Implante uma alternativa de VPN rápida para Mac OS nos roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

Não há versão de Quick VPN adequada para Mac OS. No entanto, há um número crescente de usuários que gostariam de implantar uma alternativa de VPN rápida para Mac OS. Neste artigo, o IP Securitas é usado como uma alternativa para uma VPN rápida.

Note: Você precisa fazer o download e instalar o IP Securitas em seu MAC OS antes de iniciar a configuração. Você pode baixá-lo no link a seguir:

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

Este artigo explica como implantar uma alternativa de VPN rápida para Mac OS em Rv016, RV042, RV042G e RV082 VPN Routers.

Dispositivos aplicáveis

- RV016
- RV042
- RV042G
- RV082

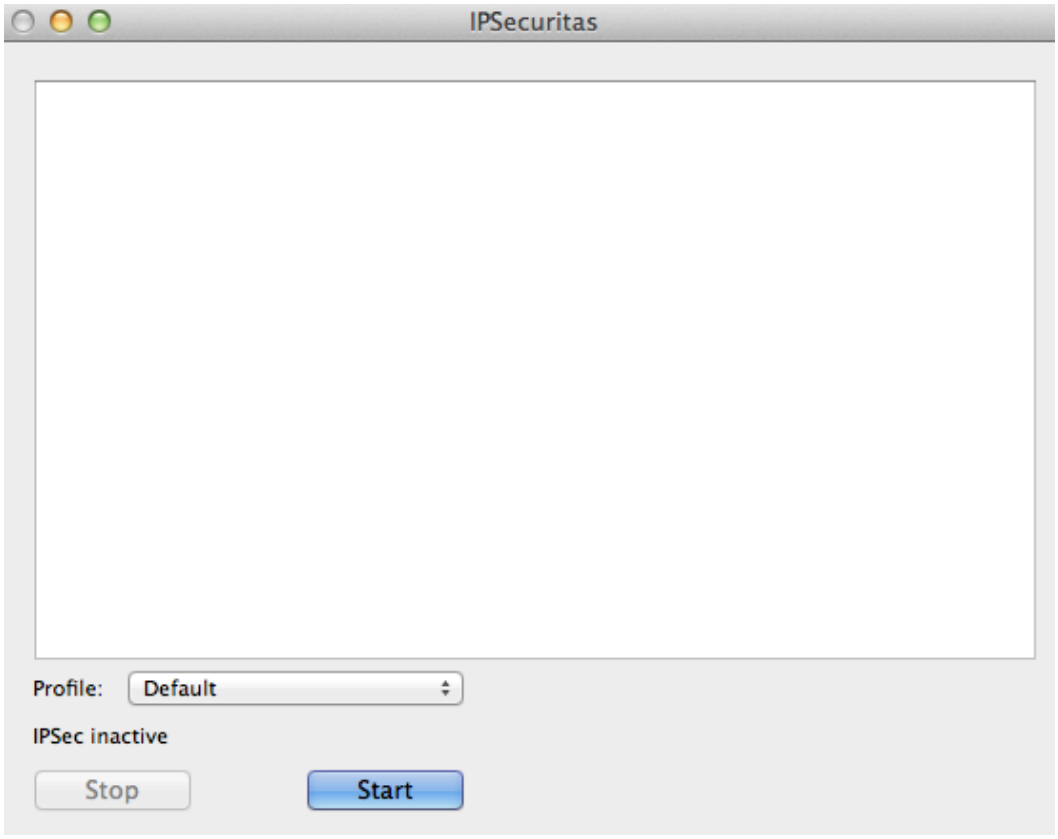
Versão de software

- v4.2.2.08

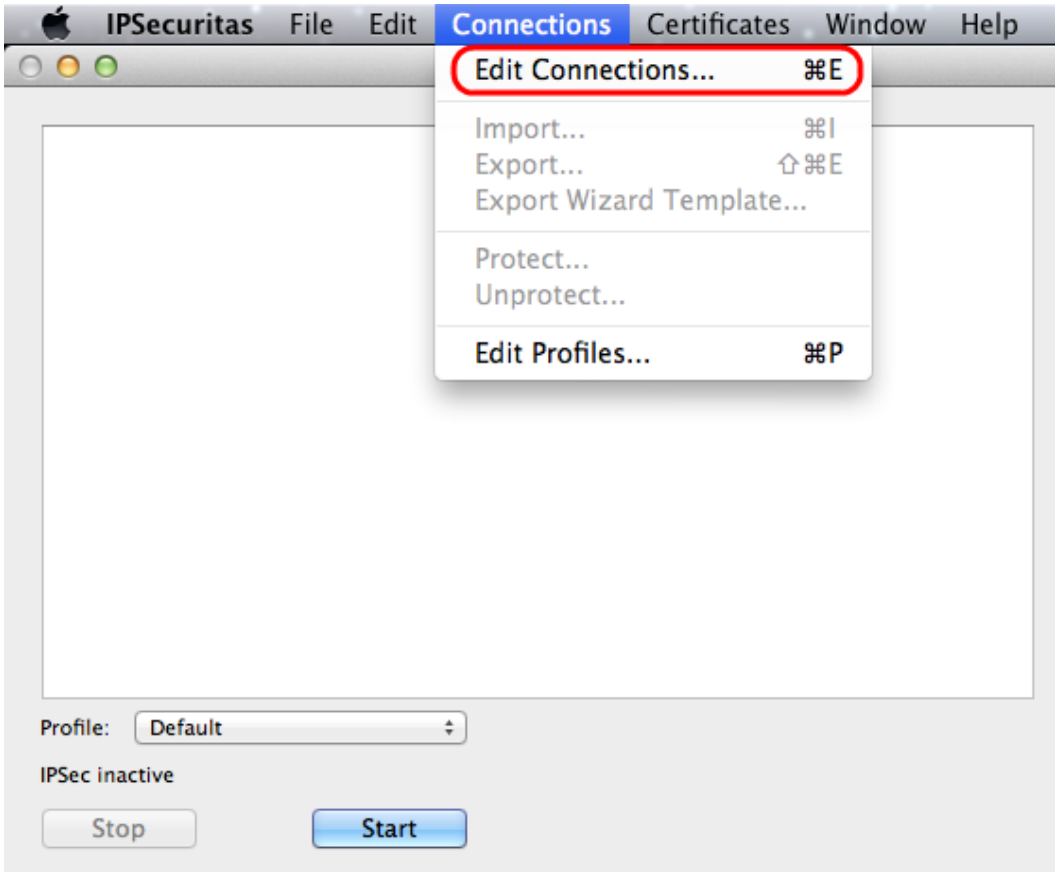
Implante uma alternativa de VPN rápida para Mac OS

Note: A configuração do VPN Client to Gateway do dispositivo precisa ser feita primeiro. Para saber mais sobre como configurar o VPN Client para Gateway, consulte *Configurar um túnel de acesso remoto (Cliente para Gateway) para VPN Clients em RV016, RV042, RV042G e RV082 VPN Routers.*

