

# Configurando o cliente Shrew Soft VPN para se conectar ao RV34X Series Router

## Objetivo

O objetivo deste documento é mostrar como usar o cliente Shrew Soft VPN para se conectar a um roteador RV340 Series.

Você pode baixar a versão mais recente do software cliente Shrew Soft VPN aqui:

<https://www.shrew.net/download/vpn>

## Dispositivos aplicáveis | Versão do software

RV340 | 1.0.3.17 (Baixe o mais recente)

RV340W | 1.0.3.17 ([Baixe o mais recente](#))

RV345 | 1.0.3.17 ([Baixe o mais recente](#))

RV345P | 1.0.3.17 ([Baixe o mais recente](#))

## Introdução/Caso de uso

A VPN IPsec (Virtual Private Network) permite obter recursos remotos com segurança estabelecendo um túnel criptografado através da Internet. Os roteadores da série RV34X funcionam como servidores IPSEC VPN e suportam o Shrew Soft VPN Client. Este guia mostrará como configurar seu roteador e o Shrew Soft Client para proteger uma conexão a uma VPN.

Este documento tem duas partes:

Configurar o RV340 Series Router

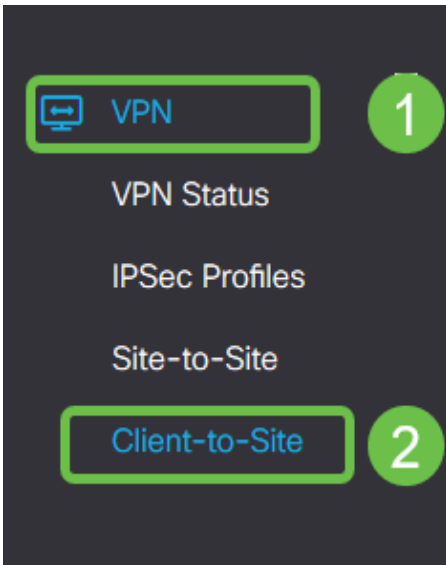
Configurar o cliente Shrew Soft VPN

**Configurar o RV34X Series Router:**

Começaremos configurando a **VPN cliente a site** no RV34x

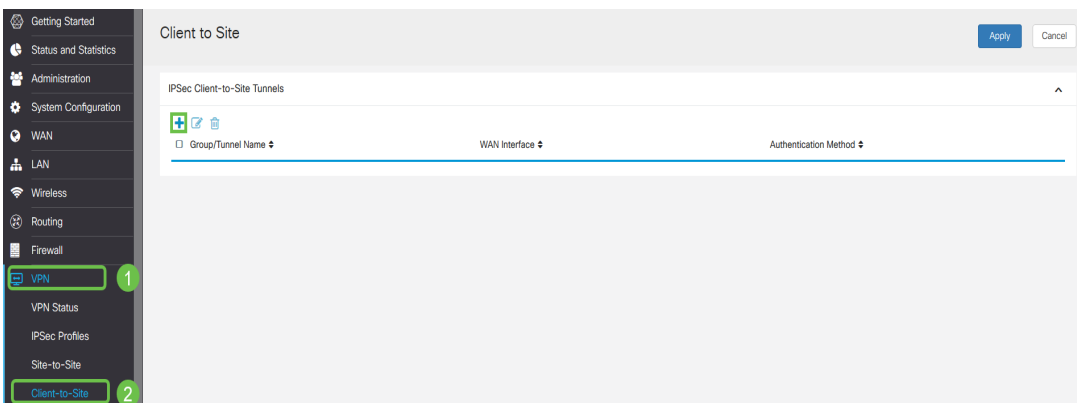
## Passo 1

Em **VPN > Cliente a Site**,



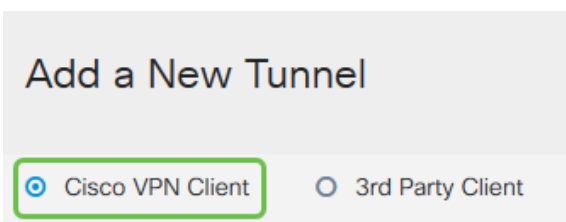
## Passo 2

Adicionar um perfil de **VPN Cliente a Site**



## Etapa 3

Selecione a opção **Cisco VPN Client**.



## Passo 4

Marque a caixa **Enable** para ativar o VPN Client Profile. Também configuraremos o *nome do grupo*, selecionaremos a **interface WAN** e inseriremos uma **chave pré-compartilhada**.

**Note:** Observe o *nome do grupo* e a *chave pré-compartilhada*, pois eles serão usados mais tarde ao configurar o cliente.

Enable:

Group Name: Clients

Interface: WAN1

---

### IKE Authentication Method

Pre-shared Key:

Minimum Pre-shared Key Complexity:  Enable

Show Pre-shared Key:  Enable

Certificate:

## Etapa 5

Deixe a **Tabela de grupos de usuários** em branco por enquanto. Isso é para o *Grupo de Usuários* no roteador, mas ainda não o configuramos. Verifique se **Mode** está definido como **Client**. Insira o **Intervalo de pool para LAN de cliente**. Usaremos 172.16.10.1 até 172.16.10.10.

