RV016、RV042、RV042G および RV082 VPN ルータの Mac OS のための速い VPN 代替を展開して下さい

目標

Mac OS のために適した速い VPN バージョンがありません。 ただし、Mac OS のために代替速い VPN を展開することを望むどんどん増える な ユーザがあります。 この技術情報では、IP Securitas は速い VPN のために代替として使用されます。

注: 設定を開始する前に MAC OS で IP Securitas をダウンロードし、インストールする必要があります。 次のリンクからそれをダウンロードできます:

http://www.lobotomo.com/products/IPSecuritas/

この技術情報は Rv016、RV042、RV042G および RV082 VPN ルータの Mac OS のための速い VPN 代替を展開する方法を説明します。

適当なデバイス

- RV016
- RV042
- RV042G
- RV082

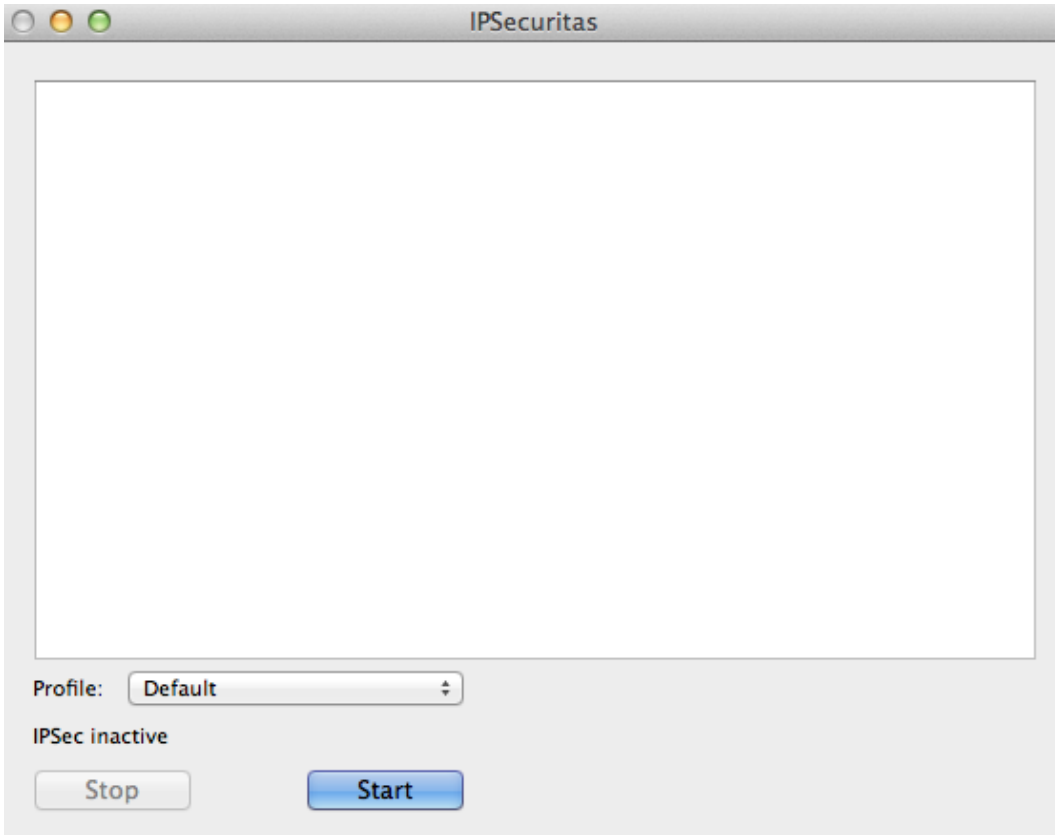
[Software Version]

