tunnelgruppe erstellen.

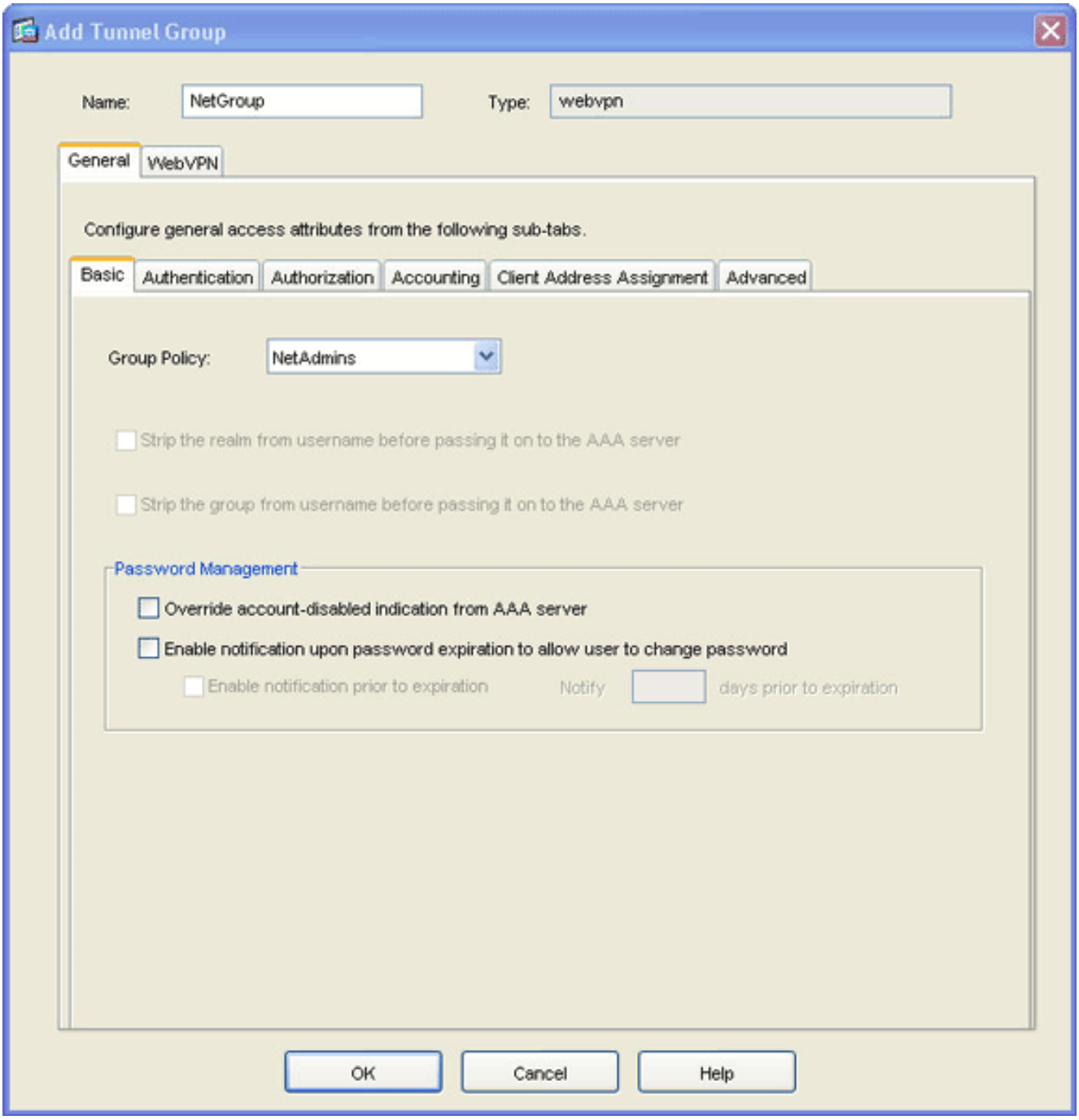
Gehen Sie wie folgt vor, um eine neue Tunnelgruppe zu erstellen:

1. Erweitern Sie **General**, und wählen Sie **Tunnel Group**

(Tunnelgruppe).



2. Klicken Sie auf **Hinzufügen**, und wählen Sie **WebVPN Access** aus.Das Dialogfeld "Tunnel-Gruppe hinzufügen" wird
angezeigt.

