L2TP over IPSec の設定

この章では、ASDM を使用してセキュリティ アプライアンス上に L2TP over IPSec を設定する方法について説明します。この章には、次の項があります。

L2TP の概要

Layer 2 Tunneling Protocol（L2TP）は、リモート クライアントがパブリック IP ネットワーク経由でプライベート企業ネットワーク サーバと安全に通信できる VPN トンネリング プロトコルです。L2TP は PPP over UDP（ポート 1701）を使用してデータをトンネリングします。

L2TP プロトコルは、クライアント / サーバ モデルに基づいています。この機能は、L2TP ネットワーク サーバ（LNS）と L2TP アクセス コンセントレータ（LAC）との間で分割されます。通常 LNS はルータなどのネットワーク ゲートウェイで実行され、LAC は、ダイヤルアップ ネットワーク アクセス サーバ（NAS）や、Microsoft Windows 2000 などの L2TP クライアントがバンドルされた PC などで実行されます。

IPSec を使用する L2TP をリモート アクセス シナリオで設定することの最大の利点は、リモート ユーザが、ゲートウェイや専用回線を使用せずにパブリック IP ネットワーク経由で VPN にアクセスできるため、POTS を使用してほとんどどこからでもリモート アクセスができることです。その他の利点として、クライアントの要件が、マイクロソフトの Dial-Up Networking（DUN; ダイヤルアップ ネットワーク）搭載の Windows 2000 だけであることです。Cisco VPN クライアント ソフトウェアなど、その他のクライアント ソフトウェアは必要ありません。

IPSec を使用する L2TP の設定では、事前共有鍵や RSA シグニチャ方式を使用した証明書、および動的（固定ではない）暗号マップの使用がサポートされています。このタスクの説明では、IKE と事前共有鍵または RSA シグニチャ設定が完了していると想定します。

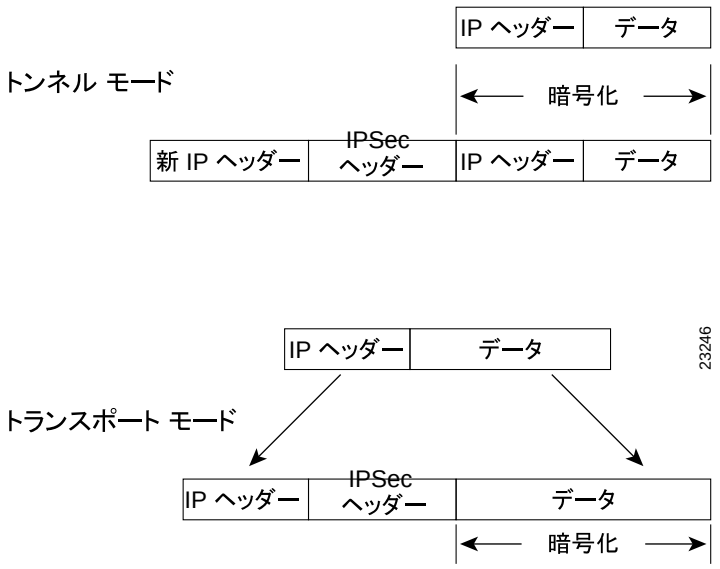
（注）　セキュリティ アプライアンスで IPSec を用いる L2TP を使用すると、LNS が Windows 2000 L2TP クライアントと相互運用できます。Cisco や他のベンダーと LAC との相互運用は、現在サポートされていません。セキュリティ アプライアンスでサポートされているのは IPSec を使用する L2TP だけで、L2TP 自体はサポートされていません。
Windows 2000 クライアントによってサポートされている最小限の IPSec セキュリティ アソシエーション ライフタイムは、300 秒です。セキュリティ アプライアンスを 300 秒未満に設定すると、Windows 2000 クライアントはそれを無視して、ライフタイムを 300 秒に設定し直します。

IPSec トランスポートとトンネル モード

デフォルトで、セキュリティ アプライアンスは IPSec トンネル モードを使用します。つまり、元の IP データ グラム全体が暗号化されて、新しい IP パケット内でペイロードとなります。このモードでは、ルータなどのネットワーク デバイスが IPSec プロキシとして動作できます。言い換えると、ルータがホストの代わりに暗号化を実行するということです。発信元ルータがパケットを暗号化し、IPSec トンネル経由で転送します。宛先ルータは、元の IP データグラムを復号化し、宛先システムに転送します。トンネルモードの最大の利点は、IPSec の利点を得るためにエンド システムを変更する必要がないことです。トンネル モードはトラフィック分析を防止します。トンネル モードを使用することで、攻撃者はトンネルのエンドポイントを判別できるだけで、トンネルされたパケットの本当の発信元や宛先はわかりません。このことは、たとえ発信元や宛先がトンネル エンドポイントと同じであっても同じです。

ただし Windows 2000 L2TP/IPSec クライアントは IPSec トランスポート モードを使用しているため、IP ペイロードだけが暗号化され、元の IP ヘッダーは元のまま残されます。このモードは、各パケットにわずか数バイト追加するだけで、パブリック ネットワーク上のデバイスがパケットの最終的な発信元と宛先がわかるという利点があります。図 10-1 に、IPSec のトンネル モードとトランスポート モードの違いを示します。