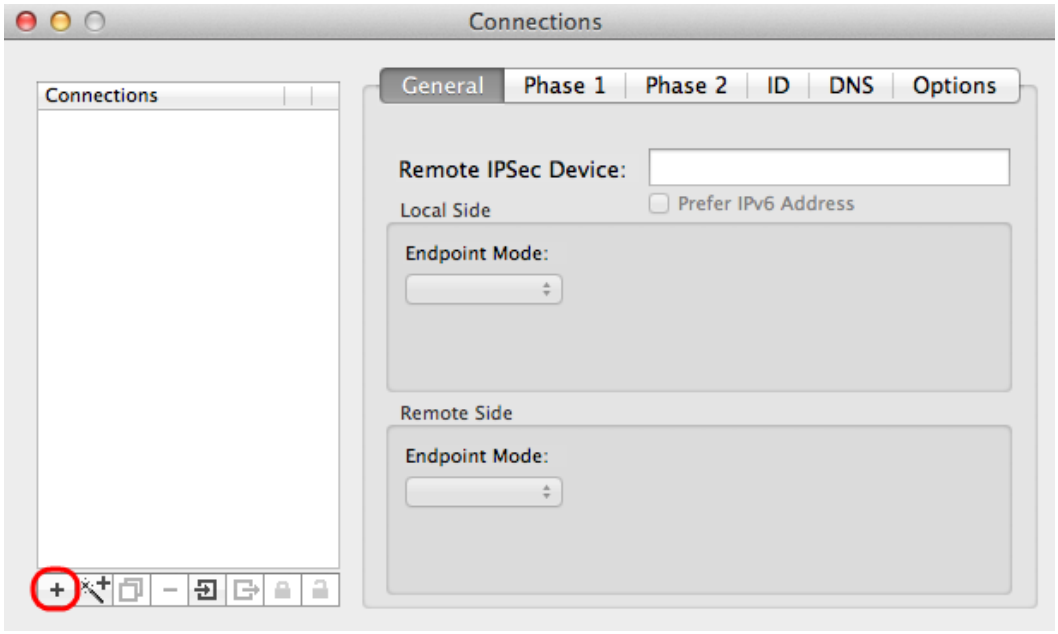
Etapa 1. Execute o IP Securitas no Mac OS. A janela *IPSecuritas* é exibida:



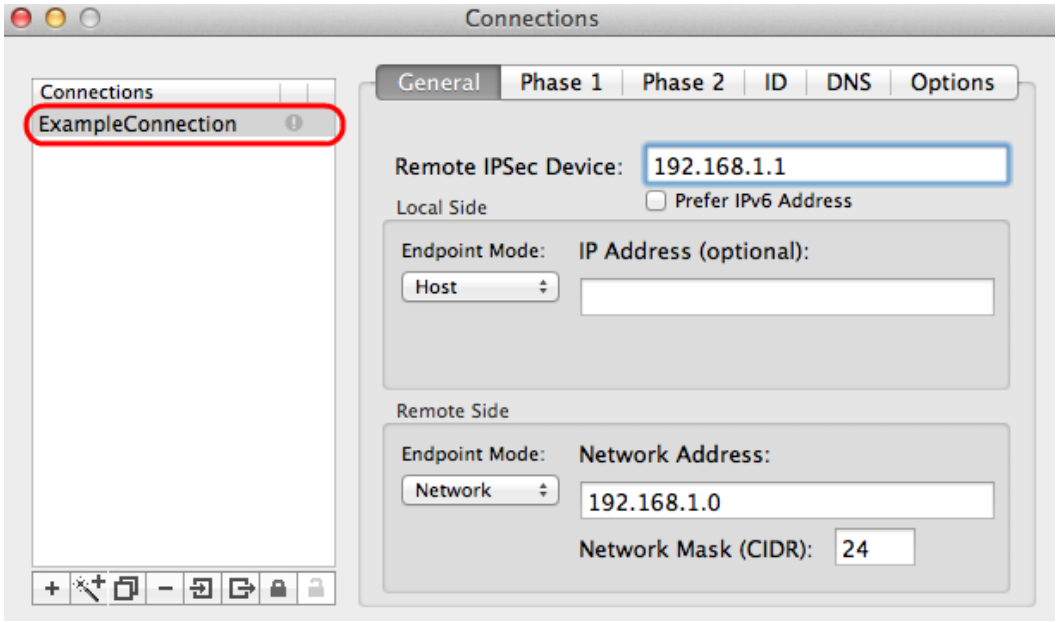
Etapa 2. Clique em Iniciar.



Etapa 3. Na barra de menus, escolha **Conexões > Editar conexões**. A janela *Conexões* é exibida.