- v4.2.2.08

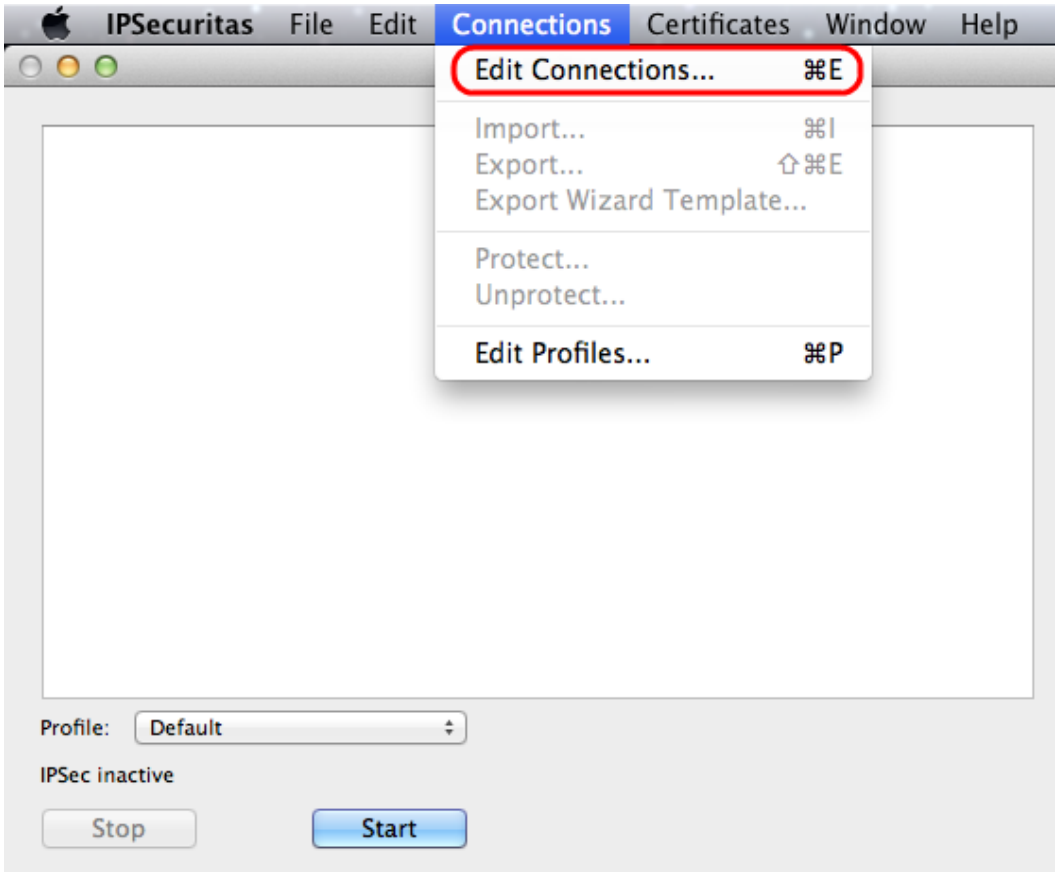
Mac OS のための速い VPN 代替を展開して下さい

注: デバイスのゲートウェイコンフィギュレーションへの VPN Client は最初にされる必要があります。 多くを知るためにゲートウェイに VPN Client を設定する方法を*設定します RV016、RV042、RV042G および RV082 VPN ルータの VPN Client のためのリモートアクセストンネル（ゲートウェイへのクライアント）を*参照して下さい。

