
# SVC の設定

SSL VPN Client（SVC）は、ネットワーク管理者がリモート コンピュータに IPSec VPN クライアントをインストールして設定しなくても、リモート ユーザが IPSec VPN クライアントの利点を活用できる VPN トンネリング テクノロジーです。SVC は、リモート コンピュータの既存の SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスをブラウザに入力します。ブラウザはそのインターフェイスに接続して WebVPN のログイン ウィンドウを表示します。ユーザがログインと認証を完了し、ユーザが SVC を*必要としている*ことをセキュリティ アプライアンスが確認すると、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロードします。セキュリティ アプライアンスが、SVC を使用する*オプション*がユーザにあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをウィンドウに表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC は自身のインストールと設定を実行します。接続終了時に（設定に応じて）、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

この項は、次の内容で構成されています。

# SVC のインストール

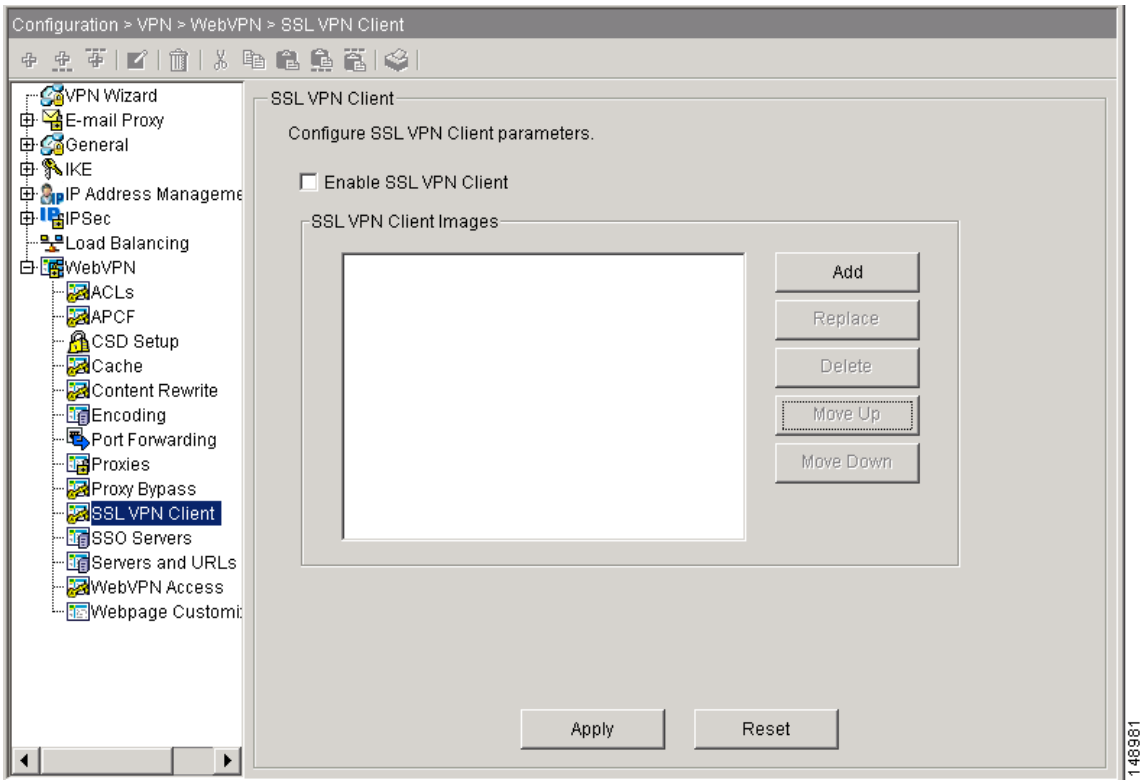
SVC のインストールは、SVC イメージをフラッシュ メモリにアップロードする手順、SVC イメージとして使用するフラッシュ メモリ上のファイルをセキュリティ アプライアンスに指定する手順、およびこのイメージをリモート コンピュータにダウンロードする順序を設定する手順で構成されています。

SVC をインストールするには、次の手順を実行します。

**ステップ 1**　SVC イメージをセキュリティ アプライアンスにアップロードします。ASDM ツールバーで、**Configuration** > **VPN** > **WebVPN** > **SSL VPN Client** を選択します。SSL VPN Client パネルが表示されます（図 3-1）。

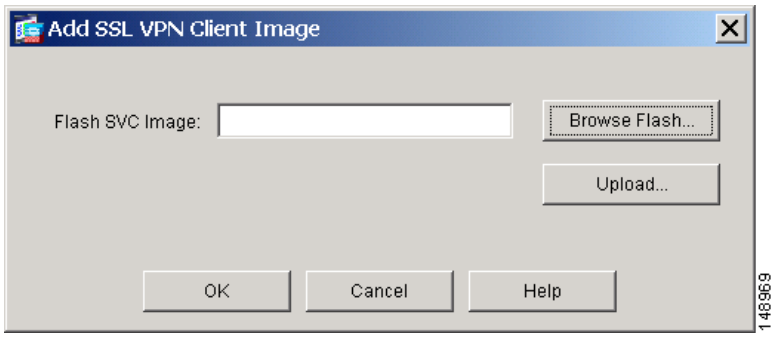
このウィンドウには、SVC イメージとして指定されているすべての SVC ファイルがリストされます。テーブルに表示される順序は、リモート コンピュータにダウンロードされる順序を反映しています。