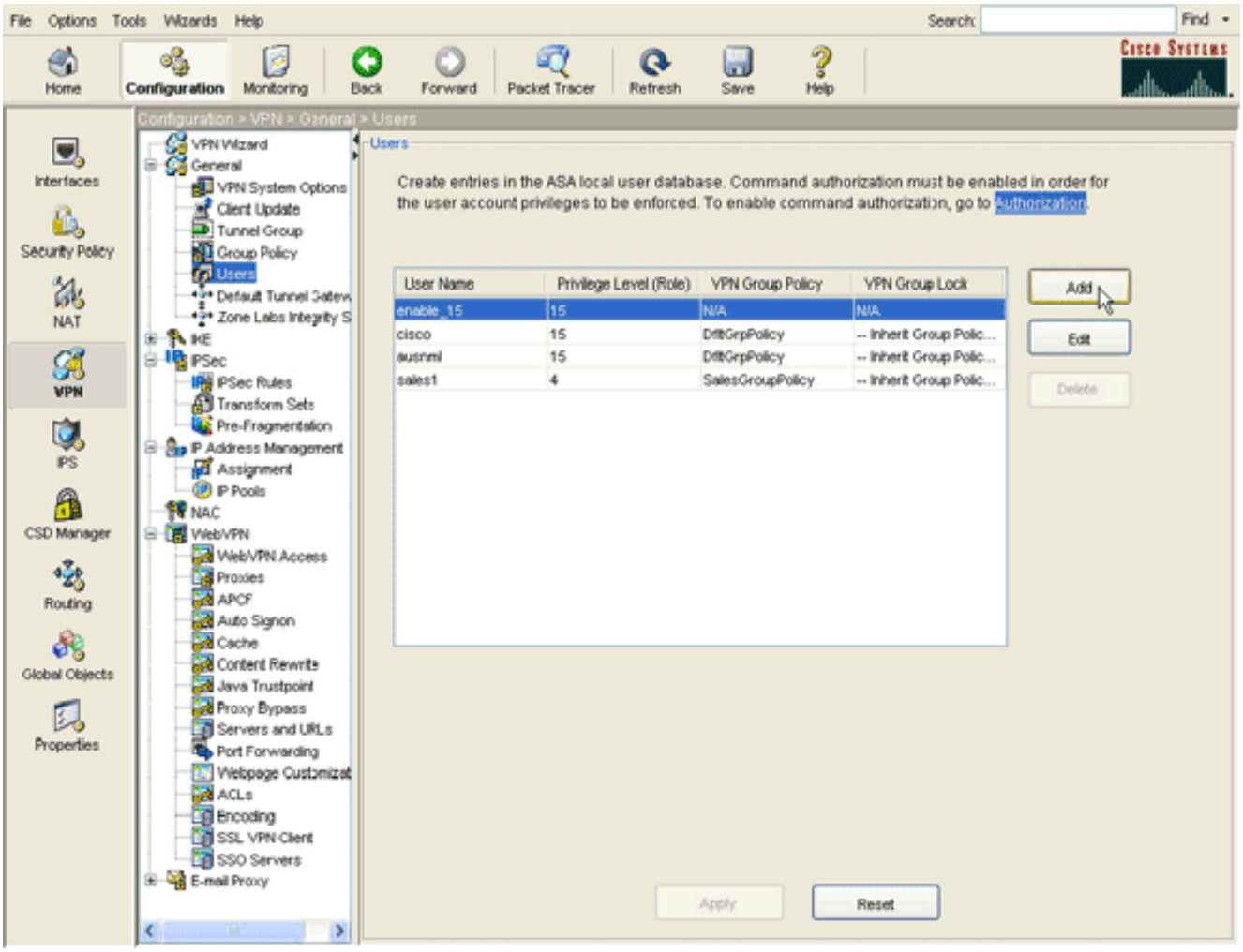


3. Geben Sie im Feld Name einen Namen ein.
4. Klicken Sie auf den Pfeil des Dropdown-Menüs **Gruppenrichtlinie**, und wählen Sie die Gruppenrichtlinie aus, die Sie in Schritt 3 erstellt haben.
5. Klicken Sie auf **OK** und dann auf **Übernehmen**.
6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.Die Eigenschaften von Tunnelgruppe, Gruppenrichtlinie und Port Forwarding sind nun miteinander verknüpft.