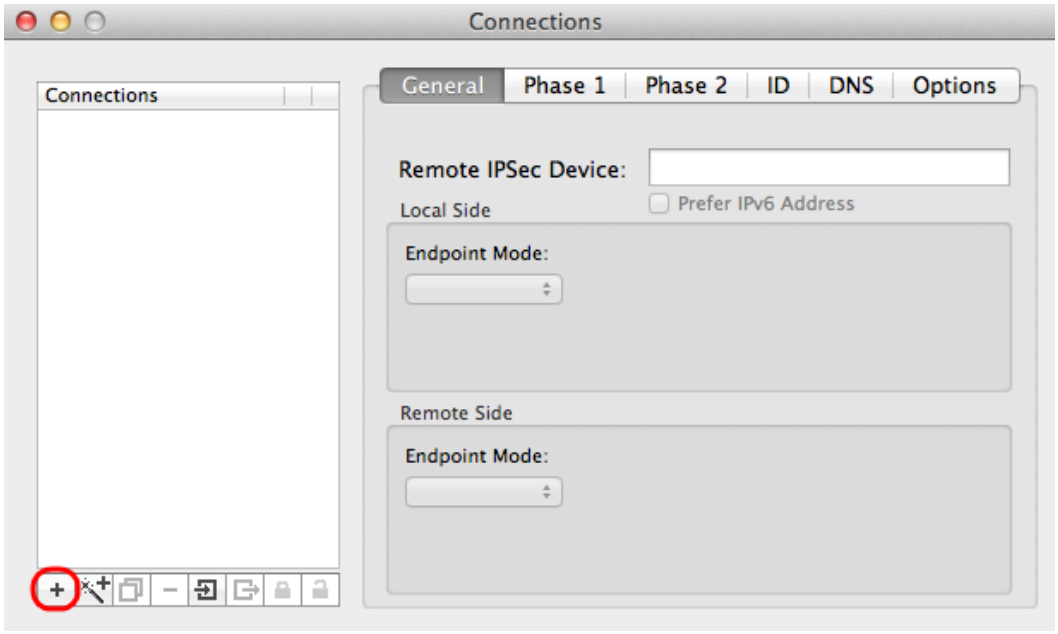
ステップ 1. Mac OS の IP Securitas を実行して下さい。 *IPSecuritas* ウィンドウは現われます:



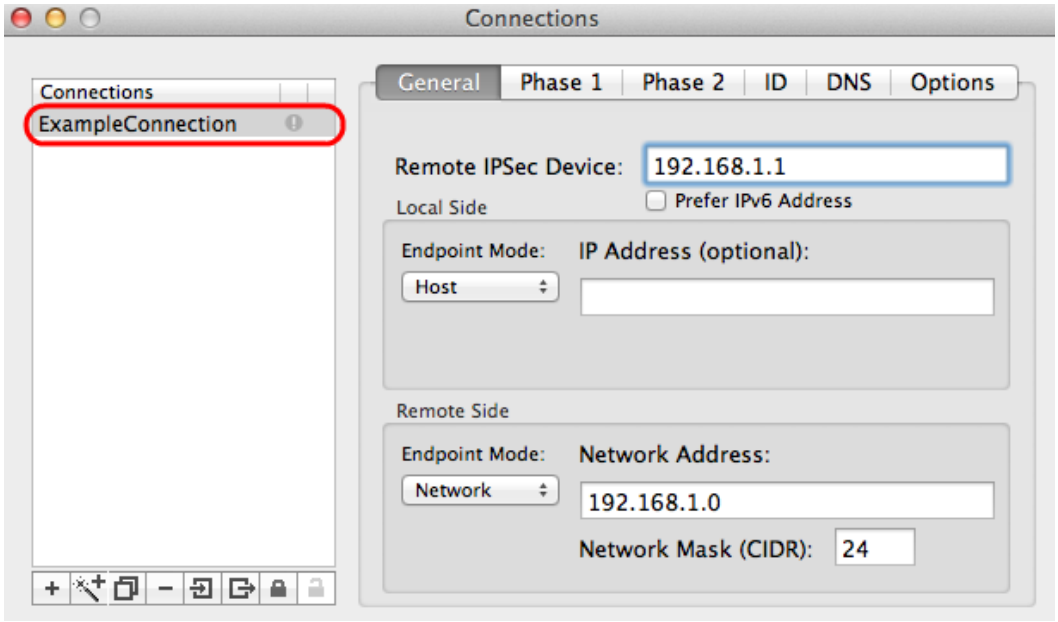
ステップ 2. 『Start』 をクリック して下さい。



ステップ 3 メニューバーから、**> Edit 接続を**『Connections』 を選択 して下さい。
*Connections ウィンドウは*現われます。