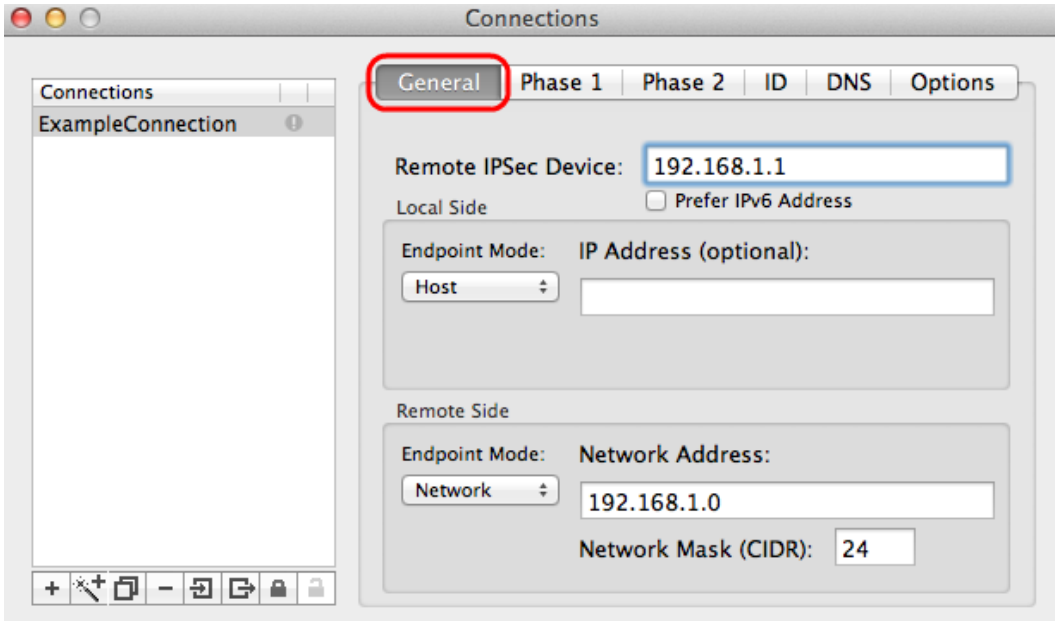


Etapa 4. Clique no **+** ícone para adicionar uma nova conexão.



Etapa 5. Insira um nome para a nova conexão em conexões.

General



Etapa 1. Clique na guia **Geral.**

Etapa 2. Insira o endereço IP do roteador remoto no campo Remote IPSec Device.

Note: Você não precisa configurar o Lado Local, pois esta configuração é para o cliente remoto. Você só precisa configurar o modo remoto.

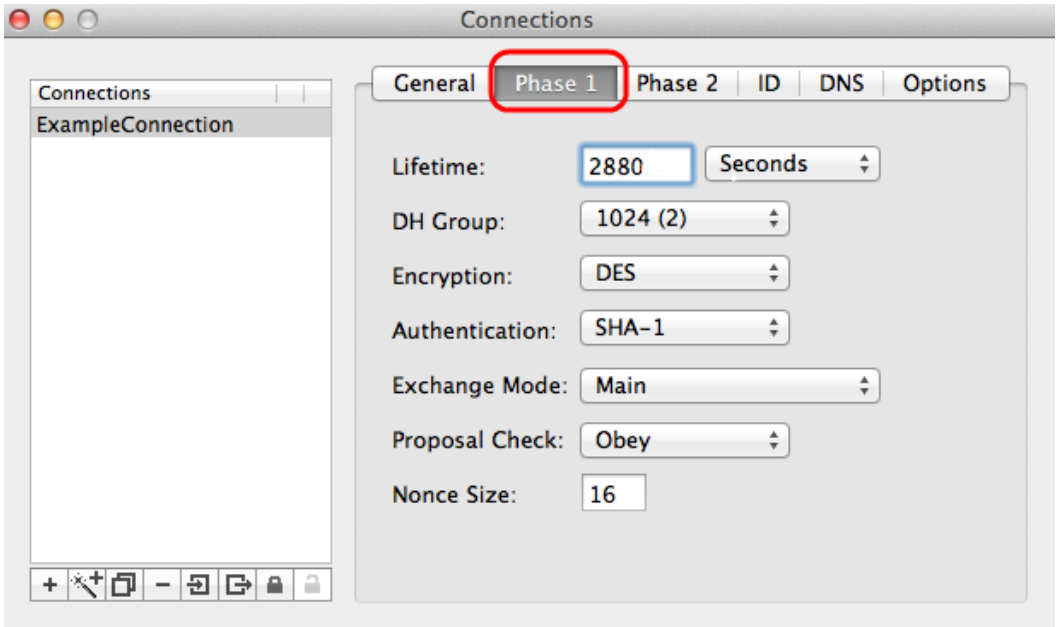
Etapa 3. Na área do lado remoto, escolha **Rede** na lista suspensa Modo de endpoint.