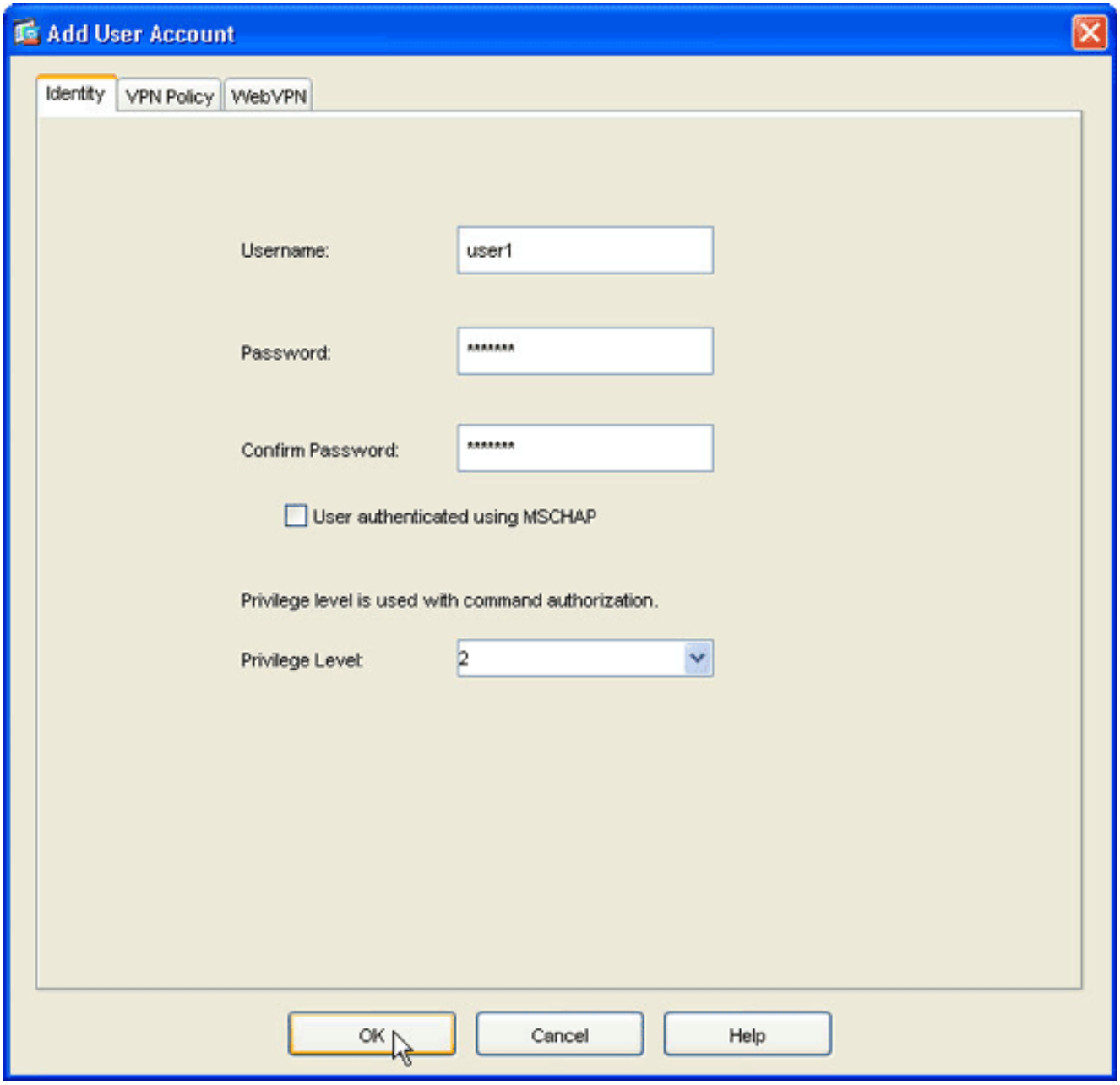
Schritt 5: Erstellen eines Benutzers und Hinzufügen dieses Benutzers zur Gruppenrichtlinie

Gehen Sie wie folgt vor, um einen Benutzer zu erstellen und der Gruppenrichtlinie diesen hinzuzufügen:

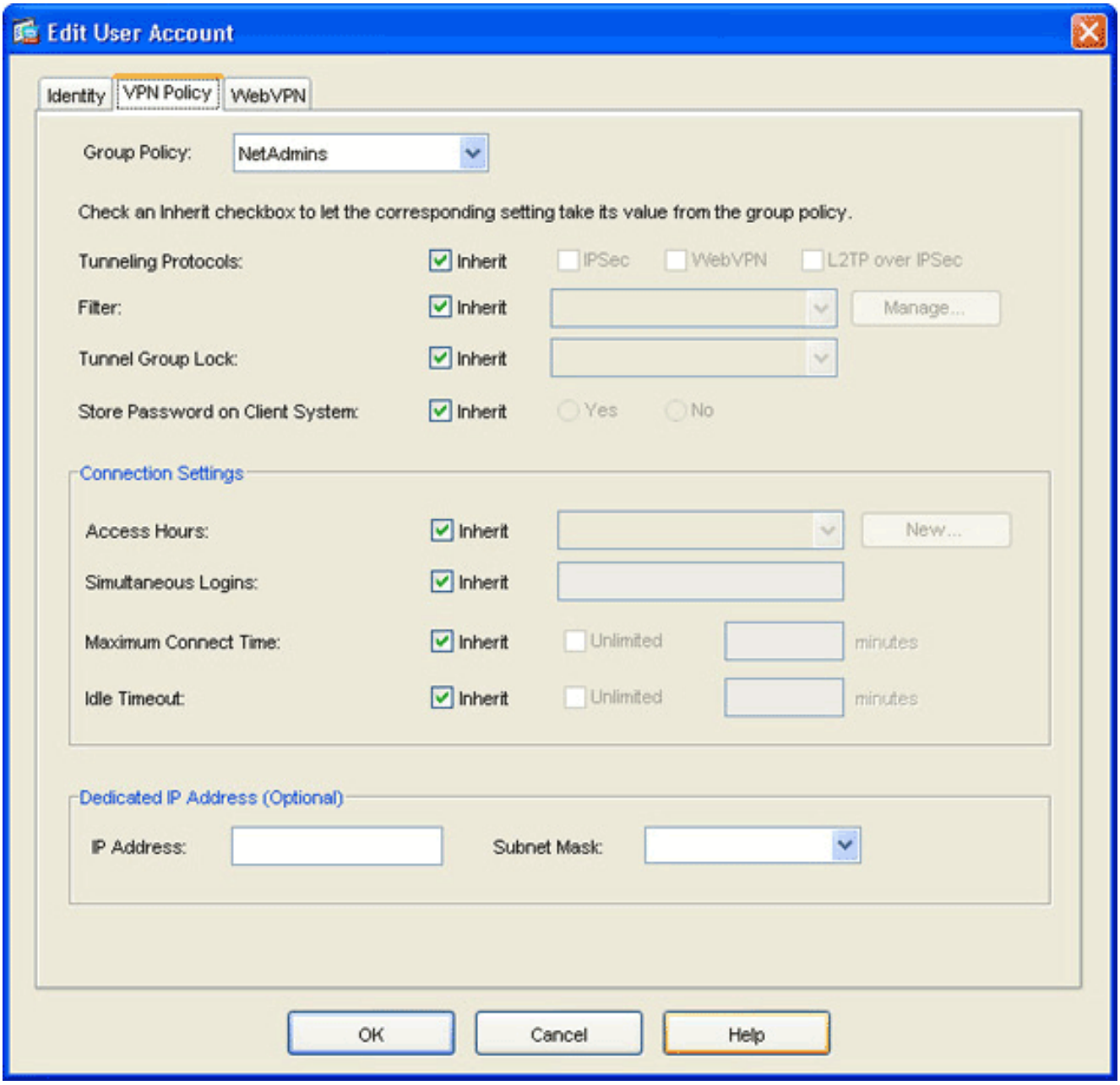
1. Erweitern Sie **Allgemein**, und wählen Sie **Benutzer aus**.



2. Klicken Sie auf die Schaltfläche **Hinzufügen**.Das Dialogfeld Benutzerkonto hinzufügen wird angezeigt.



3. Geben Sie Werte für den Benutzernamen, das Kennwort und die Berechtigungsinformationen ein, und klicken Sie dann auf die Registerkarte **VPN Policy**.



4. Klicken Sie auf den Pfeil des Dropdown-Menüs **Gruppenrichtlinie**, und wählen Sie die Gruppenrichtlinie aus, die Sie in Schritt 3 erstellt haben.Dieser Benutzer erbt die WebVPN-Eigenschaften und -Richtlinien der ausgewählten Gruppenrichtlinie.
