ASDM を使った ASA でのシンクライアント SSL VPN（WebVPN）の設定例

目次

概要

シンクライアント SSL VPN テクノロジーは、Telnet（23）、SSH（22）、POP3（110）、IMAP4（143）および SMTP（25）などのスタティック ポートを持つ一部のアプリケーションで安全なアクセスを可能にします。 シンクライアント SSL VPN をユーザ主導アプリケーション、ポリシー主導アプリケーション、またはその両方として使用できます。 つまり、ユーザ単位でアクセス権を設定するか、1 人以上のユーザを追加するグループ ポリシーを作成できます。

- **クライアントレス SSL VPN（WebVPN）**：企業のローカル エリア ネットワーク（LAN）上の HTTP サーバまたは HTTPS Web サーバへアクセスする際に SSL 対応の Web ブラウザが必要となるリモート クライアントです。 また、クライアントレス SSL VPN は、Common Internet File System（CIFS）プロトコルによる Windows ファイル ブラウジングへのアクセスも提供します。 Outlook Web Access（OWA）は、HTTP アクセスの一例です。クライアントレス SSL VPN の詳細は、『ASA でのクライアントレス SSL VPN（WebVPN）の設定例

』を参照してください。

- **シンクライアント SSL VPN（ポート転送）**：小規模な Java ベースのアプレットをダウンロードし、スタティックなポート番号を使用する Transmission Control Protocol（TCP; 伝送制御プロトコル）アプリケーションのセキュアなアクセスを可能にするリモート クライアントです。 Post Office Protocol（POP3）、Simple Mail Transfer Protocol（SMTP）、Internet Message Access Protocol（IMAP）、Secure Shell（ssh; セキュア シェル）、および Telnet は、セキュアなアクセスの例です。 ローカル マシン上のファイルが変更されるため、この方法を使用するには、ユーザにローカル管理者特権が必要です。 SSL VPN のこの方法は、一部の File Transfer Protocol（FTP; ファイル転送プロトコル）アプリケーションなど、ダイナミックなポート割り当てを使用するアプリケーションでは使用できません。**注:** User Datagram Protocol（UDP; ユーザ データグラム プロトコル）はサポートされていません。
- **SSL VPN Client（トンネル モード）**：リモート ワークステーションに小規模なクライアントをダウンロードし、社内ネットワーク上のリソースへの完全なセキュア アクセスを可能にします。 SSL VPN Client（SVC）をリモート ワークステーションに永続的にダウンロードすることも、セキュアなセッションが閉じられた後にクライアントを削除することもできます。 SSL VPN Client の詳細は、「ASDM を使用した ASA での SSL VPN Client（SVC）の設定例」を参照してください。

このドキュメントでは、Adaptive Security Appliance（ASA）でのシンクライアント SSL VPN の簡単な設定を示します。 この設定により、ASA 内にあるルータに安全に telnet 接続できます。 このドキュメントの設定は ASA バージョン 7.x 以降でサポートされています。

前提条件

要件

この設定を試す前に、リモート クライアント ステーションで以下の要件が満たされていることを確認してください。

- SSL 対応の Web ブラウザ
- SUN Java JRE バージョン 1.4 以降
- Cookie の有効化
- ポップアップの許可
- ローカルの管理者特権（必須ではないが強く推奨）

注: 最新バージョンの SUN Java JRE は、Java Web サイト から無料でダウンロードできます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス 5510 シリーズ
- Cisco Adaptive Security Device Manager（ASDM）5.2(1)**注:** ASA を ASDM で設定できるようにするには、『ASDM 用の HTTPS アクセスの許可』を参照してください。
- Cisco Adaptive Security Appliance Software Version 7.2(1)
- Microsoft Windows XP Professional（SP 2）リモート クライアント

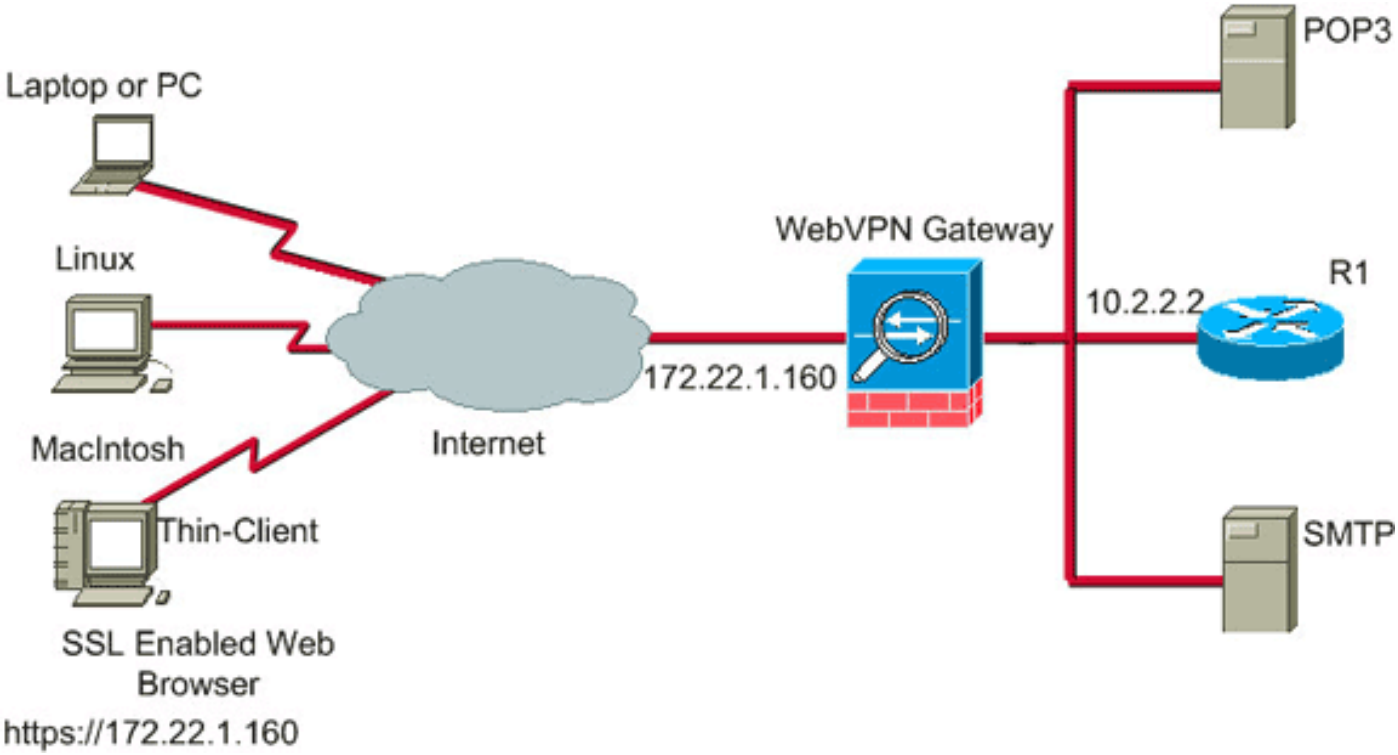
このドキュメントに記載されている情報は、ラボ環境で作成されたものです。 このドキュメントで使用されるデバイスはすべてデフォルト設定にリセットされました。 対象のネットワークが実稼動中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。 この設定で使用される IP アドレスはすべてラボ環境の RFC 1918 アドレ

スから選択されました。 これらの IP アドレスはインターネット上でルーティングできず、テスト専用です。

ネットワーク図

このドキュメントでは、このセクションで示すネットワーク設定を使用しています。

リモート クライアントが ASA でセッションを開始すると、このクライアントは小さな Java アプレットをワークステーションにダウンロードします。 クライアントには、事前設定されたリソースのリストが表示されます。



表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

セッションを開始するために、リモート クライアントで ASA の外部インターフェイスへの SSL ブラウザを開きます。 セッションを確立した後、ユーザは ASA で設定されたパラメータを使用して、Telnet またはアプリケーション アクセスを呼び出すことができます。 ASA は安全な接続をプロキシし、ユーザがデバイスにアクセスできるようにします。