Etapa 4. Insira a máscara de sub-rede no campo Máscara de rede (CIDR).

Etapa 5. Insira o endereço de rede remoto no campo Network Address (Endereço de rede).

Fase 1

A fase 1 é a associação de segurança lógica (SA) simplex entre as duas extremidades do túnel para suportar a comunicação autenticada segura.



Etapa 1. Clique na guia **Fase 1**.

Etapa 2. Digite o tempo de vida que você inseriu durante a configuração do túnel no campo Vida útil. Se o tempo expirar, uma nova chave será renegociada automaticamente. O tempo de vida da chave pode variar de 1081 a 86400 segundos. O valor padrão para a Fase 1 é 28800 segundos.

Etapa 3. Escolha a unidade de tempo apropriada para a Vida útil na lista suspensa Vida útil. O padrão é segundos.

Etapa 4. Escolha o mesmo Grupo DH que você inseriu para a configuração do túnel na lista suspensa Grupo DH. O grupo Diffie-Hellman (DH) é usado para troca de chaves.

Etapa 5. Escolha o tipo de criptografia na lista suspensa Criptografia inserida para a configuração do túnel. O método de criptografia determina o comprimento da chave usada para criptografar/descriptografar pacotes de payload de segurança de encapsulamento (ESP).

Etapa 6. Escolha o método de autenticação inserido para a configuração do túnel na lista suspensa Autenticação. O tipo de autenticação determina o método para autenticar pacotes ESP.

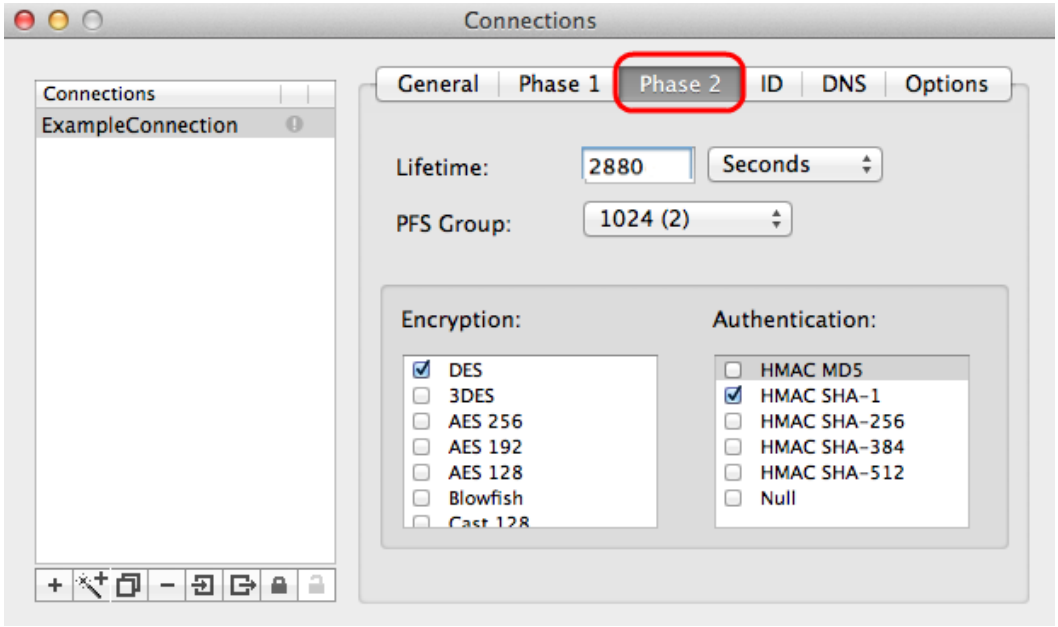
Passo 7. Escolha o modo de troca apropriado na lista suspensa Modo de troca.