5. Klicken Sie auf **OK** und dann auf **Übernehmen**.
6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

SSL-VPN-Konfiguration mit Thin-Client über 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
```

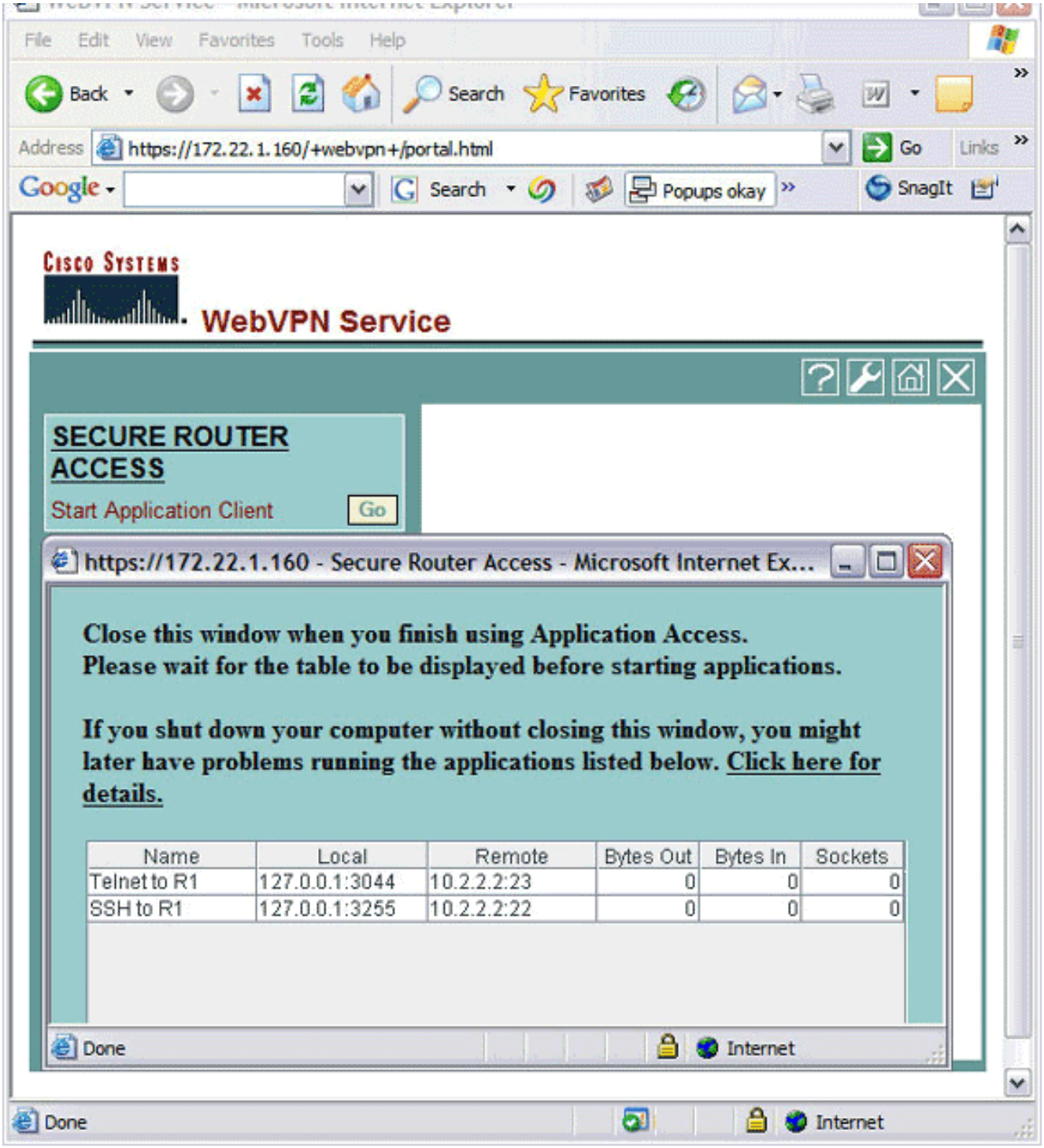
Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Vorgehensweise

In diesem Verfahren wird beschrieben, wie Sie die Gültigkeit der Konfiguration bestimmen und die Konfiguration testen.

1. Geben Sie auf einer Client-Workstation **https://*outside_ASA_IP address ein***; wobei *outside_ASA_IPAddress* die SSL-URL der ASA ist.Sobald das digitale Zertifikat akzeptiert und der Benutzer authentifiziert wurde, wird die Webseite für den WebVPN-Dienst angezeigt.