注: ASA ですでに正規セッションの構成内容が認識されているため、これらの接続に着信アクセス リストは不要です。

ASDM を使用したシンクライアント SSL VPN 設定

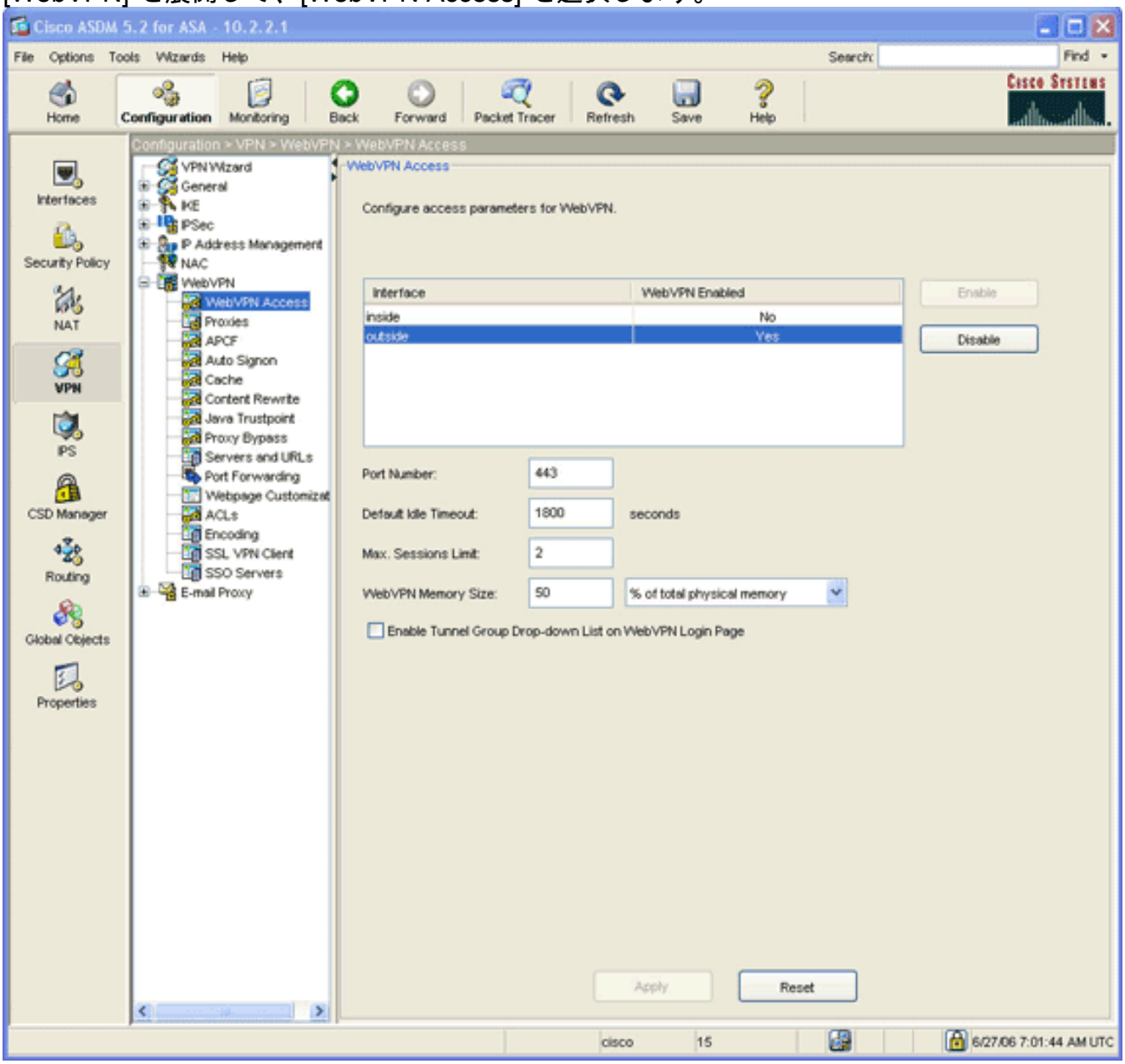
ASA でシンクライアント SSL VPN を設定するには、以下の手順に従います。

1. ASA で WebVPN を有効にする
2. ポート フォワーディング特性を設定する
3. グループ ポリシーを作成して、ポート フォワーディング リスト（手順 2 で作成）にリンクする
4. トンネル グループを作成して、グループ ポリシー（手順 3 で作成）にリンクする
5. ユーザを作成して、そのユーザをグループ ポリシー（手順 3 で作成）に追加する

手順 1：ASA で WebVPN を有効にする

ASA で WebVPN を有効にするには、以下の手順に従います。

1. ASDM アプリケーション内で [Configuration] をクリックし、次に [VPN] をクリックします。
2. [WebVPN] を展開して、[WebVPN Access] を選択します。

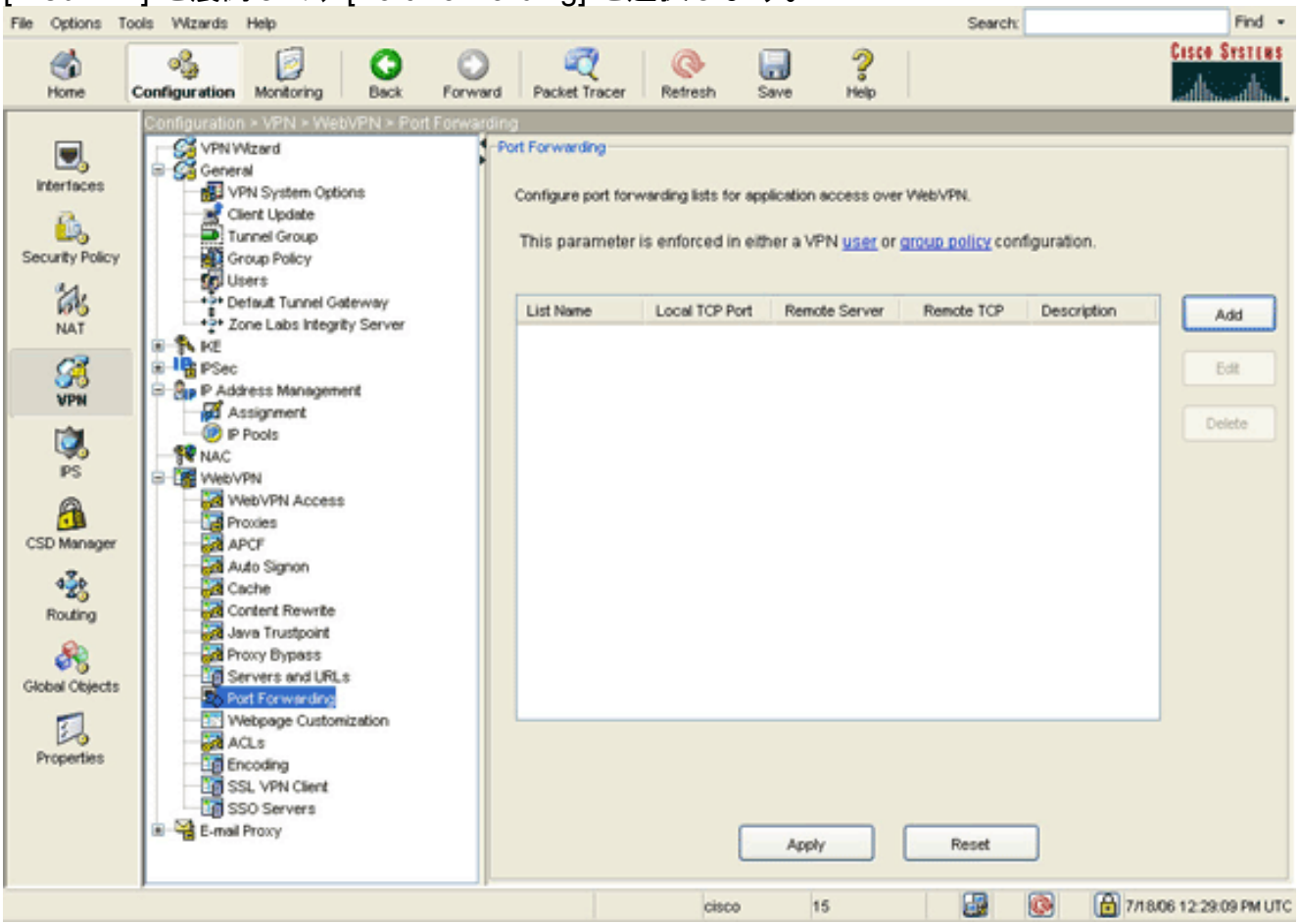


3. インターフェイスを選択し、[Enable] をクリックします。
4. [Apply] をクリックし、[Save] をクリックし、[Yes] をクリックして変更を確定します。