**図 3-1　SSL VPN Client ウィンドウ**



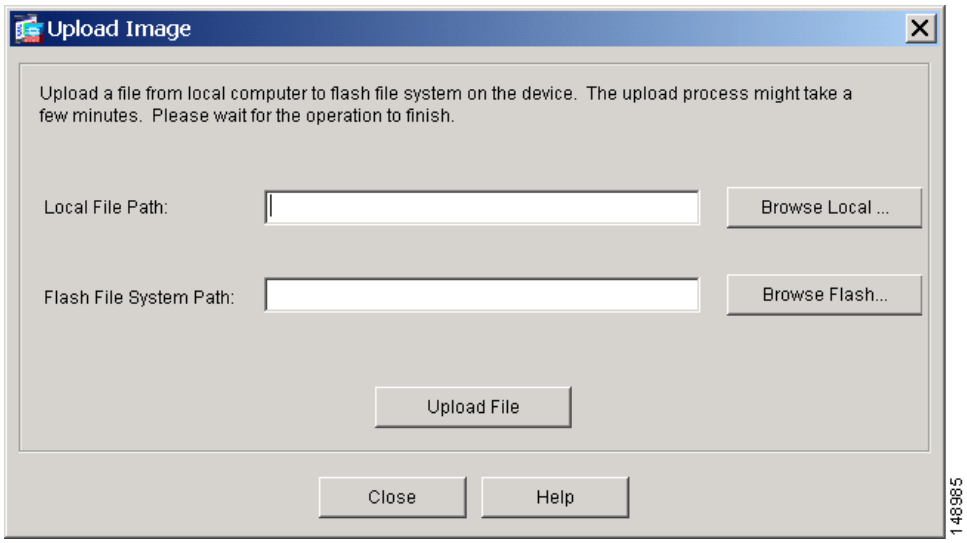

SVC イメージを追加するには、**Add** をクリックします。Add SSL VPN Client Image ダイアログボックスが表示されます（図 3-2）。

**図 3-2　Add SSL VPN Client Image ダイアログ**



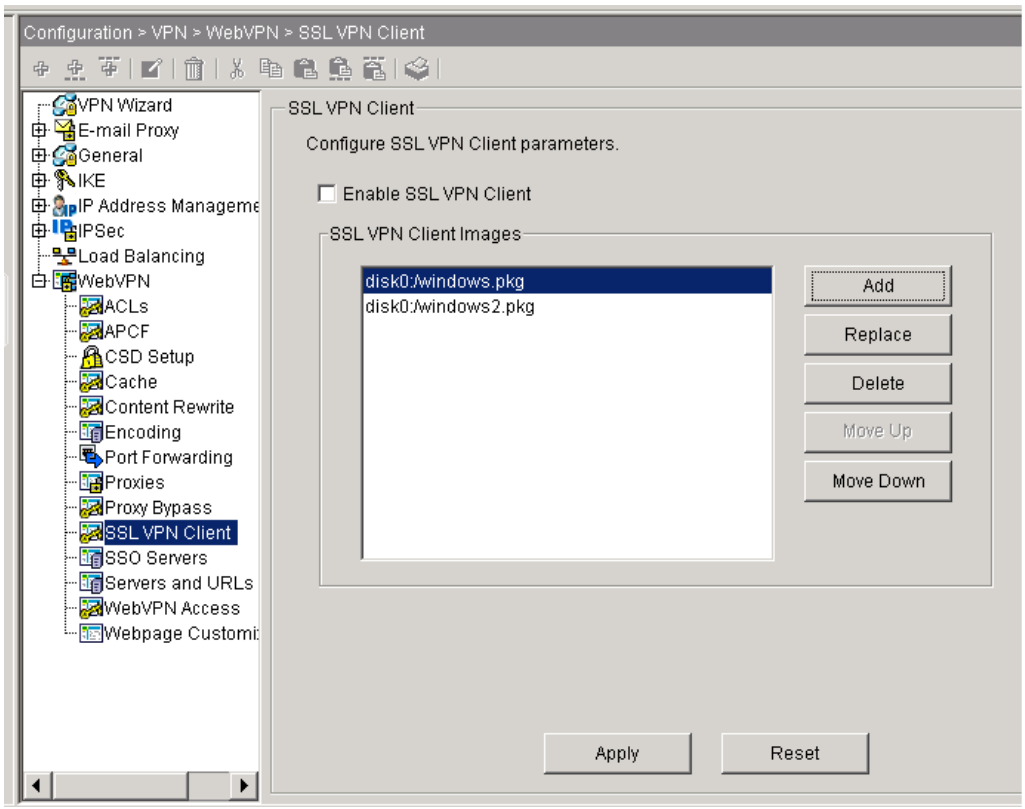

セキュリティ アプライアンスのフラッシュ メモリにすでにイメージがある場合は、Flash SVC Image フィールドにイメージの名前を入力して、**OK** をクリックします。それ以外の場合は、**Upload** をクリックして、ASDM を実行しているコンピュータを参照します。Upload Image ダイアログボックスが表示されます（図 3-3）。

**図 3-3　Upload Image ダイアログ**




Local File Path と Flash File System Path にパスを入力するか、パスを参照します。次に **Upload File** をクリックします。これで、SSL VPN Client ウィンドウに、指定した SVC イメージが表示されます（図 3-4）。

図 3-4　SVC イメージが表示された SSL VPN Client ウィンドウ

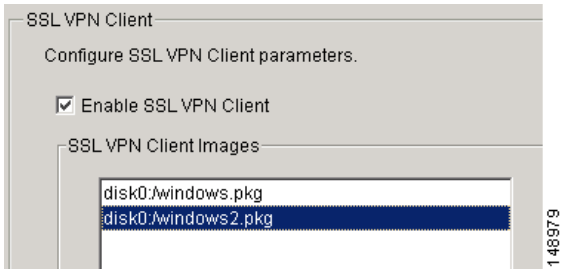



**ステップ 2**　イメージ名をクリックしてから、**Move Down** ボタンを使用して、リスト内のイメージの位置を変更します。

これにより、セキュリティ アプライアンスがリモート コンピュータにダウンロードする順序が設定されます。イメージ リストの一番上にある SVC イメージからダウンロードされます。このため、最も一般的なオペレーティング システムが使用するイメージをリストの一番上に移動する必要があります。

