# 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:

Em VPN > Cliente a Site,

_		
Ð	VPN	
	VPN Status	
	IPSec Profiles	
	Site-to-Site	
C	Client-to-Site	2

# Passo 2

Adicionar um perfil de VPN Cliente a Site

٨	Getting Started	Client to Site			Apply	Cancel
G	Status and Statistics					
쓭	Administration	IPSec Client-to-Site Tunnels				^
٥	System Configuration					
0	WAN	<ul> <li>Image: Image: Im</li></ul>	WAN Interface 🗢	Authentication Method 🗢		
4	LAN					_
Ş	Wireless					
8	Routing					
	Firewall					
ē	I VPN					
	VPN Status					
	IPSec Profiles					
	Site-to-Site					
C	Client-to-Site 2					

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 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 Method</li> <li>Pre-shared Key:</li> <li>Minimum Pre-shared Key Complexity: Show Pre-shared Key:</li> </ul>	d •••••  Enable Enable

### 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.



# 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:	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:	Ø		
Split Tunnel Table			
+ 🕜 🛍			
☑ IP Address ≑			Netmask 🗘
☑ 192.168.1.0			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		
<ul> <li>+ 𝐼 m̂</li> <li>Group/Tunnel Name </li> </ul>	WAN Interface \$	Authentication Method 🗢
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.



Digite um nome de grupo.

Overview	v	
Group Name:	VPN	

# Passo 10

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

💿 altalta cisco	RV340W-router45	00E2	×
Llear Group	ç.		Add Feature List
User Group	5		Select a Profile Clients •
Overview	Ouenieu		
Overview			Add Cancel
Group Name: VPN	4		
Local User Mem	bership List		
# 0 Join 0	User Name \$	Joined Gr	oups* 0
1 0	cisco	admin	
2 🗆	guest	guest	
* Should have at lea	st one account in the " a	fmin" group	
Web Login/NETCON Site to Site VPN	IF/RESTCONF 💿 Disab	iled O Read Only	O Administrator
Site to Site VPN	Profile Member In-use	Table	
+ 🔒			
□ # \$ Con	nection Name 🌣		
EzVPN/3rd Party			
EzVPN/3rd Party	Profile Member In-use	Table	
+ 🔒			
□ # \$ Gro	up Name 🌣		

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



#### 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.

8	Getting Started	User Groups			
6	Status and Statistics				
쓭	Administration	User Groups Table			
۰	System Configuration	100			
	System	Group \$	Web Login/NETCONF/RESTCONF \$	S2S-VPN \$	EzVPN/3rd Party \$
	Time	U VPN	Disabled	Disabled	Clients
	Log		produced	DISOUTED	Gireinta
		admin	Admin	Disabled	Disabled
	Email	guest	Disabled	Disabled	Disabled
	User Accounts				

#### Passo 13

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



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	User Accounts				
Add User Acco	punt				
User Name	vpnuser				
New Password		( Range: 0 - 127 )			
New Password Confirm					
Group	VPN v				

# Etapa 15

O novo usuário aparecerá na lista de Usuários locais.

.00	al User	Membership List	
+	/ <b>⊘</b> # ≎	🔟 📥 User Name 🗢	Group * 🗢
	1	cisco	admin
	2	guest	guest
	3	vpnuser	VPN

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

VPN Site Cor	figuration		×	
General C	lient Name R	esolution Authen	tication P	
Remote Host       Host Name or IP Address       192.168.75.113       500				
Auto Co -Local Ho Adapte Use a	Auto Configuration ike config pull  Local Host  Adapter Mode  Use a virtual adapter and assigned address			
MTU 1380	) Address Netmask	Obtain Autor	natically	
		Save	Cancel	

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

VPN Site Configuration	X	
General Client Name Resolution	on 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 Not	fications	
📝 Enable Client Login Banner		
5	Gave Cancel	

# Etapa 3

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

VPN Site Configuration				
General Client Name Resolution 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			

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

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

# 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

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

# 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

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

# 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

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 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

PN Site Configuration	X			
Client Name Resolution	Authentication Phase 1 F			
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				

Também usaremos os padrões para a guia Fase 2:

# Algoritmo de transformação: Auto

Algoritmo HMAC: Auto

Troca de PFS: Desabilitado

# Comprimir algoritmo: Desabilitado

Name Resolution Authentication Phase 1 Phase 2				
Proposal Parameters				
Transform Algorithm auto				
Transform Key Length	Test Bits			
HMAC Algorithm	auto 🔻			
PFS Exchange	disabled 💌			
Compress Algorithm	disabled 🗸			
Key Life Time limit	3600 Secs			
Key Life Data limit	0 Kbytes			

#### 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**.

ſ	VPN Access Manager				
	File Edit, View Help				
	8	•	2	0	
	Connect	Add	Modify	Delete	
	Connectio	n Name	/ Hos	st Name	Authenticat
	192.168	.75.113	192	.168.75.113	mutual-psk

# 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).

VPN Connect	t - 192.168.75.113	_ <b>D</b> X		
Connect Network				
config loaded	for cito '192 168 75 113'			
comig roaded	IOT SILE 132.100.75.115			
Condentiale				
Credentials	Credentials			
Username	vpnuser			
Password	•••••			
	Connect	Evit		
		E.M.		

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.