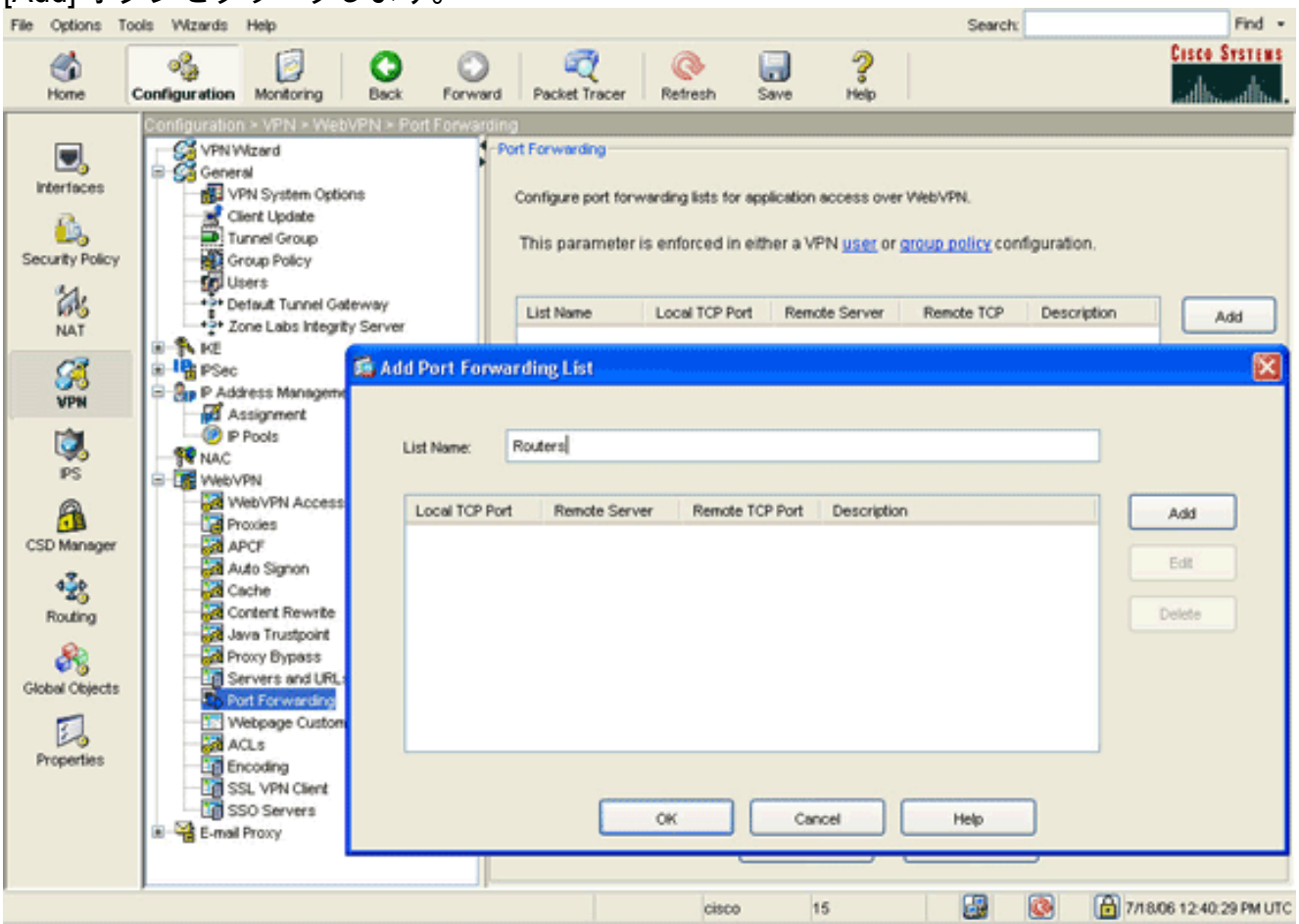
手順 2：ポート フォワーディング特性を設定する

ポート フォワーディング特性を設定するには、以下の手順に従います。

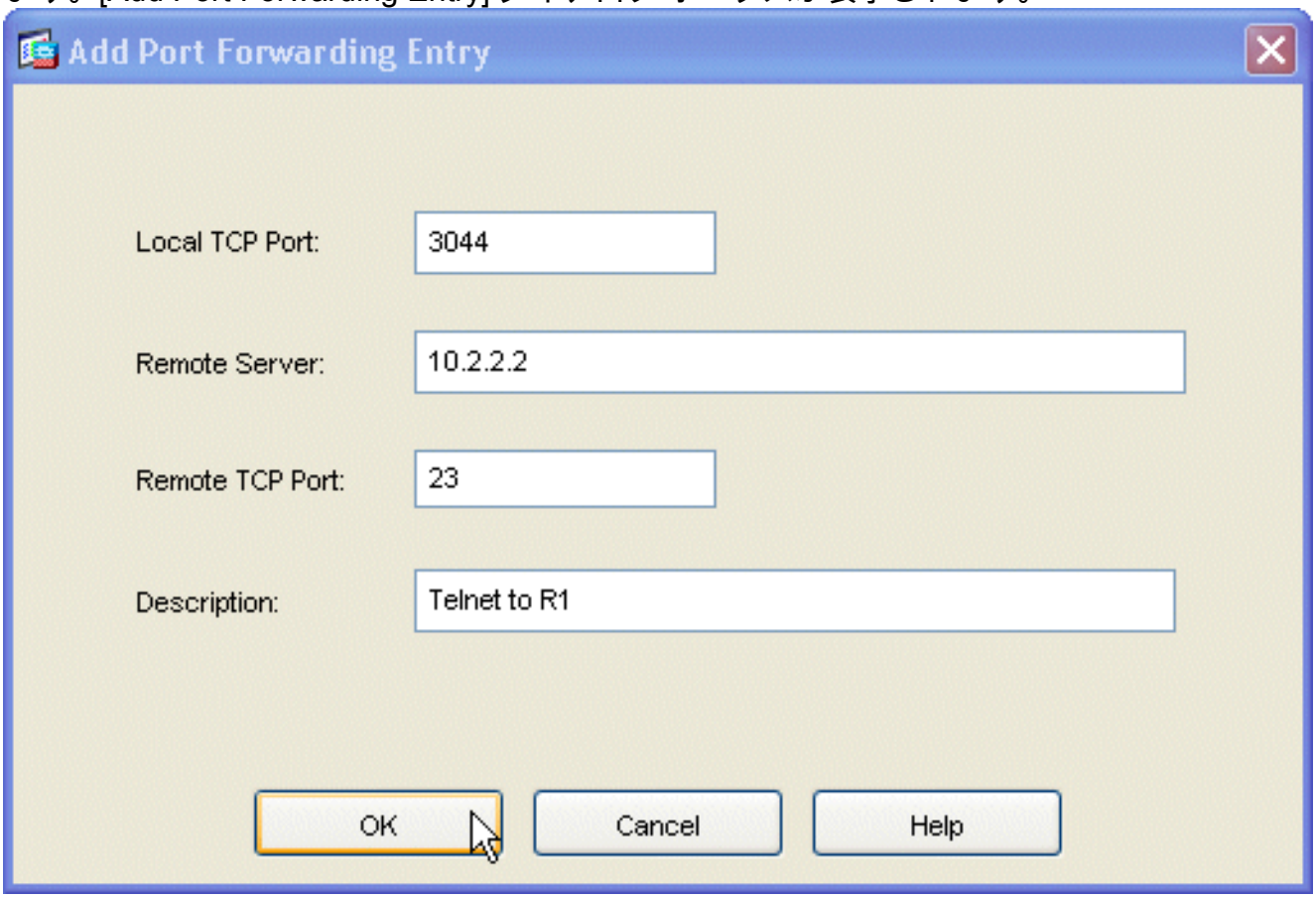
1. [WebVPN] を展開して、[Port Forwarding] を選択します。



2. [Add] ボタンをクリックします。



3. [Add Port Forwarding List] ダイアログ ボックスで、リスト名を入力して [Add] をクリックします。[Add Port Forwarding Entry] ダイアログ ボックスが表示されます。

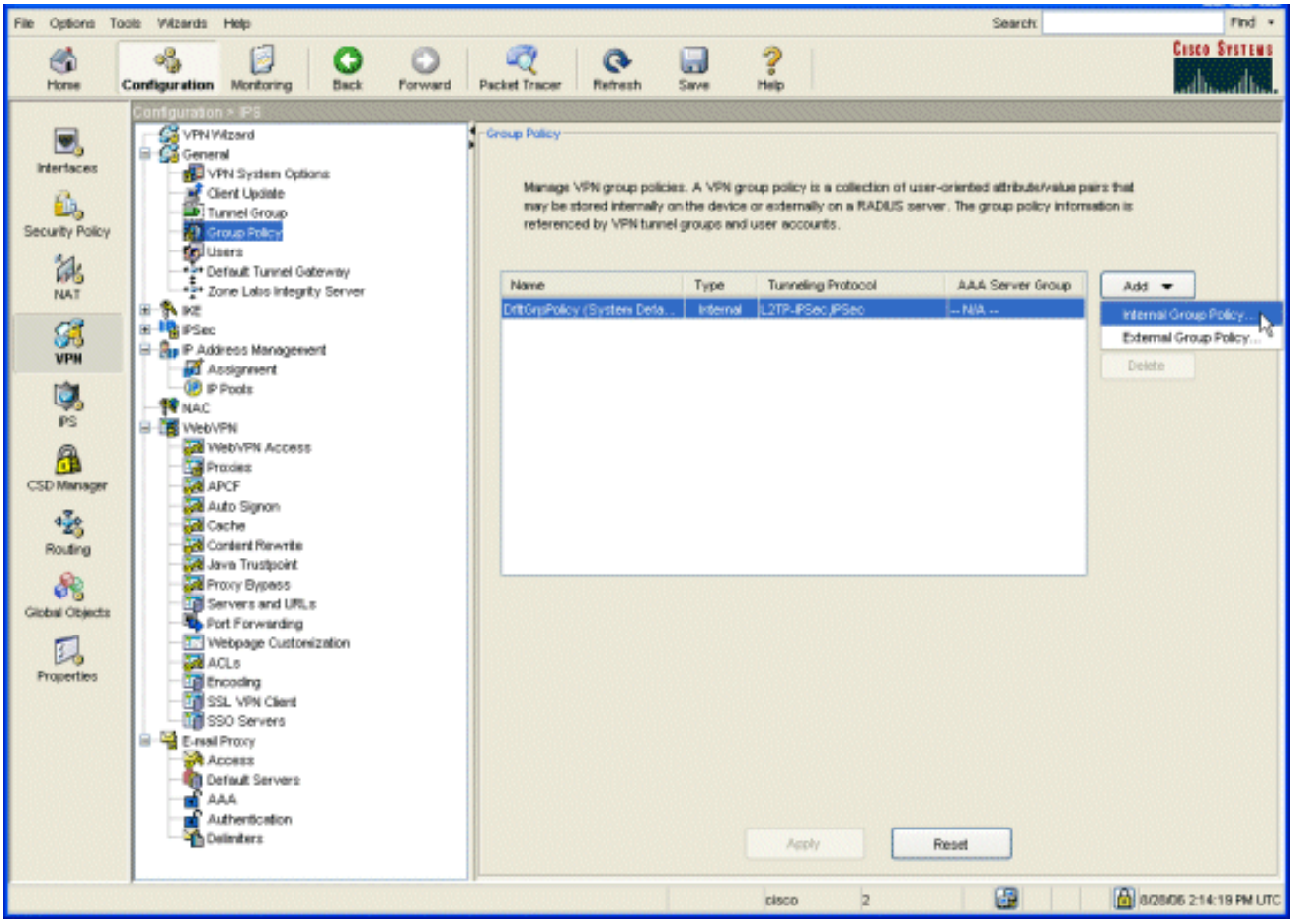


4. [Add Port Forwarding Entry] ダイアログ ボックスで、以下のオプションを入力します。[Local TCP Port] フィールドにポート番号を入力するか、デフォルト値をそのまま使用します。1024 ~ 65535 の範囲の任意の数値を入力できます。[Remote Server] フィールドに IP アドレスを入力します。この例では、ルータのアドレスが使用されています。[Remote TCP Port] フィールドにポート番号を入力します。この例では、ポート 23 が使用されています。[Description] フィールドに説明を入力し、[OK] をクリックします。
5. [OK] をクリックして、[Apply] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