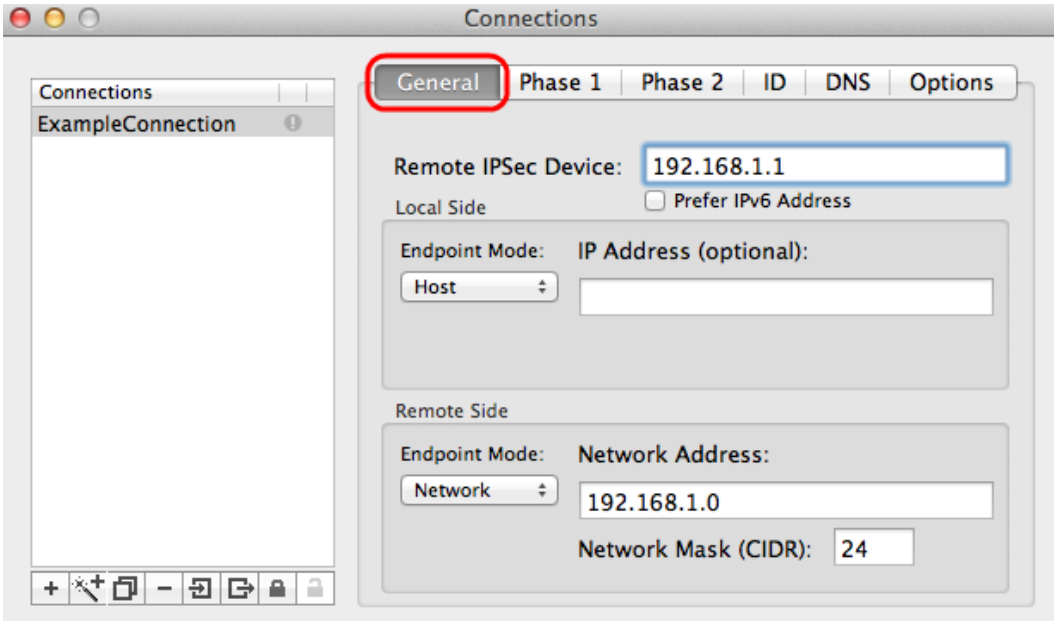


ステップ 4.新しい接続を追加するために **+ アイコンを**クリックして下さい。



ステップ 5.接続の下で新しい接続の名前を入力して下さい。

一般



ステップ 1. **General タブを**クリックして下さい。

ステップ 2.リモート IPSecデバイス フィールドでリモートルータの IP アドレスを入力して下さい。

注: この設定がリモートクライアントのためであると同時にローカル側を設定する必要はありません。 ちょうどリモートモードを設定する必要があります。

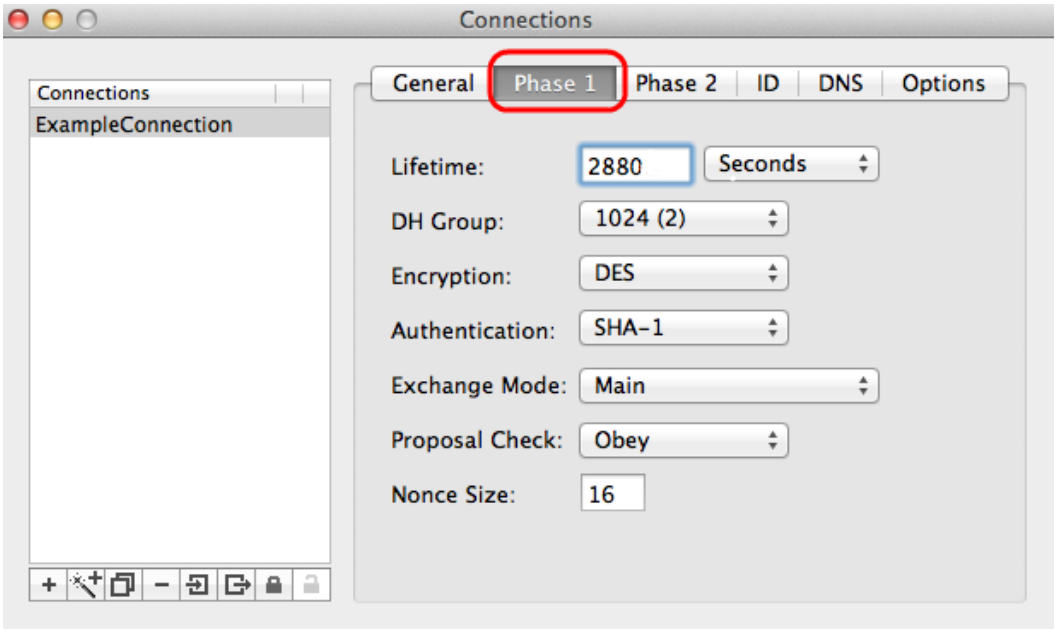
ステップ 3 リモート側 エリアで、エンドポイント モード ドロップダウン リストから**ネットワークを**選択して下さい。

