Een zachte VPN-client configureren voor aansluiting op RV34X Series router

Doel

Het doel van dit document is om te tonen hoe u de Shrew Soft VPN-client kunt gebruiken om verbinding te maken met een RV340 Series router.

U kunt de nieuwste versie van de software van de Shrew Soft VPN-client hier downloaden:

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

Toepasselijke apparaten | Software versie

RV340 | 1.0.3.17 (laatste download)

RV340 W | 1.0.3.17 (laatste download)

RV345 | 1.0.3.17 (laatste download)

RV345P router | 1.0.3.17 (laatste download)

Inleiding / gebruik case

Met IPSec VPN (Virtual Private Network) kunt u veilig externe bronnen verkrijgen door een versleutelde tunnel via het internet op te zetten. De RV34X Series routers werken als IPSEC VPN-servers en ondersteunen de Shrew Soft VPN-client. Deze gids zal u tonen om uw router en de Zachte Cliënt van de Ruw te vormen om een verbinding met een VPN te verzekeren.

Dit document bestaat uit twee delen:

Het configureren van de RV340 Series router

De zachte VPN-client tonen

Configureer de RV34X Series router:

We beginnen met het configureren van het client-naar-site VPN op de RV34x

Stap 1

In VPN > Client-to-Site,

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

Stap 2

Een client-naar-site VPN-profiel toevoegen

٩	Getting Started	Client to Site			Apply	Cancel
6	Status and Statistics					
쓭	Administration	IPSec Client-to-Site Tunnels				~
٥	System Configuration					
0	WAN	Group/Tunnel Name +	WAN Interface 🗢	Authentication Method \$		
4	LAN					_
?	Wireless					
8	Routing					
	Firewall					
	I VPN					
	VPN Status					
	IPSec Profiles					
	Site-to-Site					
C	Client-to-Site 2					

Stap 3

Selecteer de optie Cisco VPN-client.



Stap 4

Controleer het vakje Inschakelen om het VPN-clientprofiel actief te maken. We zullen ook de *groepsnaam* configureren, de **WAN-interface** selecteren en een **vooraf gedeelde sleutel** invoeren.

Opmerking: Let op de *naam van de groep* en de *vooraf gedeelde sleutel* zoals deze later bij het configureren van de client wordt gebruikt.

Enable:	
Group Name:	Clients
Interface:	WAN1 ~
IKE Authentication Metho	d
 IKE Authentication Method Pre-shared Key: 	d •••••
 IKE Authentication Method Pre-shared Key: Minimum Pre-shared Key Complexity: 	d ••••• Enable
 IKE Authentication Method Pre-shared Key: Minimum Pre-shared Key Complexity: Show Pre-shared Key: 	d ••••• Enable Enable

Stap 5

Laat de lege **gebruikersgroep** voorlopig achter. Dit is voor de *Gebruikersgroep* op de router, maar we hebben deze nog niet ingesteld. Zorg ervoor dat de **modus** is ingesteld op **client**. Geef het **wolbereik voor clientadaptertools op**. We gebruiken 172.16.10.1 tot en met 172.16.10.10.

Opmerking: Het bereik van de pool zou een uniek Subnet moeten gebruiken dat niet elders op het netwerk gebruikt wordt.

User Group:	
User Group Table	
 	
Mode:	O NEM
Pool Range for Client LAN	
Start IP:	172.16.10.1
End IP:	172.16.10.10

Stap 6

Hier configureren we de instellingen van de **Mode Configuration**. Hier zijn de instellingen die we zullen gebruiken:

Primaire DNS-server: Als u een interne DNS-server hebt of een externe DNS-server wilt gebruiken, kunt u deze hier invoeren. Anders wordt de standaard ingesteld op het RV340 LAN IP-adres. We zullen het standaard gebruiken in ons voorbeeld.