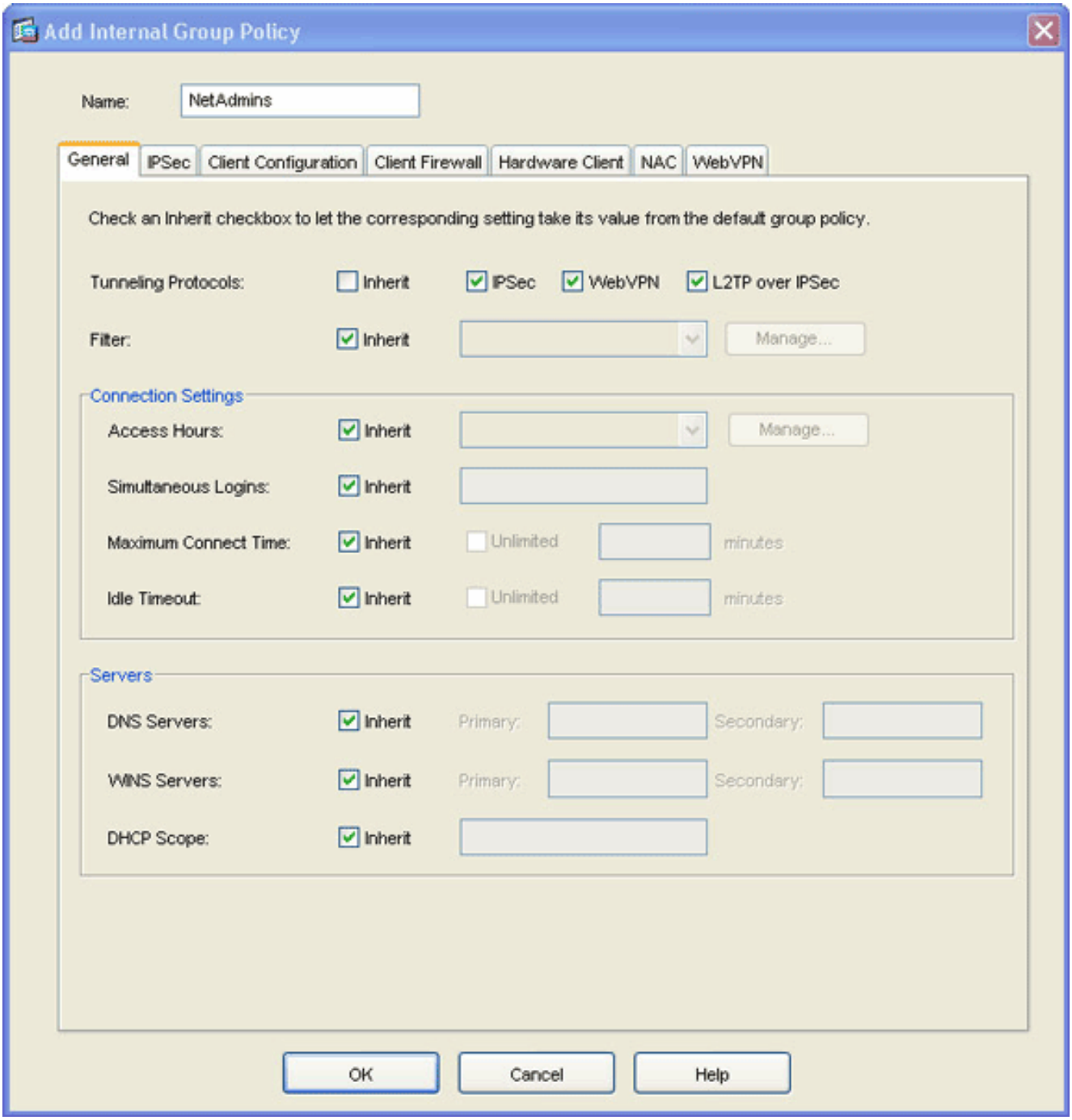
手順 3：グループ ポリシーを作成して、ポート フォワーディング リストにリンクする

グループ ポリシーを作成して、ポート フォワーディング リストにリンクするには、以下の手順に従います。

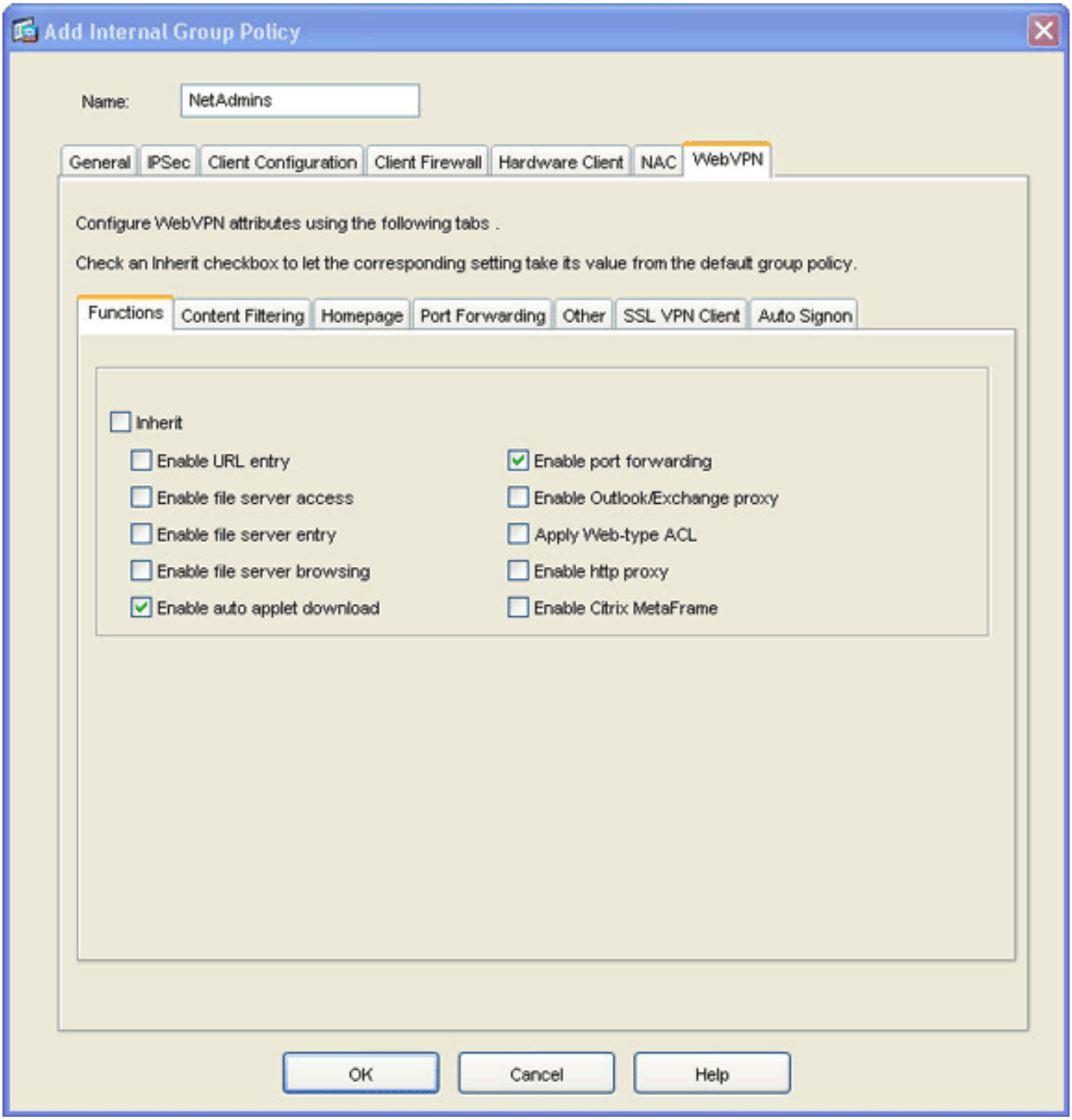
1. [General] を展開して、[Group Policy] を選択します。



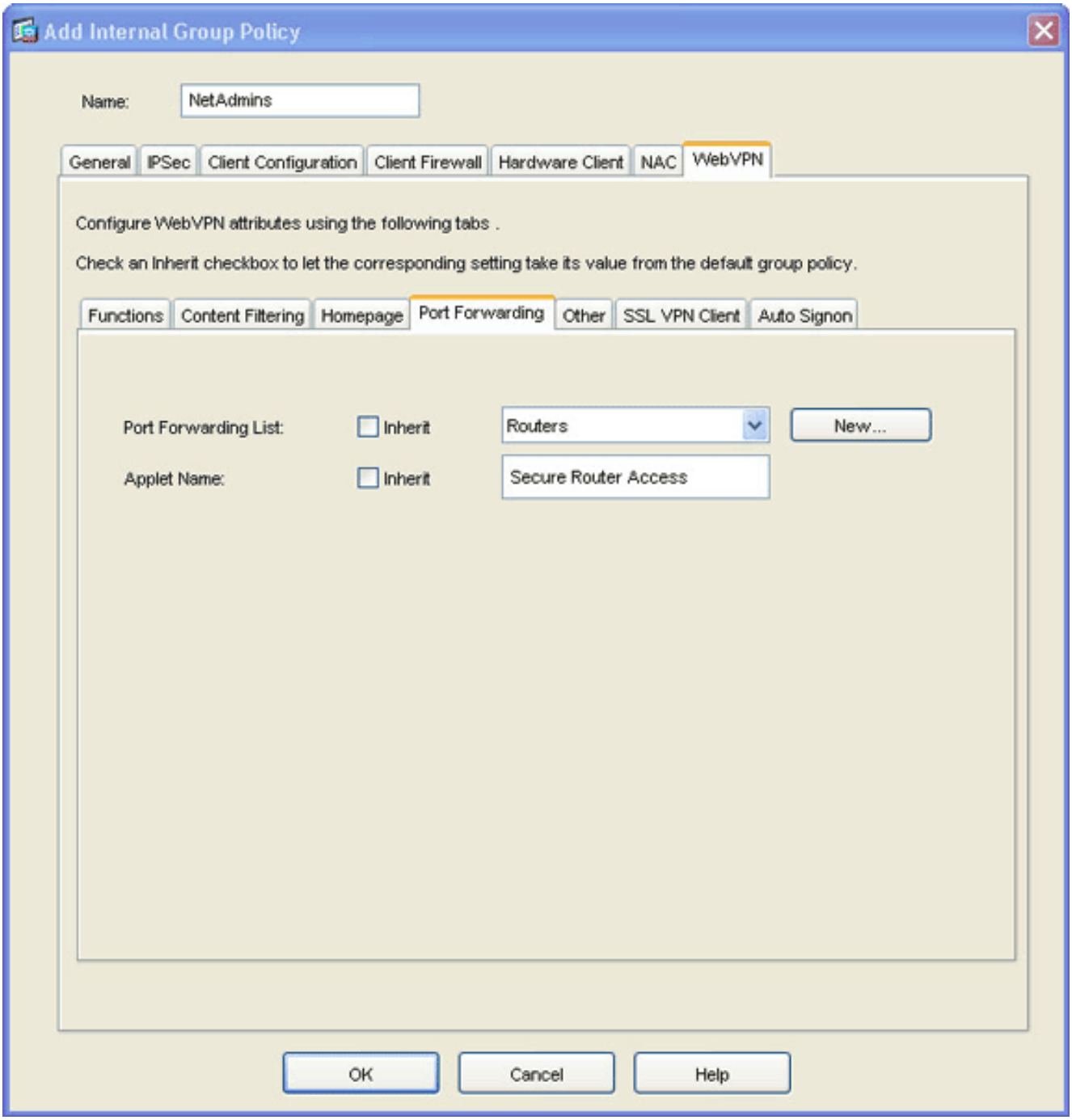
2. [Add] をクリックして、[Internal Group Policy] を選択します。[Add Internal Group Policy] ダイアログボックスが表示されます。



