

Configuración de Shrew Soft VPN Client para la conexión al RV34X Series Router

Objetivo

El objetivo de este documento es mostrar cómo utilizar el cliente Shrew Soft VPN para conectarse a un router RV340 Series.

Puede descargar la versión más reciente del software de cliente Shrew Soft VPN aquí:

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

Dispositivos aplicables | Versión de software

RV340 | 1.0.3.17 ([Descargar más reciente](#))

RV340W | 1.0.3.17 ([Descarga Más Reciente](#))

RV345 | 1.0.3.17 ([Descarga Más Reciente](#))

RV345P | 1.0.3.17 ([Descarga Más Reciente](#))

Introducción/Caso práctico

IPSec VPN (red privada virtual) permite obtener de forma segura recursos remotos mediante el establecimiento de un túnel cifrado a través de Internet. Los routers de la serie RV34X funcionan como servidores IPSEC VPN y admiten el cliente Shrew Soft VPN Client. En esta guía se muestra cómo configurar el router y el cliente de software de Cisco para asegurar una conexión a una VPN.

Este documento tiene dos partes:

Configuración del router serie RV340

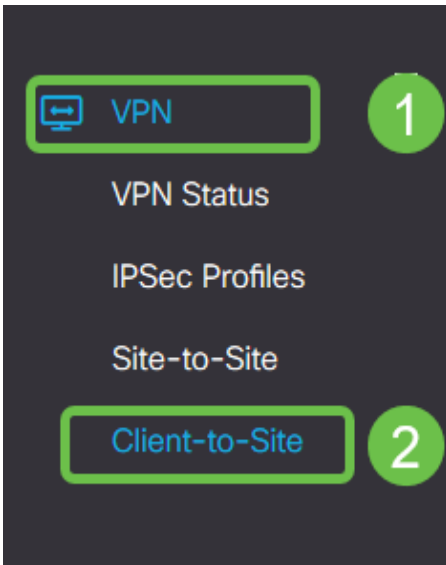
Configuración del cliente de Shrew Soft VPN

Configuración del router serie RV34X:

Comenzaremos configurando la **VPN cliente-sitio** en el RV34x

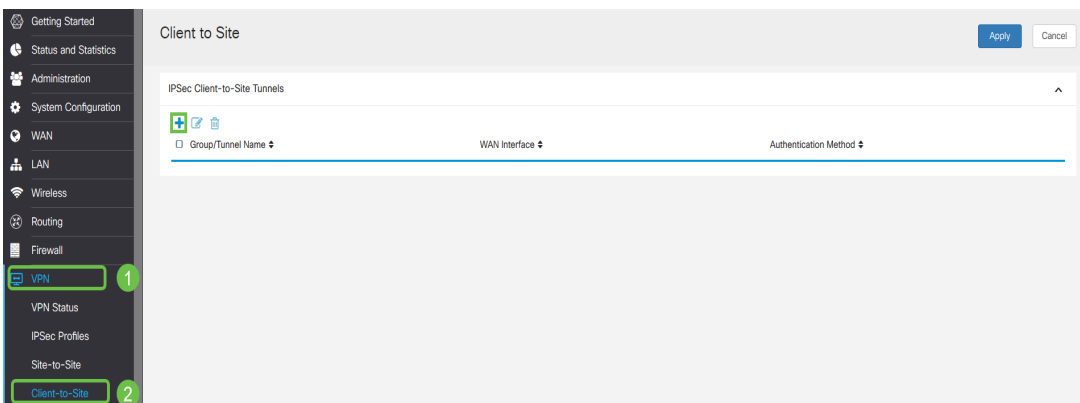
Paso 1

En **VPN > Cliente a Sitio**,



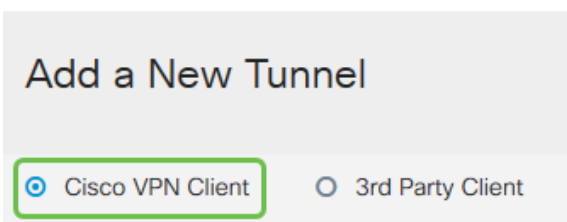
Paso 2

Agregar un perfil VPN **cliente-a-sitio**



Paso 3

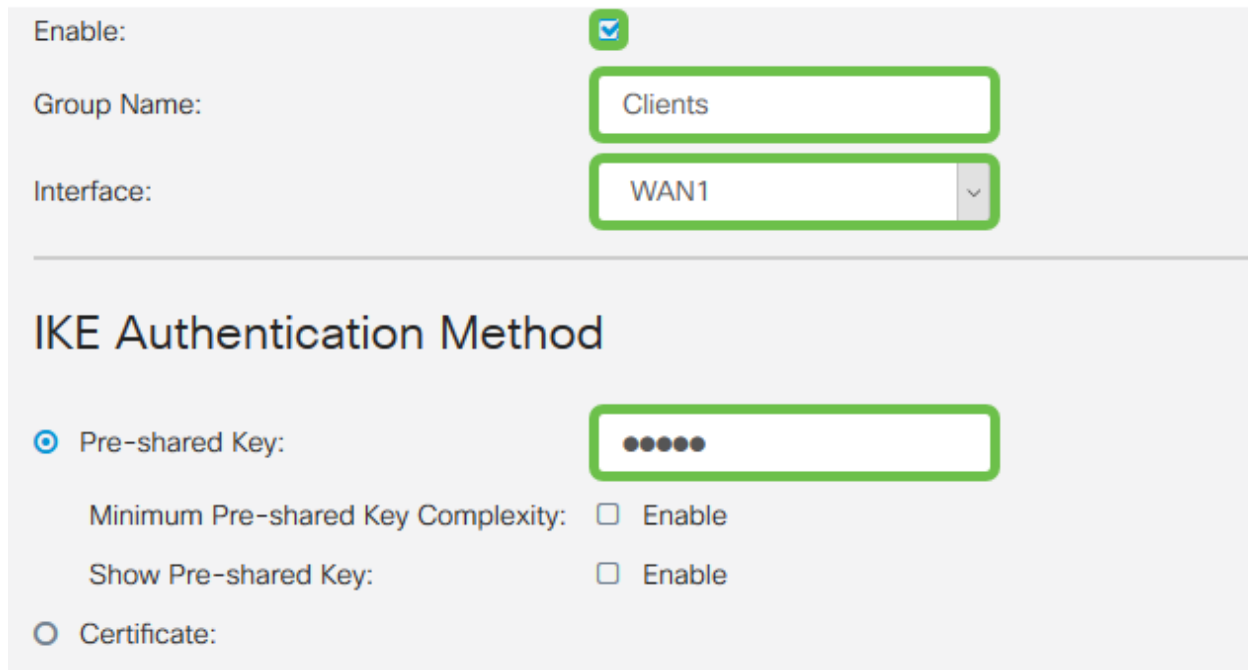
Seleccione la opción **Cisco VPN Client**.



Paso 4

Marque la casilla **Enable** para activar el perfil de cliente VPN. También configuraremos el *nombre del grupo*, seleccionaremos la **interfaz WAN** e introduciremos una **clave precompartida**.

Nota: Tenga en cuenta el *nombre de grupo* y la *clave precompartida*, ya que se utilizarán más adelante al configurar el cliente.



Enable:

Group Name: Clients

Interface: WAN1

IKE Authentication Method

Pre-shared Key: [Key field with 6 dots]

Minimum Pre-shared Key Complexity: Enable

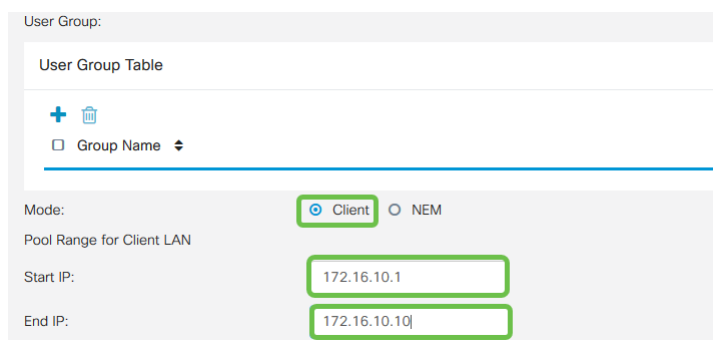
Show Pre-shared Key: Enable

Certificate:

Paso 5

Deje la **tabla de grupo de usuarios** en blanco por ahora. Esto es para el *grupo de usuarios* en el router, pero aún no lo hemos configurado. Asegúrese de que el **Modo** esté configurado en **Cliente**. Ingrese el **Rango del Conjunto para LAN del Cliente**. Utilizaremos de 172.16.10.1 a 172.16.10.10.

Nota: El rango del grupo debe utilizar una subred única que no se utiliza en ninguna otra parte de la red.



User Group:

User Group Table

+ [Add icon] [Trash icon]

Group Name

Mode: Client NEM

Pool Range for Client LAN

Start IP: 172.16.10.1

End IP: 172.16.10.10

Paso 6

Aquí es donde configuramos la configuración **de modo**. Estos son los ajustes que utilizaremos:

Servidor DNS primario: Si tiene un servidor DNS interno o desea utilizar un servidor DNS externo, puede introducirlo aquí. De lo contrario, el valor predeterminado se establece en la dirección IP de LAN RV340. Utilizaremos el valor predeterminado en nuestro ejemplo.

Túnel dividido: Marque esta opción para activar la tunelización dividida. Esto se utiliza para especificar qué tráfico pasará por el túnel VPN. Utilizaremos el túnel dividido en nuestro ejemplo.

Tabla de Túnel Dividido: Introduzca las redes a las que el cliente VPN debe tener acceso a través de la VPN. Este ejemplo utiliza la red 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 ⇅

<input checked="" type="checkbox"/> 192.168.1.0	255.255.255.0
---	---------------

Paso 7

Después de hacer clic en **Guardar**, podemos ver el perfil en la lista **Grupos de Cliente a Sitio de IPSec**.