Main — Representa o modo de troca para todos os tipos de gateway, exceto FQDN (Full Qualified Domain Name, Nome de domínio totalmente qualificado).

Agressivo — Representa o modo de troca para o gateway de Nome de Domínio Completo Qualificado (FQDN).

Fase 2

A fase 2 é a associação de segurança para determinar a segurança do pacote de dados durante a passagem dos pacotes de dados pelos dois pontos finais.



Etapa 1. Clique na guia **Fase 2**.

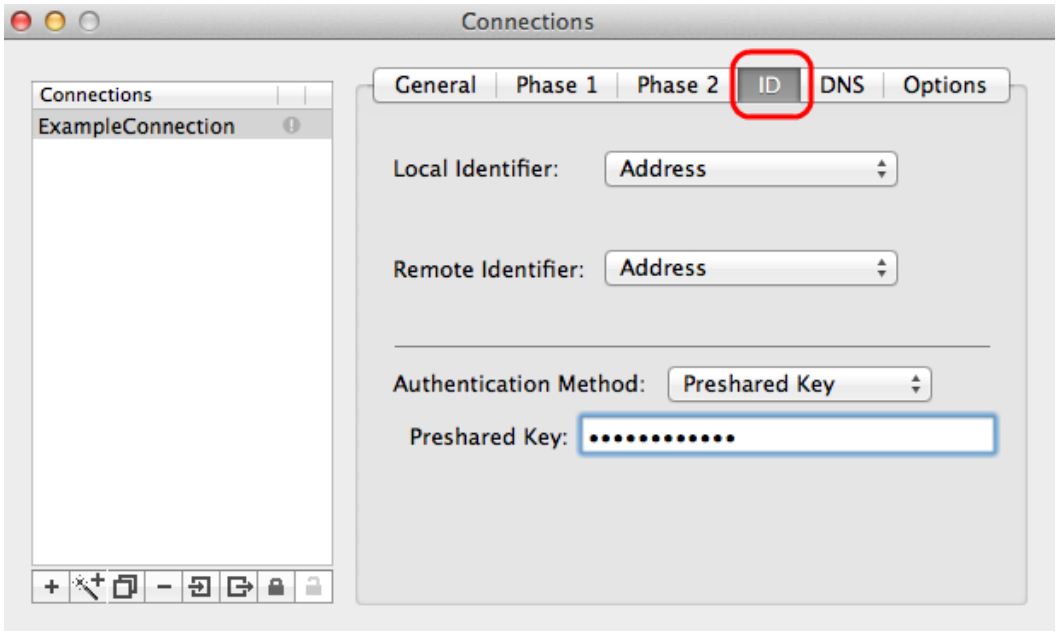
Etapa 2. Digite o mesmo tempo de vida no campo Vida útil que você inseriu para a configuração do túnel e também para a Fase 1.

Etapa 3. Escolha a mesma unidade de tempo da vida útil na lista suspensa Vida útil inserida para a configuração do túnel e Fase 1.

Etapa 4. Escolha o mesmo grupo DH na lista suspensa PFS (Perfect Forwarding Secret, segredo de encaminhamento perfeito) inserida para a configuração do túnel.