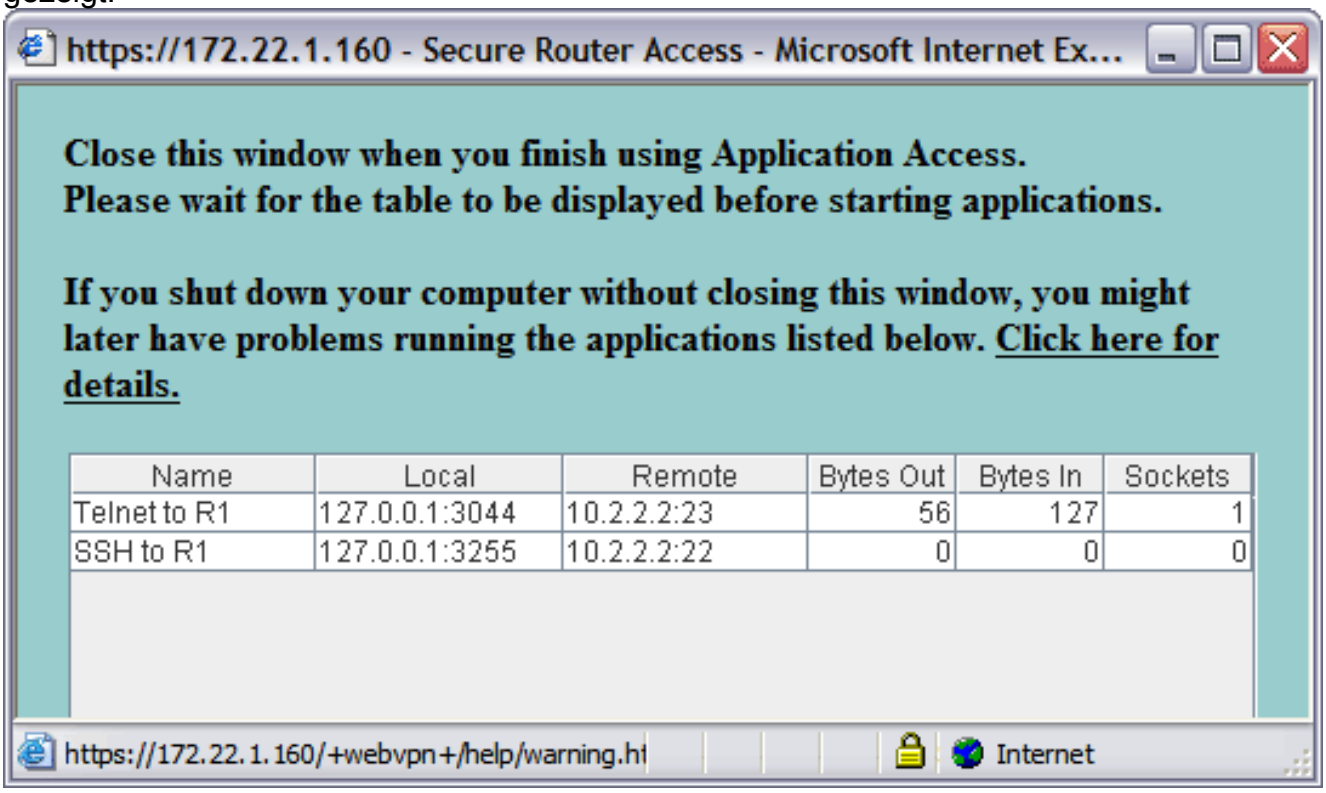


Die für den Zugriff auf die Anwendung erforderlichen Adress- und Port-Informationen werden in der lokalen Spalte angezeigt. Die Spalten Bytes Out und Bytes In zeigen keine Aktivität an, da die Anwendung zu diesem Zeitpunkt nicht aufgerufen wurde.

2. Verwenden Sie die DOS-Eingabeaufforderung oder eine andere Telnet-Anwendung, um eine Telnet-Sitzung zu starten.
3. Geben Sie an der Eingabeaufforderung **telnet 127.0.0.1 3044 ein.Hinweis:** Mit diesem Befehl wird ein Beispiel für den Zugriff auf den lokalen Port angezeigt, der im WebVPN Service-Webseiten-Bild in diesem Dokument angezeigt wird. *Der Befehl enthält keinen Doppelpunkt (:).* Geben Sie den Befehl wie in diesem Dokument beschrieben ein.Die ASA erhält den Befehl über die sichere Sitzung. Da sie eine Übersicht der Informationen speichert, weiß die ASA sofort, die sichere Telnet-Sitzung mit dem zugeordneten Gerät zu öffnen.

Sobald Sie Ihren Benutzernamen und Ihr Kennwort eingegeben haben, ist der Zugriff auf das Gerät abgeschlossen.

4. Um den Zugriff auf das Gerät zu überprüfen, überprüfen Sie die Spalten Bytes Out und Bytes In, wie in diesem Bild gezeigt:



Befehle

Mehrere **show**-Befehle sind WebVPN zugeordnet. Sie können diese Befehle in der Befehlszeilenschnittstelle (CLI) ausführen, um Statistiken und andere Informationen anzuzeigen. Detaillierte Informationen zu **show**-Befehlen finden Sie unter Verifying WebVPN Configuration.