Split-tunnel: Controleer om Split-tunneling in te schakelen. Dit wordt gebruikt om te specificeren welk verkeer via de VPN-tunnel gaat. In ons voorbeeld zullen we Split Tunnel gebruiken.

Tabel splitsen: Voer de netwerken in waarop de VPN-client toegang heeft via VPN. Dit voorbeeld gebruikt het RV340 LAN-netwerk.

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:	 <i>∎</i>		
Split Tunnel Table			
+ 🕜 💼			
IP Address ≑			Netmask 🗢
192.168.1.0			255.255.255.0

Stap 7

Nadat u op Opslaan hebt geklikt, kunt u het profiel zien in de lijst IPSec client-to-site groepen.

Client to Site		
IPSec Client-to-Site Tunnels		
+ ☞ m □ Group/Tunnel Name ≑	WAN Interface 🗢	Authentication Method \$
Clients	WAN1	Pre-shared Key

Stap 8

We zullen nu een **gebruikersgroep** configureren voor het verificeren van VPN-clientgebruikers. In **systeemconfiguratie > Gebruikersgroepen** klikt u op **"+"** om een gebruikersgroep toe te voegen.



Voer een groepsnaam in.

Overview		
Group Name:	VPN	

Stap 10

In het gedeelte **Services > EzVPN/3rd Party**, klikt u op **Add** om deze gebruikersgroep te koppelen aan het **client-to-site** profiel dat we eerder hebben geconfigureerd.

RV340W-router4500E2	
- cisco	Add Feature List
User Groups	
	Select a Profile Clients •
Overview	Add
Group Name: VPN	
Local User Membership List	
# ¢ Join ¢ User Name ¢	Joined Groups * 0
	admin
2 🗆 guest	guest
Services Web Login/NETCONF/RESTCONF @ Disabled O I Site to Site VPN Site to Site VPN Profile Member In-use Table	Read Only O Administrator
1.0	
# Connection Name	
EzVPN/3rd Party	
EzVPN/3rd Party Profile Member In-use Table	
EzVPN/3rd Party Profile Member In-use Table	

U dient de naam van de client-to-site groep nu in de lijst voor EzVPN/3rd te zien



Stap 12

Nadat u de configuratie van de gebruikersgroep **toepast**, ziet u het in de lijst **Gebruikersgroepen** en de nieuwe gebruikersgroep wordt gebruikt met het client-naar-site profiel dat we eerder hebben gemaakt.

⊗ �	Getting Started Status and Statistics	User Groups			
*	Administration	User Groups Table			
۰	System Configuration	+ (2 A			
	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				

Stap 13

We configureren nu een nieuwe gebruiker in **systeemconfiguratie** > **Gebruikersrekeningen**. Klik op "+" om een nieuwe gebruiker te maken.



Voer de nieuwe **gebruikersnaam** in samen met het **nieuwe wachtwoord**. Controleer dat de **groep** is ingesteld op de nieuwe **gebruikersgroep** die we zojuist hebben ingesteld. Klik op **Toepassen** na voltooiing.

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

Stap 15

De nieuwe gebruiker verschijnt in de lijst met lokale gebruikers.

	· 🚓 🕹	
- ⊡)#≑	User Name 🗢	Group * 🗢
1	cisco	admin
2	guest	guest
3	vpnuser	VPN

Dit voltooit de configuratie op de RV340 Series router. We zullen nu de Shrew Soft VPN-client configureren.

De ShrewSoft VPN-client configureren

We zullen nu de Shrew Soft VPN-client configureren.