3. 名前を入力するか、デフォルトのグループ ポリシー名をそのまま使用します。
4. [Tunneling Protocols] の [Inherit] チェック ボックスをオフにし、[WebVPN] チェック ボックスをオンにします。
5. ダイアログ ボックスの上部にある [WebVPN] タブをクリックして、次に [Functions] タブをクリックします。
6. [Inherit] チェック ボックスをオフにし、[Enable auto applet download] および [Enable port forwarding] チェック ボックスをオンにします（下図参照）。



7. また、[WebVPN] タブ内の [Port Forwarding] タブをクリックして、[Port Forwarding List] の [Inherit] チェック ボックスもオフにします。



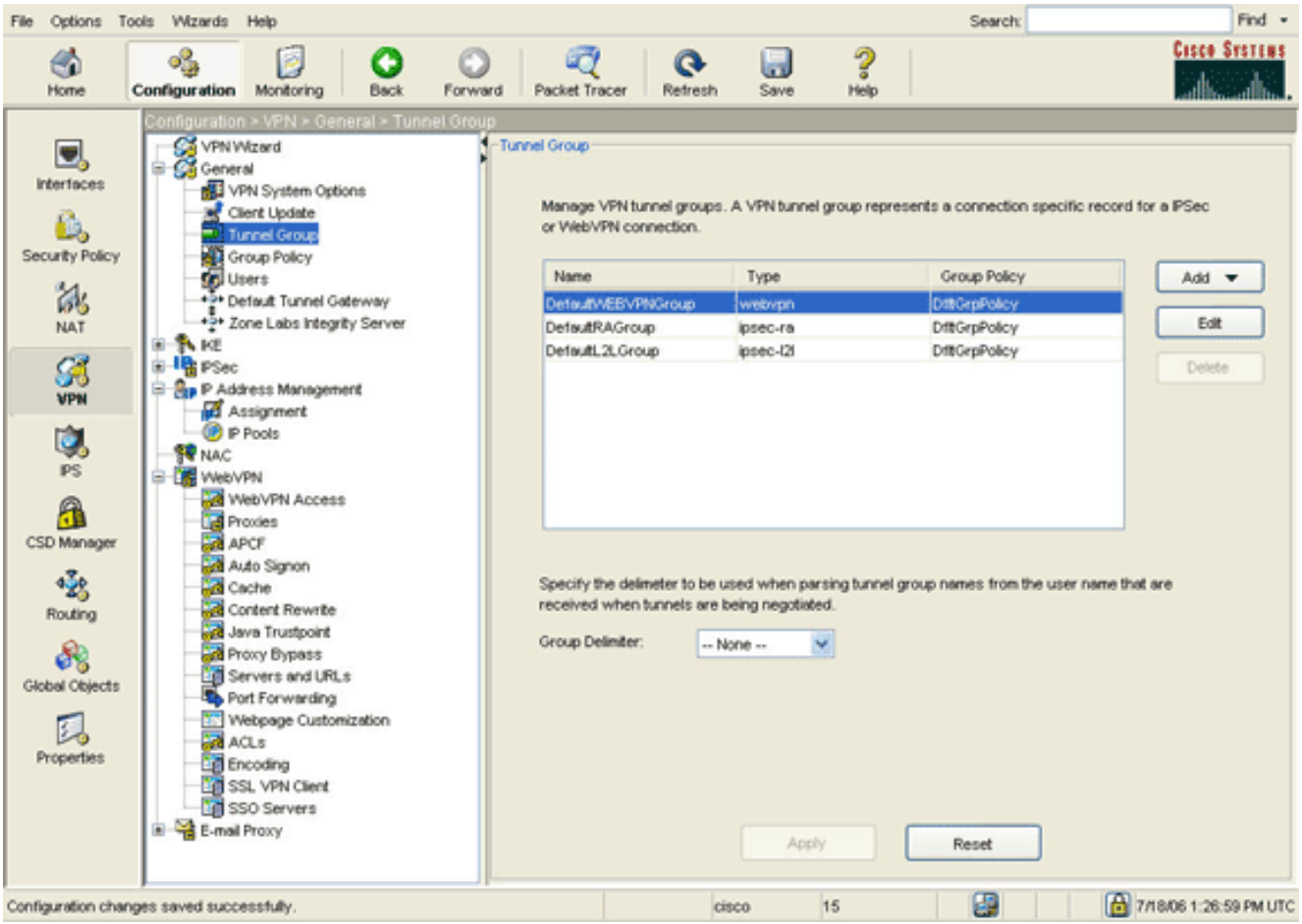
8. [Port Forwarding List] のドロップダウンの矢印をクリックして、手順 2 で作成したポート フォワーディング リストを選択します。
9. [Applet Name] の [Inherit] チェック ボックスをオフにして、テキスト フィールド内の名前を変更します。クライアントに接続時のアプレット名が表示されます。
10. [OK] をクリックして、[Apply] をクリックします。
11. [Save] をクリックし、[Yes] をクリックして変更を確定します。

手順 4：トンネル グループを作成して、グループ ポリシーにリンクする

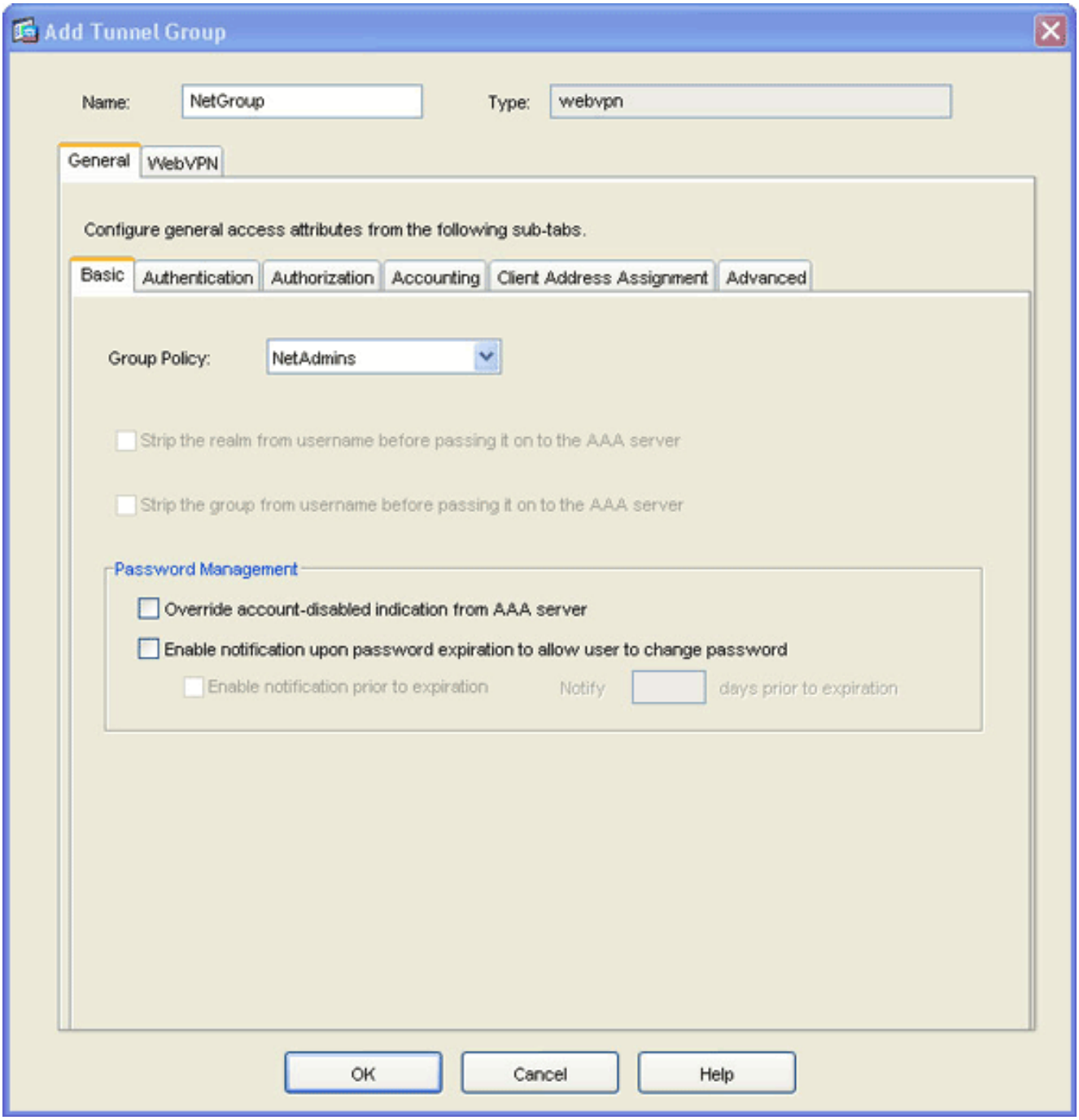
デフォルトの *DefaultWebVPNGroup* トンネル グループを編集するか、新しいトンネル グループを作成します。

新しいトンネル グループを作成するには、以下の手順に従います。

1. [General] を展開して、[Tunnel Group] を選択します。



2. **[Add]** をクリックし、**[WebVPN Access]** を選択します。[Add Tunnel Group] ダイアログ ボックスが表示されます。