Client to Site

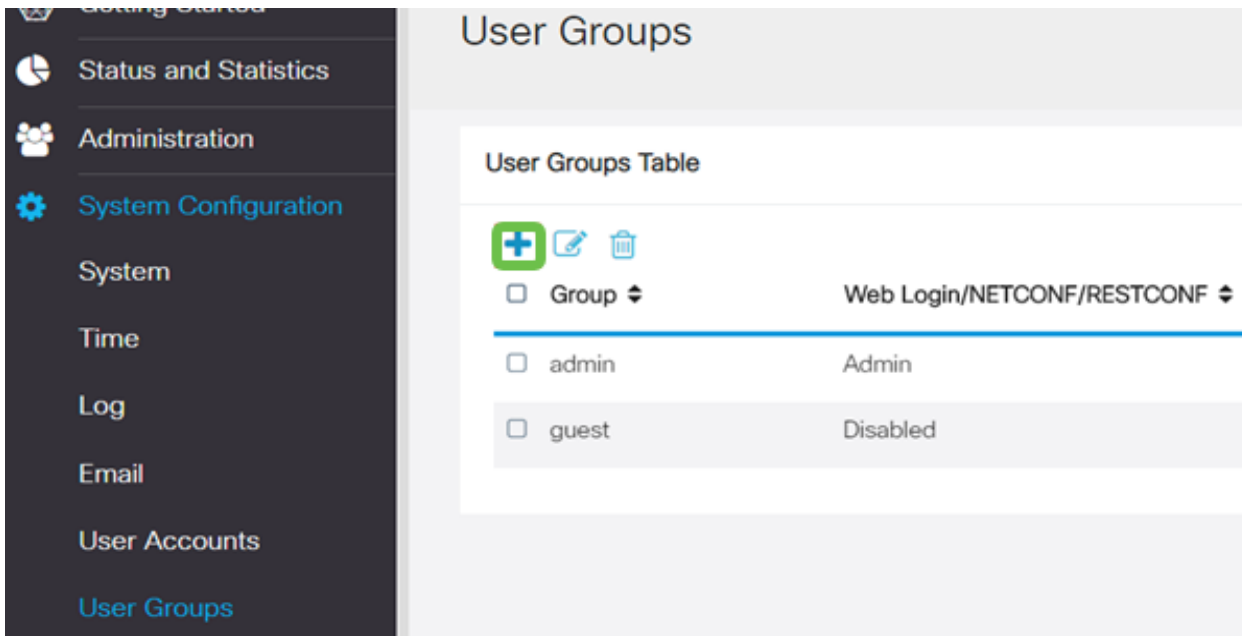
IPSec Client-to-Site Tunnels

+ [edit] [delete]

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

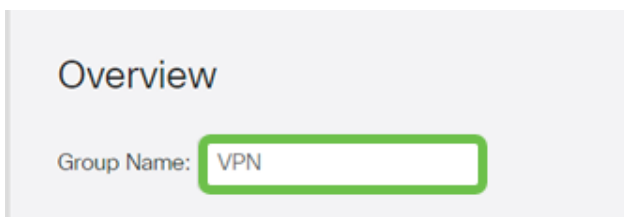
Paso 8

Ahora configuraremos un **grupo de usuarios** para que lo use para autenticar usuarios de clientes VPN. En **Configuración del sistema > Grupos de usuarios**, haga clic en "+" para agregar un grupo de usuarios.



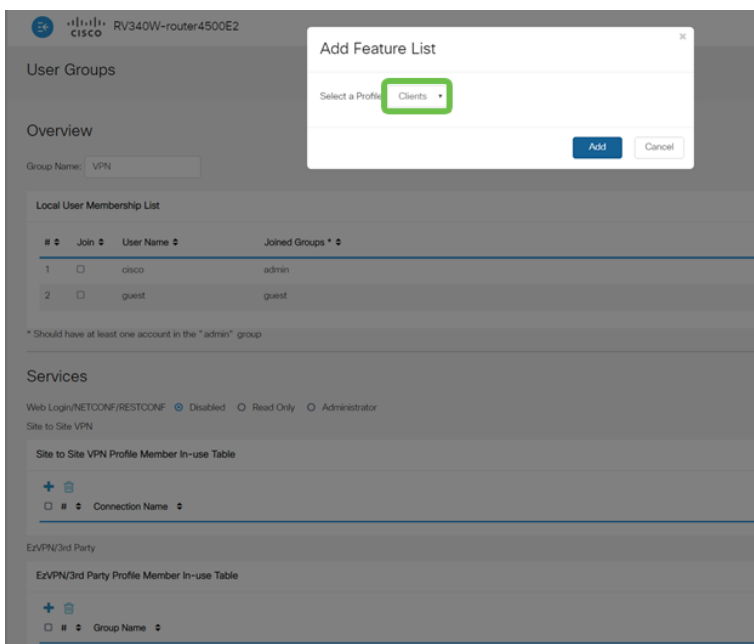
Paso 9

Introduzca un nombre de grupo.



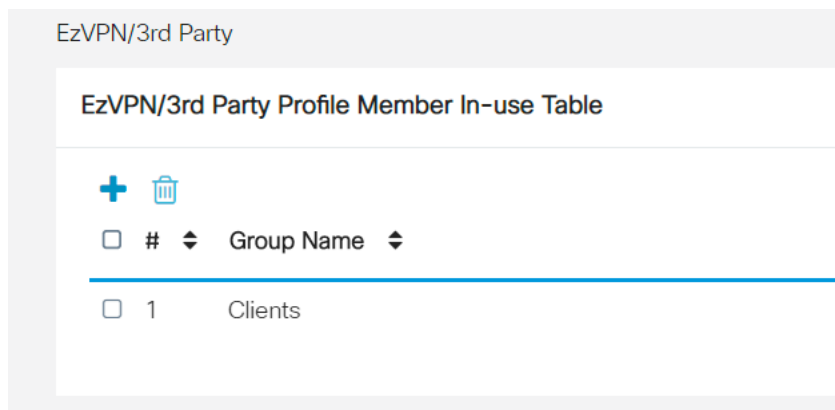
Paso 10

En la sección **Servicios > EzVPN/terceros**, haga clic en **Agregar** para vincular este grupo de usuarios al **perfil cliente a sitio** que configuramos anteriormente.