図 10-1　トンネル モードとトランスポート モードの IPSec



したがって、Windows 2000 L2TP/IPSec クライアントでセキュリティ アプライアンスに接続するためには、IPSec トランスポート モードを設定してトランスフォームする必要があります（ステップ 1 を参照）。この機能（トランスポート）を使用すると、IP ヘッダー内の情報に基づいて、中間ネットワーク上で特別な処理（たとえば、QoS）を実行できます。しかし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査は制限されます。IP ヘッダーをクリア テキストで伝送した場合、トランスポート モードでは攻撃者がトラフィック分析を実行できます。

（注）　セキュリティ アプライアンスに Cisco VPN Client Version バージョン 3.x またはバージョン 2.5 がインストールされていると、Windows 2000 で L2TP/IPSec トンネルを確立できません。Windows 2000 の Services パネルで、Cisco VPN Client バージョン 3.x の *Cisco VPN Service* または Cisco VPN Client バージョン 2.5 の *ANetIKE Service* を無効にします（**Start > Programs > Administrative Tools > Services** をクリック）。次に、**Services** パネルから IPSec Policy Agent Service を再起動し、マシンをリブートします。

L2TP over IPSec の設定

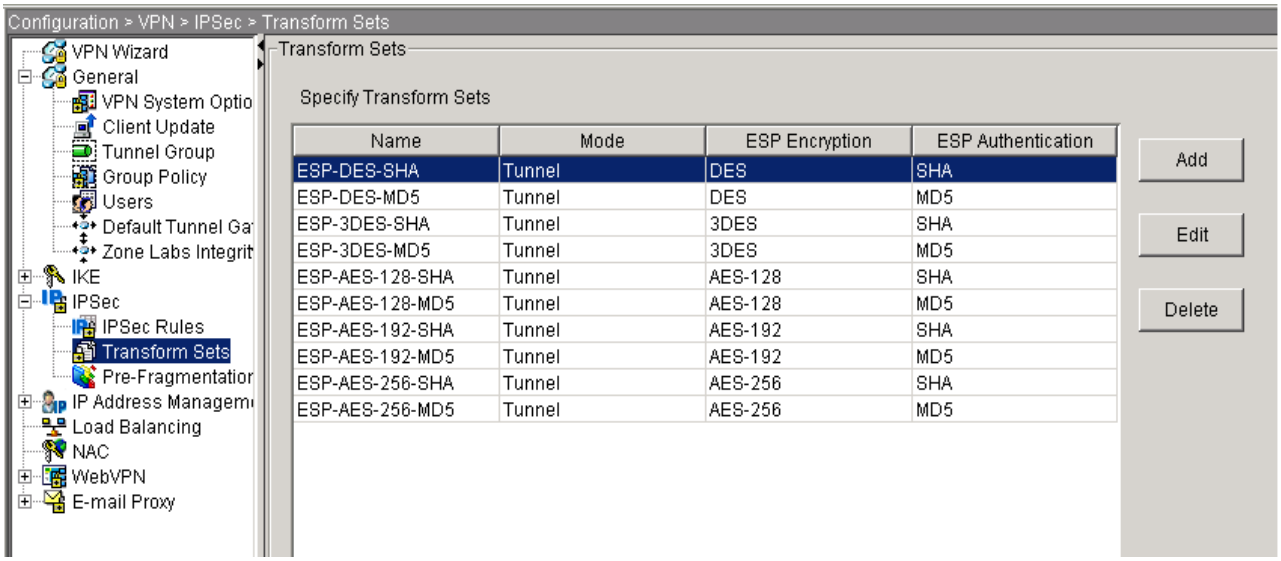
セキュリティ アプライアンスで L2TP over IPSec 接続を設定する手順は、次のとおりです。

（注）　セキュリティ アプライアンスに Cisco VPN Client バージョン 3.x または Cisco VPN 3000 Client バージョン 2.5 がインストールされていると、Windows 2000 で L2TP/IPSec トンネルを確立できません。Windows 2000 の Services パネルで、Cisco VPN Client バージョン 3.x の *Cisco VPN Service* または Cisco VPN Client バージョン 2.5 の *ANetIKE Service* を無効にします（**Start > Programs > Administrative Tools > Services** を選択）。次に、**Services** パネルから IPSec Policy Agent Service を再起動し、マシンをリブートします。

ステップ 1　IPSec トランスフォーム セットを追加し、IPSec がトンネル モードではなく、トランスポート モードを使用するように指定します。

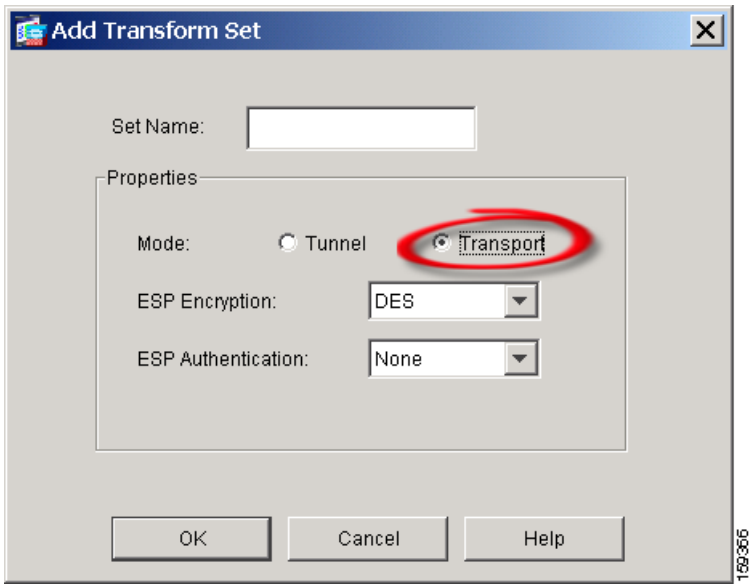
これには、**Configuration > VPN > IPSec** > **Transform Sets** を選択します。**Add** をクリックします。Transform Sets ペインが表示されます（図 10-2）。