**ステップ 3**　**Enable SSL VPN Client** チェックボックスをオンにし、セキュリティ アプライアンスによる SVC イメージのダウンロードをイネーブルにします（図 3-5）。

図 3-5　Enable SSL VPN Client チェックボックス

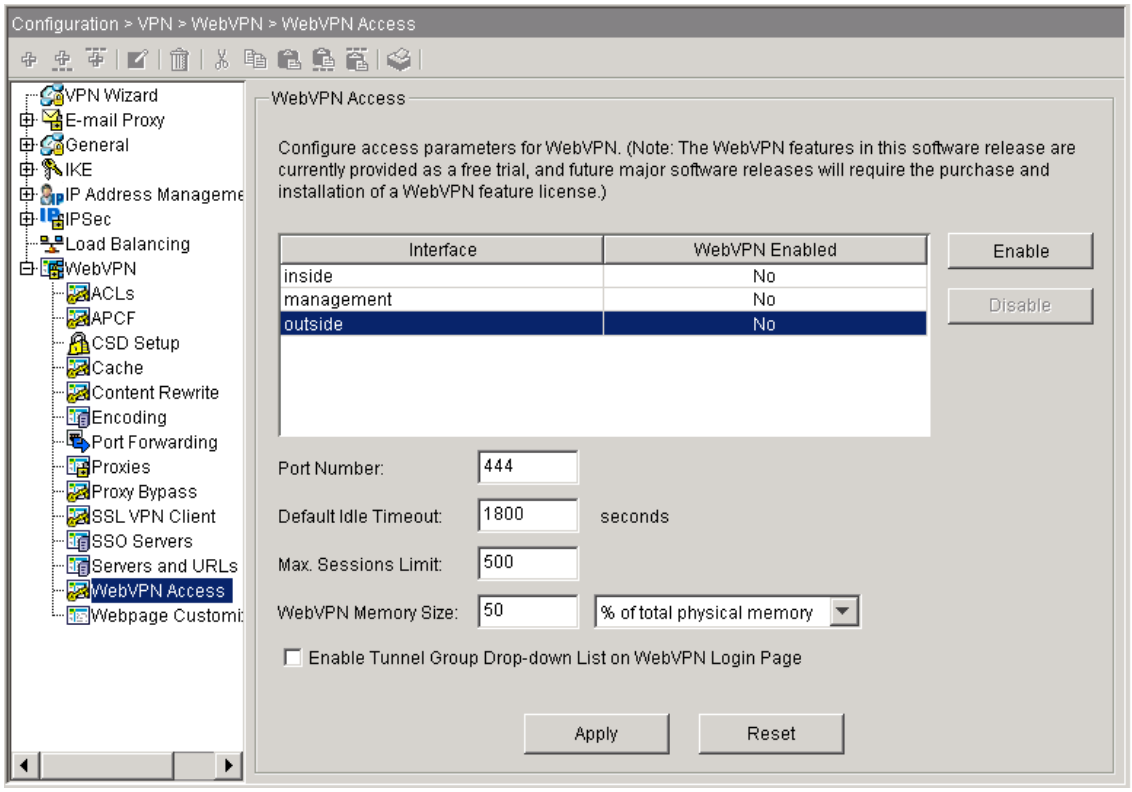


# SVC の設定

SVC を設定するには、次の手順を実行します。

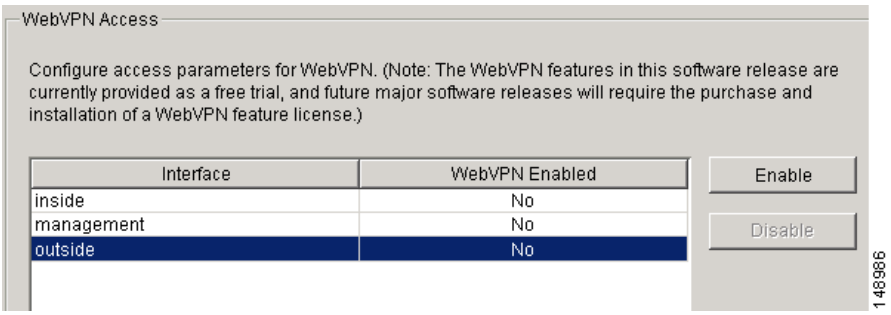
**ステップ 1**　インターフェイス上の WebVPN をイネーブルにします。ナビゲーション ペインから、**WebVPN Access** を選択します。WebVPN Access ウィンドウが表示されます（図 3-6）。

**図 3-6　WebVPN Access ウィンドウ**




インターフェイスを選択して、**Enable** をクリックします（図 3-7）。

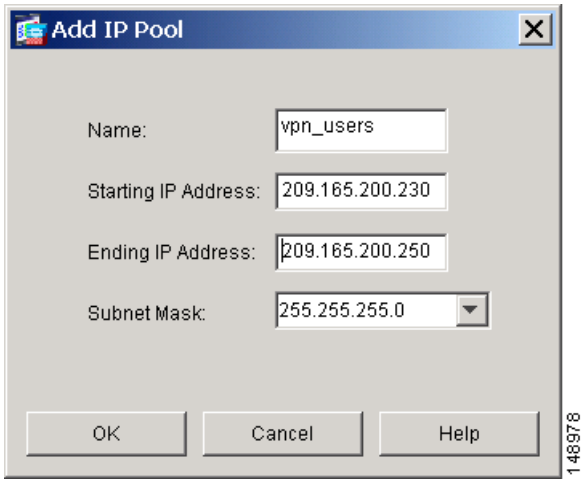
**図 3-7　インターフェイスのイネーブル化**



**ステップ 2**　アドレス割り当ての方式を設定します。DHCP とユーザ割り当てアドレッシングのいずれか 1 つ、または両方を使用できます。ローカル IP アドレス プールを作成して、プールをトンネル グループに割り当てることもできます。

IP アドレス プールを作成するには、**Configuration > VPN > IP Address Management > IP Pools** を選択します。**Add** をクリックします。Add IP Pool ダイアログが表示されます（図 3-8）。

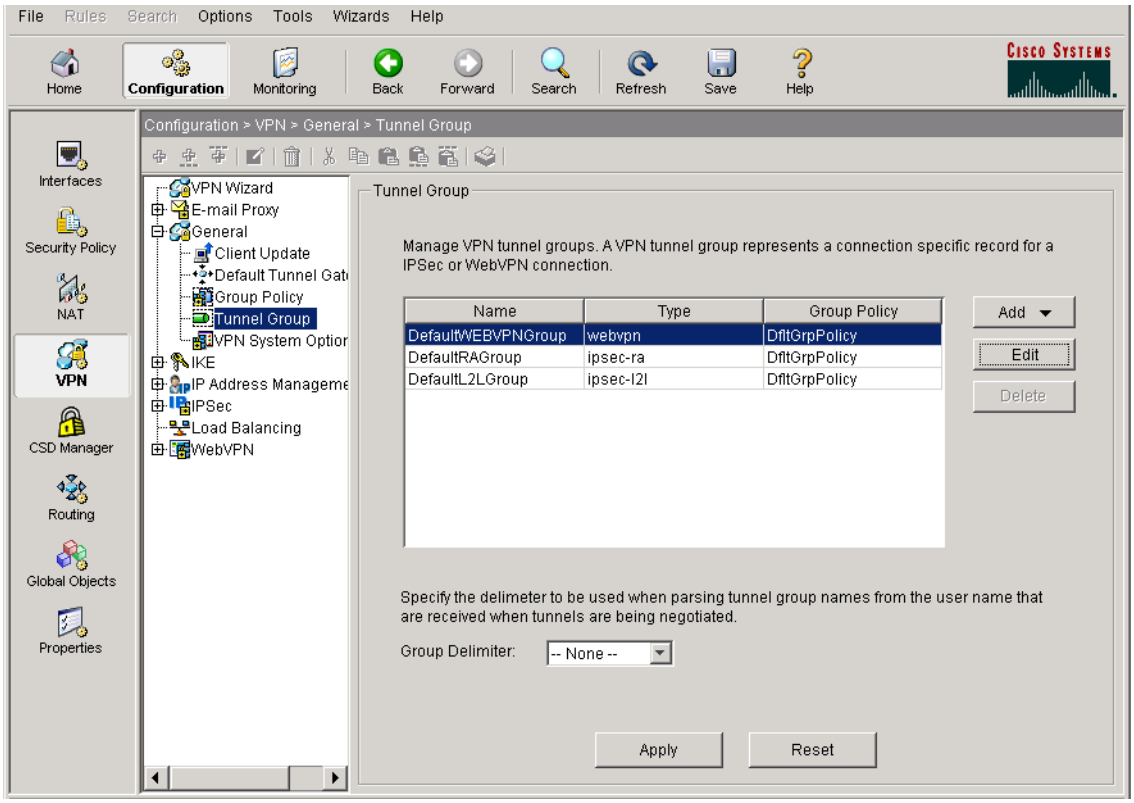
**図 3-8　Add IP Pool ダイアログ**




新しい IP アドレス プールの名前を入力します。開始 IP アドレスと終了 IP アドレスを入力してから、サブネット マスクを入力し、**OK** をクリックします。

**ステップ 3**　トンネル グループに IP アドレス プールを割り当てます。これを行うには、**Configuration > VPN > General > Tunnel Group** を選択します。Tunnel Group パネルが表示されます（図 3-9）。

図 3-9　Tunnel Group ウィンドウ



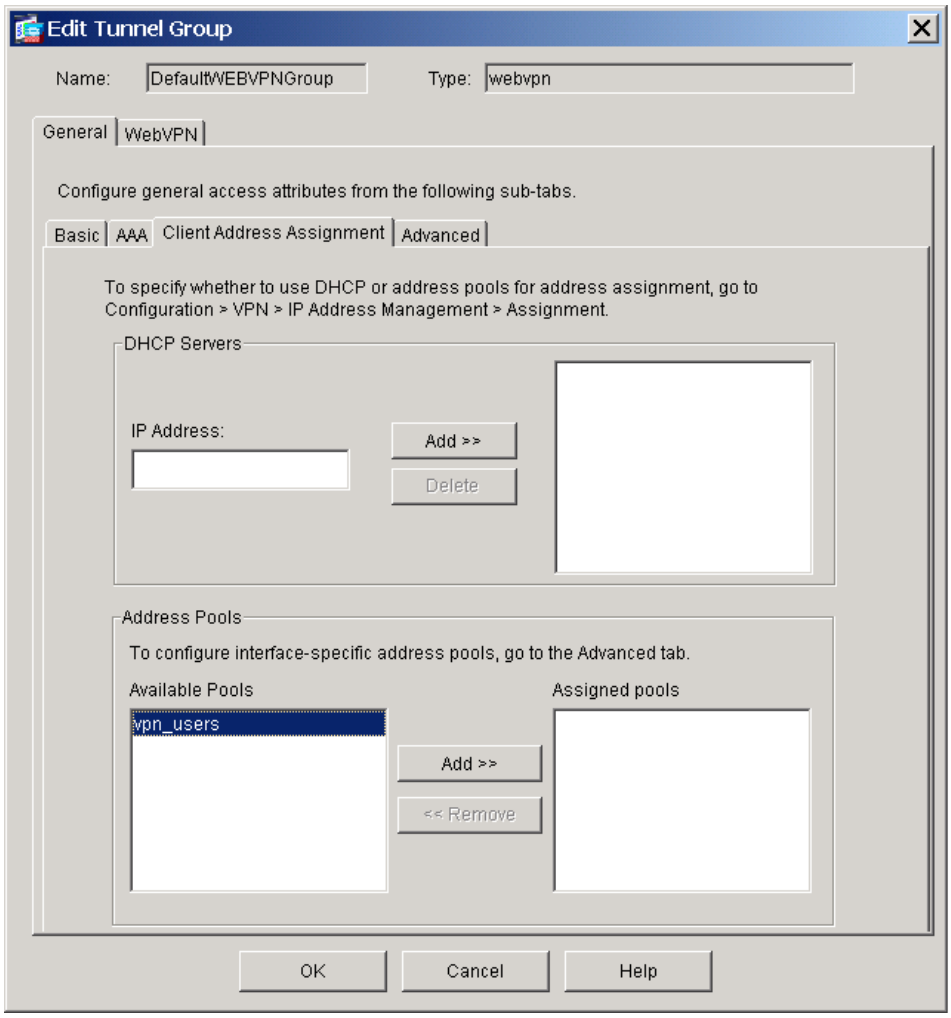

**ステップ 4**　テーブル内のトンネル グループを選択して、**Edit** をクリックします。

Edit Tunnel Group ダイアログが表示されます。

**ステップ 5**　**Client Address Assignment** タブをクリックします。

Address Pools グループ ボックスを含む **Client Address Assignment** タブが表示されます（図 3-10）。

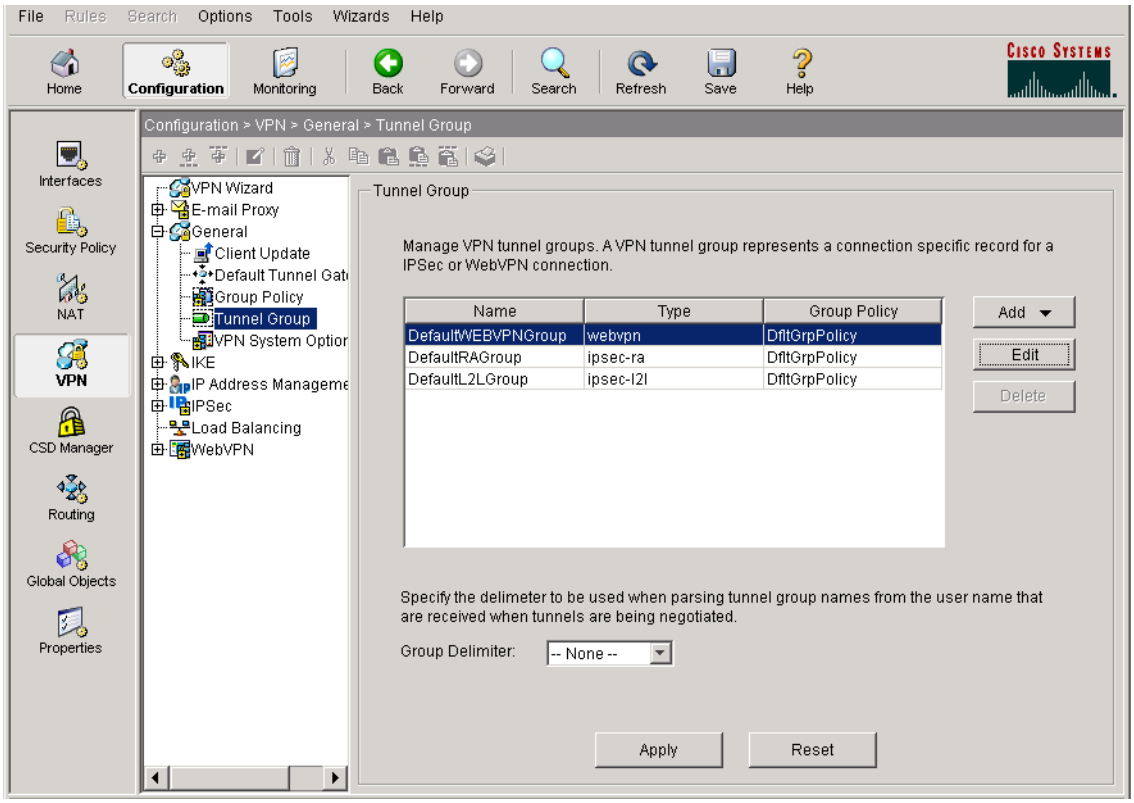
図 3-10　Edit Tunnel Group、General タブ、Client Address Assignment タブ




Address Pools グループ ボックスで、トンネル グループに割り当てるアドレス プールを選択して、**Add** をクリックします。

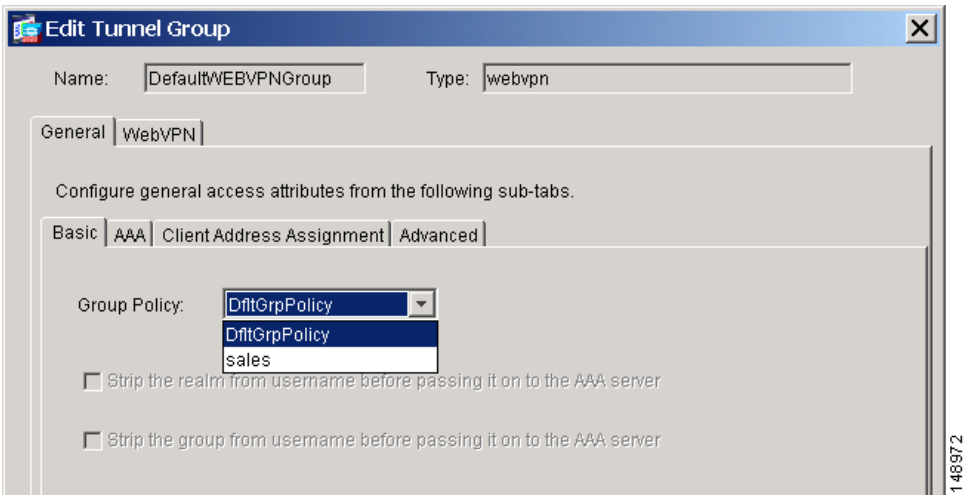
**ステップ 6**　トンネル グループにデフォルトのグループ ポリシーを割り当てます。**Configuration > VPN > General > Tunnel Group** を選択します。Tunnel Group ウィンドウが表示されます（図 3-11）。

**図 3-11　Tunnel Group ウィンドウ**




テーブルから WebVPN トンネル グループを選択して、**Edit** をクリックします。Edit Tunnel Group ダイアログ、**General** タブが表示されます（図 3-12）。

**図 3-12　Edit Tunnel Group ダイアログ、General タブ、Basic タブ**

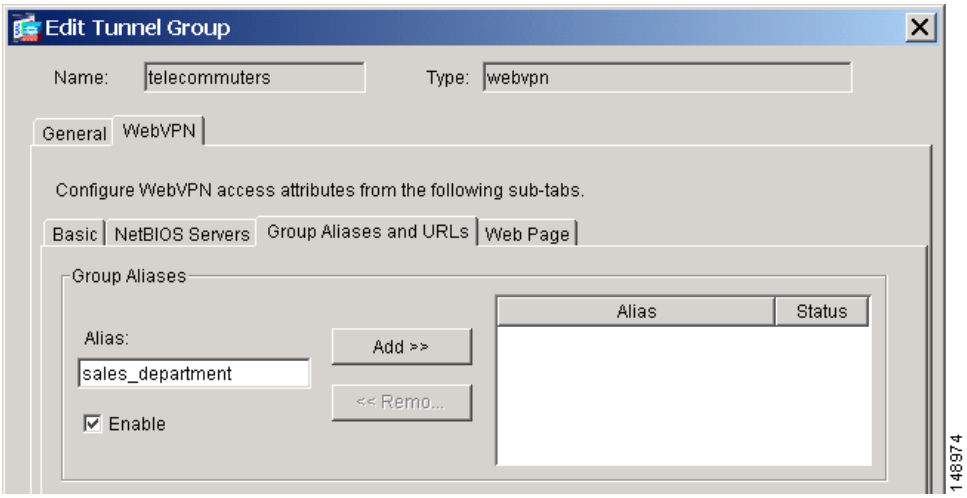



Group Policy リスト内のグループ ポリシーを選択して、**OK** をクリックします。

**ステップ 7**　WebVPN Login ページのグループ リストに表示されるグループ エイリアスを作成し、イネーブルにします。

**WebVPN** タブをクリックしてから、**Group Aliases and URLs** タブをクリックします。Group Aliases and URLs タブが表示されます（図 3-13）。

**図 3-13　Edit Tunnel Group ダイアログ、WebVPN タブ、Group Aliases and URLs タブ**



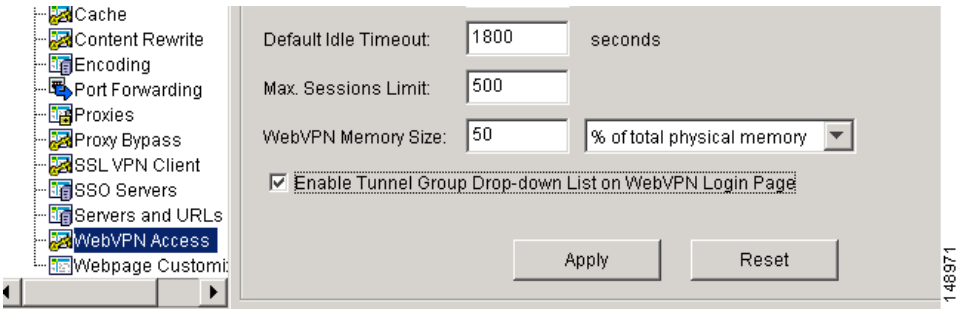

Alias フィールドに新しいエイリアスの名前を入力します。**Add** をクリックして、新しいエイリアスとして追加します。

**Enable** チェックボックスをオンにして、グループ エイリアスと URL をイネーブルにします。

**ステップ 8**　WebVPN Login ページ上のトンネルグループ リストの表示をイネーブルにします。

**Configuration > VPN > WebVPN > WebVPN Access** を選択します。WebVPN Access パネルが表示されます（図 3-14）。**Enable Tunnel Group Drop-Down List on WebVPN Login Page** チェックボックスをオンにして、**Apply** をクリックします。

**図 3-14　WebVPN Access ウィンドウ、Enable Tunnel Group Drop-Down List on WebVPN Login Page チェックボックス**

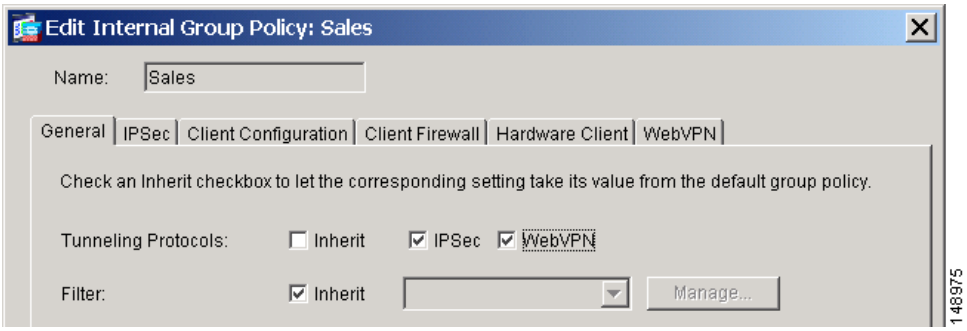


**ステップ 9**　グループまたはユーザで許可される VPN トンネリング プロトコルとして WebVPN を指定します。

ナビゲーション ペインから **Configuration > VPN > General > Group Policy** を選択します。Group Policy テーブル内のグループ ポリシーを選択して、**Edit** をクリックします。

Edit Internal Group Policy ダイアログの General タブが表示されます（図 3-15）。

**図 3-15　Edit Internal Group Policy、General タブ**




**WebVPN** チェックボックスをオンにして、トンネリング プロトコルとして WebVPN を追加します。

**ステップ 10**　ユーザまたはグループの SVC 機能を設定します。Edit User Accounts ダイアログと Edit Group Policy ダイアログの両方の **SSL VPN Client** タブにこれらの機能が表示されます。

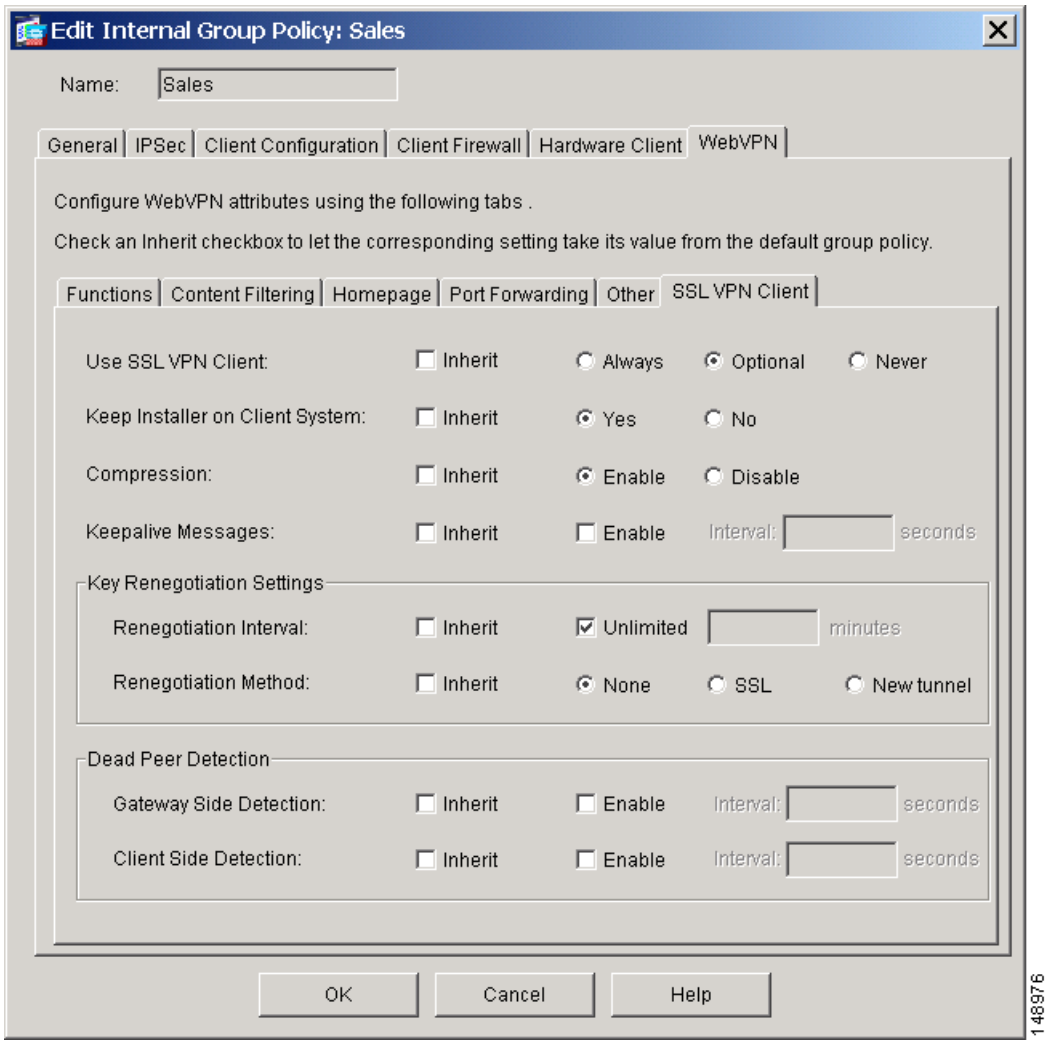
ユーザの **SSL VPN Client** タブを表示するには、次の手順を実行します。

- **Configuration > Properties > Device Administration > User Accounts** をクリックします。User Accounts パネルが表示されます。
- テーブル内のユーザを選択して、**Edit** をクリックします。Edit User Account ダイアログ、**General** タブが表示されます。
- **WebVPN** タブをクリックしてから、**SSL VPN** タブをクリックします。**SSL VPN Client** タブが表示されます（図 3-16）。

グループの **SSL VPN Client** タブを表示するには、次の手順を実行します。

- **Configuration > VPN > WebVPN > Group Policies** をクリックします。Group Policy パネルが表示されます。
- テーブル内のグループ ポリシーを選択して、**Edit** をクリックします。Edit Internal Group Policy ダイアログ、**General** タブが表示されます。
- **WebVPN** タブをクリックしてから、**SSL VPN** タブをクリックします。**SSL VPN Client** タブが表示されます。これは図 3-16 のユーザ アカウントで表示された **SSL VPN Client** タブと同じですが、こちらには **Inherit** チェックボックスが含まれていません。

図 3-16　SSL VPN Client タブ




（注）　ユーザ アカウントの場合、**SSL VPN Client** タブには、SVC 機能ごとにさらに **Inherit** チェックボックスが含まれます。**Inherit** チェックボックスをオンにすると、ユーザのグループ ポリシー内の設定に応じて機能が設定されます。

SSL VPN Client タブで次の機能を設定します。

**Use SSL VPN Client**：ユーザまたはグループで SVC を必須、オプション、またはディセーブルにします。

**Keep Installer on Client System**：リモート コンピュータの相手先固定 SVC のインストールをイネーブルにします。これにより、SVC の自動アンインストール機能がディセーブルになります。後続の SVC 接続では、SVC がリモート コンピュータにインストールされたままの状態になるため、リモート ユーザの SVC への接続時間が短縮されます。

**Compression**：SVC 圧縮は、転送されるパケットのサイズを減らすことによって、セキュリティ アプライアンスと SVC 間の通信パフォーマンスを向上させます。

**Keepalive Messages**：**Enable** チェックボックスをオンにし、キープアライブ メッセージの間隔をイネーブルにして調整し、接続のアイドル状態を維持できる時間がデバイスで制限される場合でも、プロキシ、ファイアウォール、または NAT デバイス経由の SVC 接続を開かれたままの状態にしておきます。

また、間隔を調整することによって、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースのアプリケーションをアクティブに実行していないときに SVC が接続を解除して再接続しないようにすることができます。

seconds フィールドは、15 ～ 600 秒の範囲でメッセージの間隔を指定します。

**Key Renegotiation Settings** ：セキュリティ アプライアンスと SVC が鍵を再生成するときは、暗号鍵と初期ベクトルを再ネゴシエーションして接続のセキュリティを強化します。

- **Renegotiation Interval : Unlimited** チェックボックスをオフにして、セッションの開始から鍵の再生成までの分数を、1 ～ 10080（1 週間）で指定します。
- **Renegotiation Method : None** チェックボックスをオンにして鍵の再生成をディセーブルにしたり、**SSL** チェックボックスをオンにして鍵の再生成時の SSL 再ネゴシエーションを指定したり、**New tunnel** チェックボックスをオンにして SVC 鍵の再生成時に新しいトンネルを確立したりします。

**Dead Peer Detection**：Dead Peer Detection（DPD）は、ピアが応答していないために失敗した接続をセキュリティ アプライアンス（ゲートウェイ）または SVC で迅速に検出できるようにします。

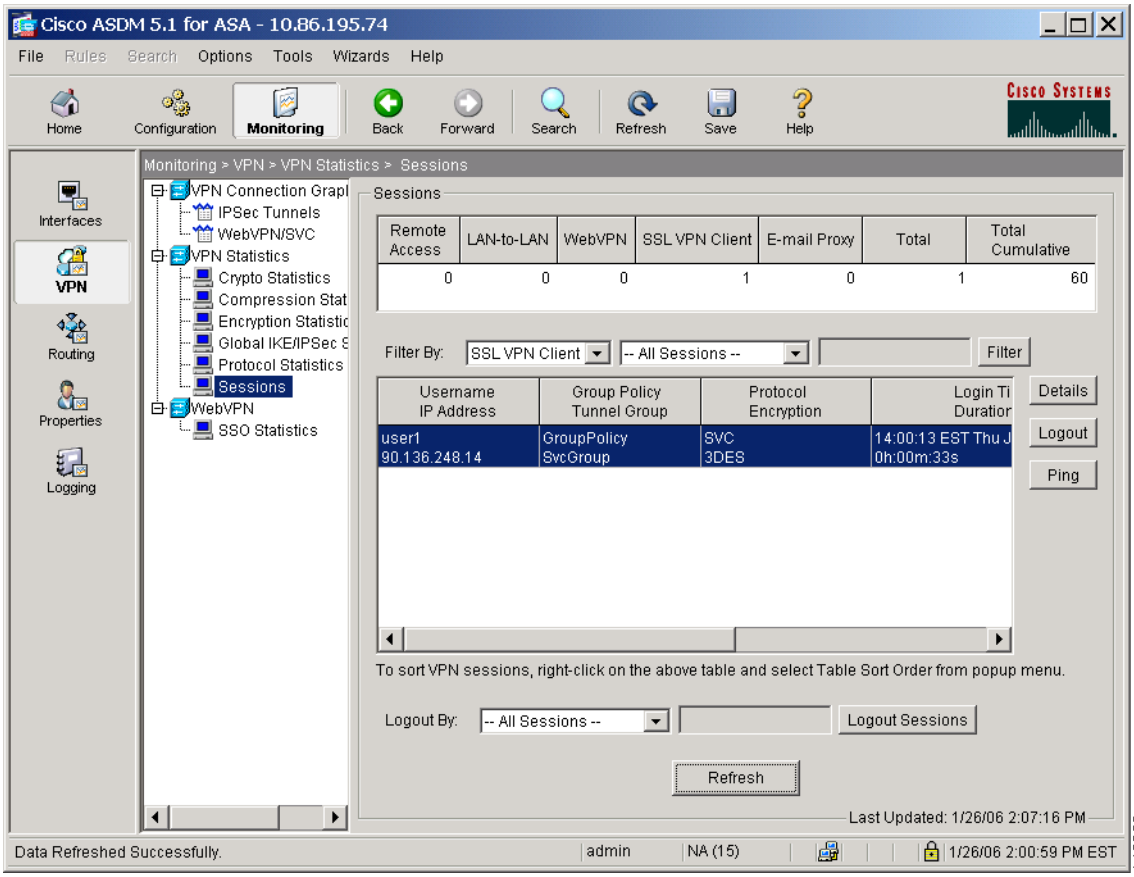
- **Gateway Side Detection : Enable** チェックボックスをオンにして、セキュリティ アプライアンス（ゲートウェイ）での DPD の実行を指定します。セキュリティ アプライアンスが DPD を実行する間隔を、30 ～ 3600 秒で入力します。
- **Client Side Detection : Enable** チェックボックスをオンにして、SVC（クライアント）での DPD の実行を指定します。SVC が DPD を実行する間隔を、30 ～ 3600 秒で入力します。

# SVC セッションの表示

Sessions ウィンドウでアクティブな SVC セッションに関する情報を表示できます。

**Monitoring > VPN > VPN Statistics > Sessions** を選択します。Sessions ウィンドウが表示されます（図 3-17）。

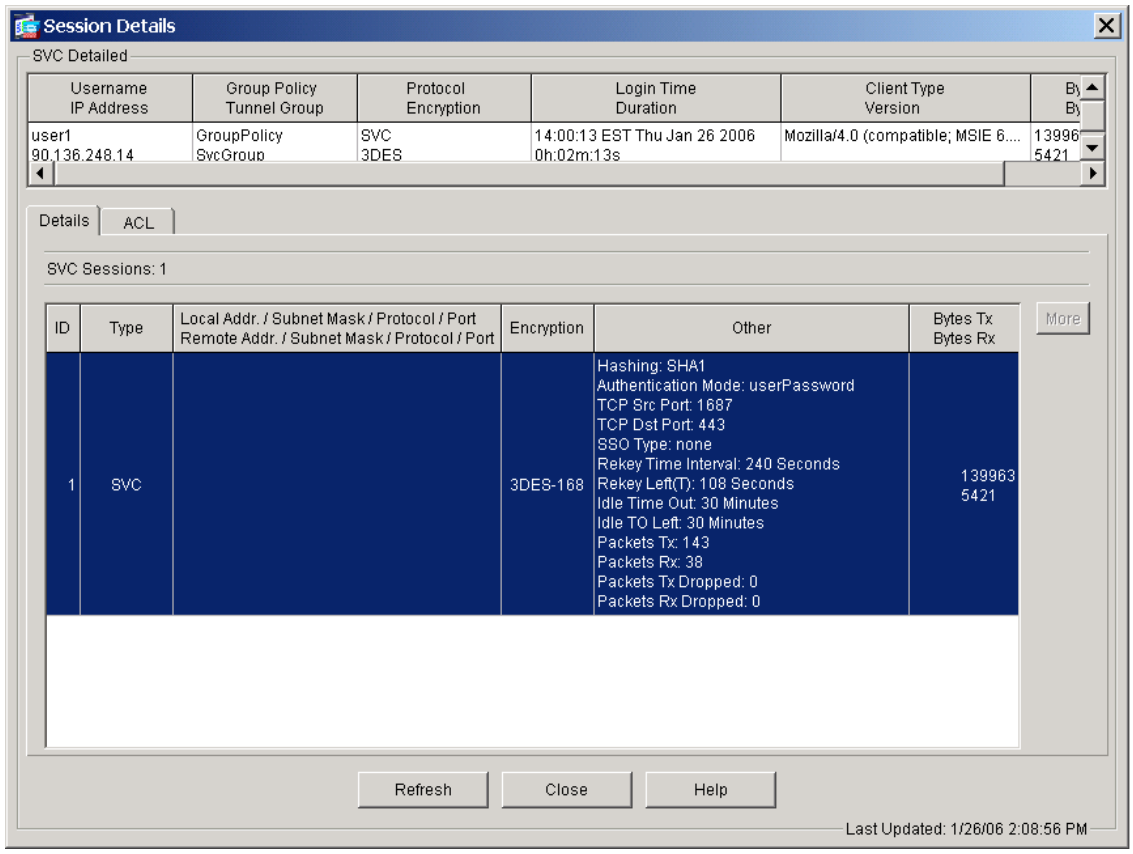
**図 3-17　VPN Statistics Sessions ウィンドウ**




Session Details ウィンドウでは、アクティブな SVC セッションに関する詳細情報を表示できます。

セッション テーブル内のセッションを選択して、**Details** をクリックします。Session Details ウィンドウが表示されます（図 3-18）。

図 3-18　Session Details ウィンドウ



# SVC セッションのログオフ

すべての SVC セッションをログオフするには、Session テーブルのアクティブ セッションのリストから終了するセッションを選択します。

**Logout** をクリックします。セッションが終了します。

**図 3-19　セッションのログオフ**