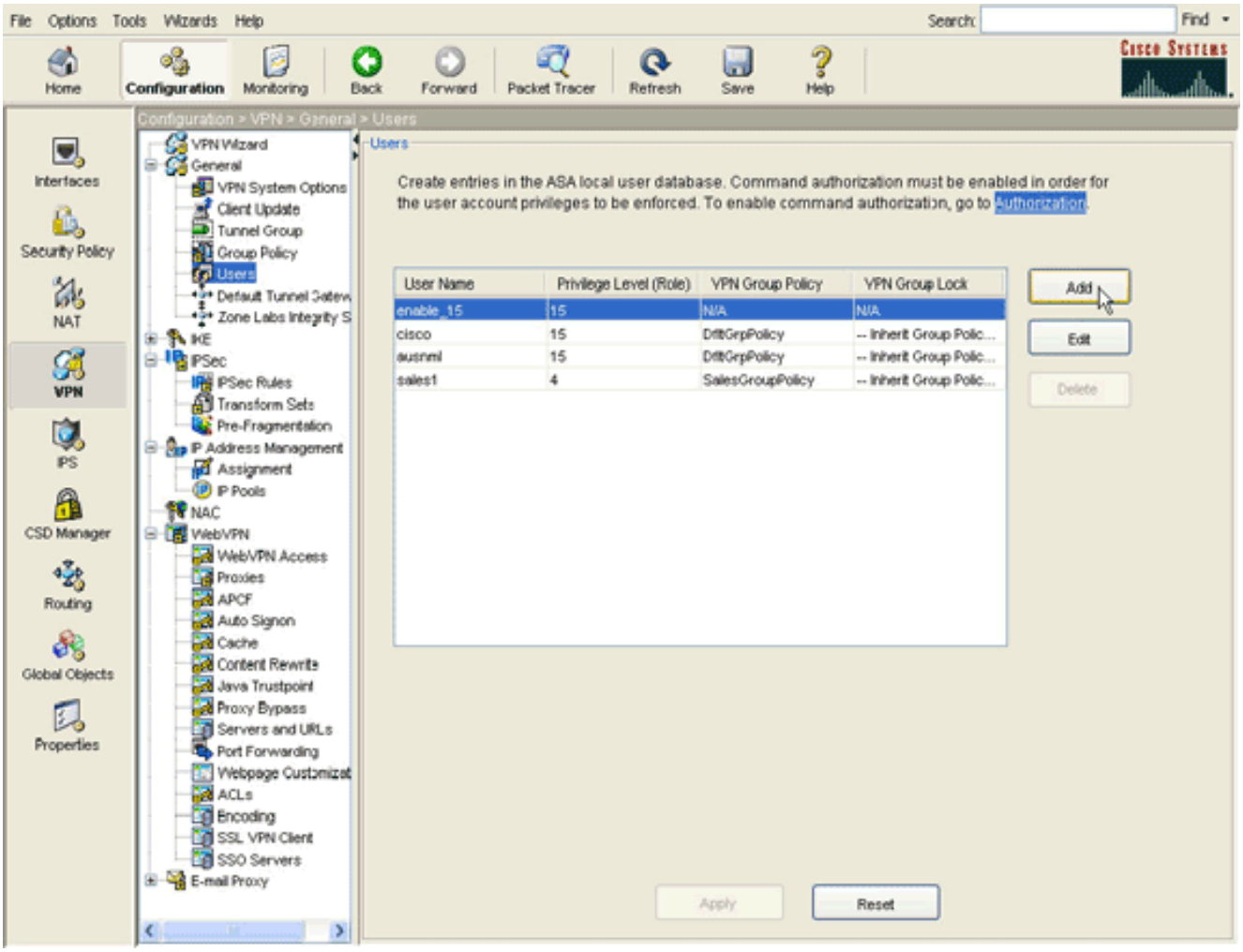


3. [Name] フィールドに名前を入力します。
4. [Group Policy] のドロップダウンの矢印をクリックして、手順 3 で作成したグループ ポリシーを選択します。
5. [OK] をクリックして、[Apply] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。これで、トンネル グループ、グループ ポリシー、およびポート フォワーディング特性がリンクされました。

