# 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:

En VPN > Cliente a Sitio,



# Paso 2

Agregar un perfil VPN cliente-a-sitio

٢	Getting Started	Client to Site			Apply	Cancel
6	Status and Statistics				_	
e	Administration	IPSec Client-to-Site Tunnels				^
٥	System Configuration					
0	WAN	Group/Tunnel Name 🕈	WAN Interface 🗢	Authentication Method 🕈		
4	LAN					_
<b>?</b>	Wireless					
8	Routing					
	Firewall					
	VPN Status					
	IPSec Profiles					
	Site-to-Site					
C	Client-to-Site 2					

# 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			
IKE Authentication Metho	d		
<ul><li>IKE Authentication Metho</li><li>Pre-shared Key:</li></ul>	d •••••		
<ul> <li>IKE Authentication Metho</li> <li>Pre-shared Key: Minimum Pre-shared Key Complexity:</li> </ul>	d ••••• □ Enable		
<ul> <li>IKE Authentication Metho</li> <li>Pre-shared Key:</li> <li>Minimum Pre-shared Key Complexity: Show Pre-shared Key:</li> </ul>	d ••••• Enable Enable		

#### 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	
+ m ☐ Group Name	
Mode:	O 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:	192.168.1.1		
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			
+ 🕜 🖮			
☑ IP Address ◆			Netmask 🗢
☑ 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					
<ul> <li>+ 𝔅 m̂</li> <li>Group/Tunnel Name ≑</li> </ul>	WAN Interface \$	Authentication Method 🗢			
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**.



Introduzca un nombre de grupo.

Overview		
Group Name:	VPN	

#### 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.

il altalta cisco	RV340W-router45	00E2	×			
User Group	s	Add Feature List				
Overview Group Name: VP1	N	Select a Profile Clients	Add Cancel			
Local User Merr	nbership List					
# 0 Join 0	User Name ¢	Joined Groups * ¢				
1 0	cisco	admin				
2 🗆	guest	guest				
* Should have at les Services Web Login/NETCO Site to Site VPN	ast one account in the " a	tenin <sup>a</sup> geroup. Ieed O Read Only O Administrator				
Site to Site VPN	Profile Member In-use	Table				
+ ⊜ □ # ≎ Co	+ 8 • • Connection Name •					
EzVPN/3rd Party						
EzVPN/3rd Part	y Profile Member In-use	Table				
EXVPN/3rd Perty Profile Member In-use Table						

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



#### 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.

8	Getting Started	User Groups			
•	Status and Statistics				
*	Administration	User Groups Table			
۰	System Configuration	1.01.0			
	System	Group ¢	Web Login/NETCONF/RESTCONF \$	S2S-VPN ¢	EzVPN/3rd Party \$
	Time	O VPN	Disabled	Disabled	Clients
	Log	admin	Admin	Disabled	Disabled
	Email	guest	Disabled	Disabled	Disabled
	User Accounts				
	User Groups				

#### Paso 13

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



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	User Accounts			
Add User Acc	ount			
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.

	⊿	user Name ≑	Group * 🗢
		cisco	admin
	2	guest	guest
3	3	vpnuser	VPN

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

VPN Site Co	nfiguration			X
General (	General Client Name Resolution Authentication			
Remote Host       Host Name or IP Address       Port         192.168.75.113       5         Auto Configuration       ike config pull				500
-Local H Adapte Use a	Local Host Adapter Mode Use a virtual adapter and assigned address			•
MTU 138	0 Addre Netma	♥ Obtain ess . ask .	Automatically	
		Save	Ca	incel

Configure la pestaña Cliente. Solo usaremos los parámetros predeterminados.

VPN Site Configuration					
General Client Name Resolutio	n Authentication P				
Firewall Options					
NAT Traversal	enable 🔻				
NAT Traversal Port	4500				
Keep-alive packet rate	15 Secs				
IKE Fragmentation	enable 🔻				
Maximum packet size	540 Bytes				
Other Options					
Enable Dead Peer Detection	n				
Enable ISAKMP Failure Noti	fications				
🔽 Enable Client Login Banner					
Save Cancel					

# Paso 3

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

VPN Site Configuration	
General Client Name Res	solution Authentication P
DNS WINS	
Enable DNS	V Obtain Automatically
Server Address #1	
Server Address #2	
Server Address #3	
Server Address #4	
DNS Suffix	Obtain Automatically
	Save Cancel

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

VPN Site Configuration	X
General Client Name Resolution Authentication	P
DNS WINS	
Enable WINS     Obtain Automatically	
Server Address #1	
Server Address #2	
Save	ncel

#### 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

VPN Site Configuration			
General Client Name Resolution Authentication	P • •		
Authentication Method Mutual PSK + XAuth			
Local Identity Remote Identity Credentials			
Identification Type			
Key Identifier	-		
Key ID String	- 11		
Clients			
Save	ancel		

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

PN Site Configuration		
General Client Name Resolution Authentication P · ·		
Authentication Method Mutual PSK + XAuth		
Local Identity Remote Identity Credentials		
Identification Type		
IP Address 🔹		
Address String		
Use a discovered remote host address		
Save Cancel		

#### Paso 7

En la ficha Autenticación > Credenciales, configure lo siguiente:

método de autentificación: Seleccionar PSK mutuo + XAuth

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

VPN Site Configuration			
General Client Name Resolution Authentication P			
Authentication Method Mutual PSK + XAuth			
Local Identity Remote Identity Credentials			
Server Certificate Autority File			
Client Certificate File			
Client Private Key File			
Pre Shared Kev			
Save Cancel			

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

/PN Site Configuration	X	
Client Name Resolution	Authentication Phase 1 P	
Proposal Parameters		
Exchange Type	aggressive 💌	
DH Exchange	group 2 🔹	
Cipher Algorithm	auto 💌	
Cipher Key Length	The Bits	
Hash Algorithm	auto 💌	
Key Life Time limit	86400 Secs	
Key Life Data limit	0 Kbytes	
Enable Check Point Compatible Vendor ID		
	Save Cancel	

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

Proposal Parameters		
Transform Algorithm	auto	•
Transform Key Length	•	Bits
HMAC Algorithm	auto	-
PFS Exchange	disabled	•
Compress Algorithm	disabled	•
Key Life Time limit	3600	Secs
Key Life Data limit	0	Kbytes

#### 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**.

O VPN Access Manager		
View Hel	р	
•	<b>1</b>	
Add N	lodify Delete	
n Name 🥠	Host Name	Authenticat
3.75.113	192.168.75.113	mutual-psk
	View Hel Add Mon Name /	Coess Manager View Help Add Modify Delete Add Modify Delete Name / Host Name 192.168.75.113

#### 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).

VPN Connect	t - 192.168.75.113	
Connect Netwo	rk	
config loaded	for site 102 100 75 112	
coning roaded	IOF SILE 192.100.75.115	
Credentials		
Username	vpnuser	
Password	•••••	
	Connect	Evit
	Connect	Exit

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.