Paso 11

Ahora debería ver el nombre de grupo **cliente a sitio** en la lista de **EzVPN/terceros**



EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

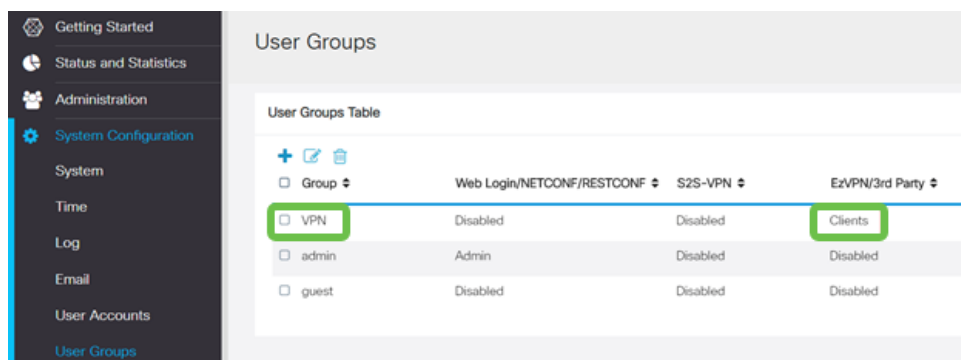
+ 

Group Name

1 Clients

Paso 12

Después de **Aplicar** la configuración del grupo de usuarios, la verá en la lista **Grupos de usuarios** y mostrará que el nuevo grupo de usuarios se utilizará con el perfil cliente a sitio que creamos anteriormente.



Getting Started

Status and Statistics

Administration

System Configuration

System

Time

Log



Email

User Accounts

User Groups

User Groups

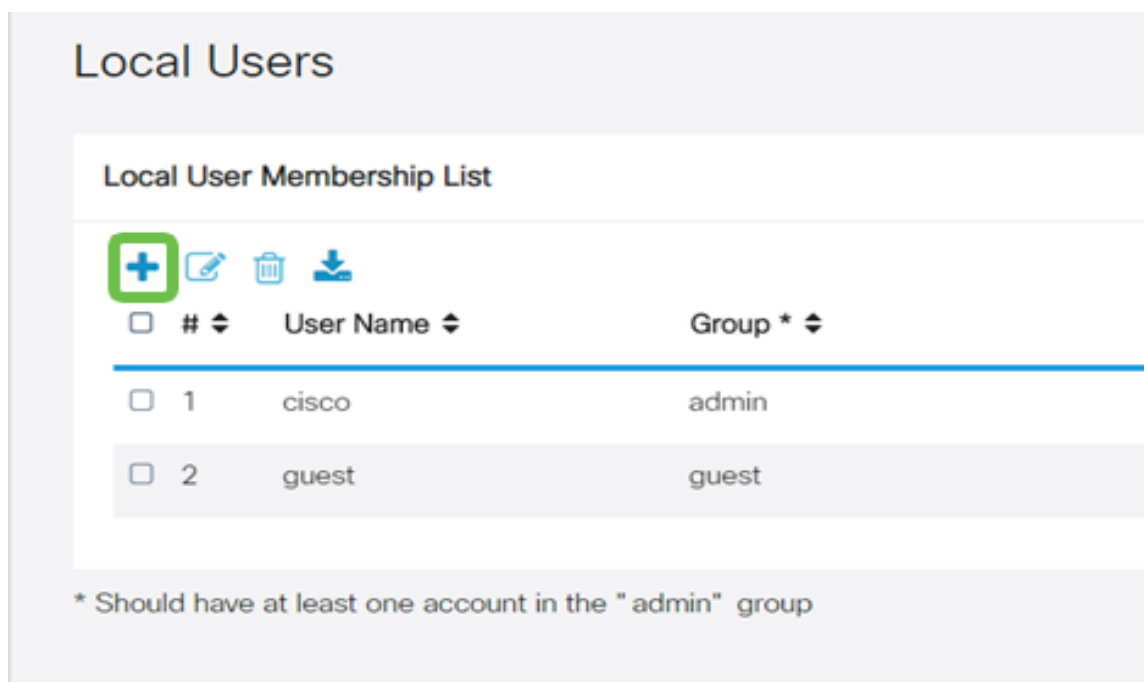
User Groups Table

+  

<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 <input type="checkbox"/>	Disabled	Disabled	Clients <input type="checkbox"/>
<input type="checkbox"/> admin <input type="checkbox"/>	Admin	Disabled	Disabled
<input type="checkbox"/> guest <input type="checkbox"/>	Disabled	Disabled	Disabled




Paso 13

Ahora configuraremos un nuevo usuario en **Configuración del sistema > Cuentas de usuario**. Haga clic en '+' para crear un nuevo usuario.



Local Users

Local User Membership List

+   

User Name Group *

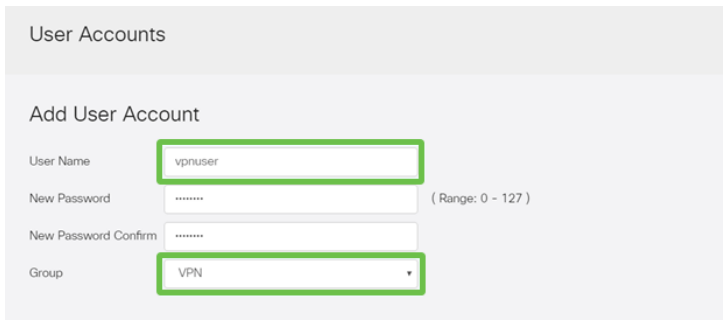
1 cisco admin

2 guest guest

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

Paso 14

Introduzca el nuevo **nombre de usuario** junto con la **nueva contraseña**. Verifique que el **grupo** esté configurado en el nuevo **grupo de usuarios** que acabamos de configurar. Haga clic en **Aplicar** cuando haya terminado.