図 10-2　Transform Sets ペイン



Add をクリックします。Add Transform Set ダイアログが表示されます（図 10-3）。

図 10-3　Add Transform Set ダイアログ

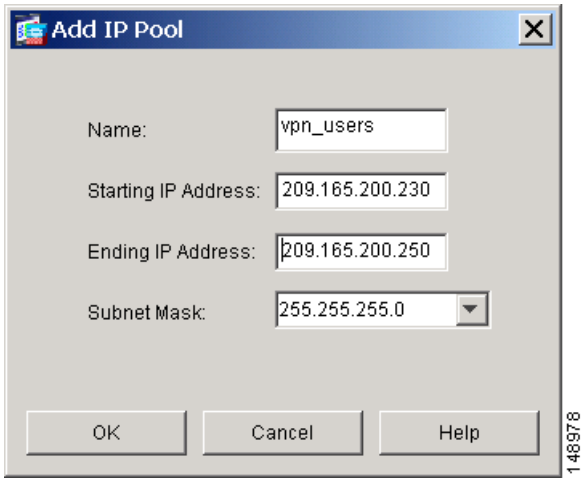


トランスフォーム セットの名前を入力します。ESP Encryption 方式と ESP Authentication 方式を選択します。**OK** をクリックします。

ステップ 2　アドレス割り当ての方式を設定します。この例では、IP アドレス プールを使用します。

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 10-4）。

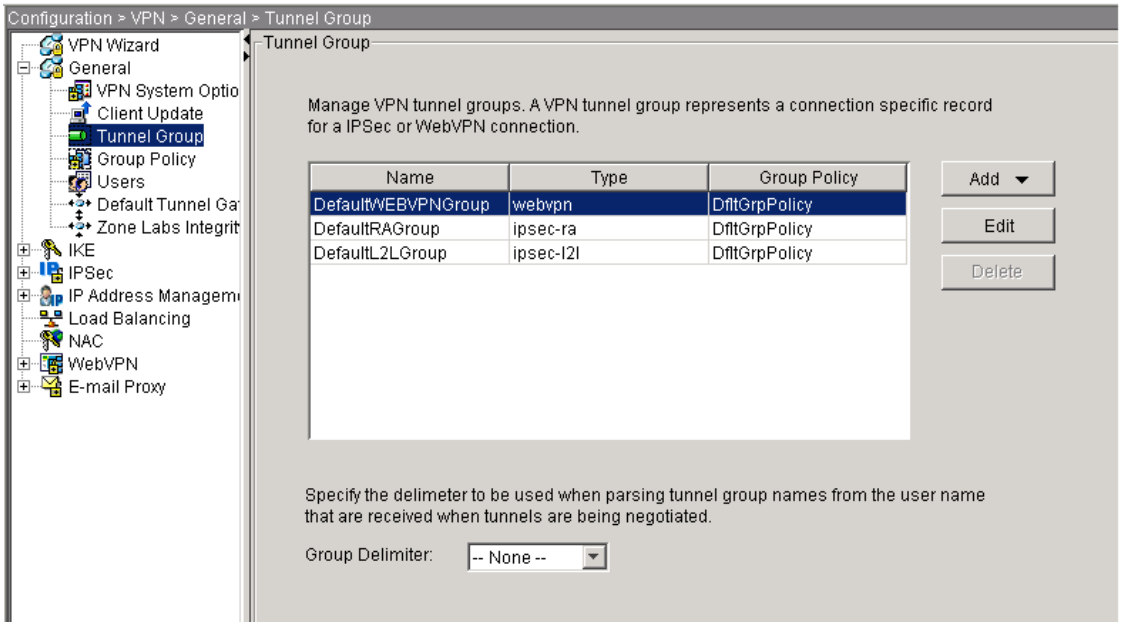
図 10-4　Add IP Pool ダイアログ



新しいアドレス 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、サブネット マスクを入力して **OK** をクリックします。

ステップ 3　IP アドレス プールをトンネル グループに割り当てます。これには、**Configuration >VPN > General > Tunnel Group** を選択します。Tunnel Group ペインが表示されます（図 10-5）。

