配置Shrew Soft VPN客戶端連線到RV34X系列路 由器

目標

本文檔旨在展示如何使用Shrew Soft VPN客戶端連線到RV340系列路由器。

您可以在以下位置下載最新版本的Shrew Soft VPN客戶端軟體:

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

適用裝置 |軟體版本

RV340 | 1.0.3.17 <u>(下載最新版本)</u>

RV340W | 1.0.3.17(下載<u>最新版</u>)

RV345 | 1.0.3.17(下載<u>最新版</u>)

RV345P | 1.0.3.17(下載<u>最新版</u>)

簡介/使用案例

IPSec VPN(虛擬專用網路)允許您通過網際網路建立加密隧道來安全地獲取遠端資源。RV34X系列路由器充當IPSEC VPN伺服器,支援Shrew Soft VPN客戶端。本指 南將向您展示如何配置您的路由器和軟體客戶端,以確保與VPN的連線。

本文檔包含兩部分:

配置RV340系列路由器

配置Show Soft VPN客戶端

配置RV34X系列路由器:

我們首先在RV34x上配置客戶端到站點VPN

在VPN > Client-to-Site中,



步**驟**2

新增**客戶端到站點VPN配**置檔案

	Getting Started	Client to Site					Annaly	Canaal
Ģ	Status and Statistics						Афріу	Caricer
쓭	Administration	IPSec Client-to-Site Tunnel	Is					~
٥	System Configuration							
0	WAN	Group/Tunnel Name 🖨		WAN Interface 🗢	,	Authentication Method \$		
4	LAN							_
?	Wireless							
R	Routing							
	Firewall							
Ē	I VPN							
	VPN Status							
	IPSec Profiles							
	Site-to-Site							
C	Client-to-Site 2							

步驟3

選擇Cisco VPN Client選項。



步驟4

選中Enable框以啟用VPN客戶端配置檔案。我們還將配置*組名稱*,選擇WAN介面,然後輸入預共用 **金鑰**。

附註:請記下Group Name和Pre-shared Key,因為它們將在以後配置客戶端時使用。

Enable:	
Group Name:	Clients
Interface:	WAN1 ~
IKE Authentication Method	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

暫時將**使用者組表**留空。這是用於路由器上的*使用者組*,但我們尚未對其進行配置。確保Mode設定 為Client。輸入客戶端LAN的池範圍。我們將使用172.16.10.1到172.16.10.10。

附註:池範圍應使用網路中其它位置未使用的唯一子網。

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

步驟6

此處我們配置模式配置設定。以下是我們將使用的設定:

主DNS伺服器:如果您有內部DNS伺服器或想要使用外部DNS伺服器,可以在此處輸入該伺服器 。否則,預設設定為RV340 LAN IP地址。我們將使用示例中的預設值。

拆分隧道:選中可啟用分割隧道。這用於指定哪些流量將通過VPN隧道。在我們的示例中,我 們將使用拆分隧道。

拆分隧道表:輸入VPN客戶端通過VPN有權訪問的網路。此示例使用RV340 LAN網路。

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

第7步

按一下Save後,我們可以在IPSec Client-to-Site Groups清單中看到配置檔案。

Client to Site						
IPSec Client-to-Site Tunnels						
 + 𝐼 iii Group/Tunnel Name ≑ 	WAN Interface 🗢	Authentication Method 🗢				
Clients	WAN1	Pre-shared Key				

步驟8

我們現在將配置用**於驗證**VPN客戶端使用者的使用者組。在System Configuration > User Groups中 ,按一下'+'以新增使用者組。



輸入組**名稱**。

Overviev	V	
Group Name:	VPN	

步驟10

在「Services」部分> EzVPN/**第**3方中,按一下Add將此使用者組連結到我們之前配置的Client-to-Site配置檔案。

Ø	cisco	RV340W-router45	500E2	×
User (Groups	3		Add Feature List
				Select a Profile Clients •
Overv	view			
Group Na	mer VPN			Add Cancel
Circop rite				
Local U	Jser Mernt	pership List		
	Join ¢	User Name ¢	Joined Gr	xups * 0
1		cisco	admin	
2		guest	guest	
Servic Web Logi Site to Sit	C OS n/NETCON e VPN	F/RESTCONF O Disa	bled O Read Only	O Administrator
Site to	Site VPN P	Profile Member In-use	Table	
+ 1				
	¢ Con	nection Name		
EzVPN/30	d Party			
EzVPN/3n	d Party /3rd Party	Profile Member In-us	e Table	
E2VPN/3n	d Party /3rd Party	Profile Member In-use	a Table	

步驟11

現在,您應該會看到**EzVPN/第3方**的清單中的客戶端**到站點組名稱**

EzVPN/3rd Party							
EzVPN/3rd Party Profile Member In-use Table							
+ 🖮	∔ ⋒						
□ # ≑	Group Name 🗢						
□ 1	Clients						

步驟12

Apply User Group配置後,您將在**User Groups**清單中看到它,它將顯示新的使用者組將與我們之前建立的客戶端到站點配置檔案一起使用。

⊗ ⊛	Getting Started Status and Statistics	User Groups						
*	Administration User Groups Table							
Ť	System	+ 🗭 📋 □ Group ≎	Web Login/NETCONF/RESTCONF \$	S2S-VPN ¢	EzVPN/3rd Party 🕈			
	Time	O VPN	Disabled	Disabled	Clients			
	Log	admin	Admin	Disabled	Disabled			
	Email User Accounts	guest	Disabled	Disabled	Disabled			
	User Groups							

現在,我們將在System Configuration > User Accounts中配置新的使用者。按一下「+」以建立新 使用者。

ocal L	Jser N	lembership List	
+0	3 🛍	*	
U #	÷	User Name ≑	Group * ♥
UI		CISCO	admin
		auest	guest

步驟14

輸入新**使用者名稱**和**新密碼**。驗證是否已將Group設定為我們剛配**置的新**使用者組。完成後按一下 Apply。



步驟15

新使用者將顯示在**本地使用者**清單中。

Local User Membership List				
+ 0				
□ #	User Name \$	Group * 🗢		
0 1	cisco	admin		
□ 2	guest	guest		
□ 3	vpnuser	VPN		

這樣即可完成RV340系列路由器的配置。我們現在將配置Shrew Soft VPN客戶端。

配置ShrewSoft VPN客戶端

我們現在將配置Shrew Soft VPN客戶端。

步驟1

開啟ShareSoft VPN訪*問管理器*,然後點選**Add**以新增配置檔案。在出現的*VPN Site Configuration* 視窗中,配置**General**頁籤:

主機名或IP地址:使用WAN IP地址(或RV340的主機名)

自動配置:選擇ike config pull

介面卡模式:選擇使用虛擬介面卡和分配的地址

PN Site Configu	iration			X		
General Client	Name Res	olution	Authent	ication P · ·		
Remote Hos	t					
Host Name or IP Address Port						
192.168.75.113 500						
Auto Configuration ike config pull						
Local Host						
Adapter Mo	de					
Use a virtu	al adapter and	assigne	ed addre	ss 🔻		
MTU		🔽 Obta	ain Auton	natically		
1380	Address					
	Netmask					
		Sav	/e	Cancel		

配置Client頁籤。我們將僅使用預設設定。

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			

步驟3

在Name Resolution頁籤> DNS頁籤中,選中Enable DNS覈取方塊,並保留Obtain Automatically覈 取方塊。

VPN Site Configuration	X			
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			
	Cancer			

步驟4

在Name Resolution頁籤> WINS頁籤中,選中Enable WINS覈取方塊,並保留Obtain Automatically 覈取方塊。

VPN Site Configuration				
General Client Name Re	solution Authentic	ation P 🔹 🕨		
DNS WINS				
Enable WINS	🔽 Obtain Automat	ically		
Server Address #1				
Server Address #2				
	Save	Cancel		

配置Authentication頁籤> Local Identity頁籤:

標識型別:選擇金鑰識別符號

金鑰ID字串:輸入在RV34x上配置的Group Name

PN 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 Cancel				

步**驟**6

在Authentication頁籤> Remote Identity頁籤中,我們將保留預設設定。

標識型別:IP 位址

使用發現的遠端主機地址框:已檢查

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				

第7步

在Authentication頁籤> Credentials頁籤中,配置以下內容:

身份驗證方法:選擇Mutual PSK +擴展驗證

預共用金鑰:輸入RV340客戶端配置檔案中配置的預共用金鑰

PN 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			
De Obere differe			
Pre Snared Kev			
Save Cancel			
Save Calicel			

步驟8

對於Phase 1頁籤,我們將保留預設設定:

Exchange型別:積極

密碼演算法:自動

雜湊演算法:自動

VPN Site Configuration				
Client Name Resolution Authentication Phase 1				
- Proposal Pa	rameters			
Exchange 7	Гуре	aggressive	-	
DH Exchan	ge	group 2	-	
Cipher Algo	orithm	auto	-	
Cipher Key	Length	•	Bits	
Hash Algor	ithm	auto	-	
Key Life Tin	ne limit	86400	Secs	
Key Life Da	ta limit	0	Kbytes	
Enable Check Point Compatible Vendor ID				
Save Cancel				

步驟9

我們還將使用Phase 2頁籤的預設值:

轉換演算法:自動

HMAC演算法:自動

PFS交換:已禁用

壓縮演算法:已禁用

VPN Site Configuration	tion Phase 1 Phase 2
Proposal Parameters	
Transform Algorithm Transform Key Length	auto ▼ ▼ Bits
HMAC Algorithm	auto 💌
PFS Exchange	disabled 🔹
Compress Algorithm	disabled 🔹
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
(Save Cancel

對於Policy頁籤,我們將使用以下設定:

策略生成級別:自動

維護持久安全關聯:已檢查

自動獲取拓撲或建立所有隧道:已檢查

由於我們在RV340上配置了**Split-Tunneling**,因此不需要在此處進行配置。

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
IPSEC Policy Configuration
Policy Generation Level auto
Maintain Persistent Security Associations
Obtain Topology Automatically or Tunnel All
Remote Network Resource
Add Modity Delete
Save Cancel
Save Cancel

完成後,按一下Save。

現在已準備好測試連線。在*VPN Access Manager*中,突出顯示連線配置檔案,然後按一下**Connect** 按鈕。

0	O VPN Access Manager					
File	e Edit	View	Help			
	8	•	2	0		
Co	nnect	Add	Modify	Delete		
Со	nnectio	n Name	/ Hos	st Name	Auther	ticat
•	192.168	.75.113	192	.168.75.113	mutual	-psk

步驟12

在出現的VPN Connect視窗中,使用在RV340上建立的**使用者帳戶**的憑證輸入Username和 Password(步驟13和14)。

VPN Connect	t - 192.168.75.113				
Connect Network					
config loaded	for site 102 100 7E 112				
coning loaded	IOF SILE 192.100.75.113				
Credentials					
Username	vpnuser				
Password	•••••				
	Connact	Evit			
	Connect	Exit			

完成後,按一下**「Connect**」。

步驟13

驗證通道是否已連線。您應該會看到通道已啟用。

VPN Connect	t - 192.168.75.113	
Connect Netwo	rk	
local id configu remote id configu pre-shared key bringing up tun network device tunnel enabled	ured igured y configured nel e configured	•
Credentials		
Username	vpnuser	
Password		
	Disconnect	Cancel

結論

在這裡,您現在設定為通過VPN連線到您的網路。