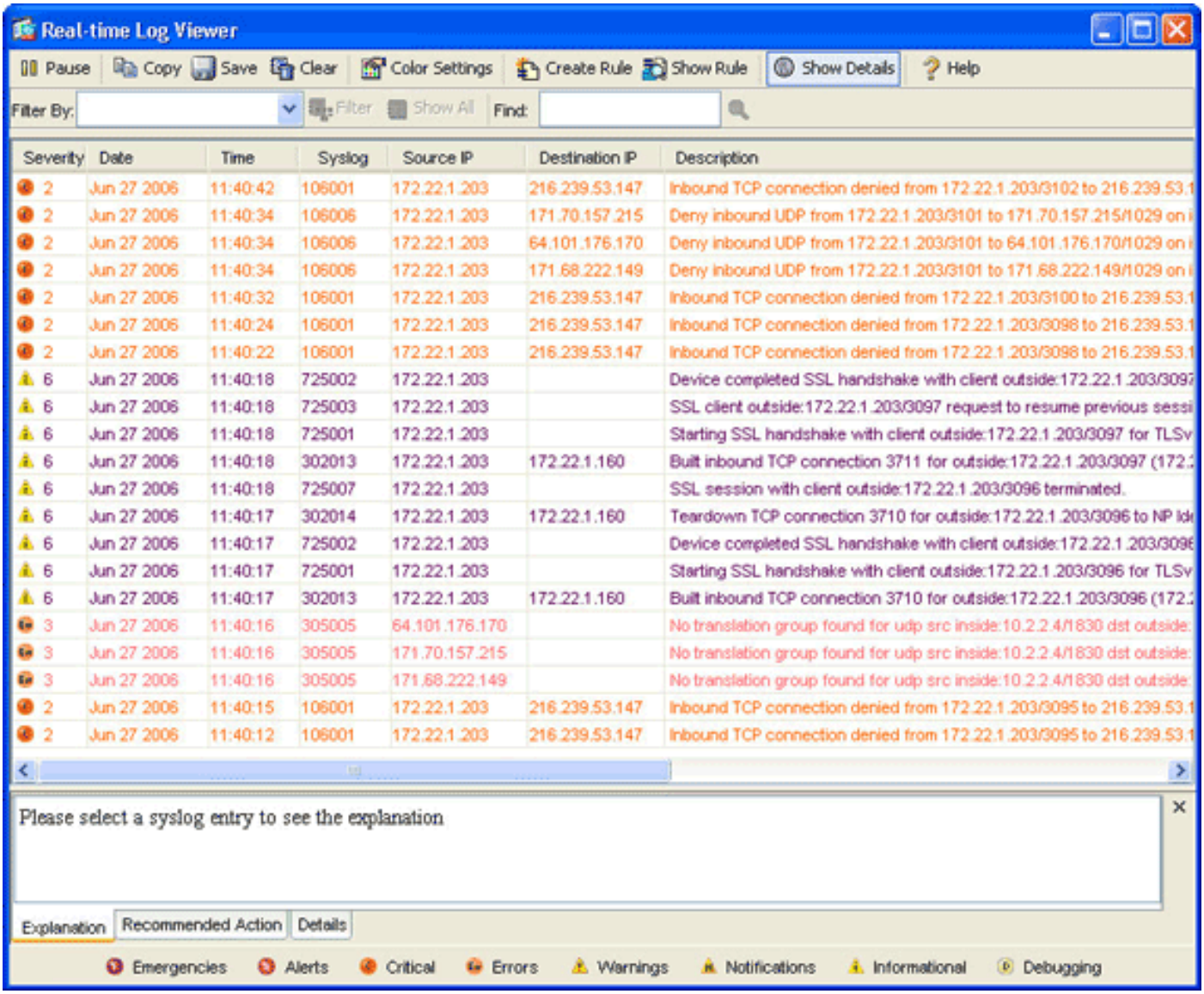
Hinweis: Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Ist der SSL-Handshake-Prozess abgeschlossen?