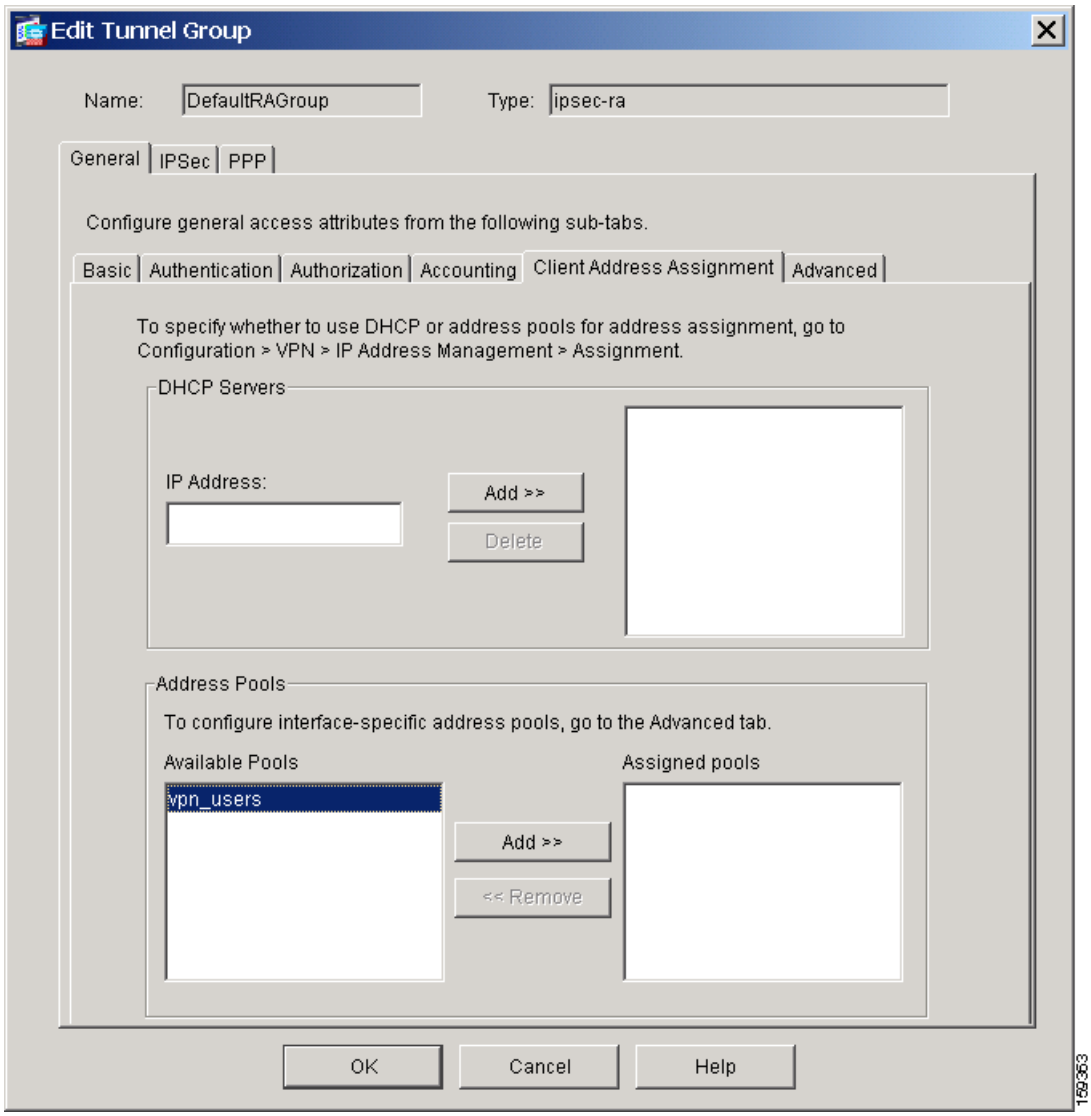
図 10-5　Tunnel Group ペイン



テーブルでトンネル グループ選択して **Edit** をクリックします。Edit Tunnel Group ダイアログが表示されます。

Client Address Assignment タブをクリックします。Client Address Assignment タブ（図 10-6）に、Address Pools グループ ボックスが表示されます。

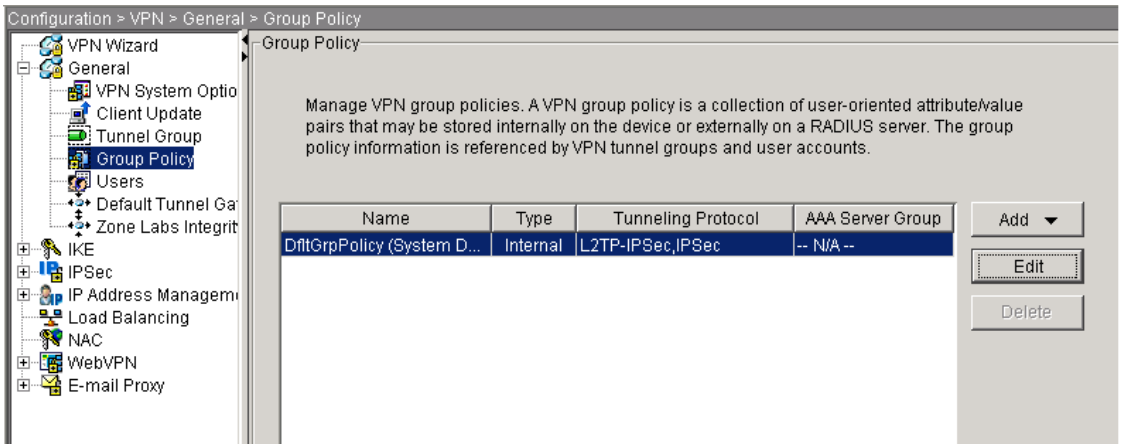
図 10-6　Edit Tunnel Group、General タブ、Client Address Assignment タブ



