RV016、RV042、RV042G、およびRV082 VPNルータでのMac OS向けQuick VPNの代替ソリューションの導入

目的

Mac OSに適したQuick VPNバージョンはありません。ただし、Mac OS用のQuick VPNの代替を導入したいと考えるユーザが増えています。この記事では、Quick VPNの代替としてIPセキュリティを使用します。

注：設定を開始する前に、MAC OSにIPセキュリティをダウンロードしてインストールする必要があります。次のリンクからダウンロードできます。

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

この記事では、Mac OS用のQuick VPNの代替をRv016、RV042、RV042G、およびRV082 VPNルータに導入する方法について説明します。

適用可能なデバイス

- RV016
- RV042
- RV042G
- RV082

[Software Version]

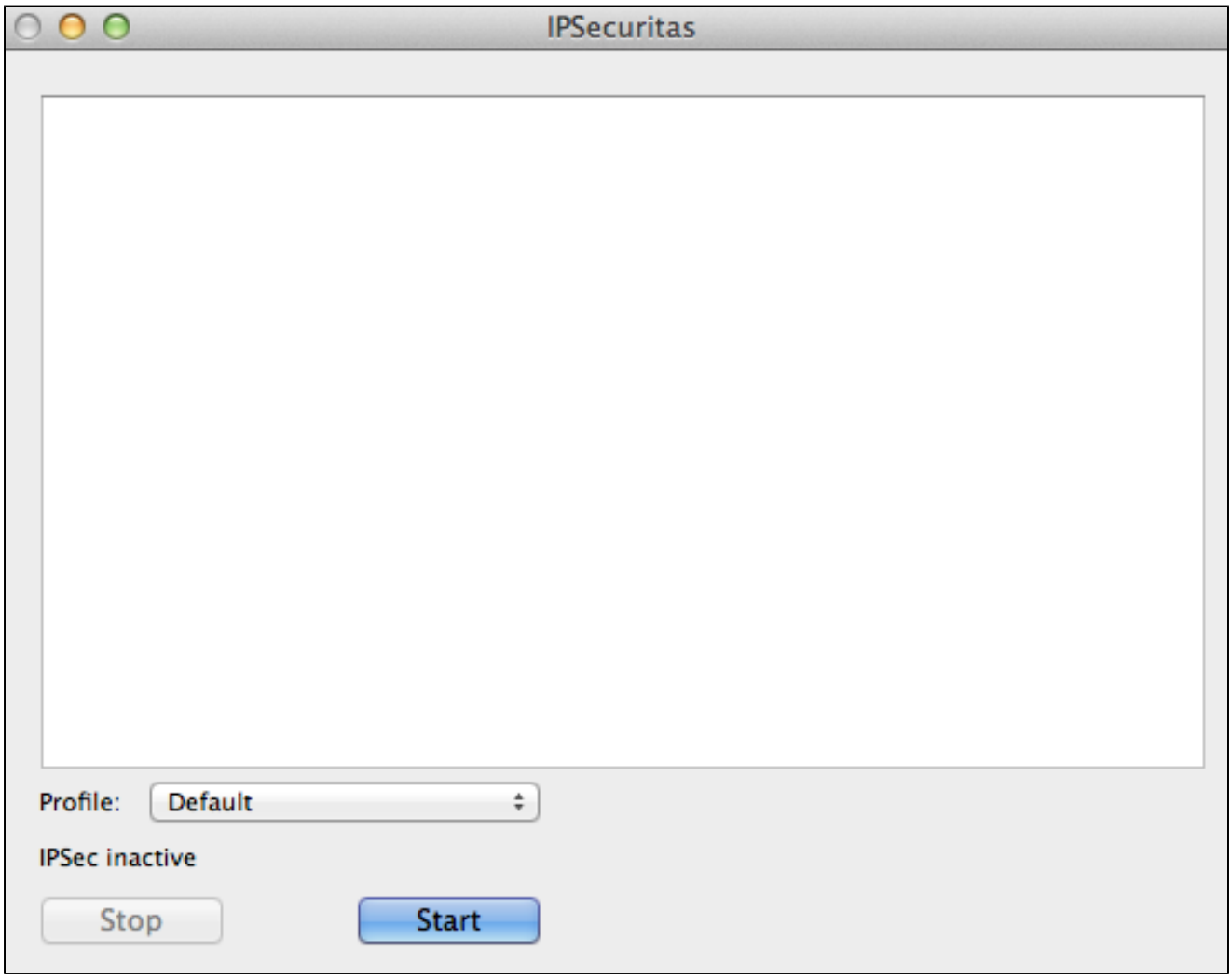
- v4.2.2.08

Mac OS用のQuick VPNの代替を導入する

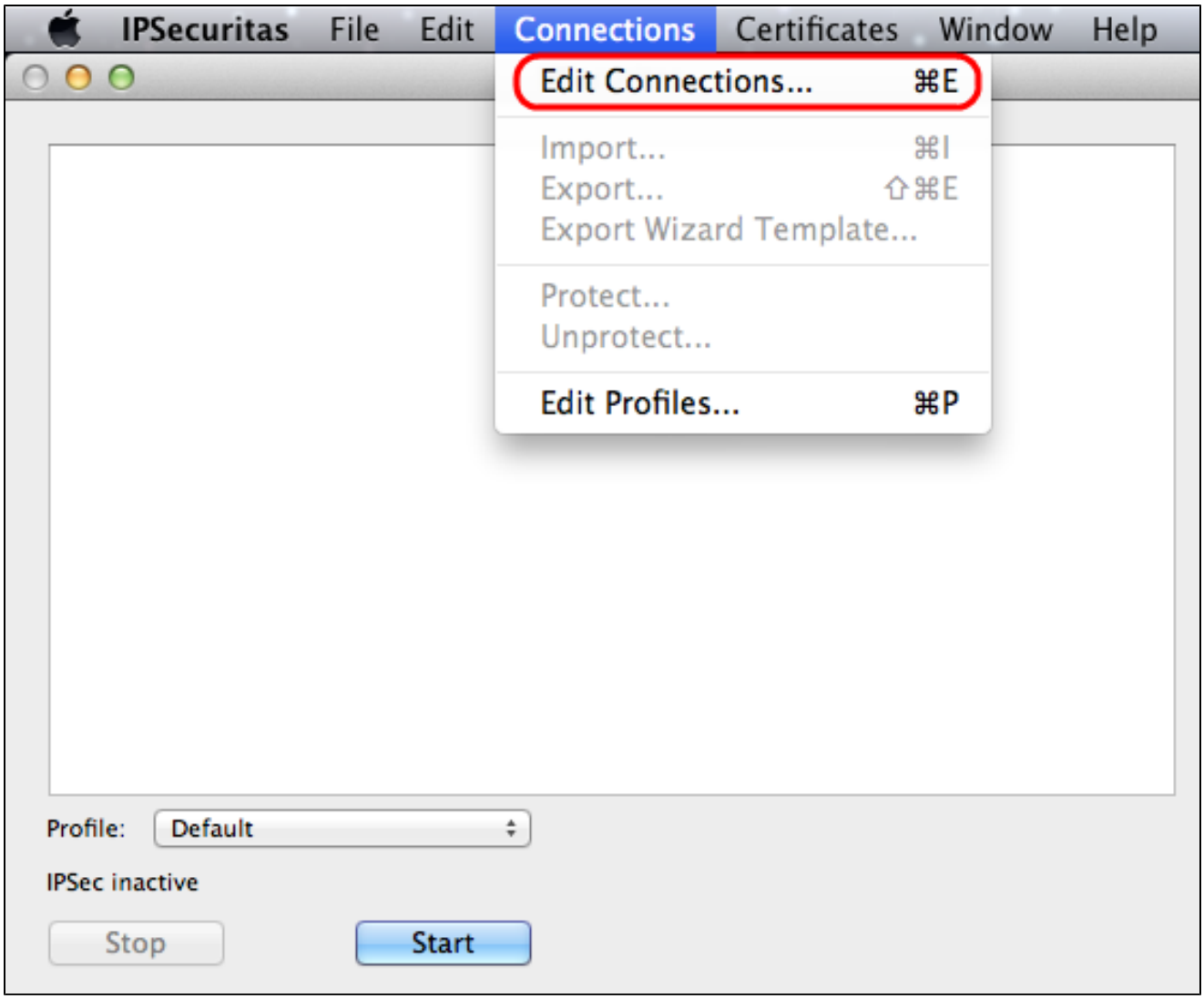
注：デバイスのVPN Clientからゲートウェイへの設定を最初に行う必要があります。VPN Clientをゲートウェイに設定する方法の詳細については、『RV016、RV042、RV042G、およびRV082 VPNルータでのVPN Client用のリモートアクセストンネル（クライアントから

ゲートウェイ）の設定』を参照してください。

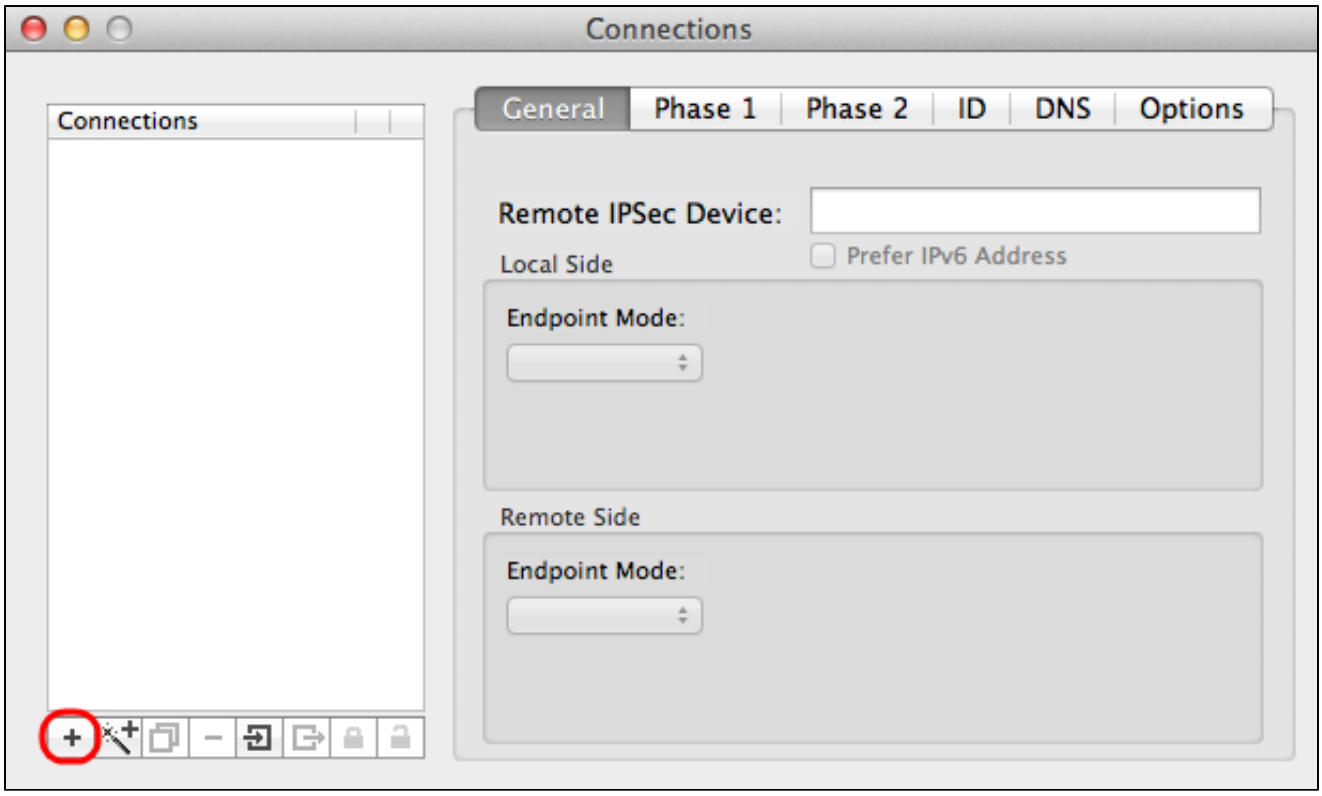
ステップ 1：Mac OSでIPセキュリティを実行します。IPSecuritasウィンドウが表示されます。



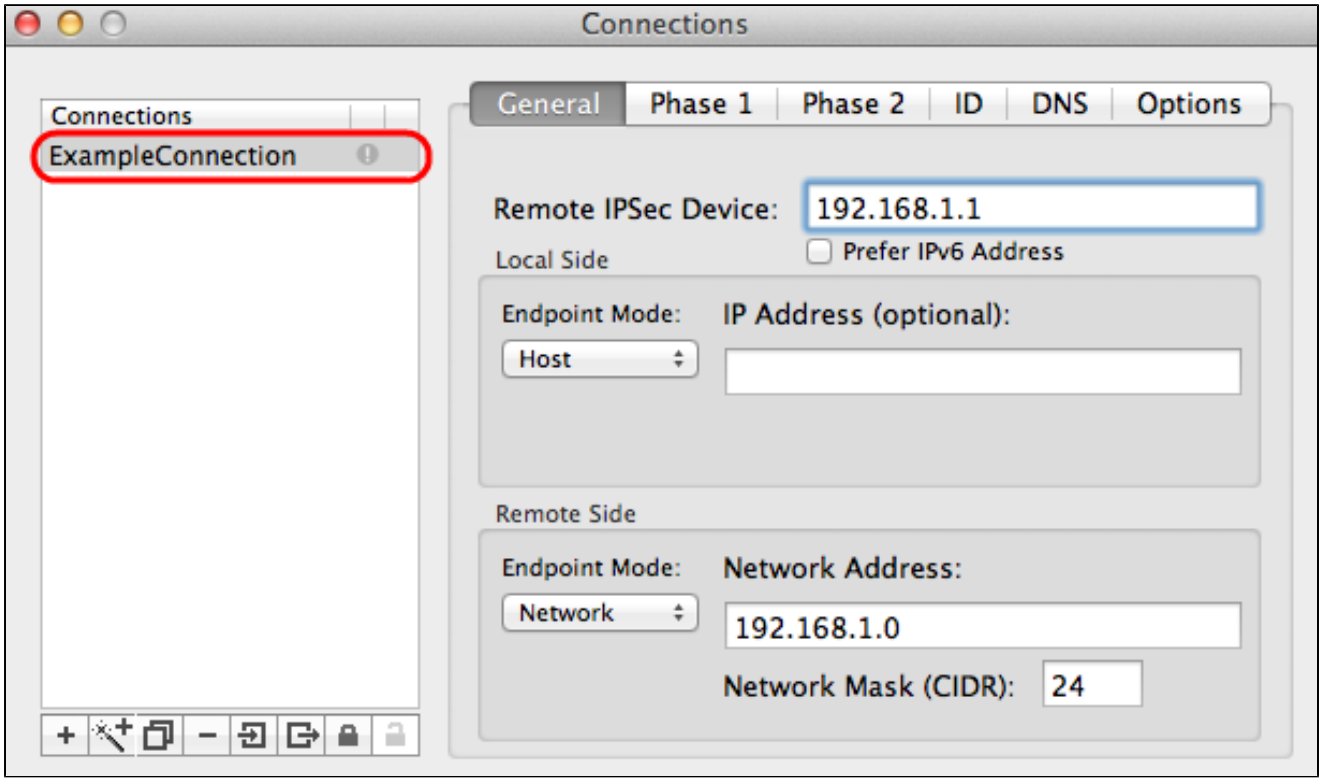
ステップ 2：[Start（スタート）] をクリックします。



ステップ 3：メニューバーから、Connections > Edit Connectionsの順に選択します。Connectionsウィンドウが表示されます。

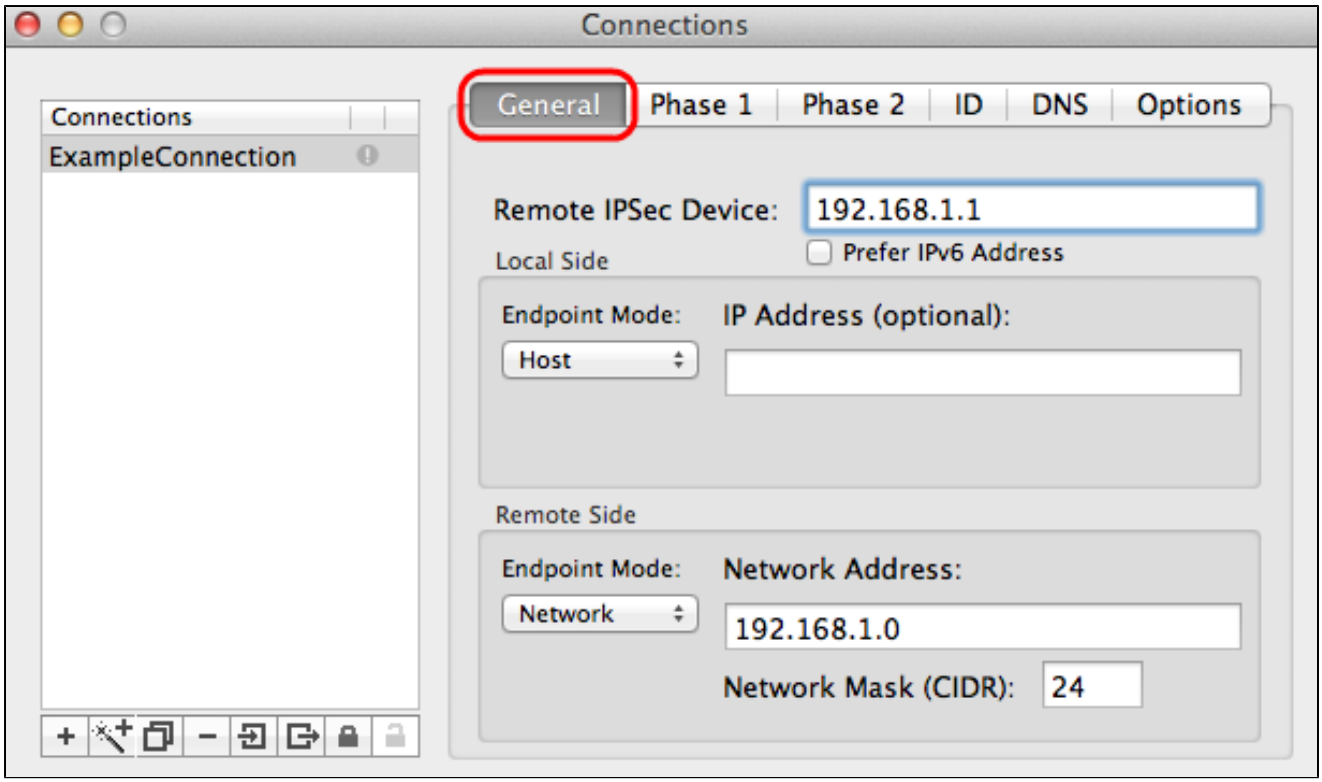


ステップ 4：+アイコンをクリックして、新しい接続を追加します。



ステップ 5：connectionsの下に新しい接続の名前を入力します。

一般



ステップ 1：[General]タブをクリックします

ステップ 2：Remote IPSec Deviceフィールドにリモートルータのアドレスを入力します。

注：この設定はリモートクライアント用であるため、ローカル側を設定する必要はありません。リモートモードを設定するだけです。

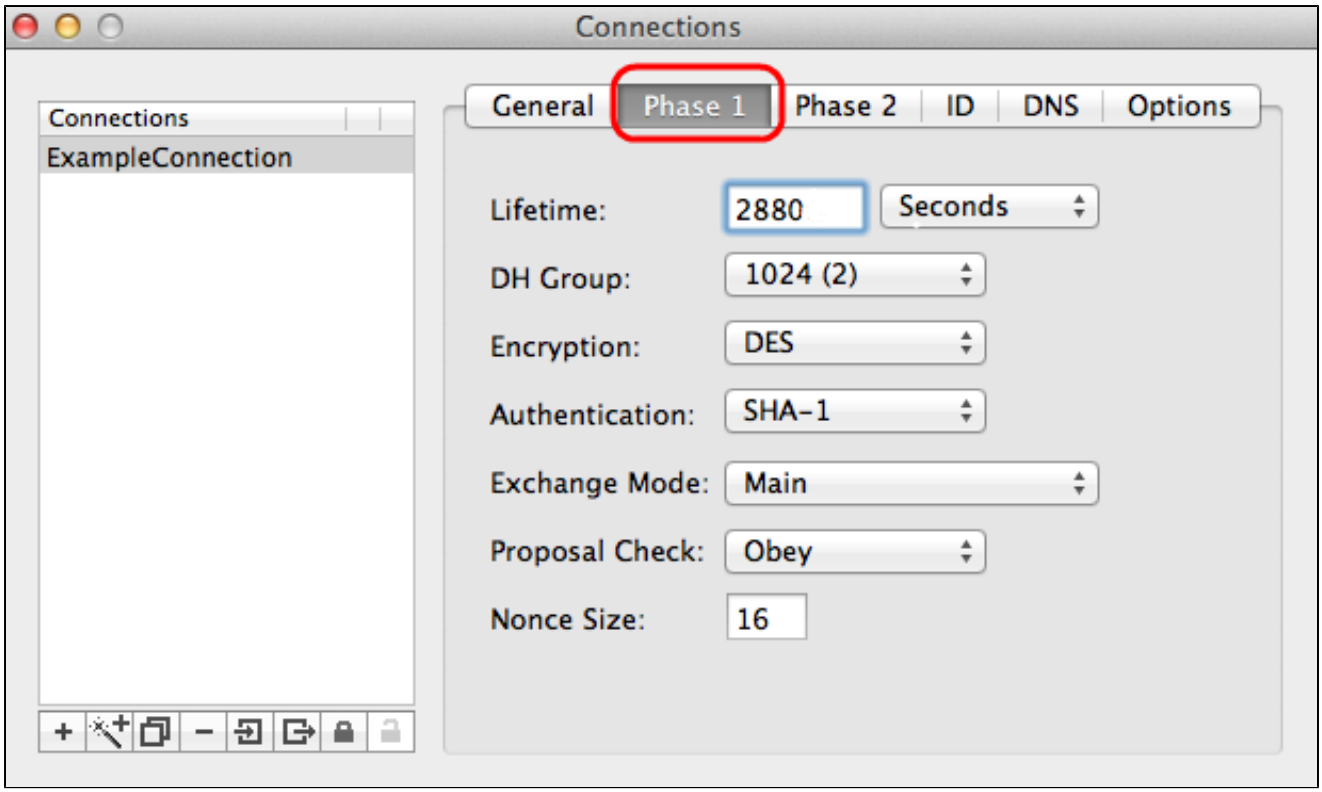
ステップ 3：Remote Side領域で、Endpoint Modeドロップダウンリストから Networkを選択します。

ステップ 4：Network Mask (CIDR)フィールドにサブネットマスクを入力します。

ステップ 5：Network Addressフィールドにリモートネットワークアドレスを入力します。

フェーズ 1

フェーズ1は、トンネルの両端の間のシンプレックスの論理セキュリティアソシエーション(SA)で、セキュアな認証通信をサポートします。



ステップ 1：Phase 1タブをクリックします。

ステップ 2：トンネルの設定時に入力したライフタイムをLifetimeフィールドに入力します。時間が経過すると、新しいキーが自動的に再ネゴシエートされます。キーのライフタイムは1081 ~ 86400秒の範囲です。Phase 1のデフォルト値は28800秒です。

ステップ 3：Lifetimeドロップダウンリストから、Lifetimeに適切な時間単位を選択します。デフォルトは秒です。

ステップ 4：DH Groupドロップダウンリストから、トンネルの設定に入力したものと同じDHグループを選択します。Diffie-Hellman(DH)グループは、キー交換に使用されます。

ステップ 5：トンネルの設定用に入力した暗号化タイプをEncryptionドロップダウンリストから選択します。暗号化方式は、Encapsulating Security Payload(ESP)パケットの暗号化/復号化に使用されるキーの長さを決定します。

手順 6：Authenticationドロップダウンリストから、トンネル設定に入力した認証方式を選択します。認証のタイプによって、ESPパケットを認証する方法が決まります。

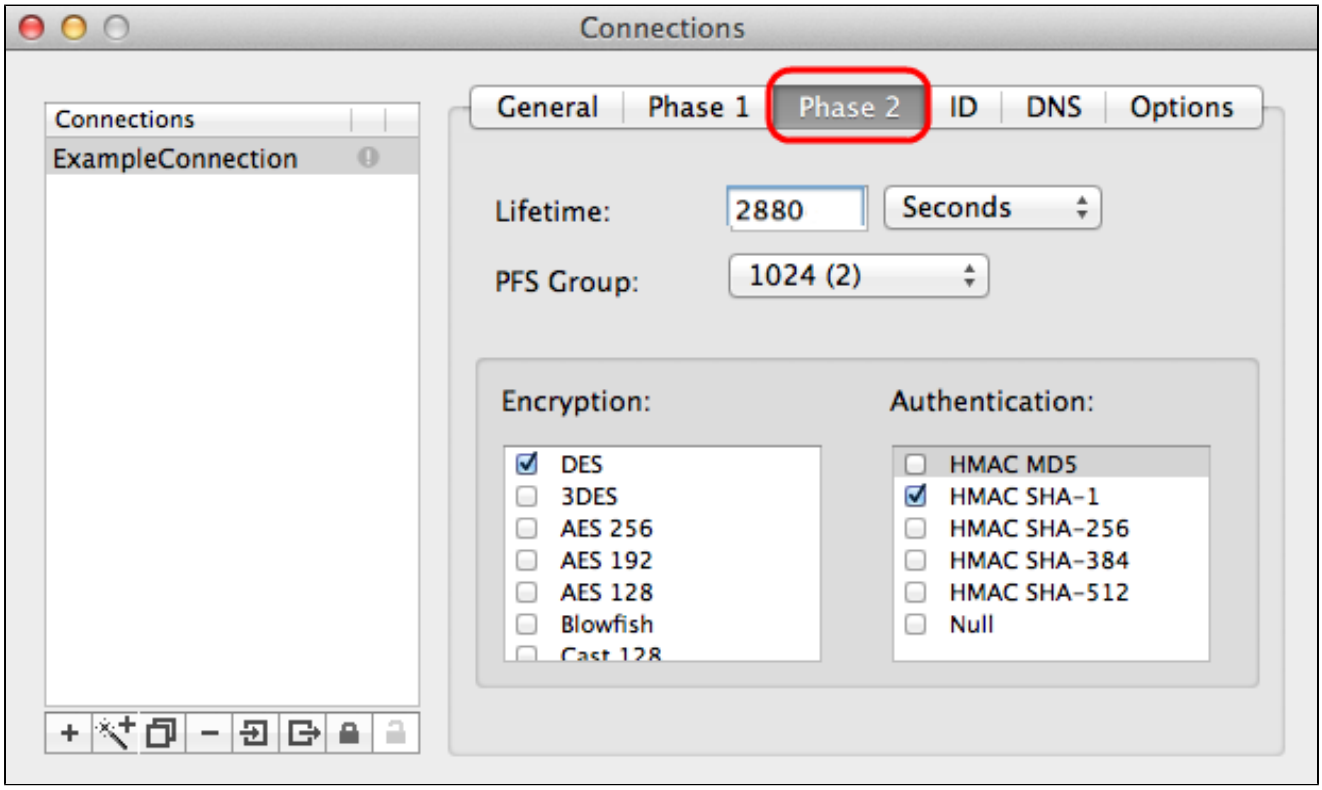
手順 7：Exchange Modeドロップダウンリストから適切なExchangeモードを選択します。

・ Main：完全修飾ドメイン名(FQDN)以外のすべてのタイプのゲートウェイのExchangeモードを表します。

・アグレッシブ：完全修飾ドメイン名(FQDN)ゲートウェイの交換モードを表します。

フェーズ 2

フェーズ2は、データパケットが2つのエンドポイントを通過する間のデータパケットのセキュリティを決定するセキュリティアソシエーションです。



ステップ 1：Phase 2タブをクリックします。

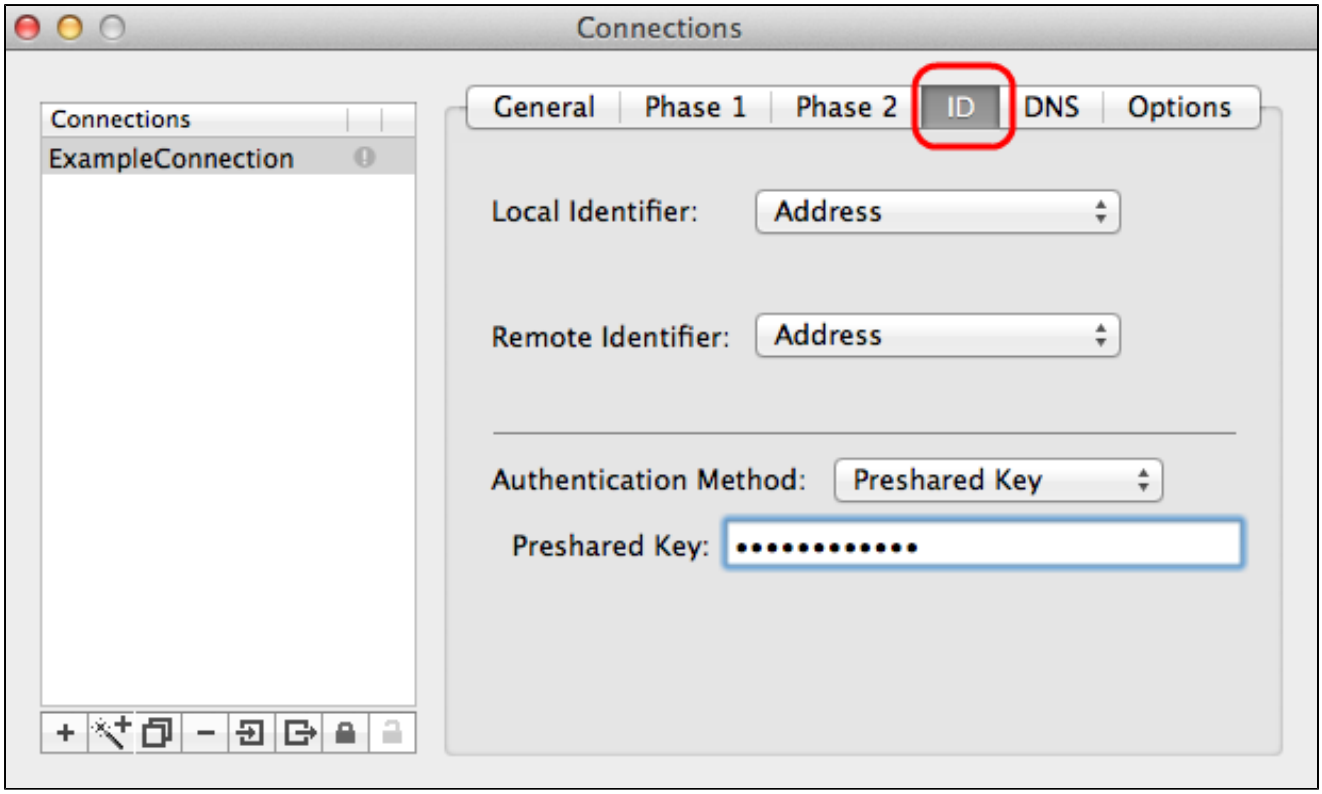
ステップ 2：トンネルの設定とフェーズ1で入力したライフタイムをLifetimeフィールドに入力します。

ステップ 3：トンネルとフェーズ1の設定で入力したライフタイムの同じ時間単位を、Lifetimeドロップダウンリストから選択します。

ステップ 4：トンネルの設定用に入力したPerfect Forwarding Secrecy(PFS)Groupドロップダウンリストから、同じDHグループを選択します。

ステップ 5：使用されていないすべての暗号化方式と認証方式のチェックマークをはずします。Phase 1タブで定義されているものだけにチェックマークを付けます。

ID



ステップ 1： IDタブをクリックします。

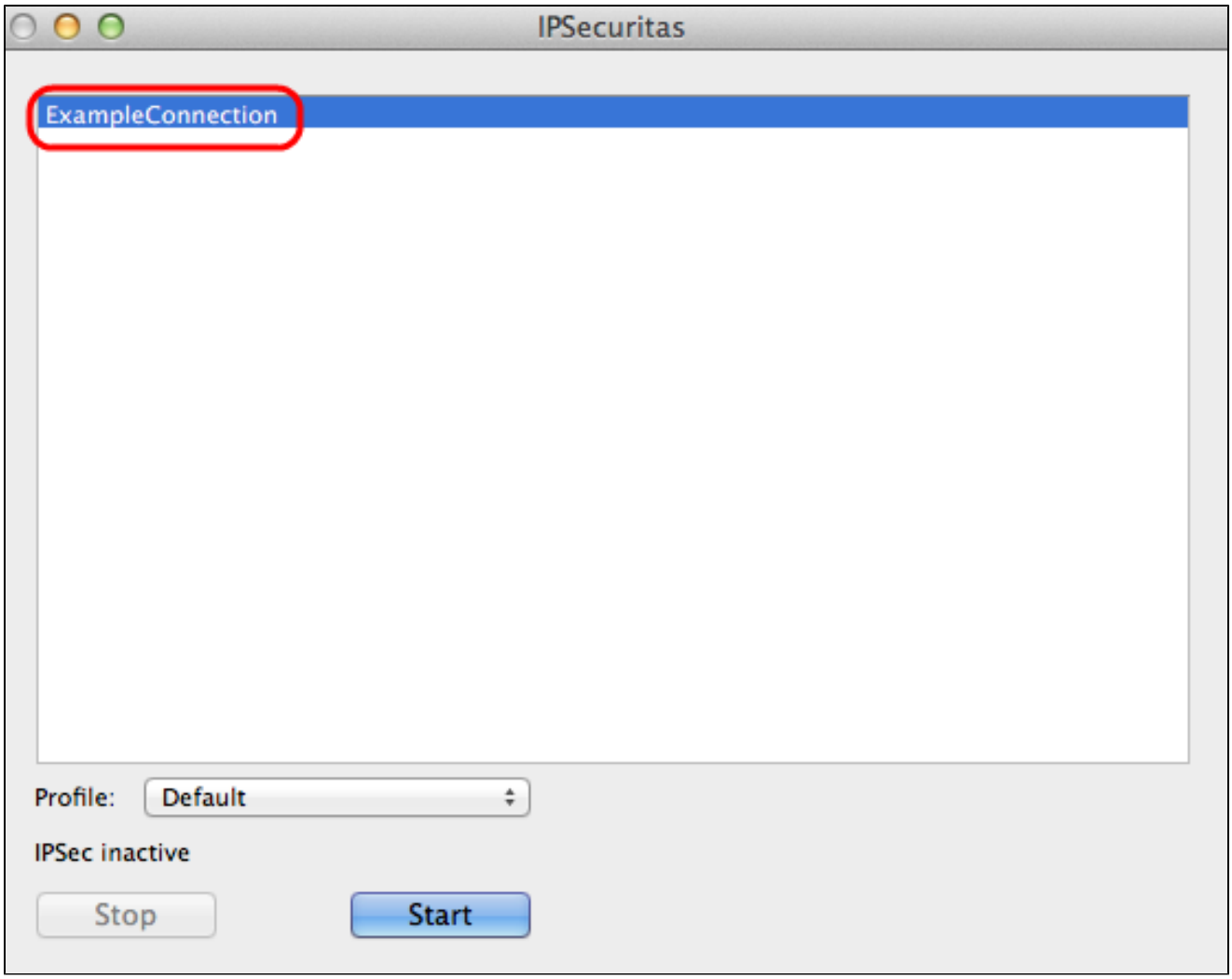
ステップ 2：Local Identifierドロップダウンリストから、トンネルと同じローカルID方式を選択します。必要に応じて、ローカルIDのタイプに応じて適切な値を入力します。

ステップ 3： Remote Identifierドロップダウンリストから、トンネルと同じリモートID方式を選択します。 必要に応じて、リモートIDのタイプに応じて適切な値を入力します。

ステップ 4： Authentication Method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ます。必要に応じて、認証方式のタイプに応じて適切な認証値を入力します。

ステップ 5：xアイコン（赤い円）をクリックして、接続ウィンドウを閉じます。設定が自動的に保存されます。IPSecuritasウィンドウが表示されます。

Connection



ステップ 1：IPSecuritasウィンドウで、Startをクリックします。その後、ユーザはVPNにアクセスするために接続されます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。