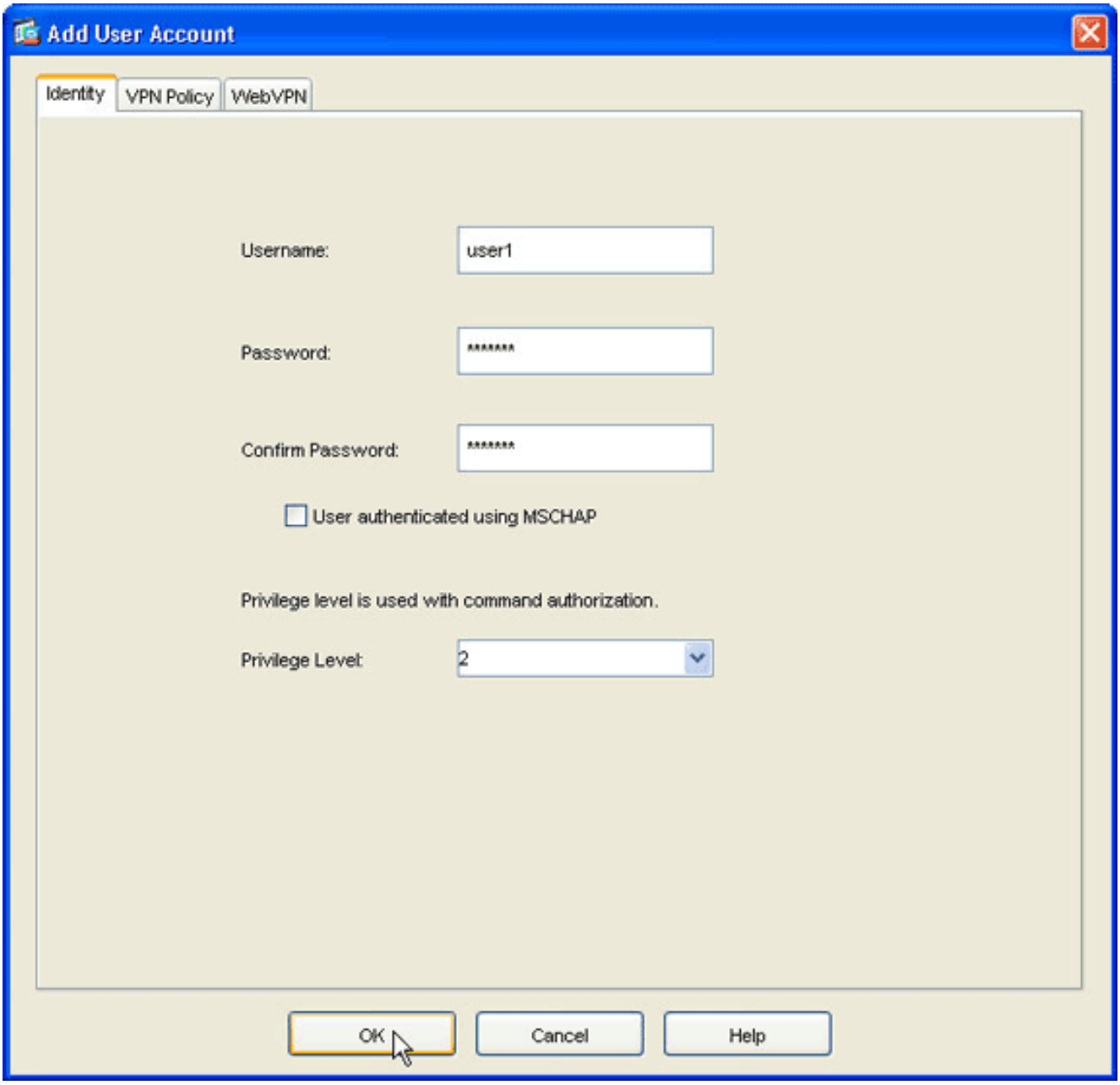
手順 5：ユーザを作成して、そのユーザをグループ ポリシーに追加する

ユーザを作成して、そのユーザをグループ ポリシーに追加するには、以下の手順に従います。

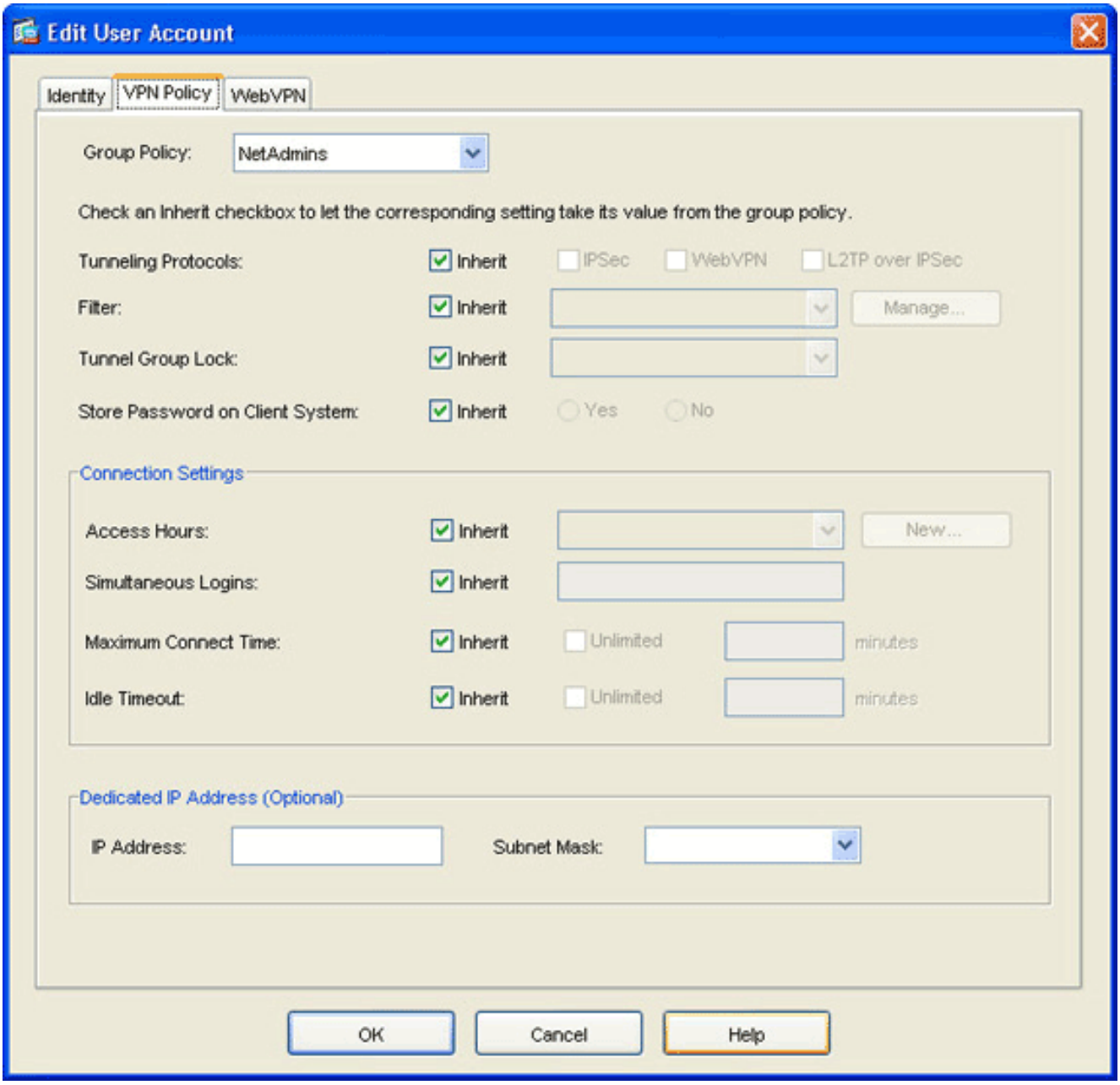
1. [General] を展開して、[Users] を選択します。



2. [Add] ボタンをクリックします。[Add User Account] ダイアログボックスが表示されます。



3. ユーザ名、パスワード、および特権情報の値を入力し、次に [VPN Policy] タブをクリックします。



4. [Group Policy] のドロップダウンの矢印をクリックして、手順 3 で作成したグループ ポリシーを選択します。このユーザは、選択したグループ ポリシーの WebVPN 特性およびポリシーを継承します。
5. [OK] をクリックして、[Apply] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