Address Pools 領域で、トンネル グループに割り当てるアドレス グループを選択し、**Add** をクリックします。Assigned pools ボックスに、アドレス プールが表示されます。

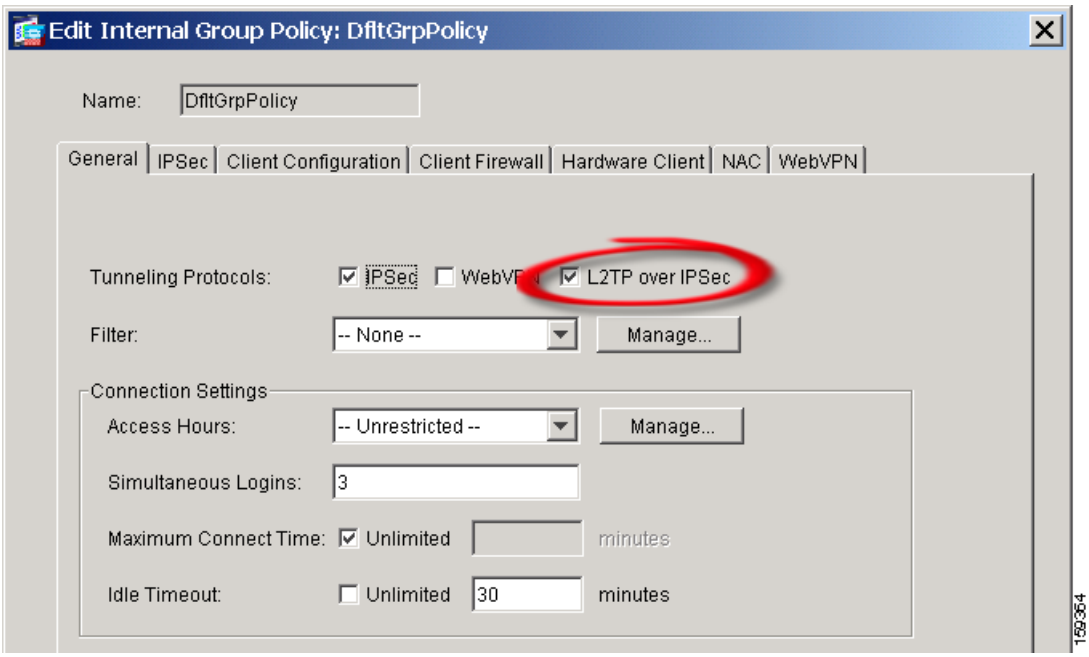
ステップ 4　L2TP over IPSec をこのグループ ポリシーの有効な VPN トンネリング プロトコルとして設定します。**Configuration > VPN > General > Group Policy** を選択します。Group Policy ペインが表示されます（図 10-7）。

図 10-7　Edit Internal Group Policy



グループ ポリシーを選択して Edit をクリックします。Edit Group Policy ダイアログが表示されます（図 10-8）。

図 10-8　Edit Group Policy ダイアログ、General タブ



L2TP over IPSec をクリックして、グループ ポリシーのプロトコルを有効にします。**OK** をクリックします。

ステップ 5　グループ ポリシーをトンネル グループにリンクし、トンネル グループ スイッチングを有効にします（オプション）。**Configuration >VPN > General > Tunnel Group** を選択して、トンネル グループの設定に戻ります。Tunnel Group ペインが表示されますトンネル グループを選択して **Edit** をクリックします。Edit Tunnel Group、General タブ、Basic タブが表示されます（図 10-9）。グループ ポリ