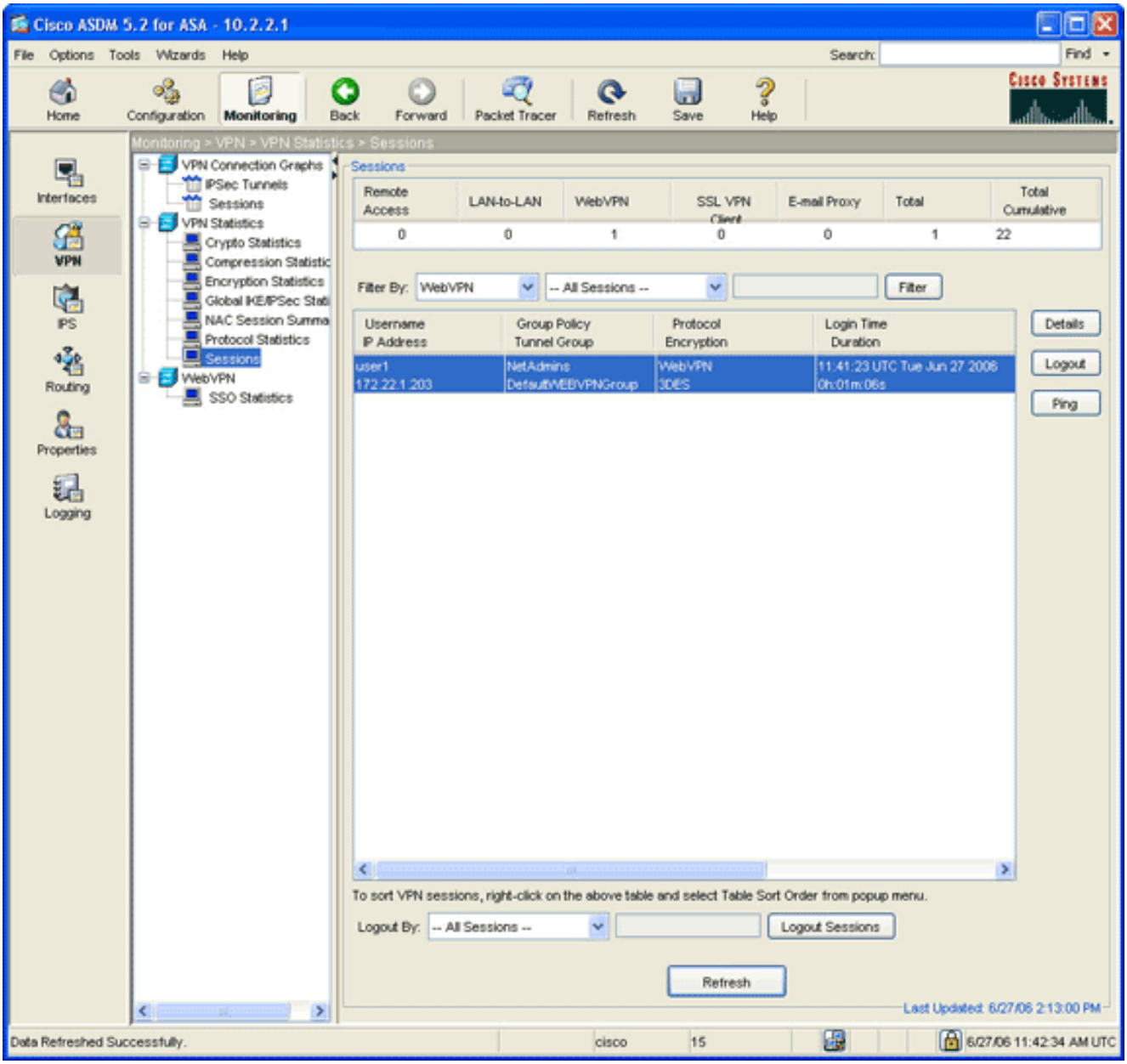
Wenn Sie eine Verbindung zur ASA herstellen, überprüfen Sie, ob das Echtzeitprotokoll den Abschluss des SSL-Handshake anzeigt.



Ist der SSL VPN Thin-Client funktionsfähig?

Gehen Sie wie folgt vor, um zu überprüfen, ob der SSL VPN Thin-Client funktioniert:

1. Klicken Sie auf **Monitoring** und dann auf **VPN**.
2. Erweitern Sie **VPN Statistics**, und klicken Sie auf **Sitzungen**.Ihre SSL VPN Thin-Client-Sitzung sollte in der Sitzungsliste angezeigt werden. Filtern Sie nach WebVPN, wie in diesem Bild
   gezeigt:



Befehle

Dem WebVPN sind mehrere **Debugbefehle** zugeordnet. Ausführliche Informationen zu diesen Befehlen finden Sie unter Verwenden von WebVPN-Debug-Befehlen.

Hinweis: Die Verwendung von **Debug-**Befehlen kann sich negativ auf Ihr Cisco Gerät auswirken. Bevor Sie **Debug-**Befehle verwenden, lesen Sie die Informationen unter Wichtige Informationen über Debug-Befehle.

Zugehörige Informationen

- Clientless-SSL-VPN (WebVPN) auf ASA-Konfigurationsbeispiel
- SSL VPN Client (SVC) auf ASA mit ASDM - Konfigurationsbeispiel
- Cisco Adaptive Security Appliances der Serie ASA 5500
- ASA mit WebVPN und Single Sign-On mit ASDM und NTLMv1 Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems