Configuration du client VPN logiciel Shrew pour la connexion au routeur de la gamme RV34X

Objectif

L'objectif de ce document est de montrer comment utiliser le client VPN logiciel Shrew pour se connecter à un routeur de la gamme RV340.

Vous pouvez télécharger la dernière version du logiciel client VPN Shrew Soft ici :

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

Périphériques pertinents | Version du logiciel

RV340 | 1.0.3.17 (Télécharger la dernière version)

RV340W | 1.0.3.17 (Télécharger la dernière version)

RV345 | 1.0.3.17 (Télécharger la dernière version)

RV345P | 1.0.3.17 (Télécharger la dernière version)

Introduction/Cas d'utilisation

Le VPN IPSec (Virtual Private Network) vous permet d'obtenir des ressources distantes en toute sécurité en établissant un tunnel crypté sur Internet. Les routeurs de la gamme RV34X fonctionnent comme des serveurs VPN IPSEC et prennent en charge le client VPN logiciel Shrew. Ce guide vous indique comment configurer votre routeur et le client logiciel Shrew pour sécuriser une connexion à un VPN.

Ce document comporte deux parties :

Configuration du routeur de la gamme RV340

Configurer le client VPN logiciel Shrew

Configurez le routeur de la gamme RV34X :

Nous commencerons par configurer le VPN client à site sur le RV34x

Étape 1

Dans VPN > Client-to-Site,

_		_
Ð	VPN	1
	VPN Status	
	IPSec Profiles	
	Site-to-Site	
C	Client-to-Site	2

Étape 2

Ajouter un profil VPN client à site

@ (}	Getting Started	Client to Site			Apply	Cancel
*	Administration	IPSec Client-to-Site Tunnels				^
¢ و	System Configuration WAN	Company Turnel Name A	WAN Interface A	Authentication Mathod A		
4	LAN					_
ন্থ জ	Wireless Routing					
	Firewall					
₽	VPN 1					
	IPSec Profiles					
C	Site-to-Site					

Étape 3

Sélectionnez l'option Client VPN Cisco.



Étape 4

Cochez la case **Enable** pour activer le profil de client VPN. Nous allons également configurer le *nom de groupe*, sélectionner l'**interface WAN** et saisir une **clé prépartagée**.

Note: Notez le *nom du groupe* et la *clé pré-partagée* car ils seront utilisés ultérieurement lors de la configuration du client.

Enable:					
Group Name:	Clients				
Interface:	WAN1 ~				
IKE Authentication Method					
IKE Authentication Metho	d				
IKE Authentication MethodPre-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				

Étape 5

Laissez la **table Groupe d'utilisateurs** vide pour le moment. Il s'agit du *groupe d'utilisateurs* sur le routeur, mais nous ne l'avons pas encore configuré. Assurez-vous que le **mode** est défini sur **Client**. Entrez la **plage de pools pour le réseau local du client**. Nous utiliserons 172.16.10.1 à 172.16.10.10.

Note: La plage de pools doit utiliser un sous-réseau unique qui n'est pas utilisé ailleurs sur le réseau.

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

Étape 6

Voici où nous configurons les paramètres **de configuration du mode**. Voici les paramètres que nous allons utiliser :

Serveur DNS principal : Si vous avez un serveur DNS interne ou souhaitez utiliser un serveur DNS externe, vous pouvez le saisir ici. Sinon, la valeur par défaut est l'adresse IP LAN RV340. Nous utiliserons la valeur par défaut dans notre exemple.

Tunnel fractionné : Cochez cette case pour activer la tunnellisation fractionnée. Ceci est utilisé pour spécifier le trafic qui passera par le tunnel VPN. Nous allons utiliser le tunnel partagé

dans notre exemple.

Table de tunnel partagée : Entrez les réseaux auxquels le client VPN doit avoir accès via le VPN. Cet exemple utilise le réseau local 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

Étape 7

Après avoir cliqué sur **Enregistrer**, nous pouvons voir le profil dans la liste **Groupes client à site IPSec**.

Client to Site		
IPSec Client-to-Site Tunnels		
 	WAN Interface 🗢	Authentication Method 🗢
Clients	WAN1	Pre-shared Key

Étape 8

Nous allons maintenant configurer un **groupe d'utilisateurs** à utiliser pour authentifier les utilisateurs du client VPN. Dans **Configuration du système > Groupes d'utilisateurs**, cliquez sur **'+'** pour ajouter un groupe d'utilisateurs.



Entrez un nom de groupe.

Overviev	v	
Group Name:	VPN	

Étape 10

Dans la section **Services > EzVPN/tiers**, cliquez sur **Ajouter** pour lier ce groupe d'utilisateurs au **profil client-site** que nous avons configuré précédemment.

Add Feature List Overview Coup Name: VPN Loal User Nembership List # 0 Joined Groups * 0 1 acco active 2 apped acco active * Should have at least one account in the "active" group Services Web Login/NETCONF/RESTOONE* © Deabled © Read Only © Administrator Size to Size VPN Size to Size VPN EXPNV3cd Party EXPNV3cd Party Profile Member In-use Table + @	8	dialia	RV340W-router	1500E2		
User Groups Overview Group Name: VPN Group Name: VPN Group Name: VPN Group Name: Conset Group Name: Conset Conset					Add Feature List	
Overview	User	Group	IS		Salart a Droffer Claute	
CVERVIEW Group Name VPN Cocal User Membership List	0					
Group Name: VPN	Over	view			Add Cancel	
Local User Membership List # 0 Joined Groups * 0 1 Gloco Joined Groups * 0 2 guest guest * Should have at least one account in the " admin" group Services Web Login/NETIONF/RESTONF © Deabled © Read Only © Administrator Size to Size VFN Size to Size VFN Size to Size VFN ExtMVIcid Party ExtMVIcid Party ExtMVIcid Party Profile Member in-use Table + @ - @ Group Name *	Group Na	ame: VPf	N			
Image: Solid Provide Member In-use Table	Local	User Merr	bership List			
1 0 cloco admin 2 0 quant quant * Should have at least one account in the " admin" group Services Web Login/NETCONF/RESTOONF © Deabled © Read Drivy © Administrator Site to Site VPN Site to Site VPN Site to Site VPN Site to Site VPN Fill # © Connection Name © EXMPN2id Party EXMPN2id Party Profile Member In-use Table + @ - # 0 - # 0 - # 0 - # 0 - # 0 - # 0 - # 0 - # 0 - # 0 - # 0 - # 0	# 0	Join ¢	User Name \$	Joined Gr	Groups * ¢	
	1		cisco	admin		
* Should have at least one account in the * admin* group Services Web Login/NETCONF/RESTOONF © Deabled © Read Only © Administrator Ser to Site VPN Site to Site VPN Site to Site VPN Site to Site VPN EVPN3rd Ramy EVPN3rd Ramy EVPN3rd Ramy Profile Member in-use Table	2		guest	guest		
EXPINISH Party EXPINISH EXPINISH Party EXPINISH EXPINISH Party EXPINISH E	Servi Web Log Site to Si	COS in/NETCOP ite VPN	NF/RESTCONF Dis	abled O Read Only	O Administrator	
B Connection Name EXVPNU3d Party EXVPNU3d Party Profile Member In-use Table B B Group Name C	340 10		Profile Methoer In-u:	ie rabie		
EXPRV3rd Party EXPRV3rd Party Profile Member In-use Table	+	🗏 II 🗢 Cor	nnection Name 🗢			
EX/PN/3rd Party Profile Member In-use Table	EzVPN/3	rd Party				
+ 🔒	EzVPN	I/3rd Party	y Profile Member In-u	se Table		
	+	i∰ #≎ Gro	oup Name 🌣			

Vous devriez maintenant voir le nom du groupe client-site dans la liste pour EzVPN/tiers



Étape 12

Après avoir **appliqué** la configuration du groupe d'utilisateurs, vous la verrez dans la liste **Groupes d'utilisateurs** et vous verrez que le nouveau groupe d'utilisateurs sera utilisé avec le profil clientsite que nous avons créé précédemment.

8	Getting Started	User Groups	3		
6	Status and Statistics				
*	Administration	User Groups Tabl	e		
۰	System Configuration				
	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				

Étape 13

Nous allons maintenant configurer un nouvel utilisateur dans **Configuration système > Comptes** d'utilisateurs. Cliquez sur '+' pour créer un nouvel utilisateur.



Entrez le nouveau **nom d'utilisateur** ainsi que le **nouveau mot de passe**. Vérifiez que le **groupe** est défini sur le nouveau **groupe d'utilisateurs** que nous venons de configurer. Cliquez sur **Apply** lorsque vous avez terminé.

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

Étape 15

Le nouvel utilisateur apparaîtra dans la liste des utilisateurs locaux.

• •	× 📾 🔸	
] #	¢ User Name ≎	Group * 🗢
) 1	cisco	admin
2	guest	guest
3	vpnuser	VPN

La configuration du routeur de la gamme RV340 est terminée. Nous allons maintenant configurer le client VPN logiciel Shrew.

Configurer le client VPN ShrewSoft

Nous allons maintenant configurer le client VPN logiciel Shrew.

Étape 1

Ouvrez le *Gestionnaire d'accès VPN* ShrewSoft et cliquez sur **Ajouter** pour ajouter un profil. Dans la fenêtre *Configuration du site VPN* qui s'affiche, configurez l'onglet **Général** :

Nom d'hôte ou adresse IP : Utiliser l'adresse IP WAN (ou le nom d'hôte du routeur RV340)

Configuration automatique : Sélectionner comme configuration pull

Mode adaptateur : Sélectionnez Utiliser une carte virtuelle et l'adresse attribuée

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

Configurez l'onglet **Client**. Nous utiliserons simplement les paramètres par défaut.

VPN Site Configuration				
General Client Name Resolution	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 Notifications				
🔽 Enable Client Login Banner				
s	ave Cancel			

Étape 3

Dans l'onglet **Résolution de noms > DNS**, cochez la case **Activer DNS** et laissez les cases **Obtenir automatiquement** cochées.

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				
DNS Suffix	Obtain Automatically			
	Save Cancel			

Dans l'onglet **Résolution de noms > WINS**, cochez la case **Activer WINS** et laissez la case **Obtenir automatiquement** cochée.

VPN Site Configuration				
General Client Name Resolution Authentication	n P 🔸 🕨			
DNS WINS				
Enable WINS 📝 Obtain Automatical	ly			
Server Address #1				
Server Address #2				
Save	Cancel			

Étape 5

Configurez l'onglet Authentification > Identité locale :

Type d'identification : Sélectionner l'identificateur de clé

Chaîne d'ID de clé : Entrez le nom du groupe configuré sur le 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				
Clients				
Save Ca	ancel			

Dans l'onglet **Authentification > Identité distante**, nous laisserons les paramètres par défaut.

Type d'identification : Adresse IP

Chaîne d'adresses : <vierge>

Utilisez une zone d'adresse d'hôte distant découverte : Coché

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			

Étape 7

Dans l'onglet Authentification > Informations d'identification, configurez les éléments suivants :

Méthode d'authentification : Sélectionner PSK mutuel + XAuth

Clé pré-partagée : Entrez la clé prépartagée configurée dans le profil client 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				

Pour l'onglet Phase 1, les paramètres par défaut restent en place :

Type d'échange : Agressif

Échange DH : groupe 2

Algorithme de chiffrement : « Auto »

Algorithme de hachage : « Auto »

VPN Site Configuration			
Client Name Resolution A	uthentication 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		

Nous utiliserons également les valeurs par défaut de l'onglet Phase 2 :

Algorithme de transformation : « Auto »

Algorithme HMAC : « Auto »

Échange PFS : Désactivé

Algorithme de compression : Désactivé

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

Étape 10

Pour l'onglet Stratégie, nous utiliserons les paramètres suivants :

Niveau de génération de stratégie : « Auto »

Tenir À Jour Les Associations De Sécurité Persistantes : Coché

Obtenir la topologie automatiquement ou Tunnel All : Coché

Puisque nous avons configuré la **tunnellisation partagée** sur le RV340, nous n'avons pas besoin de le configurer ici.



Une fois terminé, cliquez sur Save (enregistrer).

Étape 11

Nous sommes maintenant prêts à tester la connexion. Dans *VPN Access Manager*, mettez en surbrillance le profil de connexion et cliquez sur le bouton **Connect**.

O 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

Étape 12

Dans la fenêtre **VPN Connect** qui apparaît, entrez le **nom d'utilisateur** et le **mot de passe** à l'aide des informations d'identification du **compte d'utilisateur** que nous avons créé sur le RV340 (étapes 13 et 14).

S VPN Connect - 192.168.75.113					
Connect Network					
config loaded					
coning loaded	IOF SILE 192.100.75.113				
Credentials	Credentials				
Username	vpnuser				
Password	•••••				
	Convert	5.4			
	Connect	Exit			

Lorsque vous avez terminé, cliquez sur Connect.

Étape 13

Vérifiez que le tunnel est connecté. Le tunnel doit être activé.



Conclusion

Là, vous êtes maintenant configuré pour vous connecter à votre réseau via VPN.