シーを選択します。

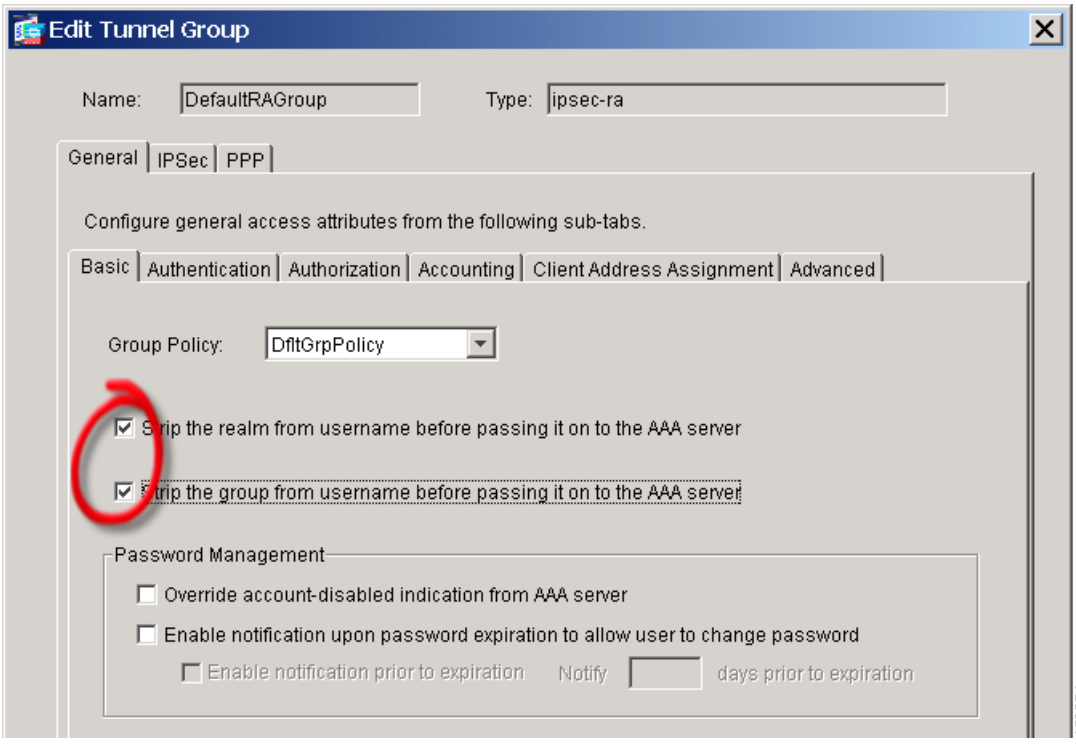
トンネル グループ スイッチングを使用すると、セキュリティ アプライアンスを、他のトンネル グループとの L2TP over IPSec 接続を確立する複数のユーザに関連付けられます。各トンネル グループには、それぞれの AAA サーバ グループと IP アドレス プールがあるため、ユーザは、各自のトンネル グループに固有の方式で認証を行えます。

この機能では、ユーザがユーザ名だけを送信するのではなく、ユーザ名とグループ名を *username@group_name* という形式で送信します。ここで、「@」は設定可能なデリミタであり、グループ名はセキュリティ アプライアンスで設定したトンネル グループ名です。

トンネル グループ スイッチングはストリップ グループ処理によって有効になります。これによりセキュリティ アプライアンスは、VPN クライアントが提供するユーザ名からグループ名を取得して、ユーザ接続のためのトンネルグループを選択できます。このようにして、セキュリティ アプライアンスは、ユーザ名のユーザの部分だけを送信して許可と認証ができます。そうでない場合（無効な場合）、セキュリティ アプライアンスはレルムも含めたユーザ名全体を送信します。

トンネル グループ スイッチを有効にするには、**Strip the realm from username before passing it on to the AAA server** をオンにし、**Strip the group from username before passing it on to the AAA server** をオンにします。**OK** をクリックします。

図 10-9　Edit Tunnel Group ダイアログ、General タブ、Basic タブ



ステップ 6　L2TP over IPSec は、PPP 認証プロトコルを使用します。トンネル グループの PPP タブで、PPP 接続に許可されるプロトコルを指定します（図 10-10）。表 10-1 は、PPP 認証のタイプとその特徴を示します。