User Accounts

Add User Account

User Name: vpnuser

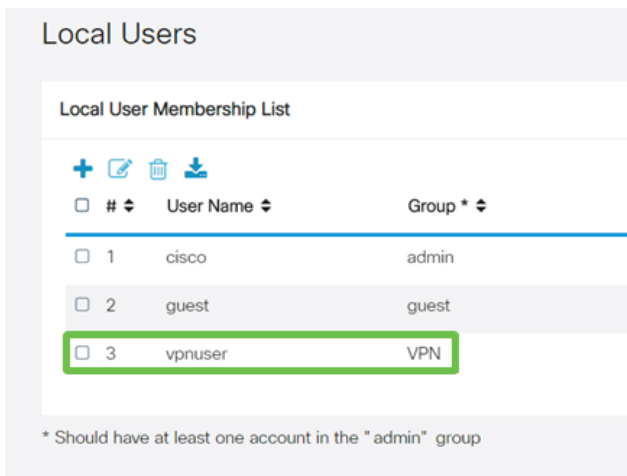
New Password: (Range: 0 - 127)

New Password Confirm:

Group: VPN

Paso 15

El nuevo **Usuario** aparecerá en la lista de **Usuarios Locales**.



Local Users

Local User Membership List

#	User Name	Group *
1	cisco	admin
2	guest	guest
3	vpnuser	VPN

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

Esto completa la configuración en el RV340 Series Router. Ahora configuraremos el cliente Shrew Soft VPN.

Configuración del cliente de VPN de ShrewSoft

Ahora configuraremos el cliente Shrew Soft VPN.

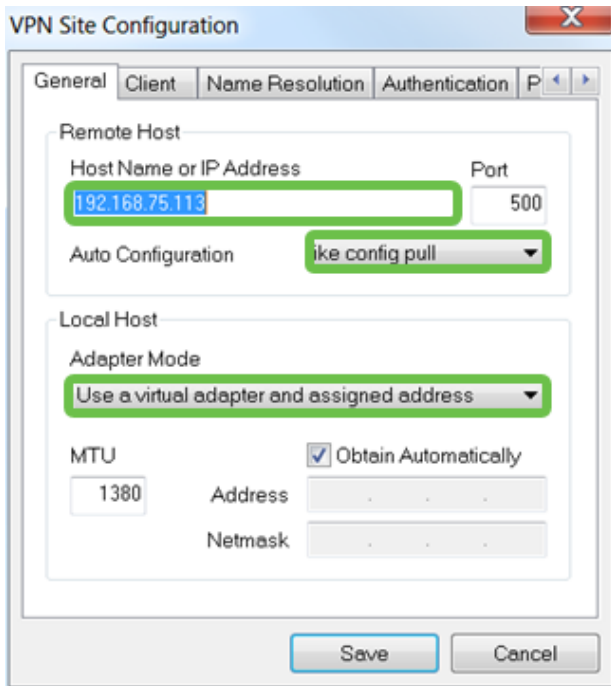
Paso 1

Abra el *administrador de acceso VPN de ShrewSoft* y haga clic en **Agregar** para agregar un perfil. En la ventana *VPN Site Configuration* que aparece, configure la **ficha General**:

Nombre de host o dirección IP: Utilice la dirección IP de WAN (o el nombre de host del RV340)

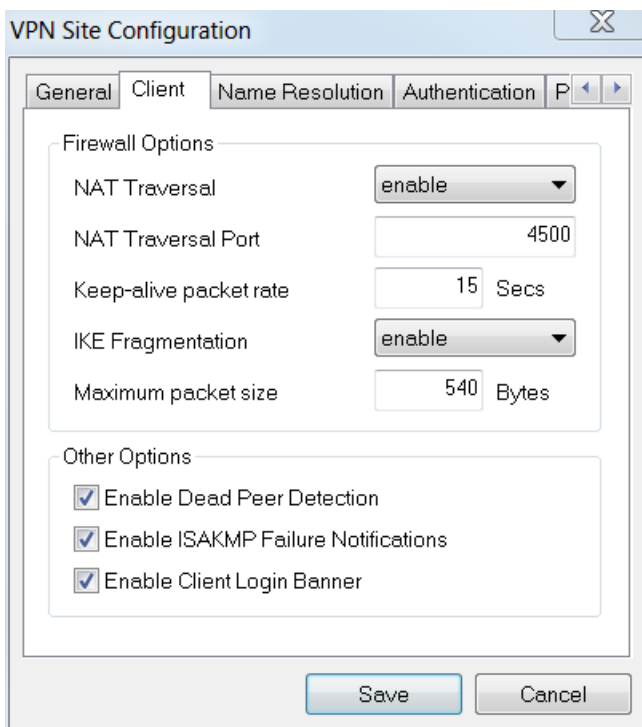
Configuración automática: Seleccione **ike config pull**