ステップ 4.ネットワークマスク（CIDR）フィールドでサブネット マスクを入力して下さい。

ステップ 5.ネットワーク アドレス フィールドでリモートネットワーク アドレスを入力して下さい。

フェーズ 1

フェーズ 1 はセキュア認証された通信をサポートするトンネルの 2 つの終わり間のシンプレックス、論理的な Security Association （ SA ）です。



ステップ 1.**フェーズ 1 タブを**クリックして下さい。

ステップ 2.ライフタイム フィールドでトンネルの設定の間に入力したライフタイムを入力して下さい。 時間が切れる場合、New 鍵は自動的に再取り決めされます。 鍵ライフタイムは 1081 から 86400 秒まで及ぶことができます。 フェーズ 1 のデフォルト値は 28800 秒です。

ステップ 3.ライフタイム ドロップダウン リストからライフタイムのための適切な時間 ユニットを選択して下さい。 デフォルトは秒です。

ステップ 4.同じをグループ ドロップダウン リストからトンネルの設定のために DH (Diffie-Hellman) 入力したグループ DH (Diffie-Hellman) 選択して下さい。 Diffie-Hellman (DH) グループは鍵交換のために使用されます。

ステップ 5.トンネルの設定のために入力した暗号化 ドロップダウン リストから暗号化タイプを選択して下さい。 暗号化の方法は暗号化するのに使用されるキー/復号化 Encapsulating Security Payload (ESP) パケットの長さを判別します。

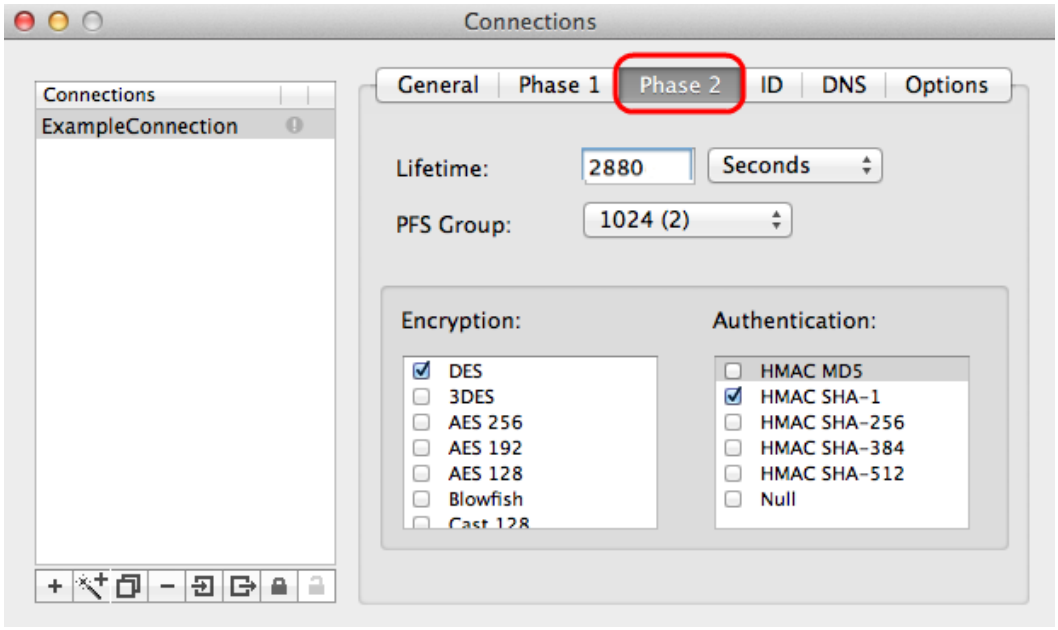
ステップ 6.認証 ドロップダウン リストからトンネルの設定のために入力した認証方式を選択して下さい。 認証の種類は ESP パケットを認証するために方式を判別します。

ステップ 7. Exchange モード ドロップダウン リストから適切な交換モードを選択して下さい。

- main —すべてのタイプの完全な修飾ドメイン名 (FQDN) を除くゲートウェイにおける交換モードを表します。
- 積極的—完全な修飾ドメイン名 (FQDN) ゲートウェイにおける交換モードを表します。

フェーズ 2

フェーズ 2 は両端が指すデータパケット パススルーの間にデータパケットのセキュリティを判別するセキュリティ結合です。



ステップ 1.**フェーズ 2 タブを**クリックして下さい。

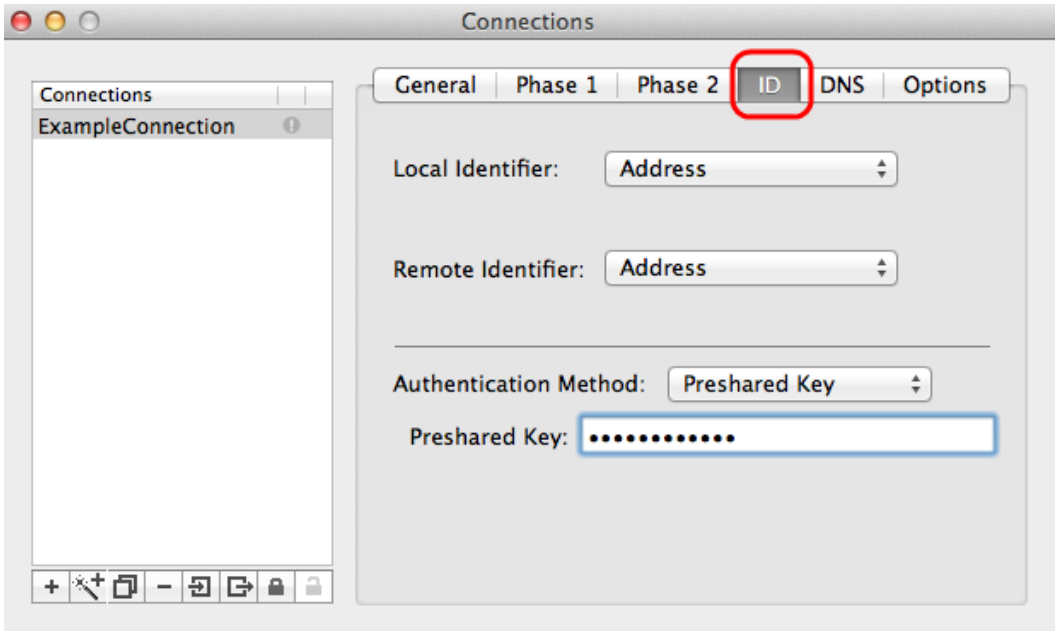
ステップ 2.トンネルおよびまたフェーズ 1.の設定のために入力したライフタイム フィールドで同じライフタイムを入力して下さい。

ステップ 3.トンネルおよびフェーズ 1.の設定のために入力したライフタイム ドロップダウン リストからライフタイムの同じ時間 ユニットを選択して下さい。

ステップ 4.トンネルの設定のために入力した完全なフォワーディング 機密性（PFS）グループ ドロップダウン リストから同じをグループ DH（Diffie-Hellman）選択して下さい。

ステップ 5.すべての未使用暗号化および認証方式のチェックを外して下さい。 フェーズ 1 タブの下で定義される物だけをチェックして下さい。

ID



ステップ 1. **ID** タブをクリックして下さい。

ステップ 2.ローカル識別子ドロップダウン リストからトンネルとローカル識別子の同じ方式を選択して下さい。 ローカル識別子の種類に従って適切な値をもし必要なら入力して下

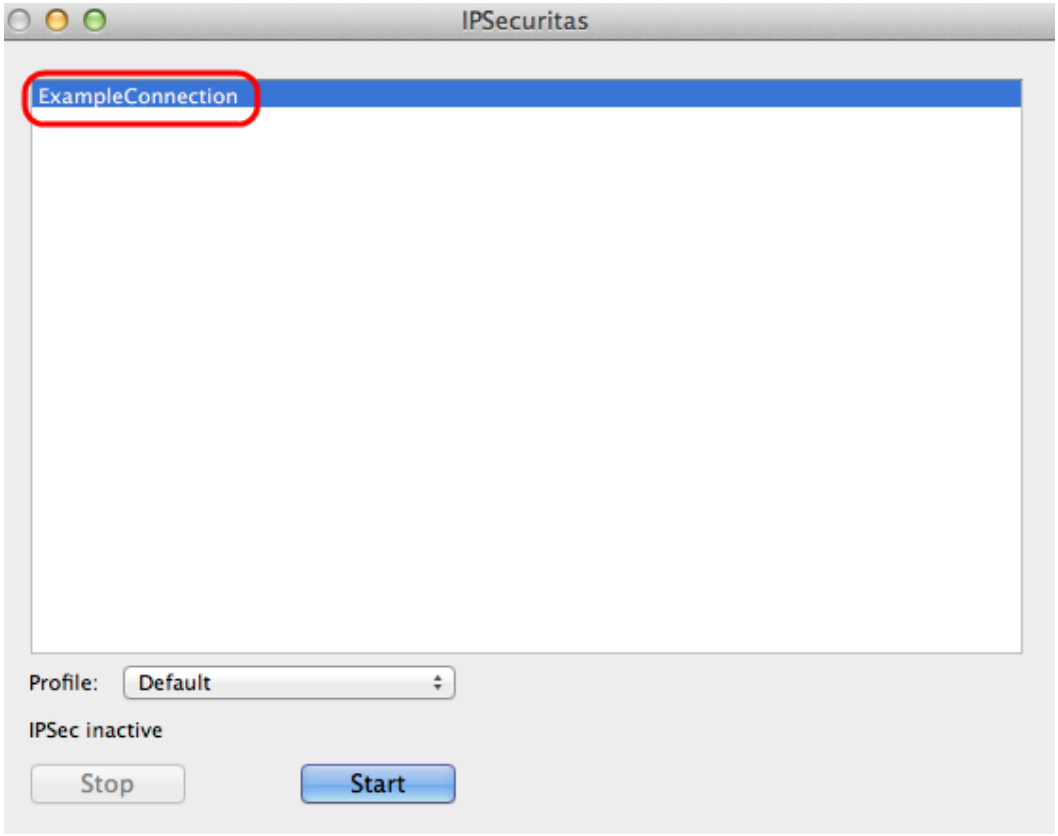
さい。

ステップ 3.リモート識別子 ドロップダウン リストからトンネルとリモート識別子の同じ方式を選択して下さい。 リモート識別子の種類に従って適切な値をもし必要なら入力して下さい。

ステップ 4.認証方式 ドロップダウン リストからトンネルと同じ認証方式を選択して下さい。 認証方式の種類に従って適切な認証値をもし必要なら入力して下さい。

ステップ 5. Connection ウィンドウを閉じるために **x** アイコン (レッド円) をクリックして下さい。 これは自動的に設定を保存します。 *IPSecuritas* ウィンドウは現われます。

接続



ステップ 1： *IPSecuritas* ウィンドウで、『Start』 をクリック して下さい。 ユーザはそれから VPN にアクセスするために接続されます。