図 10-10　Edit Tunnel Group、PPP タブ

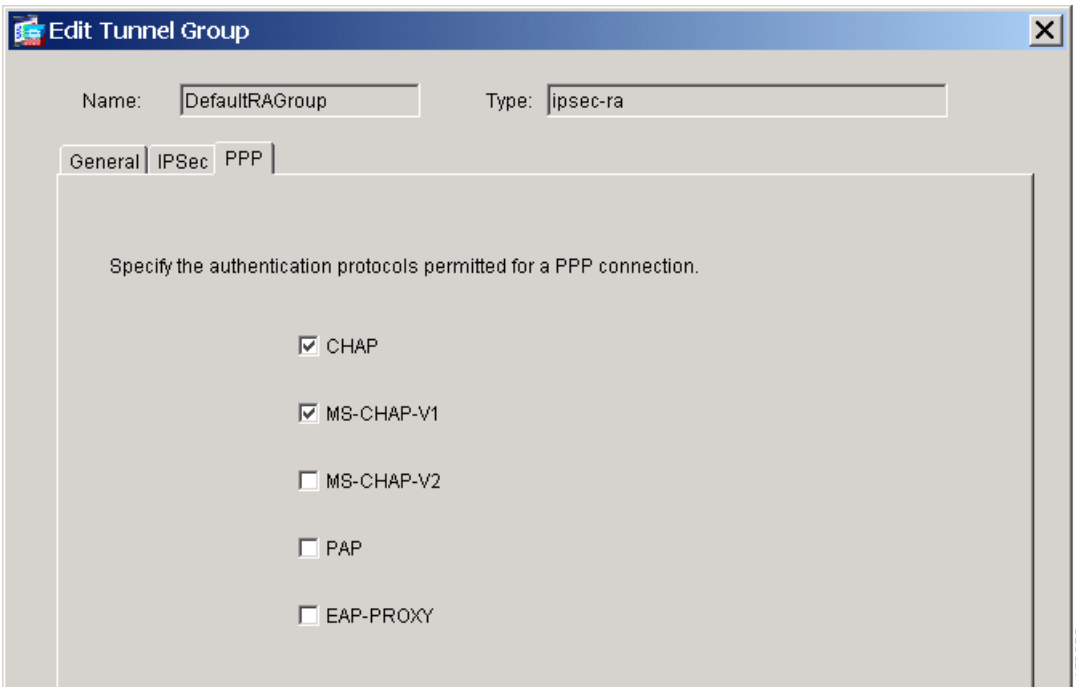


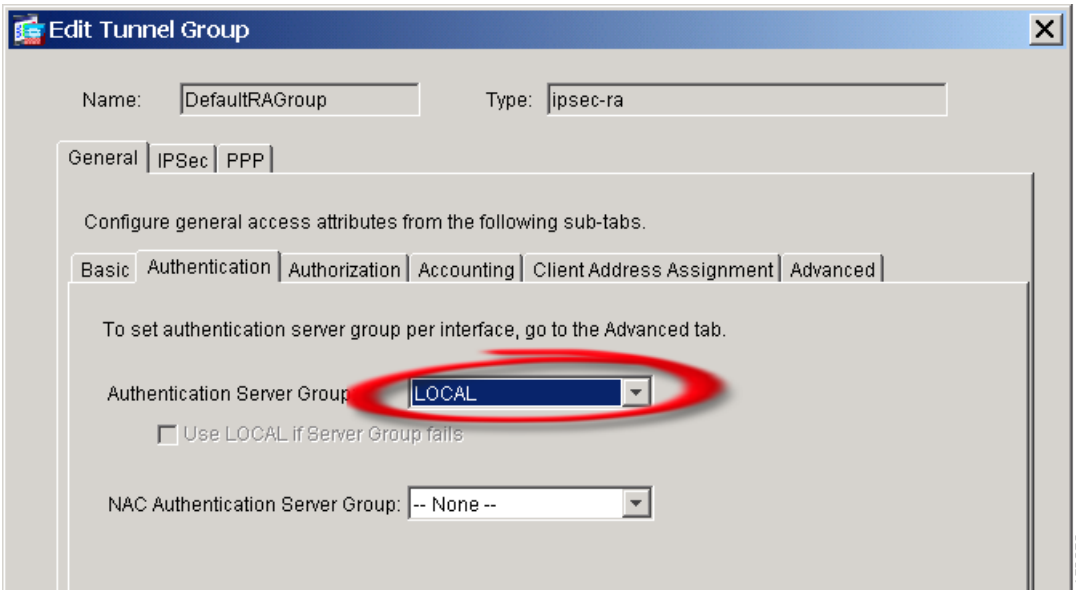
表 10-1　認証タイプの特徴

キーワード	認証タイプ	特徴
`chap`	CHAP	サーバのチャレンジに対して、クライアントは暗号化されたチャレンジとパスワードおよびクリア テキストのユーザ名を返します。このプロトコルは、PAP よりセキュアですが、データを暗号化しません。
`eap-proxy`	EAP	EAP を有効にすると、セキュリティ アプライアンスが、外部の RADIUS サーバに対して PPP 認証プロセスを代行できます。
`ms-chap-v1` `ms-chap-v2`	Microsoft CHAP バージョン 1 Microsoft CHAP バージョン 2	CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。このプロトコルは、MPPE によってデータの暗号化のための鍵を生成します。
`pap`	PAP	認証時にクリア テキストのユーザ名とパスワードを渡すため、セキュアではありません。

ステップ 7　L2TP over IPSec 接続を試みるユーザの認証方式を指定します。セキュリティ アプライアンスが認証サーバか、独自のローカル データベースかのいずれを使用するかを設定します。これには、トンネル グループの **Authentication** タブをクリックします。Authentication タブが表示されます（図 10-11）。

デフォルトで、セキュリティ アプライアンス は、ローカル データベースを使用します。つまり、Authentication Server Group ドロップダウン リストには LOCAL と表示されます。認証サーバを使用するには、リストから認証サーバを選択します。