Modo adaptador: Seleccione **Usar un adaptador virtual y dirección asignada**



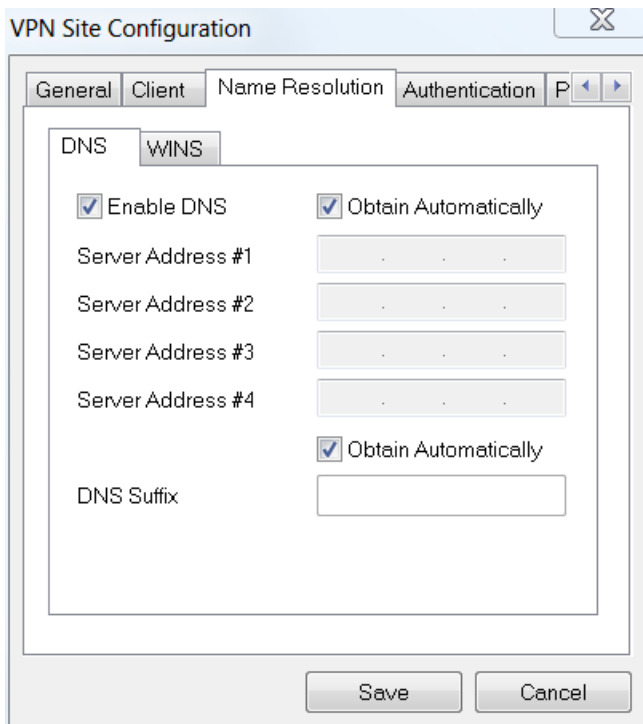
Paso 2

Configure la pestaña **Cliente**. Solo usaremos los parámetros predeterminados.



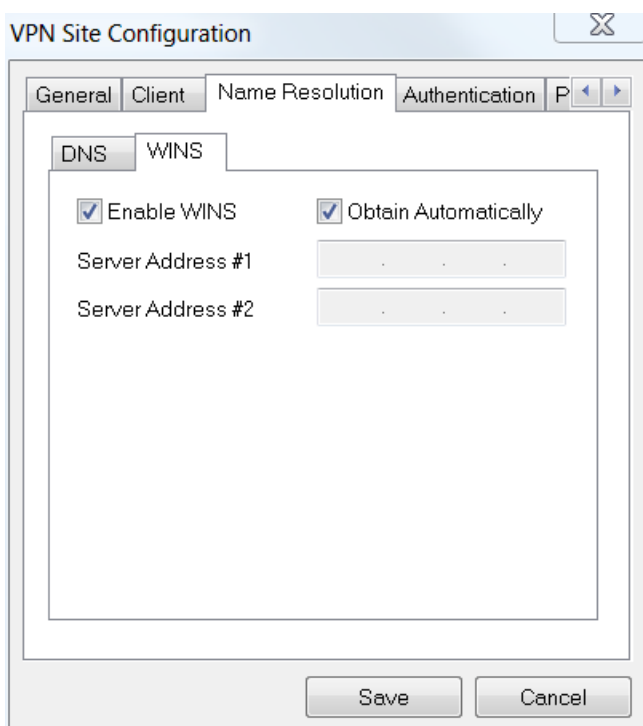
Paso 3

En la ficha **Resolución de nombres** > **ficha DNS**, active la casilla **Habilitar DNS** y deje las casillas **Obtener automáticamente** marcadas.



Paso 4

En la pestaña **Resolución de nombres** > ficha **WINS**, active la casilla **Habilitar WINS** y deje la casilla **Obtener automáticamente** marcada.

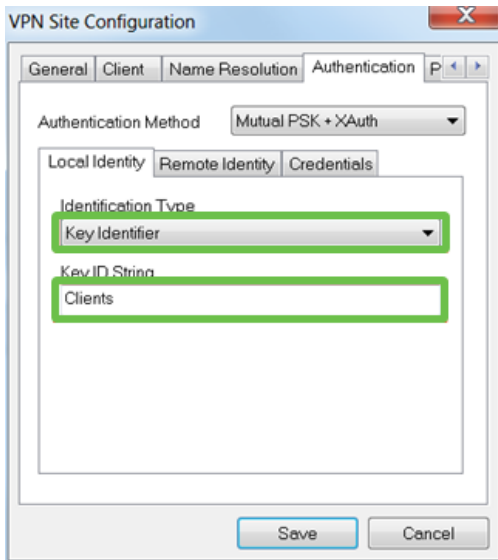


Paso 5

Configure la ficha **Authentication** > **Local Identity**:

Tipo de identificación: Seleccionar **identificador de clave**

Cadena de ID de clave: Introduzca el **nombre de grupo** configurado en el RV34x



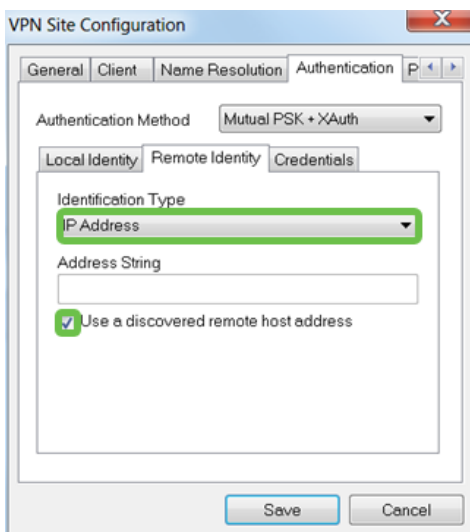
Paso 6

En la pestaña **Authentication > Remote Identity** , dejaremos las configuraciones predeterminadas.