CLI を使用したシンクライアント SSL VPN 設定

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
```

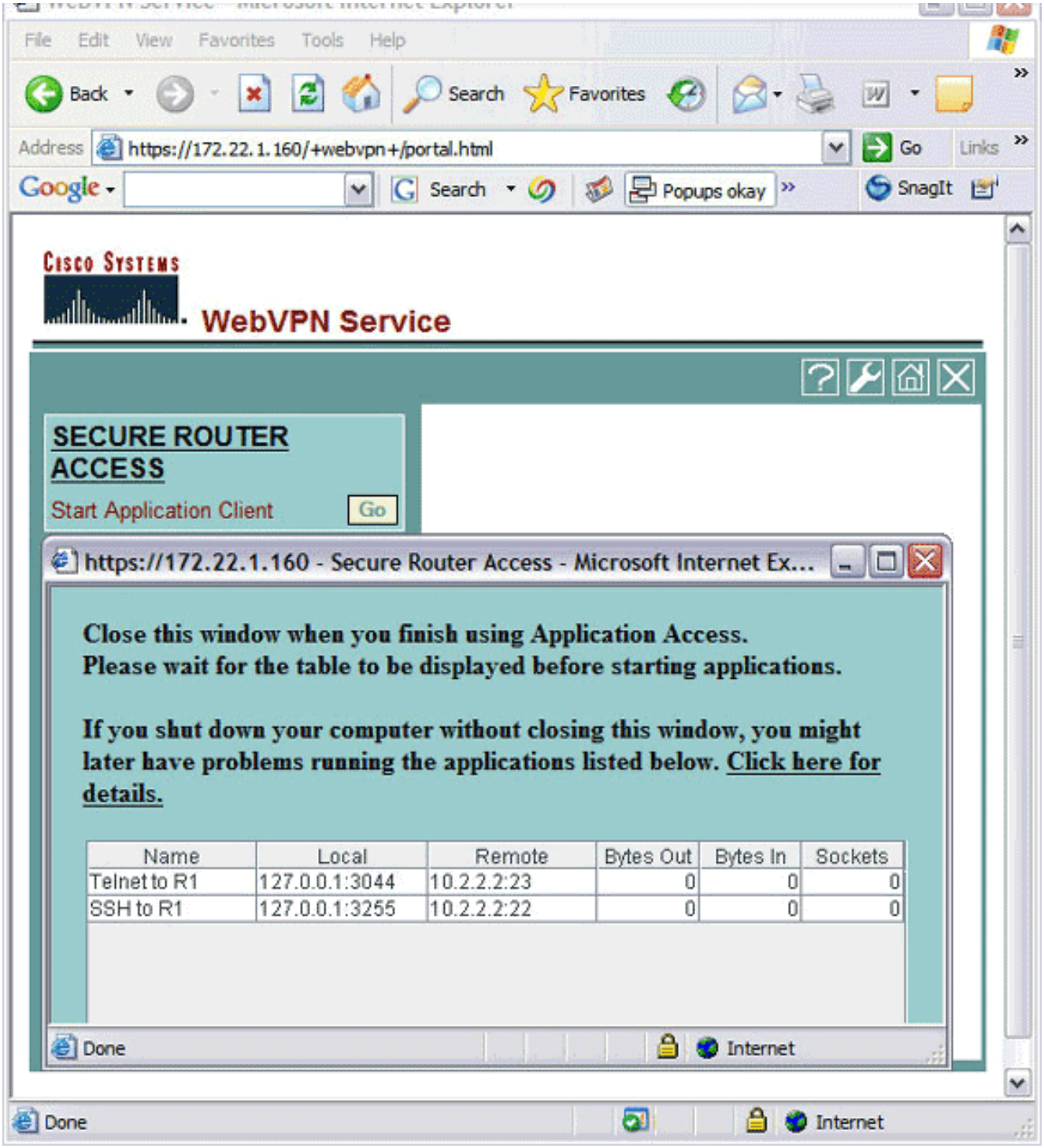
確認

このセクションでは、設定が正常に動作していることを確認します。

手順

この手順では、設定の有効性を調べる方法と設定をテストする方法を示します。

1. クライアント ワークステーションで、**https://*outside_ASA_IP Address*** と入力します。 ここで *outside_ASA_IPAddress* は、ASA の SSL URL です。デジタル証明書が受け入れられ、ユーザが認証されると、WebVPN Service Web ページが表示されます。

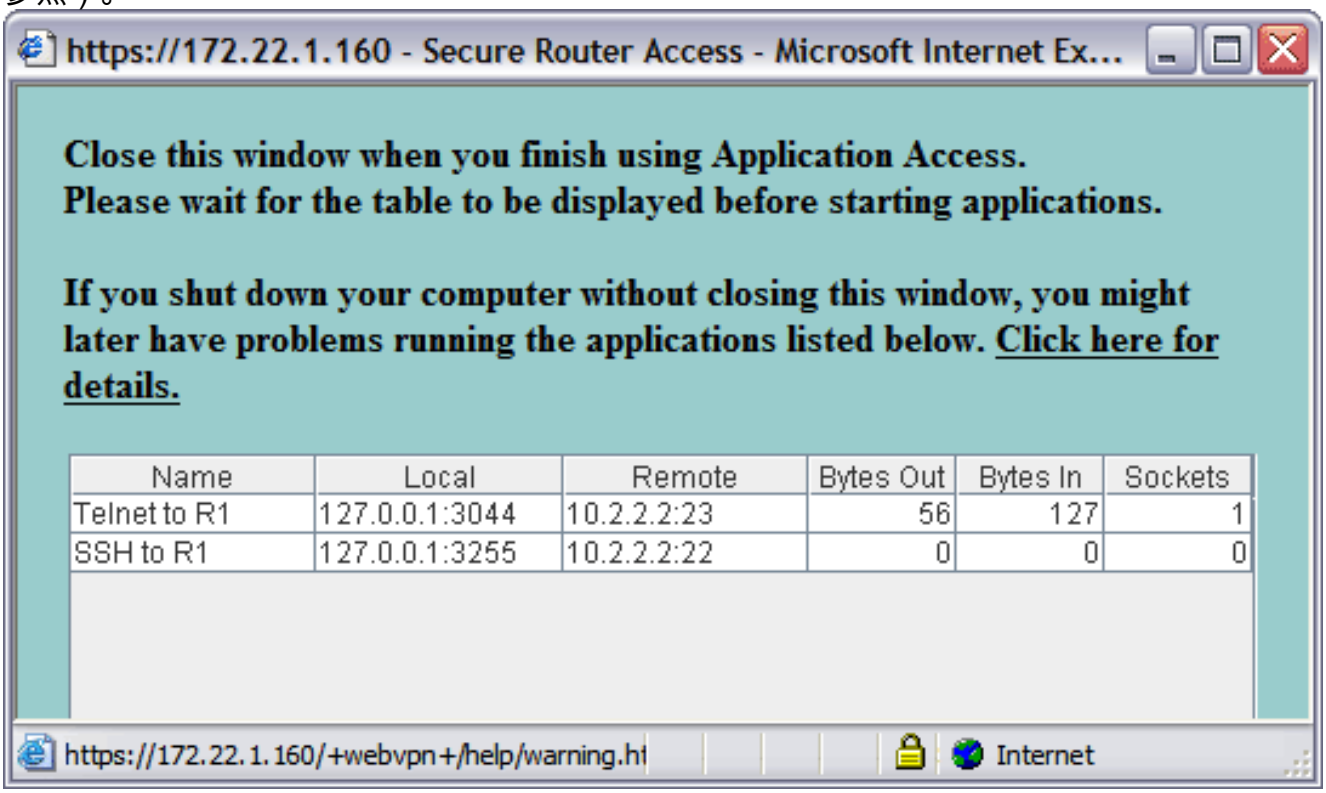


アプリケーションにアクセスするために必要なアドレスとポート情報が Local 列に表示されます。 この時点ではアプリケーションが起動していないため、Bytes Out 列および Bytes In 列に動作は表示されません。

2. DOS プロンプトまたはその他の Telnet アプリケーションを使用して、Telnet セッションを開始します。
3. コマンド プロンプトで **telnet 127.0.0.1 3044** と入力します。**注:** このコマンドは、このドキュメントの WebVPN Service Web ページの画像に表示されたローカル ポートにアクセスする方法の一例です。 *このコマンドには、コロン (:) が含まれていません。* このドキュメントで説明されているとおりに、コマンドを入力します。ASA は安全なセッション経由でコマンドを受け取ります。さらに、ASA は情報のマップを格納しているため、マップされたデバイスへの安全な Telnet セッションをすぐに開くことができます。

ユーザ名とパスワードを入力したら、デバイスへのアクセスは完了です。

4. デバイスへのアクセスを確認するには、Bytes Out 列および Bytes In 列を確認します（下図参照）。



コマンド

いくつかの **show** コマンドは WebVPN に関連しています。 これらのコマンドをコマンドラインインターフェイス（CLI）で実行して、統計情報や他の情報を表示できます。 **show** コマンドの詳細は、『WebVPN 設定の確認』を参照してください。

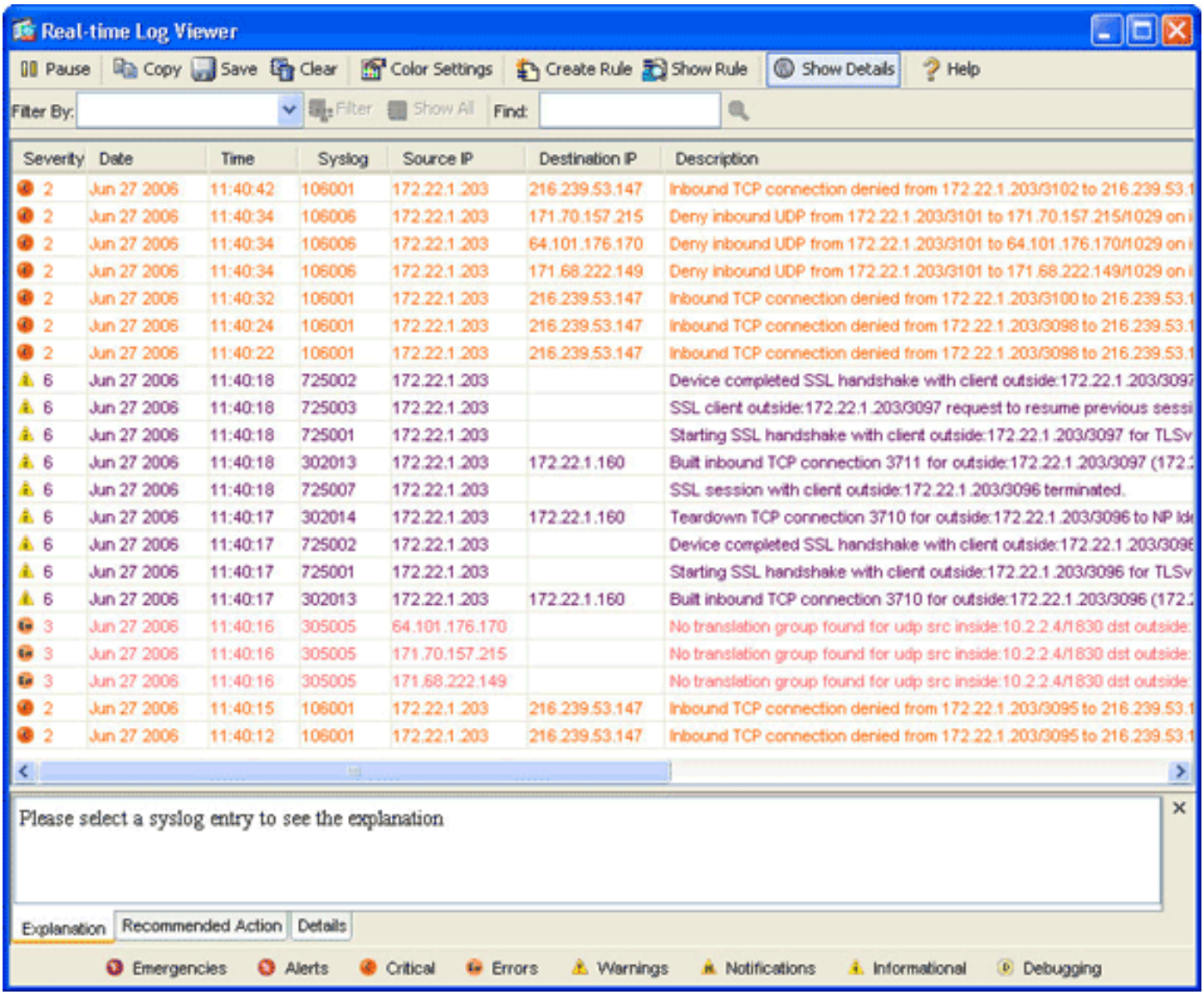
注: Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

SSL ハンドシェイク プロセスは完了しているか

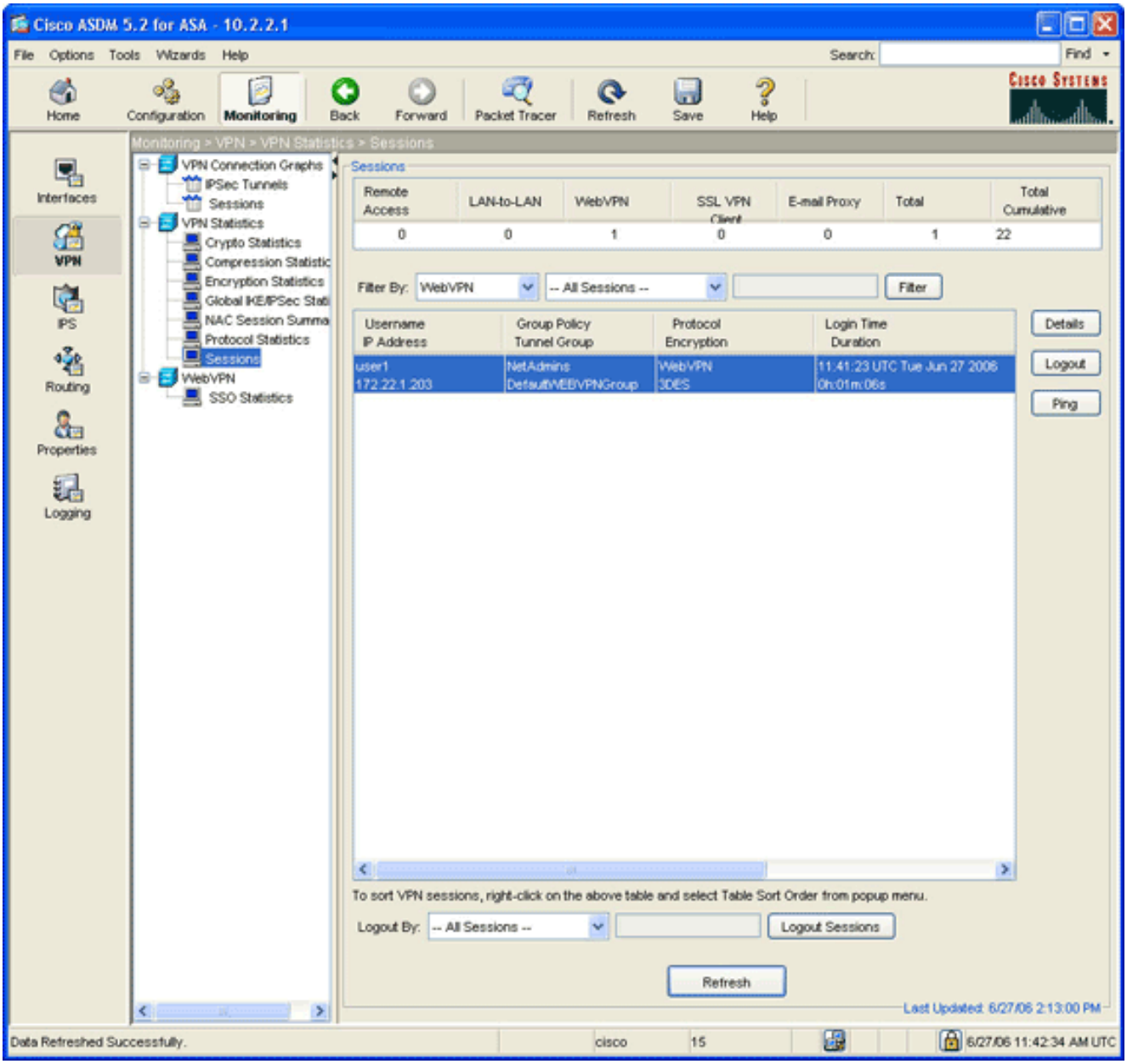
ASA に接続したら、リアルタイム ログに SSL ハンドシェイクの完了が表示されているか確認します。



SSL VPN シンクライアントは機能しているか

SSL VPN シンクライアントが機能していることを確認するには、以下の手順に従います。

1. [Monitoring] をクリックし、次に [VPN] をクリックします。
2. [VPN Statistics] を展開して、[Sessions] をクリックします。SSL VPN シンクライアント セッションがセッション リストに表示されます。 下図に示すように、必ず WebVPN でフィルタを適用してください。



コマンド

いくつかの **debug** コマンドは、WebVPN に関連しています。 これらのコマンドの詳細については、「WebVPN の Debug コマンドの使用」を参照してください。

注: debug コマンドを使用すると、Cisco デバイスに悪影響が及ぶ可能性があります。 **debug** コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

関連情報

- ASA でのクライアントレス SSL VPN (WebVPN) の設定例
- ASDM を使用した ASA での SSL VPN Client (SVC) の設定例
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- ASDM および NTLMv1 を使用した WebVPN およびシングル サインオン機能付き ASA の設定例
- テクニカルサポートとドキュメント - Cisco Systems