Etapa 5. Desmarque todos os métodos de criptografia e autenticação não utilizados. Verifique apenas os definidos na guia Fase 1.

ID



Etapa 1. Clique na guia **ID**.

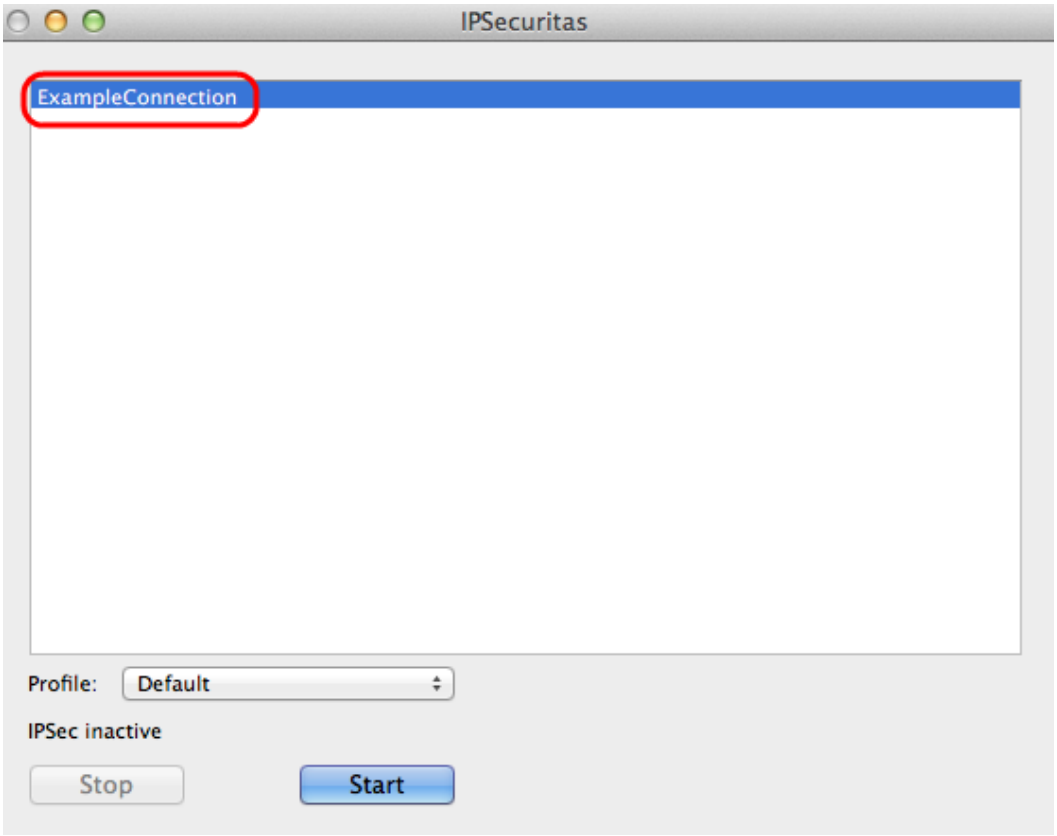
Etapa 2. Escolha o mesmo método de identificador local que o túnel na lista suspensa Identificador local. Insira o valor apropriado de acordo com o tipo de identificador local, se necessário.

Etapa 3. Escolha o mesmo método de identificador remoto que o túnel na lista suspensa Identificador remoto. Insira o valor apropriado de acordo com o tipo de identificador remoto, se necessário.

Etapa 4. Escolha o mesmo método de autenticação do túnel na lista suspensa Método de autenticação. Insira o valor de autenticação apropriado de acordo com o tipo de método de autenticação, se necessário.

Etapa 5. Clique no ícone **x** (círculo vermelho) para fechar a janela de conexão. Isso salva automaticamente as configurações. A janela *IPSecuritas* é exibida.

Conexão



Etapa 1. Na janela *IPSecuritas*, clique em **Iniciar**. O usuário é então conectado para acessar a VPN.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.