図 10-11　Edit Tunnel Group、General タブ、Authentication タブ

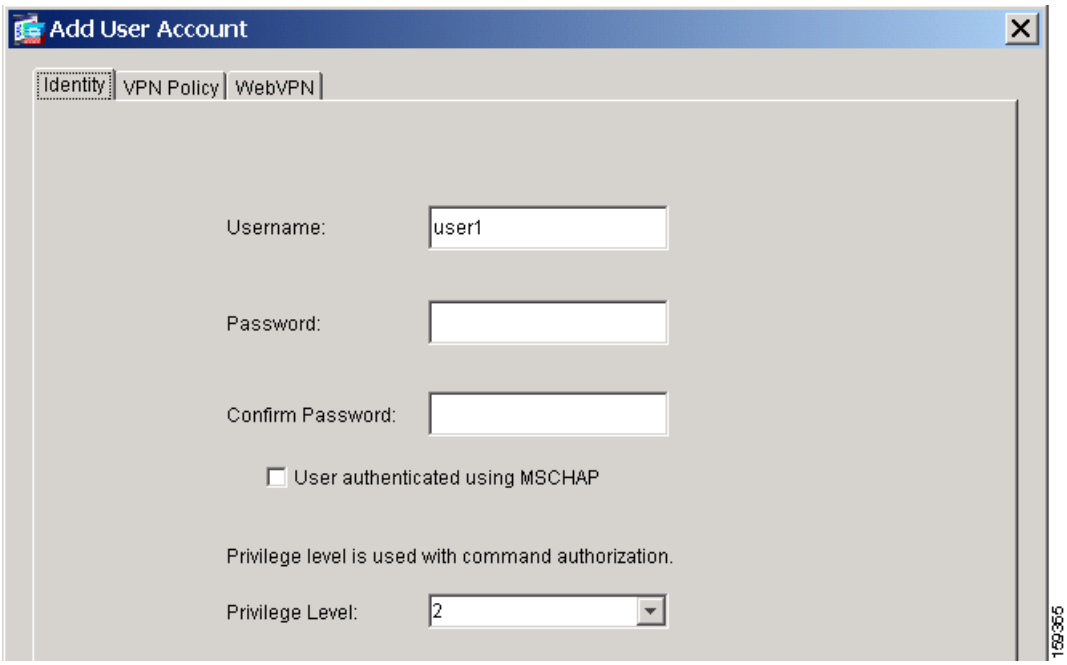


（注）　セキュリティ アプライアンスは、ローカル データベースで、PPP 認証、PAP および Microsoft CHAP バージョン 1 および 2 だけをサポートします。EAP と CHAP は、プロキシ認証サーバによって実行されます。そのため、リモート ユーザが EAP または CHAP を設定したトンネル グループに属していて、セキュリティ アプライアンスがローカル データベースを使用するように設定されている場合、ユーザは接続できません。

ステップ 8　ローカル データベースでユーザを作成します。**Configuration >Properties > Device Administration > User Accounts** を選択します。**Add** をクリックします。Add User Accounts ダイアログが開きます（図 10-12）。

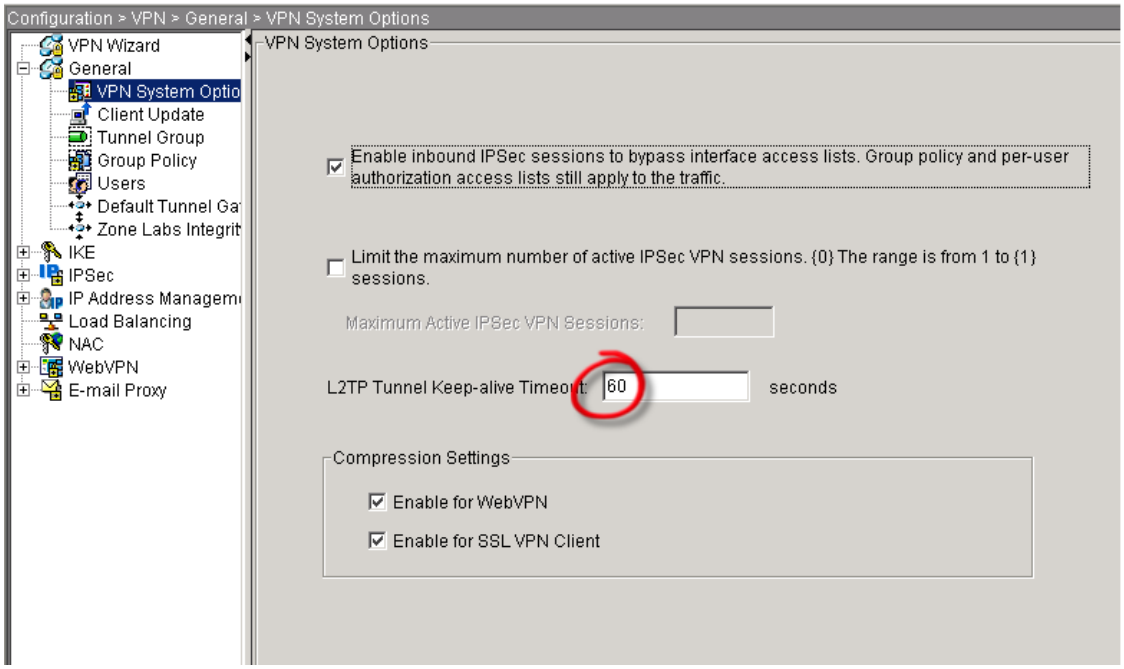
ユーザが Microsoft CHAP、バージョン 1 または 2 を使用する 2L2TP クライアントで、セキュリティ アプライアンスがローカル データベースに対して認証を行うように設定されている場合、**User Authenticated using MSCHAP** をクリックして MSCHAP を有効にする必要があります。

図 10-12　Add User Account ダイアログ



ステップ 9　hello　メッセージの間隔を秒単位で設定します。**VPN > Configuration > General > VPN System Options** を選択します。VPN System Options ペインが表示されます（図 10-13）。**L2TP Tunnel Keep-alive Timeout** フィールドに、値を秒単位で入力します。

図 10-13　VPN System Options



ステップ 10　（オプション）NAT デバイスの背後で、複数の L2TP クライアントが、セキュリティ アプライアンスへの L2TP over IPSec 接続を試みる可能性がある場合、ESP パケットが 1 つ以上の NAT デバイス経由で伝送されるように、NAT トラバーサルを有効にする必要があります。

これには、**Configuration > VPN > IKE > Global Parameters** を選択します。IKE Global Parameters ペインが表示されます（図 10-14）。インターフェイスで、ISAKMP が有効であることを確認します。**Enable IPSec over NAT-T** をオンにし、**OK** をクリックします。

図 10-14　IKE Global Parameters ペイン