Stap 1

Open de ShrewSoft *VPN Access Manager* en klik op **Add** om een profiel toe te voegen. In het venster *VPN Site Configuration* dat nu wordt weergegeven, configureren u het **tabblad General**:

Hostnaam of IP-adres: Gebruik het WAN IP-adres (of hostname van RV340)

Automatische configuratie: Selecteer NetPlooster

Adapter-modus: Selecteer Gebruik een virtuele adapter en toegewezen adres

VPN Site Configur	ation			×	
General Client	Name Res	olution	Authent	ication P · ·	
Remote Host Host Name or IP Address 192.168.75.113 Auto Configuration ke config pull					
Local Host Adapter Mode Use a virtual adapter and assigned address					
MTU 1380	V Obte	ain Auton			
Save Cancel					

Configuratie van het tabblad Client We gebruiken gewoon de standaardinstellingen.

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					
Enable ISAKMP Failure Notifications					
🔽 Enable Client Login Banner					
s	ave Cancel				

Stap 3

In het tabblad **Name Solutions > DNS**, controleert u het dialoogvenster **DNS** inschakelen en laat u de**optie Automatisch** selecteren los.

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

In het tabblad **Naam > WINS**, controleert u het dialoogvenster **WINS** inschakelen en laat u het vakje Automatisch **verkrijgen** controleren.

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

Stap 5

Configuratie van het tabblad Verificatie > tabblad Local Identity:

Identificatietype: Selecteer Key Identifier

Belangrijkste ID-string: Voer de groepsnaam in die op de RV34x is ingesteld

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	

In het tabblad **Verificatie > Remote Identity**, blijven we de standaardinstellingen behouden.

Identificatietype: IP-adres

Adres: <blanco>

Gebruik een ontdekt veld adres op afstand: gecontroleerd

VPN 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			

Stap 7

In het tabblad Verificatie > Credentials, dient u het volgende te configureren:

Verificatiemethode: Selecteer Wederom PSK + XAuth

Vooraf gedeelde sleutel: Voer de vooraf gedeelde sleutel in die is ingesteld in het RV340clientprofiel

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			

In het tabblad Fase 1 laten we de standaardinstellingen staan:

Exchange type: agressief

DH Exchange: groep 2

algoritme gebruiken: Automatisch

Hash Algoritme Automatisch

VPN Site Configuration			
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		

We gebruiken ook de standaardinstellingen voor het tabblad Fase 2:

Algoritme omzetten Automatisch

HMAC-algoritme: Automatisch

PFS-uitwisseling: Uitgeschakeld

Algoritme compressie: Uitgeschakeld

Name Resolution Authentication Phase 1 Phase 2			
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		

Stap 10

In het tabblad **Beleids** gebruiken we de volgende instellingen:

Beleidsgeneratieniveau: Automatisch

Blijvende beveiligingsassociaties behouden: gecontroleerd

Zorg voor automatisch of tunnelkenmerken: gecontroleerd

Aangezien we het **Split-Tunneling** hebben ingesteld op de RV340, hoeven we het hier niet te configureren.



Klik na voltooiing op Opslaan.

Stap 11

We zijn nu klaar om de verbinding te testen. In *VPN Access Manager* kunt u het verbindingsprofiel markeren en op de knop **Connect** klikken.

	VPN Access Manager				
-	File Edit, View Help				
	8	•	2	0	
	Connect	Add M	Modify	Delete	
Ì	Connection Name /		Ho:	st Name	Authenticat
	🚯 192.168	.75.113	192	.168.75.113	mutual-psk

Stap 12

Voer in het venster **VPN Connect** dat nu verschijnt de **gebruikersnaam** en het **wachtwoord in** met behulp van de **gebruikersaccount** die we op RV340 hebben gemaakt (stap 13 en 14).

S VPN Connect - 192.168.75.113				
Connect Network				
config loaded				
coning roaded	IOF SILE 192.100.75.115			
Credentials				
Username	Username vpnuser			
Password	•••••			
	Connect	Evit		
	Connect	EXA		

Klik na voltooiing op Connect.

Stap 13

Controleer of de tunnel is aangesloten. Je zou tunnel moeten zien ingeschakeld.



Conclusie

Daar is het, u bent nu ingesteld om verbinding te maken met uw netwerk via VPN.