**Note:** O intervalo de pool deve usar uma sub-rede exclusiva que não seja usada em outro lugar da rede.

User Group:

User Group Table

+  Group Name

---

Mode:  Client  NEM

Pool Range for Client LAN

Start IP: 172.16.10.1

End IP: 172.16.10.10

## Etapa 6

Aqui é onde definimos as configurações **de configuração do modo**. Aqui estão as configurações que usaremos:

**Servidor DNS primário:** Se você tiver um Servidor DNS interno ou quiser usar um Servidor DNS externo, você poderá inseri-lo aqui. Caso contrário, o padrão é o endereço IP da LAN RV340. Usaremos o padrão em nosso exemplo.

**Túnel dividido:** Marque para habilitar o Split Tunneling. Isso é usado para especificar qual tráfego passará pelo túnel VPN. Usaremos o Split Tunnel em nosso exemplo.

**Tabela de separação de túneis:** Insira as redes às quais o cliente VPN deve ter acesso através da VPN. Este exemplo usa a rede LAN RV340.

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain:

Backup Server 1:  (IP Address or Domain Name)

Backup Server 2:  (IP Address or Domain Name)

Backup Server 3:  (IP Address or Domain Name)

Split Tunnel:

Split Tunnel Table

+ [edit] [delete]

IP Address ↓ Netmask ↓

IP Address	Netmask
<input checked="" type="checkbox"/> 192.168.1.0	<input checked="" type="checkbox"/> 255.255.255.0

## Etapa 7

Depois de clicar em **Salvar**, podemos ver o Perfil na lista **Grupos Cliente para Site do IPSec**.

Client to Site

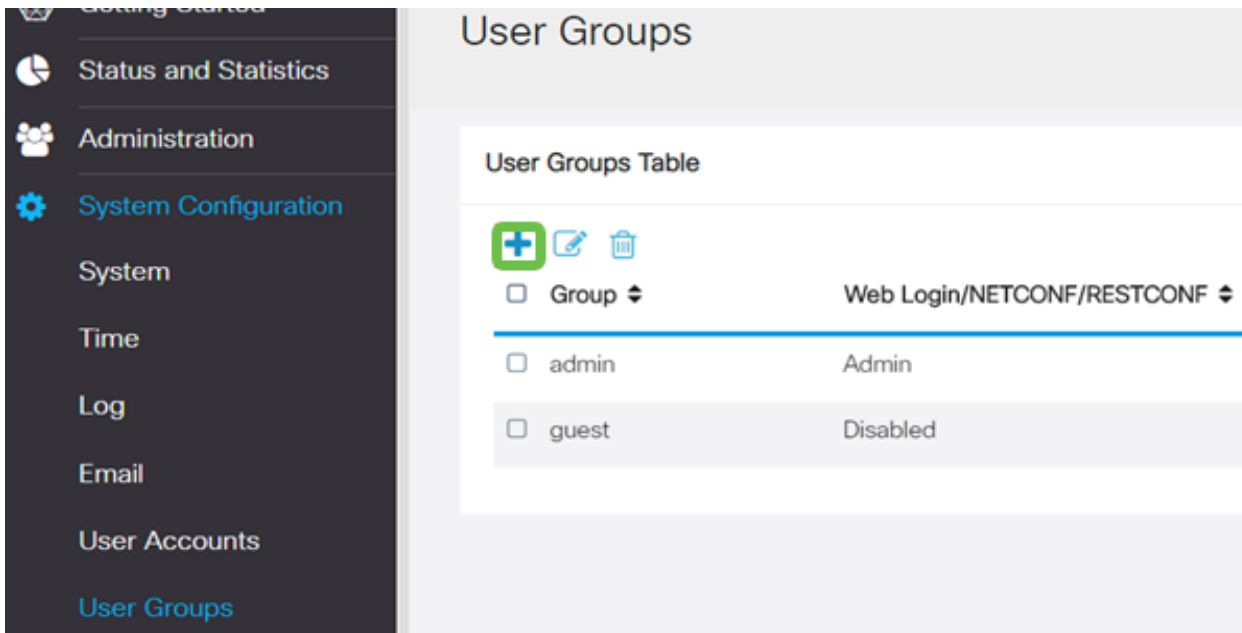
IPSec Client-to-Site Tunnels

+ [edit] [delete]

Group/Tunnel Name ↓	WAN Interface ↓	Authentication Method ↓
<input type="checkbox"/> Clients	WAN1	Pre-shared Key

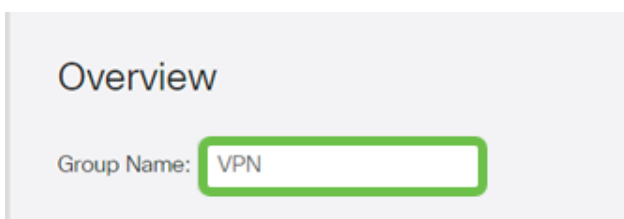
## Passo 8

Agora configuraremos um **Grupo de Usuários** para usar para Autenticar usuários de clientes VPN. Em **Configuração do sistema > Grupos de usuários**, clique em '+' para adicionar um grupo de usuários.



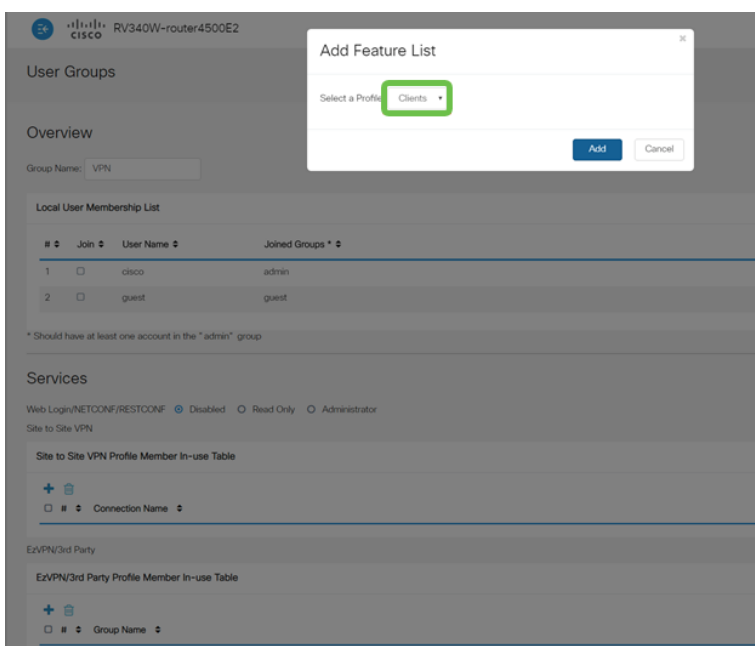
## Passo 9

Digite um nome de grupo.



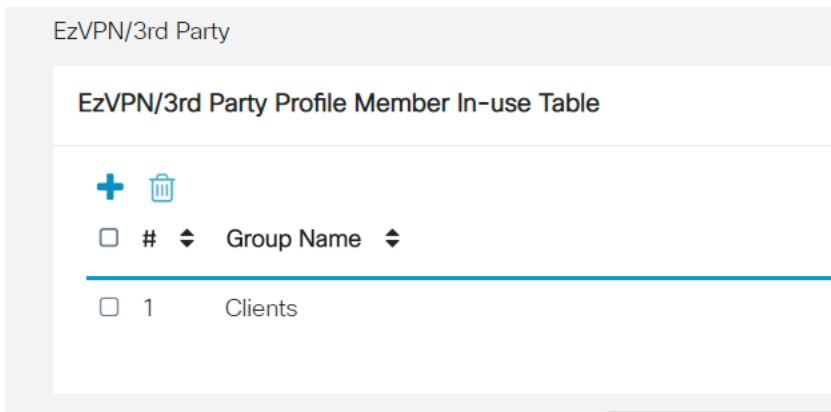
## Passo 10

Na seção **Serviços > EzVPN/Terceiros**, clique em **Adicionar** para vincular esse Grupo de Usuários ao Perfil de **Cliente para Site** configurado anteriormente.




## Passo 11

Agora você deve ver o nome do grupo **cliente a site** na lista para **EzVPN/terceiros**



EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

+ 

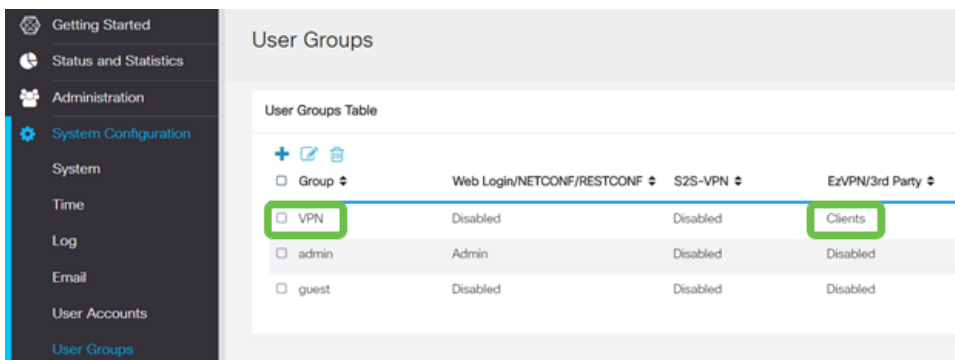
#  Group Name

---

1 Clients



## Etapa 12

Depois de **Aplicar** a configuração do Grupo de Usuários, você a verá na lista **Grupos de Usuários** e ela mostrará que o novo Grupo de Usuários será usado com o Perfil Cliente-Site que criamos anteriormente.



User Groups

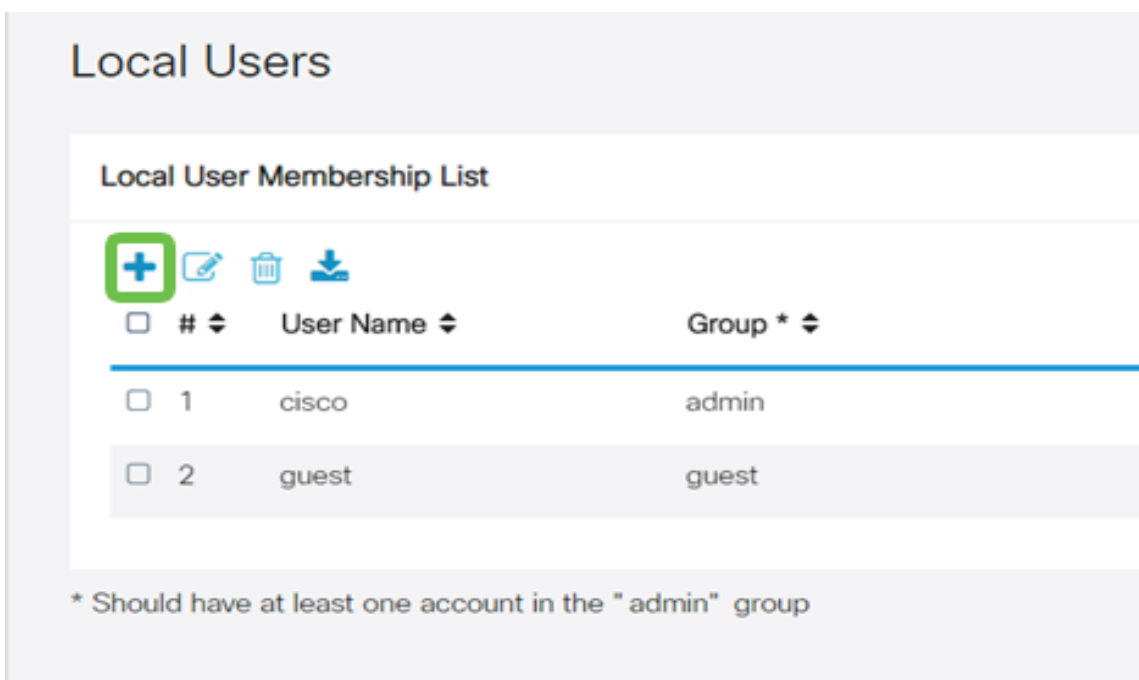
User Groups Table

+  

<input type="checkbox"/> Group <input type="checkbox"/>	Web Login/NETCONF/RESTCONF <input type="checkbox"/>	S2S-VPN <input type="checkbox"/>	EzVPN/3rd Party <input type="checkbox"/>
<input type="checkbox"/> VPN	Disabled	Disabled	<input type="checkbox"/> Clients
<input type="checkbox"/> admin	Admin	Disabled	Disabled
<input type="checkbox"/> guest	Disabled	Disabled	Disabled




## Passo 13

Agora, configuraremos um novo usuário em **Configuração do sistema > Contas de usuário**. Clique em '+' para criar um novo usuário.



Local Users

Local User Membership List

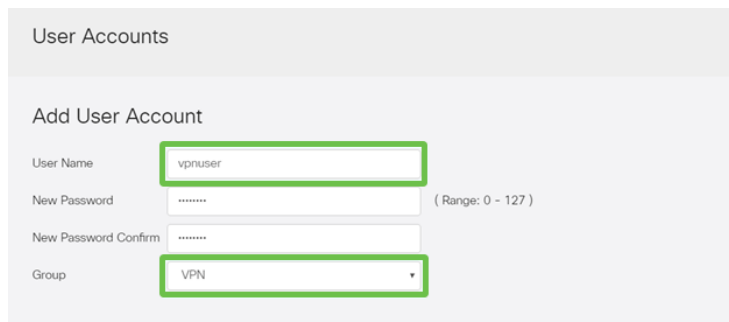
+   

<input type="checkbox"/> # <input type="checkbox"/>	User Name <input type="checkbox"/>	Group * <input type="checkbox"/>
<input type="checkbox"/> 1	cisco	admin
<input type="checkbox"/> 2	guest	guest

\* Should have at least one account in the "admin" group

## Passo 14

Insira o novo **Nome de usuário** junto com a **Nova senha**. Verifique se o **Grupo** está definido como o novo **Grupo de Usuários** que acabamos de configurar. Clique em **Apply** quando terminar.



User Accounts

Add User Account

User Name

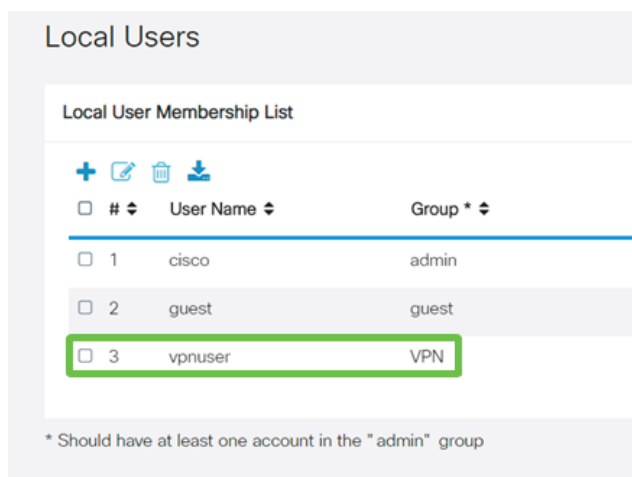
New Password  (Range: 0 - 127)

New Password Confirm

Group

## Etapa 15

O novo **usuário** aparecerá na lista de **Usuários locais**.



Local Users

Local User Membership List

+ ✎ 🗑️ ⬇️

<input type="checkbox"/>	#	User Name	Group *
<input type="checkbox"/>	1	cisco	admin
<input type="checkbox"/>	2	guest	guest
<input type="checkbox"/>	3	vpnuser	VPN

\* Should have at least one account in the "admin" group

Isso conclui a configuração no RV340 Series Router. Agora, configuraremos o cliente Shrew Soft VPN.

## Configurar o cliente VPN ShrewSoft

Agora, configuraremos o cliente Shrew Soft VPN.

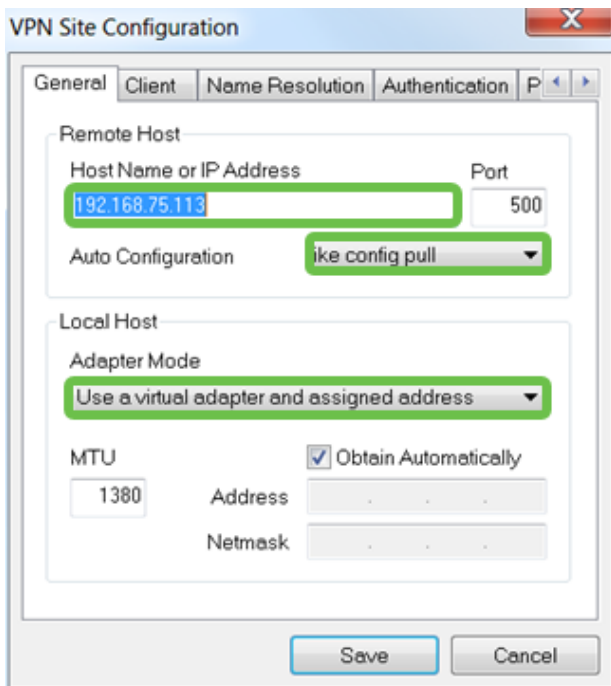
### Passo 1

Abra o *gerenciador de acesso VPN* ShrewSoft e clique em **Adicionar** para adicionar um perfil. Na janela *VPN Site Configuration* exibida, configure a guia **General**:

**Nome do host ou endereço IP:** Usar o endereço IP da WAN (ou nome de host do RV340)

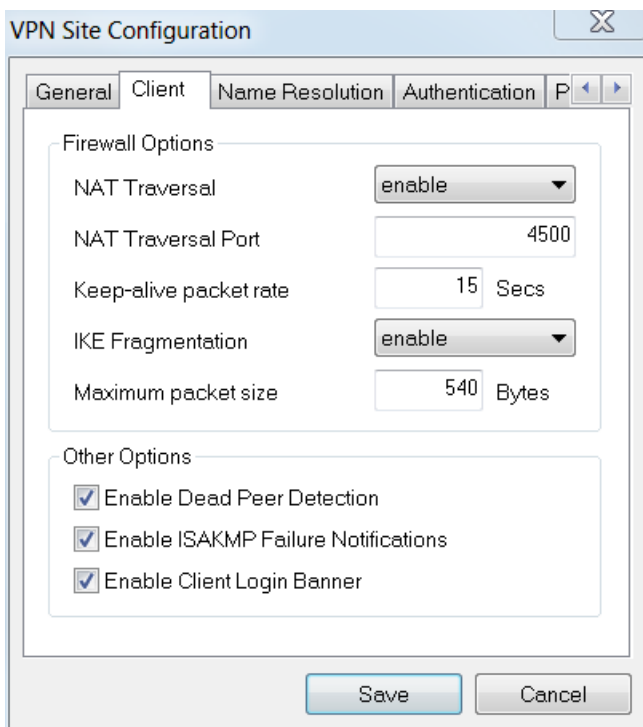
**Configuração automática:** Selecione **Ike config pull**

**Modo do adaptador:** Selecione **Usar um adaptador virtual e endereço atribuído**



## Passo 2

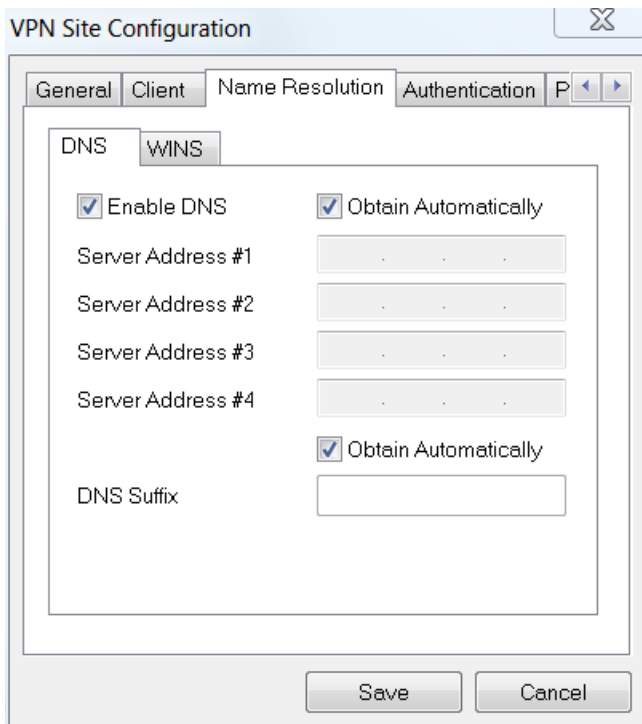
Configure a guia **Cliente**. Usaremos apenas as configurações padrão.



## Etapa 3

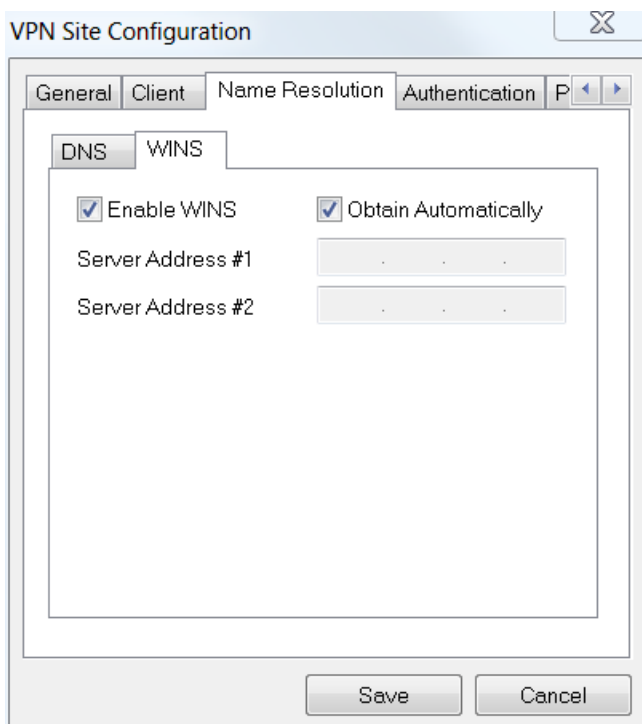
Na guia **Resolução de nome** > **DNS**, marque a caixa **Ativar DNS** e deixe as caixas **Obter automaticamente**.





#### Passo 4

Na guia **Resolução de nome > WINS**, marque a caixa **Ativar WINS** e deixe a caixa **Obter automaticamente** marcada.

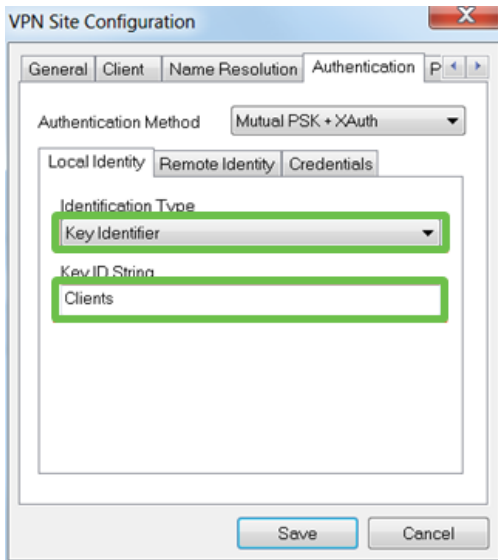


#### Etapa 5

Configure a guia **Authentication > Local Identity**:

**Tipo de identificação:** Selecionar **Identificador de Chave**

**String de ID da Chave:** Digite o nome do grupo configurado no RV34x



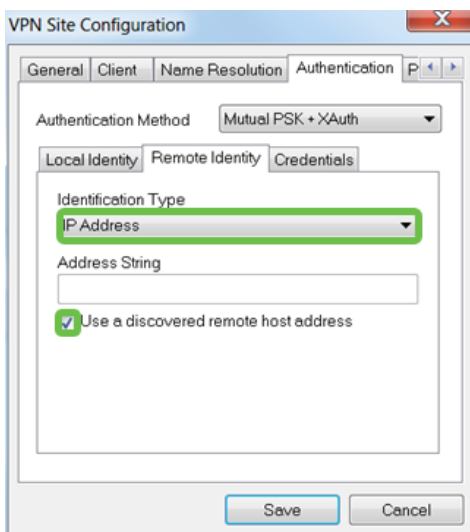
## Etapa 6

Na guia **Authentication > Remote Identity**, deixaremos as configurações padrão.

**Tipo de identificação:** IP Address

**String de Endereço:** <blank>

**Use uma caixa de endereço de host remoto descoberta:** Verificado

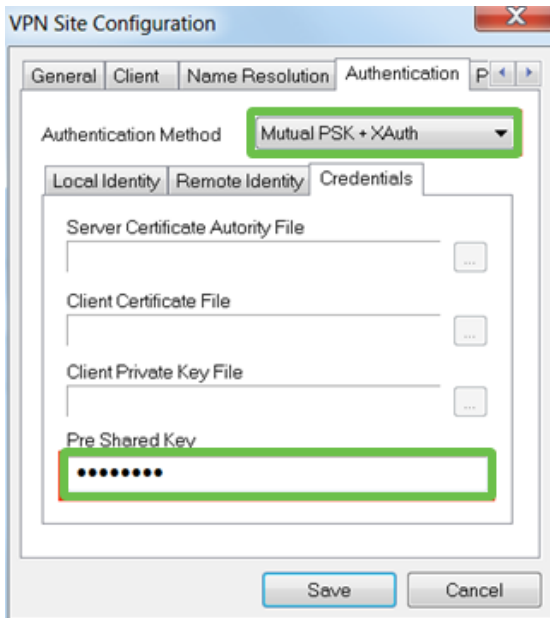


## Etapa 7

Na guia **Authentication > Credentials**, configure o seguinte:

**método de autenticação:** Selecione PSK Mútua + XAuth

**Chave pré-compartilhada:** Insira a chave pré-compartilhada configurada no perfil do cliente RV340



## Passo 8

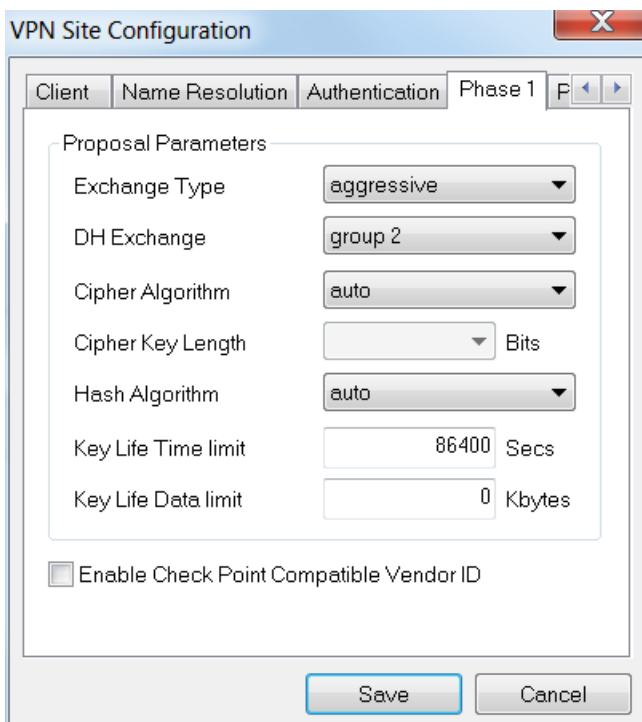
Para a guia **Fase 1**, deixaremos as configurações padrão no lugar:

**Tipo de troca:** Agressivo

**Troca DH:** grupo 2

**Algoritmo de cifra:** Auto

**Algoritmo de hash:** Auto



## Passo 9

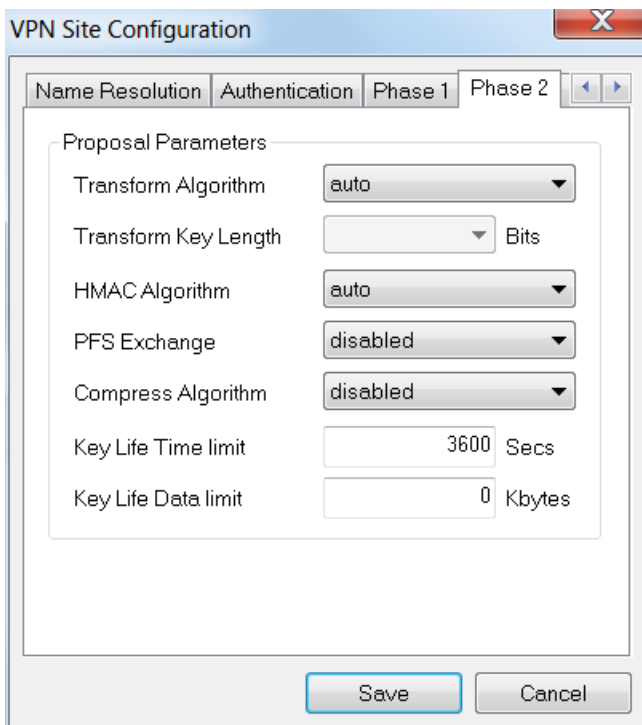
Também usaremos os padrões para a guia **Fase 2**:

**Algoritmo de transformação:** Auto

**Algoritmo HMAC:** Auto

**Troca de PFS:** Desabilitado

**Comprimir algoritmo:** Desabilitado



## Passo 10

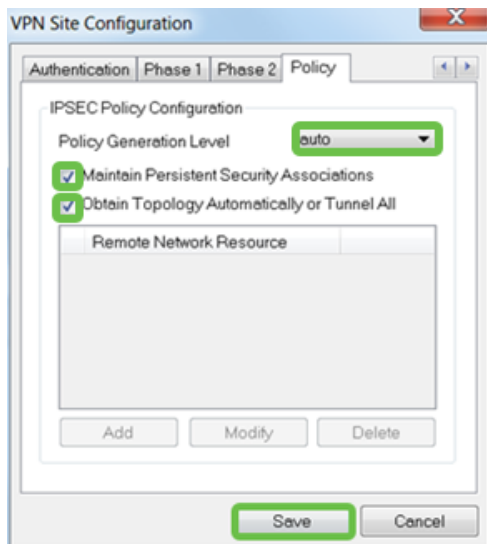
Na guia **Política**, usaremos as seguintes configurações:

**Nível de geração de política:** Auto

**Manter associações de segurança persistentes:** Verificado

**Obter Topologia Automaticamente ou Túnel Tudo:** Verificado

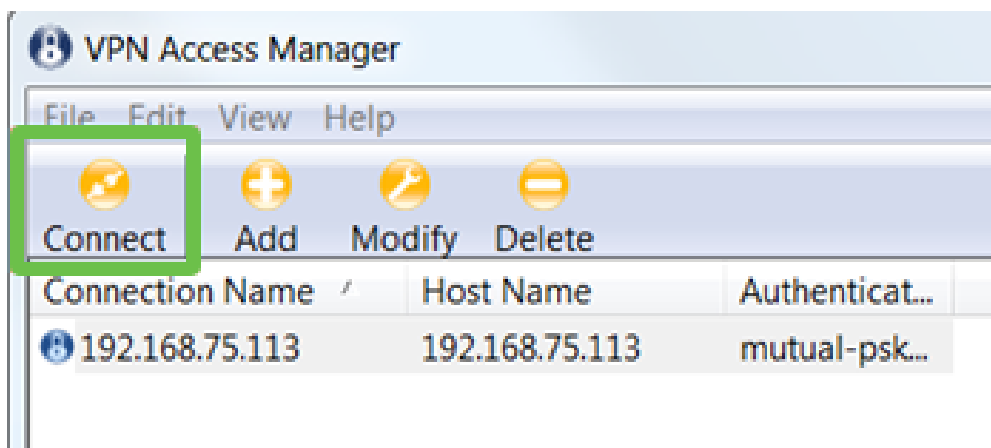
Como configuramos **Split-Tunneling** no RV340, não precisamos configurá-lo aqui.



Ao concluir, clique em **Save** (Salvar).

## Passo 11

Agora estamos prontos para testar a conexão. No *VPN Access Manager*, realce o perfil de conexão e clique no botão **Connect**.



## Etapa 12

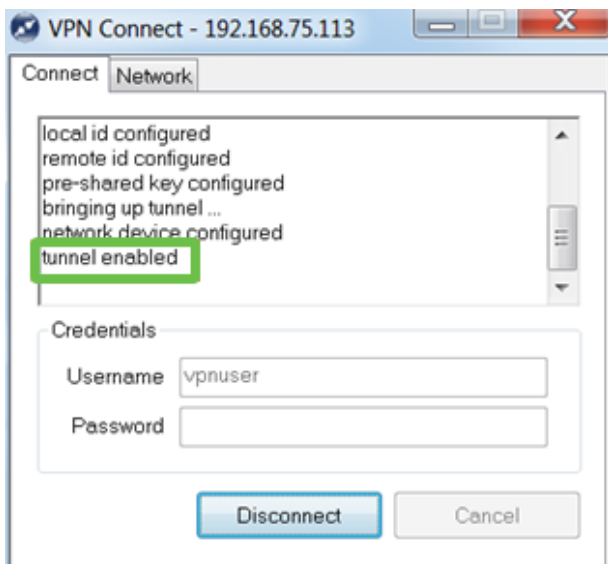
Na janela **VPN Connect** exibida, insira o **nome de usuário** e a **senha** usando as credenciais da **conta de usuário** que criamos no RV340 (etapas 13 e 14).



Quando terminar, clique em **Connect**.

### Passo 13

Verifique se o túnel está conectado. Você deve ver o **túnel ativado**.



## Conclusão

Aqui está, você agora está configurado para se conectar à sua rede via VPN.