Tipo de identificación: IP Address

Cadena de dirección: <blank>

Utilice un cuadro de dirección de host remoto detectado: Activado

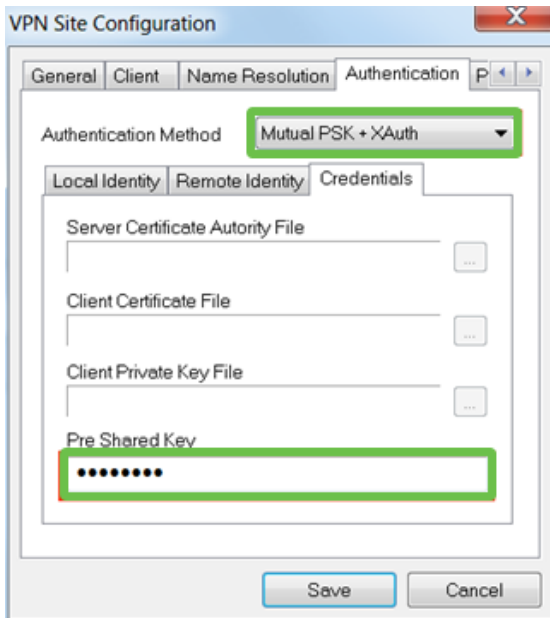


Paso 7

En la ficha **Autenticación > Credenciales**, configure lo siguiente:

método de autenticación: Seleccionar **PSK mutuo + XAuth**

Clave precompartida: Introduzca la **clave precompartida** configurada en el perfil de cliente RV340



Paso 8

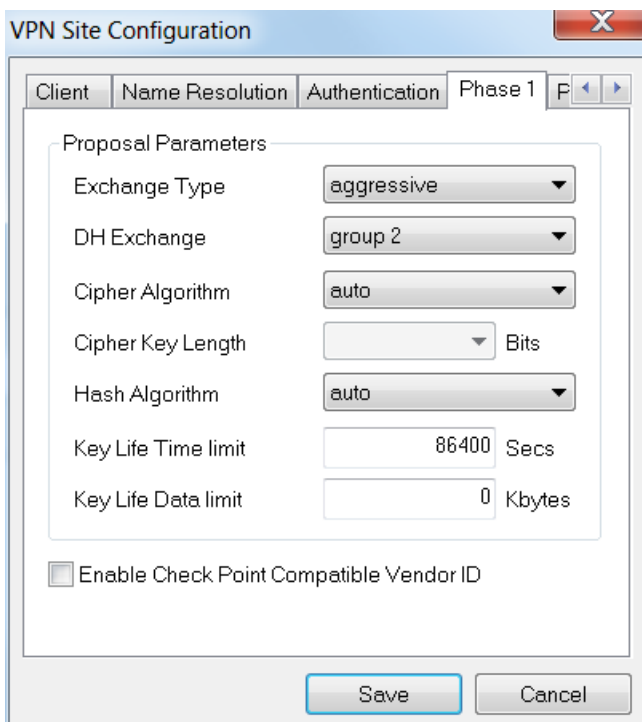
Para la pestaña **Fase 1**, dejaremos la configuración predeterminada en su lugar:

Tipo de intercambio: Agresivo

Intercambio DH: grupo 2

Algoritmo del cifrado: Auto

Algoritmo de hash: Auto



Paso 9

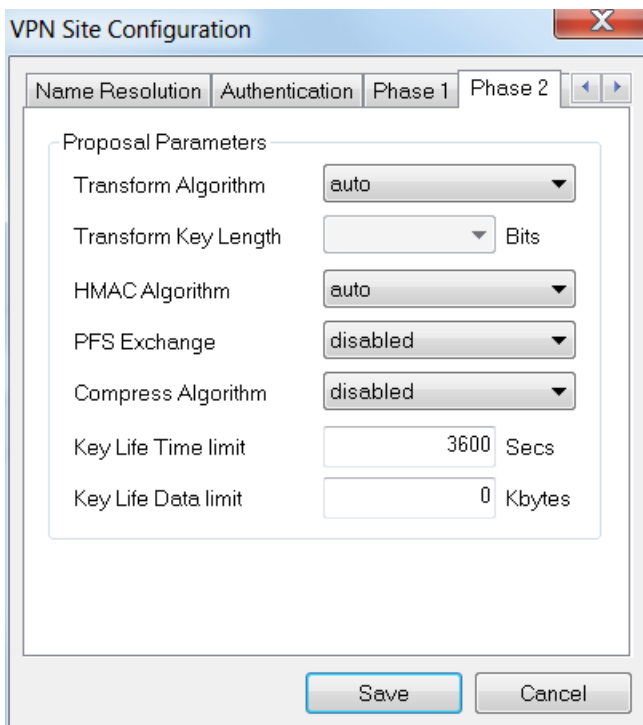
También utilizaremos los valores predeterminados para la pestaña **Fase 2**:

Algoritmo de transformación: Auto

Algoritmo HMAC: Auto

Intercambio de PFS: Inhabilitado

Algoritmo de compresión: Inhabilitado



Paso 10

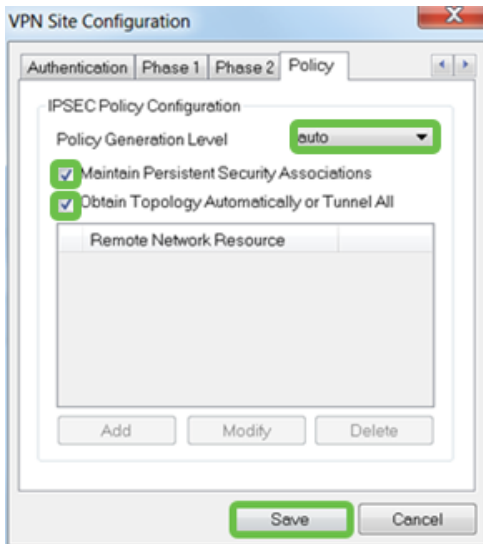
Para la ficha **Política**, utilizaremos las siguientes configuraciones:

Nivel de generación de políticas: Auto

Mantener asociaciones de seguridad persistentes: Activado

Obtener topología automáticamente o Túnel de todo: Activado

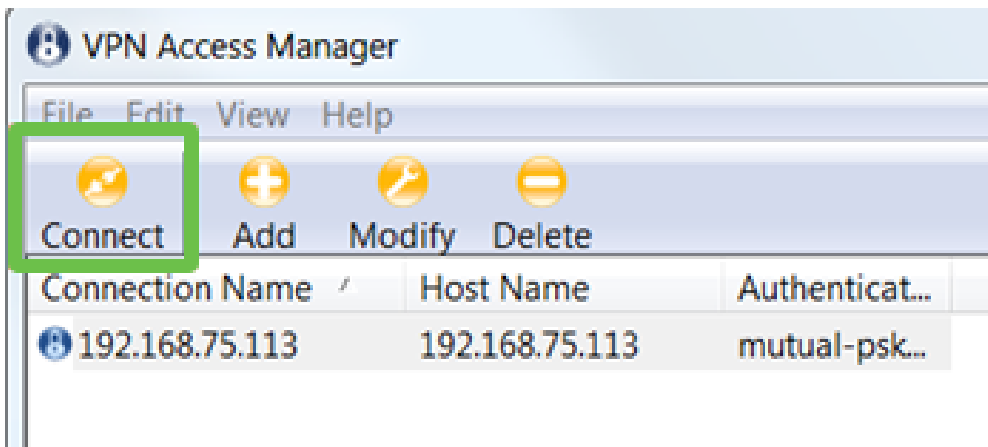
Dado que configuramos la **tunelización dividida** en el RV340, no necesitamos configurarlo aquí.



Cuando haya terminado, haga clic en **Guardar**.

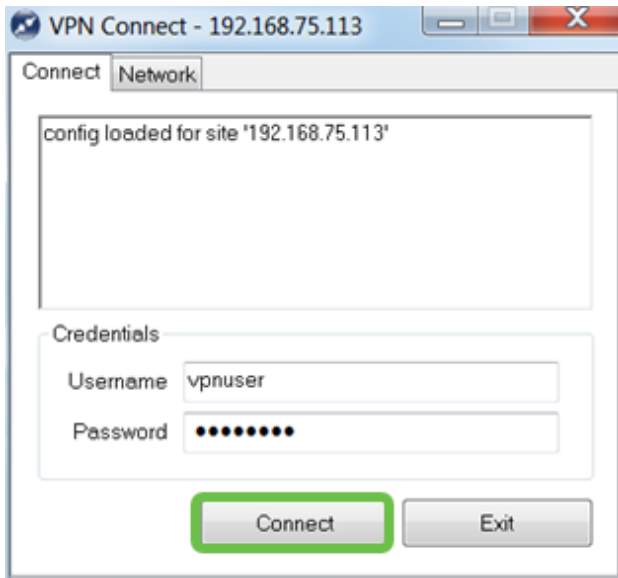
Paso 11

Ahora estamos listos para probar la conexión. En *VPN Access Manager*, resalte el perfil de conexión y haga clic en el **botón Connect**.



Paso 12

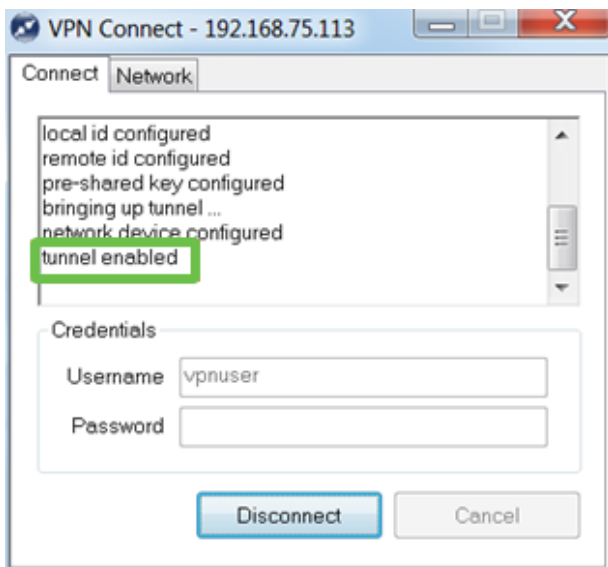
En la ventana **VPN Connect** que aparece, ingrese el **nombre de usuario** y la **contraseña** usando las credenciales para la **cuenta de usuario** que creamos en el RV340 (pasos 13 y 14).



Cuando haya terminado, haga clic en **Connect**.

Paso 13

Verifique que el túnel esté conectado. Debería ver **túnel habilitado**.



Conclusión

Ahí está, ahora está configurado para conectarse a su red a través de VPN.